

OmniAccess 700 CLI Configuration Guide

Release 2.2



26801 West Agoura Road

Calabasas, CA 91301

(818) 880-3500

FAX (818) 880-3505

support@ind.alcatel.com

US Customer Support—(800) 995-2696

International Customer Support—(818) 878-4507

Internet—service.esd.alcatel-lucent.com

Website: www.alcatel-lucent.com

Copyright

The Specifications And Information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE.

This equipment has been tested and found to comply within the limits pursuant to the (Centre for Telecom) rules. These limits are designed to provide protection against harmful interference when the equipment is operated in a commercial environment.

The following information is for the Users of the OmniAccess 700: If it is not installed in accordance with the installation instructions, it may not function exactly to the said specifications. Modifying the equipment without Alcatel-Lucent's written authorization may result in the equipment no longer complying with the said dimensions.

Copyright © 2007, Alcatel-Lucent. All rights reserved. Alcatel-Lucent and Alcatel-Lucent logo are registered trademarks of Alcatel-Lucent. The contents or specifications contained within this document are subject to change without notice.

Notwithstanding any other warranty herein, all hardware and software are provided "as is" with all faults. Alcatel-Lucent disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and non-infringement or arising from a course of dealing, usage, or trade practice. In no event shall Alcatel-Lucent be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Alcatel-Lucent have been advised of the possibility of such damages.

Table of Contents

1 Preface	1
About This Guide	1
Audience	1
Organization	2
Part I - Introduction	2
Part II - LAN Interfaces	2
Part III- WAN Interfaces	3
Part IV - Packet Classification	4
Part V - Routing Protocols	4
Part VI - Network Security CLI	5
Part VII - Quality Of Service	5
Part VIII - TCP/IP Services	6
Part IX - Lifeline (Dedicated Management Framework)	6
Document Conventions	7
Obtaining Documentation	8
Reference Publications	8
Obtaining Technical Assistance	9
Documentation Feedback	9

Part 1: Introduction

2 The Command Line Interface	13
CLI Overview	13
Introduction to CLI Modes	14
CLI User Mode	14
CLI Configuration Mode	14
CLI Sub-Configuration Mode (SCM)	14
CLI Modes	15
User Mode (UM)	17
Super User Mode (SUM)	18
Example	18
Configuration Mode (CM)	20
Interface Configuration Mode (ICM)	23
Sub-Interface Configuration Mode (S-ICM)	24
Router Configuration Mode (RCM)	25
Exiting Configuration Modes	25
Initial Setup	26
Using the Command Line Interface	27
CLI Help	27
Partial Help	30
Partial Commands	30
Command Line Editing	31

Command History	33
Configuring Interfaces	34
Interface Configuration Commands	34
Interface Types and Limitations	34
Common Interface Configuration Commands	34
Interface Show Commands	35
Clear Interface Commands	39
Shutting Down and Bring Up an Interface	39
Backup Interface	40
3 System Configuration and Monitoring	43
System Configuration and Monitoring Tasks	43
Chapter Conventions	43
Management Plane Overview	44
Out of Band Management (Console or Modem)	44
Inband Management (SSH and Telnet)	46
Idle Timeout	48
Example	48
Ping	49
Example	49
Traceroute	52
Example	52
Terminal Settings	55
Example	55
System Name	55
Example	55
AAA Configuration on OA-700	56
To Enable AAA Services	56
Example	56
Authentication Commands	57
Show Commands	73
Setting and Displaying the System Time and Date	75
Clock Set	76
Example	76
Clock Synchronize	77
Example	77
System Logging and Debugging	78
Example	79
Example 1	80
Example 2	81
Example 3	81
Example 4	81
Rate Limiting in Statlog	82
Example 1	83
Example 2	83
Example 3	83

Saving Log Messages	84
Example	84
Viewing Tech Support	85
Example	85
The File System	86
Example 1	86
Example 2	87
Copying Files	87
Example	87
Deleting Files	88
Example	88
Configuration File Management	88
Software Package Management	97
Package Types	97
Reloading the System	102
Example	102
Managing Individual Slots	103
Example	103
System Monitoring and Troubleshooting	104
Environmental Information	104
Example	104
System Hardware Information	106
Example	106
System Status	108
Example	108
To View the Current State Of LEDs	109
Example	109
To View Process Information	110
Example	110
Memory Information	111
Example	111
SNMP (Simple Network Management Protocol)	112
SNMP Basics	112
SNMP Agent and Manager	113
Example	115
SNMP Version	116
Example	116
SNMP Show Commands	117
SNMP MIB CLI	118
SNMP MIB GUI	119
4 Virtual Router Redundancy Protocol	121
Chapter Organization	121
Chapter Conventions	121
VRRP Overview	122
VRRP Configuration	123

VRRP Configuration Steps	123
VRRP Configuration Flow.....	124
VRRP CLI Commands.....	125
Modify Global VRRP Group Parameters	128
Monitor and Debug VRRP	132
VRRP Interface Tracking	134
Alcatel-Lucent's Interface Tracking Design	134
VRRP Configuration Scenario using OA-700.....	136
Procedure	136
VRRP Configuration	137

Part 2: LAN Interfaces and Configuration

5 Ethernet Interfaces on SE.....	141
Chapter Conventions	141
Ethernet Overview.....	142
Ethernet Basics	142
Ethernet Terminologies	143
Switched Ethernet	144
Full-duplex Ethernet	144
Alcatel-Lucent Specific Overview on Ethernet Interfaces.....	144
Ethernet Configuration	145
Ethernet Interface Configuration Steps	145
Ethernet Interface Configuration Flow	146
Ethernet Interface Configuration Commands	147
Ethernet Interface Show Commands.....	149
Ethernet Interface Clear Commands	152
6 Layer 2 Switching Configuration	153
Chapter Conventions.....	153
Switching Overview.....	154
Alcatel-Lucent Specific Overview on Switching.....	156
L2 Switching Configuration	158
L2 Switching Configuration Steps.....	158
L2 Switching Configuration Flow	160
L2 Switching Commands.....	161
L2 Switching Show Commands	164
L2 Switching Clear Commands	169
Switching Configuration using OA-700	170
OA-700 as a Switch with no VLANs	170
OA-700 as a Switch with VLANs	171
7 Per VLAN Spanning Tree +.....	175
Chapter Conventions	175

Per VLAN Spanning Tree (PVST+) Overview	176
PVST+ Configuration	177
PVST+ Configuration Steps.....	177
PVST+ Configuration Flow	178
PVST+ Configuration Commands	179
Show Commands in PVST+	183
PVST+ Configuration Examples	187
Example 1	187
Example 2.....	189
Topology	189
Procedure	190
8 Integrated Routing and Bridging	193
Chapter Conventions	193
Integrated Routing and Bridging Overview	194
Alcatel-Lucent Specific IRB Overview	194
IRB Configuration	195
IRB Configuration Steps	195
IRB Commands	196
IRB Configuration using OA-700	197
Topology for IRB Configuration on OA-700	197
9 802.1X Port-Based Authentication	199
Chapter Conventions	199
802.1X Overview	200
Generic terms used in 802.1X	201
Using 802.1X with VLAN Assignment	203
Alcatel-Lucent Specific Overview	203
802.1X Configuration	204
802.1X Configuration Steps.....	204
802.1X Configuration Flow	207
802.1X Configuration Commands	208
802.1X Show Commands	214
802.1X Configuration Example	216
10 Port Monitoring.....	221
Chapter Conventions	221
Port Monitoring Overview	222
Port Monitoring Configuration	223
Port Monitoring Configuration Steps.....	223
Port Monitoring Commands	224
Port Monitoring Configuration on OA-700	225

Part 3: WAN Interfaces and Protocols

11 T1/E1 Line Card	229
Chapter Organization	229
Chapter Conventions	229
T1 and E1 Overview	230
E1 Interface Overview	231
E1 Timeslot Functionalities	231
Mechanisms Supported by the E1 interface	232
E1 Modes of Operation	233
Alcatel-Lucent Specific Overview	233
E1 Configuration	234
E1 Configuration Steps	234
E1 Configuration Flow	236
E1 Configuration Commands	237
E1 Show Commands	245
Troubleshooting E1 Lines	247
T1 Interface Overview	248
Frame Formats Used in T1 Cards	248
T1 Modes of Operation	249
T1 Configuration	250
T1 Configuration Steps	250
T1 Configuration Flow	252
T1 Configuration Commands	253
T1 Show Commands	261
Troubleshooting T1 Lines	263
12 Serial Line Cards	265
Chapter Organization	265
Chapter Conventions	266
Serial Line Card (V.35/X.21) Overview	267
Alcatel-Lucent Specific Overview	268
V.35/X.21 Configuration	269
V.35/X.21 Interface Configuration Steps	269
V.35/X.21 Configuration Flow	270
V.35/X.21 Configuration Commands	271
V.35/X.21 DTE and DCE CLI Configuration Commands	272
13 High-level Data Link Control	277
Chapter Conventions	277
HDLC Overview	278
HDLC Frame Structure	278
HDLC Frame Formats	279
HDLC Protocol Operation	279
HDLC Configuration	280

HDLC Configuration Steps	281
HDLC Configuration Flow	283
HDLC Configuration Commands	284
14 Frame Relay	289
Chapter Conventions	289
Frame Relay Overview	290
Frame Relay Devices	290
Frame Relay Virtual Circuits	290
Frame Relay Network Deployments	291
Frame Relay Configuration	292
Frame Relay Configuration Steps	293
Frame Relay Configuration Flow	295
Frame Relay Commands	296
15 Point-to-Point Protocol	305
Chapter Conventions	305
PPP Overview	306
PPP Components	306
PPP Operation	306
PPP Configuration	307
PPP Configuration Steps	308
PPP Configuration Flow	310
PPP Configuration Commands	311
PPP Optional Parameters	312
PPP Show Commands	320
PPP Debug Commands	327
16 Multilink Point to Point Protocol	329
Chapter Conventions	329
MLPPP Overview	330
MLPPP Components	331
MLPPP Operation	331
Alcatel-Lucent Specific Overview on MLPPP Features	332
MLPPP Configuration	333
MLPPP Configuration Steps	334
MLPPP Configuration Flow	336
MLPPP Configuration Commands	337
MLPPP Show Commands	339
MLPPP Configuration Example	340
17 Multilink Frame Relay	343
Chapter Conventions	343
MLFR Overview	344
MLFR Components	344

MLFR Operation	344
Alcatel-Lucent Specific Overview on MLFR features	346
MLFR Configuration	346
MLFR Configuration Steps	347
MLFR Configuration Flow	350
MLFR Configuration Commands	351
MLFR Show Commands	355

Part 4: Common Classification

18 Common Classifiers	359
Chapter Conventions	359
CC Overview	360
Benefits of Alcatel-Lucent Devices Common Classifiers	361
CC Architecture	361
Before you Configure CC	362
CC Configuration	363
CC Configuration Steps	363
Elements Used in Configuring CC	364
To Configure a Match-list	367
Example	367
Rules within Match-lists	367
To Configure Rules Using the Protocol Numbers	373
Lists in CC	374
Nesting Of Match-lists	376
Show commands in CC	378
Deletion Commands in CC	381
Sample examples on the usage of CC across applications	383
Example 1	383
Example 2	384
Example 3	385

Part 5: Routing Protocols

19 Protocol Independent Features	389
Protocol Independent Features Configuration	389
Chapter Conventions	389
Protocol-Independent Configuration	390
Protocol-Independent Configuration Commands	391
20 Routing Information Protocol	417
Chapter Conventions	417
RIP Overview	418

RIP Configuration	419
RIP Configuration Steps	420
RIP Configuration Flow	422
RIP Configuration Commands	423
RIP Optional Parameters	424
RIP Show Commands	436
RIP Clear Commands	440
21 Border Gateway Protocol	441
Chapter Conventions	441
BGP Overview	442
BGP Configuration	443
BGP Configuration Steps	443
BGP Configuration Flow	445
BGP Configuration Commands	446
BGP Show Commands	448
BGP Clear Commands	451
A Typical BGP Example Using OA-700	454
22 Open Shortest Path First	457
Chapter Conventions	457
OSPF Overview	458
OSPF Configuration	459
OSPF Configuration Steps	459
OSPF Configuration Flow	461
OSPF Configuration Commands	462
OSPF Optional Parameters	463
Show Commands in OSPF	481
Clear Commands in OSPF	490
OSPF Configuration on OA-700	491
Example 1	491
23 Multicast Routing	493
Chapter Conventions	493
Multicast Overview	494
Protocol Independent Multicast (PIM)	494
Internet Group Management Protocol (IGMP)	495
RFCs	496
PIM Configuration	497
PIM Configuration Steps	497
PIM Configuration Flow	499
PIM Configuration Commands	500
Show Commands in PIM	505
Clear Commands in PIM	508
IGMP Configuration	509

IGMP Configuration Steps	509
IGMP Configuration Flow	511
IGMP Configuration Commands.....	512
Show Commands in IGMP	516
Show Commands in Multicast	517
Clear Commands in Multicast.....	518
Multicast Configuration on OA-700	519
Example 1	519
Verifying Multicast Routing.....	523

24 Policy Based Routing.....525

Chapter Conventions	525
PBR Overview.....	526
Alcatel-Lucent Specific Overview	526
PBR Configuration	527
PBR Configuration Steps.....	527
PBR Configuration Flow	529
PBR Configuration Commands	530
Show Commands in PBR.....	533
Clear Commands.....	534
PBR Configuration Example	535
Configuration Steps	535
Show Commands	536

Part 6: Network Security

25 Network Address Translation.....539

Chapter Conventions	539
NAT Overview	540
Types of NAT	540
Benefits of NAT	542
Before You Configure NAT.....	542
Alcatel-Lucent Specific Overview	542
Source NAT Configuration	543
SNAT Configuration Steps	544
SNAT Configuration Flow	546
SNAT Configuration Commands	547
Sample Configurations of SNAT on OA-700	553
Destination NAT Configuration.....	554
DNAT Configuration Steps	555
DNAT Configuration Flow.....	557
DNAT Configuration Commands.....	558
Sample Configuration Example of DNAT on OA-700.....	561
Bypass IPsec Traffic.....	562
NAT Show Commands	563

NAT Clear Commands	565
NAT Debug Commands	566
Modifying NAT Configuration	567
Insertions	567
Updates	568
NAT Deletion Commands	570

26 Filter and Firewall573

Chapter Conventions	573
Network Security - An overview	574
Network Security Terminologies	575
Firewall Mechanisms	576
Before You Configure Filters and Firewalls	577
OA-700 Specific Overview	577
Filter Configuration	578
Filter Configuration Steps	578
Filter Configuration Flow	580
Filter Configuration Commands	581
Filter Show Commands	585
Filter Deletion Commands	587
Filter Clear Commands	588
Filter Debug Commands	589
Sample Examples of Configuring Filters on OA-700	590
Managing Security Configuration	591
Insertions	591
Updates	592
Network Attacks - An Overview	594
Types of Network Attacks	594
Default Attacks (Rate-limiting / Stateful)	595
Default Attacks (Non-rate Limiting / Stateless)	597
Optional Attacks	599
Network Attack Prevention Configuration	601
Network Attack Prevention Configuration Steps	601
Network Attack Prevention Configuration Flow	603
Network Attack Prevention Configuration Commands	604
Firewall Show Commands	614
Firewall Debug Commands	620
Sample Firewall Policy Configurations on OA-700	621
Zone Configuration	623
Trusted Zone Configuration	623
Untrusted Zone Configuration	623
Semi-trusted Zone or Demilitarized Zone	624
Three Zone Firewall Example	625
Example 2: Simple Zone Configuration in OA-700	633
Time-range/Timer Configuration	635
Time-range Configuration Commands	635

Time-range Show Command.....	636
ALGs Supported in OA-700	637
ALG Configuration Commands.....	639
Customized-service Rule Based ALG Configuration	646
Customizing ALG Commands	646
UA ALG Configuration.....	649
UA ALG Commands	649
Typical Rule Based ALG and DNAT Example Using OA-700.....	652
Security - Best Practices	654
Rules for Configuring Packet Filters	654

27 IP Security - Virtual Private Network 659

Chapter Conventions	660
IPsec VPN Overview.....	661
IPsec Enabled VPN	663
IPsec Connection Types.....	663
IPsec Concepts	665
Benefits of IPsec Enabled VPN	670
Default Configuration Setting on OA-700	671
IPsec VPN Configuration	672
IPsec VPN Configuration Steps.....	672
IPsec VPN Configuration Flow	674
IPsec Configuration Commands	675
To Configure the Match-lists.....	675
IPsec Configuration with Pre-shared Key.....	675
Example.....	675
IPsec Configuration with X.509 Certificates	676
To Import a RSA Key.....	676
Example.....	676
Example.....	677
To Export RSA Keys.....	683
Example.....	683
To Delete a CA Certificate.....	683
Example.....	683
To Delete a Signed Certificate.....	684
Example.....	684
To Delete a Peer Certificate	684
Example.....	684
To Delete an RSA Key Pair	684
Example.....	684
Internet Key Exchange (IKE) Policy	685
To Configure Transform-set in IPsec.....	689
To Configure IPsec Crypto Map	691
Example.....	691
To Attach Crypto Map to an Interface.....	695
Dead Peer Detection (DPD)	696

IPsec VPN Show Commands	698
Clear Commands in IPsec	714
IPsec Scenarios on OA-700	715
Best Practices For Deploying IPsec VPN	718
Identity	718
IPsec Access Control	719
IPsec	719
Network Address Translation	720
Network Access Control	720
Interoperability	720
Routing Entry	721
IPsec NAT-Traversal	722
Scenarios Depicting IPsec Nat-traversal	723
IPsec Tunnel Interface	725
Before You Configure IPsec Tunnel Interface	725
Default Configuration	726
IPsec Tunnel Interface Configuration	727
IPsec Tunnel Interface Configuration Steps	727
IPsec Tunnel Interface Configuration Flow	729
IPsec Tunnel Interface Configuration Commands	730
IPsec Tunnel Configuration Scenarios using OA-700	737
28 Generic Routing Encapsulation	739
Chapter Organization	739
Chapter Conventions	739
GRE Overview	740
GRE Tunnel Setup	740
GRE Tunnel Features	741
Summary	742
Alcatel-Lucent Specific Overview	742
GRE Tunnel Configuration	743
GRE Configuration Steps	743
GRE Configuration Flow	745
GRE CLI Commands	746
GRE Configuration Scenarios using OA-700	749
1. GRE Configuration	749
2. GRE + IP Filters + DoS Configuration	752
3. GRE over IPsec Configuration	754
29 Transparent Firewall	757
Chapter Conventions	757
TF Overview	758
OA-700 Specific Overview	758
TF Configuration	759
TF Configuration Steps	759
TF Configuration Flow	760

TF Configuration Commands	761
Show Commands in TF	763
Clear Commands.....	764
TF Configuration on OA-700.....	765
Configuration Steps	765
Show Commands	765

Part 7: Quality of Service

30 Quality of Service769

Chapter Conventions.....	769
QoS Overview	770
Generic terms used in QoS	770
Alcatel-Lucent Specific Overview on QoS	772
Traffic Without Policing and Shaping.....	774
Traffic with Policing.....	775
Traffic with Shaping	776
Hierarchical Queuing	777
Bandwidth Sharing in Tunnels	779
QoS Configuration.....	780
QoS Configuration Steps.....	780
QoS Configuration Flow	783
QoS Configuration Commands.....	785
Class Map Configuration	785
Policy Map Configuration.....	786
Attaching a Policy Map to an Interface	789
Traffic Class Attributes Configuration	790
Auto QoS Configuration.....	798
Hierarchical Policy Configuration.....	800
QoS over Tunnel Interface	805
Example.....	805
QoS Show Commands	806
QoS Clear Commands	815
QoS Test Scenarios on OA-780.....	816
Traffic Shaping	816
Priority Queuing.....	817

31 Intrusion Detection System819

Chapter Conventions.....	819
IDS Overview	820
Alcatel-Lucent Specific Overview	820
IDS Configuration.....	820
IDS Configuration Steps.....	821
IDS Configuration Flow.....	823
IDS Configuration Commands.....	824

IDS Show Commands	830
IDS Clear Commands.....	835
IDS Debug Commands.....	836
IDS Configuration Scenario Using OA-700	837
Configuration Steps	837
Show Commands	837
IDS Topology.....	838

Part 8: TCP/IP Services

32 DHCP (Dynamic Host Configuration Protocol) Server.....841

Chapter Conventions	841
DHCP Server Overview	842
Alcatel-Lucent Specific Overview	842
DHCP Server Configuration	843
DHCP Server Configuration Steps	843
DHCP Server Configuration Flow.....	845
DHCP Server Configuration Commands	846
DHCP Server Show Commands	853
DHCP Server Test Scenarios using OA-780	856
Configuration Steps	857

33 TFTP (Trivial File Transfer Protocol) Server859

Chapter Conventions	859
TFTP Server Overview.....	860
Alcatel-Lucent Specific Overview	860
TFTP Server Configuration	861
TFTP Configuration Steps	861
TFTP Configuration Flow.....	862
TFTP Configuration Commands.....	863
TFTP Show Commands	864

34 DHCP (Dynamic Host Configuration Protocol) Relay865

Chapter Conventions	865
DHCP Relay Overview.....	866
Alcatel-Lucent Specific Overview	866
DHCP Relay Configuration	867
DHCP Relay Configuration Steps.....	867
DHCP Relay Configuration Flow	868
DHCP Relay Configuration Commands	869
DHCP Relay Test Scenarios using OA-780.....	871
Configuration Steps	871

35 DNS (Domain Name Service) Client	873
Chapter Conventions	873
DNS Client Overview	874
DNS Client Configuration	874
DNS Client Configuration Steps	875
DNS Client Configuration Flow	876
DNS Client Configuration Commands	877
DNS Client Test Scenario using OA-780	881
Configuration Steps	881

Part 9: Lifeline (Dedicated Management Framework)

36 Lifeline	885
Chapter Conventions	886
Lifeline Overview	887
Lifeline Features	888
Failure Modes supported by Lifeline.....	890
Failure Detection	891
Failure Notification.....	892
Interface Cards that are Currently Supported.....	892
Functionality Available in Lifeline Mode.....	892
Routing Considerations in Lifeline Mode	893
Operation of OA-780 in Lifeline Mode	893
CLI Commands.....	894
Recovery from Lifeline Mode to Normal Mode	897
Lifeline Configuration Scenario	898

Part 10: Appendices

A Well Defined Port Numbers for Services	3
B RFCs Supported by OA-700	11
AAA Authentication	11
SNMP.....	11
Management	11
VRRP	11
LAN	12
WAN.....	12
Layer-2 protocols	12
Routing.....	12
IPsec VPN.....	13
GRE	14
QoS.....	14

C	Failure Scenarios While Installing OA-700 Software Package.....	15
	Failure Scenarios While Installing.....	15
D	QoS Values and Mnemonics	17
	Default Values for Random-detect ip-precedence.....	17
	Default Values for Random-detect ip-dscp.....	17
	IP-DSCP Mnemonics.....	20
	IP-precedence Mnemonics.....	21
	ToS Mnemonics.....	21
E	IP Security Interoperability of OA-700.....	23
	Configuring IPsec Tunnel Between OA-700 and Cisco 2621	23
	Configuration	24
	Verification.....	28
	Configuring IPsec between OA-700 and Sonicwall (PRO 3060)	29
	Configuration	30
	Configuring Sonicwall (PRO 3060).....	32
	Verifying the Configuration	36
F	Software Licenses and Acknowledgements.....	37
	Linux Kernel.....	38
	Intel Linux Device Driver Software	38
	PMC-Sierra Linux Device Driver Software	38
	Mindspeed Linux Device Driver Software.....	39
	eCos	39
	U-Boot	40
	Linux STP.....	40
	Paul's PPP Package.....	40
	DHCP	42
	tftp-hpa	43
	Net-SNMP	44
	OpenSSH	46
	ZEBRA CLI	48
	GNU Pth - The GNU Portable Threads	49
	TCP Proxy and Reassembly	49
	Strongswan IKE.....	50
	FreeBSD Crypto Library	50
	Snort.....	51
	Mbedthis AppWeb	51
	libxslt.....	52
	BusyBox	53
	iputils	53
	e2fsprogs.....	55
	InetUtils, gawk, GDB	55
	cURL.....	56

PCRE.....	56
MD5.....	57
GNU General Public License.....	58
GNU Lesser General Public License.....	64

List of Figures

Configuration Modes 15
VRRP Configuration Flow 124
VRRP Topology 136
Ethernet Network 143
Ethernet Interface Configuration Flow 146
Layer 2 Switching 155
L2-GE Front Panel View of the RJ-45 Connector 156
L2 Switching Configuration Flow 160
Switching with no VLANs 170
Switching with VLAN 171
PVST+ Configuration Flow 178
PVST+ Topology 187
PVST+ Topology on OA-700 189
IRB Topology 197
802.1X Deployment Scenario 200
Message Exchange 202
802.1X Configuration Flow 207
802.1X Topology 216
Port Monitoring Topology 225
The OA-700 T1E1 Line Card 230
E1 Frame Structure 231
E1 Configuration Flow 236
T1 Configuration Flow 252
Serial Line Card (V.35/X.21) 268
V.35/X.21 Configuration Flow 270
An HDLC frame with an information field 278
HDLC Configuration Flow 283
FR Configuration Flow 295
PPP Configuration Flow 310
Sample Deployment Scenario for MLPPP 330
MLPPP Header in Long Sequence Number Format 331
MLPPP Header in Short Sequence Number Format 332
MLPPP Configuration Flow 336
MLFR frame format for data packets 345
MLFR frame format for control packets 345
MLFR Configuration Flow 350
Depicting Alcatel-Lucent's Common Classification 360
Elements in Common Classifiers 361
RIP Configuration Flow 422
BGP Configuration Flow 445
BGP Configuration Scenario 454
OSPF Configuration Flow 461
OSPF Configuration Scenario 491
PIM Configuration Flow 499
IGMP Configuration Flow 511
Multicast Configuration Scenario 519
PBR Configuration Flow 529
SNAT Configuration Flow 546
DNAT Configuration Flow 557
Depicting ALG Scenario 575
Filter Configuration Flow 580

Network Attack Prevention Flowchart 603
Figure Depicting Three Zones 623
Three - Zone Network Topology 624
Three Zone Firewall Network Topology 625
ALG Configuration Scenario 652
General VPN Usage 661
A General Scenario of IPsec - VPN 664
Tunnel Mode 665
Phase 1 Negotiation - Main Mode 668
Phase 2 Negotiation - Quick Mode 669
IPsec Configuration Flowchart 674
IPsec Scenario with NAT-Traversal 723
IPsec Tunnel Interface Configuration Flowchart 729
IPsec Tunnel Interface Configuration Topology 737
GRE Configuration Flow 745
GRE Configuration Topology 749
GRE+ IP Filters + DoS Configuration Topology 752
GRE + IPsec Configuration Topology 754
TF Configuration Flow 760
Data Traffic before Policing And Shaping 774
Data Traffic with Policing 775
Data Traffic with Shaping 776
Link Sharing Requirement Example 777
Link Sharing Solution 778
Link Bandwidth sharing requirements over VPN tunnels 779
QoS Configuration Flow - Auto QoS Procedure 783
QoS Configuration Flow - Standard Procedure 784
QoS Traffic Shaping Using OA-780 816
QoS Priority Queuing Using OA-780 817
IDS Configuration Flow 823
IDS Topology 838
DHCP Server Configuration Flow 845
DHCP Server Test Scenario using OA-780 856
TFTP Configuration Flow 862
DHCP Relay Configuration Flow 868
DHCP Relay Test Scenario using OA-780 871
DNS Client Configuration Flow 876
DNS Client Test Scenario using OA-780 881
Separate Management Plane 888
N+1 Redundant Management Architecture 889
Uninterrupted Access to System Management 890
Lifeline Configuration Scenario 898
IPsec Interoperability Between OA-700 and Cisco 2621 23
IPsec Interoperability Between OA-700 and Sonicwall PRO 3060 29
Configuring Local network behind Sonicwall 32
Configuring External IP Address for Sonicwall 33
Configuring IPsec Policy and Destination Network 34
Configuring IPsec Phase 1 and Phase 2 Proposals 35

CHAPTER 1 PREFACE

ABOUT THIS GUIDE

This guide describes the CLI commands used to configure different services available in the OmniAccess 700 (OA-700). It focuses on accessing the OmniAccess 700 by using the Command Line Interface (CLI). In addition to showing how to configure each feature, this guide also provides background on why user might need the service and how it works.

The following list is a sampling of what is found in this guide:

- Getting efficient use of network resources.
- Configuring the LAN and WAN interfaces effectively.
- Optimizing routing services to enhance network scalability.
- Integrating networks with different routing protocols.
- Adding intelligence and flexibility to use the ACLs across applications using the Common Classifiers.
- Setting improved security policies on the network for users and their services.
- Extending the network to new places, such as Internet, securely.
- Protecting information and network resources.

AUDIENCE

This guide is intended for networking professionals who are responsible for designing, implementing, and managing enterprise networks. This guide aims to provide unique technologies and effective practices that not only deliver value on the networking perspective but also provides an opportunity for professional growth.

ORGANIZATION

The chapters in the CLI Configuration Guide are organized into seven parts.

PART I - INTRODUCTION

The first part provides an introduction to CLI, **“The Command Line Interface”** in **Chapter 2**. This is a preparatory chapter that describes the CLI configuration considerations, tools required, an overview of the Command Line Interface and procedures that should be performed before the actual configuration.

Chapter 3 “System Configuration and Monitoring” provides an overview of the system level commands required to troubleshoot, monitor, connect the system to the network. This chapter also includes commands for Inband and Out-of-band management, setting system parameters, software management, configuration management, AAA services, SNMP, etc. The various commands described include SSH, Telnet, show version, update, show environment, show mem, show proc, etc.

Chapter 4 “Virtual Router Redundancy Protocol” details a study on VRRP implementation on the OA-700. It is a method of providing nonstop path redundancy and gateway redundancy for an enterprise network by sharing protocol and Media Access Control (MAC) addresses between redundant gateways.

PART II - LAN INTERFACES

This part introduces the commands and steps to configure the LAN interfaces. It gives a succinct overview on the Ethernet Interface configuration in **Chapter 5 “Ethernet Interfaces on SE”**.

The Bridging configuration in **Chapter 6 “Layer 2 Switching Configuration”** deals with the L2 switching Configuration on the OA-700. The chapter is organized with the L2 switching overview, configuration details in the first few sections and the configuration scenario in the end to give a real time example for configuring switching.

Chapter 7 “Per VLAN Spanning Tree +” details the VLAN commands in switching.

Chapter 8 “Integrated Routing and Bridging” deals with Switching configuration integrated with routing.

Chapter 9 “802.1X Port-Based Authentication” describes how to configure IEEE 802.1X port-based authentication on the OA-700.

Chapter 10 “Port Monitoring” chapter details the commands used to configure Port Monitoring on the OA-700.

PART III- WAN INTERFACES

This part introduces the commands and steps to configure a T1 or an E1 interface in **Chapter 11 “T1E1 Line Card”**. The different encapsulation that can be applied on an interface are described in the subsequent chapters.

Chapter 12 “Serial Line Cards” provides the configuration steps and commands to configure Serial interface (V.35/ X.21). The different encapsulation that can be applied on an interface are described in the subsequent chapters.

Chapter 13 “High-level Data Link Control” provides the configuration steps and commands to configure an High-level Data Link Control (HDLC) encapsulation on an interface.

Chapter 14 “Frame Relay” provides the configuration steps and commands for Frame Relay (FR) encapsulation on an interface. It includes the configuration commands for LMI, DLCI and FR fragmentation.

Chapter 15 “Point-to-Point Protocol” provides the configuration commands for Point-to-point (PPP) encapsulation on an interface. It includes CLI commands for configuring LCP, IPCP, Counters and Timers, Authentication, etc.

Chapter 16 “Multilink Point to Point Protocol” provides the configuration commands for Multilink Point-to-Point (MLPPP) encapsulation on an interface. It includes CLI commands for configuring a multi-link bundle interface and member link configuration.

Chapter 17 “Multilink Frame Relay” provides the configuration commands for Multilink Frame Relay (MLFR) encapsulation on an interface. It includes CLI commands for configuring a multi-link bundle interface and member link configuration.

PART IV - PACKET CLASSIFICATION

This part consists of **Chapter 18 “Common Classifiers”** that focuses on configuring the Common Classifier commands. These commands are generic across all applications. You are required to have a thorough knowledge of this chapter before you proceed to configure the NATs, Filters, etc. This chapter provides a concise overview on the concepts of creating rules, match-lists, lists, etc.

PART V - ROUTING PROTOCOLS

The aim of the fourth part is to get the most out of addressing and routing. The routing function moves data through the network efficiently and finds new paths when network changes occur. Routing also affects how large the network can grow - that is, the complexity of the topology and the stability of the network as it expands.

All the chapters in this part focus on configuring the routing services.

Chapter 19 “Protocol Independent Features” provides commands that are generic across all routing protocols. You are required to have a thorough knowledge of this chapter before you proceed to configure the routing protocols.

Chapter 20 “Routing Information Protocol” and **Chapter 21 “Border Gateway Protocol”** and **Chapter 22 “Open Shortest Path First”** provides configuration commands for configuring RIP, BGP and OSPF routing protocols.

Chapter 23 “Multicast Routing” provides Multicast routing configuration on the OA-700.

Chapter 24 “Policy Based Routing” covers the Policy Based Routing (PBR) configuration on the OA-700.

PART VI - NETWORK SECURITY CLI

This part deals with the methodologies to secure the network, protect data and users, and extend connectivity with confidence. Security services protect the confidentiality and integrity of information on the network. You are required to have a complete knowledge in configuring the match-lists (access lists) before you proceed to configure the Filters, NATs, Firewalls, and IPsecs.

Chapter 25 “Network Address Translation” covers the configuration of NATs (SNAT and DNAT configuration).

Chapter 26 “Filter and Firewall” progresses logically from basic network security, starting with filters to more sophisticated topics such as Firewall policies and Zone configuration. The “Time-range CLI” includes commands and procedure to configure scheduling in different applications, such as Firewall.

Chapter 27 “IP Security - Virtual Private Network” begins a survey of advanced security services and provides details about IPsec - a leading technology for building VPNs. IPsec building blocks include IKE, Transform Sets, Security Associations, Modes, Authentication Header (AH), Encapsulating Security Payload (ESP), and basic cryptography.

Chapter 28 “Intrusion Detection System” comprehends the commands to configure Intrusion Detection and Intrusion Prevention on the OA-700.

Chapter 29 “Generic Routing Encapsulation” provides the commands for GRE (Generic Routing Encapsulation) configuration.

Chapter 30 “Transparent Firewall” covers the Transparent Firewall (TF) configuration on the OA-700.

PART VII - QUALITY OF SERVICE

Quality of Service (QoS) refers to a broad collection of shaping technologies/ techniques. QoS is an increasingly important area of research and development in computer networking. It is especially important for the new generation of internet applications such as video-on-demand and other consumer services. QoS tools help in alleviating most congestion problems especially when there is too much traffic and a network monitoring system becomes a must.

Chapter 31 “Quality of Service” provides the configuration commands for QoS. It includes CLI commands for configuring policing, shaping, queueing network traffic, auto Qos, etc.

PART VIII - TCP/IP SERVICES

This part consists of **Chapter 32 “DHCP (Dynamic Host Configuration Protocol) Server”** that focuses on DHCP Server configuration, and **Chapter 33 “TFTP (Trivial File Transfer Protocol) Server”** that documents the TFTP Server configuration commands.

Chapter 34 “DHCP (Dynamic Host Configuration Protocol) Relay” focuses on DHCP Relay configuration.

and **Chapter 35 “DNS (Domain Name Service) Client”** documents the DNS Client configuration commands.

PART IX - LIFELINE (DEDICATED MANAGEMENT FRAMEWORK)

This part consists of **Chapter 36 “Lifeline”** that describes the Lifeline management framework, which is a key architectural aspect of the OA-780.

DOCUMENT CONVENTIONS

The following table describes the document conventions used with the commands in this document:

Convention	Description
Bold	Indicates commands and keywords
<i>Italics</i>	Indicates arguments/command input supplied by you.
[]	Square brackets enclose an optional element (keyword or argument)
< >	Braces enclose a mandatory element (keyword or argument).
	Line indicates an optional choice.
[x y]	Square brackets enclosing keywords or arguments separated by a vertical line indicates an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice. You must select one.
[w {x y}.....]	Nested sets of square brackets or braces indicate optional or required choices within the optional or required elements.
{x y}... OR [x y]...	Braces enclosing keywords or arguments with '...' indicate that the element within the brace can be repeated.
<code>Courier font</code>	Examples of information displayed on the screen.
< >	Angle brackets enclose text that is not printed on the screen such as passwords.
“no” form of the commands	The 'no' form of a command is issued to either set it to its default value or to negate it.
[^]	[^] in the command indicate negation.

The following conventions are used to attract the attention of the reader:



Note: A note contains helpful suggestions or information that may be easily overlooked.



Caution: Indicates a situation where the reader needs to be careful. Failure to observe the cautionary note could result in equipment damage or loss of data.



Warning: Warning is used in similar cases as caution. This also indicates a situation where the reader needs to pay extra attention to avoid hazardous situations.

OBTAINING DOCUMENTATION

Alcatel-Lucent provides several ways to obtain technical assistance and other technical resources. Documents can be downloaded from our support site service.esd.alcatel-lucent.com.

REFERENCE PUBLICATIONS

The following publications are part of the Alcatel-Lucent documentation suite:

- OmniAccess 700 CLI Command Reference Guide (Release 2.2)
- OmniAccess 700 Web GUI Users Guide (Release 2.2)
- OmniAccess 700 Getting Started Guide (Release 2.2)
- OmniAccess 780 Hardware Users Guide (Release 2.2)
- OmniAccess 740 Hardware Users Guide (Release 2.2)

OBTAINING TECHNICAL ASSISTANCE

For all customers, partners, resellers, and distributors who hold valid Alcatel-Lucent service contracts, the Alcatel-Lucent Technical Support Team provides 24-hour-a-day, technical support services online and over the phone.

For Customer issues and help, contact:

Alcatel-Lucent

US Customer Support: (800) 995-2696

International Customer Support: (818) 878-4507

E-mail: support@ind.alcatel.com

Website: service.esd.alcatel-lucent.com

DOCUMENTATION FEEDBACK

We value your comments and suggestions about our documentation. If you have any comments about this guide, please enter them through the Feedback link on the Alcatel-Lucent website. We will use your feedback to improve the documentation.

Part 1 Introduction



CHAPTER 2 THE COMMAND LINE INTERFACE

CLI OVERVIEW

The Command Line Interface (CLI) is the primary interface to access the **OA-700**. The CLI is the interface for console and connections via SSH, Telnet, and Modem. The CLI, which automatically starts once the required processes on the Switch Card are up provides commands that you can use to perform various tasks, including configuring the **OA-700**, monitoring and troubleshooting the system, enabling network connectivity, and verifying the system hardware.

This chapter provides an overview of the CLI. For more detailed information on the CLI syntax and a description on its parameters, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

The following topics are discussed in this chapter:

- **“Introduction to CLI Modes” on page 14**
- **“CLI Modes” on page 15**
- **“Initial Setup” on page 26**
- **“Using the Command Line Interface” on page 27**
- **“Configuring Interfaces” on page 34**

INTRODUCTION TO CLI MODES

There are several modes in the CLI, and in each mode, you can perform specific tasks. The CLI modes can be grouped under three main modes:

- [CLI User Mode](#)
- [CLI Configuration Mode](#)
- [CLI Sub-Configuration Mode \(SCM\)](#)

CLI USER MODE

In the **CLI User Mode**, you can enter commands to monitor and troubleshoot the system, network connectivity, clearing of processes, and routers. At this level, there are several broad groups of CLI commands. The two main administrative modes are **User Mode (UM)** and **Super User Mode (SUM)**. When you log in to the *OA-700* and start the CLI session, you are at the top level of the CLI User Mode which is the **User Mode (UM)**.

CLI CONFIGURATION MODE

In the configuration mode, you can configure the **OA-700** by creating a hierarchy of configuration statements by using the CLI or by creating a text (ASCII) file that contains the statement hierarchy. (The statement hierarchy is identical in both the CLI and text configuration file).

You can configure all applications of the **OA-700** including interfaces, general routing information, routing protocols, configuring NAT, configuring firewall, VPN, QoS, and user access as well as several system hardware parameters.

In the configuration mode, you can configure different applications running on the **OA-700**. It has four different configuration modes. They are: **Configuration Mode (CM)**, **Interface Configuration Mode (ICM)**, **Router Configuration Mode (RCM)** and **Sub-Configuration Mode (SCM)**.

CLI SUB-CONFIGURATION MODE (SCM)

From configuration modes, you can enter configuration sub-modes. The sub-configuration modes are used for the configuration of specific features within the scope of a given configuration mode.

CLI MODES

The different CLI modes are:

- “**User Mode (UM)**”
- “**Super User Mode (SUM)**”
- “**Configuration Mode (CM)**”
- “**Interface Configuration Mode (ICM)**”
- “**Sub-Interface Configuration Mode (S-ICM)**”
- “**Router Configuration Mode (RCM)**”

The flowchart above depicts the flow and command structure to be used to enter into the different modes of configuration accordingly.

After you successfully log into the system, you will enter the **User Mode**. At this mode, you can view only a few global show commands and have access to ping and SSH. There is no access to edit or update the configuration in this mode.

The next level is the **Super User Mode**. You can enter this mode by typing in the “**enable**” command. At this mode, you are given the flexibility to use the debug, reset, and clear commands. Even here you have no access to either insert, delete, or modify the configuration.

Type the “**config terminal**” command to enter the **Configuration Mode**. This mode is used to configure the system globally, or to enter specific configuration modes to configure specific elements such as interfaces or protocols.

In the **Application Configuration Mode**, you can enter into a specific application by entering the corresponding name such as: router OSPF, BGP, RIP, IP NAT, IP filter, firewall, etc.

By entering the interface type, slot-number, port-number, and other parameters of the interface, you will enter the **Interface Configuration Mode**. The interface configuration mode can be accessed from the configuration mode or also from the application configuration mode. After configuring an interface, you can configure a sub-interface either from the ICM or directly from the configuration mode itself.

The reverse flow is also depicted with the help of the “**Exit**” and “**End / Ctrl-Z**” commands. These commands allow you to go back to the previous mode or to exit totally out of the configuration and go to the super user mode. The command “**top**” is used to jump to configuration mode from which ever mode you are in.

USER MODE (UM)

You can start the CLI session from a console, SSH or a Telnet connection. When you start the CLI session, you are prompted for a user name / password combination. When you enter the user name and password correctly, you will automatically enter the UM. If you enter an incorrect password three consecutive times, the CLI session will be closed.

Since UM is the basic administrative level, only a limited set of commands like basic diagnostics, monitoring commands, ping, and ssh are available. The UM command set is a subset of the SUM command set. UM is also the starting point for accessing the SUM command set.

USER MODE COMMAND SET

Command (in UM)	Description
clear	Reset functions
enable	Turn on privileged commands
exit	Exit from current mode
help	Description of the interactive help system
logout	Exit from the EXEC
mping	Multicast Ping
mtrace	Trace reverse multicast path from destination to source
no	Negate a command or set its defaults
nslookup	Translate a DNS name to an IP address or vice-versa
ping	Send echo messages
quit	Quit this session
service	Set terminal line parameters
show	Show running system information
ssh	Open a SSH connection
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination

SUPER USER MODE (SUM)

To access the SUM, enter the **'enable'** command in the UM mode. SUM is a superset of the UM command set and allows you to perform tasks like process reset, clearing counters, debugging, and entering configuration modes.

Command (in UM)	Description
enable	Enables SUM.

EXAMPLE

```
ALU> enable
ALU#
```

Notes:

- As the SUM command set contains all of the commands available in UM, some commands can be entered in either mode.
- It is recommend that you set up password authentication for users who need to access the SUM command set.

The SUM mode prompt consists of the host name of the device followed by a pound sign (#) or if no host name is configured, the prompt is displayed as 'ALU#'.

SUM COMMAND SET

Command (in SUM)	Description
clear	Reset functions
clock	System Clock
configure	Enter configuration mode
copy	Copy from one file to another
crypto	IPsec VPN Module
debug	Debugging functions
delete	Delete a file
dir	List files on a filesystem
disable	Turn off privileged commands.Exits from the SUM to the UM mode.
erase	Erase a filesystem
exit	Exit from current mode
help	Description of the interactive help system

Command (in SUM)	Description
list	Listing files
load	Load dynamically loadable resources Loading the configuration file
logging	Modify message logging facilities
logout	Exit from the EXEC
mkdir	Create directory
modem	Configure the Modem
nslookup	Translate a DNS name to an IP address or vice-versa
package	Package Manipulation
ping	Send echo messages
power	Control power on specified line card
quit	Quit this session
reload	Reboot the Chassis
rmdir	Delete directory
save	Saving the configuration file
service	Set terminal line parameters
show	Show running system information
ssh	Open a ssh connection
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
undebug	Disable debugging functions
write	Write running configuration to memory, network, or terminal

CONFIGURATION MODE (CM)

From SUM, you can enter the Configuration Mode (CM). The CM is used to configure the system globally to enter specific configuration modes or to configure specific elements such as interfaces or protocols.

In this mode, you can enter commands that configure general system characteristics. CM allows you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots. To access CM, enter the following command in SUM:

Command (in SUM)	Description
<code>configure terminal</code>	Enters Configuration Mode

EXAMPLE

```
ALU#configure terminal
ALU(config)#
Enter configuration commands, one per line. End with CNTL/Z.
```

To exit the Configuration Mode and return to the SUM, enter the **Control-Z** command.

```
ALU(config)#^Z
ALU#
```

CM COMMAND SET

Command (in CM)	Description
<code>aaa</code>	Authentication, Authorization, and Accounting
<code>access-list</code>	Add an access list entry
<code>arp</code>	ARP setting
<code>auto</code>	Create Auto-QoS template
<code>banner</code>	Define a login banner
<code>class-map</code>	Set QoS Class Map.
<code>clear</code>	Terminating the Session
<code>clock</code>	System clock settings
<code>controller</code>	Select a controller to configure
<code>crypto</code>	IPSEC VPN module
<code>customized-service</code>	Customize services

Command (in CM)	Description
debug	Debugging functions (see also 'undebug')
dialer-list	Specify dialer list
dot1x	802.1X authentication settings
enable	Modify enable secret parameters
end	Exit from configure mode
firewall	Firewall configuration mode
gre-keep-alive-interval	GRE Keep Alive interval
gre-keep-alive-max-tries	GRE Keep Alive maximum try count
hostname	Set system's network name
http	HTTP Web server
https	Secure HTTP
interface	Select an interface to configure
ip	Global IP configuration sub commands
ip-policy	Define/Modify PBR policy
key-chain	Key management
license	License operations
line	Configure a terminal line
list	Define a new list/Modify an existing list
liveness	Define behavior in case of liveness test failures
logging	Modify message logging facilities
mac-address-table	Configure the mac address table
match-list	Define/Modify a match-list
no	Negate a command or set its defaults
package	Package Manipulation
policy-map	Add a Policy-Map
radius-server	Modify RADIUS query parameters
route-map	Create route-map or enter route-map command mode
router	Enable a routing process
service	Modify use of network based services

Command (in CM)	Description
show	Show running system information
snmp	Configure SNMP parameters
spanning-tree	spanning-tree configurations
ssh	SSH service
tacacs-server	Modify TACACS+ query parameters
telnet	Telnet service
tftp-server	To Provide TFTP service for file requests
time-range	Define/Modify a time range object
top	Enter top level configuration mode
transparent-forward	Define/Modify transparent-forward policy
undebug	Debugging functions (see also 'undebug')
up	Go up one mode
username	Establish User Name Authentication

INTERFACE CONFIGURATION MODE (ICM)

One of the modes that you can access from CM is the Interface Configuration Mode (ICM). Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as Gigabit Ethernet, T1 or E1, etc.

Command (in CM)	Description
<code>interface <name> <slot/port></code>	This command enables you to configure virtual interfaces such as Gigabit Ethernet, Serial (V.35/X.21), and Switchport (L2GE).
<code>interface <name> <interface-number></code>	This command enables you to configure logical interfaces such as tunnel interface, loopback, VLAN, Multilink Frame Relay, and Multilink Point-to-Point protocol.
<code>controller <slot/port></code>	This command enables you to T1 or an E1 interface. This enters Controller mode.
<code>interface Serial <slot/port:channel></code>	This command enables you to configure a channelized serial interface in the specific slot or port of the T1 or an E1 interface.

EXAMPLE

The following command configures a Gigabit Ethernet interface:

```
ALU(config)#interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)#
```

The following command configures a loopback interface:

```
ALU(config)#interface loopback 1
ALU(config-if loopback1)#
```

The following command configures a MLFR bundle interface:

```
ALU(config)# interface mlfr 100
ALU(config-if mlfr100)#
```

The following command configures a E1 controller and channelized serial interface:


```
ALU(config)# controller E1 0/0
ALU(config-controller E1)#
ALU(config-controller E1)# exit
ALU(config)#
ALU(config)#interface Serial 0/0:0
ALU(config-if Serial0/0:0)#
```

To exit the ICM and return to the CM, enter the **Exit** command.

```
ALU(config-if GigabitEthernet7/0)# exit
ALU(config)#
```

SUB-INTERFACE CONFIGURATION MODE (S-ICM)

From the CM, you can enter Sub-Interface Configuration Mode (S-ICM), which is a sub-mode of the ICM.

Command (in CM)	Description
<code>interface <name> <slot/port:channel></code>	This command enables you to configure a sub-interface on a Gigabit Ethernet interface. This enters the S-ICM.
<code>interface <name> <slot/port>.subchannel</code>	This command enables you to configure a sub-interface on a Serial (V.35/X.21) interface. This enters the S-ICM.  <p>Note: This is valid only if Frame Relay encapsulation is set on the main interface.</p>
<code>interface Serial <slot/port:channel.subchannel></code>	This command enables you to configure a sub-interface on a channelized Serial interface. This enters the S-ICM.

EXAMPLE

The following command configures a sub-interface on Gigabit Ethernet interface:

```
ALU(config)# interface GigabitEthernet 7/0:1
ALU(config-subif GigabitEthernet7/0:1)#
```

The following command configures a sub-interface on a serial (v.35/X.21) interface:

```
ALU(config)# interface Serial0/0.1
ALU(config-if Serial0/0.1)#
```

The following command configures a sub-interface on a channelized serial interface:

```
ALU(config)# interface Serial 0/0:0.1
ALU(config-if Serial0/0:0.1)#
```

To exit from the S-ICM and return to the ICM, use the **Exit** command. To end your configuration session and return to SUM mode, press **Ctrl-Z** or enter the **End** command.

ROUTER CONFIGURATION MODE (RCM)

From the CM, you can enter the Router Configuration Mode (ACM). In this mode, you can enter into any specific application by entering the corresponding name such as OSPF, BGP, RIP, IP NAT, IP filter, firewall, etc.

Router configuration mode is used for configuring all the routing protocols.

Command (in CM)	Description
<code>router bgp <1-65535></code>	Enters BGP router configuration mode.
<code>router ospf <1-65535></code>	Enters OSPF router configuration mode.
<code>router rip</code>	Enters RIP router configuration mode.
<code>ip filter <name></code>	Enters Filter configuration mode.
<code>ip nat <name></code>	Enters NAT configuration mode.

EXAMPLE

```
ALU(config)# router ospf 42
ALU(config-router ospf 42)#
```

EXITING CONFIGURATION MODES

Command (in CM)	Description
<code>end</code> or <code>^Z</code> <code>^C</code>	Ends the current configuration session (from any configuration mode) and returns to SUM.
<code>exit</code>	Exits the current configuration mode and returns to the preceding mode. For example, you can enter this command to exit from CM to SUM or from ICM to CM.
<code>top</code>	This command enables you to go one step above from the mode you are currently in. For example, if this command is entered in the ICM, control moves to the CM.

You can exit from the current configuration session by typing **End**, **Ctrl-C**, **Ctrl-Z** and return to the UM/SUM mode. You can use the **Exit** command in any configuration mode to return to the previous configuration mode.

EXAMPLE

```
ALU# configure
Enter configuration commands, one per line. End with CNTL/Z.
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# ^Z
ALU#
```

```
ALU# configure
Enter configuration commands, one per line. End with CNTL/Z.
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# end
ALU#
```

```
ALU# configure
Enter configuration commands, one per line. End with CNTL/Z.
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# ^C
ALU#
```

```
ALU# configure
Enter configuration commands, one per line. End with CNTL/Z.
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# exit
ALU(config)#
```

```
ALU# configure
Enter configuration commands, one per line. End with CNTL/Z.
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# top
ALU(config)#
```

INITIAL SETUP

Whenever the system configuration is empty, you are automatically entered into the initial setup program, which takes you through the basic configuration steps.

USING THE COMMAND LINE INTERFACE

The following topics are described in this section:

- [“CLI Help”](#)
- [“Partial Help”](#)
- [“Partial Commands”](#)
- [“Command Line Editing”](#)
- [“Command History”](#)

CLI HELP

Extensive help is available in the CLI for all commands in each mode. To see a list of commands in each mode, enter a question mark (?) at the CLI prompt. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

ENABLE CLI HELP

Command (in CM)	Description
<code>service completion spacebar-complete</code>	Enable Spacebar completion
<code>no service completion spacebar-complete</code>	Disable Spacebar completion
<code>service completion tab-complete</code>	Enable Tab completion
<code>no service completion tab-complete</code>	Disable Tab completion

EXAMPLE

```

ALU(config)# service completion spacebar-complete

ALU(config)# no service completion spacebar-complete

ALU(config)# service completion tab-complete

ALU(config)# no service completion tab-complete

```

For specific context sensitive help related to a particular mode, command, keyword, or argument, enter one of the following commands:

Command (in CM)	Description
(prompt)# help	Displays a brief description of the help system.
(prompt)# abbreviated-command-entry?	Lists commands in the current mode that begin with a particular character string.
(prompt)# abbreviated-command-entry <Tab>	Completes a partial command name.
(prompt)# ?	Lists all commands available in the command mode.
(prompt)# command?	Lists the available syntax options (arguments and keywords) for the command.
(prompt)# command keyword?	Lists the next available syntax option for the command.

WORD HELP

To view the list of commands that begin with a specific set of characters, enter the characters immediately followed by the question mark (?). Do not include a space. This type of Help is called the **Word Help**.

EXAMPLE

```
ALU(config)# show i?
** PRIVILEGE COMMANDS **
inband                inband
interfaces            Display information for all interfaces
internal              Internal info
ip                    IP information
ip-policy             ip-policy keyword
ipx                   IPX protocol
```

COMMAND SYNTAX HELP

To view a list of keywords or arguments, enter a question mark (?) in the place of a keyword or argument. Include a space before the '?'. This type of help is called the **Command Syntax Help** as the keywords / arguments associated with the command already entered are displayed.

EXAMPLE

```
ALU(config)# show ip
```

```
** PRIVILEGE COMMANDS **
access-lists          List IP access lists
as-path-access-list  List AS path access lists
community-list       List community-list
dhcp                 Dynamic Host Configuration Protocol commands
filter               filter details
mroute               Multicast
multicast             Multicast
nat                  NAT keyword
prefix-list          List IP prefix Lists
rpf                  Show RPF information for multicast source
** BASIC COMMANDS **
bgp                  BGP information
fib                  IP FIB Table Statistics
igmp                 IGMP information
interface            Interface (slot/port:channel.subchannel - chan
                    & subchan optional)
ospf                 OSPF information
pim                  PIM information
protocols            IP routing protocol process parameters and
                    statistics
rip                  IP RIP show commands
route                IP routing table
traffic              IP Traffic Statistics
vrf                  VPN Routing/Forwarding instance information
```

PARTIAL HELP

When you enter a partial command (part of a command) and press the TAB or SPACE key, the command line parser completes the command if the string entered is unique to the command mode. For this to happen, service completion should have been enabled for the key.

For example, if you enter **conf** in the **SUM** mode, this entry is associated with the **configure** command.

EXAMPLE

```
ALU# conf <Tab>
ALU# configure
```

When you use the command completion feature the CLI displays the full command name. The command is not executed until you use the Return or Enter key. This way you can modify the command if the full command was not what you intended by the abbreviation.

If the CLI cannot complete the command, it displays the list of commands that begin with that set of characters.

For example, typing `show ip i<tab>` will list all commands, which start with "show ip i" in the current command mode:

```
ALU(config)# show ip i<tab>
igmp          interface
ALU(config)# show ip i"
```



Note: Characters you enter before the question mark are reprinted to the screen to allow you to complete the command entry.

PARTIAL COMMANDS

When you enter a partial command (part of a command) and press the Enter key, the CLI executes the best matched command.

EXAMPLE

```
ALU(config)# sh ip int br
Interface          IP Address      Admin State    Oper State
GigabitEthernet3/0 unassigned      up             down
GigabitEthernet3/1 10.91.1.146    up             up
```

COMMAND LINE EDITING

MOVING THE CURSOR

Keystrokes	Function Summary	Function Details
Left Arrow or Ctrl-B	Back character	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Right Arrow or Ctrl-F	Forward character	Moves the cursor one character to the right.
Esc, B	Back word	Moves the cursor back one word.
Esc, F	Forward word	Moves the cursor forward one word.
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.
Ctrl-E	End of line	Moves the cursor to the end of the command line.
Ctrl-P or the Up Arrow key.	Previous command	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the Down Arrow key.	Next command	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.
Ctrl-I	Tab	Complete command.
History		This gives the list of all commands entered in the present session.

DELETING ENTRIES

Keystrokes	Function Details
Backspace	Deletes the character to the left of the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Esc, D	Deletes from the cursor to the end of the word.

RECALLING DELETED ENTRIES

Keystrokes	Function Details
Ctrl-Y	Recalls the most recent entry in the buffer (press keys simultaneously).

TRANSPOSING MISTYPED CHARACTERS

Keystrokes	Function Details
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.

CONTROLLING CAPITALIZATION

Keystrokes	Function Details
Esc, C	Capitalizes the letter at the cursor.
Esc, L	Changes the letters from the cursor to the end of the word to lowercase.
Esc, U	Capitalizes letters from the cursor to the end of the word.

COMMAND HISTORY

Keystrokes	Function Summary	Function Details
History		This gives the list of all commands entered in the present session.

EXAMPLE

```

ALU(config)# show history
1: enable
2: disable
3: en
4: disable
5: enable
6: configure t
7: interface GigabitEthernet 7/0
8: exit
9: interface GigabitEthernet 7/0
10: ip address 10.91.0.24/24
11: top
12: configure t
13: interface GigabitEthernet 7/05B
14: interface GigabitEthernet 7/0.1
15: interface GigabitEthernet 7/0:3.1
16: service completion spacebar-complete
17: no service completion spacebar-complete
18: no service completion
19: show history

```

CONFIGURING INTERFACES

This section describes the following:

- “Interface Configuration Commands”
- “Interface Types and Limitations”
- “Common Interface Configuration Commands”
- “Interface Show Commands”
- “Clear Interface Commands”
- “Backup Interface”

INTERFACE CONFIGURATION COMMANDS

This section contains the very basics for interface configuration in general and Ethernet interface configuration in particular. More information will be added later.

INTERFACE TYPES AND LIMITATIONS

Physical interface types are obviously decided by the hardware. In addition, certain physical interface types support sub-interfaces. For example, for 802.1Q VLANs and for Frame Relay (6-1007) DLCIs.

The sub-interfaces for 802.1Q should be in the range from 1 to 4096 as per the IEEE specification and 4096 sub-interfaces should be allowed (though not necessarily a good idea) for every physical interface. For Frame Relay, the number of DLCIs allowed per interface is decided by how many bits you choose to use for the DLCI.

COMMON INTERFACE CONFIGURATION COMMANDS

Command (in ICM)	Description
<code>description <line></code>	Adds a comment to help identify an interface.
<code>mtu <64-1500></code>	Adjusts the maximum packet size or MTU size.

INTERFACE IP CONFIGURATION

Command (in ICM)	Description
<code>ip address {<ip-address subnet-mask> <ip-address/prefix-length>}</code>	Assigns an IP address and subnet mask to the interface.

INTERFACE SHOW COMMANDS

TO VIEW THE DETAILS OF ALL INTERFACES OR A SPECIFIC INTERFACE

Command (in SUM)	Description
show interfaces [<i><name> <slot/port:channel.subchannel></i>]	This command displays the information of all the interfaces configured. This command displays information for a specific interface.
show interfaces brief	This command displays information of all the IP and non-IP interfaces configured.

EXAMPLE 1

```
ALU# show interfaces GigabitEthernet 7/0
```

```
GigabitEthernet7/0 is up, line protocol is down
  Hardware is Intel 82546, address is 0011.8b00.86a8
(0011.8b00.86a8)
  Internet address is 172.16.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Loopback not set
  Encapsulation ARPA,    keepalive not set
  Auto-duplex(Unknown), Auto(Unknown), 1000BaseTx/Fx
  ARP type: ARPA, ARP Timeout never
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0 (size/max), 0 drops; Input queue 0/0 (size/
max), 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 pause output
  0 output buffer copied, 0 interrupts, 0 failures
```

EXAMPLE 2**ALU# show interfaces loopback 1**

```
loopback1 is up, line protocol is up
  Hardware is Loopback
  Internet address not set
  MTU 1500 bytes, BW 1000000 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/0/0/0 (size/max/drops/flushes); Total output
drops: (null)
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

EXAMPLE 3**ALU# show interfaces**

```
loopback1 is up, line protocol is up
  Hardware is Loopback
  Internet address not set
  MTU 1500 bytes, BW 1000000 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/0/0/0 (size/max/drops/flushes); Total output
drops: (null)
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
Tunnel0 is up, line protocol is down
  Internet address is 192.168.1.2/30
  MTU 1476 bytes, BW 1000000 Kbit, DLY 0 usec,
    reliability 255/255, txload 0/255, rxload 0/255
  Loopback not set
```

```

Tunnel Specific Parameters:
  Configured Source IP address 202.202.202.2,
Destination 201.201.201.2,
  Key 0, Sequencing disabled, Checksum disabled,
  df-bit reset, mode GRE
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/
max) 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0
abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
Tunnel1 is up, line protocol is down
  Internet address not set
  MTU 1476 bytes, BW 1000000 Kbit, DLY 0 usec,
--More--

```

EXAMPLE 4

```
ALU#show interfaces brief
```

Interface	Status	Protocol
switchport1/0	Down	Down
switchport1/1	Down	Down
switchport1/2	Down	Down
switchport1/3	Down	Down
switchport1/4	Down	Down
switchport1/5	Down	Down
switchport1/6	Down	Down
switchport1/7	Down	Down
GigabitEthernet7/0	up	Down
GigabitEthernet7/1	up	Down
Tunnel0	up	Down
Tunnel1	up	Down
Tunnel3	up	Down
Tunnel5	up	Down
mlppp1	Down	Down

To View BRIEF DETAILS OF IP INTERFACES

Command (in CM)	Description
<code>show ip interface brief</code>	This command displays information about IP interfaces only.

EXAMPLE

ALU# show ip interface brief

```

Interface          IP Address      Admin State    Oper State
atm0/0             unassigned     down          down
atm0/1             unassigned     down          down
GigabitEthernet1/0 unassigned     down          down
GigabitEthernet1/1 unassigned     down          down
Vlan213            2.2.2.2        down          down
                   4.4.4.4 (s)
Loopback222        3.3.3.3        up            up
Loopback2          9.9.9.9        up            up
                   1.1.1.1 (s)
                   7.7.7.7 (s)
Loopback1          unassigned     up            up

```

CLEAR INTERFACE COMMANDS

Command (in UM)	Description
clear counters [<i><interface-name></i> <i><slot/port:channel.subchannel></i>]	Clears interface counters for specific port in specific slot.

EXAMPLE

```
ALU#(config)# clear counters GigabitEthernet 7/0
```

SHUTTING DOWN AND BRING UP AN INTERFACE

Command in (ICM)	Description
shutdown	This is entered in the Interface Configuration Mode. This command administratively brings down the interface.
no shutdown	This is entered in the Interface Configuration Mode. This command administratively brings up the interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# shutdown
```

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

BACKUP INTERFACE

When a primary interface goes down, an alternate interface in lieu of this primary interface can be brought up with the backup interface support.

The backup interface is more useful for the WAN interfaces when compared to the LAN interfaces. Most of the times, the dial on demand interfaces (like ISDN interfaces) act like backup interfaces for the regular WAN interfaces (like Serial/T1 or E1). But, technically nothing stops in utilizing one interface as backup to another interface with the exception of Loopback interfaces and bridged interfaces.

Usually the primary interface and the backup interface belong to the same subnet (they can have the same IP address) so that when the primary interface goes down, the same connected route gets added to routing table on the backup interface because of which static routes, routing protocols, etc., would work as is without any human intervention. But the features like firewall, policies, etc., that are applied on the primary interface would not be automatically applied to the backup interfaces. In typical scenarios, these feature configurations are also duplicated on to the backup interfaces.

The backup interface backs up only one primary interface. When an interface is specified as backup interface, it cannot be used for regular packet forwarding till the primary interface goes down. The state of a backup interface is 'standby' as long as primary interface is up.

TO CONFIGURE A BACKUP INTERFACE

Command (in ICM)	Description
<code>backup interface <interface-name></code>	Enter this command in the Interface Configuration mode. This command is used to configure the an interface as a backup interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# backup interface Serial1/0:0
```

To VIEW BACKUP INTERFACE DETAILS

Command (in ICM)	Description
show	This command displays the information of the backup interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# show
```

```
GigabitEthernet7/0 is up, line protocol is up
Hardware is Intel 82546, address is 0011.8b00.2712 (0011.8b00.2712)
Internet address not set
/*Interface Serial1/0:0 is backup interface*/
MTU 1500 bytes, BW 10000 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
Loopback not set
Encapsulation ARPA,    keepalive not set
Auto-duplex(Half), Auto(10), 1000BaseTx/Fx
ARP type: ARPA, ARP Timeout never
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/0 (size/max), 0 drops; Input queue 0/0 (size/max), 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    10 packets input, 7468 bytes, 0 no buffer
    Received 7 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer copied, 0 interrupts, 0 failures
```

ALU(config-if Serial1/0:0)# show

```
Serial1/0:0 is Standby, line protocol is down
  Internet address not set
  /*Interface is backing GigabitEthernet7/0 interface*/
  MTU 1500 bytes, BW 1536 Kbit, DLY 0 usec,
    reliability 255/255, txload 0/255, rxload 0/255
  Loopback not set
  Encapsulation hdlc, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/max) 0 drops
    Conversations: 0/0/0/0 (active/max active/max total)
    Reserved Conversations: 0/0 (allocated/max allocated)
  Available Bandwidth 1536 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  Timeslot(s) Used:1-24 (64Kbps each), Transmitter delay is 0 flags
```


CHAPTER 3 SYSTEM CONFIGURATION AND MONITORING

SYSTEM CONFIGURATION AND MONITORING TASKS

There are several mandatory and optional configuration options available to configure the OA-700. To get a clear insight on them, refer to the following sections:

- “[Management Plane Overview](#)”
- “[Terminal Settings](#)”
- “[System Name](#)”
- “[AAA Configuration on OA-700](#)”
- “[Setting and Displaying the System Time and Date](#)”
- “[System Logging and Debugging](#)”
- “[Rate Limiting in Statlog](#)”
- “[Saving Log Messages](#)”
- “[The File System](#)”
- “[Configuration File Management](#)”
- “[Software Package Management](#)”
- “[Reloading the System](#)”
- “[System Monitoring and Troubleshooting](#)”
- “[SNMP \(Simple Network Management Protocol\)](#)”

CHAPTER CONVENTIONS

Acronym	Description
AAA	Authentication, Authorization and Accounting
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-if)#
MIB	Management Information Base
UDP	User Datagram Protocol
SUM	Super User Mode - ALU#
SNMP	Simple Network Management Protocol

MANAGEMENT PLANE OVERVIEW

The **OA-700** extends the approach of control/data plane separation by introducing a management plane. This separation is reflected in the actual architecture of the system on a number of different levels including hardware and software. The management plane, as the name implies, handles all the aspects of managing the system.

The management functions of most of the network devices are directly accessible through the network that the router is connected to and through dedicated management ports. Managing the router, through any of the network interfaces, is called '**in-band**' management. Contrarily, management through any of the dedicated management ports, such as console or modem, are commonly referred to as '**out-of-band**' management.

OUT OF BAND MANAGEMENT (CONSOLE OR MODEM)

CONSOLE ACCESS

The console port is located in the front panel of the OA-700. The console parameters can be set with the commands given below.

Command (in CM)	Description
<code>[no] line console exec-timeout <0-35791> [<0-60>]</code>	This command is used to configure the timeout (in minutes or seconds) for console session. The console CLI session closes if it is idle for the specified time. The default timeout is 20 minutes. A zero input specifies that the console CLI should never exit when left idle.
<code>line console baudrate {115200 19200 2400 38400 4800 57600 9600}</code>	This command is used to configure baud rate. Default baudrate is 9600.

EXAMPLE

```
ALU(config)# line console exec-timeout 0

ALU(config)# line console exec-timeout 45 15

ALU(config)# no line console exec-timeout

ALU(config)# line console baudrate 19200
```

MODEM ACCESS

The **OA-700** can be managed using the modem port on its front panel.

Command (in SUM)	Description
<code>modem {enable disable}</code>	<p>This command is used to enable or disable the modem port.</p> <p>Use enable keyword to enable the modem port on the front panel.</p> <p>Use disable keyword to disable the accessibility to the OA-700 system via the modem.</p>



Note: AAA services has to be enabled before accessing OA-700 via a modem. For more information on this, refer to [“AAA Configuration on OA-700” on page 56](#) section in this chapter.

EXAMPLE

```
ALU(config)# modem enable
```

```
ALU(config)# modem disable
```



Note: (For more information on connecting the system to the external network (console and modem), refer to “Connecting the System to the Network” section in the **OA-780/OA-740 Hardware Users Guide**).

INBAND MANAGEMENT (SSH AND TELNET)

SSH (SECURE SHELL)

SSH is a program that enables logging into a remote machine, and provides secure communication between two systems.

- Inbound SSH access to the system is disabled by default. It is mandatory to have a user account configured for this. (See [“AAA Configuration on OA-700” on page 56](#)).
- Outbound SSH access is allowed for the user once the user has been authenticated. SSH access from the system is always enabled.

Command (in UM)	Description
<code>ssh {enable disable}</code>	Use this command to enable/disable the SSH service.
<code>ssh {<ip-address> <hostname>} <user-name> [version {1 2}]</code>	Use this command to access a remote computer by SSH.

EXAMPLE

```
ALU(config)# ssh enable
```

```
ALU(config)# ssh 172.25.19.1
```

```
WORD User name
```

```
ALU(config)# ssh 172.25.19.1 root
```

```
<cr>
```

```
ALU(config)# ssh 172.25.19.1 root
```

```
The authenticity of host '172.25.19.1(172.25.19.1)' can't be established.
```

```
RSA key fingerprint is
```

```
b5:b8:c9:6b:0e:28:df:a8:b0:06:7a:23:7f:03:96:6b.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '172.25.19.1' (RSA) to the list of known hosts.
```

```
root@172.25.19.1's password:
```

```
Last login: Mon Dec 6 17:34:48 2004
```

```
[root@linux-sw root]# exit
```

```
logout
```

```
Connection to 172.25.19.1 closed.
```

TELNET

Telnet is a user command with an underlying TCP/IP protocol for accessing remote computers. Telnet is a program that enables connection to foreign or remote host computers.

Telnet is not secure like SSH, but Telnet is supported on almost all Operating Systems.

- Inbound Telnet access to the system is disabled by default. It is mandatory to have a user account configured for this. (See “[AAA Configuration on OA-700](#)” on page 56).
- Outbound Telnet access is allowed for the user once the user has been authenticated. Telnet access from the system is always enabled.

Command (in UM)	Description
<code>telnet {enable disable}</code>	Use this command to enable/disable the Telnet service.
<code>telnet {<ip-address> <hostname>}</code>	This command starts a telnet connection to a remote computer.

EXAMPLE

```
ALU(config)# telnet enable
ALU(config) telnet 10.91.0.1
```



Note: For more information on connecting the system to the internal network, refer to the “Connecting the System to the Network” section in the **OA-780 Hardware Users Guide**.

There is a limit on the number of non-console CLI sessions, using SSH, telnet, and modem. For OA-780, the limit is four sessions and for OA-740, it is two sessions. This excludes the console session.

HTTP (HYPER TEXT TRANSFER PROTOCOL)

HTTP is the primary protocol used for the transfer of files over the World Wide Web. You can access the OA-700 using HTTP through a web browser after being authenticated. By default, the access is disabled.

Command (in UM)	Description
<code>http {enable disable}</code>	Use this command to enable/disable the HTTP service.

EXAMPLE

```
ALU(config)# http enable
```

HTTPS (HYPER TEXT TRANSFER PROTOCOL SECURE)

HTTPS, in addition to the normal HTTP uses SSL encryption for secure transmission of files.

Command (in UM)	Description
<code>https {enable disable}</code>	Use this command to enable/disable the HTTPS service.

EXAMPLE

```
ALU(config)# https enable
```

TO VIEW ACCESS SERVER STATUS

Command (in UM)	Description
<code>show access-server status</code>	Use this command to see the list of inband-management services that are currently enabled.

EXAMPLE

```
ALU(config)# show access-server status
http enable
https enable
ssh enable
```

IDLE TIMEOUT

The idle timeout for SSH, Telnet and Modem CLI sessions can be set by using the following command:

Command (in CM)	Description
<code>[no] line vty exec-timeout <0-35791> [<0-60>]</code>	<p>This command is used to configure the timeout (in minutes or seconds) for SSH, Telnet, and Modem CLI sessions. These sessions close if they are idle for the specified time.</p> <p>The default timeout is 20 minutes.</p> <p>A zero input specifies that the SSH, Telnet and Modem CLI sessions should never exit when left idle.</p>

EXAMPLE

```
ALU(config)# line vty exec-timeout 0
ALU(config)# line vty exec-timeout 45 15
ALU(config)# no line vty exec-timeout
```

PING

The ping command is used to check the connectivity to a specific host using the IP address/host name of that host.

Command (in UM)	Description
<code>ping {<ip-address> <hostname>}</code>	Use this command to check the connectivity between the OA-700 and any remote machine.

EXAMPLE

```
ALU> ping 192.168.10.121
```

```
Sending 5,64-byte ICMP Echos to 192.168.10.121,
timeout is 10 seconds
```

```
!!!!!
```

```
Success rate is 100 percent (5/5),
round-trip min/avg/max = 0.124/0.191/0.356 ms
```

EXTENDED PING

When a normal ping command is sent from a OA-700, the source address of the ping is the IP address of the interface that the packet uses to exit the router. If an extended ping command is used, the source IP address can be changed to any IP address on the OA-700. The extended ping is used to perform a more advanced check of host reachability and network connectivity.

In order to use this feature, enter 'ping' and press Enter. You are prompted for the fields as described below.

Field	Description
Enter the packet size[64]:	Specify the size (in bytes) of the ping packets that is to be sent out. The range being 44-18032. Default is 64 bytes.
Enter the number of packets[5]:	Number of ping packets (ICMP echo requests) to be sent. Default is 5 packets and is the same as in normal ping.
Enter the Target ip-address:	IP address to which the ping packets have to be sent.
Enter the Source IP Address:	Source IP address can be any IP address on the OA-700. If source IP address does not belong to OA-700, an error "Source IP Address does not belong to the box.Ping may not be successful" is thrown but still ping proceeds.

Field	Description
Enter the source interface:	Interface through which the ping packets (ICMP echo requests) are to be sent out. If none is entered, out interface is chosen depending on the Target IP address.
Enter the TOS value[0]:	Specify the Type of Service (ToS) value in the range 0-255. The requested ToS is placed in each probe, but there is no guarantee that all routers process the ToS. It is the Internet service's quality selection. The default is 0.
Enter the Time out value[2]:	Specify the timeout interval in the range 1-3600. The ping is declared successful only if the ECHO REPLY packet is received before this time interval. Default is 2 seconds.
Set the df-bit value[n]:	Specify whether or not the Don't Fragment (DF) bit is to be set on the ping packet. If yes is specified, the Don't Fragment option does not allow this packet to be fragmented when it has to go through a segment with a smaller maximum transmission unit (MTU), and you will receive an error message from the device that wanted to fragment the packet. This is useful for determining the smallest MTU in the path to a destination. The default is no.
Set the ttl value[64]:	Specify the Time to live (ttl) value in the range 1-255. The number of hops a packet can have before it is discarded in the network. Each router reduces the ttl value by one before forwarding it. It is a way of making sure that the packets destined to non-existing targets die out eventually. Default is 64.

Once the above fields are entered and ping is initiated, you will see the following output:

!!!! : Each exclamation point (!) denotes receipt of a reply. A period (.) denotes that the network server has timed out while waiting for a reply.

Success rate is 100 percent: Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.

round-trip min/avg/max = 2/4/5 ms: Round-trip travel time intervals for the protocol echo packets, including minimum/average/maximum (in milliseconds).

EXAMPLE

The following is an example of "extended ping" command:

```
ALU# ping
Enter the packet size[64]:100
Enter the number of packets[5] :7
Enter the Target ip-address:2.2.2.12
Enter the Source IP Address:
Enter the source interface:
Enter the TOS value[0]:
Enter the Time out value[2]:
Set the df-bit value[n]:
Set the ttl value[64]:
Press ^C to Stop..
Sending 7,92-byte ICMP Echos to 2.2.2.12,timeout is 2 seconds
!!!!!!!
Success rate is 100 percent (7/7),round-trip min/avg/max =
3.499/3.833/3.915 ms
```

TRACEROUTE

The traceroute utility displays the route used by IP packets on their way to a specified network/host, across a TCP/IP network. It displays the IP number and host name of the machines along that route. It is used as a network debugging tool. If there are network connectivity problems, it will show the origin of the trouble along the route.

Traceroute is also a troubleshooting utility like ping, which gives you the information about the exact hops taken by a packet to reach its destination.

Command (in UM)	Description
<code>traceroute {<ip-address> <hostname>}</code>	This command displays the route taken by IP packets.

EXAMPLE

```
ALU> traceroute 10.91.10.178
```

```
traceroute to (10.91.10.178), 30 hops max, 38 byte packets.
 1  10.91.0.1 (10.91.0.1) 0.700 ms  0.703 ms  0.621 ms
 2  10.91.10.178 (10.91.10.178) 0.951 ms  0.961 ms  0.960 ms
```

EXTENDED TRACEROUTE

The extended traceroute command is a variation of the traceroute command. An extended traceroute command can be used to see what path packets take in order to get to a destination. The command can also be used to check routing at the same time. This is helpful for troubleshooting routing loops, or to determine where packets are getting lost. You can use the extended ping command in order to determine the type of connectivity problem, and then use the extended traceroute command in order to narrow down where the problem occurs.

A "time exceeded" error message indicates that an intermediate communication server has seen and discarded the packet. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, trace prints an asterisk(*). The command terminates when any of these happens:

- the destination responds
- the maximum TTL is exceeded
- the user interrupts the trace with the escape sequence.

The following table lists the traceroute command field descriptions:

Field	Description
Enter the Target IP address:	Enter an IP address. There is no default.
Enter the Source IP Address:	The interface or IP address of the OA-700 to be used as a source address for the probes. If source IP address is not specified, the router normally picks the IP address of the outbound interface to use.
Enter the source interface:	Specify the outbound interface to send the trace packets through. Is useful when there are two routes for a destination. Trace packets will have the interface's IP address as source IP address.
Enter the Datagram Size[38]:	Specify the ICMP payload size (in bytes) in the range 36-18024. Default size is 38 bytes.
Enter the Timeout value[2]:	Enter the number of seconds to wait for a response to a probe the packet. The range being 1-3600 (in seconds). The default is 2 seconds.
Enter the Probecount[3]:	Enter the number of probes to be sent at each TTL level in the range 1-10. The default count is 3.
Enter the Minimum TTL[1]:	The TTL value for the first probe in the range 1-255. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Enter the Max TTL[30]:	The largest TTL value that can be used in the range 1-255. The traceroute command terminates when the destination is reached or when this value is reached. The default is 30. The maximum TTL value should be greater than the minimum TTL value.
Enter the Destination Port[33434]:	The destination port to be used by the UDP probe messages. Port number to be between 1-65535. The default is 33434.

Field	Description
Enter the TOS value[0]:	Specify the Type of Service (ToS) value in the range 0-255. The requested ToS is placed in each probe, but there is no guarantee that all routers process the ToS. It is the Internet service's quality selection. The default is 0.
Set the df-bit value[n]:	Specify whether or not the Don't Fragment (DF) bit is to be set on the ping packet. If yes is specified, the Don't Fragment option does not allow this packet to be fragmented when it has to go through a segment with a smaller maximum transmission unit (MTU), and you will receive an error message from the device that wanted to fragment the packet. This is useful for determining the smallest MTU in the path to a destination. The default is no.

EXAMPLE

```

ALU(config)# traceroute
Enter the Target IP address:2.2.2.12
Enter the Source IP Address:
Enter the source interface:
Enter the Datagram Size[38]:
Enter the Timeout value[2]:
Enter the Probecount[3]:
Enter the Minimum TTL[1]:
Enter the Max TTL[30]:
Enter the Destination Port[33434]:
Enter the TOS value[0x0]:
Set the df-bit value[n]:
traceroute to 2.2.2.12 (2.2.2.12), 30 hops max, 38 byte
packets.
1  2.2.2.12 (2.2.2.12) 3.151 ms *    2.2.2.12 (2.2.2.12)
4.089 ms

```

TERMINAL SETTINGS

Command (in CM)	Description
<code>terminal length <0-512></code>	Sets the terminal length for the session.
<code>terminal monitor [priority <0-7>]</code>	This command is used to display the log messages of specified and lower (numerically higher) priorities in the terminal window. This terminal could be launched through SSH or Telnet.

EXAMPLE

```
ALU(config)# terminal length 10
```

```
ALU(config)# terminal monitor
```

SYSTEM NAME

By default, the System name is "ALU". To give the system a more informative name, use the 'hostname' command. The host name shows up in the CLI prompt.

Command (in CM)	Description
<code>hostname <name></code>	To configure the system name.

EXAMPLE

```
ALU(config)# hostname ALU
```

AAA CONFIGURATION ON OA-700

The OA-700 is targeted at the edge of enterprises that have a good deal of valuable data in their networks.

It is important to ensure that the customer has knowledge and control over the following: Who can access, manage or use the system? What these users are allowed to do to the system, or through the system? What was done to the system by these users? Where the above information is stored or retrieved from?

AAA (Authentication, Authorization, and Accounting) is a system in IP-based networking to control the resources that users have access to and to keep track of the user activity over a network.

- Authentication is the process of identifying an individual, usually based on a user name and password. Authentication is based on the idea that each individual user will have some unique information, that sets the user apart from others.
- Authorization is the process of granting or denying a user access to network resources once the user has been authenticated. The amount of information and the type of services the user has access to depends on the user's authorization level.
- Accounting is the process of keeping track of a user's activity while accessing the network resources including the amount of time spent in the network, the services accessed and the amount of data transferred during the session. Accounting data is used for trend analysis, capacity planning, billing, auditing, and cost allocation.

AAA services often require a server that is dedicated to providing these three services. RADIUS, DIAMETER, TACACS, and TACACS+ are some often used AAA protocols.

To ENABLE AAA SERVICES

Command (in CM)	Description
<code>aaa services</code>	This command is used to enable the AAA services.
<code>no aaa services</code>	This command is used to disable the AAA services.

EXAMPLE

```
ALU(config)# aaa services
```

```
ALU(config)# no aaa services
```

AUTHENTICATION COMMANDS

Authentication is the process of validating the user, on the basis of some differentiating private information. It verifies that the user is who the user claims to be.

There are various authentication methods that are supported:

- Local Authentication
- RADIUS Server Group
- TACACS+ Server Group

LOCAL AUTHENTICATION METHOD

TO CONFIGURE USER ACCOUNT

Command (in CM)	Description
username <user-name> { password [5] <password> nopassword secret [5] <password>}	<p>This command is used to create a new user account and user password. The User-accounts configured using this command will form a part of the local database.</p> <p>5: If this keyword is used, then enter the password in an encrypted format.</p> <p>nopassword: This indicates that no password is required for this user to log in.</p> <p>secret: Stores the user password in an encrypted format.</p>
no username <user-name>	The ' no ' command deletes the specified user account.

EXAMPLE

```
ALU(config)# username ALU1 password pass1
```


```
ALU(config)# username ALU1 nopassword
```

```
ALU(config)# username ALU1 secret pass2
```

RADIUS SERVER GROUP CONFIGURATION

A RADIUS server group is a list of radius servers, which can be used as an authentication method in a method-list. The servers are approached in the order they are specified for authentication information.

TO CONFIGURE A RADIUS SERVER GROUP

Command (in CM)	Description
<pre>aaa server-group radius <name></pre>	<p>This command is used to configure a RADIUS server group.</p>  <p>Note: You cannot enter a RADIUS server group as 'local' as it is a reserved keyword for a pre-defined authentication method.</p> <p>This command enters the RADIUS Server-Group mode.</p>
<pre>no aaa server-group radius <name></pre>	<p>This command deletes the specified RADIUS server group.</p> <p>You cannot delete a RADIUS server group if it is associated to any method list.</p>

EXAMPLE

```
ALU(config)# aaa server-group radius rad1
ALU(config-srv-grp-rad1)#
```

The following error is displayed if you try to configure a RADIUS server group with the name 'local':

```
ALU(config)# aaa server-group radius local
The name of the Group is reserved
```

```
ALU(config)# no aaa server-group radius rad1
```


TO ADD A RADIUS SERVER TO THE RADIUS SERVER GROUP

Command (in RADIUS Server Group CM)	Description
<code>radius-server <ip-address> [{auth-port <1-6000> deadtime <1-1440> key {5 [string] <string>} retransmit <1-100> timeout <1-1000>}]</code>	This command is used to add the RADIUS server of the specified IP address into RADIUS server group. You can also specify the server specific parameters like auth-port port-number, dead time, key string, etc.
<code>no radius-server <ip-address></code>	This command removes the RADIUS Server from the server group.

EXAMPLE

```
ALU(config-srv-grp-rad1)# radius-server 1.1.1.1
```

```
ALU(config-srv-grp-rad1)# no radius-server 1.1.1.1
```

TO CONFIGURE RADIUS SERVER GROUP GLOBAL OPTIONS



Note: In the Configuration mode, you can configure RADIUS server global options like timeout, key, and authentication port. You can also configure these values on a per server basis. Per-server values should be entered in the RADIUS Server Group Configuration Mode.

The per-server parameters override the global ones, in case both are configured. Default global values for these parameters exist that will come into effect if neither per-server nor global values are configured explicitly.

The following are the RADIUS server options:

- Authentication Port (auth-port): This is the destination port on which the RADIUS server is listening.
- Deadtime: The time (in minutes) that should elapse, before you again try to connect to a non-responding server.
- Key: This is the encryption key between the OA-700 and the RADIUS server.
- Timeout: This determines the number of seconds that the OA-700 should wait for a reply from the RADIUS server before retrying.
- Retransmit: The number of retries after each “timeout” interval, before giving up on the server.

Command (in CM)	Description
<pre>[no] radius-server auth- port <1-6000></pre>	<p>This command is used to specify a global authentication port that will be applied to all the RADIUS Server Groups (provided there is no server specific port configured).</p> <p>The default authentication port is 1812.</p> <p>The 'no' command deletes the global RADIUS auth-port from the configuration, and resets it to default (for all servers that do not have a server specific port).</p>
<pre>[no] radius-server deadtime <1-1440></pre>	<p>This command is used to specify a global deadtime value that will be applied to all the RADIUS Server Groups (provided there is no server specific deadtime configured.)</p> <p>The default deadtime value is 5 minutes.</p> <p>The 'no' command deletes the global RADIUS deadtime value from the configuration, and resets it to default (for all servers that do not have a server specific deadtime value).</p>
<pre>[no] radius-server key {5 [<string>] <string>}</pre>	<p>This command is used to specify a global key that will be applied to all the RADIUS Groups (provided there is no server specific key configured).</p> <p>If '5' option is used, then enter the key string in an encrypted format.</p> <p>The default key is "" (empty string).</p> <p>The 'no' command deletes the global RADIUS key from the configuration, and resets it to default (for all servers that do not have a server specific key).</p>

Command (in CM)	Description
<pre>[no] radius-server retransmit <1-100></pre>	<p>This command is used to specify a global retransmit value that will be applied to all the RADIUS Groups (provided there is no server specific retransmit value configured).</p> <p>The default retransmit value is 3.</p> <p>The 'no' command deletes the global RADIUS retransmit value from the configuration, and resets it to default (for all servers that do not have a server specific retransmit value).</p>
<pre>[no] radius-server timeout <1-1000></pre>	<p>This command is used to specify a global timeout value that will be applied to all the RADIUS Groups (provided there is no server specific timeout value configured).</p> <p>The default timeout value is 5 seconds.</p> <p>The 'no' command deletes the global RADIUS timeout value from the configuration, and resets it to default (for all servers that do not have a server specific timeout value).</p>

EXAMPLE

```
ALU(config)# radius-server auth-port 1800

ALU(config)# radius-server deadtime 10

ALU(config)# radius-server key test


ALU(config)# radius-server retransmit 5

ALU(config)# radius-server timeout 10
```

TACACS+ SERVER GROUP CONFIGURATION

A TACACS+ server group is a list of TACACS+ servers, which can be used as an authentication method in a method-list. The servers are approached in the order they are specified for authentication information.

TO CONFIGURE A TACACS+ SERVER GROUP

Command (in CM)	Description
<pre>aaa server-group tacacs <name></pre>	<p>This command is used to configure a TACACS+ server group.</p>  <p>Note: You cannot enter a TACACS+ server group as 'local' as it is a reserved keyword for a pre-defined authentication method.</p> <p>This command enters the TACACS+ Server-Group mode.</p>
<pre>no aaa server-group tacacs <name></pre>	<p>This command deletes the specified TACACS+ server group.</p> <p>You cannot delete a TACACS+ server group if it is associated to any method list.</p>

EXAMPLE

```
ALU(config)# aaa server-group tacacs tac1
ALU(config-srv-grp-tac1)#
```

The following error is displayed if you try to configure a TACACS+ server group with the name 'local':

```
ALU(config)# aaa server-group tacacs local
The Name of the Group is reserved
```

```
ALU(config)# no aaa server-group tacacs tac1
```

To Add A TACACS+ SERVER TO THE TACACS+ SERVER GROUP

Command (in TACACS+ Server Group CM)	Description
<code>tacacs-server <ip-address> [{auth-port <1-1000> key {5 [<string>] <string>} timeout <1-1000>}]</code>	This command is used to add the TACACS+ server of the specified IP address into the TACACS+ server group. You can also specify the server specific parameters like auth-port port-number, timeout, and key string.
<code>no tacacs-server <ip-address></code>	This command removes a TACACS+ Server from the server group.

EXAMPLE

```
ALU(config-srv-grp-tac1)# tacacs-server 1.1.1.2
```

```
ALU(config-srv-grp-tac1)# no tacacs-server 1.1.1.2
```

To CONFIGURE TACACS+ SERVER GROUP GLOBAL OPTIONS



Note: In the Configuration Mode, you can configure TACACS+ server global options like timeout, key, and authentication port. You can also configure these values on a per server basis. Per-server values should be entered in the TACACS+ Server Group Configuration Mode.

The per-server parameters override the global ones, in case both are configured. Default global values for these parameters exist that will come into effect if neither per-server nor global values are configured explicitly.

The following are the TACACS+ server options:

- Authentication Port (auth-port): This is the destination port on which TACACS+ server is listening.
- Key: This is the encryption key between the OA-700 and the TACACS+ server.
- Timeout: This determines the number of seconds that the OA-700 should wait for a reply from the TACACS+ server before retrying.

Command (in CM)	Description
<pre>[no] tacacs-server auth- port <1-1000></pre>	<p>This command is used to specify a global authentication port that will be applied to all the TACACS+ Server Groups (provided there is no server specific port configured).</p> <p>The default authentication port is 49.</p> <p>The 'no' command deletes the global TACACS+ auth-port from the configuration, and resets it to default (for all servers that do not have a server specific port).</p>
<pre>[no] tacacs-server key {5 [<string>] <string>}</pre>	<p>This command is used to specify a global key that will be applied to all the TACACS+ Groups (provided there is no server specific key configured).</p> <p>If '5' option is used, then enter the key string in an encrypted format.</p> <p>The default key is "" (empty string).</p> <p>The 'no' command deletes the global TACACS+ key from the configuration, and resets it to default (for all servers that do not have a server specific key).</p>
<pre>[no] tacacs-server timeout <1-1000></pre>	<p>This command is used to specify a global timeout value that will be applied to all the TACACS+ Groups (provided there is no server specific timeout value configured).</p> <p>The default timeout value is 5 seconds.</p> <p>The 'no' command deletes the global TACACS timeout value from the configuration, and resets it to default (for all servers that do not have a server specific timeout value).</p>

EXAMPLE



```
ALU(config)# tacacs-server auth-port 100
```

```
ALU(config)# tacacs-server key test1
```

```
ALU(config)# tacacs-server timeout 10
```

ENABLE AUTHENTICATION

An extra layer of security is provided by enable-authentication. If configured, it enquires the user for a password, before granting entry into Super User Mode through CLI. If enable authentication is not configured, a user gaining CLI access through console is granted access into Super User Mode without being asked for any password. However, users logging in through remote CLI sessions (SSH, telnet and modem) are not allowed privileged access without enable authentication configuration. If an authentication method requiring user-name (RADIUS and TACACS+ server-groups), is associated with enable-authentication, then a default user name of **\$enab15\$** is used.

Command (in CM)	Description
<code>enable {secret password} [5] <password></code>	<p>Sets the password to grant access to the privileged mode.</p> <p>secret: The password is stored in an encrypted format.</p> <p>"5" specifies that the password is already given in an encrypted format.</p>  <p>Note: The password cannot contain '!' character, since it marks the beginning of a comment.</p>
<code>no enable-authentication</code>	<p>The 'no' command deletes the existing enable-password configuration, thereby disabling enable-authentication.</p>  <p>Note: As a result, console clients will be granted access to the enable-mode without being prompted the password.</p> <p>Remote clients will be denied access with the message 'No password Set'.</p> <p>This is the default behavior.</p>

EXAMPLE

```
ALU(config)# enable secret test
Secret for level 15 is set
```

METHOD-LIST CONFIGURATION

A method-list is a list of authentication methods. It specifies the sequence of authentication methods to be approached for authentication. The methods are queried in the order in which they are specified.

Possible authentication methods include a pre-defined RADIUS server group, TACACS+ server group, and local authentication.

A method-list needs to be associated with a particular type of client. Whenever a user tries to login through that type of client, the list is traversed in the order in which the methods are specified. That is to say, the first method is queried first. Now if the first method authenticates the user, the user is allowed access. If it says that the user is not authenticated, then the user is denied access. But, if there is an error in the query, then the second method in the list is approached and similar steps are repeated, until the end of the list is reached. If there are errors in queries to all the methods, then the user is denied access.

TO CONFIGURE A METHOD-LIST

Command (in CM)	Description
<code>aaa method-list <name> <methods>...</code>	This command is used to configure a method-list. A method list can be successfully configured only if the lists do not contain any invalid method like – empty radius/TACACS+ groups, etc.
<code>no aaa method-list <name></code>	This command deletes the specified method-list. You cannot delete a method list if it is associated to any client-type.

EXAMPLE

```
ALU(config)# aaa method-list m1 rad1 tac1 local
```

The following example shows that you cannot configure a method-list with an invalid method:

```
ALU(config)# aaa method-list m1 tac2
```

One of the Specified Groups doesn't have any server in it

```
ALU(config)# no aaa method-list m1
```


ASSOCIATING METHOD-LIST WITH A CLIENT-TYPE

The different client-types to which clients can belong are:


- Console
- Remote-Login
- Web (HTTP)
- dot1X (802.1X)
- Enable




Note: The Client Type 'Remote-Login' is a reference to SSH and TELNET clients.

'Enable' is the type associated with clients seeking access into Super User Mode (SUM).

You can associate only one method-list to a client-type.

Command (in CM)	Description
<code>[no] aaa authentication console <method-list-name></code>	<p>This command associates an already configured method-list with the dot1X client-type.</p> <p>The 'no' command removes the associated method-list from the console client-type.</p>
<code>[no] aaa authentication dot1x <method-list-name></code>	<p>This command associates an already configured method-list with dot.1X client-type.</p> <p></p> <p>Note: The method-list to be associated with dot1x clients should contain only RADIUS server groups as its methods.</p> <p>The 'no' command removes the associated method-list from the 802.1x client-type.</p>
<code>[no] aaa authentication enable <method-list-name></code>	<p>This command associates an already configured method-list with clients seeking access to Super User Mode.</p> <p>The 'no' command removes the associated method list from the enable client-type.</p>

Command (in CM)	Description
<pre>[no] aaa authentication remotelogin <method-list- name></pre>	<p>This command associates an already configured method-list with remote login client-type.</p>  <p>Note: The client-type 'Remote-Login' is a reference to SSH and TELNET clients.</p> <p>The 'no' command removes the associated method list from the remote login client-type.</p>
<pre>[no] aaa authentication web <method-list-name></pre>	<p>This command associates an already configured method-list with the web client-type (HTTP clients).</p> <p>The 'no' command removes the associated method-list from the web client-type.</p>

EXAMPLE

```
ALU(config)# aaa authentication console m1

ALU(config)# aaa authentication dot1x m2

ALU(config)# aaa authentication enable m1

ALU(config)# aaa authentication remotelogin m1

ALU(config)# aaa authentication web m1
```

AAA SPECIAL USERS

The system will always contain a default user called "superadmin". You will be asked to configure the password for superadmin, when the OA System boots up for the first time, or when there is no start-up configuration, in the following way:

```
Enter the new password for the superadmin:
Retype the new password:
Superadmin password updated...
```

In case of accidental loss of superadmin's password, you will be able to reset (but not recover,) the password as long as you have the physical access to the device over the console. For this purpose, there is a special user defined in the system called "recovery". This user login is valid only over the console. The default (non editable) password for this login would be the chassis ID, which is displayed as part of chassis information, both in CLI and Device Manager. The serial-number of the back panel is considered to be the chassis ID. It could be obtained through "show chassis" in this way:

EXAMPLE

```
ALU(config)# show chassis
    Physical inventory at Tue Oct 30 06:33:47 2007
    System started approximately Tue Oct 30 06:30:26 2007
    Uptime is 0 days 0 hours 4 minutes 20 seconds
L2 - 8-port copper GigE (active)
    Slot number: 0
    Part number: 902603-90
    Manufacturer: ALU
    Description: 8-port copper GigE
    Serial number: DD0512560340
    Version: 00
    Revision: 01
    Deviation: 0000
    Loader version: 2.27
    ALU-OS version: 2.2.52
    MDC
    Serial number: WL0534000127
    Deviation: 0001
    Revision: A1
    Version: 01
SE - Service engine (active)
    Slot number: 3
    Part number: 902601-90
    Manufacturer: ALU
    Description: Service engine
    Serial number: DD0538002048
    Version: 01
    Revision: 04
    Deviation: 0001
    CPU Version: 1 (Low Power Opteron)
    Opteron CPU Version: 1
    Opteron CPU Frequency: 2193 MHz
    Loader version: 2.30
```

```
ALU-OS version: 2.2.64
MDC
Serial number: WL0529000008
Deviation: 0002
Revision: 05
Version: 01
PB - Power tray (passive)
Slot number: 22
Part number: 902612-90
Manufacturer: ALU
Description: Power tray
Serial number: DD0536004050
Version: 00
Revision: 01
Deviation: 0000
SC - Switch card (active)
Slot number: 24
Part number: 902613-90
Manufacturer: ALU
Description: Switch card
Serial number: DD0536054350
Version: 00
Revision: 54
Deviation: aaaa
LoL firmware version: 2.2.56
Loader version: 2.29
ALU-OS version: 2.2.52
FP - Fan tray (passive)
Slot number: 26
Part number: 902614-90
Manufacturer: ALU
Description: Fan tray
Serial number: DD0545027001
Version: 00
Revision: 01
Deviation: 0000
BP - ALU OA780 chassis (passive)
Slot number: 29
Part number: 902611-90
Manufacturer: ALU
Description: ALU OA780 chassis
Serial number: DD0546005005
Version: 00
Revision: 01
Deviation: 0000
Base MAC: 00:11:8b:00:72:00
```

You are expected to either remember the chassis ID (**the one in bold font in the Show Chassis output given above**) or should have access to the shipment details. When you login with this user ID, the only allowed operation is to reset the superadmin password and exit from the CLI. You can then login using the newly configured superadmin password.

AAA MISCELLANEOUS COMMANDS

Command (in CM)	Description
<pre>[no] aaa authentication banner <delimiter><multi- lined string><delimiter></pre>	<p>This command is used to enter a descriptive message to be displayed before the user is asked for user-name and password credentials.</p> <p>Enter a delimiting character to start the message. This character should not appear in the message to be displayed. Enter the message and end it with the delimiting character used. (You can enter a multi-lined descriptive message).</p>
<pre>[no] aaa authentication success-message <delimiter><multi-lined string> <delimiter></pre>	<p>This command is used to enter a descriptive message to be displayed after a successfully authenticated login.</p> <p>Enter a delimiting character to start the message. This character should not appear in the message to be displayed. Enter the message and end it with the delimiting character used. (You can enter a multi-lined descriptive message).</p>
<pre>[no] aaa authentication fail-message <delimiter>< multi-lined string> <delimiter></pre>	<p>This command is used to enter a descriptive message to be displayed after a failed login attempt.</p> <p>Enter a delimiting character to start the message. This character should not appear in the message to be displayed. Enter the message and end it with the delimiting character used. (You can enter a multi-lined descriptive message).</p>
<pre>[no] aaa authentication username-prompt <prompt- text></pre>	<p>This command is used to customize the text, which is displayed to request the user trying to log in, to enter his user name. The default user name-prompt is "Username:".</p> <p>The 'no' command brings the default back into effect.</p>
<pre>[no] aaa authentication password-prompt <prompt- text></pre>	<p>This command is used to customize the text, which is displayed to request the user trying to log in, to enter his password. The default password-prompt is "Password:".</p> <p>The 'no' command brings the default back into effect.</p>

EXAMPLE

```
ALU(config)# aaa authentication banner @Only authorized access
permitted.@"
```

```
ALU(config)# aaa authentication success-message $Login attempt
successfull.$
```

```
ALU(config)# aaa authentication fail-message $Login failed!$
```

```
ALU(config)# aaa authentication username-prompt u1
```

```
ALU(config)# aaa authentication password-prompt p1
```

SHOW COMMANDS

AUTHENTICATION SHOW COMMANDS

TO VIEW LOCAL USERS DETAILS

Command (in SUM/CM)	Description
<code>show aaa-local-users-details</code>	This command displays the details of all the locally configured users on the system.

EXAMPLE

```
ALU(config)# show aaa-local-users-details
```

```
username recovery password 5 790649743532a8280244f482f6199744
username superadmin password 5 d41d8cd98f00b204e9800998ecf8427e
```

TO VIEW CONFIGURED METHOD LISTS

Command (in SUM/CM)	Description
<code>show aaa-methodlists</code>	This command displays all the configured method-lists on the system.

EXAMPLE

```
ALU(config)# show aaa-methodlists
```

```
aaa method-list m1 rad1 tac1 local
aaa method-list m2 tac1
```

TO VIEW METHOD-LISTS ASSOCIATED WITH THE CLIENT-TYPE

Command (in SUM/CM)	Description
<code>show aaa-client-methodlist-associations</code>	This command displays the associations between client types and method-lists.

EXAMPLE

```
ALU(config)# show aaa-client-methodlist-associations
```

```
aaa authentication remotellogin m2
aaa authentication web m1
```

To VIEW RADIUS SERVER GROUP CONFIGURATION

Command (in SUM/CM)	Description
<code>show aaa-radius</code>	This command shows the details of the RADIUS Server Groups configured.

EXAMPLE

```

ALU(config)# show aaa-radius
!
aaa server-group radius rad1
radius-server 1.1.1.1
!
!
aaa server-group radius rad3
radius-server 1.1.1.1 auth-port 300
!

```

To VIEW TACACS+ SERVER GROUP CONFIGURATION

Command (in SUM/CM)	Description
<code>show aaa-tacacs</code>	This command shows the details of all the TACACS+ Server Groups configured.

EXAMPLE

```

ALU(config)# show aaa-tacacs
!
aaa server-group tacacs tacl
tacacs-server 12.34.42.2
tacacs-server 23.4.2.232 auth-port 2050 key some
!

```


SETTING AND DISPLAYING THE SYSTEM TIME AND DATE

The **clock set** command sets the RTC (Real Time Clock) as well as the system's operational time and date. The RTC is set to the correct value during manufacturing, and it can be manually set very rarely. The clock's value is always set and maintained as UTC (Universal Time Coordinated) and therefore valid anywhere in the world.

The **show clock** command will display the setting of the RTC, the system clock and how the system clock is being synchronized with an external, trusted time source.

The RTC is battery powered only when the chassis is powered down, it will maintain time with reasonable accuracy even if the chassis is powered down. Typically, the RTC is only read during power up in order to initialize the system clock. However, it may be used as a trusted time source and read periodically to adjust the system time.

The system time is the time coordinated among the various processors in the chassis. It is this time that may be synchronized with an external source.

However, if the system is configured to coordinate its system time with a trusted external source (e.g., NTP), the system time and the RTC may not match. The system time and the RTC can be set to the same time by either setting the clock (see **clock set** description) or by reloading the system.



Note: The failure of the RTC to maintain the correct time after a power cycle may be a symptom of a discharged battery. The internal battery is not a field serviceable. Contact Services & Support for chassis replacement instructions.

CLOCK SET

The following commands are used to set the system clock and to view the system clock:

Command (in SUM)	Description
<code>clock set <hh:mm:ss> <mm/dd/yyyy></code>	This command allows you to set the RTC as well as the system's clock - date and time. The time must be specified as GMT. The year range is between 2000 - 2036.
<code>show clock</code>	This command displays the system's operational date and time.

EXAMPLE

```
ALU# clock set 17:59:20 09/25/2007
```

```
The system clock is changed.
Current setting is Tue Sep 25 17:59:20 2007
```

```
ALU# show clock
```

```
RTC set to Tue Sep 25 18:00:06 2007
System time is Tue Sep 25 18:00:06 2007
Not synchronized with external source
```

CLOCK SYNCHRONIZE

The clock synchronize command establishes how, from where, and how often the chassis should synchronize its time with an external source.

There are three elements to the specification:

- **Protocol**

This is the protocol to be used. Most common is the NTP protocol. Another option is the more basic rdate. It is desirable to synchronize the system time from the RTC.

- **Server**

The address of the server that is used as the external time source. This is valid only for NTP and RDATE protocols.

- **Rate**

The rate at which the synchronization should be performed. Typically, the settings are in the multi-hour range. The default value for the rate is every 12 hours.

Command (in SUM)	Description
<code>clock synchronize [{using {ntp rdate rtc} }] [server <name>] [every <number> {hours minutes}]</code>	This command establishes how the chassis should synchronize its time with an external source.

Note:

1. Server name is mandatory for ntp and rdate protocols.
2. The parameter “number” depicts the number of minutes or hours between updates.
3. The server name can be specified either in dotted numeric or domain name format.

EXAMPLE

```
ALU(config)# clock synchronize using ntp server 10.91.2.87
every 2 hours
```

This command has no output. To verify the settings, use the ‘**show clock**’ command described in this section.

SYSTEM LOGGING AND DEBUGGING

The **OA-700** can be configured for logging, based on severity of the message and module. The severity of the log messages are indicated by the priority, which varies from 0-7. Lower the numerical value of priority, higher is the criticality of the message.

- 0 - emergency
- 1 - alert
- 2 - critical
- 3 - errors
- 4 - warnings
- 5 - notifications
- 6 - informational
- 7 - debugging

The logging information can further be directed to the logging buffer, console, terminal, or remote Syslog server. By default, logging to the console and buffer logging is **"ON"**.

Command (in CM)	Description
<code>[no] logging on</code>	This command is used to enable logging of messages. By default, logging of messages is enabled. The 'no' command disables logging.
<code>[no] logging buffered [priority <0-7>/size <4-16384>]</code>	This command is used to store the log information in the memory buffer. If a priority value is given, messages of that priority and higher (numerically lower) will be buffered. Size denotes the buffer size in kilobytes and can vary from 4 - 16384 kilobytes.
<code>[no] logging remote <ip-address> [port <0-65535> priority <0-7>]</code>	This command is used to configure an external server to store log messages. The default port is 514 and default priority level is 7.
<code>[no] logging console priority <0-7></code>	This command is used to display the log messages of the specified priority and higher on the console.
<code>[no] logging system</code>	This command is used to log all the Kernel messages. By default, messages with a priority of 5 and lower will be logged.

Command (in CM)	Description
<code>[no] logging watermark <100-10000></code>	This command is used to set a watermark level (in terms of number of log messages) up to which the log messages get stored.
<code>[no] service timestamps log</code>	This command is used to display the date and time of the log messages. By default, Service timestamps log is enabled.
<code>terminal monitor <0-7></code>	This command displays log messages of the given priority and higher on a terminal that has been launched through SSH or Telnet.
<code>clear logging</code>	This clears the contents of the logging buffer.

EXAMPLE

```

ALU(config)# logging on

ALU(config)# logging buffered priority 5

ALU(config)# logging remote 1.1.1.1 priority 5

ALU(config)# logging console priority 5

ALU(config)# logging system

ALU(config)# logging watermark 10000

ALU(config)# service timestamps log

ALU(config)# terminal monitor

ALU(config)# clear logging

```

The **show logging** and **show logging buffered** commands can be used to view the current logging and debugging configuration and the logging buffer.

Command (in SUM / CM)	Description
show logging	Displays log messages with priority 6 and higher.
show logging priority <0-7>	Displays the log messages of specified priority and higher (numerically lower).
show logging tag <tag-name>	Displays the log messages in reference to the tag value. The tag is the module which generated the log. The tag name is case insensitive.
show logging string <string-value>	Displays all the messages which holds the value of the given string. A case sensitive search is performed.

EXAMPLE 1

This example shows messages of priority 6 and higher (numerically lower):

```
ALU> show logging
!
! Statlog Configuration
!
statlog global logging: enabled
buffer logging: level debugging (7)
buffer logging: size (128 k)
buffer logging: used (49.94%)
console logging: level errors (3)
system logging: level notifications (5)
logging timestamp : enabled
!
2005 Oct 13 03:31:06: %CM-6-LOG:LIVENESS 2[83000019 will report once on failure
2005 Oct 13 03:31:07: %CM-6-LOG: SCAN card removed from slot 2
2005 Oct 13 03:31:07: %CM-5-LOG: SLOT L2 (83000019) is vacated
2005 Oct 13 03:31:08: %CM-6-LOG: LIVENESS 2[83000019] will report once on failure
2005 Oct 13 03:31:08: %CM-6-LOG: SCAN card removed from slot 2
2005 Oct 13 03:31:09: %CM-5-LOG: SLOT L2 (83000019) is vacated
2005 Oct 13 03:31:09: %CM-6-LOG: LIVENESS 2[83000019] will report once on failure
2005 Oct 13 03:31:12: %CM-6-LOG: SCAN card removed from slot 2
```

EXAMPLE 2

The following example shows messages of priority 3 or higher.

```
ALU> show logging priority 3
```

```
2005 Oct 13 04:41:30: %MIM-1-LOG: Interface GigabitEthernet7/0, changed state to down
2005 Oct 13 04:41:30: %MIM-1-LOG: Line protocol on Interface
GigabitEthernet7/0, changed state to down
2005 Oct 13 14:13:06: %ntpdate-3-LOG: No server suitable for synchronization found
```

The following example shows only the messages with priority 3:

```
ALU> show logging priority 3 exact
```

```
2005 Oct 13 14:13:06: %ntpdate-3-LOG: No server suitable for synchronization found
```

EXAMPLE 3

The following example shows messages containing the text “temperature”:

```
ALU(config)# show logging string temperature
```

```
2006 Sep 19 09:59:23: %CM-7-LOG: SCAN chassis temperature 47; setting fan speed to
high succeeded
2006 Sep 19 10:00:59: %ENVAGT-4-LOG: EA.7: Cannot read temperature sensor
```

EXAMPLE 4


The following example shows messages from a particular module, say, CLI:

```
ALU> show logging tag cli
```

```
2005 Oct 13 03:49:59: %CLI-6-LOG: User: successfully entered into Super user mode
2005 Oct 13 10:44:47: %CLI-6-LOG: A Client Logged in to the Box through SSH from
10.91.2.87
2005 Oct 13 10:45:41: %CLI-6-LOGSRV: Logging buffer size set to 128K by
User:privileged user.
```

RATE LIMITING IN STATLOG

Statlog rate limiting feature stabilizes the system performance when per packet level logging is configured. These commands are used in the Configuration mode.

Command (in CM)	Description
<pre>[no] logging rate-limit <1-10000> [<1-3600>] {priority <0-7> tag <string> [subtag <string>]}</pre>	<p>This command is used to limit the number of messages (in the range 1-10000) generated by a process during a specified time interval.</p> <p>If the value of the parameter "seconds" (1-3600) is not given, default interval is taken as 1 second.</p> <p>Tag and subtag string can have only one word.</p> <p>The 'no' command removes the specified rate limiting configuration.</p>
<pre>logging rate-limit no unique</pre>	<p>This command restricts the number of messages in a given interval to that specified in the rate-limiting command and prevents logging of unique messages.</p> <p>By default, rate limiting does not prevent unique messages from being logged. If the number of messages does not exceed the number specified in the rate limiting command, the unique messages will continue to be logged.</p> <p>No preference is given to unique messages with this command.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note: Using this command may lead to the loss of certain high priority messages. It is recommended that the default option be retained.</p> </div> <p>The 'logging rate-limit unique' command restores the default setting and enables logging of unique messages.</p>
<pre>logging rate-limit unique</pre>	<p>This command restores the default setting and enables logging of unique messages.</p>

In case of conflict, wherein a message has more than one rate-limiting configuration applicable to it, say for example, for its tag and its subtag, the following order of preference is followed:

- subtag
- tag
- priority

This is implemented to provide better control and is in the reverse order of the frequency of occurrence.

EXAMPLE 1

```
2005 Nov 16 20:46:14: %snort-5-LOG: [1:499:4] ICMP Large ICMP
Packet
```

In the above message the tag is snort, priority is 5 and subtag is LOG.

To limit the number of messages coming from snort, to say, 5 in 2 seconds execute the following command:

```
ALU(config)# logging rate-limit 5 2 tag snort
```

```
2003 Dec 22 18:41:10: %CLI-6-ACL: User created Filter policy f5
```

In this message the sub-tag is ACL. To have finer control, the subtag of a particular tag can also be rate-limited.

To limit the number of messages coming from ACL's CLI plugin to 10 in a second, execute the following command:

```
ALU(config)#logging rate-limit 10 tag cli subtag acl
```

EXAMPLE 2

```
ALU(config)#logging rate-limit 50 priority 5
```

The above command limits the messages of priority 5 (notification) or lower (level 6 and 7) to 50 per second.

EXAMPLE 3

```
ALU(config)# logging rate-limit no unique
```

```
ALU(config)# logging rate-limit unique
```

SAVING LOG MESSAGES

This feature enables you to save log messages on the USB. The saved file can then be moved to another machine on the network using the copy command. This helps you to analyse logs pertaining to some attacks or protocol misbehavior at a later point in time. To save the contents of the log buffer into a file, use the commands given below. One or more of these options can be used.

Command (in SUM/CM)	Description
<code>save logging</code>	This command is used to save the information in the log buffer. By default, the information is saved in the <code>user:log/default.log</code> file.
<code>save logging filename {fpkey: user:}</code>	This command is used to save the log messages using the file name provided, in the front panel USB, or the user area as given by the user.
<code>save logging priority <0-7></code>	This command is used to save the log messages of the specified priority and higher.
<code>save logging string <string-value></code>	This command is used to save all the messages which holds the value of the specified string.
<code>save logging tag <tag-name></code>	Saves all the messages that come from a particular process specified by the tag.

EXAMPLE

```
ALU# save logging
```

```
ALU# save logging filename user:logs
```

This saves the log messages to a file named logs in the user area.

```
ALU# save logging priority 5
```

This saves all log messages of priority warning(= 4) and higher. i.e. all messages from (0 -4) priorities are stored.

By default, messages up to informational level(= 6) are stored.

```
ALU# save logging priority 5 exact
```

This saves log messages with priority equal to 5.

```
ALU# save logging string time
```

This saves log messages with string time. This is case sensitive.

```
ALU# save logging tag cli
```

This saves log messages originating from CLI.

VIEWING TECH SUPPORT

When a problem or a bug is encountered in the system, you can send the output of the following command to Alcatel-Lucent's tech-support department. This provides enough information to the technical-support department to locate and debug the error.

Command (in SUM/CM)	Description
<code>show tech-support</code>	This command displays details of all the modules running in the system.

EXAMPLE

The **'show tech-support'** command collectively shows the output of these commands:

```
show version
show clock
dir user:cores
show chassis
show running-config
show controller
show interfaces
show vlan Brief
show access-lists
show ip protocols
show ip route
show netio
show arp
show arp traffic
show mac-address-table
show subsystem
show logging priority 7
```

This command shows information about all the slots too. Since the output of all these commands would be very long, the complete output is not included here.



Note: You can also save the tech-support logs to the user area or fpkey using the command `"{show tech-support | tee [fpkey:]<filename>}"`.

THE FILE SYSTEM

There are various commands to manipulate the file system directly. Use the below given commands to find where a particular file is located in the system to list files, to create or remove directories.

Command (in SUM)	Description
<code>dir {fpkey: licenses user: }</code>	This command displays all the directories and files configured in fpkey or user location. The licenses keyword lists all the installed licenses. If none of the options are given, "user:" is taken by default.

The following commands are used to make and remove directories:

Command (in SUM)	Description
<code>mkdir {fpkey: user: }</code>	This command is used to create a new directory, inside the user area or fpkey.
<code>rmdir {fpkey: user: }</code>	This command is used to remove the specified directory, from the user area or fpkey.

EXAMPLE 1

```
ALU(config)# dir
Permission      Size Date modified      Name
-----
drwx            3072 Sep 15 06:25      cores
drwx           12288 Jun 26 06:00      lost+found
-rw-           30734 Sep 13 06:46      n
-rw-           30664 Sep 13 06:45      test
```

This command displays the contents of the 'cores' directory in the user area.

```
ndm-70(config)# dir user:cores
Permission      Size Date modified      Name
-----
-rw-           147456 Sep  5 08:31      core.1329.3.clim-sh.1157445064.24
-rw-           147456 Sep  5 13:20      core.1355.3.clim-sh.1157462445.24
-rw-           147456 Aug  3 12:11      core.1363.3.clim-sh.1154607060.24
```

EXAMPLE 2

```
ALU(config) # mkdir fpkey:
Directory []? ALUtest
```

```
ALU(config) # mkdir user:
Directory []? ALUtest
```

COPYING FILES

To copy files between different locations, use the copy command. The source can be memory, or an external location via one of the supported protocols.

Command (in SUM)	Description
copy <from-location> <to-location>	This command is used to copy files between the two locations.

EXAMPLE

```
ALU# copy tftp://10.91.0.35/my-config/config running-config
```

The **'copy'** command can also be used in an interactive mode as shown below. If the remote file details are not given, the command prompts for the same.

```
ALU(config)# copy ftp: user:
Address name of remote host []? 10.91.2.87
Remote Port [ Enter for default ] :
Source Path/File []? /tmp/test_file
Username [anonymous]? admin
Password []?
Local filename []? test_file
URL specification sanity OK, proceeding with copy (please wait)
Copy successful
```

DELETING FILES

This feature enables you to delete files using the **delete** command.

Command (in SUM)	Description
delete all { fpkey: user: }	This command is used to delete all the files in fpkey or user directory.
delete fpkey: <filename>	This command is used to delete a file in fpkey.
delete user: <filename>	This command is used to delete a file in the user area.
delete config-file <filename>	This command is used to delete a config file.



Note: Enter the file name after **fpkey:** and **user:** keyword without any space.

EXAMPLE

The following command deletes all the data in fpkey:

```
ALU(config)# delete all fpkey:
```

The following command deletes a file in fpkey:

```
ALU(config)# delete fpkey:backup_package
```

The following command deletes a file in user:

```
ALU(config)# delete user:backup_config
```

The following command deletes a config file:

```
ALU(config)# delete config-file config1
```

CONFIGURATION FILE MANAGEMENT

The system configuration is by default stored in a text file in the config: area on the internal USB key. Optionally, another USB key can be inserted into the USB port on the system front panel. This USB key is referred to as FPkey which stands for "Front Panel Key".

Multiple configuration files can be stored. 'start-up' config is the file that is read at system boot up. The configuration file that contains the currently effective configuration (which is not necessarily the same as the startup-config) is referred to as running-config. It is stored in the internal RAM, instead of the config: area. Therefore, it is not persistent with system reloads.

Optionally, you can save the configuration file under a different file name. Once the file is saved, you can use the copy commands to export it to an external system using TFTP/FTP options.

To VIEW THE CONFIGURATION

The following are the commands used to view the configuration written to USB as well as the configuration currently running and in memory.

Command (in SUM)	Description
<code>show running-config</code>	Shows the configuration currently running on the system. The command " write terminal " can also be used to view the same output.
<code>show startup-config</code>	Shows the configuration currently stored on the permanent storage media. This configuration is read at system startup.

EXAMPLE 1

```
ALU(config)# show running-config
```

```
!Current Configuration:
!
! NVRAM config last updated at 06:25:14 GMT  Wed Nov 08 2006
from line 0
! Statlog Configuration
!
logging on
logging buffered priority 7
logging buffered size 128
logging console 3
logging system 5
logging remote 1.1.1.1 port 514 priority 7
service timestamps log
hostname ndm-70
!
snmp enable
!
! PVST Global configuration
spanning-tree
modem disable
!
! SNMP Configurations
--More--
```

EXAMPLE 2

```
ALU(config)# show startup-config

!
! NVRAM config last updated at 06:25:14 GMT  Wed Nov 08 2006
from line 0
!
! Statlog Configuration
!
logging on
logging buffered priority 7
logging buffered size 128
logging console 3
logging system 5
logging remote 1.1.1.1  port 514  priority 7
service timestamps log
hostname ndm-70
! PVST Global configuration
  spanning-tree
!
snmp enable
!
modem disable
!
! SNMP Configurations
!
--More--
```


To SAVE THE CONFIGURATION

To save the running configuration to the start-up configuration, use the following commands. Both commands are identical in functionality.

Command (in SUM)	Description
save running-config	This command saves the running configuration to the start-up configuration. The command " write memory " can also be used to save the running configuration to the start-up configuration.

EXAMPLE

```
ALU# save running-config
Saving to startup-config ...
```

```
ALU# write memory
Saving to startup-config ...
```

To SAVE THE CONFIGURATION UNDER A DIFFERENT FILE NAME

To save the running configuration under a different file name use the following command:

Command (in SUM)	Description
save running-config <file-name>	This command saves the running configuration under the specified file name in the config directory.

EXAMPLE

```
ALU# save running-config my-config
Saving to my-config ...
```

To LIST THE CONFIGURATION FILES

To list the available configuration files, use the **list config-files** command.

Command (in SUM)	Description
list config-files	This command is used to list all the available configuration files in the config directory.

EXAMPLE

```
ALU# list config-files
```

```

Permission      Size Date modified      Name
-----
-rw-            10464 Dec 26 15:25      my-config
-rw-            10461 Dec 25 08:13      startup-config
```

To VIEW THE CONTENTS OF THE CONFIGURATION FILE

To view the contents of the available configuration files, use the **show config-file** command.

Command (in SUM)	Description
show config-file [<i><file-name></i>]	This command is used to show the contents of the specified configuration file.

EXAMPLE

```
ALU# show config-file my-config
```

```

!
! NVRAM config last updated at 08:13:52 GMT  Sun Dec 25 2005
by ALU
!
! Statlog Configuration
!
logging on
logging buffered priority 7
logging buffered size 10000
no logging console
logging system 4
logging remote 10.91.0.94  port 514  priority 7
logging remote 10.91.0.173  port 514  priority 7
service timestamps log
hostname SG8-BLR
modem enable
!
http enable
https enable
ssh enable
```

```
snmp enable
telnet enable
!
!
! Chassis manager configuration
!
!
! SNMP Configurations
!
snmp agent version v2c
snmp trap enable
snmp system contact sysadminblr@ALU.com
snmp system location Bangalore
snmp agent rocommunity public
!
8ec760e45da5b29afb19ed8d68a3eb5e
!
aaa services
aaa authentication login default local
enable secret 5 b96bea0fa10dc5b85cd6b6078f16a356
!
username ALU password 5 b96bea0fa10dc5b85cd6b6078f16a356
!
ip domain-list alu.com
ip domain-name .
ip name-server 10.91.0.249
!
interface loopback1
 ip address 203.124.211.225/27
 no shutdown
 top
!
interface GigabitEthernet7/0
 description GigabitEthernet 7/0
 ip address 59.144.47.105/24
 no shutdown
 top
!
!
!QoS Configuration
!
class-map high-priority-map match-any
1 match any high-priority-traffic
class-map gre-map match-any
1 match any shape-gre
class-map exclude-police-map match-any
1 match any exclude-police
class-map tunnel-class match-any
1 match any qos-tunnel
!
policy-map traffic-out-policy
 class class-default
   shape committed-rate 512000 committed-burst 96000
 class high-priority-map
```

```
    priority
  class gre-map
    shape committed-rate 350000 committed-burst 50000
  class tunnel-class
policy-map traffic-in-policy
  class class-default
    police committed-rate 750000 commit-action transmit
    committed-burst 144000 exceed-action drop
  class exclude-police-map
interface GigabitEthernet7/1
  service-policy out traffic-out-policy
  service-policy in traffic-in-policy
!
!
line vty 4
  transport input none
!
line con 0
  no exec-timeout
!
!
!
!
!
!
firewall
  session
    default timeout tcp 7200
```

To COPY THE CONFIGURATION

To copy the configuration from one filename to another or between location, use the copy command. The source can be memory, or an external location via one of the supported protocols.

Command (in SUM)	Description
<code>copy <from-location> <to-location></code>	This command is used to copy the configuration or the files between two locations.

EXAMPLE

The following command copies the running configuration to the config: area and renames it as startup-config.

```
ALU# copy running-config startup-config
```

The following command is used to copy the config file to the user area, ftp, or ftp server:

```
ALU(config)# copy running-config tftp:
Address name of remote host [10.91.2.87]?
Remote Port [ Enter for default ] :
Destination Path/File [running-config]?
URL specification sanity OK, proceeding with copy (please wait)
Copy successful
```

To LOAD A CONFIGURATION FILE

Command (in SUM)	Description
<code>load config-file <file-name></code>	<p>This command is used to load a configuration file to the running configuration. This effectively leads to the execution of all the commands in the given file.</p> <p>This file should be present in the config directory. (Use the copy commands to copy the file to the config directory).</p>

EXAMPLE

```
ALU# load config-file config1
Loading config1 to running-config...
/----- Percent Complete -----
|*****
```

To DELETE THE CONFIGURATION FILE

To delete the available configuration files, use the following command:

Command (in SUM)	Description
<code>delete config-file <file-name></code>	This command is used to delete the configuration file from the config directory.
<code>write erase</code>	This command is used to delete the startup-config permanently. The command " erase startup-config " can also be used to delete the startup-config permanently.

EXAMPLE

```
ALU# delete config-file my-config
```

```
ALU(config)# write erase
```

```
Are you sure you want to erase startup-config file yes/no
```

```
[yes]:yes
```

```
[OK] startup-config file erased.
```

SOFTWARE PACKAGE MANAGEMENT

The OA-700 is a modular system. From the hardware side, this means that different physical parts of the system can be removed, inserted, and upgraded independent of each other. From the software side, it means that software modules can be upgraded individually.

Most of the applications running on the system can be upgraded independent of each other and without system downtime. The exception is the base Linux operating system and the most basic building blocks in the system which sometimes require a reload of the specific card or the whole system for a software upgrade to take effect.

Before upgrading a software module, check the current versions of the modules, read the release notes to make sure you are aware of any potential conflicts between different module versions.

PACKAGE TYPES

Packages are the vehicles for software delivery on the OA-700. There are three kinds of packages:

1. LoL-<version>.npm

This is the collection of files that installs the operating system components. It contains the flash image for SC (Switch Card), Services Engine (SE) and other line cards.

2. ALU-apps.<version>.npm

This is the collection of application modules and is a complete software release of all features.

3. ALU-part.<version>.npm

This is one application module by itself.

TO INSTALL A PACKAGE ON THE SYSTEM

Command (in SUM/CM)	Description
<code>package install</code> { <code>fpkey:</code> <code>ftp:</code> <code>http:</code> <code>https:</code> <code>tftp:</code> <code>user:</code> }	Installs a release or a component package from the given location. The package file can be obtained from user area or <code>fpkey:</code> or it can be obtained from a remote site using FTP, TFTP, HTTP, or HTTPS.
<code>package install flash</code> { <code>fpkey:</code> <code>ftp:</code> <code>http:</code> <code>https:</code> <code>tftp:</code> <code>user:</code> }	Installs a flash image on all the cards. The package file can be obtained from user area or it can be obtained from a remote site using FTP, TFTP, HTTP, or HTTPS.



Note: If the package is installed from a remote location, it is temporarily downloaded into the user area, and deleted after the installation. So care must be taken to have enough space for the package before proceeding with the installation.

EXAMPLE

The following command installs a package after downloading it from remote site using ftp:

```

ALU(config)# package install ftp:
Remote Host : 10.91.0.87
Remote Port [ Enter for default ] :
Path/Filename : /packages/alu-apps.2.1.22.1.npm
Username [Enter for none] : user1
Password :
Downloading remote file. This could take a while...
Verifying package... NPM v1.0 format
OK.

Checking the package type ... Release: 2.1.22.1

Are you sure you want to install alu-apps.2.1.22.1.npm? (y/[n])
: y

Installing new release alu-apps.2.1.22.1.npm...OK.
Complete.
Deleting temporary file...OK.

Do you want to set-default immediately?
  Yes: Chassis will be rebooted automatically
  No : Manually run set-default at a later time
Proceed? (y/[n]) : y

Do you want to save config before proceeding ([y]/n) : y
Building configuration...
[OK]
Setting Default image to 2.1.22.1...

```


To TAKE A BACKUP OF THE PACKAGE

Command (in SUM/CM)	Description
<code>package backup</code> { <code>fpkey:</code> <code>ftp:</code> <code>tftp:</code> <code>user:</code> }	Backs up the default package at a given destination. The backup file can be stored in user area or <code>fpkey</code> . It can also be sent to a remote location using <code>ftp</code> or <code>tftp</code> .

EXAMPLE

The default package can be backed-up locally in `user:` or `fpkey:` or in a remote location using `ftp` or `tftp`.

```
ALU(config)# package backup ftp:
```

```
Remote Host : 10.91.2.87
Remote Port [ Enter for default ] :
Path : backup-apps.2.2.25.1.npm
Username [Enter for none] : vinaykumar
Password :
```

```
Backing up Applications package... Creating...
Uploading file. This could take a while...Completed.
```

To REMOVE A PACKAGE

Command (in SUM/CM)	Description
<code>package remove <package-name></code>	Removes the specified package. However, the default package cannot be removed.

EXAMPLE

To remove 2.2.25 package:

```
ALU(config)# package remove 2.2.25
```

```
Remove package 2.2.25? (y/[n]) : y
```

```
Uninstalling application package 2.2.25...OK.
```

PACKAGE SET-DEFAULT

Command (in SUM/CM)	Description
package set-default <package-name>	If the specified package is not the default package, it is set as default. The system can have multiple application packages (like 2.1.7.1, 2.1.8.1). The package being set as default should exist in the system.

EXAMPLE

To set the package 2.1.23.1 as default:

```
ALU# package set-default 2.1.23.1
```

```
Do you want to set-default immediately?
```

```
Yes: Chassis will be rebooted automatically
```

```
No : Manually run set-default at a later time
```

```
Proceed? (y/[n]) : y
```

```
Do you want to save config before proceeding ([y]/n) : y
```

```
Building configuration...
```

```
[OK]
```

```
Setting Default image to 2.1.23.1...
```

TO VIEW DETAILS OF THE PACKAGE

This command shows the version of the various software modules/components installed in the system. This shows a list of available application package images.

Command (in SUM/CM)	Description
show packages [detail <package-name>]	Shows the various packages currently installed. If the keyword ' detail ' and a package name are specified, then all the components present in that package are listed. If a package name is not specified when ' detail ' keyword is used, then the components of the default package are listed.
show version	This command displays the version information of the running package and flash image.

EXAMPLE 1

To view the package details currently installed:

ALU# show packages

```

Default  Name          Size (KB) Build Date
*        2.1.22.1    24093     Fri Jan  6 05:27:14 IST 2006

```

ALU# show packages detail 2.1.22.1

Current components:

Version	Name	Description
2.1.22.1	BGP	BGP Routing Module
2.1.22.1	DHCP-relay	DHCP Relay service
2.1.22.1	Ethernet	SE GigE / L2-GE software
2.1.22.1	GRE	GRE Encapsulation and tunneling
2.1.22.1	HTTP	HTTP server
2.1.22.1	IDS	Intrusion Detection/Prevention System
2.1.22.1	IPSec	IPSec VPN service
2.1.22.1	Infrastructure	Infrastructure components of the system
2.1.22.1	Management-OOB	Out-Of-Band Management
2.1.22.1	Management-Tools	Internal support tools
2.1.22.1	ALU-X	ModuLive Operating system
2.1.22.1	Networking-base	Networking infrastructure
2.1.22.1	OSPF	OSPF Protocol
2.1.22.1	QoS	Quality of Service
2.1.22.1	RIP	Routing Information Protocol
2.1.22.1	Routing-base	Routing Infrastructure
2.1.22.1	SNMP	SNMP-v2 support
2.1.22.1	SSH	Secure Shell Access
2.1.22.1	Security	Network Security Services
2.1.22.1	Serial	Frame-Relay, HDLC, T1E1, Serial
2.1.22.1	VRRP	Virtual Router Redundancy Protocol

21 Components Listed

EXAMPLE 2

ALU# show version

```

Alcatel-Lucent Software, Version 2.1.15
Copyright (c) 2003-2005 by Alcatel-Lucent
Built on Mon Apr 17 11:50:34 IST 2006

```

Flash version - 2.1.5

RELOADING THE SYSTEM

The **reload** command can be used to reload the system. Reload is immediate and once issued cannot be revoked. Hence, confirmation is required before the command is actually accepted. Reload has the same effect as power cycling the chassis.

System reboot is enabled by two methods. The soft reboot and the hard reboot. The hard reboot refers to system power-off. The soft reboot is enabled by using the command reload.

A message can be given with the reload command. This message will be sent to all VTYS (Virtual Tele Type) to warn users who are logged in and the message will also be written to the system log.

The following actions are needed to be taken before reloading:

1. The **reload** command requires confirmation before reloading. The default answer for the confirmation is 'N' so the user is obligated to type in a 'Y' (not case sensitive).
2. You will be asked if you want to record the current configuration information before reloading. If the information is not recorded, any changes made since the system was last started will be lost.
3. Another action is to record the current system time in the RTC. This is done in the presumption that the system time is coordinated with an external source and is therefore more accurate than the RTC. If the system time is being coordinated from the RTC, then this action is essentially a no-op.

The reload command is implemented by powering down all the slots first (see ["Managing Individual Slots"](#) section), and then restarting the switch card(s).

Command (in SUM)	Description
reload [<i>line</i>]	To reload the system, also referred to as a soft reboot.

EXAMPLE

```
ALU# reload "where's slot 7"
Do you really want to reboot the Chassis (y/[n])?y
Do you want to save config before rebooting (y/[n])n
ALU#
The system is going down NOW !!
Sending SIGTERM to all processes.
Terminated
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
Restarting system.
```

MANAGING INDIVIDUAL SLOTS

The power command allows the privileged user to control the power of slots 0-7 on the OA-780 and slots 0-1 on the OA-740. Powering down an occupied slot is almost equivalent to physically removing the card from the chassis.

Individual cards within the chassis may be managed separately by controlling their power. This may happen internally if a card is malfunctioning or has exceeded permissible environmental limits. A card may also be powered down manually using the CLI.

A slot may be powered down using the CLI power command, or it may have been powered down by some other means, such as a sensor reading that exceeds the defined range of operation. Once a slot is powered down, some form of intervention is required to power it back. The power command can be used to power it back. Alternatively, the card can be physically removed from the slot for a few seconds, then re-inserted, or the entire chassis can be power cycled.

There are **four** forms of manual intervention:

1. Physically power cycle the entire chassis.
2. Reload the entire chassis.
3. Remove the card from its slot for 10 seconds or more and re-insert it, or
4. Use the CLI to power up the slot.

Command (in SUM)	Description
<code>power slot <slot-number> {up down}</code>	This command powers down a slot or attempts to power it up again if the slot has already been powered down. This command controls the power of slot 0-7 on the OA-780 and slot 0-2 on the OA-740.

EXAMPLE

```
ALU# power slot 1 down
```

```
ALU# power slot 1 up
```

SYSTEM MONITORING AND TROUBLESHOOTING

ENVIRONMENTAL INFORMATION

The **show environment** command displays the latest known sensor readings from the occupied slots that contain line cards or switch cards. The standard readings are the temperature from the card and voltage readings taken at various places on the card. The sensor readings are monitored to ensure that they are within the defined ranges and if not, the card may be powered down.

The command can show individual card readings, or display the readings for all occupied slots. For each slot displayed, the report includes the slot number and card type, last time the card's sensors were reported, and the values of the temperature and various reference voltages on that card.

The sensor readings are monitored to ensure that they are within safe operating ranges, and if not, the card may be powered down (see section "[Managing Individual Slots](#)"). Any deviation will be noted in the log.

Command (in SUM)	Description
show environment [slot <0-7> <24-25>]	This command shows the environmental state of the various parts and modules in the system.

EXAMPLE

```
ALU> show environment
```

```
Chassis environment readings
  Report generated at Thu Apr  5 11:54:23 2007
  Chassis temperature: 36C
L2 - 8-port copper GigE
  Slot number 0
  Liveness failures will report once
  PCI configuration status: Ready
  Reported at Thu Apr  5 11:54:20 2007 (4 seconds ago)
  Temperature reading:  29.000C
  Voltage reading:    5.01V(0%)   1.25V(-3%)   2.48V(0%)
E1 - Four port E1
  Slot number 1
  Liveness failures will report once
  PCI configuration status: Ready
  Reported at Thu Apr  5 11:54:21 2007 (3 seconds ago)
  Temperature reading:  34.500C
  Voltage reading:    5.06V(1%)   1.27V(-1%)   2.46V(-1%)
SE - Service engine
  Slot number 7
  Liveness failures will report once
  PCI configuration status: Ready
  Reported at Thu Apr  5 11:54:21 2007 (3 seconds ago)
```

```
Temperature reading: 30C (card)/44C (svc-eng)
SC - Switch card
Slot number 24
Liveness failures will report once
PCI configuration status: Ready
Reported at Thu Apr 5 11:54:19 2007 (5 seconds ago)
Temperature reading: 30.000C
Voltage reading: 11.68V(-2%) 3.21V(-2%) 1.28V(0%)
2.50V(0%)
```

ALU> show environment slot 7

```
Chassis environment readings
Report generated at Thu Apr 5 11:54:23 2007
Chassis temperature: 36C
SE - Service engine
Slot number 7
Liveness failures will report once
PCI configuration status: Ready
Reported at Thu Apr 5 11:54:21 2007 (3 seconds ago)
Temperature reading: 30C (card)/44C (svc-eng)
```

Acceptable voltage range is +/- 6%. Acceptable temperatures vary depending on the card type, but generally range from 0 - 60⁰C. Warnings will be logged and the fan speed adjusted if any of the cards show a temperature greater than 50⁰C.

The Service Engine (part number 902601-90) has two temperature readings. Only the first one is monitored.

SYSTEM HARDWARE INFORMATION

The **show chassis** command provides a physical inventory of the chassis' components, including parts that are in meta-slots (i.e., not line cards). Generally, it depicts the static information about the hardware configuration. The command can be used for a specific slot or to view information for the entire chassis.

The command reports on the pluggable as well as non-pluggable (front panel) components of the system. These reports are available in common format. This command is available at all configuration modes.

Command (in SUM)	Description
show chassis [slot <0-31>]	This command provides a physical inventory of the chassis components for a specific slot or for the entire system. It does not indicate the liveness of the elements listed.

EXAMPLE

The first example is a typical card report. In this case, the switch card is in slot 24.

```
ALU> show chassis slot 24
```

```
Physical inventory at Thu Apr  5 11:54:17 2007
SC - Switch card (active)
  Slot number: 24
  Part number: 902613-90
  Manufacturer: ALU
  Description: Switch card
  Serial number: DD0536054350
  Version: 00
  Revision: 54
  Deviation: aaaa
  LoL firmware version: 2.2.56
  Loader version: 2.29
  ALU-OS version: 2.2.52
```

The following example shows a full chassis inventory:

```
ALU> show chassis
```

```
Physical inventory at Tue Oct 30 06:33:47 2007
System started approximately Tue Oct 30 06:30:26 2007
Uptime is 0 days 0 hours 4 minutes 20 seconds
L2 - 8-port copper GigE (active)
  Slot number: 0
  Part number: 902603-90
  Manufacturer: ALU
  Description: 8-port copper GigE
```

Alcatel-Lucent


```
Serial number: DD0512560340
Version: 00
Revision: 01
Deviation: 0000
Loader version: 2.27
ALU-OS version: 2.2.52
MDC
Serial number: WL0534000127
Deviation: 0001
Revision: A1
Version: 01
SE - Service engine (active)
Slot number: 3
Part number: 902601-90
Manufacturer: ALU
Description: Service engine
Serial number: DD0538002048
Version: 01
Revision: 04
Deviation: 0001
CPU Version: 1 (Low Power Opteron)
Opteron CPU Version: 1
Opteron CPU Frequency: 2193 MHz
Loader version: 2.30
ALU-OS version: 2.2.64
MDC
Serial number: WL0529000008
Deviation: 0002
Revision: 05
Version: 01
PB - Power tray (passive)
Slot number: 22
Part number: 902612-90
Manufacturer: ALU
Description: Power tray
Serial number: DD0536004050
Version: 00
Revision: 01
Deviation: 0000
SC - Switch card (active)
Slot number: 24
Part number: 902613-90
Manufacturer: ALU
Description: Switch card
Serial number: DD0536054350
Version: 00
Revision: 54
Deviation: aaaa
LoL firmware version: 2.2.56
Loader version: 2.29
ALU-OS version: 2.2.52
FP - Fan tray (passive)
Slot number: 26
Part number: 902614-90
```

```

Manufacturer: ALU
Description: Fan tray
Serial number: DD0545027001
Version: 00
Revision: 01
Deviation: 0000
BP - ALU OA780 chassis (passive)
Slot number: 29
Part number: 902611-90
Manufacturer: ALU
Description: ALU OA780 chassis
Serial number: DD0546005005
Version: 00
Revision: 01
Deviation: 0000
Base MAC: 00:11:8b:00:72:00

```

SYSTEM STATUS

Command (in SUM)	Description
<code>show system-status</code>	This command displays the status of the different cards in the system.

EXAMPLE

```
ALU(config)# show system-status
```

Slot	Description	Status
-	Switch card	Card Ready
3	Service engine	Card Ready

To VIEW THE CURRENT STATE OF LEDs

Command (in UM)	Description
<code>show led</code>	This command displays the current state of the LEDs on the front panel and the switch card(s).

EXAMPLE

```
ALU> show led
Name           State
----          -
Primary SC     green
Standby SC     vacant

Front          panel
-----
Active         green
Modem          off
Console        green
Usb            off
```

To View PROCESS INFORMATION

This command displays all the processes currently running in the system, such as SSH, RIP, BGP, Statlog, etc.

Command (in SUM)	Description
<code>show processes</code>	Displays the CPU information.

EXAMPLE

```
ALU(config)# show processes
```

```

PID  Uid      VmSize  Stat Command
  1  root          520  S   init
  2  root          SW   [keventd]
  3  root          SWN  [ksoftirqd_CPU0]
  4  root          SW   [kswapd]
  5  root          SW   [bdflush]
  6  root          SW   [kupdated]
  7  root          SW   [khubd]
 54  root          500  S   /usr/sbin/ialu /etc/ialu.conf
296  root          496  S   /bin/ash /bin/tm-sh
297  root          496  S   /bin/sh /etc/monitor
319  root         1548  S   tm -i vnet0 pm -A
322  root          380  S   cat /dev/ss_mem
323  root         2076  S   pm -A
330  root         2308  S   vrrp
331  root         1384  S   udp-agent
332  root         1520  S   statsagent
333  root         2368  S   statlogd -c
334  root         2388  S   ribmgr ribmgr initial
335  root         2544  S   srm srm initial
337  root         2308  S   aclmgr aclmgr initial
338  root         2268  S   rip rip initial
339  root         2164  S   pvstd
340  root         1884  S   pluto --nofork --nat_traversal
341  root         6336  S   ospfd ospfd initial
343  root         2268  S   mcribmgr mcribmgr initial
344  root         2096  S   ipcd ipcd initial
345  root         1972  S   ike_wr
346  root         1432  S   gre
347  root         1940  S   ea
348  root         2204  S   dnsproxy initial
349  root         2156  S   dhcprelay initial
350  root         3416  S   controld
351  root        34308  S   switchd 11
352  root         2328  S   bgp bgp initial
354  root          532  S   /bin/sh /alu/usr/sbin/core_mover.sh
607  root        46028  S   snort-alu -i eth0 -c /alu/etc/snort/
      snort.conf
7145 root          340  S   sleep 30
7146 root          672  S   rshd
7147 root          464  S   sh -c ps aux
7148 root          628  R   ps aux

```

MEMORY INFORMATION

This command displays all the necessary information related to the system memory, such as the Memory usage, memory free space, memory buffers configured, shared memory space, etc.

Command (in SUM)	Description
<code>show memory</code>	Displays the memory information.

EXAMPLE

```
ALU(config)# show memory
```

```

          total:   used:   free:  shared:  buffers:  cached:
Mem:  380014592 180305920 199708672      0   176128 43839488
Swap:         0         0         0
MemTotal:         371108 kB
MemFree:          195028 kB
MemShared:         0 kB
Buffers:           172 kB
Cached:           42812 kB
SwapCached:        0 kB
Active:           13964 kB
Inactive:        136824 kB
HighTotal:         0 kB
HighFree:          0 kB
LowTotal:         371108 kB
LowFree:          195028 kB
SwapTotal:         0 kB
SwapFree:          0 kB

```



Note: In addition to the total memory displayed, 128 MB is reserved for data buffers. This is not displayed in the total system memory.

SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

The following section gives an insight of the SNMP used in the **OA-700**. Refer to the following sections to know more about configuring and setting up the SNMP module.

- [“SNMP Basics”](#)
- [“SNMP Agent and Manager”](#)
- [“SNMP Version”](#)
- [“SNMP MIB CLI”](#)
- [“SNMP MIB GUI”](#)

SNMP BASICS

SNMP is a request-and-response protocol that is used in the transfer of network management information between two or more network entities. SNMP plays a vital role and serves as the nervous system of the entire network management system. Network management is about keeping the network up and running and monitoring, and controlling the devices in the network using conventional network technology.

Local management and remote management are the two ways of managing a device connected to a network. Local management demands human intervention where the managed object is situated. This becomes cumbersome when the network devices are numerous and widespread. Managing such a system becomes tedious and quite impossible. In such a situation SNMP is used to manage the network remotely.

Using a workstation, running one or more SNMP management applications, you can monitor and manage network devices running SNMP agent. This information is used to establish the functioning of the network and also to identify the problems in the network.

Some of the advantages of using SNMP are:

- Standardized Protocol
- Universal Acceptance
- Portability
- Lightweight
- Extensibility
- Widely Deployed

SNMP AGENT AND MANAGER

The two major components of SNMP that form an integral part of its foundation are the network device, and the agent and the manager. Let us look at each of these component individually. A network device or the managed object is a part of the network that requires some form of monitoring and management.

Agent is a mediator between the manager and the device. The agent is a program that resides in the device and not a separate entity. It collects management information from the device and makes it available to the manager. The agent implements the SNMP protocol which helps in retrieving management information as defined in the MIBs (Management Information Base) supported on the device. The agent signals an event to the manager through traps.



A **Manager** is a management system, which is a separate entity that manages the devices from a remote place through agents installed on the devices. This application runs on a computer that is used to manage one or more network management systems.


Consider an organization having its branches in different geographical locations. Administration of all the computers present in different localities would be difficult. When the System Administrator's computer is installed with the manager and all other systems and devices across all the offices are installed with the agent, management becomes easier. The administrator has to just query the agent through its manager to know the functioning of a specific device. The manager will implement the network management system, implement SNMP protocol, query agents, get responses from agents, set variables in agents, and receive asynchronous events from agents.

The communication between the manager and the agent in a network happens by means of PDU (Protocol Data Units). The PDUs allow the manager to interact with the agent in the device. The extent of management possibly depends on the data available to the manager from the agent which in turn depends on the support of MIBs on the agent.

PDUs are encapsulated in the UDP (User Datagram Protocol) for transportation across the network. UDP is a connectionless transport protocol included in the TCP/IP suite and described in RFC.

The following commands are used to enable and configure SNMP for the system:

Command (in CM)	Description
<code>snmp {enable disable}</code>	This command is used to enable or disable the SNMP session.
<code>[no] snmp agent rocommunity <community-string></code>	<p>This command configures the SNMP agent read-only community.</p>  <p>Note: The SNMP agent can be accessed only after setting the SNMP version. Use the 'snmp agent version (v1 v2c)' command to set the version of the SNMP agent.</p>
<code>[no] snmp agent rwcommunity <community-string></code>	<p>This command configures the SNMP agent read-write community.</p>  <p>Note: SNMP agent can be accessed only after setting SNMP version. Use 'snmp agent version (v1 v2c)' command to set the version of the SNMP agent.</p>
<code>[no] snmp system contact <contact></code>	This command configures the SNMP system contact details.
<code>[no] snmp system location <location></code>	This command configures the system's physical location information.

Command (in CM)	Description
<code>[no] snmp system name <name></code>	This command configures the SNMP system name.
<code>[no] snmp trap {enable <ip-address> {v1 v2c} <community-string> <1-65536>}</code>	<p>This command configures the trap destination where the agent will send the snmp traps.</p> <p>Use the 'enable' keyword enables the snmp traps.</p> <p> Note: Cannot add more than 3 trap receivers.</p> <p>Following message "Trap receiver entry with IP Address: 10.91.0.225, Port: 162 and Version: v1 already exists" will be displayed if the trap server being added is already present at the registry.</p>

EXAMPLE

```

ALU(config)# snmp agent enable

ALU(config)# snmp agent rocommunity private

ALU(config)# snmp agent rwcommunity public

ALU(config)# snmp system contact support@alcatel-lucent.com

ALU(config)# snmp system location blr

ALU(config)# snmp system name ALU1

ALU(config)# snmp trap 10.91.0.224 v1 trapcommunity 162

```

SNMP VERSION

The different versions of SNMP are SNMPv1, SNMPv2c and SNMPv3.

- **SNMPv1** is the first version of the protocol, which is defined in RFC 1157.
- **SNMPv2c** is the revised protocol, which includes enhancements of SNMPv1 in the areas of data type efficiency and performance, confirmation of event notification, error handling, set operation, transport independence, and MIB structure elements. But SNMPv2c uses the existing SNMPv1 administration structure. It is defined in several RFCs, such as RFC 1902 to 1907.
- **SNMPv3** defines the secure version of the SNMP. It also facilitates remote configuration of the SNMP entities and is defined in RFC 2576, RFC 3410-3415.

SNMPv1 and SNMPv2c are supported.



Note: SNMPv3 is not supported in the **OA-700**.

The below command sets the SNMP version for the agent.

Command (in CM)	Description
<code>snmp agent version {v1 v2c}</code>	Set the snmp version.

EXAMPLE

```
ALU(config)# snmp agent version v2c
```

SNMP SHOW COMMANDS

To VIEW SNMP DETAILS

Command (in CM)	Description
<code>show snmp details</code>	This command is used to view the SNMP configuration details.

EXAMPLE

```
ALU(config)# show snmp details
```

```
SNMP status   : Enabled
SNMP version  : [Not configured]
Traps         : [Not configured]

System information
-----
System Contact   : test
System Location  : [Not configured]

Community-Access  Community-String
-----
read-only         t1
read-write        [Not configured]

Trap-Host      Trap-Port  Version  Trap-Community
-----
10.91.0.224    8001      v1       trapcomm
10.91.0.225    162       v2c      notifcomm
```

To VIEW SNMP STATISTICS

Command (in CM)	Description
<code>show snmp stats</code>	This command displays the SNMP statistics.

EXAMPLE

```
ALU(config)# show snmp stats
```

```
11 SNMP packets input
0 Bad SNMP version errors
6 Unknown community names
0 Bad community uses
0 Encoding errors
0 Silent drops
0 Proxy drops
```

SNMP MIB CLI

The SNMP MIB objects can be queried and set according to the access defined for each MIB object in the concerned RFC. We shall go through some of the commands from the CLI to query the agent for various objects and also to set several objects based on their access. In the following examples, the SNMP version considered for this device is **v2c** and read-write community string is **public**.



Note: SNMP manager commands listed in the examples below are provided by Net-SNMP toolkit and are installed as a part of standard Linux installation. For more information on each of the commands, please refer to the main page of the respective command.

GET

The `snmpget` command can be used to retrieve the value of a MIB object.

```
snmpget -v {1/2c} -c <community-string> <agent ip-address>  
<MIB object>
```

GETNEXT

The `snmpgetnext` command can be used to retrieve the value of the next available MIB object in the lexicographically ordered tree.

```
snmpgetnext -v {1/2c} -c <community-string> <agent ip-  
address> <MIB object>
```

SET

The `snmpset` command can be issued to set the value of a MIB object.

```
snmpset -v {1/2c} -c <community-string> <agent ip-address>  
<MIB object>
```

The following commands can be used to fetch all the MIB objects supported at the agent.

```
snmpwalk -v {1/2c} -c <community-string> <agent ip-address>
```

```
snmpbulkwalk -v 2c -c <community-string> <agent ip-address>
```

SNMP MIB GUI

The SNMP MIB objects can be queried and set according to the access defined for each MIB object in the concerned MIB through MIB browser. Use any MIB browser to perform SNMP operations on the agent running on the device.



Note: Ensure that the version and community string settings of the MIB browser is compatible with the agent, before performing any operation from the MIB browser.

CHAPTER 4 VIRTUAL ROUTER REDUNDANCY PROTOCOL

This chapter provides an overview of the Virtual Router Redundancy Protocol configuration on the OA-700. VRRP can be configured on multi-access interfaces like Ethernet. VRRP is supported on GigabitEthernet (GigE) interface on the OA-700.

The **“VRRP Overview”** section serves as an additional information on VRRP. You can skip this section and move directly to the configuration **“VRRP Configuration”** section.

CHAPTER ORGANIZATION

- **“VRRP Overview”**
- **“VRRP Configuration”**
- **“VRRP Interface Tracking”**
- **“VRRP Configuration Scenario using OA-700”**

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
VRRP	Virtual Router Redundancy Protocol

VRRP OVERVIEW

VRRP eliminates the single point of failure inherent in the static default routed environment. VRRP supplies a method of providing nonstop path redundancy and gateway redundancy for an enterprise network by sharing protocol and Media Access Control (MAC) addresses between redundant gateways. The protocol consists of a virtual MAC address and a protocol address that are shared between two or more gateway routers.

VRRP specifies an election protocol that dynamically assigns responsibility of a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with the virtual router is called the Master. The Master router provides default gateway functionality for hosts on the LAN. As the default gateway, the master router forwards the packets received from the hosts on the LAN or forwards packets received for the hosts on the LAN. The election process provides forwarding responsibility to another VRRP router dynamically, if the Master becomes unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

During the startup, or through the use of the priority and preempt commands, one of the routers is chosen to be the Active router (Master) and the second router is designated as the standby (backup router). If the backup router fails to receive the hello packet of the Master router, either the local LAN segment is unstable or the Master router has had a failure. In either case the backup router assumes control of the virtual MAC and the protocol addresses.

VRRP is intended for use with IPv4 routers only. VRRP packets are sent encapsulated in IP packets. They are sent to the IPv4 multicast address assigned to VRRP.

VRRP FUNCTIONALITY

VRRP enables a group of routers to form a single virtual router to provide redundancy. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers is also known as a VRRP group.

VRRP INTERFACE TRACKING

The VRRP Interface Tracking feature extends the capabilities of the VRRP to allow tracking of specific interfaces within the router that can alter the priority of a router.

RFC

3768

VRRP CONFIGURATION

Refer the following sections to configure VRRP on your OA-700:

- [“VRRP Configuration Steps”](#)
- [“VRRP CLI Commands”](#)

VRRP CONFIGURATION STEPS

The following are the steps to be followed when configuring VRRP:

Step 1: Enter into Configuration Mode.

```
ALU# configure terminal
ALU(config)#
```

Step 2: VRRP is configured on an interface. First, configure an interface.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```



Note: The interface IP address must be configured and the operational state of the interface must be up for VRRP to operate.

Step 3: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 4: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 5: Configure VRRP on the interface and configure primary IP address for the VRRP Group. See [“To Configure VRRP Group and Primary IP Address for the Group”](#)

Step 6: Configure the **optional** parameters for the VRRP group like: Secondary IP address for the VRRP Group, Authentication, Priority, Preempt, Description, Set an Advertisement interval, Learning the advertisement interval, interface tracking. See [“Modify Global VRRP Group Parameters”](#)

Step 7: Use the **“show”** and **“debug”** commands to monitor and debug the VRRP configuration. See [“Monitor and Debug VRRP”](#)

VRRP CONFIGURATION FLOW

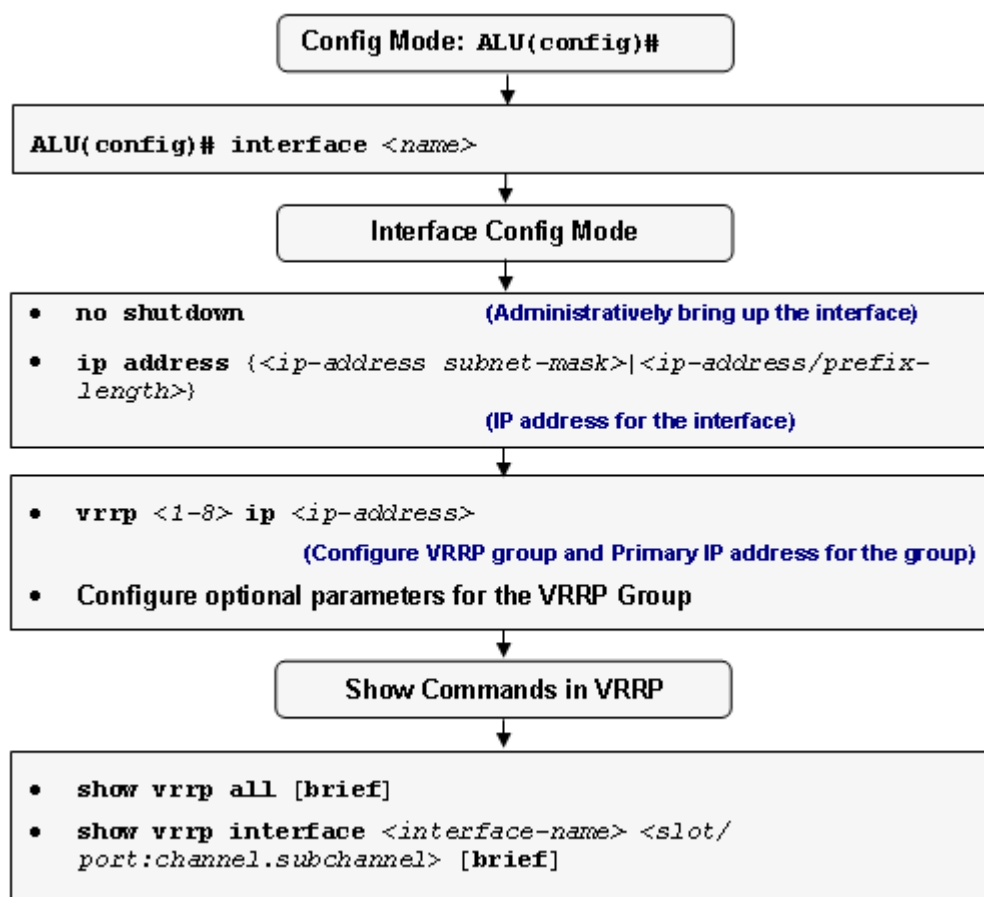


Figure 2: VRRP Configuration Flow

VRRP CLI COMMANDS

This section details the commands that are used in configuring VRRP.

TO CONFIGURE AN INTERFACE

VRRP is enabled on a per-interface basis. VRRP runs on multi-access networks like Ethernet.

Command (in CM)	Description
interface <name>	This command is used to configure an interface.

EXAMPLE

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

TO CONFIGURE VRRP GROUP AND PRIMARY IP ADDRESS FOR THE GROUP



Note: Group ID is in the range 1 - 8.

Command (in ICM)	Description
vrrp <1-8> ip <ip-address>	This command configures a VRRP group with the specified ID on the interface, and specifies a primary IP address for the VRRP group.
no vrrp <1-8> ip <ip-address>	This command removes the primary IP address for the specified VRRP group on an interface. VRRP group is disabled as a result.
no vrrp <1-8>	This command removes all configuration associated with the VRRP group on the interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)#vrrp 5 ip 10.91.0.8
ALU(config-if GigabitEthernet7/0)#no vrrp 5 ip 10.91.0.8
```

TO CONFIGURE SECONDARY IP ADDRESS FOR A VRRP GROUP



Note: The maximum number of secondary IP addresses allowed on a particular interface is 8.

Command (in ICM)	Description
vrrp <1-8> ip <ip-address> secondary	This command configures a secondary IP address for a VRRP group on an interface.
no vrrp <1-8> ip <ip-address> secondary	This command removes the secondary IP address from the VRRP group on an interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp 7 ip 10.91.0.101
secondary
```

```
ALU(config-if GigabitEthernet7/0)# no vrrp 7 ip 10.91.0.101
secondary
```

EXAMPLES OF CORRECT CONFIGURATION

The IP address must be unique across the system. The IP address used for a group cannot be used as interface address (primary or secondary) on any interface except on the interface on which the group is getting configured. It cannot be used as the group address for any other group on the same interface or on any other interface.

EXAMPLE 1

```
ALU(config-if GigabitEthernet7/0)# ip addr 10.1.1.1/24
ALU(config-if GigabitEthernet7/0)# ip addr 10.2.1.1/24
secondary
ALU(config-if GigabitEthernet7/0)# vrrp 1 ip 10.1.1.1
ALU(config-if GigabitEthernet7/0)# vrrp 2 ip 10.2.1.1
ALU(config-if GigabitEthernet7/0)# vrrp 3 ip 20.1.1.1
ALU(config-if GigabitEthernet7/0)# vrrp 4 ip 30.1.1.1
```

EXAMPLES OF INCORRECT CONFIGURATION

Consider the following examples for incorrect configuration with corresponding error messages:

EXAMPLE 1:

```
ALU(config-if GigabitEthernet3/0)#ip address 10.1.1.1/24
ALU(config-if GigabitEthernet3/0)#ip address 10.2.1.1/24
secondary
```

```
ALU(config-if GigabitEthernet3/0)#interface GigabitEthernet
3/1
ALU(config-if GigabitEthernet3/1)#ip address 20.1.1.1/24
ALU(config-if GigabitEthernet3/1)#ip address 20.2.1.1/24
secondary
```

```
ALU(config-if GigabitEthernet3/1)#vrrp 1 ip 10.1.1.1
Error - 10.1.1.1 already assigned as interface IP to
GigabitEthernet3/0
ALU(config-if GigabitEthernet3/1)#
```

```
ALU(config-if GigabitEthernet3/1)#interface GigabitEthernet
3/0
ALU(config-if GigabitEthernet3/0)#vrrp 2 ip 20.1.1.1
Error - 20.1.1.1 already assigned as interface IP to
GigabitEthernet3/1
ALU(config-if GigabitEthernet3/0)#
```

EXAMPLE 2:

```
ALU(config-if GigabitEthernet3/0)#vrrp 1 ip 10.1.1.1
ALU(config-if GigabitEthernet3/0)#vrrp 2 ip 10.2.1.1
ALU(config-if GigabitEthernet3/0)#interface GigabitEthernet
3/1
ALU(config-if GigabitEthernet3/1)#ip address 10.1.1.1/24
Error - Address already configured in a VRRP group on an
another interface
ALU(config-if GigabitEthernet3/1)#ip address 10.2.1.1/24
secondary
Error - Address already configured in a VRRP group on an
another interface
ALU(config-if GigabitEthernet3/1)#
```

MODIFY GLOBAL VRRP GROUP PARAMETERS

It is recommended that the modifications to VRRP group global parameters are done before enabling the VRRP group on the interfaces. Otherwise, this router might become a master or a slave inadvertently before finishing the customization.

For VRRP to be enabled on an interface for a group, the following three conditions have to be met:

- The primary address of the interface must be configured.
- The operational state of the interface must be up.
- The primary address of the group must be configured.

TO CONFIGURE VRRP ROUTER PRIORITY



Note: Priority cannot be changed for a VRRP group that is an IP address owner (i.e., VRRP group address same as the interface address). The default priority for this group is set to 255.

Command (in ICM)	Description
<code>vrrp <1-8> priority <1-254></code>	This command sets the priority for the router for a specific VRRP group.
<code>no vrrp <1-8> priority</code>	The “no” command restores the default priority for the VRRP group. The default priority is 100.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp 7 priority 104
```

TO CONFIGURE PRE-EMPTION TO THE VRRP GROUP



Note: Pre-emption is enabled by default.

Command (in ICM)	Description
<code>vrrp <1-8> preempt</code>	This command enables the preempt mode. By enabling the preempt mode, the configured router takes over as the master of a group if it has a higher priority than the existing master virtual router.
<code>no vrrp <1-8> preempt</code>	The “no” form of the above command disables pre-emption of the VRRP group.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp 7 preempt
```

```
ALU(config-if GigabitEthernet7/0)# no vrrp 7 preempt
```

TO DESCRIBE A VRRP GROUP



Note: User-defined string up to 80 characters is allowed.

Command (in ICM)	Description
<code>vrrp <1-8> description <string></code>	This command assigns a text description to the VRRP group.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp 7 description ALU-vrrp
```

To CONFIGURE AUTHENTICATION FOR A VRRP GROUP

Note:

- OA-700 supports null authentication and plain-text authentication.
- Maximum of 8 characters are allowed in the authentication string.

Command (in ICM)	Description
<code>vrrp <1-8> authentication text <password></code>	This command is used to set authentication for the VRRP group.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp 7 authentication text
net123
```

To SET THE ADVERTISEMENT INTERVAL

The VRRP advertisement command configures the advertisement interval for the VRRP group.

- By default the timer value is configured in seconds. It is in the range 1 - 255.
- The timer value can be configured in milliseconds by using the keyword **msec**. It is in the range 50 - 999 msec.

Command (in ICM)	Description
<code>vrrp <1-8> timers advertise {<1-255> msec <50-999>}</code>	This command is used to configure the interval between successive advertisements by the master virtual router in a VRRP group.
<code>no vrrp <1-8> timers advertise</code>	The "no" command restores the default advertisement interval. The default interval value is 1 second.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp 7 timers advertise 5
```


To LEARN THE ADVERTISEMENT INTERVAL

This command configures the backup virtual router to learn the advertisement interval used by the master virtual router.



Note: Learning is disabled by default.

Command (in CM)	Description
<code>vrrp <1-8> timers learn</code>	This command configures the backup virtual router to learn the advertisement interval used by the master virtual router.
<code>no vrrp <1-8> timers learn</code>	This command disables learning. The backup router uses the configured or the default advertisement interval to determine the downtime for the master.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp 7 timers learn
```



Note: Learning and millisecond timers are mutually exclusive. That is, learning cannot be enabled when millisecond timers are enabled and millisecond timers cannot be enabled if learning is enabled.

To CONFIGURE INTERFACE TRACKING

Command (in ICM)	Description
<code>vrrp <1-8> track-interface <interface-name></code>	This command configures the interface to be tracked that can alter the priority level of a virtual router in a VRRP group.
<code>no vrrp <1-8> track-interface</code>	The “no” command removes tracking of the interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# vrrp group track-interface serial1/0:0
```

MONITOR AND DEBUG VRRP

TO VIEW DETAILS OF ALL VRRP GROUPS

Command (in SUM/CM/ICM)	Description
<code>show vrrp all [brief]</code>	This command displays a brief or detailed status of all VRRP groups configured on the OA-700.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# show vrrp all
```

```
Interface GigabitEthernet3/0 - Group 1
State is Master
Virtual IP address is 10.1.1.1
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
Master Router is 10.1.1.1 (local), priority is 255
Master Advertisement interval is 1.000 secs
Master Down interval is 3.000 secs
```

```
Interface GigabitEthernet3/0 - Group 2
State is Master
Virtual IP address is 20.1.1.1
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 10.1.1.1 (local), priority is 100
Master Advertisement interval is 1.000 secs
Master Down interval is 3.000 secs
ALU(config-if GigabitEthernet3/0)#
```

```
ALU(config-if GigabitEthernet3/0)# show vrrp all brief
```

```
Interface Grp Prio Preempt State Master addr Group addr
GigabitEthernet3/0 1 255 Y Master 10.1.1.1 10.1.1.1
GigabitEthernet3/0 2 100 Y Master 10.1.1.1 20.1.1.1
ALU(config-if GigabitEthernet3/0)#
```

To DISPLAY VRRP INFORMATION ON A SPECIFIC INTERFACE

Command (in SUM/CM/ICM)	Description
show vrrp interface <i><interface-name> <slot/ port:channel.subchannel></i> [brief]	This command displays the VRRP groups and their status on a specified interface. (in the brief format, if specified).

EXAMPLE

```
ALU# show vrrp interface GigabitEthernet 3/0
```

```
Interface GigabitEthernet3/0 - Group 1
State is Master
Virtual IP address is 10.1.1.1
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
Master Router is 10.1.1.1 (local), priority is 255
Master Advertisement interval is 1.000 secs
Master Down interval is 3.000 secs

Interface GigabitEthernet3/0 - Group 2
State is Master
Virtual IP address is 20.1.1.1
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 10.1.1.1 (local), priority is 100
Master Advertisement interval is 1.000 secs
Master Down interval is 3.000 secs
```

To VIEW VRRP CONTROL DEBUG MESSAGES

Command (in SUM/CM/ICM)	Description
debug vrrp control {rib protocol all}	This command displays VRRP control debug messages.

EXAMPLE

```
ALU# debug vrrp control all
```

To View VRRP Management Messages

Command (SUM/CM/ICM)	Description
<code>debug vrrp management</code> {all protocol vrrpfs }	This command displays VRRP management debug messages.

EXAMPLE

```
ALU# debug vrrp management all
```

VRRP Interface Tracking

The VRRP interface tracking feature extends the capabilities of the VRRP to allow tracking of specific interfaces that can alter the priority level of a virtual router in a VRRP group.

For example, a WAN interface can be tracked. If the WAN interface goes down, then the priority of the VRRP group is lowered, and another VRRP router with the next highest priority becomes the master for that VRRP group.

ALCATEL-LUCENT'S INTERFACE TRACKING DESIGN

For each VRRP group that is configured, you can specify an interface that needs to be tracked by the VRRP module for that group. The VRRP module in the router will actively monitor the status of the specified interface. Any change in the status of the interface will affect the priority of the router. When track interface is enabled for a VRRP group, the behavior of the router is as follows:

WHEN THE TRACK INTERFACE GOES DOWN

The following section details the process followed by a router when it is either in master state or backup state, when the track interface goes down.

ROUTER IN MASTER STATE

The following actions are taken when the track interface goes down:

- The router will set its priority to 20.
- Any router with the next highest priority will take over as the master, and the state of the current master router changes to a backup state.
- In the absence of another active router with the next highest priority, the current router will become the master again to provide some limited set of services.

ROUTER IN BACKUP STATE

The router will not take any action when the track interface goes down.

WHEN TRACK INTERFACE COMES UP

The following section details the process followed by the Master and Backup routers when the track-interface comes up.

ROUTER IN MASTER STATE

- If the router is the address owner, then the router will set its operational priority to 255.
- If the router is not the address owner, then the router will set its operational priority to the configured priority.

ROUTER IN BACKUP STATE

The router in backup state will take the following actions when the track interface comes up. The actions taken vary based on whether the router is the address owner or not. This is explained in case (i) and case (ii) below:

Case (i): Router is Address Owner

If the router is the address owner and the priority is equal to track interface down priority (implies that the router went to backup because the track interface went down), it performs the following:

The router will take the following actions when the track interface comes up:

- Cancels master down timer.
- Sets the master down interval to skew time.
- Sets the operational priority to 255.
- Schedules the new master down timer.

The above action result in the router becoming the master.

Case (ii): Router is not the Address Owner:

The router will take the following action when it is not the address owner, and the track interface comes up.

- Sets the priority of the router to the configured value and stays as backup.
- Any state changes that may need to happen will happen when the next advertisement packet is received or when the master down timer fires.

ENTERING MASTER STATE

The following actions are taken before entering the master state, when the track interface is enabled:

- If the track interface is down, the operation priority is set to the track interface down priority (20).
- The router will send an advertisement with priority 20.
- The router will switch to backup state if a router with the next highest priority overrides it. Else, the router will remain in master state to provide some minimal set of services.

VRRP CONFIGURATION SCENARIO USING OA-700

The topology consists of the following components:

- OA-700
- Cisco Router
- Switch
- PC/Laptop

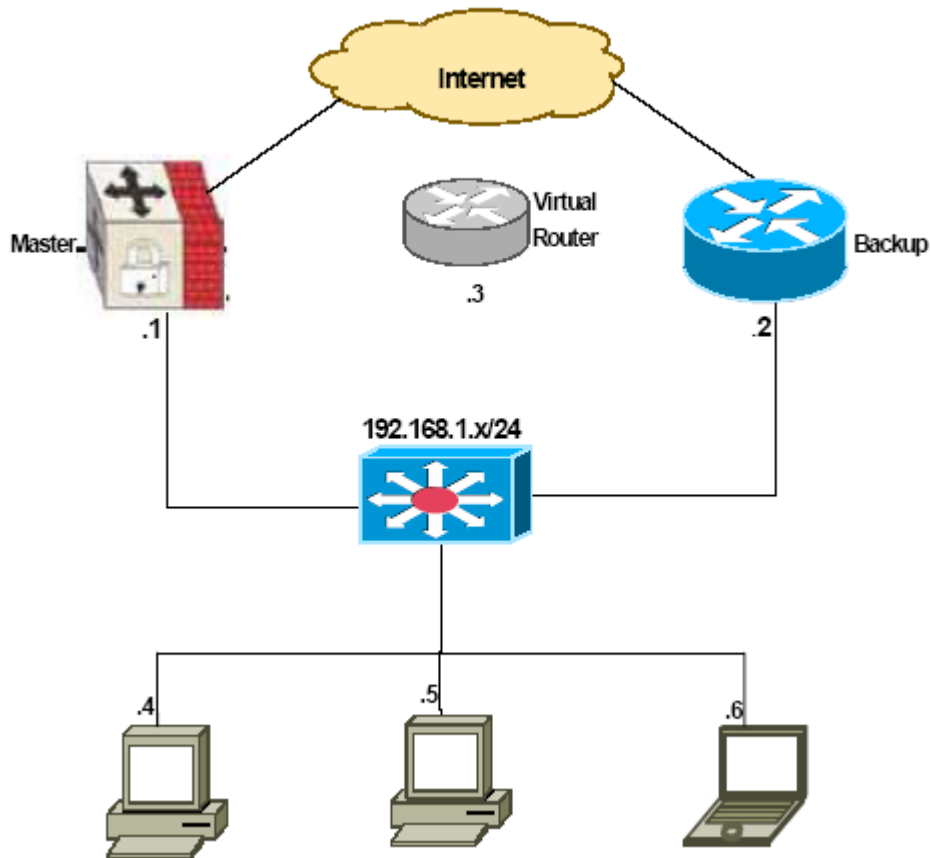


Figure 3: VRRP Topology

PROCEDURE

Configure LAN stations (192.168.1.4, 192.168.1.5, 192.168.1.6) with default gateway address of 192.168.1.3, which is IP address of Virtual Router.

VRRP CONFIGURATION

In the following example, OA-780 and Cisco belongs to VRRP Group 1.



Note: Both VRRP routers should be configured with same group ID.

In the configuration, each router has the following properties:

- OA-780
 - i. VRRP Group ID is 1
 - ii. Assign IP address as 192.168.1.3/24
 - iii. VRRP IP address is 192.168.1.3 (OA-780 becomes the master router because of the highest priority, 255)
- Cisco router
 - i. VRRP Group ID is 1
 - ii. Assign IP address 192.168.1.2 255.255.255.0
 - iii. VRRP IP address is 192.168.1.3
 - iv. Priority for the group is 110 (Cisco becomes the backup router because of the lower priority)

OA-780

```
ALU#config terminal
ALU(config)# interface GigabitEthernet7/1
ALU(config-if-GigabitEthernet7/1)# ip address 192.168.1.3/24
ALU(config-if-GigabitEthernet7/1)# vrrp 1 ip 192.168.1.3
ALU(config-if-GigabitEthernet7/1)# vrrp 1 priority 120
```

Cisco

```
Cisco(config)# interface Ethernet0/0
Cisco(config-if-Ethernet0/0)# ip address 192.168.1.2
255.255.255.0
Cisco(config-if-Ethernet0/0)# vrrp 1 ip 192.168.1.3
Cisco(config-if-Ethernet0/0)# vrrp 1 priority 110
```


Part 2 LAN Interfaces and Configuration



CHAPTER 5 ETHERNET INTERFACES ON SE

This chapter details the Ethernet Interface configuration on the OA-700. These interfaces can be used in the slots pertaining to the “**Services Engine (SE)**” on the OA-700.

The “[Ethernet Overview](#)” section serves only as an additional information on the Ethernet Interfaces. You can skip this section and directly go to the configuration details “[Ethernet Configuration](#)” section. Refer “[Alcatel-Lucent Specific Overview on Ethernet Interfaces](#)” to get a detailed overview on the usage of Ethernet interfaces on the OA-700.

Chapter Organization:

- “[Ethernet Overview](#)”
- “[Ethernet Configuration](#)”

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
GigE	Gigabit Ethernet
ICM	Interface Configuration Mode - ALU (config-interface name)#
SUM	Super User Mode - ALU#

ETHERNET OVERVIEW

In 1973, at Xerox Corporation, researcher Bob Metcalfe designed and tested the first Ethernet network. While working on a way to link a computer to a printer, Metcalfe developed the method of physically cabling the devices on the Ethernet. Ethernet has since become the most popular and most widely deployed network technology in the world.

The Ethernet standard has grown to encompass new technologies as computer networking has matured. The original Ethernet described communication over a single cable shared by all devices on the network. Once a device is attached to this cable, it has the ability to communicate with any other attached device. This allows the network to expand to accommodate new devices without requiring any modification to those devices already on the network.

Refer the following section to configure the Ethernet interfaces on your system:

- [“Ethernet Basics”](#)
- [“Ethernet Terminologies”](#)
- [“Full-duplex Ethernet”](#)
- [“Switched Ethernet”](#)

ETHERNET BASICS

Ethernet is a local area technology with networks traditionally operating within a single building, connecting devices in close proximity. At most, Ethernet devices could have only a few hundred meters of cable between them, making it impractical to connect geographically dispersed locations. Modern advancements have increased these distances considerably allowing Ethernet networks to span tens of kilometers.

ETHERNET TERMINOLOGIES

Ethernet follows a simple set of rules that govern its basic operation. The basics of Ethernet terminology include:

- **Medium** - Ethernet devices attach to a common medium that provides a path along which the electronic signals travel. Historically, this medium has been coaxial copper cable, but today it is more commonly a twisted pair or fiber optic cabling.
- **Segment** - A single shared medium as an Ethernet segment.
- **Node** - Devices that attach to that segment are stations or nodes.
- **Frame** - The nodes communicate in short messages called frames, which are variably sized chunks of information. Each frame must include, for example, both a destination address and a source address, which identify the recipient and the sender of the message. The address uniquely identifies the node. No two Ethernet devices should ever have the same address.
- **Ethernet addressing** - Ethernet addressing implements a broadcast address. A frame with a destination address equal to the broadcast address, is intended for every node on the network, and every node will both receive and process this type of frame.

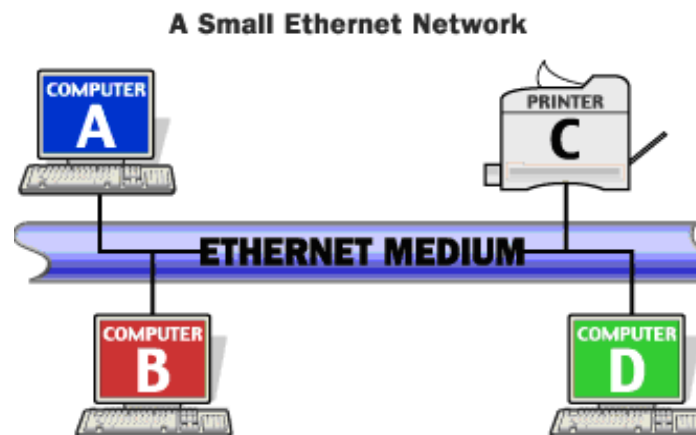


Figure 4: Ethernet Network

For example, in the figure above, when computer B transmits to printer C, computers A and D will also receive and examine the frame. However, when a station first receives a frame, it checks the destination address to see if the frame is intended for itself. If it is not, the station discards the frame without even examining its contents.

SWITCHED ETHERNET

Modern Ethernet implementations often look nothing like their historical counterparts. The legacy Ethernet was long runs of coaxial cable providing attachments for multiple stations, whereas, modern Ethernet networks use twisted pair wiring or fiber optics to connect stations in a radial pattern. Where legacy Ethernet networks transmitted data at 10 megabits per second (Mbps), modern networks can operate at 1,000 Mbps or even in Gbps.

Switched networks replace the shared medium of legacy Ethernet with a dedicated segment for each station. These segments connect to a switch, which acts much like an Ethernet bridge, but can connect many of these single station segments. Some switches today can support hundreds of dedicated segments.

FULL-DUPLEX ETHERNET

Ethernet switching gave rise to another advancement, full-duplex Ethernet. Full-duplex refers to the ability of a network, to send and receive data at the same time.

Legacy Ethernet is half-duplex, meaning information can move in only one direction at a time. In a totally switched network, nodes only communicate with the switch and never directly with each other. Switched networks also employ either twisted pair or fiber optic cabling, both of which use separate conductors for sending and receiving data. This allows end stations to transmit to the switch at the same time that the switch transmits to them, achieving a collision-free environment.

ALCATEL-LUCENT SPECIFIC OVERVIEW ON ETHERNET INTERFACES

The SE card is the main data processing center in the chassis. The SE card has two external auto-negotiable copper Gigabit Ethernet interfaces. The GigE interfaces can auto-negotiate, transmit and receive data packets at rates of 10/100/1000 Mbps.

The LEDs on SE card indicate Active or Fault conditions. The LEDs on Gigabit Ethernet ports of SE card indicate Link Status and Activity. The SE card is a dual slot line card, and can be installed in slots 2, 3 or slots 6, 7 in OA-780. In OA-740, SE can be installed in slots 2, 3.

ETHERNET CONFIGURATION

Refer to the following sections to configure an Ethernet interface on the OA-700.

ETHERNET INTERFACE CONFIGURATION STEPS

This section lists the step by step instructions to configure Ethernet interface.

Step 1: Enter into Configuration Mode.

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure Gigabit Ethernet interface. See [“To Configure GigE Interface”](#)

Step 3: Administratively bring up the interface.

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 4: Configure IP address for the interface.

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 5: Configure parameters that are optional on the interface.

- Configure Duplex Operation on the interface. See [“To Configure Duplex Operation”](#)
- Configure Flow control on the interface. See [“To Configure Flow Control”](#)
- Configure MTU on the interface. See [“To Configure MTU \(Maximum Transmission Unit\) on the Interface”](#)
- Configure Speed on the interface. See [“To Configure Speed”](#)

Step 6: View the configuration details on the interface. See [“Ethernet Interface Show Commands”](#).

Step 7: Clear interface statistics. See [“Ethernet Interface Clear Commands”](#).

ETHERNET INTERFACE CONFIGURATION FLOW

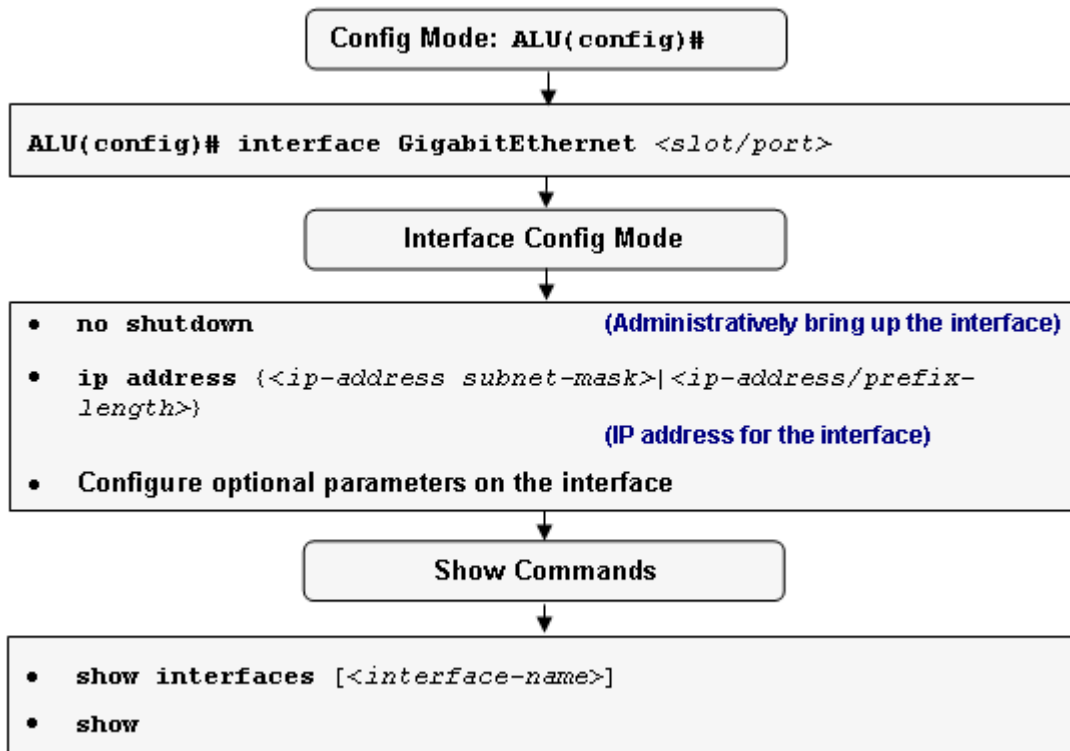


Figure 5: Ethernet Interface Configuration Flow

ETHERNET INTERFACE CONFIGURATION COMMANDS

This section provides an expansive view on the commands that are used in configuring the Ethernet Interfaces.

To CONFIGURE GIGE INTERFACE

Command (in CM)	Description
<code>interface GigabitEthernet <slot/port></code>	This command allows you to configure GigE interface.

EXAMPLE

The following example shows configuring GigE interface:

```
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)#
```

To CONFIGURE DUPLEX OPERATION

Command (in ICM)	Description
<code>duplex {auto full half}</code>	This command configures duplex operation on an interface.
<code>no duplex</code>	The “no” command sets the duplex mode to its default. The default duplex mode is “ auto ”.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# duplex full
ALU(config-if GigabitEthernet7/0)# no duplex
```

To CONFIGURE FLOW CONTROL

Command (in ICM)	Description
<code>flowcontrol {receive send} {off on}</code>	This command configures flow control on a GigE interface.
<code>no flowcontrol {receive send} {off on}</code>	The “no” command sets the flow control to its default. By default, flow control is set to “ Off ”.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# flowcontrol send on
ALU(config-if GigabitEthernet7/0)# no flowcontrol send on
```

Alcatel-Lucent

To CONFIGURE MTU (MAXIMUM TRANSMISSION UNIT) ON THE INTERFACE

Command (in ICM)	Description
mtu <64-1500>	This command is used to configure the MTU of the interface, i.e., the maximum packet size that the interface can accept.
no mtu <64-1500>	The “no” command sets the MTU to its default. The default MTU is 1500 bytes.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# mtu 100
```

```
ALU(config-if GigabitEthernet7/0)# no mtu
```

To CONFIGURE SPEED

Command (in ICM)	Description
speed [10 100 1000 auto]	This command configures the interface speed.
no speed	The “no” command sets the interface speed to its default. The default speed is “auto”.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# speed 100
```

```
ALU(config-if GigabitEthernet7/0)# no speed
```

ETHERNET INTERFACE SHOW COMMANDS

TO VIEW INTERFACE CONFIGURATION

Command (in CM/ICM)	Description
show interfaces [<i><interface-name></i>]	This command displays traffic and all the corresponding details of all the interfaces configured. If interface name is specified, corresponding details for a specified interface is displayed.

EXAMPLE 1

ALU# **show interfaces**

```

loopback1 is up, line protocol is up
  Internet address is 55.0.0.35/24
  MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
  reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation LOOPBACK, loopback not set
  Keepalive not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/0/0/0 (size/max/drops/flushes);
  Total output drops: (null)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
    loopback is up, line protocol is up
  Internet address is 11.11.11.11/24
  MTU 1500 bytes, BW 0 Kbit, DLY 0 usec, reliability 0/255,
  txload 0/255, rxload 0/255
  Encapsulation LOOPBACK, loopback not set
  Keepalive not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/0/0/0 (size/max/drops/flushes); Total
  output drops: (null)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected

```

```

0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
GigabitEthernet7/0 is up, line protocol is up
  Hardware address is 0000.2222.3333 (0000.2222.3333)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
  reliability 0/255, txload 0/255, rxload 0/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 0, loopback not set
Keepalive not set
  Auto-duplex, Auto speed, 1000BaseTx/Fx
  ARP type: ARPA, ARP Timeout never
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5985 packets input, 674968 bytes, 0 no buffer
    Received 12 broadcasts, 2 runts, 0 giants
    24 input errors, 21 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 4583 multicast, 0 pause input
    4766 packets output, 486524 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    2 lost carrier, 2 no carrier, 0 pause output
    0 output buffer copied, 0 interrupts, 0 failures
ALU#

```

EXAMPLE 2

ALU# show interfaces GigabitEthernet 7/0

```

GigabitEthernet7/0 is up, line protocol is up
  Hardware address is 0000.1111.2222 (0000.1111.2222)
  Internet address is 1.1.1.1/24
  MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
  reliability 0/255, txload 0/255, rxload 0/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 0.,
loopback not set Keepalive not set
  Auto-duplex, Auto speed, 1000BaseTx/Fx
  ARP type: ARPA, ARP Timeout never
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5397 packets input, 380818 bytes, 0 no buffer
    Received 21 broadcasts, 1 runts, 0 giants
    2 input errors, 1 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 2465 multicast, 0 pause input
    2503 packets output, 212146 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    1 lost carrier, 2 no carrier, 0 pause output
    0 output buffer copied, 0 interrupts, 0 failures
ALU#

```

To VIEW GiGE INTERFACE DETAILS

Command (in ICM)	Description
show	This command is used in the Interface Configuration Mode. This command displays traffic on the GigE interface.

EXAMPLE

```

ALU(config-if GigabitEthernet7/0)# show
GigabitEthernet7/0 is up, line protocol is up
  Hardware is Intel 82546, address is 0011.8b00.2728
(0011.8b00.2728)
  Internet address is 9.9.9.9/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Loopback not set
  Encapsulation ARPA,    keepalive not set
  Auto-duplex, 1000Mb/s, 1000BaseTx/Fx
  ARP type: ARPA, ARP Timeout never
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0 (size/max), 0 drops; Input queue 0/0
(size/max), 0 drops
  5 minute input rate 344 bits/sec, 1 packets/sec
  5 minute output rate 8 bits/sec, 0 packets/sec
    68 packets input, 5108 bytes, 0 no buffer
    Received 39 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    3 packets output, 192 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer copied, 0 interrupts, 0 failures

```

ETHERNET INTERFACE CLEAR COMMANDS

TO CLEAR COUNTERS ON GIGE INTERFACE

Command (in ICM/CM)	Description
<code>clear counters</code> <code>GigabitEthernet <slot/port></code> (<code>:subinterface_number</code>)	This command clears the counters on a specific GigE interface.

EXAMPLE

```
ALU(config)# clear counters GigabitEthernet 7/0
Clear counters on this interface [confirm]
ALU(config)#
```

TO CLEAR COUNTERS ON GIGE INTERFACE

Command (in ICM)	Description
<code>clear</code>	This command is used in the Interface Configuration Mode. This command clears the counters on a specific GigE interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# clear
Clear counters on this interface [confirm]
ALU(config)#
```

CHAPTER 6 LAYER 2 SWITCHING CONFIGURATION

This chapter covers the commands used to configure switching on the Layer 2 (L2) cards in the OA-700. It provides a broad overview on the L2 GE commands with an expansive outlook on VLAN support consisting of Access ports, Trunk ports and Hybrid ports.

The **“Switching Overview”** section serves as an additional information on L2 switching. You can skip this section, and directly go to the configuration details: **“L2 Switching Configuration”**. Refer to the **“Alcatel-Lucent Specific Overview on Switching”** for Alcatel-Lucent specific features.

Basic scenarios using switching on OA-700 is given in the last section. You can refer to this section for getting an in-depth knowledge of configuring OA-700 on a real-time system **Switching Configuration using OA-700**.

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#

SWITCHING OVERVIEW

Bridges and switches are data communication devices that operate principally at Layer 2 of the OSI reference model. As such they are widely referred to as Data Link Layer devices.

Bridges became commercially available in the early 1980s. At the time of their introduction, bridges connected and enabled packet forwarding between homogeneous networks. More recently, bridging between different networks has also been defined and standardized. Several kinds of bridges have proven important as internetworking devices. '**Transparent bridging**' is found primarily in Ethernet environments. '**Translational bridging**' provides translation between the formats and transit principles of different media types.



Note: The OA-700 supports only transparent bridging.

Bridging and switching occur at the link layer, which controls data flow, handles transmission errors, provides physical addressing, and manages access to the physical medium. By dividing large networks into self-contained units, bridges and switches provide several advantages.

The switch acts as a firewall for some potentially damaging network errors and will accommodate communication between a larger number of devices than would be supported on any single LAN connected to the bridge. Bridges and switches extend the effective length of a LAN, permitting the attachment of distant stations that was not previously permitted.

Since the only devices on the segments are the switch and the end station, the switch picks up every transmission before it reaches another node. The switch then forwards the frame over the appropriate segment, just like a bridge, but since any segment contains only a single node, the frame only reaches the intended recipient. This allows many conversations to occur simultaneously on a switched network.

Some switches support cut-through switching, which reduces latency and delays in the network, while bridges support only store-and-forward traffic switching. Switches also reduce collisions on network segments because they provide dedicated bandwidth to each network segment. Some bridges are MAC-layer bridges, which bridge between homogeneous networks, while other bridges can translate between different link layer protocols. The basic mechanics of such a translation is depicted in the graphic below.

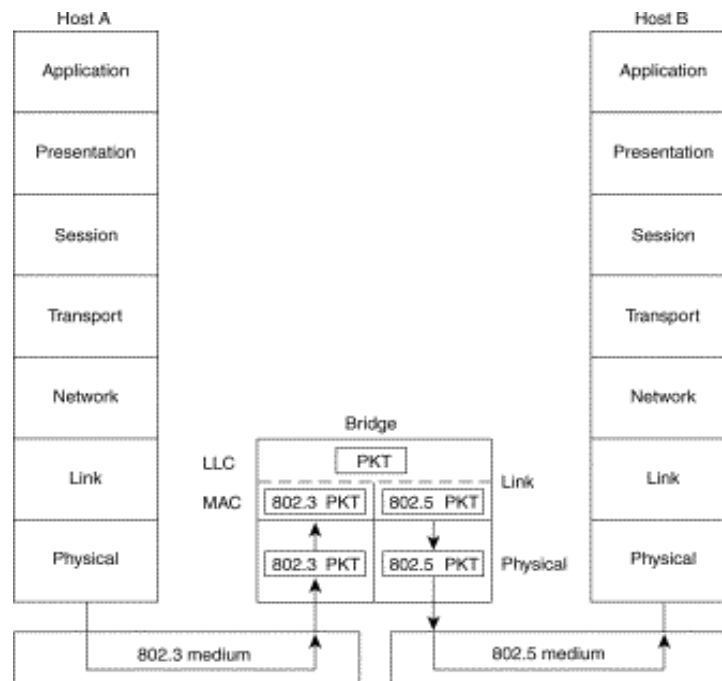


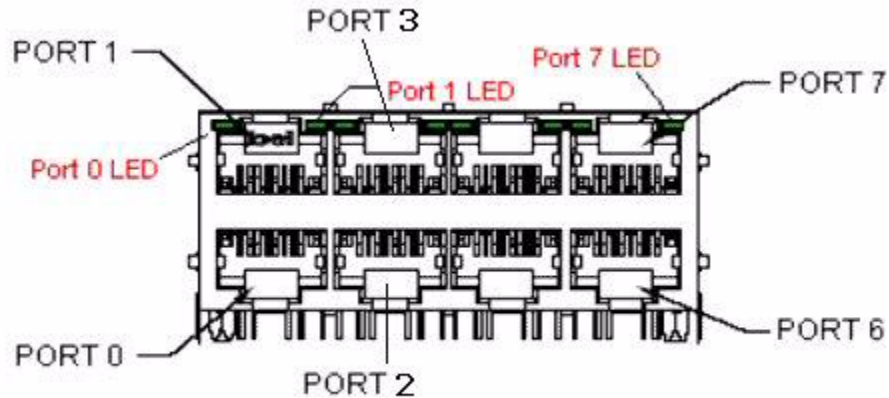
Figure 6: Layer 2 Switching

Layer 2 switches operate using physical network addresses. Physical addresses, also known as link-layer, hardware, or MAC-layer addresses, identify individual devices. Most hardware devices are permanently assigned this number during the manufacturing process.

Switches operating at Layer 2 are very fast because they are just sorting physical addresses, but they usually are not very smart - that is, they do not look at the data packet very closely to learn anything more about where it is headed.

ALCATEL-LUCENT SPECIFIC OVERVIEW ON SWITCHING

The schematic below is the L2-GE Front Panel view of the RJ-45 connector.



Green LED: On (Link up); Off (Link down); Blinking (Tx/Rx Active)

Figure 7: L2-GE Front Panel View of the RJ-45 Connector

- Each L2 card consist of eight ports.
- L2 interface can be configured for four modes of operation, namely:
 - i. **Pure bridging mode** - Packets are bridged across other switchports of pure bridging mode based on the mac-address table, without considering the VLAN tag information.
 - ii. **Access** - Used to connect end stations (LAN devices) to switch ports. Each access port can belong to a VLAN. This port can send and receive untagged packets.
 - iii. **Trunk** - A trunk port sends and receives only tagged packets.
 - iv. **Hybrid** - These ports are used to connect both VLAN-aware (tagged) devices as well as VLAN-unaware (untagged) devices.
- The default VLAN-id is VLAN-1.
- Supports software bridging, VLAN can be configured on any number of line cards.
- If VLAN spreads across the line cards, line rate switching can not be achieved.
- All interfaces are by default in the “shutdown” mode. You have to administratively bring them up by using the command “**no shutdown**”.
- Native VLANs are applicable only for hybrid modes.
- The mode of the interface can be set by using the command “**switchport mode trunk / hybrid**”. If this command is not issued and if the interface is configured with access VLAN configuration, then the interface will be set to “**access mode**”.
- If an interface has both access and trunk configuration, the interface can be set to trunk mode by using the command “**switchport mode trunk**”.

- Similarly, if an interface has both access and hybrid configuration, the interface can be set to hybrid mode by issuing the command “**switchport mode hybrid**”.
- If an interface is set to either hybrid/ trunk mode, the interface can be set to access mode by issuing the command “**no switchport mode trunk/hybrid**”, provided access configuration exists. If no access configuration exists, interface is set to pure bridging mode.
- In the Hybrid mode, if a VLAN is configured as both native VLAN and Trunk VLAN, native VLAN takes precedence.
- If no mode is configured on the switchport, and if no access VLAN configuration exists on the switchport, the switchport will be in pure bridging mode. In this mode, packets are bridged across other switchports of pure bridging mode based on the mac-address table, without considering the VLAN tag information.



Note: MTU configuration is not supported on switchport interfaces. However, MTU can be configured on VLAN interfaces.

L2 SWITCHING CONFIGURATION

Refer to the following steps to enable switching on the L2 card in the OA-700.

L2 SWITCHING CONFIGURATION STEPS

The following commands enable switching on the L2 card in the OA-700.

Step 1: Enter Configuration Mode.

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure a L2 interface. See [“To Configure an L2 Interface”](#)

Step 3: Administratively bring up the interface. See [“To Administratively Bring Up/Down the L2 Interface”](#)

L2 interface can be configured for four modes of operation. Following are the steps to configure L2 to either Access, Trunk or Hybrid mode. These steps are optional.

Configure L2 interface to operate in Pure Bridging Mode:

Step 1: Configure L2 interface to Pure Bridging mode by using **“no switchport mode”** command. See [“To Configure Mode for the L2 Interface”](#) (If no access VLAN is configured)

OR

Configure L2 interface to operate in Access Mode:

Step 1: Configure L2 interface to Access mode by using **“no switchport mode”** command. See [“To Configure Mode for the L2 Interface”](#) (if Trunk/Hybrid mode is already configured)

Step 2: Configure VLAN for Access mode. See [“To Configure VLAN for Access Mode”](#)

OR

Configure L2 interface to operate in Trunk Mode:

Step 1: Configure L2 interface to Trunk mode. See [“To Configure Mode for the L2 Interface”](#)

Step 2: Configure tagged VLANs that will be allowed when the interface is configured to Trunk mode. See [“To Configure Trunk VLAN”](#)

OR

Configure L2 interface to operate in Hybrid Mode:

Step 1: Configure L2 interface to Hybrid mode. See [“To Configure Mode for the L2 Interface”](#)

Step 2: Configure tagged VLANs that will be allowed when the interface is configured to Hybrid mode. See [“To Configure Trunk VLAN”](#)

Step 3: Configure Native VLAN (untagged VLAN). See [“To Configure Hybrid Native VLAN”](#)

Monitor and troubleshoot the configuration using the “show” commands. See [“L2 Switching Show Commands”](#)

Use the clear command to clear the MAC address table entries. See [“L2 Switching Clear Commands”](#)

L2 SWITCHING CONFIGURATION FLOW

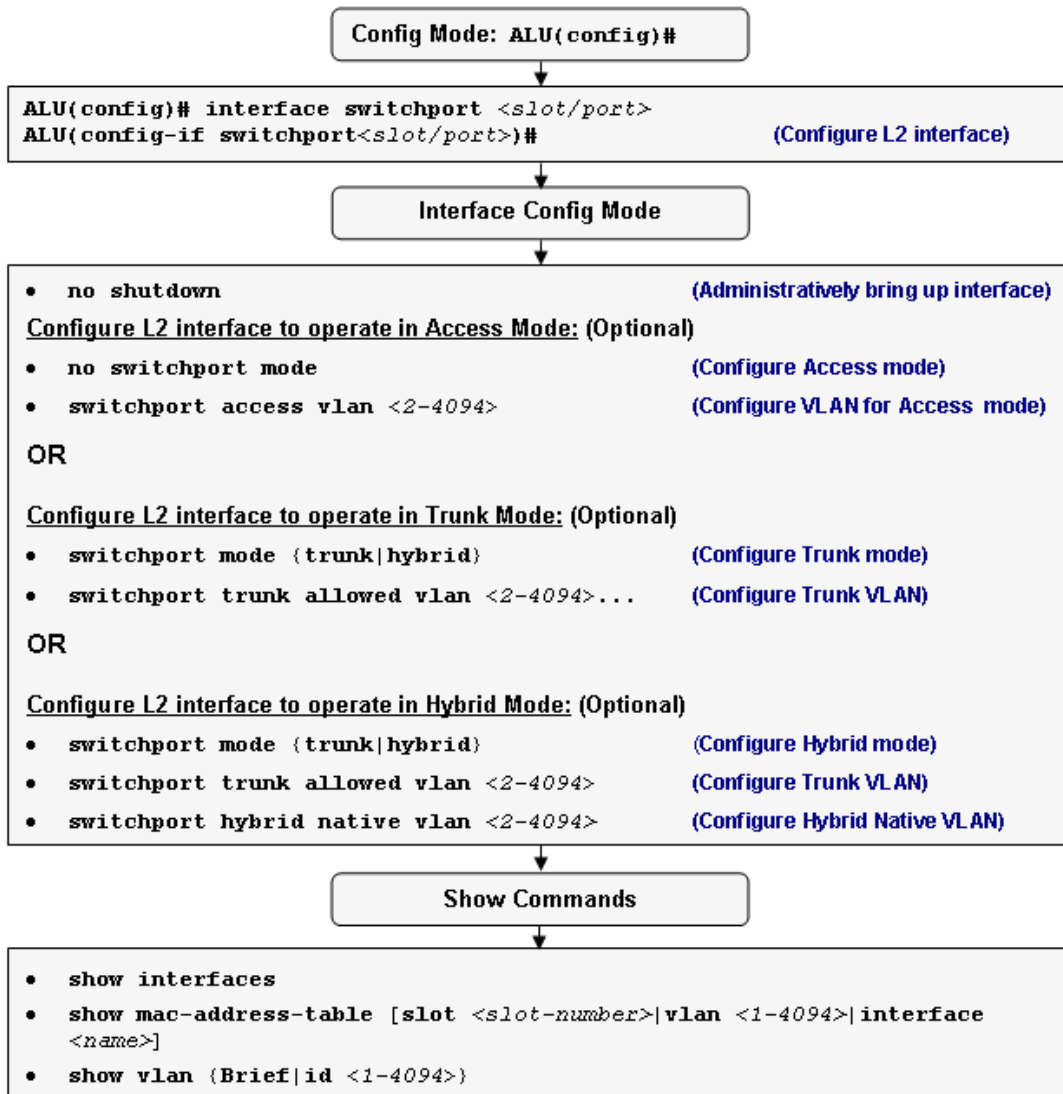


Figure 8: L2 Switching Configuration Flow

L2 SWITCHING COMMANDS

TO CONFIGURE AN L2 INTERFACE

Command (in CM)	Description
<code>interface switchport <slot/ port></code>	This command is used to configure an L2 interface.

EXAMPLE

```
ALU(config)# interface switchport 1/0
ALU(config-if switchport1/0)#
```

TO ADMINISTRATIVELY BRING UP/DOWN THE L2 INTERFACE

Command (in ICM)	Description
<code>no shutdown</code>	This command is used to administratively bring up the L2 interface.
<code>shutdown</code>	This command is used to administratively bring down the L2 interface.

EXAMPLE

```
ALU(config-if switchport1/0)# no shutdown
```

TO CONFIGURE MODE FOR THE L2 INTERFACE

Command (in ICM)	Description
<code>switchport mode {trunk hybrid}</code>	This command is used to configure the L2 interface in the trunk or hybrid mode.
<code>no switchport mode</code>	This command first removes the hybrid/trunk mode configured on the interface. If the interface is configured with access VLAN configuration, it changes to access mode since it takes precedence over the bridging mode. If no access VLAN is configured, then the interface moves to pure bridging mode .

EXAMPLE

```
ALU(config-if switchport1/0)# switchport mode trunk
ALU(config-if switchport1/0)# no switchport mode
```

To CONFIGURE VLAN FOR ACCESS MODE

Command (in ICM)	Description
<code>switchport access vlan <2-4094></code>	This command is used to configure VLANs for access mode in the range 2-4094.
<code>no switchport access vlan</code>	This command deletes the access VLANs configured on the interface. This makes it to switch over to the pure bridging mode.

EXAMPLE

```

ALU(config-if switchport1/0)# switchport access vlan 10

ALU(config-if switchport1/0)# no switchport access vlan

```

To CONFIGURE TRUNK VLAN

Command (in ICM)	Description
<code>switchport trunk allowed vlan <2-4094>...</code>	This command is used to configure VLANs for trunk mode in the range 2-4094. Multiple VLANs can be configured.
<code>no switchport trunk allowed vlan <2-4094>...</code>	This command deletes the trunk VLANs configured on the interface.

EXAMPLE

```

ALU(config-if switchport1/0)# switchport trunk allowed vlan 3

ALU(config-if switchport1/0)# switchport trunk allowed vlan 5 8
9

ALU(config-if switchport1/0)# no switchport trunk allowed vlan
3 5

```


To CONFIGURE HYBRID NATIVE VLAN

Command (in ICM)	Description
<code>switchport hybrid native vlan <2-4094></code>	This command is used to configure Native VLAN for hybrid mode in the range 2-4094.
<code>no switchport hybrid native vlan</code>	This command deletes the native VLAN configured on the interface, and resets it to its default. The default hybrid native VLAN ID is 1.

EXAMPLE

```

ALU(config-if switchport1/0)# switchport hybrid native vlan 7
ALU(config-if switchport1/0)# no switchport hybrid native vlan

```

L2 SWITCHING SHOW COMMANDS

TO VIEW THE CHASSIS INFORMATION

Command (in ICM)	Description
show chassis	This command displays all the cards configured on the OA-700. Issue this command to check if the L2 card is installed appropriately in the system.

EXAMPLE

ALU> show chassis

```

Physical inventory at Tue Oct 30 06:33:47 2007
System started approximately Tue Oct 30 06:30:26 2007
Uptime is 0 days 0 hours 4 minutes 20 seconds
L2 - 8-port copper GigE (active)
Slot number: 0
Part number: 902603-90
Manufacturer: ALU
Description: 8-port copper GigE
Serial number: DD0512560340
Version: 00
Revision: 01
Deviation: 0000
Loader version: 2.27
ALU-OS version: 2.2.52
MDC
Serial number: WL0534000127
Deviation: 0001
Revision: A1
Version: 01
SE - Service engine (active)
Slot number: 3
Part number: 902601-90
Manufacturer: ALU
Description: Service engine
Serial number: DD0538002048
Version: 01
Revision: 04
Deviation: 0001
CPU Version: 1 (Low Power Opteron)
Opteron CPU Version: 1
Opteron CPU Frequency: 2193 MHz
Loader version: 2.30
ALU-OS version: 2.2.64
MDC
Serial number: WL0529000008
Deviation: 0002
Revision: 05
Version: 01

```

PB - Power tray (passive)
Slot number: 22
Part number: 902612-90
Manufacturer: ALU
Description: Power tray
Serial number: DD0536004050
Version: 00
Revision: 01
Deviation: 0000

SC - Switch card (active)
Slot number: 24
Part number: 902613-90
Manufacturer: ALU
Description: Switch card
Serial number: DD0536054350
Version: 00
Revision: 54
Deviation: aaaa
LoL firmware version: 2.2.56
Loader version: 2.29
ALU-OS version: 2.2.52

FP - Fan tray (passive)
Slot number: 26
Part number: 902614-90
Manufacturer: ALU
Description: Fan tray
Serial number: DD0545027001
Version: 00
Revision: 01
Deviation: 0000

BP - ALU OA780 chassis (passive)
Slot number: 29
Part number: 902611-90
Manufacturer: ALU
Description: ALU OA780 chassis
Serial number: DD0546005005
Version: 00
Revision: 01
Deviation: 0000
Base MAC: 00:11:8b:00:72:00

To VIEW INTERFACES

Command (in CM/ICM)	Description
show interfaces	This command if issued in the Configuration mode, displays the statistics of all the interfaces including the information of all the L2 ports.
show	This command if issued in the Interface Configuration Mode displays the statistics of only that particular interface.

EXAMPLE

```
ALU(config-if switchport0/0)# show
```

```
switchport0/0 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0011.8b00.0e21
(0011.8b00.0e21)
  MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  loopback not set, Keepalive not set
  Auto-duplex, Auto, 1000BaseTx/Fx
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0(size/max),0 drops;Input queue 0/0(size/max), 0drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1950230 packets input, 722390067 bytes
    Received 48676 broadcasts, 0 runts, 0 giants,0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun,0 ignored
    0 watchdog, 14154 In multicast, 0 pause input
    0 input packets with dribble condition detected
  1971500 packets output, 842881406 bytes, 328 Sent broadcasts
  0 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 Out multicast, 0 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out
```

To VIEW VLANs CONFIGURED ON OA-700

Command (in CM)	Description
<code>show vlan {Brief id <1-4094>}</code>	<ul style="list-style-type: none"> The “show vlan Brief” command displays all the VLANs that are configured on the OA-700. The “show vlan id” displays the configuration of a specific vlan-id.

EXAMPLE

ALU# `show vlan id 10`

VLAN_ID	Status	Interface name	Mode
-----	-----	-----	-----
10	Inactive	switchport0/0	Access

ALU(config)# `show vlan Brief`

VLAN_ID	Status	Interface name	Mode
-----	-----	-----	-----
1	Inactive	switchport0/2	No-Mode
		switchport0/3	No-Mode
		switchport0/4	No-Mode
		switchport0/5	No-Mode
10	Inactive	switchport0/0	Access
		switchport0/7	Access
		switchport0/6	Trunk
20	Inactive	switchport0/1	Access

To VIEW THE MAC-ADDRESS-TABLE

Command (in CM)	Description
<code>show mac-address-table [slot <slot-number> vlan <1-4094> interface <name>]</code>	This command displays the mac-address-table learnt by the system.



Note: The current release supports only dynamic learning of MAC-addresses.

EXAMPLE

ALU# `show mac-address-table`

Mac Address	Interface	Vlan	Type
-----	-----	-----	-----
0001.2924.2959	switchport0/0	10	Dynamic
0001.e6b0.77eb	switchport0/0	10	Dynamic
0006.1bd4.3847	switchport0/0	10	Dynamic
0006.1bd4.655d	switchport0/0	10	Dynamic
00c0.9f33.6d23	switchport0/0	10	Dynamic
00c0.9f33.6e54	switchport0/0	10	Dynamic
00c0.9f33.7c84	switchport0/0	10	Dynamic
0000.5e00.0101	switchport0/1	20	Dynamic
0008.a16b.6597	switchport0/1	20	Dynamic
0008.a170.59ea	switchport0/1	20	Dynamic
0008.a170.5e1d	switchport0/1	20	Dynamic
0008.a170.5e21	switchport0/1	20	Dynamic
0008.a177.fecc	switchport0/1	20	Dynamic
0008.a177.fece	switchport0/1	20	Dynamic
0008.a178.4b19	switchport0/1	20	Dynamic
0008.a17b.ba3d	switchport0/1	20	Dynamic
000c.f1c3.85a9	switchport0/1	20	Dynamic
ALU#			

L2 SWITCHING CLEAR COMMANDS

TO CLEAR THE MAC-ADDRESS-TABLE

Command (in CM)	Description
<code>clear mac-address-table Dynamic [slot <slot-number> vlan <1-4094>]</code>	This command clears the mac-address-table learnt by the system.

EXAMPLE

```
ALU # clear mac-address-table Dynamic
```

SWITCHING CONFIGURATION USING OA-700

When no VLANs are configured on the L2 ports, all ports of the switch belong to one broadcast domain. All the L2 ports participate in pure bridging.

OA-700 AS A SWITCH WITH NO VLANs

The topology consists of the following components:

- 1 OA-700
- 6 PCs/Laptops

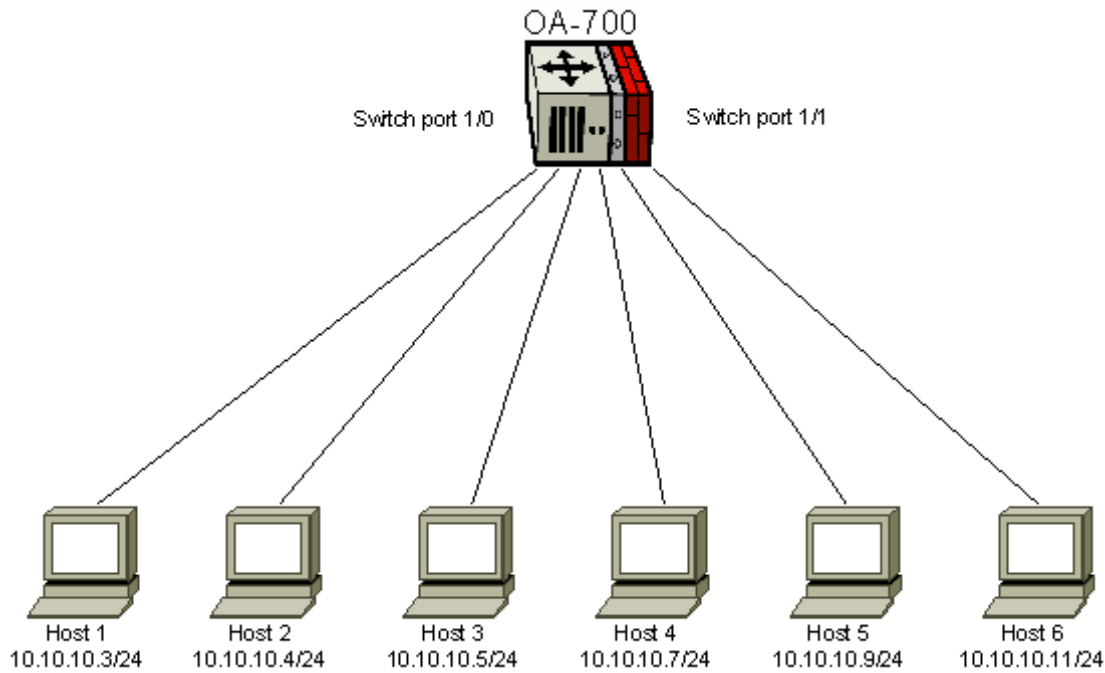


Figure 9: Switching with no VLANs

PROCEDURE

By default, all Switch ports will be in bridged mode. They belong to 1 broadcast domain.

```
ALU(config)# interface switchport1/0  
ALU(config-if switchport1/0)#
```

```
ALU(config-if switchport1/0)# no shutdown
```

To check for reachability between hosts, verify with ping from, say Host 1 to Host 5.

OA-700 AS A SWITCH WITH VLANS

TOPOLOGY

The topology consists of the following components:

- 1 OA-700
- 6 PC/Laptops
- 3 VLANs configured

L2 ports can be configured for 3 Modes of operation: Access, Trunk, Hybrid

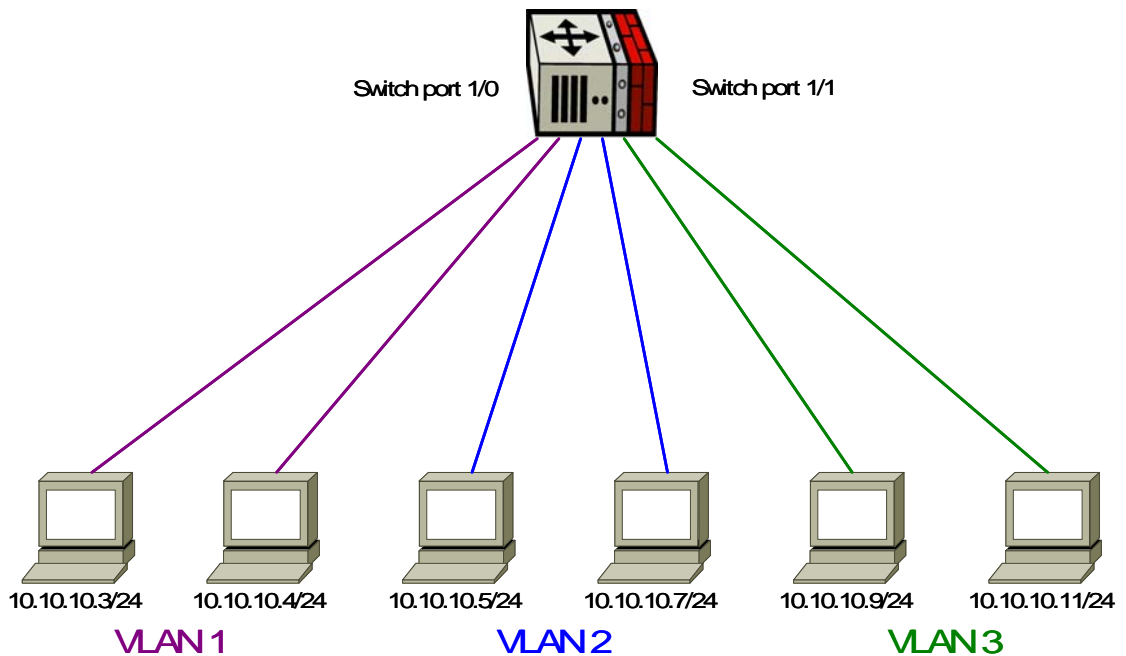


Figure 10: Switching with VLAN

PROCEDURE

3 VLANs - VLAN1, VLAN2, VLAN3 are configured.

VLAN 1 is configured with ports S0/2 and S0/3. VLAN2 is configured with ports S0/4 and S0/5 and VLAN3 is configured with ports S0/6 and S0/7.

Hence, hosts 1 and 2 belong to VLAN1, hosts 3 and 4 belong to VLAN2, and hosts 5 and 6 belong to VLAN3.

To CONFIGURE ACCESS VLAN

```
ALU(config-if switchport1/0)# switchport access vlan 10
ALU(config-if switchport1/0)#
```

To DELETE ACCESS VLAN CONFIGURED

```
ALU(config-if switchport1/0)# no switchport access vlan
```

To CONFIGURE TRUNK VLAN

```
ALU(config-if switchport1/0)# switchport trunk allowed
vlan 3
ALU(config-if switchport1/0)#

ALU(config-if switchport1/0)# switchport trunk allowed vlan
5
ALU(config-if switchport1/0)#

ALU(config-if switchport1/0)# switchport mode trunk
```

To DELETE TRUNK VLAN CONFIGURED

```
ALU(config-if switchport1/0)# no switchport mode
```

To CONFIGURE HYBRID VLAN

```
ALU(config-if switchport1/0)# switchport hybrid native vlan
7
ALU(config-if switchport1/0)#

ALU(config-if switchport1/0)# switchport mode hybrid
```

To DELETE HYBRID VLAN CONFIGURED

```
ALU(config-if switchport1/0)# no switchport mode
```

VLAN SHOW COMMAND

```
ALU(config)# show vlan id 10
```

SHOWS PORTS PARTICIPATING IN VLAN1

```
ALU(config)# show vlan id 1
```

Shows interface statistics along with its VLAN information (if VLAN configured on that interface).

Each VLAN is a separate broadcast domain. There is reachability between hosts within same VLAN. This can be verified with ping from, say host 1 to host 2. However, ping from host 1 to host 5 would fail.

CHAPTER 7 PER VLAN SPANNING TREE +

This chapter documents the commands for bridging configuration. These commands are used to configure the Per VLAN Spanning Tree Protocol Plus (PVST+). For a more detailed information on the parameter descriptions and their corresponding default values, refer to the *OmniAccess 700 CLI Command Reference Guide*.

This chapter includes the configuration steps, CLI syntax with its description and configuration examples. The commands are described in sequential order of configuration.

This chapter is divided into the following sections:

- [“Per VLAN Spanning Tree \(PVST+\) Overview”](#)
- [“PVST+ Configuration”](#)
- [“PVST+ Configuration Examples”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#

PER VLAN SPANNING TREE (PVST+) OVERVIEW

Spanning-Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

Multiple active paths between stations cause loops in the network. If a loop exists in the network topology, the potential exists for duplication of messages. When loops occur, some switches see stations appear on both sides of the switch. This condition confuses the forwarding algorithm, and allows duplicate frames to be forwarded.

To provide path redundancy, Spanning-Tree Protocol defines a tree that spans all switches in an extended network. Spanning-Tree Protocol forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path. Spanning-Tree Protocol operation is transparent to end stations, which are unaware whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Per-VLAN Spanning Tree + (PVST+) maintains a spanning tree instance for each VLAN configured in the network. Since PVST + treats each VLAN as a separate network, it has the ability to load balance traffic (at layer-2) by forwarding some VLANs on one trunk and other V lans on another trunk without causing a Spanning Tree loop.

PVST+ CONFIGURATION

Refer to the following sections to configure PVST+ on your system:

- [“PVST+ Configuration Steps”](#)
- [“PVST+ Configuration Flow”](#)
- [“PVST+ Configuration Commands”](#)

PVST+ CONFIGURATION STEPS

This section lists step by step instructions to be followed while configuring the PVST+.

Step 1: Enter Configuration Mode.

```
ALU# configure terminal
ALU(config)#
```

Step 2: Enable PVST+. See [“To Enable PVST+”](#)

Step 3: To configure Forward-time / Hello-time / Max-age / Priority for PVST+. See [“To Set Forward-time / Hello-time / Max-age / Priority for PVST+”](#) **(Optional)**

Step 4: Configure L2 interface.

```
ALU(config)# interface switchport <slot/port>
ALU(config-if switchport<slot/port>)#
```

Example:

```
ALU(config)# interface switchport 1/0
ALU(config-if switchport1/0)#
```

Configure PVST+ Optional parameters on a L2 interface:

- To disable/enable PVST+ on an L2 interface. See [“To Disable/Enable PVST+ on an Interface”](#)
- Set the PVST+ cost. See [“To Calculate the PVST+ Cost”](#)
- Set the Port-priority. See [“To Set PVST+ Port Priority”](#)

Step 5: Use the show commands to recheck and view the details configured. See [“Show Commands in PVST+”](#)

PVST+ CONFIGURATION FLOW

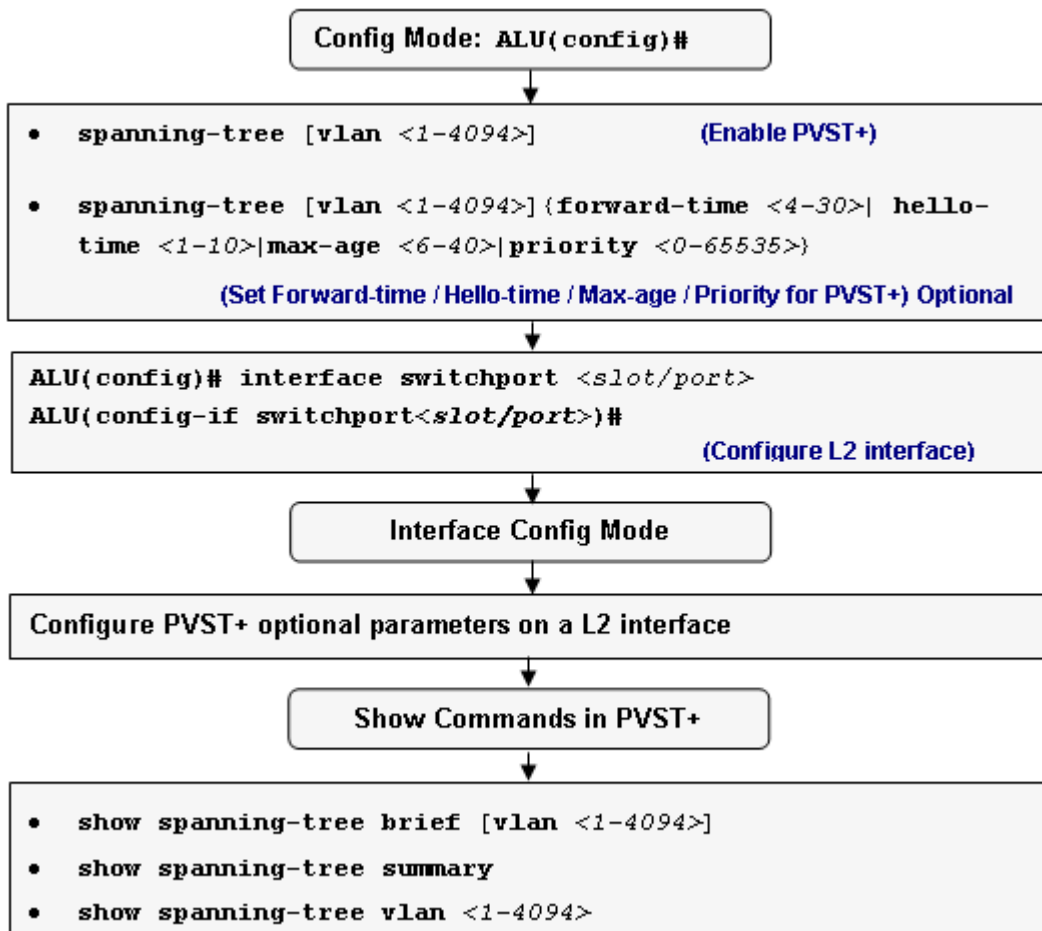


Figure 11: PVST+ Configuration Flow

PVST+ CONFIGURATION COMMANDS

This section details on the commands, which are used to configure Spanning Tree Protocol.

To ENABLE PVST+



Note: Each “spanning tree” command will be based on some VLAN. If the VLAN-ID is not entered, by default it is taken as VLAN-1.

Command (in CM)	Description
<code>spanning-tree [vlan <1-4094>]</code>	This command is entered in the configuration mode. This command enables a spanning-tree for VLAN.
<code>no spanning-tree [vlan <1-4094>]</code>	The “no” command disables the configured spanning-tree for a VLAN.

EXAMPLE

The following command enables the spanning tree for the **default VLAN-id, i.e., VLAN-1:**

```
ALU(config)# spanning-tree
```

The deletion of the spanning tree will follow the same rule.

```
ALU(config)# no spanning-tree
```

The following example configures spanning tree for VLAN 100:

```
ALU(config)# spanning-tree vlan 100
```

The deletion of the spanning tree will follow the same rule.

```
ALU(config)# no spanning-tree vlan 100
```

To SET FORWARD-TIME / HELLO-TIME / MAX-AGE / PRIORITY FOR PVST+

Command (in CM)	Description
<code>spanning-tree [vlan <1-4094>] {forward-time <4-30> hello-time <1-10> max-age <6-40> priority <0-65535>}</code>	This command is entered in the configuration mode to configure a PVST+ Forward-time/Hello-time/Maximum-age/Bridge priority.
<code>no spanning-tree [vlan <1-4094>] {forward-time <4-30> hello-time <1-10> max-age <6-40> priority <0-65535>}</code>	The "no" command resets the PVST+ Forward-time/Hello-time/Maximum-age/Bridge priority to its default. The default for each of the parameter is given below: <ul style="list-style-type: none"> • Forward time: 15 seconds • Hello-time: 2 seconds • Max-age: 20 seconds • Priority: 32768



Note: - If you do not enter a VLAN-ID, by default it is taken as VLAN-1.

- The following formula has to be satisfied when configuring the forward-time, hello-time and max-age:

$$(\text{forward-time} - 1) * 2 \geq \text{max-age} \ \&\& \\ \text{max-age} \geq ((\text{hello-time} + 1) * 2)$$
EXAMPLE

The following examples configures the PVST+ Forward-time to 30, Hello-time to 10 and Maximum-age to 40:

```
ALU(config)# spanning-tree vlan 100 forward-time 30
ALU(config)# spanning-tree vlan 100 hello-time 10
ALU(config)# spanning-tree vlan 100 max-age 40
```

The following command resets the PVST+ Forward-time/Hello-time/Maximum-age/Bridge priority to its default:

```
ALU(config)# no spanning-tree vlan 100 forward-time
ALU(config)# no spanning-tree vlan 100 hello-time
ALU(config)# no spanning-tree vlan 100 max-age
```

To DISABLE/ENABLE PVST+ ON AN INTERFACE

Command (in ICM)	Description
<code>spanning-tree [vlan <1-4094>] spanning-disabled</code>	This command is entered in the interface configuration mode. This disables the Spanning-tree on a specific interface.
<code>no spanning-tree [vlan <1-4094>] spanning-disabled</code>	The “no” command enables the Spanning-tree on a specific interface.

EXAMPLE

```
ALU(config-if switchport1/0)# spanning-tree vlan 100 spanning-disabled
```

```
ALU(config-if switchport1/0)# no spanning-tree vlan 100 spanning-disabled
```

To CALCULATE THE PVST+ COST

Command (in ICM)	Description
<code>spanning-tree [vlan <1-4094>] cost <1-65535></code>	This command is entered in the interface configuration mode. This command calculates the path cost of PVST+ on a specific interface.
<code>no spanning-tree [vlan <1-4094>] cost <1-65535></code>	The “no” command resets the PVST+ cost to its default value. The default PVST+ cost is 4.



- Note:**
- When two bridges compete for position as the root bridge, configure the PVST cost to prioritize an interface.
 - The PVST+ cost is configured on a per port basis.

EXAMPLE

```
ALU(config-if switchport1/0)# spanning-tree vlan 100 cost 1000
```

```
ALU(config-if switchport1/0)# no spanning-tree vlan 100 cost
```

To SET PVST+ PORT PRIORITY

Command (in ICM)	Description
<code>spanning-tree [vlan <1-4094>] port-priority <0-255></code>	This command is entered in the Interface Mode. This command is used to prioritize a specific interface.
<code>no spanning-tree [vlan <1-4094>] port-priority <0-255></code>	The “no” command resets the PVST+ port-priority to its default value. The default PVST+ port-priority is 128.



- Note:**
- When two bridges compete for position as the root bridge, port-priority command is used to prioritize an interface.
 - PVST+ Port Priority is configured on a per port basis.

EXAMPLE

```
ALU(config-if switchport1/0)# spanning-tree vlan 100 port-
priority 250
```

```
ALU(config-if switchport1/0)# no spanning-tree vlan 100 port-
priority
```

SHOW COMMANDS IN PVST+

TO VIEW A BRIEF CONFIGURATION OF PVST+

Command (in SUM/CM)	Description
<code>show spanning-tree brief [vlan <1-4094>]</code>	This command displays the spanning tree configuration details in brief.

EXAMPLE 1

```
ALU# show spanning-tree brief vlan 1
```

```
VLAN1
Spanning tree enabled protocol IEEE
ROOT ID      Priority 32768
              Address 00.07.50.0c.a1.00
              Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority 32768   Address 00.11.8b.00.27.12
Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec

Port
Name          Port ID Prio Cost   Designated
              sts Cost Bridge ID   Port ID
-----
switchport0/0 128.8  128   4   FWD 0 00.07.50.0c.a1.00 128.13
switchport0/1 128.7  128   4   DIS 0 00.11.8b.00.27.12 128.7
switchport0/2 128.6  128   4   DIS 0 00.11.8b.00.27.12 128.6
switchport0/3 128.5  128   4   DIS 0 00.11.8b.00.27.12 128.5
switchport0/4 128.4  128   4   DIS 0 00.11.8b.00.27.12 128.4
switchport0/5 128.3  128   4   DIS 0 00.11.8b.00.27.12 128.3
switchport0/6 128.2  128   4   DIS 0 00.11.8b.00.27.12 128.2
switchport0/7 128.1  128   4   DIS 0 00.11.8b.00.27.12 128.1
```

EXAMPLE 2

```
ALU(config)# show spanning-tree brief vlan 1
```

```
VLAN1
Spanning tree enabled protocol IEEE
ROOT ID Priority 32768
    Address 00.11.8b.00.27.12
    This bridge is the root
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768
    Address 00.11.8b.00.27.12
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Port
Name          Port ID Prio Cost  Sts  Designated
-----
switchport1/0 128.8 128 4  FWD  0    00.11.8b.00.27.12 128.8
switchport1/1 128.7 128 4  FWD  0    00.11.8b.00.27.12 128.7
switchport1/2 128.6 128 4  FWD  0    00.11.8b.00.27.12 128.6
switchport1/3 128.5 128 4  FWD  0    00.11.8b.00.27.12 128.5
switchport1/4 128.4 128 4  FWD  0    00.11.8b.00.27.12 128.4
switchport1/5 128.3 128 4  FWD  0    00.11.8b.00.27.12 128.3
switchport1/6 128.2 128 4  DIS  0    00.11.8b.00.27.12 128.2
switchport1/7 128.1 128 4  DIS  0    00.11.8b.00.27.12 128.1
```

To VIEW SUMMARIZED PVST+ DETAILS

Command (in SUM/CM)	Description
<code>show spanning-tree summary</code>	This command displays the summary of the spanning tree information.

EXAMPLE 1

```
ALU# show spanning-tree summary
```

```
Name          Blocking Listening Learning Forwarding  STP Active
-----
VLAN1          7           0           0           1           8
VLAN2          0           0           0           1           1
VLAN3          0           0           0           1           1
-----
3 VLANs        7           0           0           3           10
```

```
ALU#
```

EXAMPLE 2

```
ALU(config)# show spanning-tree summary
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN1	2	0	0	6	8
1 VLANs	2	0	0	6	8

TO VIEW THE PVST+ DETAILS ON A VLAN

Command (in SUM/CM)	Description
<code>show spanning-tree vlan <1-4094></code>	This command displays the VLAN based spanning tree information.

EXAMPLE 1

```
ALU# show spanning-tree vlan 2
```

```
Spanning tree 2 is executing the IEEE compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, address 00.11.8b.00.27.21
Configured hello time 2, max age 20,forward delay 15
Current root has priority 2, address 00.07.50.0c.a1.03
Root port is 128.8 cost of root path is 4
Topology change flag not set, detected flag not set
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0
Interface switchport0/0 (port 8) in Spanning tree 2 is Forwarding
Port path cost 4, Port priority 128
Designated root has priority 2, address 00.07.50.0c.a1.03
Designated bridge has priority 2, address 00.07.50.0c.a1.03
Designated port Id is 128.13 path cost 4
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 0, received 535
```

EXAMPLE 2

```
ALU(config)# show spanning-tree vlan 1
```

```
Spanning tree 1 is executing the IEEE compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, address 00.11.8b.00.27.12
Configured hello time 2, max age 20,forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 1, topology change 0, notification 0
Interface switchport1/0 (port 8) in Spanning tree 1 is Forwarding
Port path cost 4, Port priority 128
Designated root has priority 32768, address 00.11.8b.00.27.12
Designated bridge has priority 32768, address 00.11.8b.00.27.12
Designated port Id is 128.8 path cost 0
Timers: message age 0, forward delay 0, hold 0
```

```
BPDU: sent 120, received 0
Interface switchport1/1 (port 7) in Spanning tree 1 is Forwarding
  Port path cost 4, Port priority 128
  Designated root has priority 32768, address 00.11.8b.00.27.12
  Designated bridge has priority 32768, address 00.11.8b.00.27.12
  Designated port Id is 128.7 path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 120, received 0
Interface switchport1/2 (port 6) in Spanning tree 1 is Forwarding
  Port path cost 4, Port priority 128
  Designated root has priority 32768, address 00.11.8b.00.27.12
  Designated bridge has priority 32768, address 00.11.8b.00.27.12
  Designated port Id is 128.6 path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 120, received 0
Interface switchport1/3 (port 5) in Spanning tree 1 is Forwarding
  Port path cost 4, Port priority 128
  Designated root has priority 32768, address 00.11.8b.00.27.12
  Designated bridge has priority 32768, address 00.11.8b.00.27.12
  Designated port Id is 128.5 path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 120, received 0
Interface switchport1/4 (port 4) in Spanning tree 1 is Forwarding
  Port path cost 4, Port priority 128
  Designated root has priority 32768, address 00.11.8b.00.27.12
  Designated bridge has priority 32768, address 00.11.8b.00.27.12
  Designated port Id is 128.4 path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 120, received 0
Interface switchport1/5 (port 3) in Spanning tree 1 is Forwarding
  Port path cost 4, Port priority 128
  Designated root has priority 32768, address 00.11.8b.00.27.12
  Designated bridge has priority 32768, address 00.11.8b.00.27.12
  Designated port Id is 128.3 path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 120, received 0
Interface switchport1/6 (port 2) in Spanning tree 1 is Disabled
  Port path cost 4, Port priority 128
  Designated root has priority 32768, address 00.11.8b.00.27.12
  Designated bridge has priority 32768, address 00.11.8b.00.27.12
  Designated port Id is 128.2 path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 0, received 0
Interface switchport1/7 (port 1) in Spanning tree 1 is Disabled
  Port path cost 4, Port priority 128
  Designated root has priority 32768, address 00.11.8b.00.27.12
  Designated bridge has priority 32768, address 00.11.8b.00.27.12
  Designated port Id is 128.1 path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 0, received 0
```


PVST+ CONFIGURATION EXAMPLES

EXAMPLE 1

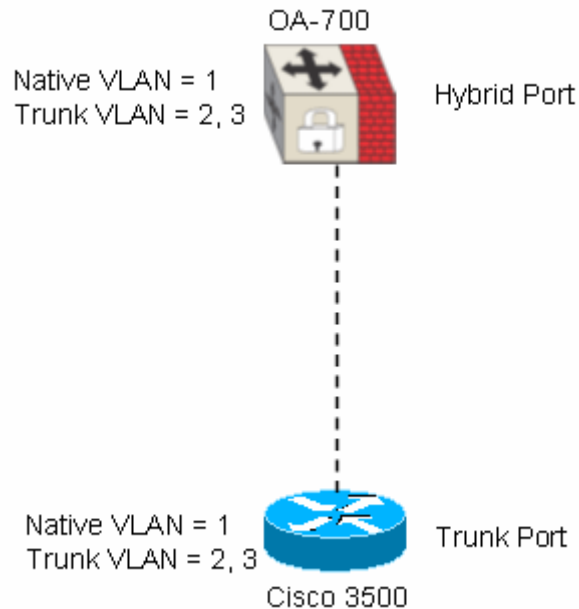


Figure 12: PVST+ Topology

FOR SPANNING TREE

Spanning Tree for vlan 1: Cisco is Root
 Spanning Tree for vlan 2: Cisco is Root
 Spanning Tree for vlan 3: OA-700 is Root

ALCATEL-LUCENT CONFIGURATION

```
PVST Global configuration
spanning-tree
spanning-tree vlan 2
spanning-tree vlan 3
spanning-tree vlan 3 priority 3

interface switchport0/0
switchport mode hybrid
switchport trunk allowed vlan 2 3
no shutdown

interface switchport0/1
shutdown

interface switchport0/2
shutdown
```

```
interface switchport0/3
shutdown

interface switchport0/4
shutdown

interface switchport0/5
shutdown

interface switchport0/6
shutdown

interface switchport0/7
shutdown

interface GigabitEthernet7/0
shutdown

interface GigabitEthernet7/1
shutdown
```

CISCO CONFIGURATION

```
hostname Switch

spanning-tree vlan 2 priority 2
ip subnet-zero

interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk

interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
```

```

interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface VLAN1
  no ip address
  no ip directed-broadcast
  no ip route-cache
  shutdown

switch#

```

EXAMPLE 2

Configure PVST+ on the OA-700: Spanning Tree provides a mechanism for loop detection and guarantees only one path exists between two end stations. Spanning Tree is not turned on by default on L2-GE.

When no VLANs are configured on the L2-ports, all ports of the switch belong to one broadcast domain. All the L2 ports will participate in pure bridging if they are not configured for access or trunk or hybrid.

TOPOLOGY

The topology consists of the following components:

- 1 OA-700
- 6 PCs/Laptops

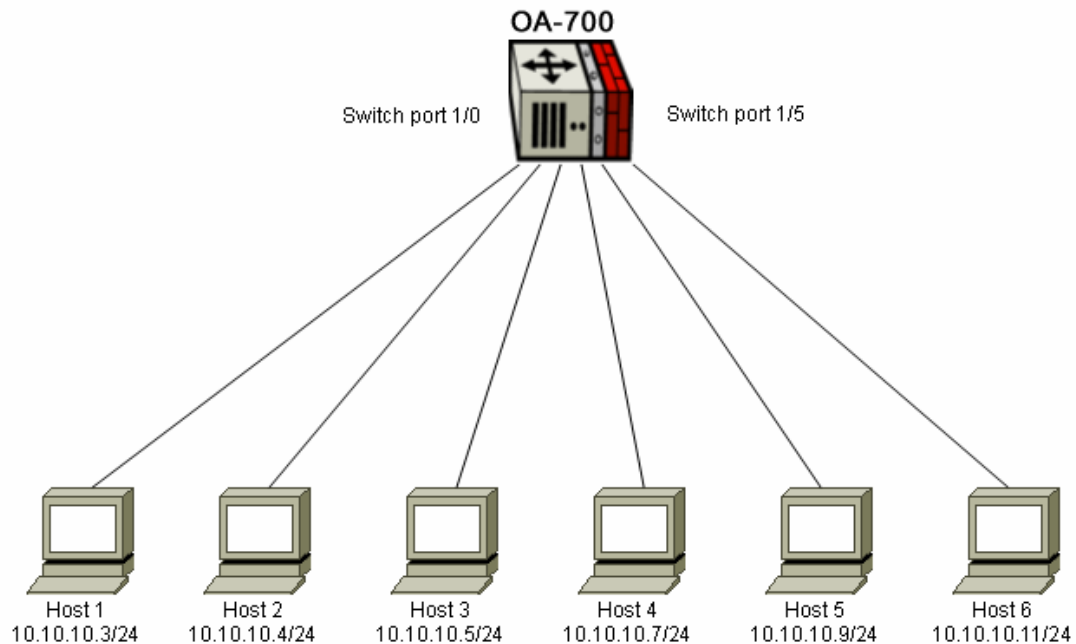


Figure 13: PVST+ Topology on OA-700

PROCEDURE

By default, all switchports will be in bridged mode. They belong to 1 broadcast domain. Spanning tree can be enabled (recommended) by using the following commands:

```
ALU(config)#interface switchport 1/0
ALU(config-if switchport1/0)#no shutdown

ALU(config-if switchport1/0)#interface switchport 1/1
ALU(config-if switchport1/1)#no shutdown

ALU(config-if switchport1/1)#interface switchport 1/2
ALU(config-if switchport1/2)#no shutdown

ALU(config-if switchport1/2)#interface switchport 1/3
ALU(config-if switchport1/3)#no shutdown

ALU(config-if switchport1/3)#interface switchport 1/4
ALU(config-if switchport1/4)#no shutdown

ALU(config-if switchport1/4)#interface switchport 1/5
ALU(config-if switchport1/5)#no shutdown

ALU(config)# spanning-tree
ALU(config-if switchport1/2)#interface switchport 1/0
ALU(config-if switchport1/0)#spanning-tree cost 1000
```

CHECK THE CONFIGURATION WITH THE SHOW COMMAND

```

ALU(config)# show spanning-tree brief vlan 1
VLAN1
Spanning tree enabled protocol IEEE
ROOT ID Priority 32768
      Address 00.11.8b.00.27.12

      This bridge is the root
      Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
      Bridge ID Priority 32768

      Address 00.11.8b.00.27.12
      Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
      Port                               Designated
      Name                               Port ID Prio Cost Sts Cost Bridge ID
      Port ID
-----
switchport1/0 128.8 128 4 FWD 0 00.11.8b.00.27.12 128.8
switchport1/1 128.7 128 4 FWD 0 00.11.8b.00.27.12 128.7
switchport1/2 128.6 128 4 FWD 0 00.11.8b.00.27.12 128.6
switchport1/3 128.5 128 4 FWD 0 00.11.8b.00.27.12 128.5
switchport1/4 128.4 128 4 FWD 0 00.11.8b.00.27.12 128.4
switchport1/5 128.3 128 4 FWD 0 00.11.8b.00.27.12 128.3
switchport1/6 128.2 128 4 DIS 0 00.11.8b.00.27.12 128.2
switchport1/7 128.1 128 4 DIS 0 00.11.8b.00.27.12 128.1

```

CHECK FOR REACHABILITY BETWEEN HOSTS

This can be verified with ping from, say Host 1 to Host 5.

CHAPTER 8 INTEGRATED ROUTING AND BRIDGING

This chapter covers the commands used to configure Integrated Routing and Bridging (IRB) on the OA-700.

The “[Integrated Routing and Bridging Overview](#)” section serves as a comprehensive study on the IRB information. “[IRB Configuration](#)” details the command used to configure IRB on the OA-700. The last section “[IRB Configuration using OA-700](#)” provides a real-time scenario for configuring IRB on the OA-700.

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#

INTEGRATED ROUTING AND BRIDGING OVERVIEW

When there is a requirement to bridge local traffic within several segments while having hosts on the bridged segments, to reach the hosts or routers on routed networks, IRB is configured on the system.

Using this feature, local or unroutable traffic is bridged among bridge interfaces and routable traffic is routed to other routed interfaces.

IRB allows the user to both route and bridge a protocol in the same router with connectivity between all the interfaces.

ALCATEL-LUCENT SPECIFIC IRB OVERVIEW

The L2-GE card on the OA-700 system is a VLAN-aware Ethernet switch. However, for routing across VLANs or between traffic on the L2-GE card and other cards such as the T1 or an E1 card, there has to be a mechanism to detect traffic that is to be routed, and subject it to normal IP packet processing activities such as filters, NAT, IPsec, FIB lookup, etc. Hence a L2-GE port will then be capable of taking part in both bridging and routing at the same time. This technology is called IRB on the OA-700.

If the physical ports belonging to a VLAN are thought of as defining a logical bridge/switch, then the mechanism of sending an incoming packet from this bridge to the logical router inside the OA-700 is to connect the bridge and the router by a logical VLAN interface. This interface forms a logical pipe between the bridge and the router inside the system. So, the router inside sees the packet as coming in on a VLAN interface, which behaves like other interfaces such as Ethernet, Serial, etc., from the point of view of IP services.

Once the packet has undergone the ingress policies configured on the VLAN interfaces, as well as a FIB lookup, an egress interface is found and the packet is acted on by the policies configured on this egress interface. If it turns out that the egress interface is a physical interface such as Ethernet or T1 or an E1 or even a sub-interface on a physical interface (e.g., a Frame Relay sub-interface), then everything proceeds as usual. If the egress interface is a logical VLAN interface, then it will be sent out of the appropriate physical interface port(s) that belong to the VLAN.

IRB CONFIGURATION

The following section details the configuration steps and commands to configure IRB on the OA-700.

IRB CONFIGURATION STEPS

Step 1: Configure the VLAN interface. This could also be for VLAN 1. See [“To Configure VLAN Interface”](#)

Step 2: Attach the VLAN to one or more switchports (through the CLI commands for access, trunk and hybrid ports).

(Refer chapter on switching [“Layer 2 Switching Configuration”](#) for a detailed insight on the VLAN commands)

Step 3: Configure IP address, and attach policies such as Filter, IDS, etc., on the VLAN interface (through known CLI commands for other services).



-
- Note:**
- A given VLAN interface for IRB can be used only on the 8 ports of the same L2-GE card.
 - The IRB VLANs cannot be configured on the Service Engine ports.
-

IRB COMMANDS

To CONFIGURE VLAN INTERFACE

Command (in CM)	Description
<code>interface vlan <1-4094></code>	This command is used to configure a VLAN interface.

EXAMPLE

```
ALU(config)# interface vlan 10
ALU(config-if Vlan 10)#
```

To VIEW VLAN STATISTICS

Command (in CM)	Description
<code>show interfaces vlan <1-4094></code>	This command displays the VLAN statistics of the VLAN-ID specified on the interface.

EXAMPLE

```
ALU(config)# show interfaces vlan 10

vlan10 is up
Hardware is none, address is 0011.8b00.0e28 (0011.8b00.0e28)
Internet address is 10.91.0.1/24
MTU 1500 bytes, BW 0 Kbit, DLY 0 usec, reliability 0/255, txload 0/255,
rxload 0/255
loopback not set,  Keepalive not set
Auto-duplex, Auto, 1000BaseTx/Fx
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/0(size/max),0 drops;Input queue 0/0 (size/max), 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
2034961 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors,0 CRC, 0 frame,0 overrun,1580 ignored
0 watchdog, 0 multicast, 0 pause input
2035879 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
```

IRB CONFIGURATION USING OA-700

TOPOLOGY FOR IRB CONFIGURATION ON OA-700

The topology consists of the following components:

- 1 OA-700
- A Serial Connector
- 6 PCs/Laptops

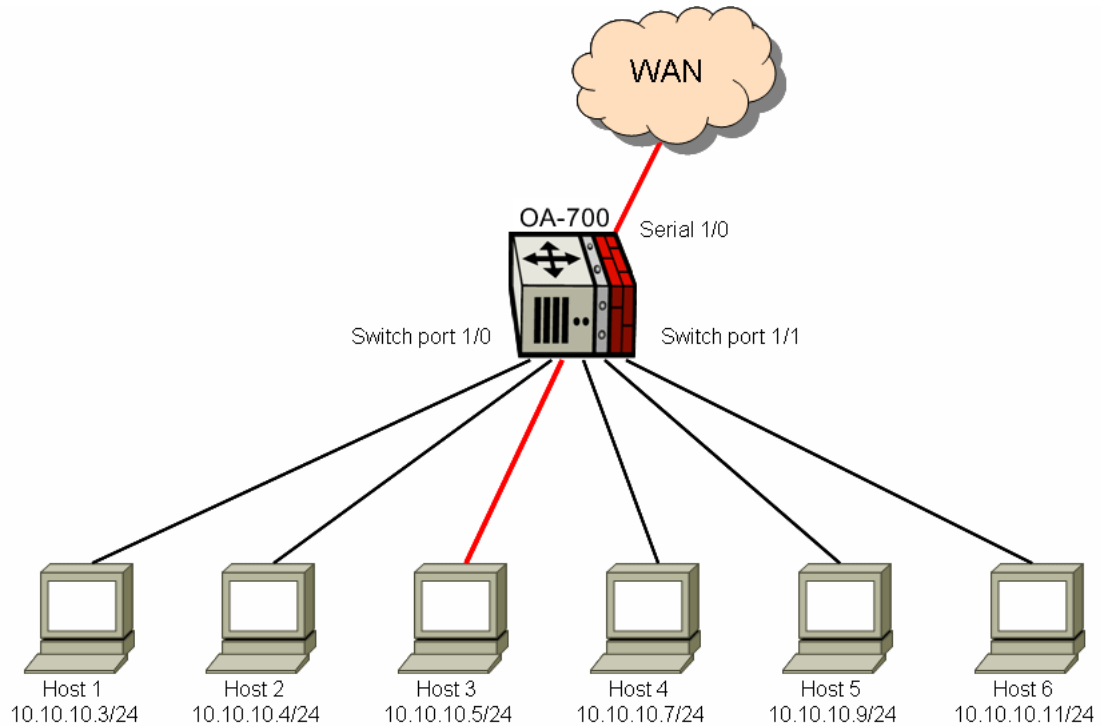


Figure 14: IRB Topology

PROCEDURE

By default, all switchports will be in bridge mode. They belong to one broadcast domain.

CONFIGURE BRIDGING

```
ALU(config)# interface switchport1/0
ALU(config-if-switchport1/0)#
ALU(config-if-switchport1/0)# no shutdown
ALU(config-if-switchport1/0)# switchport access vlan 100
```

CONFIGURE A VIRTUAL INTERFACE

```
ALU(config)# interface vlan 100
ALU(config-if Vlan 100)# no shutdown
ALU(config-if Vlan 100)# ip address 10.10.10.20/24
```

CHECK FOR REACHABILITY BETWEEN HOSTS

Verify by pinging from 10.10.10.5 to 10.10.10.20, and also ping to check for WAN connectivity. For ex: ping from 10.10.10.5 to any HTTP address.

CHAPTER 9 802.1X PORT-BASED AUTHENTICATION

This chapter describes how to configure IEEE 802.1X port-based authentication on the OA-700. This chapter includes the configuration steps, CLI syntax with its description and configuration examples. The commands are described in sequential order of configuration.

For a more detailed information on the parameter descriptions and their corresponding default values, refer to the *OmniAccess 700 CLI Command Reference Guide*.

This chapter is divided into the following sections:

- [“802.1X Overview”](#)
- [“802.1X Configuration”](#)
- [“802.1X Configuration Example”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode -ALU#
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#

802.1X OVERVIEW

The IEEE 802.1X standard, Port Based Network Access Control, defines a mechanism for port-based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructure. It provides a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics. It also prevents access to that port when the authentication and authorization fails.

The following diagram shows the deployment scenario of 802.1X. This diagram shows the supplicant, authenticator, and authentication server in a 802.1X network. The 802.1X requires one authenticator port. In the diagram, controlled port and uncontrolled port are the logical port in Authenticator System. The controlled port shown here is not authorized and therefore it is not allowing traffic. The uncontrolled port in Authenticator system is basically used for sending/receiving 802.1x control frame. Once authentication is successful, then the controlled port will be open to access the service offered by authenticator.

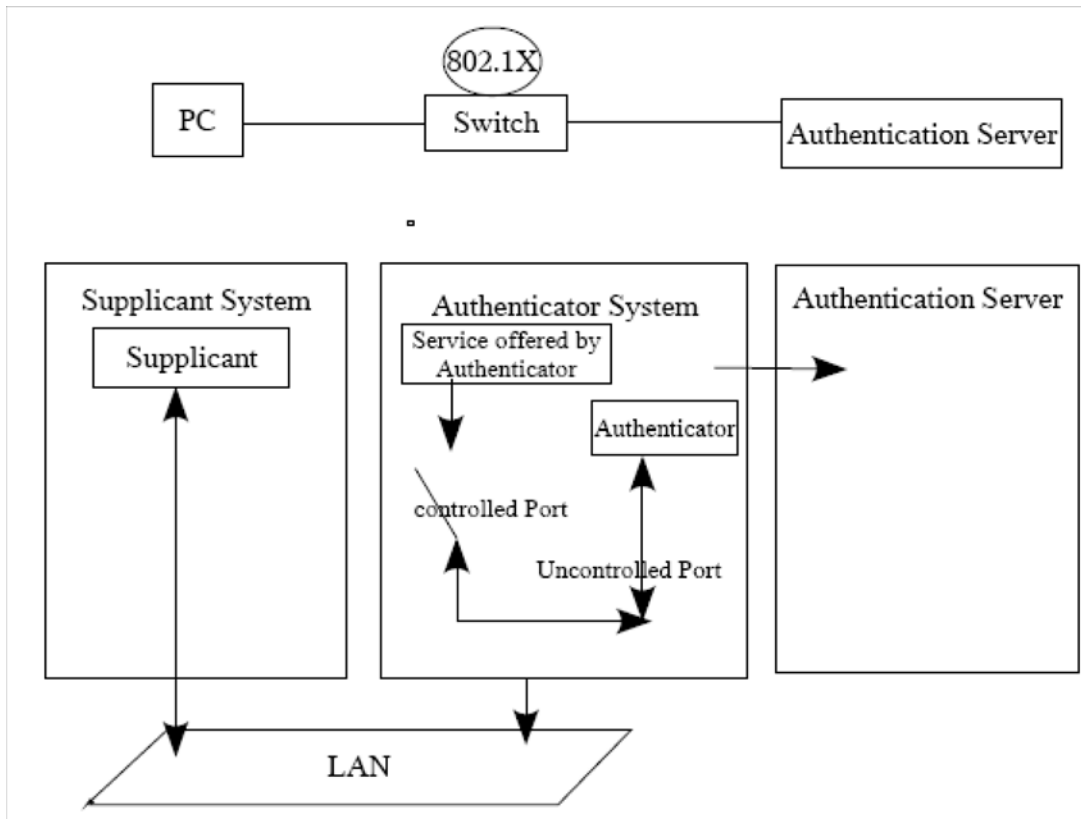


Figure 15: 802.1X Deployment Scenario

GENERIC TERMS USED IN 802.1X

Supplicant

An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of the link. The supplicant is sometimes called as 802.1X client.

Authenticator

An Entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.

Authentication Server

An entity that provides an authentication service to an authenticator. This service determines from the credentials provided by the supplicant whether the supplicant is authorized to access the services provided by the OA-700 in which the Authenticator resides. The example of the authentication servers: RADIUS server, TACACS Server, etc.

EAPOL

The protocol in 802.1X is called EAP encapsulation over LANs (EAPOL). 802.1X is a standard for passing EAP over a wired LAN. It packages EAP messages in Ethernet frames.

The following is the communications among Supplicant, Authenticator, and Authentication Server.

- The authenticator sends an "EAP-Request/Identity" packet to the supplicant as soon as it detects that the link is active.
- The supplicant sends an "EAP-Response/Identity" packet to the authenticator, which is then passed on to the authentication (RADIUS) server.
- The authentication server sends back a challenge to the authenticator, such as with a token password system. The authenticator unpacks this from RADIUS packet and repackages it into EAPOL and sends it back to the supplicant. Different authentication methods will vary this message and the total number of messages.
- The supplicant responds to the challenge via the authenticator and passes the response onto the authentication server.
- If the supplicant provides proper identity, the authentication server responds with a success message, which is then passed onto the supplicant. The authenticator now allows access to the LAN.

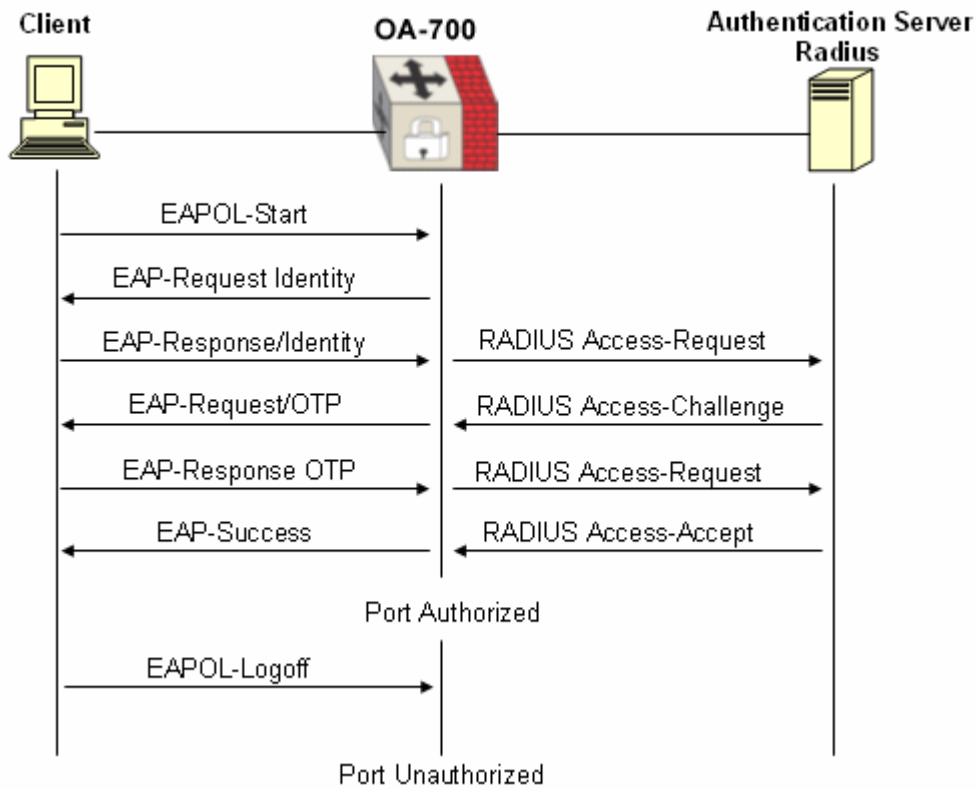


Figure 16: Message Exchange

USING 802.1X WITH VLAN ASSIGNMENT

After successful 802.1X authentication of a port, the RADIUS server sends the VLAN assignment to configure the switchport. The RADIUS server database maintains the user name-to-VLAN mappings, which assigns the VLAN based on the user name of the client connected to the switch port.

When configured on the switch and the RADIUS server, 802.1X with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server, the port is configured in its access VLAN after successful authentication.
- If the VLAN information from the RADIUS server is not valid, the port remains in the configured access VLAN.
- Otherwise, if all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If the multiple-hosts mode is enabled on an 802.1X port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- If the multi-auth mode is enabled on a 802.1X port, the dynamic VLAN featured is disabled, i.e., VLAN information received from RADIUS server will not do any effect on the port.

To configure VLAN assignment, you need to perform these tasks:

- Enable AAA services.
- Enable 802.1X (the VLAN assignment feature is automatically enabled when you configure 802.1X on an access port).
- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch:
 - [64] Tunnel-Type = VLAN
 - [65] Tunnel-Medium-Type = IEEE-802
 - [81] Tunnel-Private-Group-ID = VLAN ID

Attribute [64] must contain the value VLAN (type 13).

Attribute [65] must contain the value 802 (type 6).

Attribute [81] specifies the VLAN name or VLAN ID assigned to the 802.1X-authenticated user.

ALCATEL-LUCENT SPECIFIC OVERVIEW

Alcatel-Lucent's Gigabit Ethernet line card (L2GE Card) is used for layer-2 functionality. 802.1X is a port based authentication protocol, which provides the access to the port. Before giving any access to the hosts, which are connected to L2GE Ports, needs to be authenticated on L2GE ports.

802.1X CONFIGURATION

Refer to the following sections to configure 802.1X on the OA-700:

- [“802.1X Configuration Steps”](#)
- [“802.1X Configuration Flow”](#)
- [“802.1X Configuration Commands”](#)

802.1X CONFIGURATION STEPS

This section lists step by step instructions to be followed while configuring the 802.1X.

Step 1: To enable 802.1X port-based authentication, you should **enable AAA services** and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to the authentication server to authenticate a user.

```
ALU(config)# aaa services
ALU(config)# aaa server-group radius <name>
ALU(config-rad-grp)# radius-server <ip-address> key
<string>
ALU(config-rad-grp)# exit
```

```
ALU(config)# aaa method-list <name> <methods>...
ALU(config)# aaa authentication dot1x <method-list-
name>
```

Example:

```
ALU(config)# aaa services
ALU(config)#aaa server-group radius rad1
ALU(config-rad1-grp)# radius-server 10.0.0.254 key
admin
ALU(config-rad1-grp)# exit
```

```
ALU(config)# aaa method-list m1 rad1
ALU(config)# aaa authentication dot1x m1
```

The above CLI commands are the minimum and mandatory steps to enable 802.1X port-based authentication.

For more details on AAA configuration commands, refer to the [“System Configuration and Monitoring”](#) chapter in this guide).

Step 2: Enter Configuration Mode.

```
ALU# configure terminal
ALU(config)#
```

Step 3: Enable 802.1X port-based authentication globally. See [“To Enable 802.1X Port-based Authentication Globally”](#)

Step 4: Configure L2 interface.

```
ALU(config)# interface switchport <slot/port>
ALU(config-if switchport<slot/port>)#
```

Example:

```
ALU(config)# interface switchport 5/0
ALU(config-if switchport5/0)#
```



Note: The L2 interface on which 802.1X configured should not be in 'Trunk/Hybrid' mode. And, also port monitoring should not be configured on the interface.

Step 5: Administratively bring up the interface.

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if switchport5/0)# no shutdown
```

Step 6: Enable 802.1X port-based authentication on the L2GE interface. See ["To Enable 802.1X Port-based Authentication on L2 Interface"](#)

Step 7: Configure 802.1X Optional parameters on a L2 interface. See ["Configure 802.1X Optional Parameters on a L2 interface"](#)

- Enable periodic reauthentication. See ["To Enable Periodic Reauthentication"](#)
- Configure time-out for periodic reauthentication. See ["To Configure Time-out for Periodic Reauthentication"](#)
- Configure time-out for quiet-period. See ["To Configure Time-out for Quiet Period"](#)
- Configure Switch-to-client Retransmission time. See ["To Configure Switch-to-client Retransmission Time"](#)
- Configure switch-to-client retransmission time for EAP-request frames. See ["To Configure Switch-to-client Retransmission Time for EAP-request Frames"](#)
- Configure switch-to-client frame retransmission number. See ["To Configure Switch-to-client Frame Retransmission Number"](#)

- Enable multiple hosts/multiple authentication. See [“To Enable Multiple Hosts”](#)
- Reset configurable 802.1X parameters to default Values. See [“To Reset Configurable 802.1X Parameters To Default Values”](#)
- Manually reauthenticate the client. See [“To Manually Reauthenticate the Client”](#)
- Initialize the authentication for the client. See [“To Initialize the Authentication for the Client”](#)

Step 8: Use the show commands to recheck and view the details configured. See [“802.1X Show Commands”](#)

802.1X CONFIGURATION FLOW

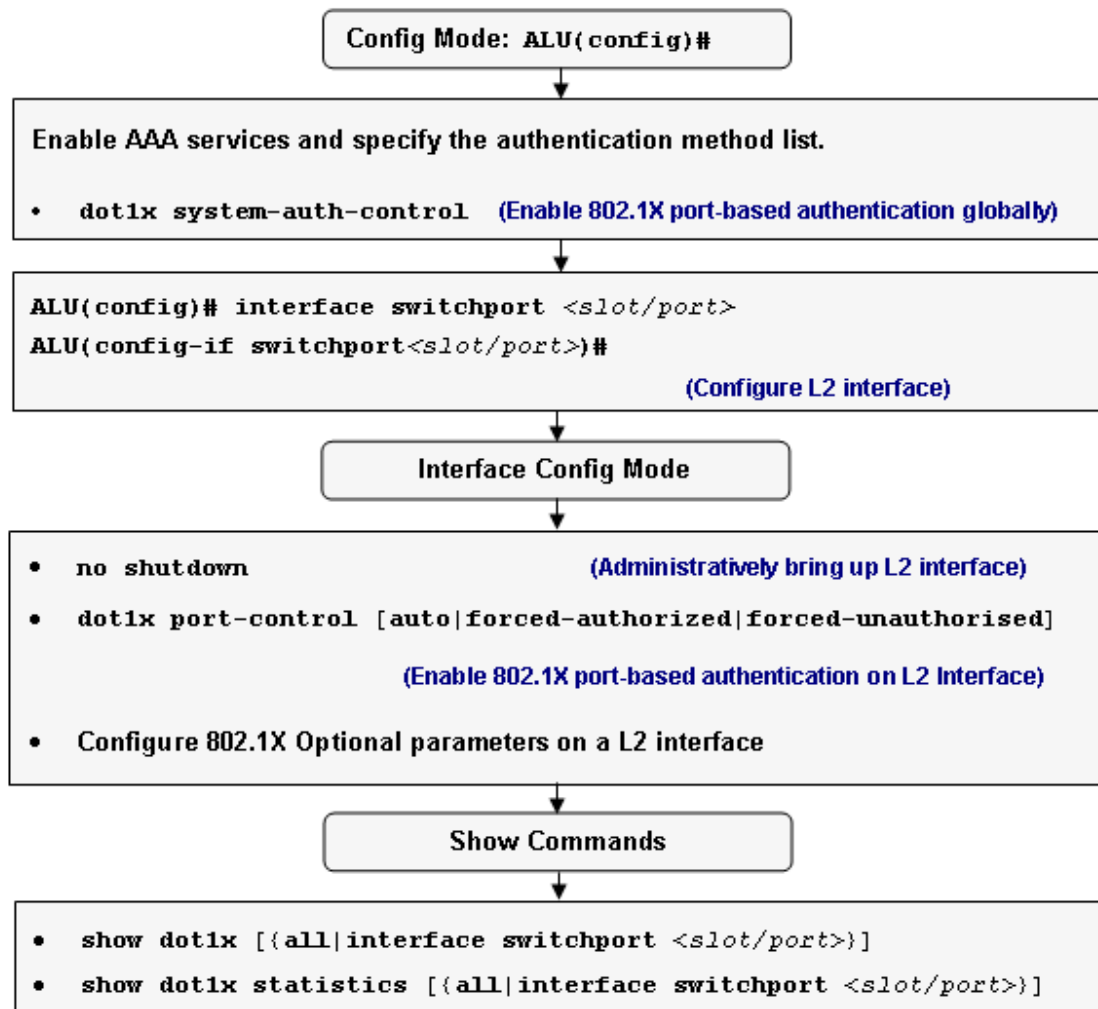


Figure 17: 802.1X Configuration Flow

802.1X CONFIGURATION COMMANDS

This section details on the commands, which are used to configure 802.1X.

To ENABLE 802.1X PORT-BASED AUTHENTICATION GLOBALLY

Command (in CM)	Description
<code>dot1x system-auth-control</code>	This command is entered in the configuration mode. This command is used to enable 802.1X port-based authentication globally. When enabled, the port-based authentication on the interface will be 'forced-authorized'.
<code>no dot1x system-auth-control</code>	This command is used to disable 802.1X port-based authentication globally.

EXAMPLE

```
ALU(config)# dot1x system-auth-control
ALU(config)# no dot1x system-auth-control
```

To ENABLE 802.1X PORT-BASED AUTHENTICATION ON L2 INTERFACE

Command (in ICM)	Description
<code>dot1x port-control</code> [auto forced-authorized forced-unauthorized]	This command is entered in the Interface Configuration Mode. This command is used to enable 802.1X port-based authentication on the L2 interface. Auto: Network access is granted only on authorization. Force-authorized: Network access is granted without authorization. Force-unauthorized: Port is disabled for data transfer.
<code>no dot1x port-control</code> [auto forced-unauthorized forced-unauthorized]	This command is used to disable 802.1X port-based authentication on the L2 interface, and resets to its default. The default authentication is forced-authorized.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x port-control auto
ALU(config-if switchport5/0)# no dot1x port-control auto
```

CONFIGURE 802.1X OPTIONAL PARAMETERS ON A L2 INTERFACE

To ENABLE PERIODIC REAUTHENTICATION

Command (in ICM)	Description
<code>dot1x reauthentication</code>	This command is used to enable periodic reauthentication of the client. By default, this is disabled.
<code>no dot1x reauthentication</code>	This command is used to disable periodic reauthentication of the client.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x reauthentication
```

```
ALU(config-if switchport5/0)# no dot1x reauthentication
```

To CONFIGURE TIME-OUT FOR PERIODIC REAUTHENTICATION

Command (in ICM)	Description
<code>dot1x timeout reauth-period</code> <code><1-65535></code>	This command sets the number of seconds between reauthentication attempts. This is valid only if periodic reauthentication is enabled.
<code>no dot1x timeout reauth-period</code> [<code><1-65535></code>]	This command sets the reauthentication period to its default. The default is 3600 seconds.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x timeout reauth-period 4500
```

```
ALU(config-if switchport5/0)# no dot1x timeout reauth-period
```

To CONFIGURE TIME-OUT FOR QUIET PERIOD

Command (in ICM)	Description
<code>dot1x timeout quiet-period <1-3600></code>	This command sets the number of seconds that the OA-700 remains in the quiet state following a failed authentication exchange with the client.
<code>no dot1x timeout quiet-period [<1-3600>]</code>	This command sets the quiet period to its default. The default is 60 seconds.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x timeout quiet-period 50
```

```
ALU(config-if switchport5/0)# no dot1x timeout quiet-period
```

To CONFIGURE SWITCH-TO-CLIENT RETRANSMISSION TIME

Command (in ICM)	Description
<code>dot1x timeout tx-period <1-3600></code>	This command sets the number of seconds that the OA-700 waits for a response to an EAP-request/identity frame from the client before retransmitting the request.
<code>no dot1x timeout tx-period [<1-3600>]</code>	This command sets the tx-period to its default. The default is 30 seconds.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x timeout tx-period 60
```

```
ALU(config-if switchport5/0)# no dot1x timeout tx-period
```


TO CONFIGURE SWITCH-TO-CLIENT RETRANSMISSION TIME FOR EAP-REQUEST FRAMES

Command (in ICM)	Description
<code>dot1x timeout supp-timeout <1-65535></code>	This command sets the switch-to-client retransmission time for the EAP-request frame.
<code>no dot1x timeout supp-timeout [<1-65535>]</code>	This command sets the supp-timeout to its default. The default is 30 seconds.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x timeout supp-timeout 40
ALU(config-if switchport5/0)# no dot1x timeout supp-timeout
```

TO CONFIGURE SWITCH-TO-CLIENT FRAME RETRANSMISSION NUMBER

Command (in ICM)	Description
<code>dot1x max-request <1-10></code>	This command sets the number of times that the switch sends an EAP-request/identity frame to the client (assuming no response is received) before restarting the authentication process.
<code>no dot1x max-request [<1-10>]</code>	This command sets the max-request to its default. The default is 2.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x max-request 3
ALU(config-if switchport5/0)# no dot1x max-request
```

To ENABLE MULTIPLE HOSTS

You can attach multiple hosts to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the host becomes unauthorized on the port, all attached hosts are denied access to the network.

In multiple authentication mode, all the hosts have to be authenticated for network access. Only those hosts that are authenticated will be able to access the network.

Command (in ICM)	Description
<code>dot1x host-mode {multi-host multi-auth}</code>	This command is used to allow multiple hosts (clients) or multiple authentication on an 802.1X-authorized port. Make sure that the port-based authentication for the specified L2 interface is set to 'auto'. (See "To Enable 802.1X Port-based Authentication on L2 Interface")
<code>no dot1x host-mode</code>	This command disables multiple hosts/multiple authentication mode on the port, and resets to 'single host mode', which is the default.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x host-mode multi-host
```

```
ALU(config-if switchport5/0)# no dot1x host-mode
```

To RESET CONFIGURABLE 802.1X PARAMETERS TO DEFAULT VALUES

Command (in ICM)	Description
<code>dot1x default</code>	This command is used to reset the configurable 802.1X parameters to the default values.

EXAMPLE

```
ALU(config-if switchport5/0)# dot1x default
```

TO MANUALLY REAUTHENTICATE THE CLIENT

Command (in CM)	Description
<code>dot1x re-authenticate interface switchport <slot/port></code>	This command is used to manually reauthenticate the clients connected to a port.

EXAMPLE

```
ALU(config)# dot1x re-authenticate interface switchport 5/0
```

TO INITIALIZE THE AUTHENTICATION FOR THE CLIENT

Command (in CM)	Description
<code>dot1x initialize interface switchport <slot/port></code>	This command initializes the authentication for the client connected to a port.

EXAMPLE

```
ALU(config)# dot1x initialize interface switchport 5/0
```

802.1X SHOW COMMANDS

TO VIEW THE 802.1X CONFIGURATION

Command (in SUM/CM)	Description
show dot1x [{all interface switchport <slot/port>}]	This command is used to display the 802.1X configuration of all switchports or of a particular switchport.

EXAMPLE

```
ALU(config)# show dot1x interface switchport 5/0
```

```
-----  
802.1X is enabled on switchport5/0
```

```
reauth-enabled :      Disable  
reauth-period :      3600  
quiet-period :       60  
tx-period :         30  
supp-timeout :      30  
server-timeout :    30  
max-req :           2  
operation_mode : Single-Host  
port-control :      Auto
```

```
Supplicant : 00.0D.62.2B.76.FA  
Status :      Authorized  
Current Identifier : 3
```

```
Authenticator state machine  
State :      Authenticated  
Reauth count: 0
```

```
Backend state machine  
State :      Idle  
Request count : 0
```

```
Reauthentication state machine  
state :      Initialize
```

To VIEW THE 802.1X STATISTICS

Command (in SUM/CM)	Description
show dot1x statistics [{all interface switchport <slot/port>}]	This command is used to display the 802.1X statistics of all switchports or of a particular switchport.

EXAMPLE

```
ALU# show dot1x statistics interface switchport 5/0
```

```
-----
802.1X is enabled on switchport5/0
Rx:      EAPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
         start     Logoff     Invalid    Total      Resp/ID   Resp/oth  LenError
         5         1         0         16         5         5         0

Last          Last
EAPOLVer     EAPOLSrc
2            00.0D.62.2B.76.FA

Tx:          EAPOL      EAP      EAP
         Total      Req/ID    Req/oth
         23         5         10
```

To VIEW MAC ADDRESS OF THE AUTHENTICATED SUPPLICANT

Command (in SUM/CM)	Description
show dot1x interface switchport <slot/port> authenticated-mac	This command displays the mac-address of the authenticated supplicant.

EXAMPLE

```
ALU# show dot1x interface switchport 0/0 authenticated-mac
```

```
00.0D.62.2B.76.FA
```

802.1X CONFIGURATION EXAMPLE

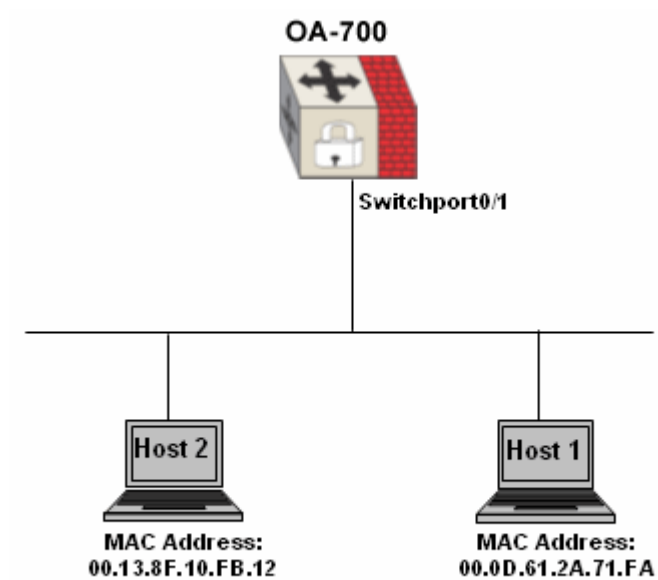


Figure 18: 802.1X Topology

ALCATEL-LUCENT CONFIGURATION

```
!Current Configuration:
!
! Statlog Configuration
!
logging on
logging buffered priority 7
logging buffered size 128
logging console 7
logging system 5
service timestamps log
hostname ALU
!
!VRF Configuration
!
! MULTICAST Configuration
!
!
dot1x system-auth-control
!
! SNMP Configurations
!
!
aaa services
!
```

```
username recovery password 5
0bf5de4fce714a3141a079734a60796e
username superadmin password 5
d41d8cd98f00b204e9800998ecf8427e
!
!
aaa server-group radius rad-01
radius-server 182.168.20.253 key ALU
!
!
!
aaa method-list method-01 rad-01
!
aaa authentication dot1x method-01
!
aaa authorization enable
!
!
interface GigabitEthernet7/0
ip address 192.168.20.1/24
no shutdown
top
!
interface GigabitEthernet7/1
shutdown
top
!
interface Vlan100
ip address 192.168.10.1/24
no shutdown
top
!
interface switchport0/0
switchport access vlan 100
dot1x port-control auto
no shutdown
top
!
interface switchport0/1
switchport access vlan 100
dot1x port-control auto
dot1x host-mode multi-auth
no shutdown
top
!
interface switchport0/2
shutdown
top
!
interface switchport0/3
shutdown
top
!
interface switchport0/4
```

```

        shutdown
    top
    !
interface switchport0/5
    shutdown
    top
    !
interface switchport0/6
    shutdown
    top
    !
interface switchport0/7
    shutdown
    top
    !
end

```

CHECK THE CONFIGURATION WITH THE SHOW COMMAND

ALU# show dot1x all

```

Global 802.1X parameters
System-auth-control: Enable

```

802.1X port summary

Port Name	Status	Operation Mode	Mode	Authorized
switchport0/0	Enabled	Single-Host	Auto	n/a
switchport0/1	Enabled	Multi-Auth	Auto	yes
switchport0/2	Disabled	Single-Host	Force-Authorized	n/a
switchport0/3	Disabled	Single-Host	Force-Authorized	n/a
switchport0/4	Disabled	Single-Host	Force-Authorized	n/a
switchport0/5	Disabled	Single-Host	Force-Authorized	n/a
switchport0/6	Disabled	Single-Host	Force-Authorized	yes
switchport0/7	Disabled	Single-Host	Force-Authorized	n/a

802.1X port details

```

-----
802.1X is enabled on switchport0/0
reauth-enabled :      Disable
reauth-period  :      3600
quiet-period   :       60
tx-period      :       30
supp-timeout   :       30
server-timeout :       30
max-req        :        2
operation_mode : Single-Host
port-control   :      Auto

```

```

Supplicant : 00.00.00.00.00.00
Status :      Unauthorized
Current Identifier :      14

```

```

Authenticator state machine
State :      Initialize

```



```
Reauth count:          0

Backend state machine
State :                Idle
Request count :       0

Reauthentication state machine
state :                Initialize
-----
802.1X is enabled on switchport0/1
reauth-enabled :      Disable
reauth-period :      3600
quiet-period :       60
tx-period :          30
supp-timeout :       30
server-timeout :     30
max-req :            2
operation_mode :     Multi-Auth
port-control :       Auto

Supplicant : 00.13.8F.10.FB.12
Status :           Authorized
Current Identifier : 3

Authenticator state machine
State :           Authenticated
Reauth count:    0

Backend state machine
State :           Idle
Request count :  0

Reauthentication state machine
state :           Initialize

Supplicant : 00.0D.61.2A.71.FA
Status :           Authorized
Current Identifier : 15

Authenticator state machine
State :           Authenticated
Reauth count:    0

Backend state machine
State :           Idle
Request count :  0

Reauthentication state machine
state :           Initialize
-----
802.1X is disabled on switchport0/2

-----
802.1X is disabled on switchport0/3

-----
802.1X is disabled on switchport0/4

-----
```

802.1X is disabled on switchport0/5

802.1X is disabled on switchport0/6

802.1X is disabled on switchport0/7

CHAPTER 10 PORT MONITORING

This chapter covers the commands used to configure Port Monitoring on the OA-700.

The “[Port Monitoring Overview](#)” section serves as an additional information on the port monitoring. You can skip this section, and directly forward to the configuration section of this chapter, detailed in “[Port Monitoring Configuration](#)”.

For instructions on using the port monitoring commands and descriptions on each of their parameters with the corresponding default values for each, refer to the *OmniAccess 700 CLI Command Reference Guide*.

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
SUM	Super User Mode

PORT MONITORING OVERVIEW

Port monitoring is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port, where the packet can be studied. A network administrator uses port monitoring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep a close track of switch performance and alter it if necessary.

An administrator configures port monitoring by assigning a port to copy all packets and another port where those packets will be sent. A packet bound for or heading away from the first port will be forwarded onto the second port as well. The administrator places a protocol analyzer on the port receiving the mirrored data to monitor each segment separately. The analyzer captures and evaluates the data without affecting the client on the original port.



Note: Port Monitoring is not enabled across cards.

PORT MONITORING CONFIGURATION

The following lists the steps to configure Port Monitoring on the OA-700:

PORT MONITORING CONFIGURATION STEPS

Step 1: Configure L2 interface.

```
ALU(config)# interface switchport <slot/port>
ALU(config-if switchport<slot/port>)#
```

Example:

```
ALU(config)# interface switchport 1/0
ALU(config-if switchport1/0)#
```



Note: The L2 interface on which port monitoring is being configured should not be in 'Trunk/Hybrid' mode. And, also 802.1X should not be configured on the interface.

Step 2: Administratively bring up the interface.

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if switchport1/0)# no shutdown
```

Step 3: Configure Port Monitoring. See ["To Configure Port Monitoring"](#)

Step 4: View port monitoring configuration details. ["To View Port Monitor Details"](#)

PORT MONITORING COMMANDS

TO CONFIGURE PORT MONITORING

Command (in ICM)	Description
<code>port monitor interface switchport <slot/port> [{both egress ingress}]</code>	This command is entered in the Interface Configuration Mode. This command is used to configure port monitoring. Specify the traffic to be monitored. You can either monitor ingress/egress traffic or both. By default, the both (egress and ingress) traffic is monitored.
<code>no port monitor interface switchport <slot/port> [{both egress ingress}]</code>	This command is used to disable port monitoring. Specify the slot/port on which traffic is not to be monitored.

EXAMPLE

The following example shows that the switchports 1/6 and 1/7 are to be monitored. Switchport 1/0 being the monitoring port, the port receives the mirrored data from switchports 1/6 and 1/7.

```
ALU(config-if switchport1/0)# port monitor switchport 1/6
both
```

```
ALU(config-if switchport1/0)# port monitor switchport 1/7
ingress
```

```
ALU(config-if switchport1/0)# no port monitor switchport 1/7
ingress
```

TO VIEW PORT MONITOR DETAILS

Command (in SUM/CM)	Description
<code>show port monitor [interface switchport <slot/port>]</code>	This command displays the port monitoring details on the specified port.

EXAMPLE

```
ALU(config)# show port monitor
```

```
PORT-MONITERING  PORT-MONITERED  TRAFFIC-TYPE
-----
switchport1/0   switchport1/6  both
                  switchport1/7  ingress
```

PORT MONITORING CONFIGURATION ON OA-700

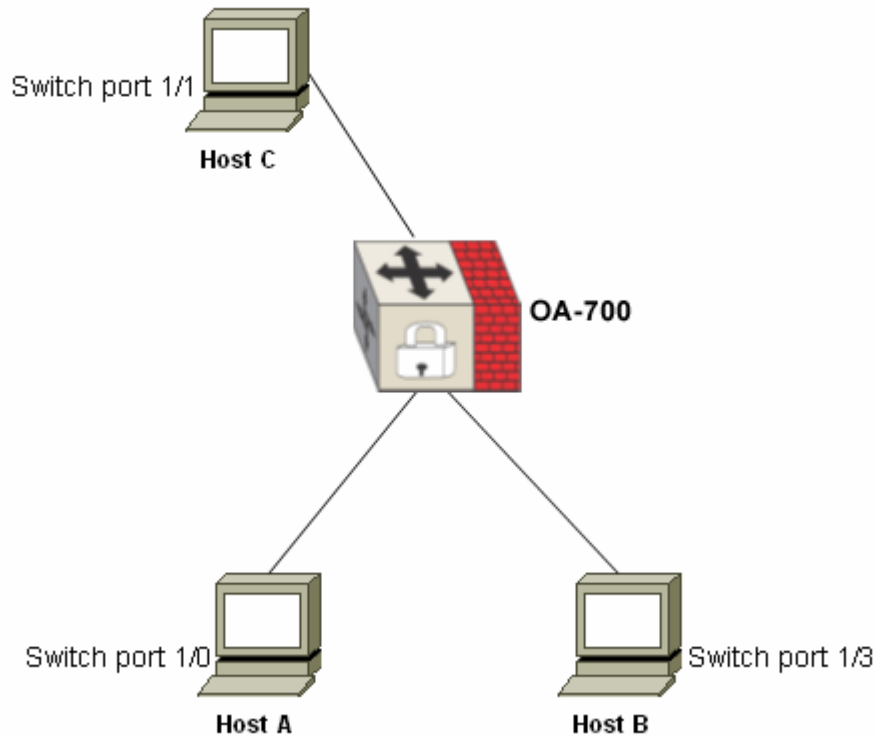


Figure 19: Port Monitoring Topology

PROCEDURE

The above topology shows that the Host A, Host B, and Host C are connected to switchport 1/0, 1/3, and 1/1 respectively.

Switchport 1/0 is to be monitored (for both ingress and egress traffic) using switchport 1/3. Switchport 1/3 being the monitoring port, has to receive the mirrored data from switchport 1/0.

To configure port monitoring, the following configuration is to be used:

CONFIGURE PORT MONITORING

```
ALU(config)# interface switchport 1/3
ALU(config-if switchport1/3)# port monitor switchport 1/0
both
```

CHECK THE CONFIGURATION WITH THE SHOW COMMAND

```
ALU(config)# show port monitor
```

```
PORT-MONITORING  PORT-MONITERED  TRAFFIC-TYPE
-----
switchport1/3   switchport1/0  both
```


Part 3 WAN Interfaces and Protocols



CHAPTER 11 T1E1 LINE CARD

This chapter describes steps to configure the T1E1 line card.

In this chapter, T1 and E1 configurations are dealt separately. This chapter describes various configuration steps to configure T1 interface, see [“T1 Configuration”](#) and E1 interface, see [“E1 Configuration”](#).

CHAPTER ORGANIZATION

This chapter is divided into the following sections:

- [“T1 and E1 Overview”](#)
- [“Alcatel-Lucent Specific Overview”](#)
- [“E1 Interface Overview”](#)
- [“E1 Configuration”](#)
- [“T1 Interface Overview”](#)
- [“T1 Configuration”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
CCM	Controller Configuration Mode - ALU (config-controller)#
ICM	Interface Configuration Mode - ALU (config-interface name)#

T1 AND E1 OVERVIEW

The T1 and E1 interfaces are two different, independent standardized TDM (Time Division Multiplexing) technologies. These technologies enable the transmission of several (multiplexed) voice/data channels simultaneously on the same transmission facility.

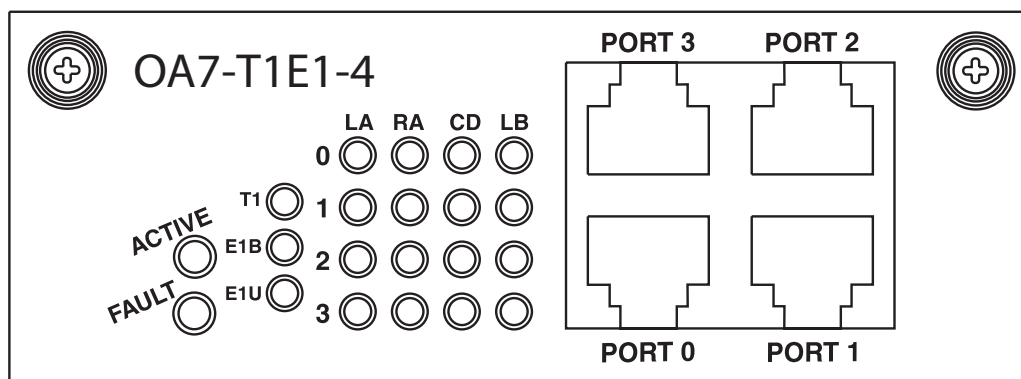


Figure 20: The OA-700 T1E1 Line Card



Note: For information on the LED status of the T1E1 line card with respect to each port, please refer “**OA-780/OA-740 Hardware Users Guide**”.

The T1 and E1 is designed for use in businesses. The T1 standard is mostly deployed in Japan and North American countries, while the E1 is prevalent in Europe and most of the Asian countries, including India. The E1s and the T1s belong to the physical layer in the OSI reference model, thus Layer 2 technologies like the FR, PPP, Cisco HDLC, MLPPP, MLFR, etc., are carried over it.

The OA-700 supports both T1 and E1 line cards.

E1 INTERFACE OVERVIEW

The E1 interface provides a transmission rate of 2.048 Mbps. It can support up to 32 user channels, though usually 31 channels are used as dedicated user channels in framed mode.

An E1 basic frame is made up of 256 bits, 32 timeslots, each containing 8 bits. Each timeslot provides a 64 Kbps data throughput. An E1 line connects two points in one of which, the information is multiplexed and in the second demultiplexed.

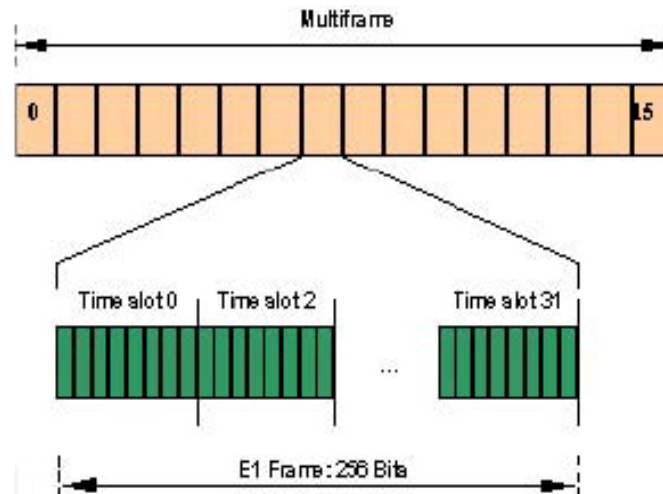


Figure 21: E1 Frame Structure

The following sections detail on the E1 configuration:

- [“E1 Timeslot Functionalities”](#)
- [“Mechanisms Supported by the E1 interface”](#)
- [“E1 Modes of Operation”](#)

E1 TIMESLOT FUNCTIONALITIES

The 32 time slots of an E1 card are denoted by TS0, TS1,.....TS31, respectively. Their individual functionalities are given below.

- TS0 is dedicated for synchronization, alarms and messages, unless configured differently.
- TS16 is usually used for signaling, but can carry data as well.
- TS1-TS15 and TS17-TS31 are used for carrying user data.

MECHANISMS SUPPORTED BY THE E1 INTERFACE

In order to provide a reliable and accurate service, the E1 interface supports several mechanisms for synchronization, error correction and detection, management and performance messages and signaling.

These mechanisms and their way of operation are explained in the following sections.

THE SYNCHRONIZATION MECHANISM

To verify that the received bits are mapped to the correct channels, a synchronization mechanism is activated. This mechanism is independent of any clock, and does not synchronize the clocks. Clock recovery is achieved by the shape of the signal.

The synchronization information is carried in the TS0 of every even frame. Such a frame is called "**Frame Alignment Signal (FAS)**". An FAS carries the unique pattern 0011011 (bits 1 - 7), that specifies the alignment of the frame.

THE SIGNALING MECHANISM

Signaling mechanisms provide a wide range of functions and their protocol is application specific. Two modes of signaling are employed, namely:

- Common Channel Signaling (CCS) - In this mode of operation one or more channels of 64 kbit/s are dedicated for signaling and the information carried in them asynchronously serves all other channels. TS16 is usually used for this purpose.
- Channel Associated Signaling (CAS) - In each Multiframe, each channel has a predetermined frame. In this frame, half of TS16 is dedicated for this channel signaling information.

E1 MODES OF OPERATION

The E1 interface supports 3 different kinds of bit structures: Frame, Multiframe, and Unframed. The mode of operation dictates how the bits are structured and consequently the way it will be interpreted. The E1 modes are listed below:

- Unframed (UNF): A stream of bits at 2.048 Mbps. No channels are associated to any specific group of bits. In an unframed operational mode, none of the mechanisms described above is used.
- Framed (FR): 31 time-slots are used to transfer data. Detection of the frame boundaries (synchronization) is achieved using TS0.
- Multiframe (MF): TS0 is used for the synchronization of the Multiframes. All other channels are unaffected. Multiframe structure is used for two purposes: CAS signaling and Cyclic Redundancy Check (CRC). Each of these modes are independent from the use of the other.
- MF + CAS: Same as MF + One channel that is dedicated for signaling (CAS).
- MF + CRC: Using the Si bits of each FAS to deliver the CRC - 4.
- MF + CAS/CCS + CRC
- ESF + CAS
- ESF + FDL
- ESF + CAS/CRC/FDL.
- CCS: Can be used in each of the framed formats by dedicating one channel (usually TS-16) for delivering the signaling messages in a predetermined protocol.

ALCATEL-LUCENT SPECIFIC OVERVIEW

- In E1 lines, cable-length is referred to as Line Termination. There is no variation of Long and Short cable length.
- OA-700 supports fractional T1 or E1.
- OA-700 supports Unframed E1.
- OA-700 supports channelized T1 or E1.

E1 CONFIGURATION

Refer to the following sections to configure an E1 controller on the OA-700:

- [“E1 Configuration Steps”](#)
- [“E1 Configuration Flow”](#)
- [“E1 Configuration Commands”](#)
- [“E1 Show Commands”](#)
- [“Troubleshooting E1 Lines”](#)

E1 CONFIGURATION STEPS

The following are the steps to configure an E1 interface:

Step 1: Set the card type to E1 [“To Set the Card type to E1”](#)

Step 2: Enter Controller Configuration Mode. See [“To Configure an E1 Controller”](#)

Step 3: Configure channel groups on the controller. See [“To Configure Channelized E1”](#). This command creates a channel-group that will form a channelized serial interface.

Step 4: Administratively bring up the E1 controller. See [“To Bring Up/Shutdown the E1 Controller”](#)

Step 5: Configure Optional parameters for E1. See [“Configure Optional Parameters for E1 Controller”](#)

- Configure framing. See [“To Configure Framing”](#)
- Configure the line-termination. See [“To Configure Line-termination”](#)
- Configure the linecoding scheme. See [“To Configure Linecode”](#)
- Configure clock source. See [“To Set the Card type to E1”](#)

Step 6: Enter Interface Configuration Mode to configure the channelized serial interface. See [“To Configure a Serial Interface”](#)



Note: Creation of a channel-group is a pre-requisite prior to configuring a serial interface.

Step 7: Administratively bring up the serial interface. See [“To Bring up and Shutdown the Interface”](#)

Step 8: Configure the IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-  
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if Serial0/0:0)# ip address 20.20.20.20/24
```

Step 9: Configure encapsulation. See [“To Set Encapsulation on the Interface” \(Optional\)](#)

Step 10: Configure MTU (Maximum Transmission Unit) on the Interface. See [“To Configure MTU on the Interface” \(Optional\)](#)

Step 11: See [“To View the E1 Controller Configuration”](#) to view the E1 configuration details.

Step 12: View the interface configuration details. See [“To View Interface Configuration”](#) command.

E1 CONFIGURATION FLOW

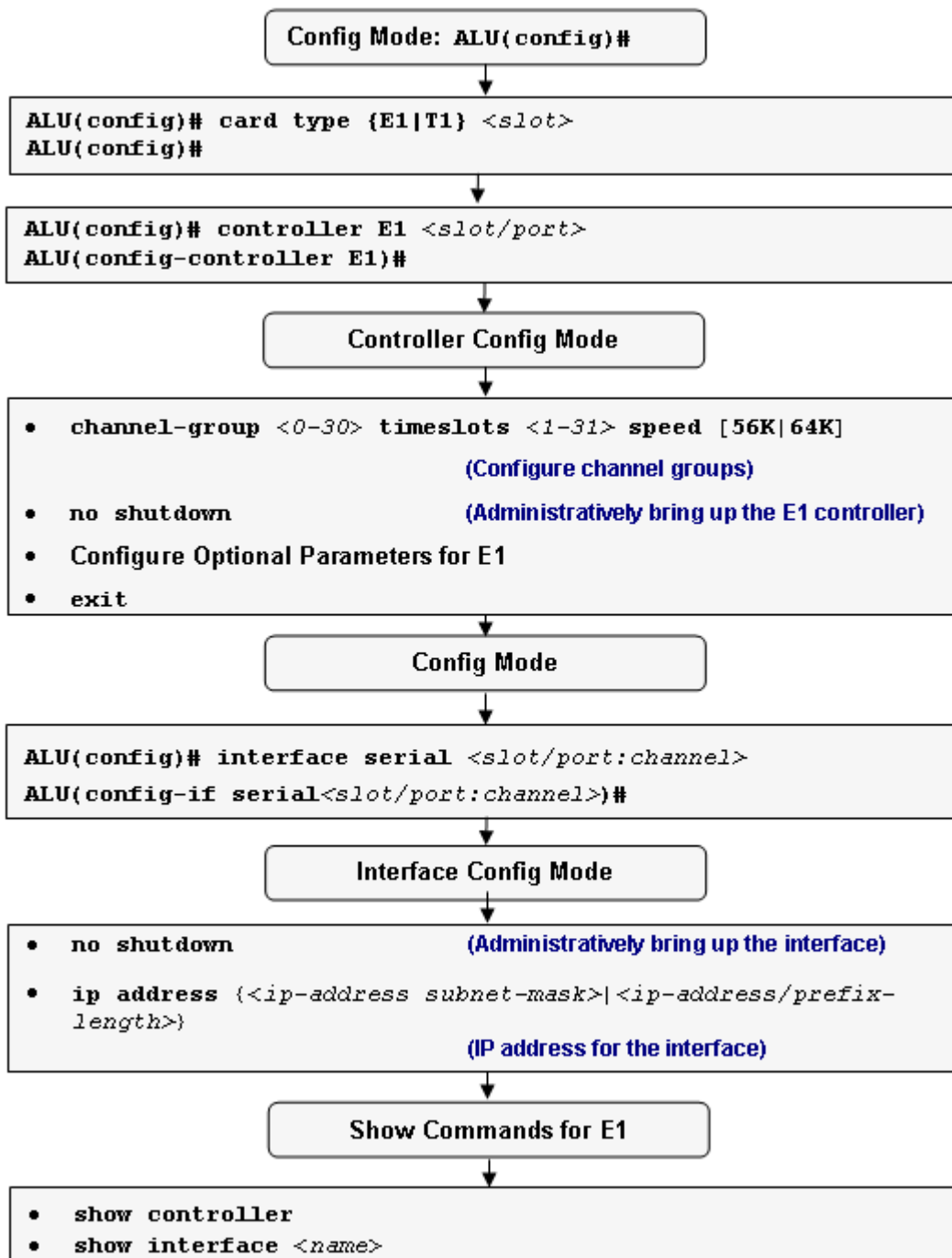


Figure 22: E1 Configuration Flow

E1 CONFIGURATION COMMANDS

This section provides details about the commands that are used in configuring an E1 interface.

TO SET THE CARD TYPE TO E1

Command (in CM)	Description
<code>card type {E1 T1} slot</code>	Use this command to set the card type to E1.

EXAMPLE

The following example sets the card type of the E1 controller:

```
ALU(config)# card type E1 0
```



Note: The line card is not functional until card type is set. Reboot/Reload the chassis to change the card type, which will remove the previous configuration. Use **controller** and **channel-group** commands to reload the card type.

TO CONFIGURE AN E1 CONTROLLER

Command (in CM)	Description
<code>controller {E1 T1} <slot/port></code>	This command configures an E1 or T1 controller. Use E1 keyword to configure an E1 controller.

EXAMPLE

```
ALU(config)# controller E1 0/0
ALU(config-controller E1)#
```

TO CONFIGURE CHANNELIZED E1

The controller can be channelized. This implies that more than one channel-group can be configured on a controller.

Command (in CCM)	Description
<code>channel-group <0-30> timeslots <1-31> speed [56K 64K]</code>	This command is used to create channel-groups that vary from 0-30 and set timeslots that vary from 1-31. This enables the interface on the controller. Default value of speed: 64 Kbps.
<code>no channel group <0-30></code>	This command removes the channel group configured on the controller.



Note: The OA-700 supports unframed E1 and channelized E1. You can configure only 20 channel groups per card.

EXAMPLE

The following example configures a channel group on controller E1 at the first slot and at the 0th port:

1. Variations of the channel-group to associate different timeslots with the serial interface are shown:

To associate all the timeslots with the controller:

```
ALU(config-controller E1)#channel-group 0 timeslots 1-31
```

To associate contiguous timeslots with the controller:

```
ALU(config-controller E1)#channel-group 0 timeslots 1-10
ALU(config-controller E1)#channel-group 0 timeslots 4,5,6
```

To associate non-contiguous timeslots with the controller:

```
ALU(config-controller E1)#channel-group 0 timeslots 1,4,20
```

2. In the above example, the channel-group command is shown only with a value of '0'. Now the values in the range of 0-30 can be used:

To configure multiple channel groups, with absolute values of timeslots

```
ALU(config-controller E1)#channel-group 0 timeslots 1
ALU(config-controller E1)#channel-group 1 timeslots 2
```

To configure multiple channel groups, with contiguous values of timeslots

```
ALU(config-controller E1)#channel-group 3 timeslots 10-13
```

To configure multiple channel groups, with non-contiguous values of timeslots

```
ALU(config-controller E1)#channel-group 2 timeslots 3,6,9
```



Note: Timeslots cannot overlap, hence one timeslot cannot be part of more than one channel-group.

To BRING UP/SHUTDOWN THE E1 CONTROLLER

Command (in CCM)	Description
<code>no shutdown</code>	This command is used in the Controller Configuration Mode. This command is used to administratively bring up the controller.
<code>shutdown</code>	This command is entered in the controller configuration mode to administratively bring down the controller.

EXAMPLE

The following example administratively brings up the controller:

```
ALU(config)#controller E1 1/0
ALU(config-controller E1)# no shutdown
```

The following example shuts down the controller:

```
ALU(config)# controller E1 1/0
ALU(config-controller E1)# shutdown
```



Note: Online Insertion and Removal (OIR) functionality is supported on the T1 and E1 cards. After re-insertion, the default state of the controller is in '**shutdown**' state.

To CONFIGURE UNFRAMED E1

E1 controller can be configured as unframed, which is also known as the "clear channel mode". If the controller is configured in unframed mode:

- System creates channel group 0 comprising of **all** timeslots.
- There is no provision to configure a channelized or framed E1. This implies that unframed and channelized functionality are mutually exclusive.

Following are the sequence of commands to configure E1 into Unframed mode. 'No' version of this command will restore the default framing mode, i.e., **esf**.

```
ALU(config)#controller E1 0/0
ALU(config-controller E1)#no shutdown
ALU(config-controller E1)#unframed
ALU(config-controller E1)#no unframed
```

As system is creating channel-group 0, serial interface will be available, and you will require to configure it too.

```
ALU(config)#interface Serial 0/0:0
ALU(config-if Serial 0/0:0)#no shutdown
```

CONFIGURE OPTIONAL PARAMETERS FOR E1 CONTROLLER

To CONFIGURE FRAMING

Command (in CCM)	Description
<code>framing {crc4 no-crc4}</code>	Use this command to configure framing to either crc4 or no-crc4.
<code>no framing</code>	The “ no ” command sets the framing to its default. The default framing value is crc4 in case of E1.

The service provider determines which framing type, either crc4 or no-crc4 is required for your E1 circuit.

EXAMPLE

The following example sets the E1 frame type to no crc4:

```
ALU(config-controller E1)#framing no-crc4
```

The following example sets the E1 frame type to crc4:

```
ALU(config-controller E1)# no framing
```

To CONFIGURE LINE-TERMINATION

Command (in CCM)	Description
<code>line-termination {75 120}</code>	Use this command to configure a line impedance of 75 or 120.
<code>no line-termination</code>	The “ no ” command sets the impedance value to its default. The default line-termination value is 120 ohm.

EXAMPLE

The following example selects 120 as the E1 line impedance:

```
ALU(config-controller E1)#line-termination 120
```

To CONFIGURE LINECODE

Command (in CCM)	Description
<code>linecode {ami hdb3}</code>	This command is used to set a Line Encoding for the E1 interface.
<code>no linecode</code>	The “no” command sets the linecode to its default. The default linecode value is HDB3.

The E1 service provider determines the linecode type, whether ami or hdb3 is required for your E1 circuit.



Note: If ‘ami’ linecode is configured, configure timeslot speed to 56Kbps to ensure ones density.

EXAMPLE

The following example sets the line code type for E1 to ami:

```
ALU(config-controller E1)# linecode ami
```

The following example sets the line code type for E1 to hdb3:

```
ALU(config-controller E1)# no linecode
```

To SET A CLOCKSOURCE ON E1

Command (in CCM)	Description
<code>clocksource {internal line}</code>	This command is entered in the controller configuration mode to set clocksource for E1 interface. The keyword “ clocksource ” is used to configure clock signals.
<code>no clocksource</code>	The “no” keyword sets the clocksource to its default. The default value for clocksource is internal.

EXAMPLE

The following example configures the E1 0 clocksource to line:

```
ALU(config-controller E1)# clocksource line
```

The following example configures the E1 0 clocksource to internal:

```
ALU(config-controller E1)# no clocksource
```


To CONFIGURE A SERIAL INTERFACE

Command (in CM)	Description
<code>interface Serial <slot/ port:channel></code>	This command is entered in the Configuration Mode to configure a serial interface in the specific slot or port of the E1 card.

EXAMPLE

The following example enters into the interface configuration mode with a serial interface having slot-number 0, port 0 with group 0:

```
ALU(config-controller E1)# exit
ALU(config)#
ALU(config)#interface Serial 0/0:0
ALU(config-if Serial0/0:0)#
```

To BRING UP AND SHUTDOWN THE INTERFACE

Command (in ICM)	Description
<code>no shutdown</code>	This command is entered in the interface configuration mode to administratively bring up the interface.
<code>shutdown</code>	This command is entered in the interface configuration mode to administratively bring down the interface.

EXAMPLE

```
ALU(config)#interface Serial 0/0:0
ALU(config-if Serial0/0:0)# shutdown

ALU(config)#interface Serial 0/0:0
ALU(config-if Serial0/0:0)# no shutdown
```



Note: We support Online Insertion and Removal (OIR) functionality for T1E1 line card.

TO SET ENCAPSULATION ON THE INTERFACE

Command (in ICM)	Description
<code>encapsulation {frame-relay ppp hdlc mlfr <bundle_id> mlppp <bundle_id>}</code>	This command is entered in the interface configuration mode to set encapsulation on the interface.
<code>no encapsulation</code>	The “no” command sets the encapsulation to its default. The default encapsulation is HDLC.

EXAMPLE

The following example shows how to set the FR encapsulation:

```
ALU(config-if Serial 0/0:0)# encapsulation frame-relay
```

TO CONFIGURE MTU ON THE INTERFACE

Command (in ICM)	Description
<code>mtu <64-1500></code>	This command is used to configure the MTU value on the serial interface, i.e., the maximum size of the transmitted layer 2 payload.
<code>no mtu</code>	The “no” command sets the MTU to its default. The default MTU is 1500 bytes.

EXAMPLE

```
ALU(config-if Serial0/0:0)# mtu 1200
```

```
ALU(config-if Serial0/0:0)# no mtu
```

E1 SHOW COMMANDS

TO VIEW THE E1 CONTROLLER CONFIGURATION

Command (in SUM)	Description
<code>show controller</code>	This command displays controller status that is specific to the controller hardware.

The show controller E1 command displays the status of the E1 controller and displays information about clocksources and other settings for the ports.

EXAMPLE

```

ALU# show controller
E1 1/0 is administratively down.
E1 1/1 is administratively down.
E1 1/2 is up.
  Line Card type is Channelized E1
  Line termination is 120ohm
  No Alarm Detected
  Framing is crc4, Line Code is hdb3, Clock Source is internal
  Total Data (Since last clearing of counters)
    1 Line Code Violation, 0 Framing Errors
    0 CRC Errors, 0 Far End Block Errors
E1 1/3 is administratively down.
ALU# show controller E1 1/2
E1 1/2 is up.
  Line Card type is Channelized E1
  Line termination is 120ohm
  No Alarm Detected
  Framing is crc4, Line Code is hdb3, Clock Source is internal
  Total Data (Since last clearing of counters)
    1 Line Code Violation, 0 Framing Errors
    0 CRC Errors, 0 Far End Block Errors

```

To VIEW INTERFACE CONFIGURATION

Command (in SUM)	Description
show interfaces <name>	This command displays the configuration of the specified interface.

EXAMPLE

This example shows the details of the interface specified.

ALU# show interfaces Serial 1/2:0

```
Serial1/2:0 is up, line protocol is up
  Internet address is 1.1.1.1/24
  MTU 1500 bytes, BW 64 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Loopback not set
  Encapsulation hdlc,   keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/max) 0
drops
  Conversations: 0/0/0/0 (active/max active/max total)
  Reserved Conversations: 0/0 (allocated/max allocated)
  Available Bandwidth 64 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    7 packets input, 154 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  7 packets output, 154 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
Timeslot(s) Used:1 (64Kbps each), Transmitter delay is 0 flags
```

TROUBLESHOOTING E1 LINES

This section lists the commands to troubleshoot the E1 line cards.

COMMANDS TO ENABLE AND DISABLE LOOPBACK

Command (in CCM)	Description
<code>loopback {{local network {line payload} remote {line payload}}</code>	Use the loopback controller configuration command to put the T1 or E1 line into loopback mode. It can be used to verify connectivity.
<code>no loopback</code>	The “ no ” command disables the loopback on the interface. By default, Loopback is disabled for the E1 lines.

EXAMPLE

The following configuration establishes a loopback of the incoming E1 signal on controller E1 0:

```
ALU(config)#controller E1 1/0
ALU(config-controller E1)# loopback network line
```

The following example disables the loopback on controller E1 0:

```
ALU(config)# controller E1 0/0
ALU(config-controller E1)# no loopback
```

T1 INTERFACE OVERVIEW

The T1 interface provides a transmission rate of 1.544 Mbps. It can support up to 24 user channels, each at a 64 Kbps access rate. The T1 interface supports 4 different bit structures, dictated by the mode of operation: Frame, Super Frame, Extended Super Frame, and Unframed.

These bit structures determine how the bits are interpreted. A T1 basic frame is made up of 24 timeslots plus 1 framing bit added to them. Each timeslot is regarded as a channel of 64 Kbps bandwidth. The frame length is 193 bits ($24 \times 8 + 1$). A framing bit creates a channel of 8 Kbps and is used for messages, synchronization and alarms.

The following sections detail sequence of commands to configure a T1 line card:

- [“Frame Formats Used in T1 Cards”](#)
- [“T1 Modes of Operation”](#)

FRAME FORMATS USED IN T1 CARDS

The T1 standard defines two frame formats, as described below.

THE SUPER FRAME (SF)

A Superframe is a structure constructed of 12 Frames, numbered 1 - 12. It is also called as the D4 frame. Two mechanisms can be activated using SF's synchronization mechanism, which is always activated, and signaling mechanism, which is optional.

- **The synchronization mechanism** - The 12 framing bits, which are the leading bits of each frame in one SF form a unique pattern. With this pattern, synchronization is achieved and verified (it is used to identify the frame boundaries and the SF boundaries).
- **The signaling mechanism** - If CAS is in use, every 6th frame in the SF contains one "robbed" bit in each byte of information (channel). This "robbed" bit carries the information of this specific channel. The last bit of each TS is "robbed" for the purpose of signaling. These "robbed" bits form a channel with capacity of 10.666 Kbps. If CCS is in use, then one Timeslot (TS), usually TS 24, is dedicated for signaling purposes.

THE EXTENDED SUPER FRAME (ESF)

Also known as D5 frame or FE. Each extended superframe consists of 24 frames. The ESF has four different framing types:

- **Synchronization** - Bit sequence 001011 in frames 4, 8, 12, 16, 20, 24 - when working with ESF, synchronization is achieved by checking the 6 bit-long pattern that is created from every 4th framing bit.
- **Signaling** - This mechanism is very similar to the signaling mechanism of the SF, except that it can be used for ABCD signaling using four different bits.
- **CRC-6** - Frames 2, 6, 10, 14, 18, 22 - This mechanism provides the ability to monitor the transmission quality of the DS1 facility. It uses every 4th bit of the framing bits in the ESF, beginning at the second one.
- **Data Link** - Frames 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23 - operates using every second framing bit, beginning at the first frame of the ESF. These bits create a 4 Kbps data link called the Facility Data Link (FDL). This channel is used for delivering maintenance information and supervisory control. Two kinds of messages are carried on the FDL channel, each using a different format, namely the Scheduled messages and the Unscheduled messages.

T1 MODES OF OPERATION

When using the T1 interfaces, several modes of operation are available. These modes are listed below:

- Superframe (SF): Data transferred using the SF format.
- SF + CAS: The CAS is carried over the robbed bits of each 6th and 12th frame detected by the SF format.
- ESF
- ESF + CAS
- ESF + FDL
- ESF + CAS/CRC/FDL.
- CCS: Can be used in each of the framed formats by dedicating one channel (usually TS-24) for delivering the signaling messages in a predetermined protocol.

T1 CONFIGURATION

Refer to the following sections to configure a T1 line card on your OA-700:

- [“T1 Configuration Steps”](#)
- [“T1 Configuration Flow”](#)
- [“T1 Configuration Commands”](#)
- [“T1 Show Commands”](#)
- [“Troubleshooting T1 Lines”](#)

T1 CONFIGURATION STEPS

Following are the steps to configure T1 interface:

Step 1: Set the card type to T1 [“To Set the Card type to T1”](#)

Step 2: Enter Controller Configuration Mode. See [“To Configure T1 Controller”](#)

Step 3: Configure channel-groups on the controller before entering into interface configuration mode. See [“To Configure Channelized T1”](#). This command creates a channel-group that will form a channelized serial interface.

Step 4: Administratively bring up the T1 controller. See [“To Bring Up/Shutdown the T1 Controller”](#)

Step 5: Configure Optional parameters for T1. See [“Configure Optional Parameters for T1 Controller”](#)

- Configure cablelength. See [“To Configure a Short Cablelength”](#), [“To Configure a Long Cablelength”](#)
- Configure framing. See [“To Configure Framing on T1”](#)
- Configure linecoding scheme. See [“To Configure Linecoding on T1”](#)
- Configure clocksource. See [“To Configure Clocksource”](#)

Step 6: Enter Interface Configuration Mode to configure the channelized serial interface. See [“To Configure a Serial Interface”](#)



Note: Creation of a channel-group is a pre-requisite prior to configuring a serial interface.

Step 7: Administratively bring up the interface. See [“To Bring Up/Shutdown the Interface”](#)

Step 8: Configure the IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-  
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if Serial0/0:0)# ip address 20.20.20.20/24
```

Step 9: Configure encapsulation on the interface. See [“To Set Encapsulation on the Interface” \(Optional\)](#)

Step 10: Configure MTU (Maximum Transmission Unit) on the Interface. See [“To Configure MTU on the Interface” \(Optional\)](#)

Step 11: See [“To View the Controller Configuration”](#) to view T1 configuration.

Step 12: View the interface configuration details. See [“To View Interface Configuration”](#) command.

T1 CONFIGURATION FLOW

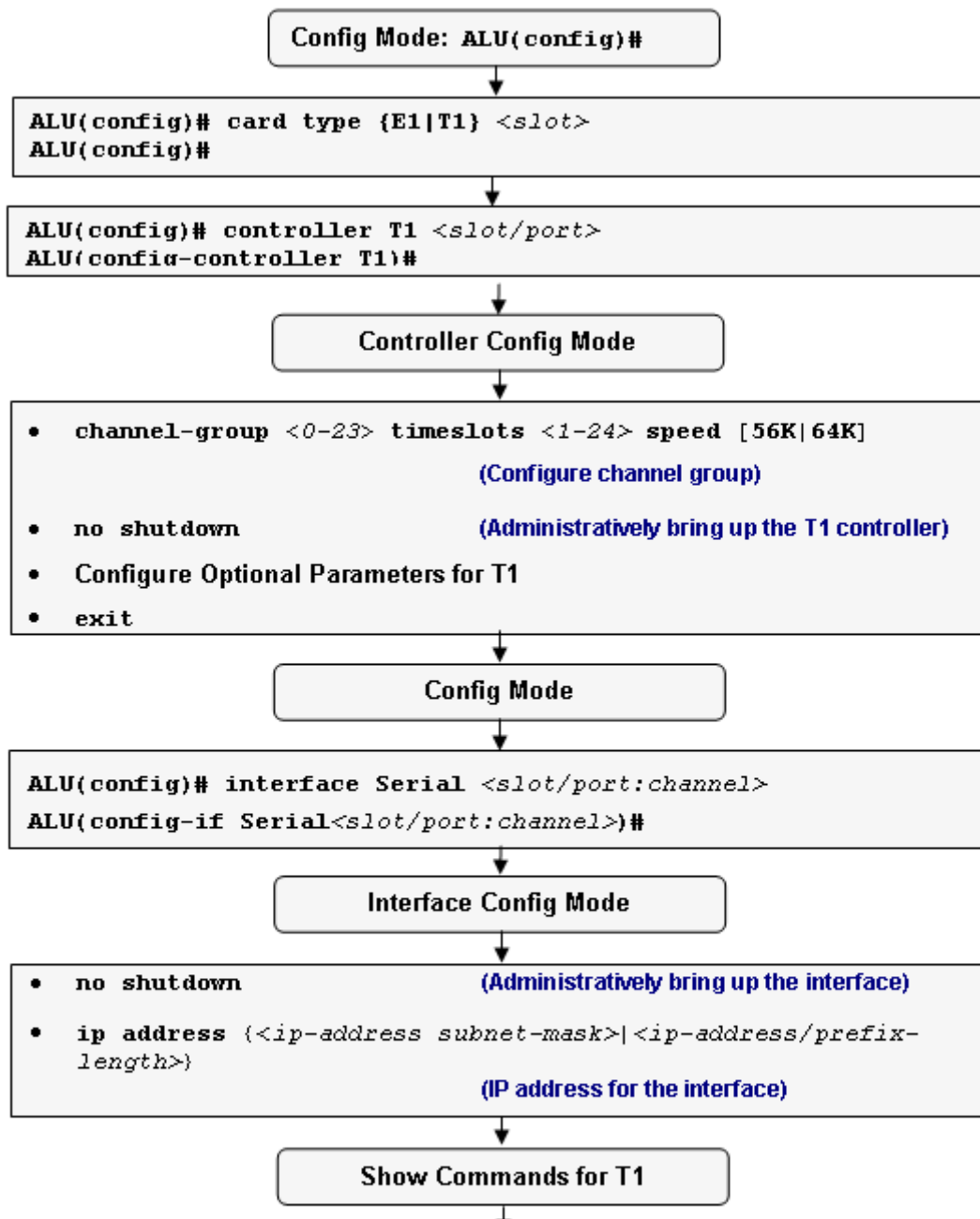


Figure 23: T1 Configuration Flow

T1 CONFIGURATION COMMANDS

This section comprises the commands that are used in configuring the T1 controller.

To SET THE CARD TYPE TO T1

Command (in CM)	Description
<code>card type {E1 T1} slot</code>	Use this command to set the card type to T1.

EXAMPLE

```
ALU(config)# card type T1 0
```



Note: The line card is not functional until card type is set. Reboot/Reload the chassis to change the card type, which will remove the previous configuration. Use **controller** and **channel-group** commands to reload the card type.

To CONFIGURE T1 CONTROLLER

Command (in CM)	Description
<code>controller {E1 T1} <slot/port></code>	This command configures a E1 or T1 controller. Use T1 keyword to configure a port in the T1 mode. The T1 has a bandwidth of 1.544 Mbps.

EXAMPLE

```
ALU(config)# controller T1 0/0
ALU(config-controller T1)#
```

To CONFIGURE CHANNELIZED T1

The controller can be channelized. This implies that more than one channel-group can be configured on a controller.

Command (in CCM)	Description
<code>channel-group <0-23> timeslots <1-24> speed [56K 64K]</code>	This command is entered in the controller configuration mode to create channel-groups that vary from 0-23 and set timeslots that vary from 1-24. The default speed is 64 Kbps.
<code>no channel-group <0-23></code>	This command removes the channel-groups configured on the controller.



Note: You can configure only 20 channel-groups per card.

The following example configures a channel group on controller T1 at the first slot and at the 0th port:

EXAMPLE**1. Variations of the channel-group to associate different timeslots with the serial interface are shown:**

To associate all the timeslots with the controller:

```
ALU(config-controller T1)#channel-group 0 timeslots 1-24
```

To associate contiguous timeslots with the controller:

```
ALU(config-controller T1)#channel-group 0 timeslots 1-10
ALU(config-controller T1)#channel-group 0 timeslots 1,2,3
```

To associate non-contiguous timeslots with the controller:

```
ALU(config-controller T1)#channel-group 0 timeslots 1,4,20
```

2. In the above example, the channel-group command is shown only with a value of '0'. The following example uses value in the range of 0-23:

To configure multiple channel groups, with absolute values of timeslots:

```
ALU(config-controller T1)#channel-group 0 timeslots 1
ALU(config-controller T1)#channel-group 1 timeslots 2
```

To configure multiple channel groups, with contiguous values of timeslots:

```
ALU(config-controller T1)#channel-group 3 timeslots 10-13
```

To configure multiple channel groups, with non-contiguous values of timeslots:

```
ALU(config-controller T1)#channel-group 2 timeslots 3,6,9
```



Note: Timeslots cannot overlap, hence one timeslot cannot be part of more than one channel-group

To BRING UP/SHUTDOWN THE T1 CONTROLLER

Command (in CCM)	Description
<code>no shutdown</code>	This command is entered in the controller configuration mode on the T1 controller. The keyword “ no shutdown ” will administratively bring up the controller.
<code>shutdown</code>	This command is entered in the controller configuration mode on the T1 controller. The keyword “ shutdown ” will administratively bring down the controller.

EXAMPLE

```
ALU(config-controller T1)# no shutdown
```

```
ALU(config-controller T1)# shutdown
```



Note: We support Online Insertion and Removal (OIR) functionality for T1E1 line card.

CONFIGURE OPTIONAL PARAMETERS FOR T1 CONTROLLER

To CONFIGURE A LONG CABLELENGTH

Command (in CCM)	Description
<code>cablelength long {-15db -22.5db -7.5db 0db}</code>	This command is used to configure transmit and receive levels for a cable length (line build-out) longer than 660 ft for a T1 trunk.
<code>no cablelength</code>	The “ no ” command sets the cable length to its default. The default length of the cable for a T1 is Long 0db.

The transmit attenuation value is best obtained by experimentation. If the signal received by the far-end equipment is too strong, reduce the transmit level by entering additional attenuation.

EXAMPLE

The following example changes transmit attenuation of controller T1 of slot 0 and port 0 to appropriate level for long cables:

```
ALU(config-controller T1)# cablelength long -22.5db
```

To CONFIGURE A SHORT CABLELENGTH

Command (in CCM)	Description
<code>cablelength short {110ft 220ft 330ft 440ft 550ft 660ft}</code>	This command is entered in the controller configuration mode to set the cablelength for the T1 interface.
<code>no cablelength</code>	The “no” command sets the cable length to its default. The default length of the cable for a T1 is Long 0db.

The command sets transmit attenuation for a cable length (line build-out) of 660 feet or shorter for a T1 trunk.

EXAMPLE

The following example sets the transmit attenuation of controller T1 of slot 1 and port 1 to the appropriate levels for a cable between 111 and 220 feet long:

```
ALU(config)#controller T1 1/1
ALU(config-controller T1)# cablelength short 220
```

The following example sets the cablelength to its default:

```
ALU(config)#controller T1 1/1
ALU(config-controller T1)# no cablelength
```

To CONFIGURE FRAMING ON T1

Command (in CCM)	Description
<code>framing {esf sf}</code>	This command is entered in the controller configuration mode to configure framing type.
<code>no framing</code>	The “no” command sets the framing to its default. The default framing value for T1 is esf.

The service provider determines which framing type, either sf or esf is required for your T1 circuit.

EXAMPLE

The following example configures frame type as super frame for T1:

```
ALU(config-controller T1)#framing sf
```

The following example resets the T1 frame type to esf:

```
ALU(config-controller T1)# no framing
```

To CONFIGURE LINECODING ON T1

Command (in CCM)	Description
<code>linecode {ami b8zs}</code>	This command is entered in the controller configuration mode to configure the line-code type for a T1 line.
<code>no linecode</code>	The “no” command sets the linecoding value its default. The default linecoding value is b8zs.

The T1 service provider determines which line-code type, ami, or b8zs, is required for your T1 circuit.

EXAMPLE

The following example specifies AMI as the linecode type for a T1 line:

```
ALU(config-controller T1)# linecode ami
```

The following example sets b8zs, as the linecode type:

```
ALU(config-controller T1)# no linecode
```

To CONFIGURE CLOCKSOURCE

Command (in CCM)	Description
<code>clocksource {internal line}</code>	This command is entered in the controller configuration mode to set clocksource for T1 interface. The keyword " clocksource " is used to transmit clock signals.
<code>no clocksource</code>	The “no” command sets the clocksource to its default. The default value for clocksource is internal.

EXAMPLE

The following example configures the T1 0 clocksource for line:

```
ALU(config-controller T1)# clocksource line
```

The following example configures the T1 0 clocksource for internal:

```
ALU(config-controller T1)# no clocksource
```


To CONFIGURE A SERIAL INTERFACE

Command (in CM)	Description
<code>interface Serial <slot/ port:channel></code>	This command is entered in the Interface configuration mode to configure a serial interface.

EXAMPLE

The following example creates an interface at slot 0 and port 0 at group 0:

```
ALU(config)#interface Serial0/0:0
ALU(config-if Serial0/0:0)#
```

To BRING UP/SHUTDOWN THE INTERFACE

Command (in ICM)	Description
<code>no shutdown</code>	This command is entered in the interface configuration mode to bring up the interface.
<code>shutdown</code>	This command is entered in the interface configuration mode to shutdown the interface.

EXAMPLE

```
ALU(config-if Serial0/0:0)# no shutdown
```

```
ALU(config-if Serial0/0:0)# shutdown
```

To SET ENCAPSULATION ON THE INTERFACE

Command (in ICM)	Description
<code>encapsulation {frame-relay ppp hdlc mlfr <bundle_id> mlppp <bundle_id>}</code>	This command is entered in the interface configuration mode to set encapsulation to the interface.
<code>no encapsulation</code>	The “no” command sets the encapsulation to its default. The default encapsulation is HDLC.

EXAMPLE

```
ALU(config-if Serial0/0:0)# encapsulation frame-relay
```

```
ALU(config-if Serial0/0:0)# encapsulation ppp
```

```
ALU(config-if Serial0/0:0)# no encapsulation
```

To CONFIGURE MTU ON THE INTERFACE

Command (in ICM)	Description
<code>mtu <64-1500></code>	This command is used to configure the MTU value on the serial interface, i.e., the maximum size of the transmitted layer 2 payload.
<code>no mtu</code>	The “no” command sets the MTU to its default. The default MTU is 1500 bytes.

EXAMPLE

```
ALU(config-if Serial0/0:0)# mtu 100
```

```
ALU(config-if Serial0/0:0)# no mtu
```

T1 SHOW COMMANDS

TO VIEW THE CONTROLLER CONFIGURATION

Command (in SUM)	Description
<code>show controller</code>	This command displays controller status that is specific to the controller hardware.

The show controllers command displays the status of T1 controllers and displays information about clocksources and other settings for the ports.

EXAMPLE

ALU# show controller

T1 1/0 is administratively down.

T1 1/1 is administratively down.

T1 1/2 is up.

Line Card type is Channelized T1

Cablelength is long 0db

No Alarm Detected

Framing is esf, Line Code is b8zs, Clock Source is internal

Total Data (Since last clearing of counters)

0 Line Code Violation, 0 Framing Errors

0 Out of Frame, 0 Bit Errors

T1 1/3 is administratively down.

ALU# show controller T1 1/2

T1 1/2 is up.

Line Card type is Channelized T1

Cablelength is long 0db

No Alarm Detected

Framing is esf, Line Code is b8zs, Clock Source is internal

Total Data (Since last clearing of counters)

0 Line Code Violation, 0 Framing Errors

0 Out of Frame, 0 Bit Errors

TO VIEW INTERFACE CONFIGURATION

Command (in SUM)	Description
show interfaces <name>	This command displays the configuration of the specified interface.

EXAMPLE

This example shows the details of the interface specified.

```

ALU# show interfaces Serial 1/2:0
Serial1/2:0 is up, line protocol is up
  Internet address is 1.1.1.1/24
  MTU 1500 bytes, BW 64 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Loopback not set
  Encapsulation hdlc,   keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/
max) 0 drops
    Conversations: 0/0/0/0 (active/max active/max total)
    Reserved Conversations: 0/0 (allocated/max allocated)
    Available Bandwidth 64 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    7 packets input, 154 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    7 packets output, 154 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  Timeslot(s) Used:1 (64Kbps each), Transmitter delay is 0 flags

```

TROUBLESHOOTING T1 LINES

This section lists the commands to troubleshoot the T1 line cards.

To ENABLE LOOPBACK

Command (in CCM)	Description
<code>loopback {local network {line payload} remote {line- payload}}</code>	Use the loopback controller configuration command to put the T1 or E1 line into loopback mode. It can be used to verify connectivity.
<code>no loopback</code>	The “no” command disables the loopback mode set on the interface. The default loopback for T1 lines is Local.

EXAMPLE

The following example establishes a loopback of the incoming T1 signal on controller T1 0:

```
ALU(config)# controller T1 0/0
ALU(config-controller T1)# loopback network payload
```

The following example disables the loopback on the controller T1 0:

```
ALU(config)# controller T1 0/0
ALU(config-controller T1)# no loopback
```


CHAPTER 12 SERIAL LINE CARDS

This chapter describes configuration of the Serial Line Cards (V.35/ X.21). This chapter includes the configuration steps, CLI syntax with its description and configuration examples. The commands are described in sequential order of configuration.

For instructions on using the commands and to get a detailed description on each of their parameters, refer to the Serial Line Cards chapter in the **OmniAccess 700 CLI Command Reference Guide**.

CHAPTER ORGANIZATION

This chapter is divided into the following sections.

- **“Serial Line Card (V.35/X.21) Overview”**
- **“Alcatel-Lucent Specific Overview”**
- **“V.35/X.21 Configuration”**
- **“V.35/X.21 Configuration Commands”**

CHAPTER CONVENTIONS

Acronym	Description
CRC	Cyclic Redundancy Check
DCE	Data Circuit-Terminating Equipment
DTE	Data Terminal Equipment
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
OIR	Online Insertion and Removal
RxC	Receive Clock
TxC	Transmit Clock

SERIAL LINE CARD (V.35/X.21) OVERVIEW

In synchronous communications, data is sent as frames of sizes that vary from a few bytes through 1500 bytes for Ethernet or 4096 bytes for most Frame Relay systems. The clock is embedded in the data stream encoding, or provided on separate clock lines such that the sender and receiver are always in synchronization during a frame transmission.

There are two types of devices that communicate over a Serial Interface: DTE (Data Terminal Equipment) and DCE (Data Circuit-Terminating Equipment).

A DTE connects to a network through a DCE device. In a typical scenario, a DTE device is connected to a DCE device. The DCE device provides a clock signal that paces the communication between the device and the router.

V.35 and **X.21** are well known communication protocols over synchronous serial lines.

- **V.35 Interface**

The V.35 interface was originally specified by CCITT as an interface for 48kbps line transmissions. It has been adopted for all line speeds above 20kbps.

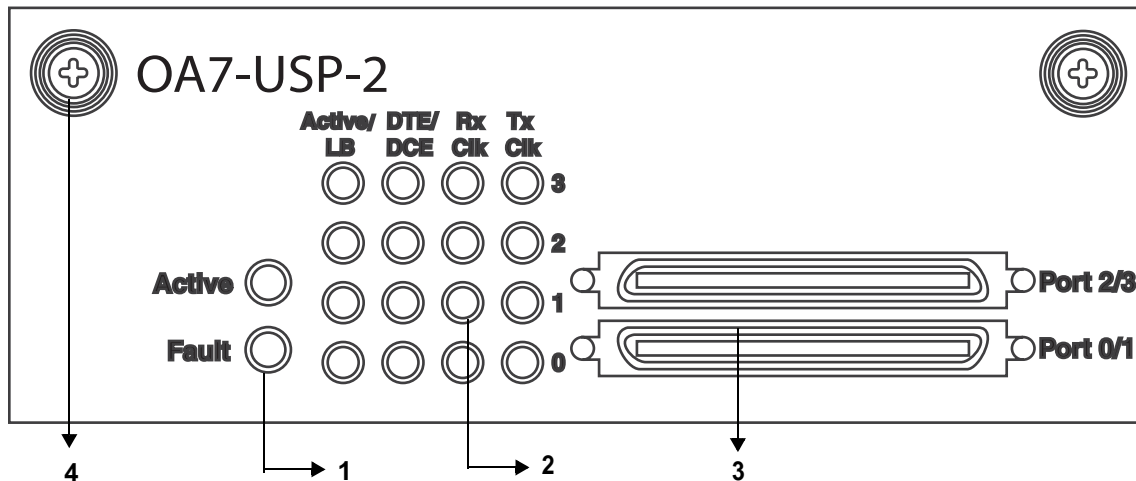
V.35 is a mixture of balanced and common earth signal interfaces. The control lines including DTR, DSR, DCD, RTS, and CTS are single wire common earth interfaces. The data and clock signals are balanced signals.

- **X.21 Interface**

The physical interface between the DTE and the DCE is defined in ITU-T recommendation X.21. The DCE provides a full-duplex, bit-serial, synchronous transmission path between the DTE and the local PSE.

ALCATEL-LUCENT SPECIFIC OVERVIEW

The Serial Line Card provides up to 4 synchronous serial interfaces for the OA-780 and OA-740 platform. Each interface supports full-duplex operation at speeds up to 2 Mbps. The card has 2 external ports/connectors. The serial cable that is connected to each port/connector provides 2 ports and determines the physical interfaces type (V.35 or X.21) and mode of operation (DTE/DCE).



1. V.35/X.21 Card LEDs
2. V.35/X.21 Port LEDs
3. 68 pin VHDCI Connector
4. Thumb Screw

Figure 24: Serial Line Card (V.35/X.21)



Note: For information on the pin out connection and the LED status of the Serial Line Card with respect to each port, please refer the “**OA-780/OA-740 Hardware Users Guide**”.

FEATURE SUPPORTED

The serial card provides the following features:

- V.35 and X.21 physical interfaces
- DTE and DCE modes
- Data rate up to 2 Mbps per interface
- Layer2 protocols - HDLC, PPP, Frame Relay, Multilink PPP, Multilink Frame Relay on each serial interface
- OIR of the line card

V.35/X.21 CONFIGURATION

Refer to the following sections to configure V.35/X.21 interface on OA-700:

- [“V.35/X.21 Interface Configuration Steps”](#)
- [“V.35/X.21 Configuration Flow”](#)
- [“V.35/X.21 DTE and DCE CLI Configuration Commands”](#)

V.35/X.21 INTERFACE CONFIGURATION STEPS

This section lists the instructions to configure **V.35/X.25** interface.

Step 1: Enter Configuration Mode

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure a Serial interface. See [“To Configure a Serial Interface”](#)

Step 3: Administratively bring up the interface. See [“To Bring Up/Down a Serial \(V.35/X.21\) Interface”](#)

Step 4: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if Serial0/0)# ip address 20.20.20.20/24
```

Step 5: Configure optional parameters for V.35/X.21 DTE and DCE. See [“V.35/X.21 DTE and DCE CLI Configuration Commands”](#)

- Configure Clock Rate. See [“To Configure Clock Rate”](#)
- Configure CRC. See [“To Configure CRC”](#)
- Configure Clock Inversion. See [“To Configure Invert Transmit Clock”](#)
- Configure Loopback. See [“To Configure Loopback”](#)
- Set Encapsulation. See [“To Set Encapsulation”](#)
- Configure MTU. See [“To Configure MTU”](#)

Step 6: See [Show Interface Details](#) to view the interface configuration.

V.35/X.21 CONFIGURATION FLOW

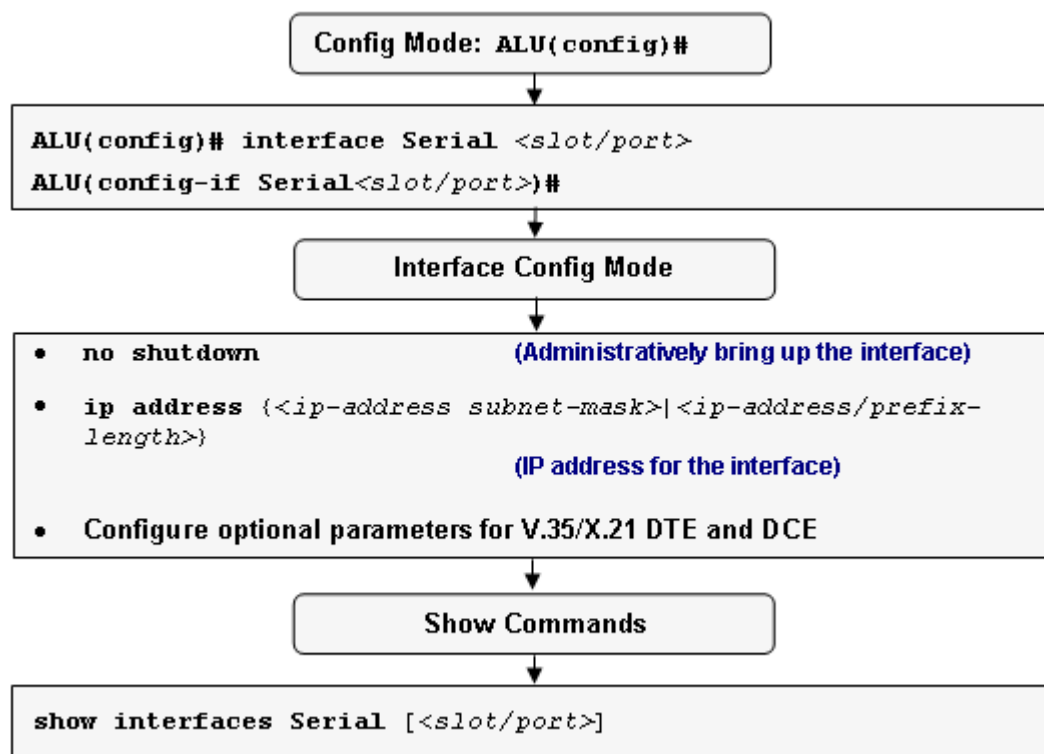


Figure 25: V.35/X.21 Configuration Flow

V.35/X.21 CONFIGURATION COMMANDS

This section provides details about the commands that are used in configuring the V.35/X.21 interface.

TO CONFIGURE A SERIAL INTERFACE

Command (in CM)	Description
<code>interface Serial <slot/port></code>	Enters Serial Interface Configuration Mode. This command is entered in the Configuration Mode to configure a serial interface in a specific slot/port of the V.35/X.21 card.

EXAMPLE

```
ALU(config)#interface Serial0/0
ALU(config-if Serial0/0)#
```

TO BRING UP/DOWN A SERIAL (V.35/X.21) INTERFACE

Command (in ICM)	Description
<code>no shutdown</code>	This command is entered in the interface configuration mode to administratively bring up the interface.
<code>shutdown</code>	This command is entered in the interface configuration mode to administratively bring down the interface.

EXAMPLE

The following example administratively brings up the V.35/X.21 interface

```
ALU(config)#interface Serial 0/0
ALU(config-if Serial0/0)# no shutdown
```

The following example administratively bring down the V.35/X.21 interface

```
ALU(config)#interface Serial 0/0
ALU(config-if Serial0/0)# shutdown
```

V.35/X.21 DTE AND DCE CLI CONFIGURATION COMMANDS

To CONFIGURE CLOCK RATE

The clock rate command enables you to configure the speed of the clock.

Command (in ICM)	Description
<code>clockrate {64000 128000 256000 512000 1024000 2048000}</code>	This command configures the clock rate.
<code>no clockrate {64000 128000 256000 512000 1024000 2048000}</code>	The “no” command sets the clock rate to default 64000 bps.

EXAMPLE

```
ALU(config-if Serial0/0)#clockrate 256000
```

```
ALU(config-if Serial0/0)#no clockrate
```

To CONFIGURE CRC

Command (in ICM)	Description
<code>crc {16 32}</code>	32: This command enables the 32 bit CRC. 16: This command enables the 16 bit CRC.
<code>no crc {16 32}</code>	The “no” command sets CRC to default value 16.

EXAMPLE

```
ALU(config-if Serial0/0)#crc 16
```

```
ALU(config-if Serial0/0)#no crc
```

To CONFIGURE INVERT TRANSMIT CLOCK

When DTE/DCE is using external clock source, long cables at high speed might introduce phase shift in transmitted data and clock. Clock inversion can reduce errors by correcting the phase shift.



Note: By default, the transmit clock is not inverted.

Command (in ICM)	Description
<code>invert-txc</code>	This command inverts the transmit clock to correct phase shift between the clock and the data.
<code>no invert-txc</code>	The “ no ” command will set the clock to original phase.

EXAMPLE

```
ALU(config-if Serial0/0)# invert-txc
```

```
ALU(config-if Serial0/0)#no invert-txc
```

To CONFIGURE LOOPBACK

Loopback command can be used for troubleshooting and diagnostic purpose. When interface is configured in loopback mode, Tx data and Tx clock loop to internal controller as Rx data and Rx clock. In the same way, Rx data and Rx clock on line loop out on line as Tx data and Tx clock.

Command (in ICM)	Description
<code>loopback</code>	This command configures an interface in loopback mode.
<code>no loopback</code>	The “no” command removes the loopback configured on the interface.

EXAMPLE

```
ALU(config-if Serial0/0)# loopback
```

```
ALU(config-if Serial0/0)#no loopback
```

To SET ENCAPSULATION

The encapsulation command is used to set encapsulation on the interface.

Command (in ICM)	Description
<code>encapsulation {frame-relay ppp hdlc mlfr <bundle_id> mlppp <bundle_id>}</code>	Sets the encapsulation on a specified interface.

EXAMPLE

```
ALU(config-if serial 0/0:0)# encapsulation frame-relay
```

To CONFIGURE MTU

The MTU command is used to configure the MTU value on the serial interface, i.e., the maximum size of the transmitted layer 2 payload.

Command (in ICM)	Description
<code>mtu <64-1500></code>	Configures the MTU value on the serial interface.

EXAMPLE

```
ALU(config-if Serial 0/0:0)# mtu 1200
```


SHOW INTERFACE DETAILS

Command (in ICM)	Description
<code>show interfaces Serial [<slot/port>]</code>	Displays the interface details for the specified interface.

EXAMPLE

ALU# show interfaces Serial 0/0

```
Serial0/0 is up, line protocol is up
  X.21 DTE Serial attached
  Internet address is 15.0.0.1/8
  MTU 1500 bytes, BW 2048 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  loopback not set
  Encapsulation hdlc, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue: 0 0 (size/max) 0 drops:Input queue 0/0 (size/max) 0 drops
    Conversations: 0/0/0 (active/max active/max total)
    Reserved Conversations: 0/0 (allocated/max allocated)
    Available Bandwidth 2048 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    12105 packets input, 167342 bytes, 0 no buffer
    0 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    31734317 packets output, 3037327615 bytes, 0 no buffer
    8833175 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```



Note: You can view the details of the interface in the Interface Configuration Mode with a **'show'** command without entering into the user mode.

CLEAR INTERFACE COUNTERS

Command (in ICM)	Description
<code>clear counters Serial <slot/ port></code>	Clears the counters for the specified interface.

EXAMPLE

```
ALU# clear counters Serial 0/0
```



Note: You can clear the counters of the interface in the Interface Configuration Mode with a 'clear' command without entering into the user mode.

CHAPTER 13 HIGH-LEVEL DATA LINK CONTROL

This chapter comprises the commands required to configure a High-level Data Link Control (HDLC) encapsulation on a T1 or E1 interface or a Serial Interface (V.35/X.21). You are required to refer to the [“T1E1 Line Card”](#) and [“Serial Line Cards”](#) chapters before proceeding to this.

This chapter includes a conceptual overview of HDLC and covers an introduction of HDLC architecture with the steps involved to configure HDLC encapsulation with the necessary commands. To get an in-depth view on the description of the argument-list or parameters and the default values, refer to the *OmniAccess 700 CLI Command Reference Guide*.

The [“HDLC Overview” on page 278](#) serves as an additional information on the HDLC protocol. You can skip this section, and go straight to the [“HDLC Configuration” on page 280](#) for configuration details.

CHAPTER CONVENTIONS

Acronym	Description
HDLC	High-level Data Link Control
ICM	Interface Configuration Mode - ALU (config-interface name)#

HDLC OVERVIEW

Layer 2 of the OSI model is the data link layer. One of the most common layer 2 protocols is the High-level Data Link Control (HDLC) protocol. In fact, many other layer 2 protocols are based on HDLC, particularly its framing structure.



Note: The OA-700 supports only Cisco HDLC.

The following sections describe HDLC:

- [“HDLC Frame Structure”](#)
- [“HDLC Frame Formats”](#)
- [“HDLC Protocol Operation”](#)

HDLC FRAME STRUCTURE

HDLC data units transmitted from one station to another are referred to as "frames". The figure shown below is a graphical representation of an HDLC frame with information field.

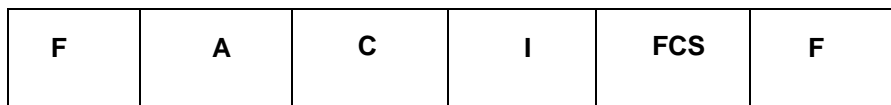


Figure 26: An HDLC frame with an information field

Field Name	Size (in bits)
Flag Field(F)	8 bits
Address Field(A)	8 bits
Control Field(C)	8 or 16 bits
Information Field(I)	Variable; Not used in some frames
Frame Check Sequence(FCS)	16 or 32 bits
Closing Flag Field(F)	8 bits

HDLC FRAME FORMATS

The standard frame of the HDLC protocol handles both data and control messages. The length of the address field is commonly 0, 8, or 16 bits, depending on the data link layer protocol. The 8 or 16 bit control field, provides a flow control number and defines the frame type (control or data). The exact use and structure of this field depends upon the protocol using the frame.

Data is transmitted in the information field, which can vary in length depending upon the protocol using the frame. Layer 2 frames are carried in the information field. Error Control is implemented by appending a Cyclic Redundancy Check (CRC) to the frame, which is 16 bits long in most protocols.

HDLC PROTOCOL OPERATION

HDLC is the default encapsulation on serial lines and it uses HDLC framing with packet contents defined as follows:

- The first ("address") octet is set to 0x0F for unicast packets and 0x8F for broadcast packets.
- The second ("control") octet is always 0.

The next two octets are a 16-bit "protocol code". IP at the higher-level would be represented with the code 0x0800. Bytes after this are higher-level protocol data.

Packets with type 0x8035 carry a protocol referred to as SLARP. SLARP has two functions: IP address determination and serial line keepalive.

For the SLARP keepalive protocol, each system sends the other a keepalive packet at a user-configurable interval. The default interval is 10 seconds.

Both systems must use the same interval to ensure reliable operation. Each system assigns sequence numbers to the keepalive packets it sends, starting with zero, independent of the other system. These sequence numbers are included in the keepalive packets that are sent to the other system. The sequence number of the last keepalive packet received from the peer system is also included in each keepalive packet, as assigned by the peer system. This number is called the returned sequence number. Each system keeps track of the last returned sequence number it has received. Immediately before sending a keepalive packet, the system compares the sequence number of the packet which is about to send with the returned sequence number in the last keepalive packet that is received. If two differ by 3 or more, it considers the serial line as failed, and will not route further higher-level data across it until an acceptable keepalive response is received.

HDLC CONFIGURATION

Refer to the following sections to enable HDLC encapsulation on a T1 or E1 interface or a Serial interface (V.35/X.21):

- [“HDLC Configuration Steps”](#)
- [“HDLC Configuration Flow”](#)
- [“HDLC Configuration Commands”](#)

HDLC CONFIGURATION STEPS

This section lists the commands for HDLC configuration.



Note: The following HDLC configuration commands are shown for a T1 interface as an example. The steps are similar for configuration of HDLC on an E1 interface.

Step 1: Enter Configuration Mode

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure T1 controller

```
ALU(config)# controller T1 <slot/port>
ALU(config-controller T1)#
```

Step 3: Configure the channel-group on the controller before entering the Interface Configuration Mode. This command creates a channel-group that forms a channelized serial interface.

```
ALU(config-controller T1)# channel-group <0-23>
timeslots <1-24> speed [56K|64K]
```



Note: Creation of a channel-group is a pre-requisite for configuring a Serial interface on a T1 or an E1 controller.

Step 4: Administratively bring up the controller

```
ALU(config-controller T1)# no shutdown
```

Step 5: Exit from the controller mode

```
ALU(config-controller T1)# exit
ALU(config)#
```



Note: The above steps can be skipped if the T1 or E1 controller has already been configured. For more details on configuring a T1 or an E1 controller, refer to the [“T1E1 Line Card”](#) chapter.

The above steps can also be skipped if you are configuring HDLC on a **Serial interface (V.35/X.21)**. The steps (**Step 6 - Step 12**) hold good for configuration of HDLC on a V.35/X.21 interface, except that there is no channel group number in the interface name. Configure serial interface using the following command:

```
ALU(config)# interface Serial <slot/port>
ALU(config-if Serial<slot/port>)#
```

Example:

```
ALU(config)#interface Serial0/0
ALU(config-if Serial0/0)#
```

For more details on configuring a Serial interface (V.35/X.21), refer to the [“Serial Line Cards”](#) chapter.

Step 6: Enter Serial interface configuration mode

```
ALU(config)# interface Serial <slot/port:channel>
ALU(config-if Serial<slot/port:channel>)#
```

Example:

```
ALU(config)#interface Serial0/0:0
ALU(config-if Serial0/0:0)#
```

Step 7: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if Serial0/0:0)# no shutdown
```

Step 8: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if Serial0/0:0)# ip address 20.20.20.20/24
```

Step 9: Configure HDLC encapsulation. By default, the system has HDLC encapsulation on an interface. There is no need to explicitly configure it. See [“To Configure HDLC Encapsulation”](#)



Note:

If the encapsulation on the interface is pre-configured for either Frame Relay or PPP (Point to Point), then configure HDLC encapsulation. See [“To Set Encapsulation to its Default \(HDLC\)”](#)

Step 10: Configure the HDLC Keepalive Interval. See [“To Configure HDLC Keepalive Interval”](#) (Optional)

Step 11: Configure loopback detection. See [“To Enable Loopback Detection”](#) command. (Optional)

Step 12: View the status of HDLC. See [“Show Interface Status”](#)

HDLC CONFIGURATION FLOW

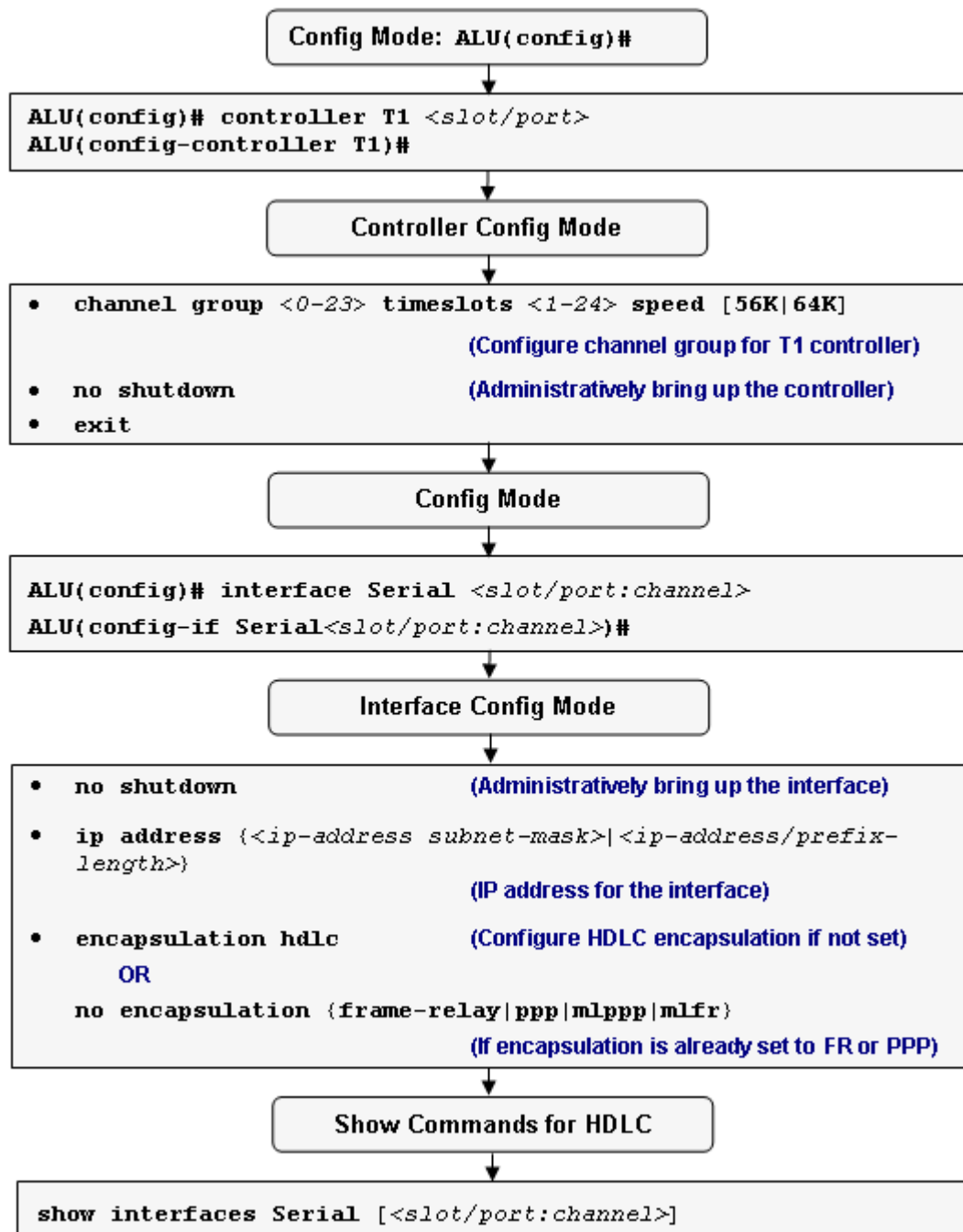


Figure 27: HDLC Configuration Flow

HDLC CONFIGURATION COMMANDS

This section details the HDLC configuration commands.

To SET ENCAPSULATION TO ITS DEFAULT (HDLC)

Enter this command in the Interface Configuration Mode.

Command (in ICM)	Description
<code>no encapsulation {frame-relay ppp mlppp mlfr}</code>	This command is used to configure encapsulation on the interface to HDLC. This command is applicable only if the encapsulation is already set to Frame Relay or PPP.

EXAMPLE

```
ALU(config-if Serial0/0:0)# no encapsulation frame-relay
```

To CONFIGURE HDLC ENCAPSULATION

Command (in ICM)	Description
<code>encapsulation hdlc</code>	This command is entered in the Interface Configuration Mode. This command is used to configure encapsulation on an interface to HDLC.

EXAMPLE

```
ALU(config-if Serial0/0:0)# encapsulation hdlc
```

To CONFIGURE HDLC KEEPALIVE INTERVAL

Enter this command in the Interface Configuration mode.

Command (in ICM)	Description
<code>hdlc keepalive <0-32767></code>	This command configures the HDLC keepalive interval. The same value shall be configured on the peer. A value of '0' turns off the keepalive feature.
<code>no hdlc keepalive</code>	This command resets the keepalive interval to its default. The default keepalive interval is 10 seconds .

EXAMPLE

The following example sets the keepalive interval to 12:

```
ALU(config-if Serial0/0:0)# hdlc keepalive 12
```

To ENABLE LOOPBACK DETECTION

Command (in ICM)	Description
<code>hdlc down-when-looped</code>	This command is used to bring down the line protocol when loopback is detected on the interface.
<code>no hdlc down-when-looped</code>	This command disables bringing down of the line protocol when loopback is detected on the interface. This is the default behavior.

EXAMPLE

```
ALU(config-if Serial0/0:0)# no hdlc down-when-looped
```

HDLC SHOW COMMANDS

SHOW INTERFACE STATUS

Command (in SUM/CM)	Description
<code>show interfaces Serial [<slot/ port:channel>]</code>	Use this command to verify if HDLC is the current encapsulation on the interface, and to check the interface details.

EXAMPLE

ALU# show interfaces Serial 0/0:0

```
Serial0/0:0 is up, line protocol is up
 Internet address is 7.7.7.1/24
 MTU 1500 bytes, BW 1536 Kbit, DLY 0 usec,
   reliability 255/255, txload 0/255, rxload 2/255
 Loopback not set
 Encapsulation hdlc, keepalive set (10 sec)
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Queueing strategy: fifo
 Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/
max) 0 drops
   Conversations: 0/0/0/0 (active/max active/max total)
   Reserved Conversations: 0/0 (allocated/max allocated)
   Available Bandwidth 1536 kilobits/sec
 5 minute input rate 16 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
   370 packets input, 8880 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0
abort
   367 packets output, 8074 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
   0 carrier transitions
 Timeslot(s) Used:1-24 (64Kbps each), Transmitter delay is 0
flags
ALU#
```

HDLC DEBUG COMMANDS

To ENABLE DEBUGGING ON HDLC

Command (in SUM or CM)	Description
<code>debug hdlc all [detail-level <1-9>]</code>	This command shows all the debug messages pertaining to HDLC functionality.
<code>debug hdlc keepalive [output {all log vty}]</code>	This command shows the HDLC keepalive messages.

EXAMPLE

```
ALU(config)# debug hdlc all
```

```
ALU(config)# debug hdlc keepalive
```

To DISABLE DEBUGGING ON HDLC

Command (in SUM or CM)	Description
<code>no debug hdlc {all keepalive}</code>	The “ no ” command disables the debug functionality. By default, debug is disabled.

EXAMPLE

```
ALU(config)# no debug hdlc all
```


CHAPTER 14 FRAME RELAY

This chapter includes the commands for configuring Frame Relay (FR) encapsulation on a T1 or E1 interface or a Serial (V.35/X.21) interface. You are required to refer to the **“T1E1 Line Card”** and **“Serial Line Cards”** chapters before proceeding to this.

This chapter includes instructions for configuring Frame Relay Local Management Interface and Data-link Connection Identifiers on an interface/sub-interface through the CLI. For instructions on using the FR commands and descriptions on each of their parameters with the corresponding default values for each, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

The overview section serves only as an additional information on the FR protocol. You can skip this section and directly proceed to **“Frame Relay Configuration”** section.

This chapter is divided into the following sections:

- **“Frame Relay Overview”**
- **“Frame Relay Configuration”**

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU #
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
S-ICM	Sub-Interface Configuration Mode - ALU (config-subif serial slot/port:channel.subchannel)#
DLCI	Data-link Connection Identifier
LMI	Local Management Interface

FRAME RELAY OVERVIEW

FR is a WAN protocol that operates at the physical and data-link layers of the OSI reference model. This protocol was originally designed for use across ISDN interfaces but today it is used over a variety of other network interfaces as well.

The following sections provide an overview of the FR encapsulation:

- [“Frame Relay Devices”](#)
- [“Frame Relay Virtual Circuits”](#)
- [“Frame Relay Network Deployments”](#)

FRAME RELAY DEVICES

Devices attached to a FR WAN fall into two general categories:

- **DTE** - These are considered to be the terminating equipment for a specific network and typically located on the customer premises.
- **DCE** - These are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network.

FRAME RELAY VIRTUAL CIRCUITS

FR provides connection-oriented data-link layer communication. This means that a defined connection exists between each pair of devices and that each such connection is associated with a connection identifier. This service is implemented by using the FR virtual circuit, which is essentially a logical connection created between two DTEs. A virtual circuit provides for a bi-directional communication path between one DTE device and another, and is uniquely identified by a DLCI.

Virtual circuits are of two types:

- **Switched Virtual Circuits (SVC)** - These are temporary connections used in situations requiring only sporadic data transfer between DTE devices across FR network. The actual deployment of SVCs is minimal in today's FR network.
- **Permanent Virtual Circuits (PVC)** - These are permanently established connections that are used for frequent and consistent data transfers between DTE devices across a FR network.

FRAME RELAY NETWORK DEPLOYMENTS

A typical FR network consists of a number of DTE devices, such as routers, connected to remote ports on multiplexer equipment via traditional point-to-point services such as T1, Fractional T1, or 56 Kb circuits. FR is deployed in both public carrier-provided networks and in private enterprise networks.

- **Public Carrier-Provided Networks** - The Frame Relay switching equipment is located in the central office of a telecommunications carrier. Subscribers are charged based on their network use but are relieved from administering and maintaining the Frame Relay network equipment and service. Generally, the DCE equipment is owned by the telecommunications provider, and the DTE equipment is owned by the customer or leased from the service provider. The majority of today's FR networks are public carrier-provided networks.
- **Private Enterprise Networks** - In private FR networks, the administration and maintenance of the network is the responsibility of an enterprise.

FRAME RELAY CONFIGURATION

Refer to the following sections to enable FR encapsulation on a T1 or E1 line card:

- [“Frame Relay Configuration Steps”](#)
- [“Frame Relay Configuration Flow”](#)
- [“Frame Relay Commands”](#)

FRAME RELAY CONFIGURATION STEPS

This section lists the commands for configuring FR.



Note: The following FR configuration commands are shown for a T1 interface as an example. The steps are similar for configuration of FR on an E1 interface.

Step 1: Enter the Configuration Mode

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure T1 controller

```
ALU(config)# controller T1 <slot/port>
ALU(config-controller T1)#
```

Step 3: Configure the channel-group on the controller before entering the Interface Configuration mode. This command creates a channel-group that will form a channelized serial interface.

```
ALU(config-controller T1)# channel group <0-23>
timeslots <1-24> speed [56K|64K]
```



Note: Creation of a channel-group is a pre-requisite for configuring a Serial Interface on a T1 or an E1 controller.

Step 4: Administratively bring up the controller

```
ALU(config-controller T1)# no shutdown
```

Step 5: Exit from the controller mode

```
ALU(config-controller T1)# exit
ALU(config)#
```



Note: The above steps can be skipped if the T1 or E1 controller has already been configured. For more details on configuring a T1 or an E1 controller, refer to the [“T1E1 Line Card”](#) chapter.

The above steps can also be skipped if you are configuring FR on a **Serial interface (V.35/X.21)**. The steps (**Step 6 - Step 12**) hold good for configuration of FR on a V.35/ X.21 interface, except that there is no channel group number in the interface name. Configure a serial interface using the following command:

```
ALU(config)# interface Serial <slot/port>
ALU(config-if Serial<slot/port>)#
```

Example:

```
ALU(config)#interface Serial0/0
ALU(config-if Serial0/0)#
```

For more details on configuring a Serial interface (V.35/X.21), refer to the [“Serial Line Cards”](#) chapter.

Step 6: Enter the Serial interface configuration mode

```
ALU(config)# interface Serial <slot/port:channel>
ALU(config-if Serial<slot/port:channel>)#
```

Example:

```
ALU(config)#interface Serial0/0:0
ALU(config-if Serial0/0:0)#
```

Step 7: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if Serial0/0:0)# no shutdown
```

Step 8: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if Serial0/0:0)# ip address 20.20.20.20/24
```

Step 9: Configure Frame Relay encapsulation. See [“To Enable FR Encapsulation on an Interface”](#)

Step 10: Configure Frame Relay LMI (Local Management Interface). See [“Local Management Interface \(LMI\)” \(Optional\)](#)

Step 11: Configure Data-link Connection Identifier (DLCI) on the interface. See [“Data-Link Connection Identifier”](#)



Note: FR DLCI can also be configured on a sub-interface. Multiple sub-interfaces with different FR DLCI are also configurable.

Step 12: View the status of the Frame Relay protocol on a specified interface. See [“Frame Relay Show Commands”](#)

FRAME RELAY CONFIGURATION FLOW

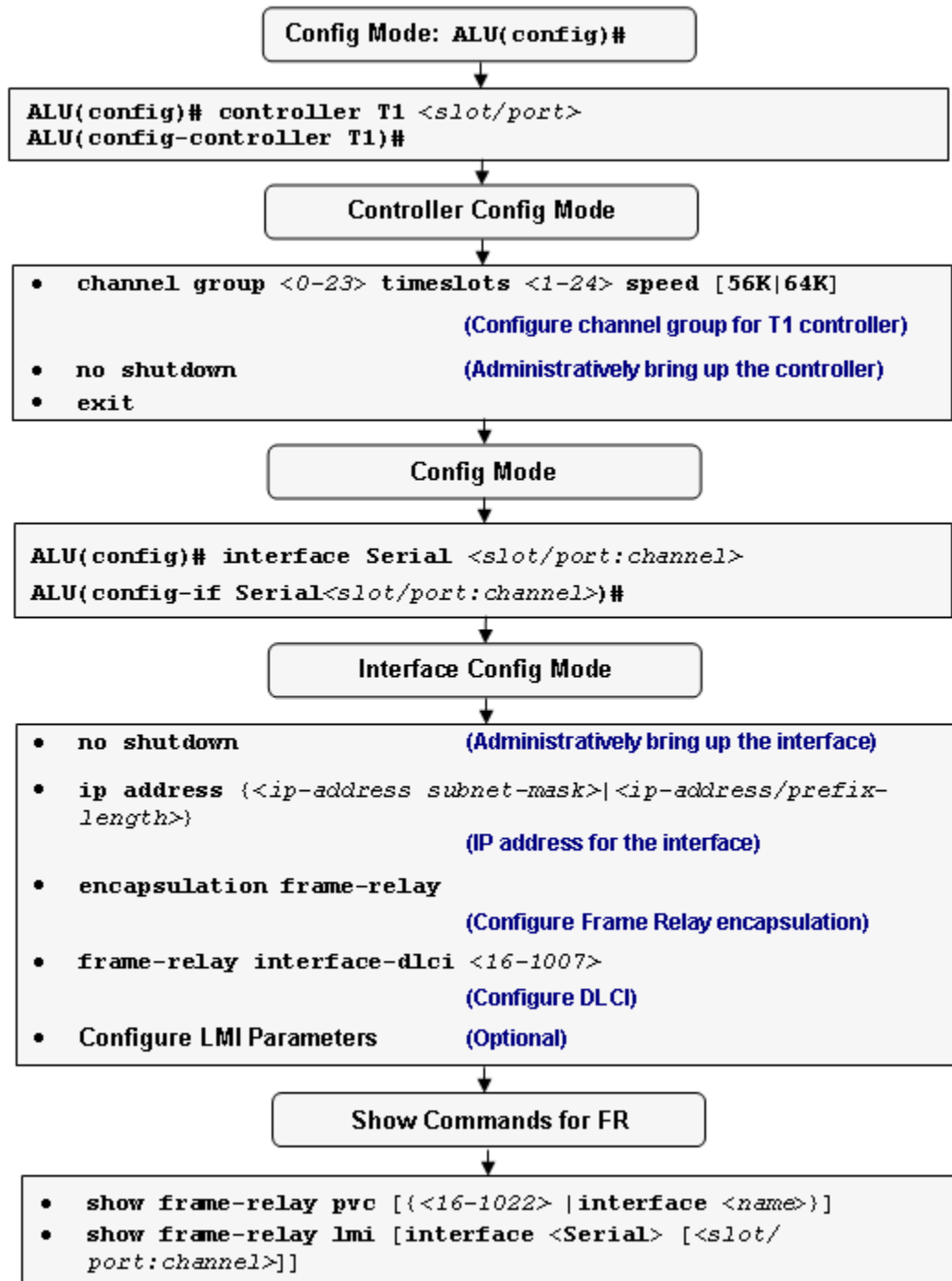


Figure 28: FR Configuration Flow

FRAME RELAY COMMANDS

This section provides details about the commands that are used in configuring Frame Relay encapsulation.

TO ENABLE FR ENCAPSULATION ON AN INTERFACE

This command is entered in the Interface Configuration mode.

Command (in ICM)	Description
<code>encapsulation frame-relay</code>	This command is entered in the Interface Configuration mode. This command is used to set encapsulation on an interface to Frame Relay.
<code>no encapsulation frame-relay</code>	The “no” command resets the encapsulation to its default. The default encapsulation on a serial interface is HDLC.

EXAMPLE

```
ALU(config-if Serial 0/0:0)# encapsulation frame-relay
```

```
ALU(config-if Serial 0/0:0)# no encapsulation frame-relay
```

LOCAL MANAGEMENT INTERFACE (LMI)

The LMI is a set of enhancements to the basic FR specification. It provides a number of features for managing complex networks. LMI virtual circuit status messages provide communication and synchronization between FR DTE and DCE devices. These messages are used to periodically report on the status of the PVCs. This prevents data from being sent into black holes.

TO CONFIGURE LMI TYPE

Enter this command in the Interface Configuration mode.

Command (in ICM)	Description
<code>frame-relay lmi-type {ansi/q933a}</code>	This command is used to set the LMI type to either ANSI or Q933A.
<code>no frame-relay lmi-type</code>	The "no" command sets the LMI type to its default value. The default LMI type is auto-sense .



Note: LMI Autosense is activated by default as the system acts as a DTE. The LMI autosense will be activated when the physical interface is up and LMI type is not configured on that interface.

EXAMPLE

The following example sets the LMI to ANSI standard:

```
ALU(config-if Serial0/0:0)# frame-relay lmi-type ansi
```

The following example sets the LMI-type to its default, i.e., auto-sense:

```
ALU(config-if Serial0/0:0)# no frame-relay lmi-type
```

To CONFIGURE THE LMI KEEPALIVE VALUE

Enter this command in the Interface Configuration mode.

Command (in ICM)	Description
<code>frame-relay keepalive <0-32767></code>	This command is used to configure the LMI Keepalive interval. The default LMI Keepalive value is 10 .
<code>no frame-relay keepalive</code>	The “ no ” command resets the LMI Keepalive interval to ‘0’.

The LMI keepalive value should typically be equal to the corresponding interval at the switch.

EXAMPLE

The following example sets the LMI keepalive interval to 12:

```
ALU(config-if Serial0/0:0)#frame-relay keepalive 12

ALU(config-if Serial0/0:0)# no frame-relay keepalive
```

To SET A FULL STATUS POLLING INTERVAL

Enter this command in the Interface Configuration mode.

Command (in ICM)	Description
<code>frame-relay lmi-n391dte <1-255></code>	This command is used to set the full status polling interval on a DTE interface.
<code>no frame-relay lmi-n391dte</code>	The “ no ” command sets the polling interval to its default value. The default polling interval is 6 .

EXAMPLE

The following example sets the polling interval to 8:

```
ALU(config-if Serial0/0:0)#frame-relay lmi-n391dte 8
```

The following example sets the polling interval to default, i.e., 6:

```
ALU(config-if Serial0/0:0)# no frame-relay lmi-n391dte
```


To SET DTE ERROR THRESHOLD

This command is entered in the Interface Configuration mode.

Command (in ICM)	Description
<code>frame-relay lmi-n392dte <1-10></code>	This command sets the DTE error threshold.
<code>no frame-relay lmi-n392dte</code>	The “no” command sets the error threshold to its default value. The default value is 3 .

EXAMPLE

The following example sets the DTE error threshold to 6:

```
ALU(config-if Serial0/0:0)# frame-relay lmi-n392dte 6
```

The following example sets the DTE error threshold to default, i.e., 3:

```
ALU(config-if Serial0/0:0)# no frame-relay lmi-n392dte
```

To SET DTE MONITORED EVENT COUNT

Command (in ICM)	Description
<code>frame-relay lmi-n393dte <1-10></code>	This command sets the DTE monitored events count.
<code>no frame-relay lmi-n393dte</code>	The “no” command sets the lmi-n393dte to its default value. The default value is 4 .

EXAMPLE

The following example sets the DTE monitored events count to 7:

```
ALU(config-if Serial0/0:0)# frame-relay lmi-n393dte 7
```

The following example sets the lmi-n393dte to its default value, i.e., 4:

```
ALU(config-if Serial0/0:0)# no frame-relay lmi-n393dte
```

DATA-LINK CONNECTION IDENTIFIER

FR virtual circuits are identified by DLCIs. These values are typically assigned by the FR service provider. The DLCIs have a local significance, which means their values are unique to the link.



Note: The system provides support for point-to-point FR DLCIs only. A DLCI is configured on an interface or a sub-interface.

To CONFIGURE DLCI

Command (in ICM/Sub-ICM)	Description
<code>frame-relay interface-dlci</code> <16-1007>	This command is used to configure a DLCI on an interface/sub-interface.
<code>no frame-relay interface-dlci</code> <16-1007>	The “no” command deletes the configured DLCI from the interface.

EXAMPLE

The following example sets the DLCI value to 100:

```
ALU(config-if Serial 0/0:0)# frame-relay interface-dlci 100
```

The following example deletes the DLCI configured:

```
ALU(config-if Serial 0/0:0)# no frame-relay interface-dlci
100
```

Note: FR can also be configured on a sub-interface. And, multiple sub-interfaces with FR can be configured.

For configuring Frame Relay on a sub-interface, follow the steps given below:

Step 1: Repeat the steps **Step 1 to Step 7** as given in the section “[Frame Relay Configuration Steps](#)”

Step 2: Configure sub-interface on a serial interface.

```
ALU(config)# interface Serial <slot/port:channel.subchannel>
ALU(config-if Serial <slot/port:channel.subchannel>)#
```

Example:

```
ALU(config)# interface Serial 0/0:0.1
ALU(config-if Serial0/0:0.1)#
```

Step 3: Configure IP address for the sub-interface

```
ALU(config-if Serial <slot/port:channel.subchannel>)# ip
address {<ip-address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if Serial0/0:0.1)# ip address 124.123.10.1  
255.255.253.3
```

Step 4: Repeat **Step 11** as given in the section **“Frame Relay Configuration Steps”**

- Configure DLCI on the sub-interface



Note: If you are configuring FR on a sub-interface on a **Serial interface (V.35/X.21)**, configure a sub-interface using the following command:

```
ALU(config)# interface Serial <slot/port>.subchannel  
ALU(config-if Serial<slot/port.subchannel>)#
```

Example:

```
ALU(config)#interface Serial0/0.1  
ALU(config-if Serial0/0.1)#
```

FRAME RELAY SHOW COMMANDS

The following commands are used to view the FR configuration details:

To VIEW FRAME RELAY PVC

Command (in SUM/CM)	Description
<code>show frame-relay pvc</code> [<code>{<16-1022></code> <code>/interface <name>}</code>]	This command displays the status of the Frame Relay Permanent Virtual Circuit (PVC).

EXAMPLE

The following example displays the status of the PVC identified by DLCI 200:

```
ALU(config-if Serial0/0:0)# show frame-relay pvc interface
Serial 0/0:0
```

```
PVC Statistics for interface Serial0/0:0 (Frame Relay DTE)
DLCI = 200, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0:0
  input pkts      0          output pkts      0
  in bytes        0          out bytes        0
  in pkts dropped 0          out pkts dropped 0

  in FECN pkts   0          out FECN pkts   0
  in BECN pkts   0          out BECN pkts   0
  in DE pkts     0          out DE pkts     0
  out bcast pkts 0          out bcast bytes 0
```

```
ALU(config-if Serial0/0:0)#
```

To VIEW FR LMI DETAILS

Command (in SUM/CM)	Description
show frame-relay lmi [interface <Serial> [<i><slot/ port:channel></i>]]	This command displays the FR LMI configuration details and parameters.

EXAMPLE

The following example displays the FR LMI configuration details and parameters for all the interfaces:

```
ALU(config-if Serial0/0:0)#show frame-relay lmi
```

```
LMI Statistics for interface Serial0/0:0 (Frame Relay DTE)
LMI TYPE = AUTOSENSE
Invalid Unnumbered info      0  Invalid Prot Disc          0
Invalid dummy Call Ref       0  Invalid Msg Type           0
Invalid Status Message       0  Invalid Lock Shift         0
Invalid Information ID        0  Invalid Report IE Len     0
Invalid Report Request        0  Invalid Keep IE Len        0
Num Status Enq. Sent         0  Num Status msgs Rcvd       0
Num Update Status Rcvd       0  Num Status Timeouts        0
```

The following example displays the FR LMI configuration details and parameters for a specific interface:

```
ALU(config-if Serial0/0:0)#show frame-relay lmi interface  
Serial 0/0:0
```

```
LMI Statistics for interface Serial0/0:0 (Frame Relay DTE)
LMI TYPE = AUTOSENSE
Invalid Unnumbered info      0  Invalid Prot Disc          0
Invalid dummy Call Ref       0  Invalid Msg Type           0
Invalid Status Message       0  Invalid Lock Shift         0
Invalid Information ID        0  Invalid Report IE Len     0
Invalid Report Request        0  Invalid Keep IE Len        0
Num Status Enq. Sent         0  Num Status msgs Rcvd       0
Num Update Status Rcvd       0  Num Status Timeouts        0
```

FR DEBUG COMMANDS

TO ENABLE DEBUGGING ON FR

Command (in SUM or CM)	Description
<code>debug frame-relay all [detail-level <1-9>]</code>	This command shows all the debug messages pertaining to FR functionality.
<code>debug frame-relay {fse keepalive mlfr} [{output {all log vty {<1-256> all console this}}}]</code>	This command shows the debug FR Full Status/Keepalive/Multi-Link Protocol messages.

EXAMPLE

```
ALU(config)# debug frame-relay all
```

```
ALU(config)# debug frame-relay fse
```

TO DISABLE DEBUGGING ON FR

Command (in SUM or CM)	Description
<code>no debug frame-relay {all fse keepalive mlfr}</code>	The “no” command disables the debug functionality. By default, debug is disabled.

EXAMPLE

```
ALU(config)# no debug frame-relay all
```

CHAPTER 15 POINT-TO-POINT PROTOCOL

This chapter includes the commands for configuring Point-to-Point Protocol (PPP) encapsulation on a T1 or E1 interface or a Serial Interface (V.35/X.21). You are required to refer to the **“T1E1 Line Card”** and **“Serial Line Cards”** chapters before proceeding to this.

This chapter includes steps to configure PPP (LCP, IPCP, Timers and Counters, authentication), and troubleshoot PPP through the CLI. For instructions on using the PPP commands and descriptions on each of their parameters, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

Refer to the following to configure PPP encapsulation on an interface:

- **“PPP Overview”**
- **“PPP Configuration”**

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
CHAP	Challenge Handshake Authentication Protocol
EAP	Extensible Authentication Protocol
HDLC	High Level Data Link Control
ICM	Interface Configuration Mode - ALU (config-interface name)#
IPCP	IP Control Protocol
LCP	Link Control Protocol
NCP	Network Control Protocol
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
SUM	Super User Mode - ALU #

PPP OVERVIEW

The PPP protocol emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, network protocol multiplexing, link configuration, link quality testing, error detection and option negotiation for such capabilities as network layer address and data compression. PPP supports these functions by providing an extensible LCP and a family of NCPs to negotiate optional configuration parameters and facilities. PPP supports IP through IPCP.

PPP and its associated protocols are specified in the following IETF documents:

- PPP (RFC 1661)
- PPP in HDLC-like framing (RFC 1662)
- IPCP (RFC 1332)
- PAP (RFC 1334)
- CHAP (RFC 1994)
- EAP (RFC 3748)

The Alcatel-Lucent implementation of PPP conforms to the above specifications.

PPP COMPONENTS

PPP provides a method for transmitting datagrams over point-to-point links. On a serial interface, PPP contains four main components:

- **HDLC-like Framing** - PPP uses framing similar to HDLC as a basis for encapsulating datagrams over serial links. (For more information, see [“High-level Data Link Control”](#) chapter.)
- **LCP** - PPP uses an extensible LCP to establish, configure, and test data link connection.
- **Authentication** - Authentication protocols PAP, CHAP, EAP are used to authenticate the peer.
- **NCP** - PPP uses a family of NCPs for establishing and configuring different network layer protocols.

PPP OPERATION

To establish communication over a PPP link, the originating PPP peer first sends LCP messages to configure the data link. After the link has been established and optional facilities have been negotiated as needed by LCP, each PPP end-point may authenticate its peer. Then NCP messages are sent to choose and configure one or more network layer protocols.

When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communication until an explicit LCP or NCP message terminates the connection, or until events like user intervention or an expiry of a keep alive timer occur.

PPP CONFIGURATION

- [“PPP Configuration Steps”](#)
- [“PPP Configuration Flow”](#)
- [“PPP Configuration Commands”](#)
- [“PPP Show Commands”](#)

PPP CONFIGURATION STEPS

This section lists the commands for PPP configuration.



Note: The following PPP configuration commands are shown for a T1 interface as an example. The steps are similar for configuration of PPP on an E1 interface.

Step 1: Enter Configuration Mode

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure T1 Controller

```
ALU(config)# controller T1 <slot/port>
ALU(config-controller T1)#
```

Step 3: Configure the channel-group on the controller before entering the Interface Configuration Mode. This command creates a channel-group that forms a channelized serial interface.

```
ALU(config-controller T1)# channel group <0-23>
timeslots <1-24> speed [56K|64K]
```



Note: Creation of a channel-group is a pre-requisite for configuring a Serial Interface on a T1 or an E1 controller.

Step 4: Administratively bring up the controller

```
ALU(config-controller T1)# no shutdown
```

Step 5: Exit from the controller mode

```
ALU(config-controller T1)# exit
ALU(config)#
```



Note: The above steps can be skipped if the T1 or E1 controller has already been configured. For more details on configuring a T1 or an E1 controller, refer to the [“T1E1 Line Card”](#) chapter.

The above steps can also be skipped if you are configuring PPP on a **Serial interface (V.35/X.21)**. The steps (**Step 6 - Step 10**) hold good for configuration of PPP on a V.35/X.21 interface, except that there is no channel group number in the interface name. Configure serial interface using the following command:

```
ALU(config)# interface Serial <slot/port>
ALU(config-if Serial<slot/port>)#
```

Example:

```
ALU(config)#interface Serial0/0
ALU(config-if Serial0/0)#
```

For more details on configuring a Serial interface (V.35/X.21), refer to the [“Serial Line Cards”](#) chapter.

Step 6: Enter the Serial interface configuration mode

```
ALU(config)# interface Serial <slot/port:channel>
ALU(config-if Serial<slot/port:channel>)#
```

Example:

```
ALU(config)#interface Serial0/0:0
ALU(config-if Serial0/0:0)#
```

Step 7: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if Serial0/0:0)# no shutdown
```

Step 8: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if Serial0/0:0)# ip address 20.20.20.20/24
```

Step 9: Set encapsulation to PPP on the interface. See [“To Set PPP Encapsulation on an Interface”](#)**Step 10: Configure PPP Optional Parameters.** See [“PPP Optional Parameters”](#)

- Configure LCP parameters. See [“Link Control Protocol Configuration”](#)
- Configure IPCP parameters. See [“IP Control Protocol \(IPCP\) Configuration”](#)
- Configure Timers and Counters. See [“PPP Counters and Timers Configuration”](#)
- Configure authentication through user name and password. See [“PPP Authentication Configuration”](#)

Step 11: Use the [“PPP Show Commands”](#) to view PPP configuration.

PPP CONFIGURATION FLOW

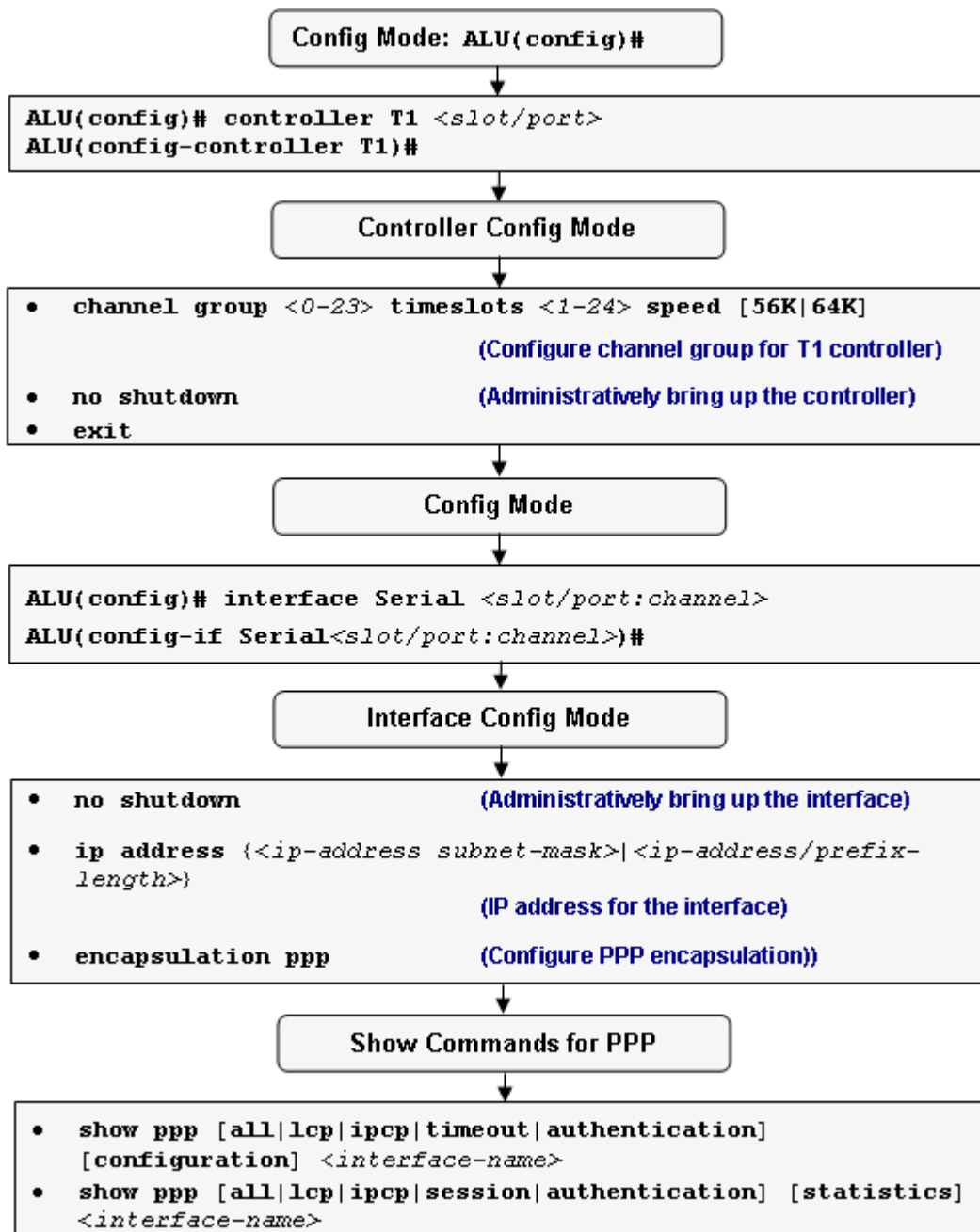


Figure 29: PPP Configuration Flow

PPP CONFIGURATION COMMANDS

For default IP over PPP functionality, you just need to configure the following on a Serial interface:

- Administratively bring up the interface
- Configure IP Address
- Set PPP Encapsulation

The default behavior will be as follows. It will be a PPP end-point that will advertise its configured IP address (or 0.0.0.0 if not configured) during IPCP but not allow its negotiation (no accept-local). It will also not negotiate the peer IP address (accept-peer). There will be no authentication. All timers and counters will be protocol defaults. There will be no compression.

There will be no negotiation of DNS or WINS addresses. LCP negotiation will be attempted max-configure times as soon as encapsulation is changed to PPP, and on failure, it will be further restarted after an interval. Note that all “no” commands for counters and timers reset the parameters to default values.

To SET PPP ENCAPSULATION ON AN INTERFACE

Command (in ICM)	Description
<code>encapsulation ppp</code>	This command is entered in the Interface Configuration Mode. This command sets the encapsulation on an interface to PPP.
<code>no encapsulation ppp</code>	This command sets the encapsulation to its default. The default encapsulation on a serial interface is HDLC.

EXAMPLE

```
ALU(config)# interface Serial1/0:0
ALU(config-if Serial1/0:0)# encapsulation ppp
```

```
ALU(config-if Serial1/0:0)# no encapsulation ppp
```

PPP OPTIONAL PARAMETERS

LINK CONTROL PROTOCOL CONFIGURATION

The LCP (Link Control Protocol) provides a method of establishing, configuring, maintaining, and terminating the PPP connection. In order to be sufficiently versatile and portable to a wide variety of environments, PPP provides the LCP. LCP is used to automatically negotiate the authentication protocol, MRU, or to detect a looped-back link, etc.

TO INITIATE LCP NEGOTIATION MANUALLY

Command (in ICM)	Description
<code>ppp lcp negotiate</code>	This command is used to initiate the LCP negotiation on the interface.

EXAMPLE

```
ALU(config-if Serial1/0:0)# ppp lcp negotiate
```



Note: LCP negotiation is automatically started when the encapsulation is set to PPP or when the link is administratively brought up on a PPP interface, or when the MTU is changed on the interface.

TO SET ECHO-INTERVAL

Command (in ICM)	Description
<code>ppp lcp echo-interval <0-255></code>	This command is used to set the interval between the LCP echo requests sent. "0" implies that no echo requests are sent.
<code>no ppp lcp echo-interval</code>	The "no" command sets the echo-interval to its default value. The default value is 10 seconds .

EXAMPLE

```
ALU(config-if Serial1/0:0)# ppp lcp echo-interval 200
```

```
ALU(config-if Serial1/0:0)# no ppp lcp echo-interval
```

To SET MAX UNANSWERED ECHO REQUESTS

Command (in ICM)	Description
<code>ppp lcp max-echo <0-30></code>	This command denotes the maximum number of unanswered LCP echo requests sent before LCP decides that the peer is down. The value “0” implies that the link will not be brought down on the basis of unanswered echo requests.
<code>no ppp lcp max-echo</code>	The “no” command sets the maximum number of unanswered LCP echo requests to its default, i.e., 5 .

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp lcp max-echo 20
```

```
ALU(config-if Serial0/0:0)# no ppp lcp max-echo
```

To SET LCP RESTART INTERVAL

Command (in ICM)	Description
<code>ppp timeout restart-interval <0-255></code>	This command defines the interval after which the LCP/NCP negotiation will be reattempted after it is terminated.
<code>no ppp timeout restart-interval</code>	The “no” command sets the LCP/NCP restart-interval to its default. The default LCP/NCP restart-interval is 30 seconds.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp timeout restart-interval 10
```

```
ALU(config-if Serial0/0:0)# no ppp timeout restart-interval
```

IP CONTROL PROTOCOL (IPCP) CONFIGURATION

IPCP negotiates IP address assignments. The OA-700 exchanges IPCP messages with the peer for negotiating options relating to IP. The IPCP phase occurs after the LCP phase and the optional authentication phase.

TO INITIATE IPCP NEGOTIATION MANUALLY

Command (in ICM)	Description
<code>ppp ipcp negotiate</code>	This command is used to initiate the IPCP negotiation on the interface.



Note: By default, the OA-700 system responds to IPCP negotiation initiated by the peer. Auto-negotiation happens when the IP address is changed on the interface.

EXAMPLE

```
ALU(config-if Serial1/0:0)# ppp ipcp negotiate
```

TO SET IPCP ADDRESS PARAMETERS

Command (in ICM)	Description
<code>ppp ipcp address accept-local</code>	This command sets a flag to accept a local IP address given to it by the peer during IPCP. By default, the flag is set to reject the local IP address from the peer during IPCP.
<code>no ppp ipcp address accept-local</code>	The “no” command sets the flag to reject the local IP address given to it by its peer during IPCP. This is the default behavior.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp ipcp address accept-local
```

```
ALU(config-if Serial0/0:0)# no ppp ipcp address accept-local
```


To SET IPCP ADDRESS ACCEPT-PEER

Command (in ICM)	Description
<code>ppp ipcp address accept-peer</code>	This command sets the flag to accept the peer's IP address during IPCP. By default, the flag is set to accept the peer's IP address during IPCP.
<code>no ppp ipcp address accept-peer</code>	The "no" command sets the flag to reject the peer's IP address during IPCP.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp ipcp address accept-peer
```

```
ALU(config-if Serial0/0:0)# no ppp ipcp address accept-peer
```

To SET IPCP ADDRESS POOL

Command (in ICM)	Description
<code>ppp ipcp address pool <ip-address></code>	This command enables you to configure an IP address pool for IPCP to give an IP address to its peer. By default, no IP address pool is configured for IPCP.
<code>no ppp ipcp address pool</code>	The "no" command removes the IP address pool for IPCP.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp ipcp address pool 10.10.10.10
```

```
ALU(config-if Serial0/0:0)# no ppp ipcp address pool
```

PPP COUNTERS AND TIMERS CONFIGURATION

This section covers the configuration of PPP Timers and Counters.

TO SET TIMER FOR RETRANSMISSION OF PACKETS

Command (in ICM)	Description
<code>ppp timeout restart-timer <1-30></code>	This command sets a timer for retransmission of LCP and NCP packets.
<code>no ppp timeout restart-timer</code>	The “no” command resets the restart-timer to its default. The default restart-timer value is “ 3 seconds ”.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp timeout restart-timer 13
```

```
ALU(config-if Serial0/0:0)# no ppp timeout restart-timer
```

TO SET TIMEOUT MAX-TERMINATE

Command (in ICM)	Description
<code>ppp timeout max-terminate <1-30></code>	This command sets the maximum number of terminate request packets (LCP or NCP) sent without receiving a Terminate Ack, before assuming that the peer is unable to respond.
<code>no ppp timeout max-terminate</code>	The “no” command sets the max-terminate value to its default. The default max-terminate value is “ 2 seconds ”.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp timeout max-terminate 10
```

```
ALU(config-if Serial0/0:0)# no ppp timeout max-terminate
```

To SET TIMEOUT MAX-CONFIGURE

Command (in ICM)	Description
<code>ppp timeout max-configure <1-30></code>	This command sets the maximum number of configure request packets (LCP or NCP) sent without receiving a valid Ack/NaK/Reject, before assuming that the peer is unable to respond.
<code>no ppp timeout max-configure</code>	The “no” command sets the max-configure value to its default. The default max-configure value is “ 10 seconds ”.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp timeout max-configure 15
```

```
ALU(config-if Serial0/0:0)# no ppp timeout max-configure
```

To SET TIMEOUT MAX-FAILURE

Command (in ICM)	Description
<code>ppp timeout max-failure <1-30></code>	This command sets the maximum number of configure NaK packets (LCP or NCP) sent without sending a Configure Ack before assuming that configuration is not converging.
<code>no ppp timeout max-failure</code>	The “no” command sets the max-failure value to its default. The default max-failure value is “ 5 seconds ”.

EXAMPLE

```
ALU(config-if Serial0/0:0)#ppp timeout max-failure 10
```

```
ALU(config-if Serial0/0:0)# no ppp timeout max-failure
```

PPP AUTHENTICATION CONFIGURATION

On some links, it may be desirable to require a peer to authenticate itself before allowing network-layer protocol packets to be exchanged.

To enable this authentication, PPP supports authentication protocols such as PAP, CHAP, EAP. Authentication is not mandatory.

TO SET PPP AUTHENTICATION

Command (in ICM)	Description
<code>ppp authentication {pap/chap/eap}</code>	This command enables you to configure an authentication protocol for authenticating the peer.
<code>no ppp authentication</code>	The "no" command removes the authentication protocol for authenticating the peer.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp authentication pap
```

```
ALU(config-if Serial0/0:0)# no ppp authentication
```

TO SET THE AUTHENTICATION USER NAME

Command (in ICM)	Description
<code>ppp authentication username <username></code>	This command is used to set a user name for PPP authentication on the server side.
<code>no ppp authentication username</code>	The "no" command deletes the configured PPP authentication user name on the server side.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp authentication username ALU
```

```
ALU(config-if Serial0/0:0)# no ppp authentication username
```

To SET THE AUTHENTICATION PASSWORD

Command (in ICM)	Description
<code>ppp authentication password <password></code>	This command enables you to set a password for PPP authentication on the server side.
<code>no ppp authentication password</code>	The “no” command deletes the configured PPP authentication password on the server side.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp authentication password pass1
```

```
ALU(config-if Serial0/0:0)# no ppp authentication password
```

To SET THE AUTHENTICATION CLIENT USER NAME

Command (in ICM)	Description
<code>ppp authentication client-username <username></code>	This command is used to set user name for PPP authentication on the client side.
<code>no ppp authentication client-username</code>	The “no” command deletes the configured authentication user name on the client side.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp authentication client-username client1
```

```
ALU(config-if Serial0/0:0)# no ppp authentication client-username
```

To SET THE AUTHENTICATION CLIENT-PASSWORD

Command (in ICM)	Description
<code>ppp authentication client-password <password></code>	This command is used to set the password for PPP authentication on the client side.
<code>no ppp authentication client-password</code>	The “no” command deletes the configured authentication password on the client side.

EXAMPLE

```
ALU(config-if Serial0/0:0)# ppp authentication client-password pass1
```

```
ALU(config-if Serial0/0:0)# no ppp authentication client-password
```

PPP SHOW COMMANDS

The following commands are used to view the PPP configuration details and statistics.

To VIEW PPP CONFIGURATION

Command (in SUM/CM)	Description
<code>show ppp all configuration</code> <code><interface-name></code>	Displays all the PPP configuration information for a specified interface.

EXAMPLE

```
ALU# show ppp all configuration Serial 0/0:0
```

```

LCP Max Echoes                : 5
LCP Echo Interval              : 60 (sec)
LCP Restart Interval           : 30 (sec)

IPCP pool IP address           : 50.51.52.54
IPCP local IP address from peer: Reject
IPCP peer IP address           : Reject

PPP Restart timer              : 3 (sec)
PPP Max Terminate              : 2
PPP Max Configure              : 10
PPP Max Failure                : 5

Authentication protocol        : pap
Authentication username        : user1
Authentication password        : secret1
Authentication client-username : user2
Authentication client-password : secret2

```

To VIEW PPP STATISTICS

Command (in SUM)	Description
show ppp all statistics <interface-name>	Displays detailed statistics for PPP for a specified interface.

EXAMPLE

ALU# show ppp all statistics Serial 0/0:0

```
PPP data packets received:      0
PPP control packets received:  22
Packets dropped:                0
```

```
PPP sessions initiated:        1
PPP sessions received:         1
PPP sessions successful:       2
PPP sessions terminated:       1
```

	IN	OUT
LCP Configure Requests:	2	2
LCP Configure Acks:	2	2
LCP Configure Naks:	0	0
LCP Configure Rejects:	0	0
LCP Terminate Requests:	0	0
LCP Terminate Acks:	0	0
LCP Code Rejects:	0	0
LCP Protocol Rejects:	0	0
LCP Echo Requests:	4	4
LCP Echo Replies:	4	4
LCP Discard Requests:	0	0
LCP Invalid Packets:	0	0

	IN	OUT
IPCP Configure Requests:	4	2
IPCP Configure Acks:	2	2
IPCP Configure Naks:	0	2
IPCP Configure Rejects:	0	0
IPCP Terminate Requests:	0	0
IPCP Terminate Acks:	0	0
IPCP Code Rejects:	0	0
IPCP Invalid Packets:	0	0

	IN	OUT
PAP Authentication Requests:	2	2
PAP Authentication Acks:	2	2
PAP Authentication Naks:	0	0
PAP Invalid Packets:	0	0

	IN	OUT
CHAP Challenges:	0	0
CHAP Responses:	0	0
CHAP Successes:	0	0
CHAP Failures:	0	0
CHAP Invalid Packets:	0	0

	IN	OUT
EAP Requests:	0	4
EAP Responses:	4	0
EAP Successes:	0	2
EAP Failures:	0	0
EAP Invalid Packets:	0	0

TO VIEW INTERFACE STATISTICS

Command (in SUM)	Description
show interfaces <name>	Displays detailed statistics and other information for a specified interface.

EXAMPLE

The following example shows the states for LCP, CHAP Client, EAP Server, and IPCP in the "show interfaces" output.

```
ALU(config-if Serial0/0:0)# show interfaces Serial 0/0:0
```

```
Serial0/0:0 is up, line protocol is up
Internet address is 100.101.102.103/24
MTU 1200 bytes, BW 1544 Kbit, DLY 0 usec,
reliability 0/255, txload 0/255, rxload 0/255
  loopback not set
  Encapsulation ppp, Keepalive set (10 sec)
  LCP: Open
  CHAP Client: Open
  EAP Server: Open
  IPCP: Open

Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/max) 0
drops
  Conversations: 0/0/0/0 (active/max active/max total)
  Reserved Conversations: 0/0 (allocated/max allocated)
  Available Bandwidth 1544 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  50 packets input, 0 bytes, 0 no buffer
```



```

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
60 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
Timeslot(s) Used:1-31, Transmitter delay is 0 flags

```

PPP LCP SHOW COMMANDS

The following commands are used to view the PPP LCP configuration details, and statistics:

To VIEW THE PPP LCP CONFIGURATION

Command (in SUM)	Description
<code>show ppp lcp configuration</code> <code><interface-name></code>	Displays the PPP LCP configuration information for a specified interface.

EXAMPLE

```
ALU# show ppp lcp configuration Serial 0/0:0
```

```

LCP Max Echoes      : 5
LCP Echo Interval   : 60 (sec)
LCP Restart Interval : 30 (sec)

```

To VIEW THE PPP LCP STATISTICS

Command (in SUM)	Description
<code>show ppp lcp statistics</code> <code><interface-name></code>	Displays detailed LCP statistics for a specified interface.

EXAMPLE

```
ALU# show ppp lcp statistics Serial 0/0:0
```

```

                                     IN          OUT
LCP Configure Requests:              2          2
LCP Configure Acks:                  2          2
LCP Configure Naks:                   0          0
LCP Configure Rejects:                0          0
LCP Terminate Requests:               0          0
LCP Terminate Acks:                   0          0
LCP Code Rejects:                     0          0
LCP Protocol Rejects:                 0          0
LCP Echo Requests:                    2          2
LCP Echo Replies:                     2          2
LCP Discard Requests:                 0          0
LCP Invalid Packets:                  0          0

```

PPP IPCP SHOW COMMANDS

The following commands are used to view the PPP IPCP configuration and statistics:

To VIEW THE PPP IPCP CONFIGURATION

Command (in SUM)	Description
<code>show ppp ipcp configuration</code> <code><interface-name></code>	Displays PPP IPCP configuration information for a specified interface.

EXAMPLE

```
ALU# show ppp ipcp configuration Serial 0/0:0
```

```
IPCP pool IP address: 50.51.52.54
IPCP local IP address from peer: Reject
IPCP peer IP address: Reject
```

To VIEW THE PPP IPCP STATISTICS

Command (in SUM)	Description
<code>show ppp ipcp statistics</code> <code><interface-name></code>	Displays detailed IPCP statistics for a specified interface.

EXAMPLE

```
ALU# show ppp ipcp statistics Serial 0/0:0
```

	IN	OUT
IPCP Configure Requests:	6	13
IPCP Configure Acks:	6	6
IPCP Configure Naks:	5	0
IPCP Configure Rejects:	2	0
IPCP Terminate Requests:	0	2
IPCP Terminate Acks:	2	0
IPCP Code Rejects:	0	0
IPCP Invalid Packets:	0	0

PPP COUNTERS AND TIMERS SHOW COMMANDS

Command (in SUM)	Description
<code>show ppp timeout configuration</code> <code><interface-name></code>	Displays the timer and counter configuration information for a specified interface.

EXAMPLE

```
ALU# show ppp timeout configuration Serial 0/0:0
```

```
PPP Restart timer: 3 (sec)
PPP Max Terminate: 2
PPP Max Configure: 10
PPP Max Failure : 5
```

TO VIEW THE PPP SESSION STATISTICS

Command (in SUM)	Description
<code>show ppp session statistics</code> <code><interface-name></code>	Displays detailed statistics for PPP sessions for a specified interface.

EXAMPLE

```
ALU# show ppp session statistics Serial 0/0:0
```

```
PPP data packets received:      0
PPP control packets received:   20
Packets dropped:                0

PPP sessions initiated:         1
PPP sessions received:          1
PPP sessions successful:        2
PPP sessions terminated:        1
```

PPP AUTHENTICATION SHOW COMMANDS

The following commands are used to view the PPP authentication configuration:

TO VIEW THE PPP AUTHENTICATION DETAILS

Command (in SUM)	Description
<code>show ppp authentication configuration <interface-name></code>	Displays the PPP authentication configuration information for a specified interface.

EXAMPLE

```
ALU# show ppp authentication configuration Serial 0/0:0
```

```
Authentication protocol: pap
Authentication username: user1
Authentication password: secret1
```

TO VIEW THE PPP AUTHENTICATION STATISTICS

Command (in SUM)	Description
<code>show ppp authentication statistics <interface-name></code>	Displays detailed statistics for PPP authentication for a specified interface.

EXAMPLE

```
ALU# show ppp authentication statistics Serial 0/0:0
```

```

                                     IN          OUT
PAP Authentication Requests:         2          2
PAP Authentication Acks:             2          2
PAP Authentication Naks:              0          0
PAP Invalid Packets:                 0          0

                                     IN          OUT
CHAP Challenges:                     0          0
CHAP Responses:                      0          0
CHAP Successes:                      0          0
CHAP Failures:                       0          0
CHAP Invalid Packets:                0          0

                                     IN          OUT
EAP Requests:                        0          4
EAP Responses:                       4          0
EAP Successes:                       0          2
EAP Failures:                        0          0
EAP Invalid Packets:                 0          0

```

PPP DEBUG COMMANDS

TO ENABLE DEBUGGING ON PPP

Command (in SUM or CM)	Description
<code>debug ppp all [detail-level <1-9>]</code>	This command shows all the debug messages pertaining to the PPP functionality.
<code>debug ppp echo [output {all log vty}]</code>	This command shows the LCP echo requests and reply messages.

EXAMPLE

```
ALU(config)# debug ppp all
```

```
ALU(config)# debug ppp echo
```

TO DISABLE DEBUGGING ON PPP

Command (in SUM or CM)	Description
<code>no debug ppp {all echo}</code>	The “ no ” command disables the debug functionality. By default, debug is disabled.

EXAMPLE

```
ALU(config)# no debug ppp echo
```


CHAPTER 16 MULTILINK POINT TO POINT PROTOCOL

This chapter includes the commands for configuring Multilink Point-to-Point Protocol (MLPPP) encapsulation on a T1 or an E1 interface or a Serial (V.35/X.21) interface. You are required to refer to the [“T1E1 Line Card”](#) and [“Serial Line Cards”](#) chapters before proceeding to this.

Refer to the [“Alcatel-Lucent Specific Overview on MLPPP Features”](#) for Alcatel-Lucent specific features.

The chapter is divided into the following sections:

- [“MLPPP Overview”](#)
- [“MLPPP Configuration”](#)

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
CPE	Customer Premises Equipment
ICM	Interface Configuration Mode - ALU (config-interface name)#
IPCP	IP Control Protocol
FR	Frame Relay
LCP	Link Control Protocol
MLPPP	Multi Link Point to Point Protocol
MRRU	Maximum Receive Reconstructed Unit
PPP	Point-to-Point Protocol
SPE	Service Provider Equipment
SSHNF	Short Sequence Header Number Format
SUM	Super User Mode - ALU#

MLPPP OVERVIEW

WAN connectivity can be expensive for an enterprise, and often consists of T1 or E1 or T3 or E3 lines. Some enterprises require more bandwidth than a T1 or an E1 can provide, but cannot afford a T3 or E3. One option is to set up multiple T1 or E1 lines between the enterprise gateway and the ISP and use them as different IP interfaces, and then perhaps use Equal Cost Multi-Path (ECMP) for load balancing the traffic over these links. However, this solution requires re-configuration at the IP level and can be potentially complicated.

A feasible solution is to create a virtual bundle interface between the system and its peer, and attach multiple physical interfaces or channels to it on an as-needed basis. All IP-related configuration is placed on the bundle interface. The member links can be added or removed from the bundle at any time, and the bundle is up as long as there is at least one member link. This mechanism leaves all IP configuration intact, even while changing the bandwidth of the bundle by adding or removing links.

The Layer-2 protocol needs to co-operate in this effort, so the peer can learn about the fact that a link has been attached to a bundle. The protocol also needs to help maintain this association.

The protocols that have been enhanced for this purpose are PPP and FR, as they are common on serial interfaces, such as T1 or E1. The resultant technologies are called Multilink PPP (RFC 1990) and Multilink FR (FRF 16.1).

MLPPP is an extension to PPP. See [“Point-to-Point Protocol”](#) for information about PPP. Microsoft Windows, Linux, and other operating systems support MLPPP. Many routers also support Multilink PPP.

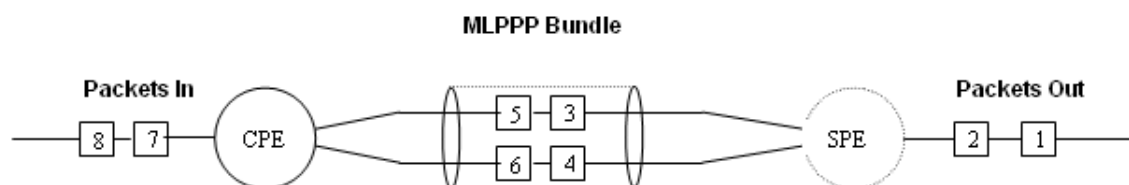


Figure 30: Sample Deployment Scenario for MLPPP

MLPPP COMPONENTS

A typical MLPPP configuration has at least two components:

- A bundle interface
- An interface running PPP that is made multilink-enabled and attached to the bundle interface.

MLPPP OPERATION

To establish communication over a PPP Multilink, an MRRU (Maximum Receive Reconstructed Unit) configuration option is sent to the peer during LCP negotiation. Optionally, an Endpoint Discriminator Option or SSHNF Option may also be sent out. LCP negotiation and optional link authentication take place on each bundle link. IPCP negotiation happens over the bundle, meaning IPCP packets may be sent on any one of the bundle links. Certain LCP packets like LCP Echo-Request and LCP Echo-Reply may be transmitted over the bundle. IP packets are sent over the bundle.

The MLPPP packet is encapsulated using an MLPPP header which is different from the standard PPP header. It contains a sequence number and additionally allows for fragmentation or re-assembly of the packet.

MLPPP is also referred to as MP or MPPP.

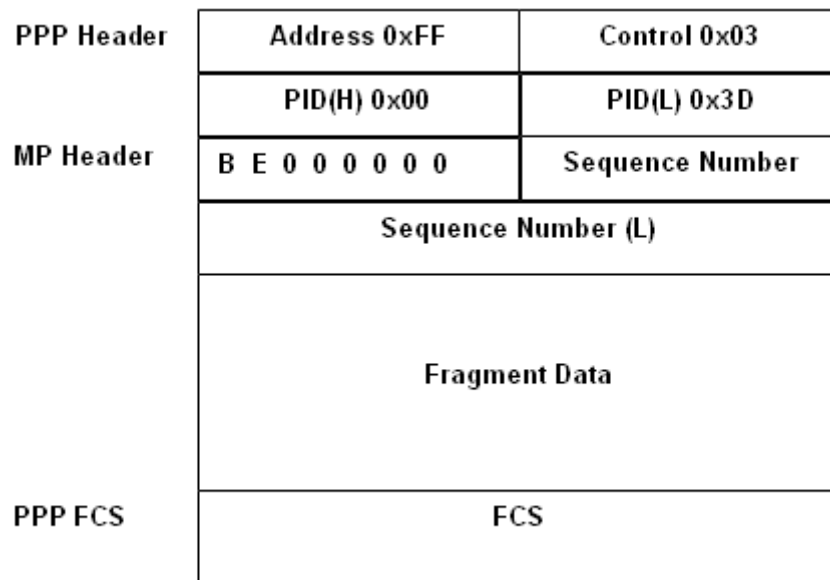


Figure 31: MLPPP Header in Long Sequence Number Format

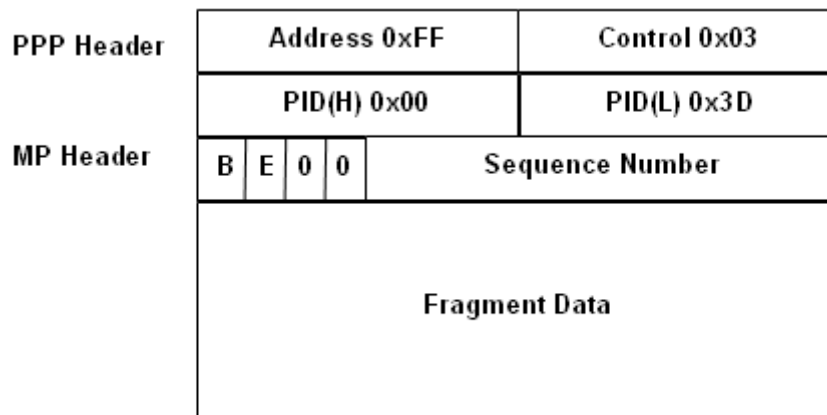


Figure 32: MLPPP Header in Short Sequence Number Format

ALCATEL-LUCENT SPECIFIC OVERVIEW ON MLPPP FEATURES

The following features are available with the current release:

- The OmniAccess 700 supports RFC 1990 (MLPPP Protocol) without necessarily conforming to all the optional items mentioned in the specification.
- Specifically, the system supports the logical aggregation, into a configured MLPPP bundle of any number of channelized or fractional T1 or E1 interfaces, Serial (V.35/X.21) interfaces, etc. This bundle behaves like a virtual IP interface.
- Multiple MLPPP bundles may be statically configured on the system. MLPPP protocol negotiation or data reaching the system on an unconfigured interface are dropped. Bundles cannot be deleted, but can be shutdown and thereby made unusable.
- The packet distribution across the MLPPP member links within a bundle is handled in a weighted roundrobin fashion, the weight being the bandwidth of the links.
- Authentication optionally happens at each member link, and is supported through PAP, CHAP or EAP as configured.
- IP routing protocols as well as policies such as ACL, NAT, IDS, IPsec, etc., may be applied on the bundle.
- MLPPP fragmentation/reassembly is currently not supported.
- The default MTU is 1500 on an MLPPP bundle interface. That makes the MRRU (Maximum Received Restructured Unit) value to 1506 that accounts for the 6 extra bytes of the MLPPP header. If there are interoperability issues with the peer, the MRRU value of the peer MLPPP interface has to be adjusted accordingly.

MLPPP CONFIGURATION

- [“MLPPP Configuration Steps”](#)
- [“MLPPP Configuration Flow”](#)
- [“MLPPP Configuration Commands”](#)
- [“MLPPP Show Commands”](#)

MLPPP CONFIGURATION STEPS

This section lists the commands for MLPPP configuration.



Note: The following MLPPP configuration commands are shown for a T1 interface as an example. The steps are similar for configuration of MLPPP on an E1 interface.

Step 1: Enter Configuration Mode

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure T1 Controller

```
ALU(config)# controller T1 <slot/port>
ALU(config-controller T1)#
```

Step 3: Configure the channel-group on the controller before entering the Interface Configuration Mode. This command creates a channel-group that forms a channelized serial interface.

```
ALU(config-controller T1)# channel group <0-23>
timeslots <1-24> speed [56K|64K]
```



Note: Creation of a channel-group is a pre-requisite for configuring a Serial Interface on a T1 or an E1 controller.

Step 4: Administratively bring up the controller.

```
ALU(config-controller T1)# no shutdown
```

Step 5: Exit from the controller mode

```
ALU(config-controller T1)# exit
ALU(config)#
```



Note: The above steps can be skipped if the T1 or E1 controller has already been configured. For more details on configuring a T1 or an E1 controller, refer to the [“T1E1 Line Card”](#) chapter.

The above steps can also be skipped if you are configuring MLPPP on a **Serial interface (V.35/X.21)**. The steps (**Step 6 - Step 12**) hold good for configuration of MLPPP on a V.35/X.21 interface, except that there is no channel group number in the interface name. Configure a serial interface using the following command:

```
ALU(config)# interface Serial <slot/port>
ALU(config-if Serial<slot/port>)#
```

Example:

```
ALU(config)#interface Serial0/0
ALU(config-if Serial0/0)#
```

For more details on configuring a Serial interface (V.35/X.21), refer to the [“Serial Line Cards”](#) chapter.

Bundle Configuration

Step 6: Configure MLPPP Bundle Interface. See [“To Configure MLPPP Bundle Interface”](#)

Step 7: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if mlppp100)# no shutdown
```

Step 8: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if mlppp100)#ip address 20.20.20.20/24
```



Note: Bundle Configuration is a pre-requisite for Member Link Configuration.

Step 9: Configure MLPPP load threshold. See [“To Configure MLPPP Load Threshold” \(Optional\)](#)

Member Link Configuration

Step 10: Enter Serial interface configuration mode for Member Link Configuration

```
ALU(config)# interface Serial <slot/port:channel>
ALU(config-if Serial<slot/port:channel>)#
```

Example:

```
ALU(config)#interface Serial0/0:0
ALU(config-if Serial0/0:0)#
```

Step 11: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if Serial0/0:0)# no shutdown
```

Step 12: Configure encapsulation on the interface. See [“To Set MLPPP Encapsulation on an Interface”](#)

Step 13: Use the [“MLPPP Show Commands”](#) to view the MLPPP configuration.

MLPPP CONFIGURATION FLOW

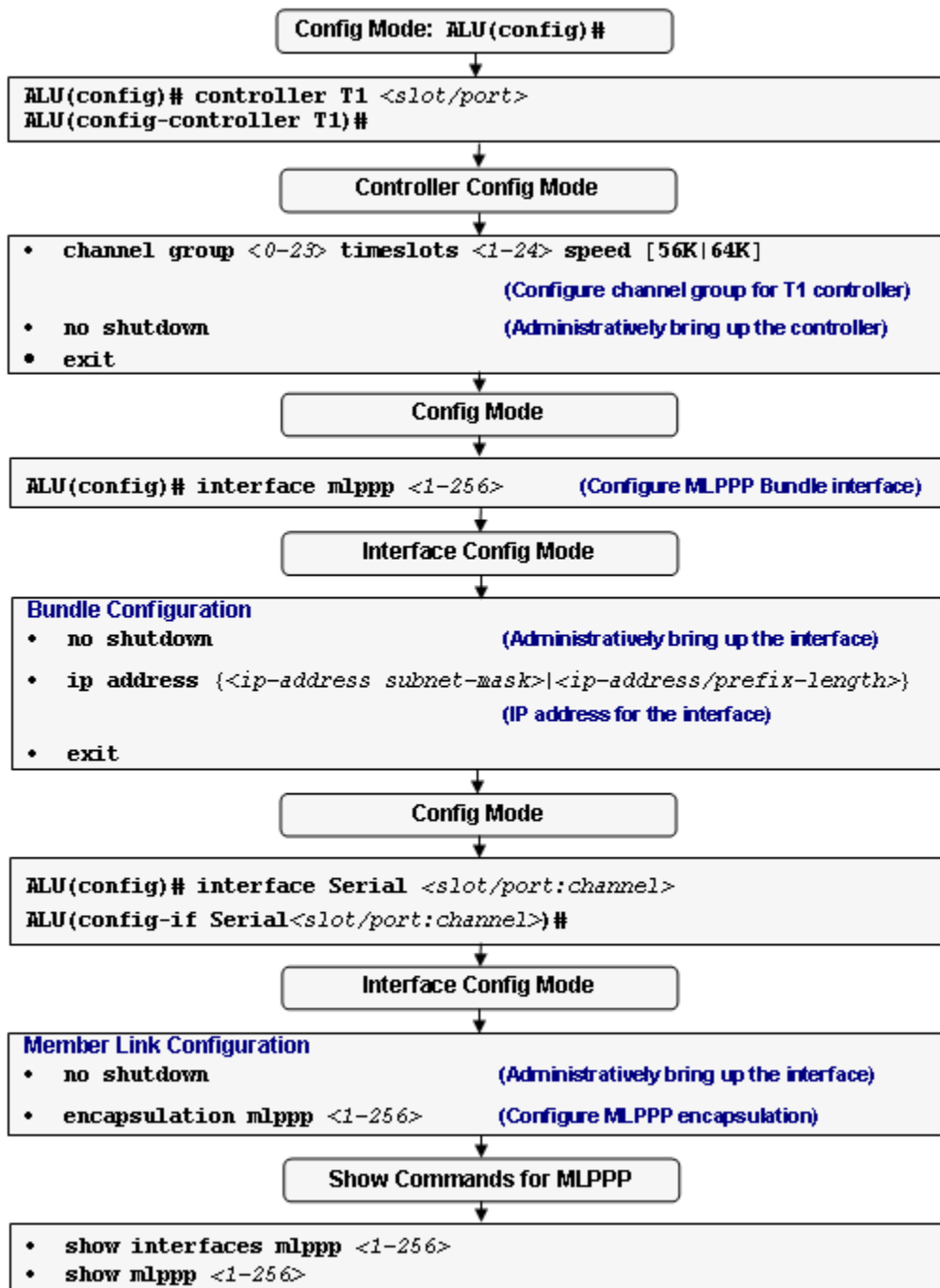


Figure 33: MLPPP Configuration Flow

MLPPP CONFIGURATION COMMANDS

To configure MLPPP, first a bundle interface needs to be configured and then MLPPP encapsulation is set on the member interfaces, to link them to the bundle.

Once a bundle interface is configured, LCP, authentication protocols such as PAP, CHAP and EAP and Protocol Timers can still be configured on an individual interface. However, IPCP should be configured on the bundle interface and not on the member link.

All commands, including the show commands relating to IPCP and PPP Counters and Timers can be applied on the MLPPP bundle interface. Refer to the [“Point-to-Point Protocol”](#) chapter for more information on these commands.

IP routing protocols as well as policies such as ACL, NAT, IDS, IPsec, etc., configured on an individual interface will not be effective as long as the interface is part of the MLPPP bundle. Once the interface is no longer part of the bundle, the policies configured on the individual interface will become active.

TO CONFIGURE MLPPP BUNDLE INTERFACE

Command (in CM)	Description
<code>interface mlppp <1-256></code>	This command creates a MLPPP bundle interface that is identified by the bundle ID. The range of the bundle ID is between 1 and 256.

EXAMPLE

```
ALU(config)# interface mlppp 100
ALU(config-if mlppp100)#
```

TO CONFIGURE MLPPP LOAD THRESHOLD

Command (in ICM)	Description
<code>mlppp load-threshold {high low} {outbound inbound} <1-255></code>	This command sets the load-threshold on an MLPPP bundle.
<code>no mlppp load-threshold {high low} {outbound inbound}</code>	This command removes the load threshold on the MLPPP bundle.

EXAMPLE

```
ALU(config-if mlppp100)# mlppp load-threshold high outbound 100
ALU(config-if mlppp100)# no mlppp load-threshold high outbound
```

To SET MLPPP ENCAPSULATION ON AN INTERFACE

Command (in ICM)	Description
<code>encapsulation mlppp <1-256></code>	This command sets MLPPP encapsulation on an interface. The interface becomes a member link of the bundle interface identified by the bundle ID.
<code>no encapsulation mlppp</code>	This command sets the encapsulation to its default. The default encapsulation on a serial interface is HDLC.

EXAMPLE

```
ALU(config)#interface Serial1/0:0
ALU(config-if Serial1/0:0)# encapsulation mlppp 100

ALU(config-if serial1/0:0)# no encapsulation mlppp
```


MLPPP SHOW COMMANDS

To VIEW MLPPP CONFIGURATION

Command (in SUM/CM/ICM)	Description
<code>show interfaces mlppp <1-256></code>	Displays the configuration of the MLPPP bundle interface specified.
<code>show mlppp <1-256></code>	Displays the PPP status on the member links of the specified MLPPP bundle interface.

EXAMPLE

```
ALU(config)#show interfaces mlppp 10
```

```
mlppp10 is up, line protocol is up
Internet address is 3.3.3.3/24
MTU 1494 bytes, BW 512 Kbit, DLY 0 usec,
Encapsulation mlppp, loopback not set
IPCP: Open
Last input never, output never, output hang never
Last clearing of "show interface" counters never
  2 packets input (2 Control packets, 0 Data packets), 28 bytes
  2 packets output (2 Control packets, 0 Data packets), 28 bytes
  0 packets dropped, 0 giants received
```

```
ALU(config)# show mlppp 10
```

```
MLPPP bundle 10 link state information:
IPCP:                               Open
MEMBER LINKS      LCP      AUTH CLIENT AUTH SERVER
  Serial0/0:1      Open      -----
    (PAP) Open
  Serial0/0:0      Open      -----
    (CHAP) Open
```

MLPPP CONFIGURATION EXAMPLE

The following example illustrates the configuration of a bundle interface and then the member link configuration.

To configure MLPPP, first a bundle interface needs to be configured, and then MLPPP encapsulation is set on interfaces to link them to a bundle.

a) Configuration of bundle interface

```
ALU> enable
ALU#configure terminal
ALU(config)#interface mlppp 10
ALU(config-if mlppp10)#ip address 3.3.3.3 255.255.255.0
ALU(config-if mlppp10)#no shutdown
ALU(config-if mlppp10)#exit
ALU(config)#
```

b) Configuration of Serial interfaces and linking them to the bundle

```
ALU(config)#controller T1 0/0
ALU(config-controller T1)#channel-group 0 timeslots 1
ALU(config-controller T1)#exit
ALU(config)#
ALU(config)#interface Serial 0/0:0
ALU(config-if Serial0/0:0)#no shutdown
ALU(config-if Serial0/0:0)#encapsulation mlppp 10
```

```
ALU(config)#controller T1 0/0
ALU(config-controller T1)#channel-group 1 timeslots 2
ALU(config-controller T1)#exit
ALU(config)#
```

```
ALU(config)#interface Serial 0/0:1
ALU(config-if Serial0/0:1)#no shutdown
ALU(config-if Serial0/0:1)#encapsulation mlppp 10
```

c) Viewing MLPPP Configuration

```
ALU(config)#show interfaces Serial 0/0:0
Serial0/0:0 is Down, line protocol is down
  Internet address not set
  MTU 1500 bytes, BW 64 Kbit, DLY 0 usec,
    reliability 0/255, txload 0/255, rxload 0/255
  Loopback not set
  Encapsulation mlppp, keepalive set (10 sec)
  LCP: Initial
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/max) 0
  drops
    Conversations: 0/0/0/0 (active/max active/max total)
```

```

Reserved Conversations: 0/0 (allocated/max allocated)
Available Bandwidth 64 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
Timeslot(s) Used:1 (64Kbps each), Transmitter delay is 0 flags

```

ALU(config)#show interfaces mlppp 10

```

mlppp10 is up, line protocol is up
Internet address is 3.3.3.3/24
MTU 1494 bytes, BW 512 Kbit, DLY 0 usec,
Encapsulation mlppp, loopback not set
IPCP: Open
Last input never, output never, output hang never
Last clearing of "show interface" counters never
  2 packets input (2 Control packets, 0 Data packets), 28 bytes
  2 packets output (2 Control packets, 0 Data packets), 28 bytes
  0 packets dropped, 0 giants received

```

ALU(config)# show mlppp 10

```

MLPPP bundle 10 link state information:
IPCP:          Open
MEMBER LINKS   LCP      AUTH CLIENT     AUTH SERVER
Serial0/0:1    Open      Open            -----
(PAP) Open
Serial0/0:0    Open      Open            -----
(CHAP) Open

```

CHAPTER 17 MULTILINK FRAME RELAY

This chapter includes the commands for configuring Multilink Frame Relay (MLFR) encapsulation on a T1 or an E1 interface or a Serial (V.35/X.21) interface. You are required to refer to the **“T1E1 Line Card”** and **“Serial Line Cards”** chapters before proceeding to this.

Refer to the **“Alcatel-Lucent Specific Overview on MLFR features”** section for Alcatel-Lucent specific features.

The chapter is divided into the following sections:

- **“MLFR Overview”**
- **“MLFR Configuration”**
- **“MLFR Configuration Commands”**

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
MLFR	Mutilink Frame Relay
SUM	Super User Mode - ALU#

MLFR OVERVIEW

MLFR is defined in FRF 16.1. It is an extension to the Frame Relay Protocol. See [“Frame Relay”](#) chapter for information about the basic protocol. For a background of the multilink concept, refer to [“Multilink Point to Point Protocol”](#).

MLFR COMPONENTS

A typical MLFR configuration has at least two components:

- A bundle interface
- An interface running Frame Relay is made multilink-enabled and attached to the bundle interface.

MLFR OPERATION

After the bundle interface is configured and an interface running Frame Relay is made multilink enabled, bundle and link identifiers are configured appropriately. This results in the transmission of appropriate Link Integrity Protocol messages on the bundle link. Once the bundle link state machine reaches the UP state, normal Frame Relay Link Management (LMI) procedures are started over the bundle. This means the LMI packets can be sent over any of the associated bundle links as they are all going to the same peer. After LMI comes up, the line protocol is said to be up on the bundle and if IP addresses have been configured at both ends of the bundle, IP packets can be sent over the bundle.

The MLFR packet is encapsulated using an MLFR header, which is different from the standard Frame Relay header. It contains a sequence number and also allows for fragmentation/reassembly of the MLFR packet.

MLFR is also referred to as MFR.

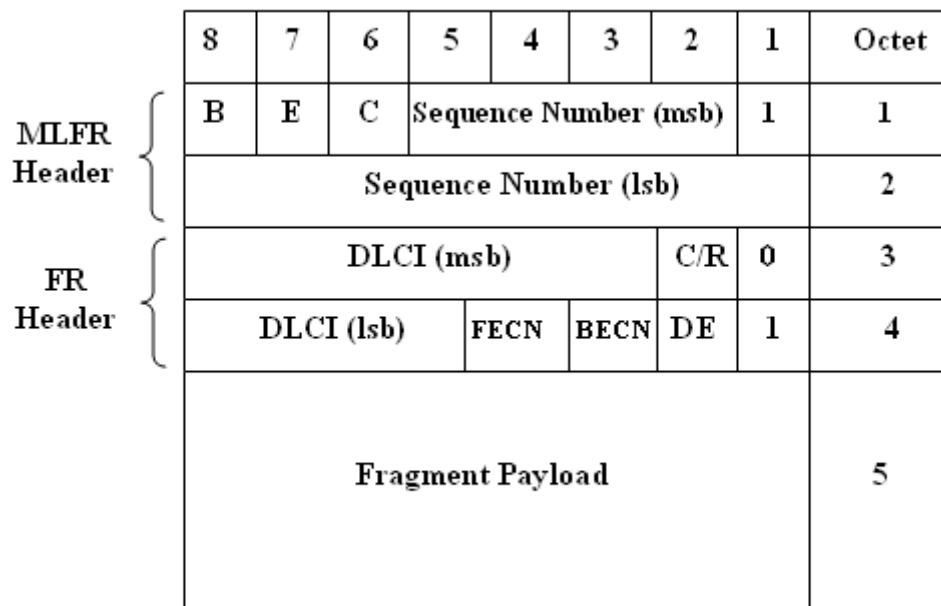


Figure 34: MLFR frame format for data packets

8	7	6	5	4	3	2	1	Octet
B(1)	E (1)	C(0)	0	0	0	0	1	1
0	0	0	0	0	0	0	0	2
Message Type								3
Information Element 1								4
Information Element N								5

Figure 35: MLFR frame format for control packets

ALCATEL-LUCENT SPECIFIC OVERVIEW ON MLFR FEATURES

The following features are available with the current release:

- The OA-700 supports FRF 16.1 (Multilink Frame Relay UNI/NNI Implementation Agreement) without necessarily conforming to all the optional items mentioned in the specification.
- Specifically, the system will support the logical aggregation into a configured MLFR bundle to support any number of interfaces, including channelized and fractional serial interfaces. This bundle will behave like a virtual IP interface.
- Multiple MLFR bundles can be statically configured on the system. However, bundles will not be created dynamically. MLFR protocol negotiation or data reaching the system on an unconfigured interface will be dropped. Bundles cannot be deleted, but can be shut down and thereby made unusable.
- The packet distribution across the MLFR member links within a bundle will be handled in a roundrobin fashion.
- The bundle identifier and the link identifier will be configurable, as will the values of certain protocol timers and counters.
- IP routing protocols as well as policies such as ACL, NAT, IDS, IPsec, etc., may be applied on the bundle.
- The Alcatel-Lucent OA-700 implementation does not include Link Fragmentation and Interleaving, Vendor Extension Information Element, and SNMP MIB support.

MLFR CONFIGURATION

- [“MLFR Configuration Steps”](#)
- [“MLFR Configuration Flow”](#)
- [“MLFR Configuration Commands”](#)

MLFR CONFIGURATION STEPS

This section lists the instructions to be followed while configuring MLFR.



Note: The following MLFR configuration commands are shown for a T1 interface as an example. The steps are similar for configuration of MLFR on an E1 interface.

Step 1: Enter Configuration Mode

```
ALU# configure terminal
ALU(config)#
```

Step 2: Configure T1 controller

```
ALU(config)# controller T1 <slot/port>
ALU(config-controller T1)#
```

Step 3: Configure the channel-group on the controller before entering the Interface Configuration Mode. This command creates a channel-group that will form a channelized serial interface.

```
ALU(config-controller T1)# channel group <0-23>
timeslots <1-24> speed [56K|64K]
```



Note: Creation of a channel-group is a pre-requisite for configuring a Serial Interface on a T1 or an E1 controller.

Step 4: Administratively bring up the controller.

```
ALU(config-controller T1)# no shutdown
```

Step 5: Exit from the controller mode

```
ALU(config-controller T1)# exit
ALU(config)#
```



Note: The above steps can be skipped if the T1 or E1 controller has already been configured. For more details on configuring a T1 or an E1 controller, refer to the [“T1E1 Line Card”](#) chapter.

The above steps can also be skipped if you are configuring MLFR on a **Serial interface (V.35/X.21)**. The steps (**Step 6 - Step 16**) hold good for configuration of MLFR on V.35/X.21 interface, except that there is no channel group number in the interface name. Configure a serial interface using the following command:

```
ALU(config)# interface Serial <slot/port>
ALU(config-if Serial<slot/port>)#
```

Example:

```
ALU(config)#interface Serial0/0
ALU(config-if Serial0/0)#
```

For more details on configuring a Serial interface (V.35/X.21), refer to the [“Serial Line Cards”](#) chapter.

Bundle Configuration

Step 6: Configure MLFR Bundle Interface. See [“To Configure MLFR Bundle Interface”](#)

Step 7: Administratively bring up the interface.

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if mlfr100)# no shutdown
```

Step 8: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>/<ip-address/prefix-length>}
```

Example:

```
ALU(config-if mlfr100)# ip address 20.20.20.20/24
```

Step 9: Configure Frame Relay LMI (Local Management Interface) type. See [“To Configure Local Management Interface \(LMI\) Type” \(Optional\)](#)

Step 10: Configure Data Link Connection Identifiers (DLCI) on the interface. See [“To Configure Data-link Connection Identifier \(DLCI\)”](#)

Step 11: Assign a Bundle Identification (BID) name to the MLFR bundle configured above. See [“To Assign Bundle Identification \(BID\) to the Bundle” \(Optional\)](#)

Member Link Configuration

Step 12: Enter Serial interface configuration mode

```
ALU(config)# interface Serial <slot/port:channel>
ALU(config-if Serial<slot/port:channel>)#
```

Example:

```
ALU(config)#interface Serial0/0:0
ALU(config-if Serial0/0:0)#
```

Step 13: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if Serial0/0:0)# no shutdown
```

Step 14: Set encapsulation to MLFR. See [“To Set MLFR Encapsulation on an Interface”](#)

Step 15: Configure MLFR Optional Parameters.

- Assign Link Identification (LID) to the interface. See [“To Assign Link Identification \(LID\) to the Interface”](#)
- Configure the Hello interval. See [“To Configure Hello Interval”](#)
- Configure the Acknowledge interval. See [“To Configure the Acknowledge Interval”](#)
- Configure the retry count. See [“To Configure the Retry Count”](#)

Step 16: Use the show commands to view the MLFR configuration. See [“MLFR Show Commands”](#)

MLFR CONFIGURATION FLOW

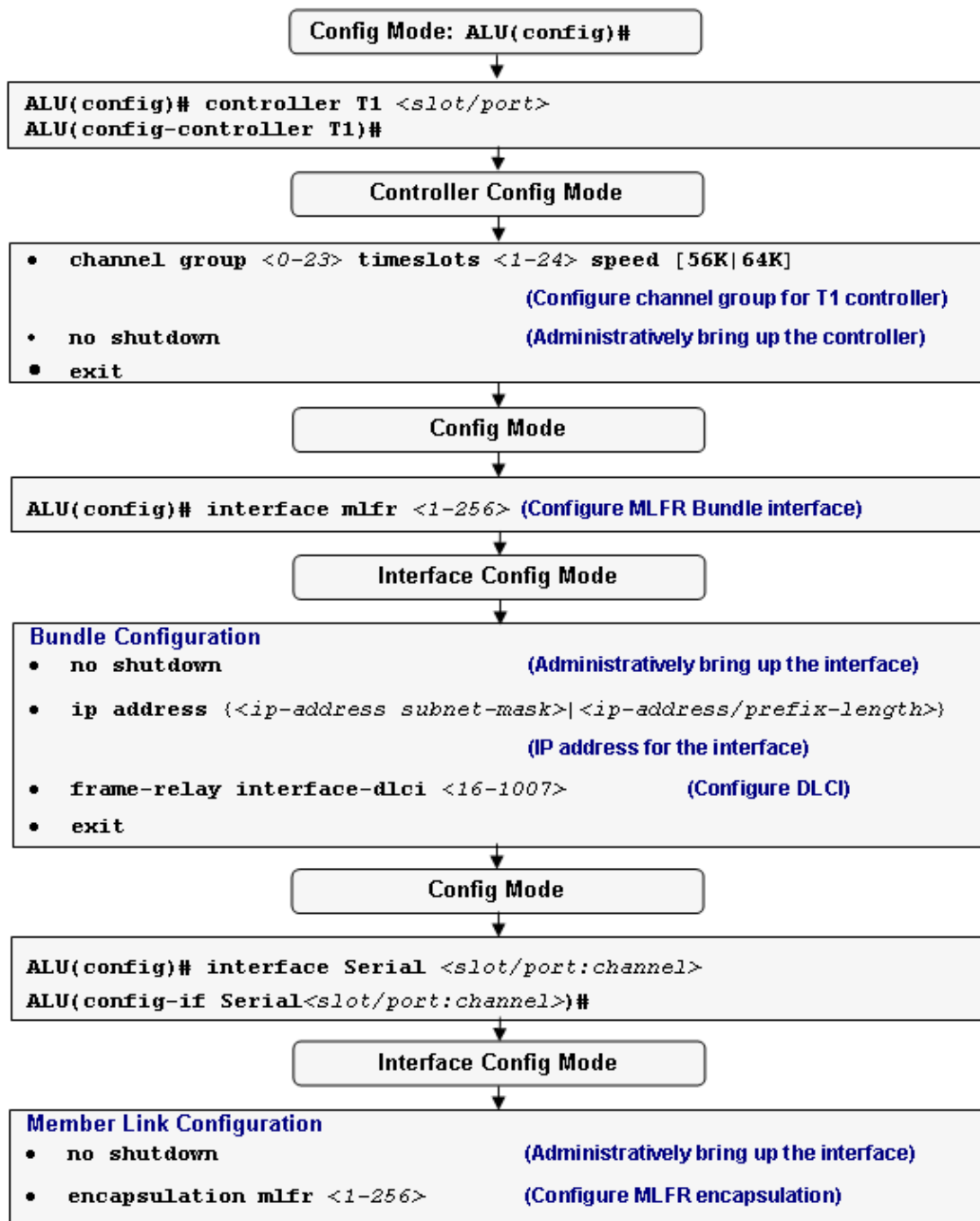


Figure 36: MLFR Configuration Flow

MLFR CONFIGURATION COMMANDS

To configure an MLFR, first a bundle interface needs to be configured. Then MLFR encapsulation is set on individual interfaces that become a part of the bundle by member link configuration.

IP routing protocols as well as policies such as ACL, NAT, IDS, IPsec, etc., configured on an individual interface will not be effective as long as the interface is part of the MLFR bundle. When the interface is no longer part of the bundle, the policies configured on the individual interface become active.

TO CONFIGURE MLFR BUNDLE INTERFACE

Command (in CM)	Description
<code>interface mlfr <1-256></code>	This command configures a MLFR bundle interface that is identified by a user specified number. This number can vary from 1 - 256.

EXAMPLE

```
ALU(config)# interface mlfr 100
ALU(config-if mlfr100)#
```

TO CONFIGURE LOCAL MANAGEMENT INTERFACE (LMI) TYPE

Command (in ICM)	Description
<code>frame-relay lmi-type {ansi/q933a}</code>	This command is used to set the LMI type to either ANSI or Q933A.
<code>no frame-relay lmi-type {ansi/q933a}</code>	The “no” command sets the LMI type to its default value. The default LMI type is auto-sense .



Note: LMI Autosense is activated by default as the system acts as a DTE. The LMI autosense will be activated when the physical interface is up and LMI type is not configured on that interface.

EXAMPLE

The following example sets the LMI to ANSI standard:

```
ALU(config-if mlfr100)# frame-relay lmi-type ansi
```

The following example sets the LMI-type to its default, i.e., ‘auto-sense’:

```
ALU(config-if mlfr100)# no frame-relay lmi-type
```

To CONFIGURE DATA-LINK CONNECTION IDENTIFIER (DLCI)

Command (in ICM)	Description
<code>frame-relay interface-dlci <16-1007></code>	This command is used to configure a DLCI on an MLFR interface.
<code>no frame-relay interface-dlci <16-1007></code>	The “no” command deletes the configured DLCI from the MLFR interface.

EXAMPLE

The following example sets the DLCI value to 100:

```
ALU(config-if mlfr100)# frame-relay interface-dlci 100
```

The following example deletes the DLCI configured:

```
ALU(config-if mlfr100)# no frame-relay interface-dlci 100
```

To ASSIGN BUNDLE IDENTIFICATION (BID) TO THE BUNDLE

Command (in ICM)	Description
<code>mlfr bid <name></code>	This command assigns a bundle identification (BID) name to the bundle interface. The bid name can be a maximum of 255 characters.
<code>no mlfr bid <name></code>	This command removes the configured bid name from the bundle interface.

EXAMPLE

```
ALU(config-if mlfr100)# mlfr bid ALU1
```



Note: Configuring a Bundle Interface is a pre-requisite to Member Link configuration.

To SET MLFR ENCAPSULATION ON AN INTERFACE

Command (in ICM)	Description
<code>encapsulation mlfr <1-256></code>	This command sets the encapsulation on an interface to MLFR, and attaches it to the bundle interface configured.
<code>no encapsulation mlfr <1-256></code>	This command sets the encapsulation to its default. The default encapsulation on a serial interface is HDLC.

EXAMPLE

```

ALU(config)#interface Serial1/0:0
ALU(config-if Serial1/0:0)# encapsulation mlfr 100

ALU(config-if Serial1/0:0)# no encapsulation mlfr

```

To ASSIGN LINK IDENTIFICATION (LID) TO THE INTERFACE

Command (in ICM)	Description
<code>mlfr lid <name></code>	This command assigns a link identification (LID) name to the interface that is part of the bundle. The LID can be a maximum of 255 characters.
<code>no mlfr lid <name></code>	This command removes the configured LID name from the interface that is part of the bundle.

EXAMPLE

```

ALU(config-if Serial0/0:0)# mlfr lid ALU-wan-link

ALU(config-if Serial0/0:0)# no mlfr lid ALU-wan-link

```

To CONFIGURE HELLO INTERVAL

Hello interval is the duration in seconds between successive hello messages sent.

Command (in ICM)	Description
<code>mlfr hello-interval <1-180></code>	This command configures the hello interval. The range of this interval is from 1 to 180 seconds.
<code>no mlfr hello-interval <1-180></code>	This command resets the hello interval to its default value, i.e., 10 seconds.

EXAMPLE

```
ALU(config-if Serial0/0:0)# mlfr hello-interval 15
```

```
ALU(config-if Serial0/0:0)# no mlfr hello-interval 15
```

To CONFIGURE THE ACKNOWLEDGE INTERVAL

Acknowledge interval is the duration (in seconds) that the bundle link waits for a hello message from its peer, or the duration it waits before resending the hello message.

Command (in ICM)	Description
<code>mlfr ack-interval <1-10></code>	This command configures the acknowledge interval. The range of this interval is from 1 second to 10 seconds.
<code>no mlfr ack-interval <1-10></code>	This command resets the acknowledge interval to its default, i.e., 4 seconds.

EXAMPLE

```
ALU(config-if Serial0/0:0)# mlfr ack-interval 5
```

```
ALU(config-if Serial0/0:0)# no mlfr ack-interval 5
```


To CONFIGURE THE RETRY COUNT

Retry count is the number of times the bundle link will send out a hello message before any acknowledgment is received from its peer.

Command (in ICM)	Description
<code>mlfr retry-count <1-5></code>	This command configures the retry count to the number specified. The range of this number is from 1 to 5.
<code>no mlfr retry-count <1-5></code>	This command resets the retry count to its default, i.e., 2.

EXAMPLE

```
ALU(config-if Serial0/0:0)# mlfr retry-count 3
```

```
ALU(config-if Serial0/0:0)# no mlfr retry-count 3
```

MLFR SHOW COMMANDS

To VIEW MLFR CONFIGURATION

Command (in SUM/CM)	Description
<code>show interfaces mlfr [<1-256>]</code>	Displays the configuration of the MLFR bundle interface specified.
<code>show mlfr [<1-256>]</code>	Displays the protocol status on the member links of the specified MLFR bundle interface.
<code>show interfaces Serial [<slot/port:channel>]</code>	Use this command to verify if MLFR is the current encapsulation on the interface, and to check the interface details.

EXAMPLE

```
ALU(config)# show interfaces mlfr 1
```

```
mlfr1 is up, line protocol is up
 Internet address is 192.168.1.1/24
 Bundle id is mlfr1, keepalive set (10 sec)
 LMI enq sent 26219, LMI stat recvd 325, LMI upd recvd 0, DTE LMI up
 LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
 LMI DLCI 0 LMI type is CCITT(q933a) frame relay DTE
 MTU 1500 bytes, BW 3072 Kbit, DLY 0 usec,
   reliability 255/255, txload 0/255, rxload 0/255
 Encapsulation mlfr-bundle, loopback not set
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
   614 packets input( 325 control packets, 289 data packets),34295 bytes
   26599 packets output( 26216 control packets, 383 data packets),458430 bytes
   53 packets dropped 0 giant packets
```

```
ALU# show mlfr 1
```

```
MLFR bundle 1 link state information:
```

MEMBER LINKS	PROTOCOL STATE	BID	LID
Serial0/1:1	UP	mlfr1	Serial0/1:1
Serial0/0:1	UP	mlfr1	Serial0/0:1

```
ALU# show interfaces Serial 0/0:1
```

```
Serial0/0:1 is up, line protocol is up
Internet address not set
MTU 1500 bytes, BW 1536 Kbit, DLY 0 usec,
  reliability 255/255, txload 0/255, rxload 0/255
Loopback not set
Encapsulation mlfr, MLFR Bundle Id: 1
Hello Interval: 10(secs)
Ack-interval :4(secs), Max Retry count :3
Link state : UP
Statistics:
  Current Retry Count is 0
  Add_link_sent:4, Add_link_rcvd:1
  Add_link_ack_sent:1, Add_link_ack_rcvd:2
  Rm_link_sent:0, Rm_link_rcvd:0
  Rm_link_ack_sent:0, Rm_link_ack_rcvd:0
  Hello_sent:55, Hello_rcvd:56
  Hello_ack_sent:56, Hello_ack_rcvd:55
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue: 0/0 (size/max) 0 drops; Input queue: 0/0 (size/max) 0 drops
  Conversations: 0/0/0/0 (active/max active/max total)
  Reserved Conversations: 0/0 (allocated/max allocated)
  Available Bandwidth 1536 kilobits/sec
5 minute input rate 24 bits/sec, 0 packets/sec
5 minute output rate 24 bits/sec, 0 packets/sec
  1237 packets input, 32681 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  1249 packets output, 49735 bytes, 0 underruns
  0 output errors, 0 collisions, 16 interface resets
  0 output buffer failures, 0 output buffers swapped out
  18 carrier transitions
Timeslot(s) Used:1-24 (64Kbps each), Transmitter delay is 0 flags
```



Note: All the show commands that take IP interface name as an argument will also take MLFR interface as a parameter.

Part 4 Common Classification



CHAPTER 18 COMMON CLASSIFIERS

This chapter gives an insight of all the commands to configure the match-lists. It is divided into the following sections:

- **“CC Overview”**
- **“CC Configuration”**
- **“Sample examples on the usage of CC across applications”**

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
Match-list CM	Match-list Configuration Mode - ALU (config-match-list-name)#

CC OVERVIEW

Common Classification (**CC** herein after) is commonly used within the network devices in order to selectively categorize packet traffic and deal with it differently. CC find its application in various areas such as:

- Filtering for allowing selective route re-distribution from one routing protocol to another
- Firewalling
- Tunnelling
- Categorizing and prioritizing traffic for meeting the QoS requirements.

The evolution of network devices has thrown up some interesting facts. As new features were developed, the classification became more complex and varied. This complexity grew from the fact that people wanted to match traffic on increasing number of packet fields. Enhancement in speeds of the interface and switching has increased ascent on classification performance. Last but not the least, a generic classification model was required in order to match traffic classes which could be used for variety of services like QoS, VPN, Firewall, IDS, etc.

The OA-700 incorporates multiple services like routing, switching, firewall, VPN, and QoS. As part of our unified architecture, we have evolved a common classifier design which decouples classification and action. Thus, the same classifier can be used across all applications.

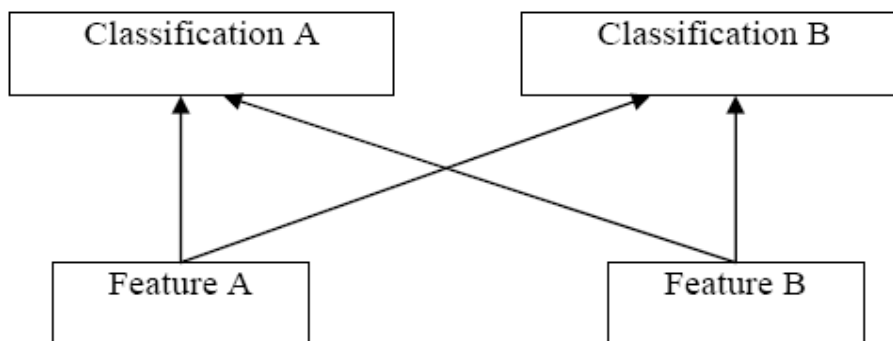


Figure 37: Depicting Alcatel-Lucent's Common Classification

BENEFITS OF ALCATEL-LUCENT DEVICES COMMON CLASSIFIERS

Following are the benefits of Alcatel-Lucent common classifiers:

- Usage of common classification by different features.
- Classification can be optimized and hence would lead to better performance of the devices.
- Unified and consistent syntax, which allows users to manage their classification configuration separately from the feature specific parameters and configuration.
- Extension or enhancements can be made to the classification configuration without the need to make any changes to the feature configuration.

CC ARCHITECTURE

A key design aspect of the CC is that it separates the classification from the action. This allows the classification to be performed once for a particular packet, and then different features can use the result to derive their own action. The below diagram depicts usage of common classification by different features.

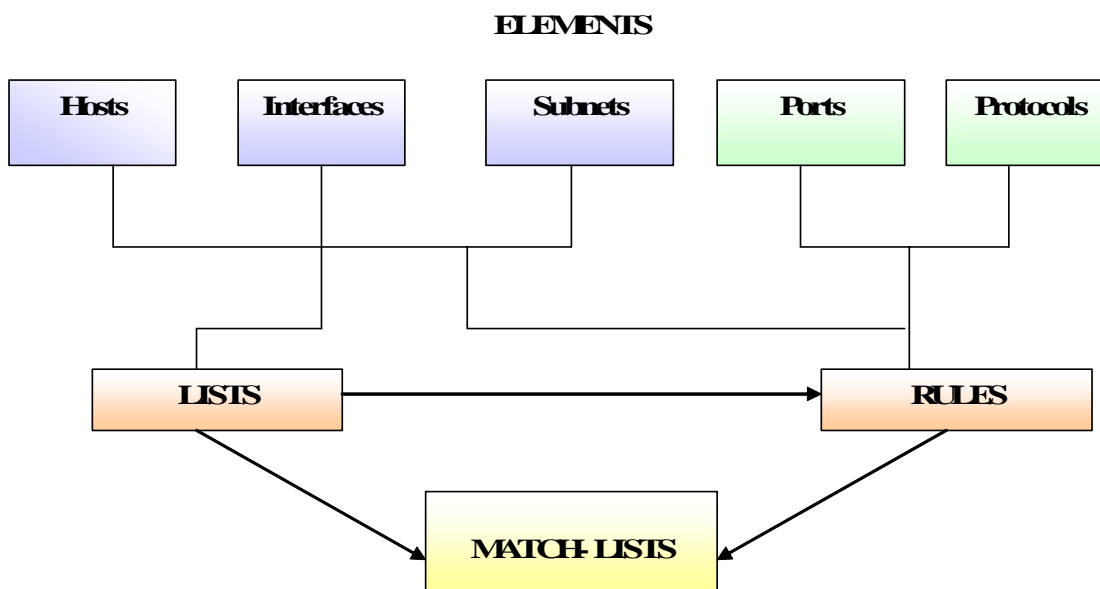


Figure 38: Elements in Common Classifiers

Classifications, referred in applications are known by names assigned to them when they are first defined. The classifications themselves are composed of a number of elements and are designed to be nested or serialized. Ultimately, classifications are composed of one or more rulesets, each of which consist of one or more rules. Rules themselves can consist of individual elements arranged in a specific manner, and can include references to lists of elements.

The elements (and lists of elements) are referred by rules or rulesets. Elements are the basic building blocks, and includes IP addresses, host names, networks (address/prefixes masks), interface names, TCP/UDP port numbers (services), and other IP header fields (IP Precedence, protocol, etc.).

Lists are named lists comprising of one or more meaningful elements (only some elements are allowed in lists), as well as references to other lists. A generic packet type can be used by higher level processing of the packet such as Application Level Gateways (ALG), and assigned when the packet is initially classified.

BEFORE YOU CONFIGURE CC

Consider the following points before configuring the match-lists:

- If no protocol is specified, then IP is the default protocol.
- Fields that are not referenced in the rule are by default considered a wildcard match e.g., if the protocol portion of the rule is not specified, it is automatically considered as an `any' match. The keyword `**any**' can be used to indicate a wildcard match. This is in reference to the '**match any**' and '**match all**' configuration.
- Rules start with Line number/Rule number 1 and follow a sequential order. These rules follow no priority.
- The keyword "**from**" defines the source port for a TCP or UDP protocol.
- The keyword "**service**" defines the destination port for a TCP or UDP protocol.
- The keyword "**type**" keyword kicks in ALGs (Application Level Gateways).

CC CONFIGURATION

This section covers the following:

- [“CC Configuration Steps”](#)
- [“Elements Used in Configuring CC”](#)
- [“Rules within Match-lists”](#)
- [“Lists in CC”](#)
- [“Nesting Of Match-lists”](#)
- [“Show commands in CC”](#)
- [“Deletion Commands in CC”](#)

CC CONFIGURATION STEPS

The following section gives the overview of the steps required to configure the common classifiers on the OA-700, which includes the “Lists and Match-lists”.

Step 1: At the inception, you are required to have a thorough knowledge of the elements used in configuring CC before proceeding further. The elements give a deeper understanding of the concept and framework required to configure lists, match-lists and arguments used for configuring advanced rulesets within the match-lists. See [“Elements Used in Configuring CC”](#)

Step 2: Configure Match-lists. See [“To Configure a Match-list”](#)

Step 3: Configure the appropriate rules within the match-list sub-configuration mode. These rules are a combination of different elements and their arguments. See [“Rules within Match-lists”](#)

Step 4: You are required to have a thorough knowledge of Lists (though “lists” are optional), since it acts as a powerful tool to minimize the number of rules within a match-list. See [“To Configure a List”](#)

Step 5: A match-list can be referenced and included in a new match-list. See [“Nesting Of Match-lists”](#)

Step 6: To view the configuration, see [“Show commands in CC”](#).

Step 7: The configured rules and match-lists can be removed with the help of the respective deletion commands. See [“Deletion Commands in CC”](#)

ELEMENTS USED IN CONFIGURING CC

Classifications are composed of one or more rulesets each of which consists of one or more rules. Rules in turn consists of individual elements arranged in a specific manner. Elements are the basic building blocks and include the following:

ELEMENT TYPES AND THEIR DESCRIPTIONS

This section provides details on the various parameters used while configuring the Common Classifiers.

Element Type	Description
IP address/mask (Subnet/Prefix)	Specifies the IP address and mask or IP address with prefix. Host can be specified for a single IP address without a mask.
Host	Implies a single IP address without a mask. The keyword "host" must be prefixed with an IP address.
from	Specifies a 16 bit UDP or TCP Source port.
service	Specifies a 16 bit UDP or TCP Destination port.
interface	Refers to an interface in the system.
Protocol	The protocols supported are: IP, TCP, UDP, and ICMP. It is also possible to define a specific protocol like IKE by using the keyword "Protocol".
IP Precedence	Specifies the IP precedence.
ToS	Specifies the Type of Service.
ICMP type and subtype	When ICMP is specified as protocol, the ICMP type and sub-type can be included in the ruleset.
TCP Flags	TCP flags such as RST, SYN, FIN, ACK, URG. This is valid only when the protocol is TCP.
Fragment flag	Used to match an IP fragment.
Packet length	Specifies a packet length.
Range used with Packet Length	Specifies the range of a packet length.
Traffic type or class (Type)	A higher level description of the packet stored in the packet context, derived from some application or feature. Used by the ALGs (Application Level Gateways).
DSCP	Specifies IP Differential Service Code Point (DSCP).



Note: The elements ToS, IP-Precedence, and DSCP are all going to be part of IP-header-> ToS field.

For configuration purpose, DSCP and ToS, IP-Precedence are mutually exclusive. This means you cannot configure DSCP if you have configured either ToS or IP-Precedence and vice versa.

MNEMONICS FOR DSCP

Mnemonic	Description
af11	Assured Forwarding 11
af12	Assured Forwarding 12
af13	Assured Forwarding 13
af21	Assured Forwarding 21
af22	Assured Forwarding 22
af23	Assured Forwarding 23
af31	Assured Forwarding 31
af32	Assured Forwarding 32
af33	Assured Forwarding 33
af41	Assured Forwarding 41
af42	Assured Forwarding 42
af43	Assured Forwarding 43
cs1	Class Selector 1
cs2	Class Selector 2
cs3	Class Selector 3
cs4	Class Selector 4
cs5	Class Selector 5
cs6	Class Selector 6
cs7	Class Selector 7
default	Default
ef	Expedited Forwarding

MNEMONICS FOR IP-PRECEDENCE

Mnemonic	Description
routine	Match packets with routine precedence (0)
priority	Match packets with priority precedence (1)
immediate	Match packets with immediate precedence (2)
flash	Match packets with flash precedence (3)
flash-override	Match packets with flash override precedence (4)
critical	Match packets with critical precedence (5)
internet	Match packets with internetwork control precedence (6)
network	Match packets with network control precedence (7)



Note: The change applies to the following rule commands IP, TCP, UDP, AH, ESP.

MNEMONICS FOR TOS

Mnemonic	Description
max-reli	Maximum reliability (2)
max-tput	Maximum throughput (4)
min-cost	Minimize monetary cost (1)
min-delay	Minimize delay (8)
normal	Normal Service (0)

To CONFIGURE A MATCH-LIST

Command (in CM)	Description
<code>match-list <name></code>	This command is used to configure a match-list. This enters Match-list Configuration Mode.

EXAMPLE

```
ALU(config)# match-list test
ALU(config-match-list-test)#
```

RULES WITHIN MATCH-LISTS

Rules are the main classification component, and are constructed using a specific syntax that may reference other elements and/or lists as part of the rule. A single rule roughly corresponds to one line of an match-list without the permit/deny action. Rules indicate specific fields of packets that must match in order for the rule itself to match. A group of rules is termed as a **ruleset**, which forms a **match-list**.

Rulesets are the collection of rules that are grouped into a single classification and become the objects that different features refer when binding classification to their parameters. Apart from this, these rules are applied for all flows irrespective of the interfaces. Each rule is differentiated by a line number.

In general, the following have to be considered before configuring a rule:

- The Source / Destination (from / to) order of the fields must configure a rule.
- The fields specified in the rule must all match for the rule to be matched, so the components of the rule can be considered to have a boolean AND function applied.



Note: A match-list matches if **any** of the rule matches.

- In the situation where a list is used, any of the members of the list may match, but at least one must match before that field is considered a match for that rule.
- The “**service**” keyword in TCP and UDP protocols refer to the destination port. Currently, the ‘service’ keyword in TCP or UDP can have only the following values:
`ftp-data | ftp | ssh | telnet | smtp | dns | tftp | http | pop2 | pop3 | imap | snmp | snmptrap | bgp`

- The “**from**” keyword in TCP and UDP protocols refer to the source port.
- The keyword “**type**” is used to access the ALGs.
- There is no ordering of rules inside a match-list. All the rules are of same priority. The rule numbers are used only for reference.
- The ordering of keywords after the initial protocol and source/destination fields is not defined, and can be in any order. Some keywords are mutually exclusive, and/or dependant on other keywords e.g the service specification is only applicable for TCP or UDP packets, and is mutually exclusive with the fragment keyword.
- The usage of the AH and ESP keywords are similar to IP protocol. Their applications are usually in the security domains.
- The protocol keyword is used to assign a number to the protocol types in use. The protocol name to number mapping can be found at <http://www.iana.org/assignments/protocol-numbers>.

To CONFIGURE A RULE

Command (in Match-list CM)	Description
[<1-65535>] [<protocol>] [<source>] [<destination>] [from <port number>] [to <port number>]] [<fields to be matched>]	This command is used to configure a rule for protocols like IP, TCP, UDP, etc.

EXAMPLE

```
ALU(config-match-list-test)# 10 tcp host 1.1.1.1/32 any from 6050 to 80
```

The above concept can be made clear by referring to the following examples:

EXAMPLE

Ex 1:

To classify traffic coming from network 192.168.10.0/24 and going to 192.168.11.0/24, the match-list would look as shown below.

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# tcp prefix 192.168.10.0/24 prefix 192.168.11.0/24 service ssh
```

The following two examples depicts the usage of elements like the interface and the prefix:

Ex 2:

The following example shows how multiple rules can be configured within the same match-list:

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 tcp prefix 10.0.0.0/8 interface
GigabitEthernet 3/0 service ssh

ALU(config-match-list-m1)# 2 udp interface GigabitEthernet
7/0 interface GigabitEthernet 3/0 fragment length eq 1659

ALU(config-match-list-m1)# 3 icmp any any length gt 92
```

Ex 3:

To classify traffic coming from network 192.168.10.0/24 and going to 192.168.11.0/24. Match-list M1 depicts this. Match-lists 2 and 3 depicts the usage of UDP and ICMP protocols in CC.

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 tcp prefix 192.168.10.0/24
prefix 192.168.11.0/24 service ssh

ALU(config)# match-list m2
ALU(config-match-list-m2)# 1 udp interface GigabitEthernet
3/0 interface GigabitEthernet 7/0

ALU(config)# match-list m3
ALU(config-match-list-m3)# 1 icmp any any
```

To CONFIGURE RULES FOR IP

Command (in Match-list CM)	Description
<pre>[<1-65535>] ip {any host <source ip-address>} interface <name> list <name> prefix <source ip-address/prefix length>} {any host <destination ip-address>} interface <name> list <name> prefix <destination ip-address/prefix length>} [dscp {<0-63> <dscp-mnemonics>} fragment ip-precedence {<0-7> <precedence-mnemonics>} length {<1-1500> {eq ge gt le lt range <1-1500>}} tos {<0-15> <tos-mnemonics>} type {ftp normal rpc sip tftp}]</pre>	<p>This command is used to configure rules for IP in a match-list.</p> <p>You can define a rule with subnets, host addresses, or interfaces or list of any of them.</p>

EXAMPLE

Ex 1:

The following example configures a IP rule with 'any any' and type 'ftp':

```
ALU(config-match-list-test)# ip any any type ftp
```

Ex 2:

These rules used in the match-list example below, once configured can be applied to all/any applications just by referencing its name. You need not have to repeatedly configure the match-list for every application.

```
ALU(config)# match-list 101
ALU(config-match-list-101)# 1 ip any prefix 10.0.0.0/8 type ftp
ALU(config-match-list-101)# 2 ip prefix 21.1.1.0/24 host 41.2.2.2
```

Ex 3:

The power and flexibility of the rulesets can be best seen when the list references are used, especially in multiple fields, e.g., the following configuration:

```
ALU(config)# list i1 prefix 10.0.0.0/8 prefix 11.0.0.0/8
ALU(config)# list i2 prefix 20.0.0.0/8 prefix 21.0.0.0/8

ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 ip list i1 list i2 type normal
ALU(config-match-list-m1)# 2 ip list i1 list i2 type rpc
ALU(config-match-list-m1)# 3 ip list i1 list i2 type ftp
ALU(config-match-list-m1)# 4 ip list i1 list i2 type tftp
```


To CONFIGURE RULES FOR TCP

Command (in Match-list CM)	Description
<pre>[<1-65535>] tcp {any host <source ip-address> interface <name> list <name> prefix <source ip-address/prefix length>} {any host <destination ip-address> interface <name> list <name> prefix <destination ip-address/prefix length>} [ack dscp {<0-63> <dscp-mnemonics>} established fin fragment from <1-65536> ip-precedence {<0-7> <precedence-mnemonics>} length {<1-1500> {eq ge gt le lt range <1-1500>}} rst service {<1-65536> <protocol>} syn urg tos {<0-15> <tos-mnemonics>} type {ftp normal rpc sip tftp}]</pre>	<p>This command is used to configure rules for TCP protocol in a match-list.</p>

EXAMPLE

Ex 1:

The following example configures a TCP rule with 'any any' and service 'smtp', and another TCP rule with 'any any' and type 'normal':

```
ALU(config-match-list-test)# tcp any any service smtp

ALU(config-match-list-test)# tcp any any type normal
```

Ex 2:

This example gives a list of possible rules that can be used in a match-list, with a comparison of the 'service' keyword used in case of "tcp".

```
ALU(config-match-list-m1)# ip prefix 10.0.0.0/8 any
ALU(config-match-list-m1)# ip host 10.0.0.0 any
ALU(config-match-list-m1)# ip prefix 192.168.1.0/24 host 10.0.0.0
ALU(config-match-list-m1)# tcp interface GigabitEthernet7/0 interface GigabitEthernet 3/0 service smtp
```

Ex 3:

The power and flexibility of the rulesets can be best seen when the list references are used, especially in multiple fields e.g the following configuration:

```
ALU(config)# list i1 prefix 10.0.0.0/8 prefix 11.0.0.0/8
ALU(config)# list i2 prefix 20.0.0.0/8 prefix 21.0.0.0/8
ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 tcp list i1 list i2 service telnet
```

To CONFIGURE RULES FOR UDP

Command (in Match-list CM)	Description
<pre>[<1-65535>] udp {any host <source ip-address> interface <name> list <name> prefix <source ip-address/prefix length>} {any host <destination ip-address> interface <name> list <name> prefix <destination ip-address/prefix length>} [dscp {<0-63> <dscp-mnemonics>} fragment from <1-65536> ip-precedence {<0-7> <precedence-mnemonics>} length {<1-1500> {eq ge gt le lt range <1-1500>}} service {<1-65536> <protocol>} tos {<0-15> <tos-mnemonics>} type {ftp normal rpc sip tftp}]</pre>	<p>This command is used to configure rules for the UDP protocol in a match-list.</p>

EXAMPLE

Ex 1:

The following example configures a UDP rule with 'any any' and service 'tftp':

```
ALU(config-match-list-test)# udp any any service tftp
```

Ex 2:

In this example, we have 2 networks 192.168.1.0/24 and 192.168.2.0/24, which need to communicate with 2 other networks 192.168.18.0/24 and 192.168.19.0/24 using tftp. This can be represented by the classifier as:

```
ALU(config)# list L3 prefix 192.168.1.0/24 prefix
192.168.2.0/24
ALU(config)# list L4 prefix 192.168.18.0/24 prefix
192.168.19.0/24
```

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 udp list L3 list L4 service
tftp
```

To CONFIGURE RULES FOR ICMP

Command (in Match-list CM)	Description
<pre>[<1-65535>] icmp {any host <source ip-address> interface <name> list <name> prefix <source ip-address/prefix length>} {any host <destination ip-address> interface <name> list <name> prefix <destination ip-address/prefix length>} [dscp {<0-63> <dscp-mnemonics>} fragment icmp-type <0-255> [icmp-subtype <0-255>] ip-precedence {<0-7> <precedence-mnemonics>} length {<1-1500> {eq ge gt le lt range <1-1500>}} tos {<0-15> <tos-mnemonics>}]</pre>	<p>This command is used to configure rules for the ICMP protocol in a match-list.</p>

EXAMPLE

The following example configures a ICMP rule with 'any any' and icmp-type value 10, and icmp-subtype value 5:

```
ALU(config-match-list-test)# icmp any any icmp-type 10 icmp-subtype 5
```

To CONFIGURE RULES USING THE PROTOCOL NUMBERS

Command (in Match-list CM)	Description
<pre>[<1-65535>] protocol <1-65535> {any host <source ip-address> interface <name> list <name> prefix <source ip-address/prefix length>} {any host <destination ip-address> interface <name> list <name> prefix <destination ip-address/prefix length>} [dscp {<0-63> <dscp-mnemonics>} fragment ip-precedence {<0-7> <precedence-mnemonics>} length {<1-1500> {eq ge gt le lt range <1-1500>}} tos {<0-15> <tos-mnemonics>} type {ftp normal rpc sip tftp}]</pre>	<p>This command is used to configure rules using the protocol numbers.</p>

EXAMPLE

The following example configures a rule using the Protocol number '1' with 'any any' and dscp value 10:

```
ALU(config-match-list-test)# 10 protocol 1 any any dscp 10
```

LISTS IN CC

Lists are a defined group of elements like group of Interfaces, IP addresses, and subnets, which are referenced by the match-lists to create a rule. This is helpful when you need to create some complex rules, which references several group of interfaces or IP addresses.

If the list is also referenced in a rule, any member of the list can match the rule, so the relationship between the members of the list, is a boolean. Lists may also include other lists by referencing the other list's name, effectively extending the list by concatenating the elements in the other lists.

TO CONFIGURE A LIST

Command (in CM)	Description
<pre>list <name> {host <ip-address>... include <list-name>... interface <name>... prefix <ip-address/ prefix-length>...}</pre>	Use this command to configure lists, which can be used within match-lists.

EXAMPLE

Ex 1:

Lists may also include other lists by referencing the other list's name, effectively extending the list by combining the elements in the other list as shown below:

```
ALU(config)# list l1 interface GigabitEthernet 3/0 interface
serial 1/0:0
```

```
ALU(config)# list l2 prefix 10.0.0.0/8 prefix 20.0.0.0/8
```

```
ALU(config)# list Zone1 list l1 list l2
```

Ex 2:

In this example, there are two networks 192.168.1.0/24 and 192.168.2.0/24, which need to communicate with two other networks 192.168.18.0/24 and 192.168.19.0/24. This can be represented by CC as:

```
ALU(config)# list L3 prefix 192.168.1.0/24 prefix
192.168.2.0/24
```

```
ALU(config)# list L4 prefix 192.168.18.0/24 prefix
192.168.19.0/24
```

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 tcp list L3 list L4 service
telnet
ALU(config-match-list-m1)# 2 tcp list L3 list L4 service
telnet
ALU(config-match-list-m1)# 3 udp list L3 list L4 service
snmp
```

Ex 3:

The example below specifies lists of interfaces and subnets. These lists can be used in the match-lists for specific applications.

```
ALU(config)# list L1 interface GigabitEthernet 7/0 interface
GigabitEthernet 7/1
ALU(config)# list L2 prefix 192.168.12.0/24 prefix
192.168.13.0/24

ALU(config)# match-list m1
ALU(config-match-list-m1)#1 udp list L1 list L2 service snmp
```

Ex 4:

In this example, we have 2 hosts 192.168.1.0 and 192.168.1.1, which need to communicate with 2 other hosts 192.168.18.0 and 192.168.18.1 This can be represented by the classifier as:

```
ALU(config)# list L3 host 192.168.1.0 host 192.168.1.1
ALU(config)# list L4 host 192.168.18.0 host 192.168.18.1

ALU(config)# match-list m2
ALU(config-match-list-m2)# tcp list L3 list L4 service
telnet
```

Ex 5:

This example shows a simple usage of match-list with a single rule.

```
ALU(config)# list L1 host 21.1.1.1 interface GigabitEthernet
7/0

ALU(config)# match-list m1
ALU(config-match-list-m1)# ip list L1 prefix 20.1.0.0/16
```

Ex 6:

The match-list in the example shown below, specifies rule for SSH and POP3 traffic from any source and destined for network 192.168.12.0/24 and 192.168.13.0/24.

```
ALU(config)# list L1 prefix 192.168.12.0/24 prefix
192.168.13.0/24

ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 tcp any list L1 service ssh
ALU(config-match-list-m1)# 2 tcp any list L1 service pop3
```

NESTING OF MATCH-LISTS

Another key feature of the Unified classification is the capability of nesting. A match-list configured earlier can be referenced and included in a new match-list. This prevents you from re-writing same rules for a different match-list.

TO ENABLE NESTING OF MATCH-LISTS

Command (in Match-list CM)	Description
<code>include <match-list name></code>	Enter this command in the specific Match-list Configuration Mode. This command is used to include a match-list/s that is already configured inside another match-list.

EXAMPLE

Ex 1:

In the example below, the match-list m2 contains the rule of match-list m1 in addition to the other rules specific to match-list m2.

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# ip prefix 192.168.1.0/24    host
192.168.1.72

ALU(config)# match-list m2
ALU(config-match-list-m2)# tcp any any service ssh
ALU(config-match-list-m2)# tcp prefix 192.168.2.0/24 any
service smtp
ALU(config-match-list-m2)# include m1
```

Ex 2:

Consider another example to configure match-lists, using appropriate rulesets with the 'include' keyword.

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# 1 prefix 10.0.0.0/8 host 21.1.1.1
ALU(config-match-list-m1)# 2 list l2 list l3

ALU(config)# match-list m2
ALU(config-match-list-m2)# 1 tcp any any service ssh
ALU(config-match-list-m2)# 2 udp prefix 22.1.1.0/8 any
ALU(config-match-list-m2)# 3 ip host 21.1.1.1 type rpc

ALU(config-match-list-m2)# 4 include m1
```



Note: There is no ordering of rules inside a match-list. All the rules are of same priority. The rule numbers are used only for reference.

Ex 3:

Consider the following example with the necessary modes of configurations included:

```
ALU> en
ALU# configure terminal
ALU(config)# list l1 host 192.168.0.4 prefix 192.168.0.1/24
interface GigabitEthernet7/0

ALU(config)# list l2 host 192.168.0.3 include l1
ALU(config)# match-list m1

ALU(config-match-list-m1)# tcp any list l1 length 23 from
ssh service range 23 35
ALU(config-match-list-m1)# exit

ALU(config)# match-list m2
ALU(config-match-list-m2)# include m1
```

SHOW COMMANDS IN CC

To VIEW LISTS

Command (in SUM)	Description
<code>show list [<name>]</code>	This command displays the details of all the lists that are configured. Specify the list name to view the details of a specific list.

EXAMPLE

The following example displays details of all the lists configured:

```
ALU(config)# show list
```

```
list 11 host 5.5.5.5 host 4.4.4.4 prefix 6.6.6.0/24
list 12 host 5.3.4.6 prefix 1.10.10.0/24
```

The following example displays the details of the list L1 and L2 configured:

```
ALU(config)# show list 11
```

```
list 11 host 5.5.5.5 host 4.4.4.4 prefix 6.6.6.0/24
ALU(config)#
```

```
ALU(config)# show list 12
```

```
list 12 host 5.3.4.6 prefix 1.10.10.0/24
ALU(config)#
```


To VIEW MATCH-LISTS

Command (in SUM)	Description
show match-list [<i><name></i>]	This command displays the details of all the match-lists that are configured. Specify the match-list name to view the details of a specific match-list.

EXAMPLE

The following example displays details of all the match-lists configured:

```
ALU(config-match-list-m1)# show match-list
```

```
match-list m1
1 icmp any any
2 tcp any any service http
3 ip any any type ftp
```

```
match-list m2
1 tcp any any service ssh
```

```
match-list m3
1 udp any any
```

The following example displays the details of match-lists m1 and m2:

```
ALU(config-match-list-m1)# show match-list m1
```

```
match-list m1
1 icmp any any
2 tcp any any service http
3 ip any any type tftp
```

```
ALU(config-match-list-m1)# show match-list m2
```

```
match-list m2
1 tcp any any service ssh
2 udp any any
```

To VIEW A SPECIFIC RULE

Command (in Match-list CM)	Description
<code>show rule <1-65535></code>	This command is entered within the Match-list Configuration Mode to display the details of the rule corresponding to the line/rule number specified.

EXAMPLE

The following example displays the details of the rule in line number 2:

```
ALU(config-match-list-m1)# show rule 2
```

```
2 udp prefix 22.1.1.0/8 any
```

The following example displays the details of the rule in line number 1:

```
ALU(config-match-list-m1)# show rule 1
```

```
1 tcp any any service ssh
```

To VIEW THE DETAILS OF THE INCLUDED MATCH-LIST

Command (in Match-list CM)	Description
<code>show include</code>	This command is entered within the Match-list Configuration Mode to display all the match-lists which are included/nested with the match-list under consideration.

EXAMPLE

The following example displays the details of match-list m1:

```
ALU(config-match-list-m2)# show include
```

```
match-list m1
```

```
1 tcp any any service ssh
```

```
2 udp prefix 22.1.1.0/8 any
```

DELETION COMMANDS IN CC

To DELETE A LIST

Command (in CM)	Description
<code>no list <name></code>	This command deletes the list with reference to its name.



Note: If a list is in use, it cannot be deleted. The deletion of lists cannot be globally applied to all the lists that are configured. They can be deleted one at a time.

EXAMPLE

The following example deletes the list L1:

```
ALU(config)# no list L1
```

To DELETE A MATCH-LIST

Command (in CM)	Description
<code>no match-list <name></code>	This command deletes the match-list with reference to its name.



Note: If a match-list is in use, it cannot be deleted. The deletion of match-lists, as in case of lists, cannot be globally applied to all the match-lists that are configured. They can be deleted only one at a time.

EXAMPLE

The following example deletes the match-list M1:

```
ALU(config)# no match-list M1
```

To DELETE A RULE

Command (in Match-list CM)	Description
no rule <1-65535>	This command is entered in the Match-list Configuration mode to delete a specific rule from that Match-list, with reference to its line/rule number.

EXAMPLE

Consider the following example:

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# 10 tcp host 1.1.1.1/32 any from
6050 to 80
```

Now, to delete the rule having rule number 10, use the 'no rule' command:

```
ALU (config-match-list-m1)# no rule 10
```

To DELETE THE INCLUDED MATCH-LIST

Command (in Match-list CM)	Description
no include <match-list name>	Enter this command in the specific Match-list Configuration Mode. This command is used to delete the match-list, that is included in another match-list.

EXAMPLE

Consider the following example:

```
ALU(config)# match-list m2
ALU(config-match-list-m2)# 1 tcp any any service ssh
ALU(config-match-list-m2)# 2 udp prefix 22.1.1.0/8 any
ALU(config-match-list-m2)# 3 include m1
```

Now, to delete the included match-list, use the 'no include' command:

```
ALU(config-match-list-m2)# no include match-list m1
```

SAMPLE EXAMPLES ON THE USAGE OF CC ACROSS APPLICATIONS

EXAMPLE 1

The example below shows a series of match-list configurations for different applications.

```
match-list blr-tunnel
  1 ip prefix 10.91.0.0/24 prefix 10.0.1.0/24

match-list SV-tunnel
  1 ip prefix 10.0.1.0/24 prefix 10.91.0.0/24

match-list ike
  1 udp host 203.196.196.74 host 64.174.59.66 from 500

match-list esp
  1 esp host 203.196.196.74 host 64.174.59.66

match-list nat
  1 ip prefix 10.91.0.0/24 any

match-list ike-SV
  1 udp host 64.174.59.66 host 203.196.196.74 from 500

match-list esp-SV
  1 esp host 64.174.59.66 host 203.196.196.74

match-list icmp
  1 icmp prefix 10.91.0.0/24 prefix 10.0.1.0/24

match-list icmp-traffic
  1 icmp any any

match-list dos
  1 ip any any

match-list ospf
  1 89 any any
```

EXAMPLE 2

In the following example, there are several rulesets ('match-lists'), as well as a client (a 'filter', roughly equivalent to an 'access-group' specification) that references the different rulesets and applies actions (permit or deny) to the packets that are matched in the various classifications.

```
list L1
  interface GigabitEthernet 7/0 prefix 10.1.0.0/16
  prefix 20.0.0.0/8 host 30.1.1.1 host 40.1.1.0

list L2
  prefix 192.168.0.0/16 prefix 192.170.0.0/16

list L3
  interface GigabitEthernet 3/0 interface GigabitEthernet 7/1

match-list m1
  ip List L1 interface GigabitEthernet 7/0

match-list m2
  tcp any List L2 service telnet
  tcp any List L2 type normal

match-list m3
  ip prefix 192.99.55.0/24 any
  udp prefix 11.0.0.0/8 host 12.1.1.1 IP Precedence 5
  tcp L1 interface GigabitEthernet 7/1 service smtp
  ip any L2
  ip any L1
  include m2

ip filter f1
  match all m1 m2 permit
  match m3 permit
  match m2 deny reset
```

EXAMPLE 3

In the following example, we have 2 networks 192.168.1.0/24 and 192.168.2.0/24 which need to communicate with 2 other networks 192.168.18.0/24 and 192.168.19.0/24 using telnet. This can be represented by the classifier as:

```
list L3
  prefix 192.168.1.0/24 prefix 192.168.2.0/24

list L4
  prefix 192.168.18.0/24 prefix 192.168.19.0/24

match-list m1
  tcp list L3 list L4 service telnet
```

Now, a filter can be created and applied to the appropriate interface.

```
ip filter f1
  match m1 permit
  interface GigabitEthernet 7/1
    ip filter in f1
```


Part 5 Routing Protocols

CHAPTER 19 PROTOCOL INDEPENDENT FEATURES

PROTOCOL INDEPENDENT FEATURES CONFIGURATION

This chapter describes configuration of the IP routing protocol-independent features. Refer to the following sections to configure Protocol Independent features on your system:

- [“Protocol-Independent Configuration”](#)
- [“Protocol-Independent Configuration Commands”](#)
- [“Protocol Independent Features Show Commands”](#)
- [“Protocol Independent Features Clear Command”](#)

CHAPTER CONVENTIONS

Acronym	Description
UM	User Mode - ALU>
SUM	Super User Mode - ALU #
CM	Configuration Mode - ALU (config)#
RCM	Router Configuration Mode - ALU (config-router ospf)#
Route map CM	Route Map Configuration Mode -ALU (config-route-map)#
Standard IP Access list CM	Configuration Mode - ALU (config-std-nac1)#
Extended IP Access list CM	Configuration Mode - ALU (config-ext-nac1)#
ICM	Interface Configuration Mode - ALU (config-if)#

PROTOCOL-INDEPENDENT CONFIGURATION

To configure optional protocol-independent features, perform any of the tasks described in the following sections:

- **“Configure Static Routes”**
- **“Configure IP Unnumbered Interface”**
- **“Configure Access-List”**
- **“Configure Prefix-list”**
- **“Configure AS-path Access-list”**
- **“Configure Route Maps”**
- **“Redistribute Routing Information”**
- **“Filtering Routing Information”**
- **“Configure Administrative Distance”**
- **“Configure Maximum Paths”**
- **“Protocol Independent Features Clear Command”**
- **“Protocol Independent Features Show Commands”**

PROTOCOL-INDEPENDENT CONFIGURATION COMMANDS

The following sections detail the Protocol-independent configuration commands in the OA-700.

CONFIGURE STATIC ROUTES

Static routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the routing protocol cannot build a route to a particular destination.

When an interface goes down, all static routes through that interface are removed from the IP routing table. Also, when the address specified for the forwarding router in a static route is invalid (not reachable), the static route is removed from the IP routing table.

- Static routes for Point-to-point links (like Serial, GRE tunnel interfaces) can be configured without Gateway IP address.
- Static routes for Ethernet interfaces have to be configured with gateway IP address.
- If gateway address as well as interface name is specified in the static route, then route is activated only if gateway is reachable through the specified interface.

Router might not be able to determine the routes to all other networks. In that case, you can configure default static route.



Note:

You can override static routes with dynamic routing information by assigning administrative distance.

You can configure route for same network through different interfaces, and with different weights. In this case, route with less administrative distance is used for forwarding. But, when route with less administrative distance becomes unreachable, router starts using route with the next highest administrative distance.

Command (in CM)	Description
<code>ip route {destination network subnet-mask destination network/prefix-length} {<gateway-ip-address> <interface-name> [<gateway-ip-address>]} [<1-255>]</code>	This command is used to configure a static route.

EXAMPLE

```
ALU(config)# ip route 1.1.1.0/24 2.2.2.2
```

CONFIGURE IP UNNUMBERED INTERFACE



Note: This is valid only for Serial point-to-point and ISDN interfaces only.

Typically to make an interface 'IP enabled', an IP address is configured on it. However, configuring IP addresses for point-to-point interfaces leads to wasting internet IP addresses/IP subnets. To solve this problem, the concept of unnumbered interfaces is used.

The IP unnumbered configuration command enables IP processing on an interface without assigning it an explicit IP address. The IP unnumbered interface can "borrow" the IP address of another interface already configured on the router that is up and running.

It is recommended that the unnumbered interface point to a loopback interface since loopback interface does not fail.

Command (in ICM)	Description
<code>ip unnumbered <interface-name> <slot/port></code>	<p>This command is used in the Interface Configuration mode.</p> <p>This command is used to configure an interface to be an unnumbered interface and associate a numbered IP interface with it.</p> <p>Use of this command results in the IP address being shared by two interfaces.</p>
<code>no ip unnumbered <interface-name> <slot/port></code>	This command is used to unconfigure the unnumbered interface.

- The interface specified must be the name of another interface in the system that has an IP address, not another unnumbered interface.
- If the associated/numbered interface is configured as an unnumbered interface, then the existing IP address shall be deleted and the interface shall be made as an unnumbered interface. In this case, the unnumbered interface also loses the IP address.
- If the IP address on the associated numbered interface is deleted, then the unnumbered interface also loses the IP address.
- If the associated numbered interface is deleted, then the unnumbered interface loses the IP address.
- Unnumbered IP on Serial interfaces shall support PPP, HDLC, FR, MLPPP, MLFR, encapsulations.



Note: OA-700 supports static routing over unnumbered interfaces. Dynamic routing protocols on unnumbered interface (RIP, OSPF, and BGP) are not supported.

EXAMPLE

Configuring a Serial interface to be an unnumbered interface. The IP address configured on the GigabitEthernet 7/0 interface is also assigned to the interface Serial 0/0:0, and both interfaces involved function normally.

```
ALU(config)# interface serial 0/0:0
ALU(config-serial-0/0:0)# ip unnumbered GigabitEthernet 7/0
```

Configuring Ethernet as an unnumbered interface throws up an error:

```
ALU(config)# interface GigabitEthernet 7/0
ALU(config-serial-0/0:0)# ip unnumbered Loopback 0
Point-to-point interfaces only
```

CONFIGURE ACCESS-LIST

Access-lists are an ordered sequence of individual statements, each having a permit or deny result. Evaluation of ACL consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is aborted once the first statement match is found and an action associated with the statement match is performed.

The main result from the evaluation of an access-list is permit or deny. When applied to redistribution, an ACL determines if a particular route can or cannot be redistributed.

Each ACL ends with an implicit deny statement, by design convention; there is no similar convention for route-maps. If the end of a route-map is reached during matching attempts, the result depends on the specific application of the route-map. Access-lists are used in route map as a matching parameter.



Note: In OA-700, access lists are only used for control plane filtering. BGP uses access-lists for filtering update packets from/to neighbor. BGP also uses community-lists and as-path lists.

For filter functionality, refer "[Filter and Firewall](#)" chapter.

There are 2 types of access-lists:

- Standard access-list
- Extended access-list

Standard access lists uses only source IP addresses configured in the ACL. Extended access-list uses both source IP addresses as well as destination IP address. Extended access lists are more convenient to use when some networks must be allowed and some disallowed, within the same major network.

To CONFIGURE STANDARD ACCESS-LIST

Command (in CM)	Description
access-list {<1-99> <1300-1999>} { deny permit } { <i>ip-address</i> [<i>network-number</i>] <i>ip-address/prefix-length</i> any host < <i>host-ipaddress</i> >} [log]	This command is used to configure a Standard Access-list.

EXAMPLE

```
ALU(config)# access-list 1 deny 1.0.0.0/8
```

```
ALU(config)# access-list 2 permit 20.0.0.0/8
```

To CONFIGURE EXTENDED ACCESS-LIST

Command (in CM)	Description
access-list {<100-199> <2000-2699>} { deny permit } {<0-255> gre icmp ipinip pim rsvp tcp udp } { <i>source-ip-address</i> [<i>network-number</i>] <i>source-ip-address/prefix-length</i> any host < <i>source-host-ipaddress</i> >} { <i>destination-ip-address</i> [<i>network-number</i>] <i>destination-ip-address/prefix-length</i> any host < <i>destination-host-ipaddress</i> >} [log]	This command is used to configure an Extended Access-list.

EXAMPLE

```
ALU(config)# access-list 101 permit ip 162.168.0.0 0.0.0.0
255.255.252.0 0.0.0.0
```


CONFIGURE IP ACCESS-LIST

IP Access-lists are named access-lists. This allows standard and extended access-lists to be given names instead of number. Rules are specified in the IP Access-lists Configuration Mode. One access list can have multiple rules. Rules specify permit or deny actions. Rules are searched in the given order. If one rule is not matched, it starts searching for the next rule. These IP access lists can be used in route-maps for matching.

TO CONFIGURE STANDARD IP ACCESS-LIST

Command (in CM)	Description
<code>ip access-list standard {<1-99> <1300-1999> <access-list-name>}</code>	This command is used to define a named access list. And, enters Standard Access-list Configuration Mode.

EXAMPLE

```
ALU(config)# ip access-list standard test
ALU(config-std-nacl)#
```

TO CONFIGURE STANDARD IP ACCESS-LIST RULE

Command (in Standard IP Access-list CM)	Description
<code>{permit deny} {any host <host-ip-address> <ip-address/prefix-length> <ip-address subnet-mask>} [log]</code>	This command is used to configure a rule for a Standard IP Access-List. You can configure multiple rules for an IP access list.

EXAMPLE

```
ALU(config-std-nacl)# permit host 10.0.0.1
ALU(config-std-nacl)# permit 11.0.0.0/8
```

TO CONFIGURE EXTENDED IP ACCESS-LIST

Command (in CM)	Description
<code>ip access-list extended {<100-199> <2000-2699> <access-list-name>}</code>	This command is used to define a named access list. And, enters Extended Access-list Configuration Mode.

EXAMPLE

```
ALU(config)# ip access-list extended test
ALU(config-ext-nacl)#
```

To CONFIGURE EXTENDED IP ACCESS-LIST RULE

Command (in Extended IP Access-list CM)	Description
<pre>{permit deny} {igmp icmp ip ipinip pim rsvp tcp udp <0-255>} {any host <host-ip-address> <source-ip- address/prefix-length> <source- ip-address subnet-mask>} [operators] {any host <host-ip- address> <destination-ip-address/ prefix-length> <destination-ip- address subnet-mask>} [log] [log- input] [enable fragment] [precedence [<0-7> <keywords>] [tos [<0-15> <keywords>]]]</pre>	<p>This command is used to configure a rule for a Extended IP Access-List.</p> <p>You can configure multiple rules for an IP access list.</p>

EXAMPLE

```
ALU(config-ext-nacl)# permit ip 24.0.0.0/8 25.0.0.0/8
```

```
ALU(config-ext-nacl)# deny ip any 13.0.0.0/8
```

CONFIGURE COMMUNITY-LIST

There are two types of Community-lists:

- Standard Community-list
- Extended Community-list

Standard community-lists are used to configure well-known communities and specific community numbers. Extended community-lists are used to filter communities using a regular expression.

Regular expressions are used to configure patterns to match community attributes. All of the standard rules of access-lists apply to the configuration of extended community lists. Regular expressions are supported by the expanded range of extended community-list numbers.

TO CONFIGURE STANDARD COMMUNITY-LIST

Command (in CM)	Description
<code>ip community-list <1-99> {deny permit} [<1-4294967295> <AA:NN> internet local-AS no- advertise no-export]</code>	This command is used to configure a Standard Community-list. Creates a community-list for BGP and controls access to it.

EXAMPLE

```
ALU(config)# ip community-list 1 permit internet
```

```
ALU(config)# ip community-list 2 permit no-export
```

TO CONFIGURE EXTENDED COMMUNITY-LIST

Command (in CM)	Description
<code>ip community-list <100-199> {deny permit} <regular- expression></code>	This command is used to configure a Extended Community-list.

CONFIGURE PREFIX-LIST

IP Prefix-list provides prefix based filtering mechanism. In addition to the access-list functionality, IP Prefix-list has prefix length range specification and sequential number specification. You can add or delete prefix based filters to arbitrary points of prefix-list using sequential number specification.

Command (in CM)	Description
<code>ip prefix-list <name> [seq <1-4294967294>] {{deny permit} <ip-address/prefix-length> {ge le} <0-32> description <line>}</code>	This command is used to configure a Prefix-list.

EXAMPLE

In the following example, permit updates for any network with a prefix mask length less than or equal to 23. Denies all network updates with a network mask length greater than 23.

```
ALU(config)# ip prefix-list test permit 0.0.0.0/0 le 23
```



Note: Less than or equal to prefix numbers and greater than or equal to prefix numbers can be used together. The order of the le and ge commands does not matter.

CONFIGURE AS-PATH ACCESS-LIST

A regular expression is a pattern used to match against an input string. In case of BGP, we can have a regular expression to match particular autonomous system path. This is used to filter updates from neighbors.

Command (in CM)	Description
<code>ip as-path access-list <1-199> {deny permit} <regular-expression></code>	This command is used to configure AS-path Access-list.

EXAMPLE

In the following example, the IP as-path access-list commands create an as-path access list named '1' to deny only those routes that include paths from or through autonomous systems 100:

```
ALU(config)# ip as-path access-list 1 deny _100_
```

CONFIGURE ROUTE MAPS

Route-maps are an ordered sequence of individual statements, each having a permit or deny result. Evaluation of route-maps consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and an action associated with the statement match is performed.

Route-maps frequently use Access-lists as matching criteria. Typical route-maps not only permit (some) redistributed routes but also modify information associated with the route. Route-maps are more flexible than ACLs and can verify routes based on criteria. For example, a route-map can verify if the type of route is internal or if it has a IP address.

During redistribution, if the route does not match any clause in a route-map then the route redistribution is denied, as if the route-map contained deny statement at the end.

Route-maps are preferred if you intend to either modify route information during redistribution or if you need more powerful matching capability. Route-map is also used for many different tasks like Border Gateway Protocol (BGP) neighbor update modification.

Command (in CM)	Description
<code>route-map <name> [permit deny] [<1-65535>]</code>	<p>This command is used to configure route maps to control route redistribution. It is also used in BGP to set/match community, as-path list, etc.</p> <p>The range for the rule/sequence number is 1-65535.</p> <p>This sequence number signifies the priority of a route-map rule.</p>

EXAMPLE

```
ALU(config)# route-map rip-to-ospf deny 10
ALU(config-route-map)# match ip address prefix-list test
ALU(config-route-map)# set route-type external type-1

ALU(config)# route-map ospf-to-eigrp permit 20
```

Example of redistribution of RIP into OSPF using route-map:

In the following example, routes from RIP are redistributed to OSPF only if route is not matched with the prefix list 'test'. All the redistributed routes will have metric type set to 'type-1'.

```
ALU(config)# router ospf 1
ALU(config-router ospf 1)# redistribute rip 1 route-map rip-to-ospf
ALU(config-router ospf 1)# default metric 10
```

Each Route-map has number. In this example, route-map rules have sequence numbers 10, 20. Sequence numbers allow you to do these actions:

- Easily delete one specific route-map rule
- Insert a new route map rule between two existing route-map sequences.
- Route-maps can have permit and deny action.
- If route matches match criteria in route-map then route-map action is performed. So if result is permit we allow redistribution of routes.
- If one route-map sequence number is not matched then next sequence number of the route-map is evaluated.

Each route-map has two sets of configuration:

- match: Applies this match criteria for the route.
- set: If match criteria is permit then it modifies the routing information as per set rules

So for each redistribution command, the router first evaluates the match command of a route-map. If the match criteria succeeds, then the route is redistributed or rejected as per route-map action. Then using set commands router change the routing information,

- To redistribute route or to perform set action, all the match criteria should be satisfied.
- If a set command is not present in a route-map, then the route is redistributed without modification of its current attributes.

To CONFIGURE ROUTE-MAP MATCH PARAMETERS

One or more match commands follow a route-map configuration. If there are no match commands, then match result is permit. Configure at least one match command.

Command (in Route-map CM)	Description
match as-path <1-199>	Matches a BGP autonomous system path access list.
match community [<1-99>] [<100-199>] [exact-match]	Matches a BGP community-list.
match ip address {<1-99> <1300-2699> <access-list name>/ prefix-list <prefix-list name>}	Matches a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or perform policy routing on packets.
match ip next-hop {<1-99> <1300-2699> <access-list name>/ prefix-list <prefix-list name>}	Matches a next-hop router address passed by one of the access-lists/prefix-lists.
match ip route-source {<1-99> <1300-2699> <access-list name>/ prefix-list <prefix-list name>}	Matches the address specified by the specified advertised access lists/prefix-lists.
match metric <0-4294967295>	Matches the specified metric.
match interface <interface-name>	Matches the specified next hop route out of one of the interfaces specified.
match route-type { external [{ type-1 type-2 }] internal local nssa-external }	Matches the specified route type.

EXAMPLE

```

ALU(config-route-map)# match as-path 1
ALU(config-route-map)# match community 1
ALU(config-route-map)# match ip address prefix-list testprefix
ALU(config-route-map)# match ip next-hop 1
ALU(config-route-map)# match ip route-source 5
ALU(config-route-map)# match metric 10
ALU(config-route-map)# match interface GigabitEthernet 7/0
ALU(config-route-map)# match route-type external type-2

```

To CONFIGURE ROUTE-MAP SET PARAMETERS

One or more set commands follow a route-map configuration. If there are no set commands other than the match commands, the matching routes are not altered.

Command (in Route-map CM)	Description
set community {<1-4294967295> AA:NN additive local-as no-advertise no-export none}	Sets the community attribute.
set comm-list {<1-99> <100-199>} delete	Removes the communities from the community attribute of an inbound or outbound update.
set dampening <1-45> <1-20000> <1-20000> <1-255>	Sets BGP route dampening factors.
set local-preference <0-4294967295>	Assigns a local preference to the BGP path.
set weight <0-4294967295>	Use this command to set weight of route. BGP has weight attribute. If the same route is received from multiple routers, then weight is used to give preference to some route. Route with highest weight is preferred.
set origin {igp egp <1-65535> incomplete}	Sets the BGP origin code.
set as-path {tag prepend [<1-65535>]}	Modifies the BGP autonomous system path.
set metric <0-4294967295>	Sets the metric value to the redistributed routes. This command is normally used in route-maps for redistribution.
set metric-type {internal external type-1 type-2}	Sets the metric type of the redistributed routes.

EXAMPLE

```
ALU(config-route-map)# set community 10
ALU(config-route-map)#set comm-list 130 delete
ALU(config-route-map)# set dampening 10 2000 2000 15
ALU(config-route-map)# set local-preference 100
ALU(config-route-map)# set weight 10
```



```

ALU(config-route-map)# set origin incomplete

ALU(config-route-map)# set as-path tag

ALU(config-route-map)# set metric 10

ALU(config-route-map)# set metric-type type-1

```

REDISTRIBUTE ROUTING INFORMATION

Redistributing information from one routing protocol to another applies to all of the IP-based routing protocols. You can also conditionally control the redistribution of routes between routing protocols by using Route-maps, and Access-lists.

One routing protocol exports the routes to other routing protocols. OSPF, RIP and BGP can import as well as export routes to other dynamic routing protocols. Connected routes and static routes cannot import routes from other routing protocols. They can only redistribute routes to other dynamic routing protocols.

Although redistribution is a protocol-independent feature, some of the match and set commands are specific to a particular protocol.

Command (in RCM)	Description
<code>redistribute {connected static bgp <1-65535> ospf <1-65535>}[metric <0-16777214> metric-type <1-2> route-map <map-name> tag <0-4294967295> subnets]</code>	This command is used redistribute routes to OSPF.
<code>redistribute {bgp <1-65535> connected ospf <1-65535> [match {{external nssa-external}[1 2] internal}]] static} [metric {<1-16> transparent}] route-map <route-map reference>]</code>	This command is used redistribute routes to RIP.
<code>redistribute {{connected static rip} [metric <0-4294967295> weight <0-65535> route-map <name>] ospf <1-65535> [match [external [type1 type2] internal nssa-external [type1 type2]]] metric <0-4294967295> weight [0-65535] route-map <name>]}</code>	This command is used redistribute routes to BGP.
<code>default-metric <1-4294967295></code>	Causes the current routing protocol to use the same metric value for all redistributed routes (BGP, OSPF, and RIP).

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable tampering with dynamic information, carelessly exchanging routing information between different routing protocols can create routing loops.

EXAMPLE

```
ALU(config-router ospf 1)#redistribute static metric 19 metric-type 1
```

```
ALU(config-router rip)#redistribute bgp 1 route-map test
```

```
ALU(config-router bgp AS1)#redistribute ospf 1 route-map testospf weight 10
```

```
ALU(config-router ospf1)# default-metric 10
```

FILTERING ROUTING INFORMATION

Sometimes it becomes necessary to advertise some route using routing protocol and still not to send any routing traffic out of interfaces. Classical example of this is when we run OSPF over GRE tunnel interface. In this case, site routes are advertised. To prevent routing protocol traffic in the site network, you can use default interface command or else use route redistribution mechanism.

TO PREVENT ROUTING UPDATES THROUGH AN INTERFACE

To prevent other routers on a local network from learning about routes dynamically, you can keep routing update messages from being sent through a router interface. Keeping routing update messages from being sent through a router interface prevents other systems on the interface from learning about routes dynamically. This feature applies to all IP-based routing protocols except BGP.

To prevent routing updates through a specified interface, enter the following command:

Command (in RCM)	Description
passive-interface <interface-name>	Enter this command in Router Configuration Mode. Suppresses sending of routing updates through the specified interface.

EXAMPLE

```
ALU(config-router ospf1)#passive-interface GigabitEthernet 7/0
```

To CONFIGURE DEFAULT PASSIVE INTERFACES

If you have many interfaces on a router, then there are two possibilities for obtaining routing information from these interfaces:

- Configure a routing protocol such as OSPF on the interfaces and redistribute connected interfaces. But, this may cause lots of Type-5 LSAs in the network.
- Configure the routing protocol on all interfaces and manually set them as passive. But, this may cause routing protocol traffic on these interfaces.

The solution to the above problem is to configure the routing protocol on all interfaces and manually set the passive-interface router configuration on the interfaces where adjacency is not desired.

With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single passive-interface default command. Then configure individual interfaces where adjacencies are desired using the 'no passive-interface' command.

Command (in RCM)	Description
<code>passive-interface default</code>	Sets all interfaces as passive by default.
<code>no passive-interface <interface-name></code>	Activates only those interfaces that need to have adjacencies set.

EXAMPLE

```
ALU(config-router ospf1)# passive-interface default
```

```
ALU(config-router ospf1)# no passive-interface GigabitEthernet
7/0
```

To verify the passive interfaces, use '**show ip ospf interface**' command.

To CONTROL ADVERTISING OF ROUTES IN ROUTING UPDATES

To prevent other routers from learning one or more routes, you can suppress routes from being advertised in routing updates. Suppressing routes in route updates prevents other routers from learning the interpretation of a particular device of one or more routes.

To suppress routes from being advertised in routing updates, enter the following command:

Command (in RCM)	Description
<code>distribute-list {<1-199> <1300-2699> <access-list-name>} prefix <prefix-list> {in out} {interface-name}</code>	Permits or denies routes from being advertised in routing updates depending upon the action listed in the access list.
<code>distribute-list {<1-199> <1300-2699>} gateway <ip-prefix-list name> /prefix <ip-prefix-list name> {in out} [[GigabitEthernet Serial] <slot/port> Loopback <0-14487>]</code>	This command suppresses networks from being advertised in routing updates. The distribute-list in command is used to filter networks in received routing updates.



Note: The OA-700 does not support Distribute-list feature in OSPF.

EXAMPLE

```
ALU(config-router bgp AS1)#distribute-list 1 in GigabitEthernet 7/0
```

```
ALU(config-router rip)# distribute-list prefix prefix-example in GigabitEthernet 7/0
```

CONFIGURE ADMINISTRATIVE DISTANCE

To give a preference to a specific routing protocol routes, you can use the administrative distance. Each routing protocol has a default administrative distance as listed in the table below.

Default Administrative Distance

Route Source	Default Distance
Connected interface	0
Static route	1
Exterior BGP	20
OSPF	110
RIP	120
Interior BGP	200
Unknown	255

Filtering sources of routing information prioritizes routing information from different sources, because some pieces of routing information may be more accurate than others. An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers.

In a network, some routing protocols and some routers can be more reliable than others as sources of routing information. Also, when multiple routing protocols are running on the same interface, it is possible for the same route to be advertised by more than one of them. By specifying administrative distance values, you enable the router to intelligently discriminate between sources of routing information.

The router will always pick the route whose routing protocol has the lowest administrative distance.

To CONFIGURE ADMINISTRATIVE DISTANCE

Command (in RCM)	Description
<code>distance <1-255> [[ip-address subnet-mask/ip-address/prefix-length][<1-99> <1300-1999>]]</code>	This command is used to define an administrative distance for OSPF or RIP or BGP. The default distance for RIP is 120. The default distance for OSPF is 110. The default distance is 20 for EBGp and 200 for IBGP.
<code>distance ospf {external inter-area intra-area} <1-255>}}</code>	This command performs the same function as the distance command used with an access list. However, the distance OSPF command allows you to set a distance for an entire group of routes, rather than a specific route that matches an access-list.
<code>distance bgp <1-255> <1-255> <1-255></code>	This command is used to configure distance for external, internal, and local routes.

EXAMPLE

```
ALU(config-router rip)# distance 130 10.0.0.0/8 20

ALU(config-router bgp AS1)#distance 10 100.0.0.0/8 1

ALU(config-router ospf 1)# distance 60 10.0.0.0/8

ALU(config-router ospf 1)# distance ospf external 10

ALU(config-router bgp AS1)#distance bgp 30 10 5
```



Note: You can also use administrative distance to rate the routing information from routers running the same routing protocol. This application is generally discouraged if you are unfamiliar with this particular use of administrative distance as it can result in inconsistent routing information, including forwarding loops.

CONFIGURE MAXIMUM PATHS

By default, OSPF, BGP, and Static routes can install a maximum number of 16 ECMP paths. And, RIP installs maximum 8 ECMP paths.

Static route maximum path limit is not configurable.

Command (in RCM)	Description
<code>maximum-paths <number of paths></code>	Enter this command in the Router Configuration Mode. This command is used to configure the maximum number of ECMP paths to be allowed in a routing table.

EXAMPLE

```
ALU(config-router ospf 1)# maximum-paths 5
```

PROTOCOL INDEPENDENT FEATURES SHOW COMMANDS

You can display specific statistics such as the contents of IP routing table. Information provided can be used for debugging.

TO VIEW CONFIGURED ROUTING PROTOCOLS

Show Command (in SUM)	Description
<code>show ip protocols [summary]</code>	Displays the parameters and current state of the active routing protocol process.

EXAMPLE

ALU# show ip protocols

```
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 27 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240 seconds
  Default redistribution metric is 3
    Redistributing External Routes from:
      connected metric 3
      static metric 4
  Default version control: send version 2, receive version 2
  Automatic network summarization is in effect
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Interface          Send    Recv    Key-chain
  GigabitEthernet7/1  2       2
  loopback1          2       2
Routing for Networks:
  1.0.0.0
  4.0.0.0
Routing Information Sources:
  Gateway            Interface          Distance  Last Update
  1.1.1.1             GigabitEthernet7/1  115       00:00:00
Distance: (default is 120)
```

ALU# show ip protocols summary

```
Index Process Name
0      ospf 1
1      ospf 2
2      rip
3      bgp 200
4      static
5      connected
6      connected-ppp
ALU#
```


To VIEW ACCESS-LIST CONFIGURATION

Show Command (in SUM)	Description
show access-lists [<i><1-2699></i> <i><access-list name></i>]	This command displays the access-list configuration.

EXAMPLE

ALU# show access-lists

```
Standard IP access list 1
  deny 1.0.0.0 0.255.255.255 (0 packets)
Standard IP access list 2
  permit 20.0.0.0 0.255.255.255 (0 packets)
Extended IP access list 101
  permit ip 162.168.0.0 0.0.0.0 255.255.252.0 0.0.0.0 (0 packets)
ALU#
```

To VIEW IP ACCESS-LIST CONFIGURATION

Show Command (in SUM)	Description
show ip access-lists [<i><1-199></i> <i><1300-2699></i> <i><access-list name></i>]	This command displays the IP access-list configuration.

EXAMPLE

ALU# show ip access-lists

```
Standard IP access list test
  permit host 10.0.0.1 (0 packets)
  permit 11.0.0.0 0.255.255.255 (0 packets)
  deny 12.0.0.0 0.255.255.255 (0 packets)
ALU#
```

To VIEW IP PREFIX-LIST CONFIGURATION

Show Command (in SUM)	Description
show ip prefix-list [<i><prefix-list name></i>]	This command displays the IP Prefix-list configuration.

EXAMPLE

ALU# show ip prefix-list
ip prefix-list test
seq 5 deny 10.0.0.0/8 ge 23
ALU#

To VIEW IP AS-PATH ACCESS-LIST CONFIGURATION

Show Command (in SUM)	Description
show ip as-path-access-list [<i><1-199></i>]	This command displays the AS-path - access-list configuration.

EXAMPLE

```
ALU# show ip as-path-access-list
```

```
AS path access list 1
    deny_100_
ALU#
```

To VIEW ROUTE-MAP CONFIGURATION

Show Command (in SUM)	Description
show route-map [<i><route-map name></i>]	This command displays the route-map configuration.

EXAMPLE

```
ALU# show route-map
```

```
route-map test, permit, sequence 1
  Description:
  Exit Policy:
  Match clauses:
    community (community-list filter): 1
    ip address (access-lists): prefix-list testprefix
  Set clauses:
route-map test, deny, sequence 2
  Description:
  Exit Policy:
  Match clauses:
  Set clauses:
ALU#
```

ALU# show route-map testset

```

route-map testset, permit, sequence 5
  Description:
  Exit Policy:
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
    metric 10
route-map testset, permit, sequence 10
  Description:
  Exit Policy:
  Match clauses:
  Set clauses:
    metric 20
ALU#

```

To VIEW IP COMMUNITY-LIST CONFIGURATION

Show Command (in SUM)	Description
show ip community-list [<1-199>]	This command displays the IP Community-list configuration.

EXAMPLE**ALU# show ip community-list**

```

Community standard access list 1
  permit internet
Community standard access list 2
  permit no-export
ALU#

```

To VIEW ROUTING TABLE

Show Command (in SUM)	Description
show ip route [{ <i>network-number/ip-address/prefix length</i> } [longer-prefixes] ospf [<1-65535>] connected bgp rip summary supernets-only]	Displays the current state of a routing protocol. You can filter show IP route output to view specific protocol routes.

EXAMPLE 1

ALU# show ip route

```
Codes: R - RIP, O - OSPF, C - connected
       S - static, M - mcstatic, B - BGP
       IA - OSPF inter area route, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
       * - candidate default route
```

Gateway of last resort is not set

```

5.0.0.0/24 is subnetted, 3 subnets
C    5.5.0.0 [0/0] is directly connected, Serial0/0:0
C    5.5.1.0 [0/0] is directly connected, Serial0/0:1
C    5.5.2.0 [0/0] is directly connected, Serial0/0:2
6.0.0.0 is variably subnetted, 2 subnets, 2 masks
S    6.6.6.0/24 [1/0] is directly connected, Serial0/0:2
O    6.6.6.6/32 [110/10][1] via 5.5.0.1, Serial0/0:0
                        via 5.5.1.1, Serial0/0:1
                        via 5.5.2.1, Serial0/0:2
S    7.0.0.0/8 [1/0] is directly connected, Serial0/0:0
                        is directly connected, Serial0/0:1
10.0.0.0/24 is subnetted, 1 subnet
C    10.91.2.0 [0/0] is directly connected, GigabitEthernet7/0
99.0.0.0/24 is subnetted, 1 subnet
C    99.99.99.0 [0/0] is directly connected, loopback1
S    100.0.0.0/8 [1/0] via 10.91.2.5, GigabitEthernet7/0
ALU#
```

EXAMPLE 2**ALU# show ip route static**

```
Codes: R - RIP, O - OSPF, C - connected
       S - static, M - mcstatic, B - BGP
       IA - OSPF inter area route, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
       * - candidate default route

6.0.0.0/24 is subnetted, 1 subnet
S      6.6.6.0 [1/0] is directly connected, Serial0/0:2
S      7.0.0.0/8 [1/0] is directly connected, Serial0/0:0
           is directly connected, Serial0/0:1
S     100.0.0.0/8 [1/0] via 10.91.2.5, GigabitEthernet7/0
ALU#
```

EXAMPLE 3**ALU# show ip route connected**

```
Codes: R - RIP, O - OSPF, C - connected
       S - static, M - mcstatic, B - BGP
       IA - OSPF inter area route, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
       * - candidate default route

5.0.0.0/24 is subnetted, 3 subnets
C      5.5.0.0 [0/0] is directly connected, Serial0/0:0
C      5.5.1.0 [0/0] is directly connected, Serial0/0:1
C      5.5.2.0 [0/0] is directly connected, Serial0/0:2
10.0.0.0/24 is subnetted, 1 subnet
C     10.91.2.0 [0/0] is directly connected, GigabitEthernet7/0
99.0.0.0/24 is subnetted, 1 subnet
C     99.99.99.0 [0/0] is directly connected, loopback1
ALU#
```

EXAMPLE 4

ALU# show ip route summary

Route Source	Networks	Subnets	Overhead	Memory (bytes)
connected	0	1	42	36
static	1	0	42	36
ospf 1	227	2	9618	8244
Total	228	3	9702	8316

Mask distribution:

- 3 routes at length 8
- 1 route at length 16
- 226 routes at length 24
- 1 route at length 32

ALU#

EXAMPLE 5

ALU# show ip route supernets-only

```
S 172.0.0.0/8 [1/0] via 1.1.1.5, GigabitEthernet7/1
O E2 193.0.0.0/8 [110/20][1] via 1.1.1.2, GigabitEthernet7/1
ALU#
```

PROTOCOL INDEPENDENT FEATURES CLEAR COMMAND

Command (in SUM)	Description
<code>clear ip route *</code>	Clears all routes from the IP routing table.

EXAMPLE

ALU# clear ip route *

CHAPTER 20 ROUTING INFORMATION PROTOCOL

This chapter covers the Routing Information Protocol (RIP) configuration used in the OA-700. It provides a broad overview on RIP V1 and V2 configuration including the timer, authentication, default route, and monitoring commands.

The “[RIP Overview](#)” section serves only as an additional information on RIP. You can skip this section, and directly go to the configuration section of this chapter detailed in “[RIP Configuration](#)”.

For a detailed information on the RIP commands, refer to the RIP chapter in the *OmniAccess 700 CLI Command Reference Guide*.

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
RCM	Router Configuration Mode - ALU (config-router rip)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
RIP	Routing Information Protocol

RIP OVERVIEW

RIP is a Distance Vector or Bellman-Ford routing protocol. It is one of the oldest and widely used interior gateway protocols. Version 1 of RIP is documented in RFC 1058. RIP version 1 has certain well-known limitations, such as classful routing. RIP version 2 attempted to fix some of the problems with RIP version 1. In particular, RIP version 2 supports CIDR and has also added support for authentication.

RIP uses User Datagram Protocol (UDP) data packets to exchange routing information. The routing information updates are sent at regular time intervals (by default, 30 seconds in Alcatel-Lucent's implementation). If the router does not receive any updates from a neighboring router for a time interval known as the invalid timer, it marks all routes from the neighboring router as invalid. And if there is still no sign of life from the neighboring router after the router's flush timer has expired, all the routes are removed.

RIP uses hop count as metric and the max metric is 15. A metric of 16 means the network is unreachable, a metric of 0 means the network is directly connected.

A default route can be received from another RIP router or it can source the default route itself. In both the cases, the default route is advertised to other RIP routers via RIP. A default route can be sourced either with the default-information originate command or from another routing protocol via redistribution.

RIP CONFIGURATION

Refer to the following sections to configure RIP on your system:

- [“RIP Configuration Steps”](#)
- [“RIP Configuration Flow”](#)
- [“RIP Configuration Commands”](#)
- [“RIP Show Commands”](#)

RIP CONFIGURATION STEPS

This section lists step by step instructions to be followed while configuring RIP (v1 and v2.) on your system.

Step 1 to Step 5 are the minimum configuration requirements for enabling RIP. Step 6 describe other important but optional configuration commands for RIP.

Step 1: Configure an interface. Enter the Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```



Note: RIP can be configured on Gigabit Ethernet, Serial, Tunnel, VLAN, Loopback, ISDN, DSL interfaces.

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Enable RIP. See [“To Enable RIP”](#)

Step 5: Configure the major networks to run RIP. See [“To Configure a RIP Network”](#)

Step 6: Configure RIP optional parameters. See [“RIP Optional Parameters”](#)

- Specify a RIP Version. See [“To Specify a RIP Version”](#)
- Configure RIP Behavior on an Interface. See [“To Configure RIP Behavior on an Interface”](#)

- Enable or Disable Split Horizon. See [“To Enable/Disable Split Horizon”](#)
- Enable or Disable Broadcast Updates. See [“To Enable/Disable Broadcast Updates”](#)
- Configure Passive Interfaces. See [“To Configure Passive Interfaces”](#)
- Configure RIP Neighbor. See [“To Configure RIP Neighbor”](#)
- Configure Administrative Distance. See [“To Configure Administrative Distance”](#)
- Configure Default Metric Value. See [“To Configure Default Metric Value”](#)
- Configure RIP Timers. See [“To Configure RIP Timers”](#)
- Apply Offsets to Routing Metrics. See [“To Apply Offsets to Routing Metrics”](#)
- RIP Authentication. See [“RIP Authentication”](#)
- RIP and Default Route. See [“RIP and Default Route”](#)
- Configure Auto Summary. See [“To Configure Auto Summary”](#)
- RIP Redistribution. See [“RIP Redistribution”](#)

RIP CONFIGURATION FLOW

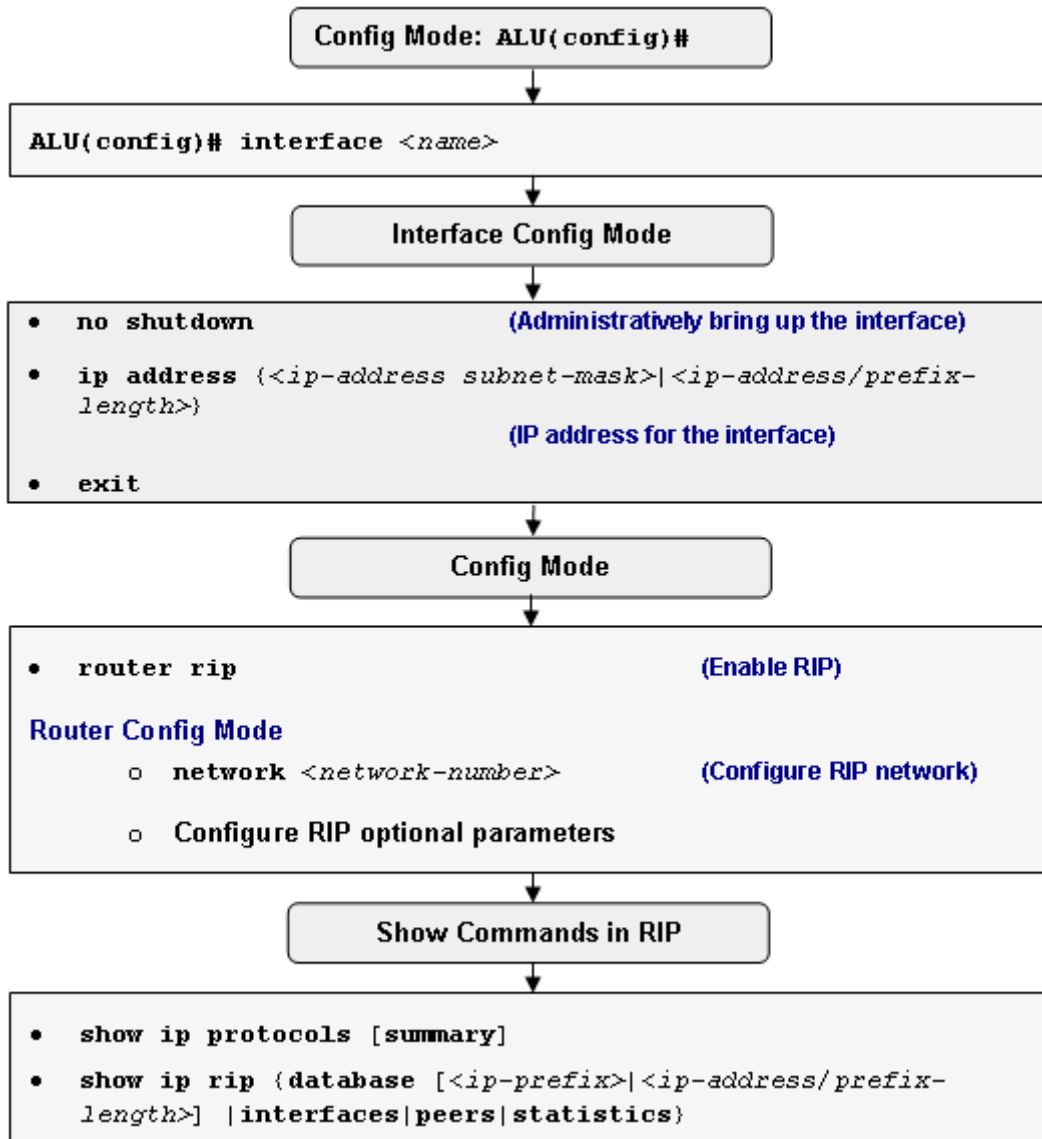


Figure 39: RIP Configuration Flow

RIP CONFIGURATION COMMANDS

To ENABLE RIP

Command (in CM)	Description
<code>router rip</code>	This command enters into the Router Configuration mode. This enables to configure RIP specific commands.

EXAMPLE

```
ALU(config)# router rip
ALU(config-router rip)#
```

To CONFIGURE A RIP NETWORK

RIP sends updates to the interfaces in the specified networks. If an interface's network is not specified, it will not be advertised in any RIP update. There is no limit to the number of network commands you can use on the router. RIP routing updates will be sent and received only through interfaces which falls in the configured network.

Command (in RCM)	Description
<code>network <network-number></code>	Associates a specific network with a RIP routing process.
<code>no network <network-number></code>	The 'no' command disables the configured network. RIP stops sending updates through interfaces on this network. Also these interfaces will not be advertised in any RIP updates.

EXAMPLE


```
ALU(config-router rip)# network 10.0.0.0

ALU(config-router rip)# no network 10.0.0.0
```

RIP OPTIONAL PARAMETERS

The following commands are the important but optional configuration commands for RIP v1 and v2.

TO SPECIFY A RIP VERSION

Command (in RCM)	Description
<code>version {1 2}</code>	<p>This command is used to configure RIP version - v1/v2 on the OA-700.</p> <p>Configure RIP version to v1 to send and receive only RIPv1 messages, and configure RIP version to v2 to send and receive only RIPv2 messages.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>Note: RIPv2 is an enhancement of RIPv1 and not a separate protocol.</p> <p>By default, RIP process configured on OA-700 system sends only RIPv1 messages but receives both RIPv1 and RIPv2 messages.</p> </div> </div>
<code>no version</code>	This command resets the configured routing protocol version.

EXAMPLE

```
ALU(config-router rip)# version 1
```

```
ALU(config-router rip)# no version
```

To CONFIGURE RIP BEHAVIOR ON AN INTERFACE

The interface-level compatibility switches recommended by RFC 1723 are implemented with the following commands "**ip rip send version**" and "**ip rip receive version**".

Command (in ICM)	Description
ip rip {send receive} version [1] [2]	Use this command in the Interface Configuration mode. This command is used to control the RIP behavior as to what version of RIP packets should be sent or received on an interface. You can override the RIP behavior configured on a per interface basis.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip rip send version 1 2
```

To ENABLE/DISABLE SPLIT HORIZON

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken.

RIP uses Split Horizon and Poison Reverse to ensure that routes learned on a particular interface are not re-advertised out of that same interface, or if they are, that they are advertised as unreachable.

Command (in ICM)	Description
ip split-horizon [poison-reverse]	This command enables the split horizon mechanism.
no ip split-horizon [poison-reverse]	This command disables the split horizon mechanism.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip split-horizon
```

```
ALU(config-if GigabitEthernet7/0)# no ip split-horizon
```

To ENABLE/DISABLE BROADCAST UPDATES

In RIP Version 2, routing updates are sent to multicast address. You can change this behavior by enabling the following command.

Command (in ICM)	Description
<code>ip rip v2-broadcast</code>	Use this command to send routing updates to broadcast address. This command is used to allow RIP Version 2 update packets to be sent as broadcast packets instead of multicast packets.
<code>no ip rip v2-broadcast</code>	The 'no' command disables sending of routing updates to broadcast address.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip rip v2-broadcast
```

```
ALU(config-if GigabitEthernet7/0)# no ip rip v2-broadcast
```

To CONFIGURE PASSIVE INTERFACES

The "**passive interface**" command can be issued under RIP to make the OA-700 system a silent host on the specified data link. Like other hosts, it listens to the RIP broadcasts on the link and updates the routing table accordingly.

Command (in RCM)	Description
<code>passive-interface</code> { {GigabitEthernet Serial} <slot/port> Loopback <0-14487> default }	This command is used to control the set of interfaces with which you want to exchange routing updates.
<code>no passive-interface</code> { {GigabitEthernet Serial} <slot/port> Loopback <0-14487> default }	The 'no' command disables the configured passive interfaces.

EXAMPLE

```
ALU(config-router rip)# passive interface GigabitEthernet 7/0
```

```
ALU(config-router rip)#no passive interface GigabitEthernet 7/0
```


To CONFIGURE RIP NEIGHBOR

Command (in RCM)	Description
neighbor <neighbor-address>	Defines a neighboring router to exchange the routing information.
no neighbor <neighbor-address>	The 'no' command disables a configured neighbor router.

EXAMPLE

```
ALU(config-router rip)# neighbor 172.19.3.1
```

```
ALU(config-router rip)# no neighbor 172.19.3.1
```



Note: The addition of a **"neighbor"** command under the RIP processes enable RIP to send a unicast advertisement on interface while the **"passive-interface"** command continues to prevent broadcast updates on the link.

This is explained below:

```
!
interface GigabitEthernet 3/1
ip address 172.19.3.1/24
!
!
router rip
network 172.19.0.0
neighbor 172.19.3.1
passive-interface GigabitEthernet 3/1
!
```

To CONFIGURE ADMINISTRATIVE DISTANCE

Command (in RCM)	Description
distance <1-255> [[ip-address subnet-mask/ip-address/prefix-length][<1-99> <1300-1999>]]	This command is used to define an administrative distance. The default distance is 120.
no distance <1-255>	The 'no' command sets administrative distance to default.

'Show ip protocols' command shows the default distance for all routing protocols.

EXAMPLE

```
ALU(config-router rip)# distance 130 10.0.0.0/8 20
```

```
ALU(config-router rip)# no distance
```

To CONFIGURE DEFAULT METRIC VALUE

A default metric helps to solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, a default metric provides a reasonable substitute and enables the redistribution to proceed.

Command (in RCM)	Description
<code>default-metric <1-16></code>	This command sets the default metric values of redistributed routes.
<code>no default-metric <1-16></code>	The 'no' command sets the metric of redistributed routes to its default. The metric of redistributed connected and static routes is set to 0, otherwise default metric is set to 1.

EXAMPLE

```
ALU(config-router rip)# default metric 10
```

```
ALU(config-router rip)# no default metric 10
```



Note: Use **default-metric** command in conjunction with the **redistribute** (see [“To Configure Redistribution”](#)) configuration command to make the current routing protocol to use the same metric value for all the redistributed routes.

This is explained below:

```
!
router rip
network 172.19.0.0
default-metric 10
redistribute static
redistribute ospf 1 metric 5
```

As per the example, all the routes imported from the Static routing protocol will be assigned metric of 10.

In case of routes imported from OSPF routing protocol, a metric of 5 is assigned to all the routes.

To CONFIGURE RIP TIMERS

Routing protocols use several timers that determine the variables such as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs.

You can make the following timer adjustments in the same order as given below:

- Update: The time between routing updates (in seconds). Default is 30 seconds.
- Invalid: The interval after which a route is declared invalid (in seconds) Default is 180 seconds.
- Holddown: The interval during which routing information regarding different alternate paths is suppressed (in seconds). Default is 180 seconds
- Flush: Amount of time that must pass before a route is removed from the routing table (in seconds). Default is 240 seconds
- Sleeptime: Interval for postponing routing updates in the event of a flash update (in milliseconds)

Command (in RCM)	Description
<code>timers basic <0-4294967295> <1-4294967295> <0-4294967295> <1-4294967295> [<1-4294967295>]</code>	This command is used to adjust routing protocol timers to tune the routing protocol performance to better suit your internetwork needs. You can make the timer adjustments in the following order: Update, invalid, holddown, flush, sleeptime. All these are mandatory, except sleeptime.
<code>no timers basic</code>	This command disables the routing timers.

EXAMPLE

```
ALU(config-router rip)# timers basic 10 30 30 90
```

```
ALU(config-router rip)# no timers basic
```



Note: The Invalid and Holddown timer interval should be at least three times the value of Update timer. For Flush timer, the interval should be longer than the larger of the Invalid and Holddown values. If Flush interval is less than the sum of the Update and Holddown values, the proper Holddown interval cannot elapse, which results in a new route being accepted before the Holddown interval expires. Choose these values properly to improve network convergence time and to control routing traffic.

To APPLY OFFSETS TO ROUTING METRICS

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. Optionally, you can limit the offset list with either an access list or an interface. An offset-list increases the value of routing metrics.

Command (in RCM)	Description
<pre>offset-list {{<0-99> <1300-1999> <access-list name>} {in out}} {<0-16>} [{GigabitEthernet Serial} <slot/port> Loopback <0-14487>]</pre>	Applies an offset to the routing metrics.
<pre>no offset-list {{<0-99> <1300-1999> <access-list name>} {in out}} {<0-16>} [{GigabitEthernet Serial} <slot/port> Loopback <0-14487>]</pre>	The 'no' command disables the configured offset-list.

The **offset-list** command specifies a number to add to the metric of a route entry and references an access-list to determine which route entries to modify. This is explained in the example given below:

EXAMPLE

```
ALU(config)#access-list 1 permit 10.33.0.0 0.0.0.0

ALU(config)#router rip
ALU(config-router)#network 192.168.1.0
ALU(config-router)#network 10.0.0.0
ALU(config-router)#offset-list 1 in 2 Serial0/0:1
```

The syntax of the offset-list says, "Examine RIP advertisements incoming from interface Serial0/0:1. For route entries matching the addresses specified in access-list 1, add 2 hops to the metric."

If no interface is identified, the list will modify either all incoming updates or all outgoing updates specified by the access-list on any interface.

RIP AUTHENTICATION



Note: **RIP Version 1 does not support authentication.**

If you are sending and receiving RIP Version 2 packets, RIP authentication on an interface can be enabled. The key chain determines the set of keys that can be used on an interface. If a key chain is not configured, no authentication is performed on that interface, not even the default authentication.

We support two modes of authentication on an interface for which RIP authentication is enabled: **Plain Text Authentication** and **MD5 Authentication**. The default authentication in every RIP Version 2 packet is Plain Text Authentication.

The OA-700 implementation of RIPv2 message authentication includes the choice of simple password or MD5 authentication and the option of defining multiple keys, or passwords, on a "Key chain".

TO CONFIGURE KEY CHAIN

Command (in CM)	Description
key-chain <i><key-chain name></i>	This command is used to configure a key chain.

EXAMPLE

```
ALU(config)# key-chain allen
ALU(config-keychain allen)#
```

TO CONFIGURE A KEY

Command (in Key-chain Mode)	Description
key <i><0-2147483647></i>	This command is used to configure a key that can be used on an interface in the range 0-2147483647.

EXAMPLE

```
ALU(config-keychain allen)# key 100
ALU(config-keychain-key 100)#
```

To CONFIGURE A KEY PASSWORD

Command (in Key-chain Key Mode)	Description
key-string <i><key string></i>	This command is used to configure the password for the key.

EXAMPLE

```
ALU(config-keychain-key 100)# key-string sg123
```

To ENABLE RIP AUTHENTICATION ON AN INTERFACE

To enable RIP authentication, authentication key chain and authentication mode should be configured on the interface.

Command (in ICM)	Description
ip rip authentication key-chain <i><key-chain name></i>	Use the following command in the Interface Configuration mode. This command is used to associate a key chain to an interface. This enables RIP authentication.
no ip rip authentication key-chain <i><key-chain name></i>	The 'no' command removes the key chain associated to an interface. This disables RIP authentication.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip rip authentication key-chain allen
```

```
ALU(config-if GigabitEthernet7/0)# no ip rip authentication key-chain allen
```

TO CONFIGURE RIP AUTHENTICATION MODE

Command (in ICM)	Description
<code>ip rip authentication mode {md5 text}</code>	Use the following command in the Interface Configuration mode. This command is used to configure the authentication mode to be used by the interface (or let it default mode). The default authentication mode is Plain Text authentication.
<code>no ip rip authentication mode</code>	The 'no' command sets the authentication mode to its default, i.e, plain Text authentication.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip rip authentication mode md5
```

```
ALU(config-if GigabitEthernet7/0)# no ip rip authentication mode
```

TO DISABLE THE VALIDATION OF SOURCE IP ADDRESS

By default, the router verifies whether the incoming RIP updates originate from an address on the same IP subnet as the interface it is received on. To disable this behavior, use the following command in the Router Configuration mode.

Command (RCM mode)	Description
<code>no validate-update-source</code>	Disables the validation of the source IP address of the incoming RIP routing updates. By default, RIP validates the source IP address of incoming RIP routing updates.
<code>validate-update-source</code>	This command validates the source IP address of incoming RIP routing updates.

EXAMPLE

```
ALU(config-router rip)# no validate-update-source
```

```
ALU(config-router rip)# validate-update-source
```

RIP AND DEFAULT ROUTE



Note: **RIP Version 1 does not support Default Route.**

A default route can be received from another RIP router or it can source the default route by itself. In both cases, the default route is advertised to other RIP routers. A default route can be sourced either with the `default-information originate` command or from another routing protocol via redistribution.

To CONFIGURE DEFAULT INFORMATION ORIGINATE

Command (RCM mode)	Description
<code>default-information originate</code>	This command is used to generate default route into RIP.
<code>no default-information originate</code>	The ' no ' command disables default-information originate feature.

EXAMPLE

```
ALU(config-router rip)# default-information originate
```

```
ALU(config-router rip)# no default-information originate
```

To CONFIGURE AUTO SUMMARY

Command (RCM)	Description
<code>auto-summary</code>	This command restores the default behavior of automatic summarization of the subnet routes into network-level routes. By default, this feature is enabled.
<code>no auto-summary</code>	The ' no ' command disables auto-summary, and sends sub-prefix routing information across classful network boundaries.

EXAMPLE

```
ALU(config-router rip)# auto-summary
```

```
ALU(config-router rip)# no auto-summary
```


RIP REDISTRIBUTION

Redistribution is used to import routes from other routing protocols. This feature gives option to selectively import the route and also set metrics using route maps.

To CONFIGURE DISTRIBUTE LIST

Command (RCM)	Description
distribute-list {<1-199>/<1300-2699> gateway <ip-prefix-list name> prefix <ip-prefix-list name>} { in out } [{ GigabitEthernet Serial } <slot/port> Loopback <0-14487>]	This command suppresses networks from being advertised in routing updates. The distribute-list in command is used to filter networks in received routing updates.
no distribute-list {<1-199> <1300-2699> gateway prefix }	This command disables the functionality to filter networks in routing updates.

Specify either an access list or a prefix list with the distribute-list command. Use the gateway keyword only with the prefix-list keyword.

EXAMPLE

```
ALU(config-router rip)# distribute-list prefix prefix-example
in GigabitEthernet 7/0
```

```
ALU(config-router rip)# no distribute-list prefix prefix-
example in GigabitEthernet 7/0
```

To CONFIGURE REDISTRIBUTION

Command (RCM)	Description
redistribute { bgp <1-65535> connected ospf <1-65535> match {{ external nssa-external }[1 2] internal }} static } [metric {<1-16> transparent } route-map <route-map reference>]	This command is used to import routes from other routing protocols.
no redistribute { bgp <1-65535> connected ospf <1-65535> match {{ external nssa-external }[1 2] internal }} static } [metric {<1-16> transparent } route-map <route-map reference>]	This command disables the redistribution of routes.

EXAMPLE

```
ALU(config-router rip)# redistribute bgp 1 metric 10
```

RIP SHOW COMMANDS

The following **show** commands are described in the example given below:

To VERIFY IP ROUTE SUMMARIZATION

Command (in SUM)	Description
<code>show ip protocols [summary]</code>	Displays a detailed routing configuration. Summary keyword can be used to have a summary of the routing configuration.

EXAMPLE

The **show ip protocols** command in **SUM** can be used to verify summarization configuration as shown in the example below:

```
ALU# show ip protocols
```

```
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 27 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240 seconds
  Default redistribution metric is 3
    Redistributing External Routes from:
      connected metric 3
      static metric 4
  Default version control: send version 2, receive version 2
  Automatic network summarization is in effect
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Interface          Send    Recv    Key-chain
  GigabitEthernet7/1  2       2
  loopback1          2       2
Routing for Networks:
  1.0.0.0
  4.0.0.0
Routing Information Sources:
  Gateway            Interface          Distance  Last Update
  1.1.1.1             GigabitEthernet7/1  115       00:00:00
  Distance: (default is 120)
```

To VIEW IP RIP DATABASE

Command (in SUM)	Description
<code>show ip rip database [<ip-prefix>/<ip-address/prefix-length>]</code>	Displays all route entries in the RIP routing database.

EXAMPLE

ALU#`show ip rip database`

```

                                RIP Route Table
                                -----
1.0.0.0/8      : auto-summary
1.1.1.0/24    : directly connected, GigabitEthernet7/0
10.0.0.0/8    : auto-summary
10.91.2.0/24  : directly connected, GigabitEthernet7/1
12.0.0.0/8    : learnt via RIP, metric = 1 tag = 0 via 10.91.2.5,
                00:00:00 ago, on GigabitEthernet7/1
ALU#

```

To VIEW IP RIP INTERFACES

Enter this command in the Configuration Mode as follows:

Command (in SUM)	Description
<code>show ip rip interfaces</code>	Displays summary address entries in the RIP database.

EXAMPLE

ALU# `show ip rip interfaces`

```

                                RIP Interface Table
                                -----
Interface      Interface Address      Interface Mask      Send Ver  Recv Ver  Flags
GigabitEthernet7/0  1.1.1.2          255.255.255.0      2         2         B S
GigabitEthernet7/1  10.91.2.6        255.255.255.0      2         2
(Flags - U: Unnumbered P:Passive B:V2 Broadcast S:Split horizon disabled)
ALU#

```

To VIEW IP RIP PEERS

Command (in SUM)	Description
<code>show ip rip peers</code>	Displays the RIP peer table details.

EXAMPLE

ALU#`show ip rip peers`

```

RIP Peer Table
-----
Peer Address  Interface          LastUpd(sec) Rcv Ver Bad Pkts BadRoutes
1.1.1.1       GigabitEthernet7/0 865          2      0      0
10.91.2.5     GigabitEthernet7/1 25           2      0      0
ALU#
    
```

To VIEW IP RIP STATISTICS

Command (in SUM)	Description
<code>show ip rip statistics</code>	Displays the RIP statistics including both the global and interface statistics.

EXAMPLE

ALU# `show ip rip statistics`

```

RIP Global Statistics
-----
Route Changes Route Queries Rx Bad Msgs Routes Learnt Routes Held down
1              0              19          1              0
ALU#
    
```

```

RIP Interface Statistics
-----
Interface
GigabitEthernet7/0 Routes learned 0 Updates sent 0 11
                   Bad msgs received 14 Trig Updates sent 0 2
                   Auth failures 0 Responses sent 0 0
                   *Unicast tx failure 0 Routes advertised 0 3
                   Bcast tx failures 0 Updates received 0 40
                   Mcast tx failures 0 Requests received 0 0
                   Bad Rtes received 0 0
GigabitEthernet7/1 Routes learned 1 Updates sent 0 8
                   Bad msgs received 5 Trig Updates sent 0 0
                   Auth failures 0 Responses sent 0 0
                   *Unicast tx failure 0 Routes advertised 0 1
                   Bcast tx failures 0 Updates received 0 3
                   Mcast tx failures 0 Requests received 0 0
                   Bad Rtes received 0 0
ALU#
    
```

To VIEW KEY-CHAIN

Command (in SUM)	Description
show key-chain	Displays the configured key chain on the interface.

EXAMPLE

```

ALU> show key-chain
key-chain alu1
  key 1
    key-string alcatel-lucent
    Accept lifetime (00:00:00 01 Jan 2000) - (Infinite) [Valid
Now]
    Send lifetime (00:00:00 02 Feb 2001) - (Infinite) [Valid
Now]
key-chain alu2  key 2
  key-string lucent
    Accept lifetime (Always Valid) - (Always Valid) [Valid Now]
    Send lifetime (Always Valid) - (Always Valid) [Valid Now]

ALU> show key-chain alu1
key-chain alu1
  key 1
    key-string alcatel-lucent
    Accept lifetime (00:00:00 01 Jan 2000) - (Infinite) [Valid
Now]
    Send lifetime (00:00:00 02 Feb 2001) - (Infinite) [Valid Now]

```

RIP CLEAR COMMANDS

The section below details the procedure to clear RIP configuration on your system.

TO RESTART THE RIP PROCESS

Command (in SUM)	Description
<code>clear ip rip {database statistics}</code>	Clears the RIP database or the RIP statistics.

EXAMPLE

```
ALU# clear ip rip database
```

CHAPTER 21 BORDER GATEWAY PROTOCOL

This chapter covers the Border Gateway Protocol (BGP) configurations used in the OA-700. It provides a broad overview on BGP-4 configuration including the neighbors, networks, advertising networks, reset, and monitoring commands.

The “**BGP Overview**” section serves as an additional information on BGP. You can skip this section, and directly forward to the configuration section of this chapter, detailed in “**BGP Configuration**”.

For instructions on using the BGP commands and descriptions on each of their parameters with the corresponding default values for each, refer to the *OmniAccess 700 CLI Command Reference Guide*.

CHAPTER CONVENTIONS

Acronym	Description
AS	Autonomous System
BGP	Border Gateway Protocol
CM	Configuration Mode - ALU (config)#
RCM	Router Configuration Mode - ALU (config-router bgp)#
SUM	Super User Mode - ALU#

BGP OVERVIEW

BGP is an inter-Autonomous System routing protocol. The primary function for a BGP speaking system is to exchange network reachability information (NLRI) with other BGP systems. This network reachability information includes information on the list of Autonomous Systems (ASs). This is sufficient to construct a graph of AS connectivity from which routing loops may be pruned and some policy decisions at the AS level may be enforced. The Alcatel-Lucent implementation of BGP supports BGP-4 specified in RFC 1771.

Each BGP update message consists of a list of NLRI and a set of Path Attributes shared amongst them. Common path-attributes are AS_PATH, NEXT-HOP, etc. BGP uses locally configured policies for route-selection among the different updates.

BGP neighbors form a TCP connection between one another. They exchange messages to open and confirm the connection parameters. The initial data flow is the entire BGP routing table. Incremental updates are sent as the routing tables change. BGP does not require periodic refresh of the entire BGP routing table, therefore a BGP speaker must retain the current version of the entire BGP routing tables from all of its peers for the duration of the connection. Keepalive messages are sent periodically to ensure the liveness of the connection. Notification messages are sent in response to errors or special conditions.

BGP CONFIGURATION

Refer to the following sections to configure BGP on your system:

- [“BGP Configuration Steps”](#)
- [“BGP Configuration Commands”](#)
- [“BGP Show Commands”](#)
- [“BGP Clear Commands”](#)



Note: This chapter lists only the mandatory steps to configure BGP. There are various other optional parameters that can be configured for BGP. To know more about the optional commands, refer to the BGP chapter in the ***OmniAccess 700 CLI Command Reference Guide***.

BGP CONFIGURATION STEPS

This section lists steps to configure BGP.

Step 1: Enter into Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Enable BGP Router. This enters the BGP Router Configuration Mode. See [“To Enable BGP Routing”](#)

Step 5: Configure BGP neighbors. See [“To Configure BGP Neighbors”](#)

Step 6: Configure the networks. See [“To Configure Networks to be Advertised”](#)

Step 7: View BGP configuration. See [“BGP Show Commands”](#)

Step 8: Reset BGP configuration. See [“BGP Clear Commands”](#)

BGP CONFIGURATION FLOW

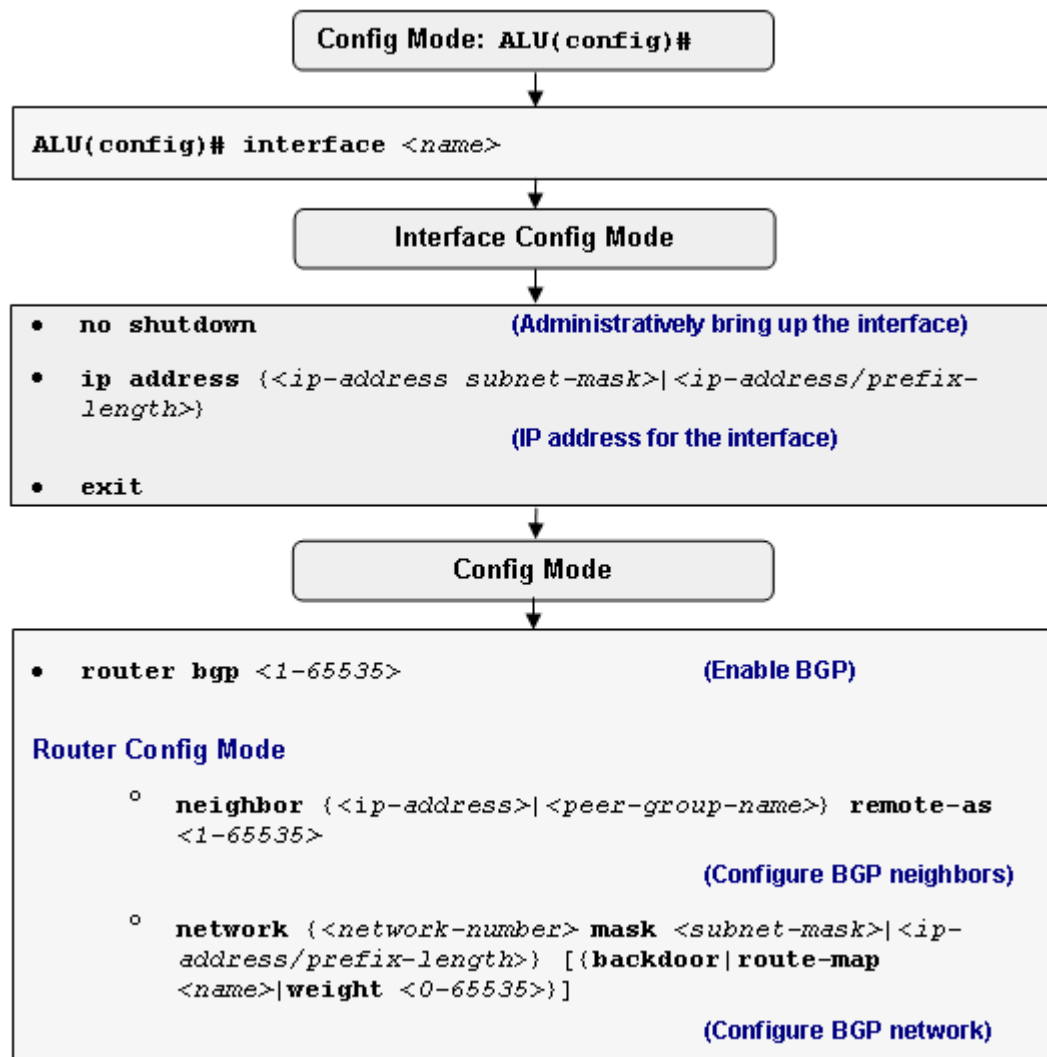


Figure 40: BGP Configuration Flow

BGP CONFIGURATION COMMANDS

There are several mandatory and optional configuration options available to configure BGP in OA-700. Some of the basic configuration required for a BGP connection with a peer is described in the following sections in this chapter.

To ENABLE BGP ROUTING

Command (in CM)	Description
<code>router bgp <1-65535></code>	This command enables BGP routing. This enters Router Configuration Mode. The range 1-65535 indicates Autonomous System number.

EXAMPLE

```
ALU(config)# router bgp 30
ALU(config-router bgp AS30)#
```



Note: Private AS value can range from 64512 to 65535.

To CONFIGURE BGP NEIGHBORS

After you have enabled the BGP routing process, the next step is to configure BGP neighbors. Every neighbor that this router wishes to peer with needs to be configured.

A BGP neighbor can be either internal or external.

- **Internal Neighbor:** Neighbors who are in the same AS. This is also referred to as an iBGP connection.
- **External Neighbor:** Neighbors who are in different AS. This is also commonly referred to as an eBGP connection. External neighbors are usually adjacent to each other, if they are not, **ebgp multihop** needs to be configured for that neighbor.

Command (in RCM)	Description
<code>neighbor {<ip-address> <peer-group-name>} remote-as <1-65535></code>	Configures a BGP neighbor and the AS to which this neighbor belongs.

EXAMPLE

```
ALU(config-router bgp AS30)# neighbor 1.1.1.1 remote-as 100
```

To CONFIGURE NETWORKS TO BE ADVERTISED

For eBGP, the network statement is one way to decide which networks from the router's own routing table will go into the router's BGP table and be announced to its eBGP peers. The route must have an exact match in the router's own routing table, otherwise it will not be advertised by BGP. The network statement decides where the update is to be sent.

This command is also used to configure BGP weight. A weight, is a number that can be assigned to a path so that the path selection process can be controlled. The administrative weight is local to the router.

Command (in RCM)	Description
<pre>network {<network-number> mask <subnetmask> <ip-address/ prefix-length>} [{backdoor route-map <name> / weight <0-65535>}]</pre>	<p>Use this command to specify the networks to be advertised through BGP.</p> <p>backdoor: This specifies a backdoor route to a BGP border router that will provide better information about the network.</p> <p>0-65535 specifies an absolute weight to a BGP network.</p>

EXAMPLE

```
ALU(config-router bgp AS30)#network 35.0.0.0/8
```

BGP SHOW COMMANDS

The following commands are used to view the BGP configuration details on your OA-700:

To VIEW BGP ROUTING TABLE DETAILS

Command (in SUM/CM)	Description
show ip bgp [<i><network-number></i> <i><ip-address/prefix-length></i>] [longer-prefixes]	This command displays the entries in the BGP routing table.

EXAMPLE

```
ALU# show ip bgp
```

```
BGP local router ID is 111.111.111.111
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Prefix/len	Next Hop	Metric	LocPref	Weight	Path
*> 1.0.0.0/8	1.1.1.2	200	100	70	100i
*> 4.0.0.0/8	1.1.1.2	200	100	70	100i
*> 5.0.0.0/8	1.1.1.2	200	100	70	100i
*> 6.0.0.0/8	1.1.1.2	200	100	70	100i
* d 7.0.0.0/8	1.1.1.2	200	100	70	100i
*> 111.111.111.0/24	111.111.111.112	110	100	50	300?
* d 118.0.0.0/24	111.111.111.112	110	100	50	300?

```
ALU#
```

To VIEW THE BGP SUMMARY

Command (in SUM/CM)	Description
show ip bgp summary	This command verifies whether peering is established with the router's neighbors and displays the basic statistics for messages and prefixes.

EXAMPLE

```
ALU# show ip bgp summary
```

```
BGP router identifier 111.111.111.111, local AS number 200
7 Prefix entries using 416 bytes of memory
7 Path entries for prefixes using 392 bytes of memory
Dampening enabled. 0 History paths. 2 Dampened paths
3 Path attribute entries using 672 bytes of memory
2 Aspath entries using 614 bytes of memory
2 Community entries using 44 bytes of memory
```

Neighbor	V	AS	MsgRcvd	MsgSent	InQ	OutQ	Up/Down	State/PfxRcd
1.1.1.2	4	100	342	333	0	0	00:12:46	5
111.111.111.112	4	300	323	331	0	0	00:17:39	2

```
ALU#
```

To VIEW BGP NEIGHBORS

Command (in SUM/CM)	Description
<code>show ip bgp neighbors <ip-address> [advertised-routes dampened-routes flap-statistics paths [<regular-expression>] received-routes routes]</code>	This command displays the information about the TCP and BGP neighbor connections.

EXAMPLE

ALU# show ip bgp neighbors

```

BGP neighbor is 1.1.1.2, remote AS 100, external link
  BGP version 4, remote router id 3.3.3.3
  BGP state = Established, up for 00:12:08
  Last read 00:00:07, Last sent 00:00:07
  Hold time is 180,  keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 342 messages, 0 notifications, 0 in queue
  Sent 333 messages, 7 notifications, 0 in queue
  Minimum time between advertisement runs is 30 seconds

For Address Family IPv4 Unicast
  Route refresh request: received 0, sent 0
  Number of Unicast prefixes received 5
  Prefixes advertised 1, accepted 5, filtered 0, dampened 1
  Number of updates pending 0, withdrawals pending 0
  Route map for incoming advertisements is metric1

  Connections established 9; dropped 8
  Last reset 00:12:44, due to Interface Flap
  Connection state is ESTAB
Local host: 1.1.1.1, Local port: 32835
Foreign host: 1.1.1.2, Foreign port: 179

iss: 0   snduna: 0   sndnxt: 0   sndwnd: 2
irs: 0   rcvnxt: 0   rcvwnd: 0

SRTT: 0 ms,  RTTO: 51964 ms,  RTV: 34464 ms,  minRTT: 0 ms
BGP neighbor is 111.111.111.112, remote AS 300, external link
  BGP version 4, remote router id 118.0.0.1
  BGP state = Established, up for 00:17:01
  Last read 00:01:00, Last sent 00:00:01
  Hold time is 180,  keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 322 messages, 1 notifications, 0 in queue
  Sent 331 messages, 8 notifications, 0 in queue
  Minimum time between advertisement runs is 30 seconds

For Address Family IPv4 Unicast

```

```
Route refresh request: received 0, sent 0
Number of Unicast prefixes received 2
Prefixes advertised 0, accepted 2, filtered 0, dampened 1
Number of updates pending 0, withdrawals pending 0
Route map for incoming advertisements is metric

Connections established 10; dropped 9
Last reset 00:17:05, due to BGP Notification sent, Cease Error
Connection state is ESTAB
Local host: 111.111.111.111, Local port: 179
Foreign host: 111.111.111.112, Foreign port: 32832

iss: 0   snduna: 0   sndnxt: 0   sndwnd: 2
irs: 0   rcvnxt: 0   rcvwnd: 0

SRTT: 0 ms,  RTTO: 18750 ms,  RTV: 7500 ms, minRTT: 0 ms
ALU#
```


BGP CLEAR COMMANDS

When two BGP routers are configured as neighbors, they establish BGP peering and exchange routing information. If changes are done to the BGP configuration, such as filter, version or timers, at a later point, the BGP connection must be reset for the changes to take effect.

For changes that apply to the BGP connection between two neighbors, a hard reset is required for these changes to take effect. This will reset the BGP session, and all routes in the BGP table from this neighbor will be lost.

A soft reset does not reset the BGP session. A soft reset updates the routing table for inbound and/or outbound routing updates. This soft reset allows the dynamic exchange of route refresh requests and routing information between BGP routers, and the subsequent re-advertisement of the respective outbound routing table.

There are outbound and inbound soft resets. An inbound soft reset is required for changes to the routing policy for a specific peer, such as route-maps, distribute-lists, prefix-lists, and filter-lists that affect the inbound updates. An outbound soft reset is required for the policy changes affecting outbound updates.

- When soft reset is used to send a new set of updates to a neighbor, it is called **outbound soft reset**. For this type of reset, the connection is not reset and the inbound routing table is not affected.
- When soft reset is used to generate inbound updates from a neighbor where both neighbors support the route refresh capability, it is called **dynamic inbound soft reset**. Route refresh capability is advertised in the OPEN message and no pre-configuration is required. This does not reset the BGP session.
- To use soft reset when both BGP peers do not support the route refresh capability, **configured inbound soft reset** can be used. This requires pre-configuration, it stores all received inbound routing-policy updates without modification.

To RESET THE BGP CONNECTION WITH A HARD RESET

To do a hard reset of the BGP connection, use the following command:

Command (in SUM)	Description
<code>clear ip bgp { * <neighbor-address> <peer-group-name> }</code>	This command clears the set BGP configuration details.

EXAMPLE

```
ALU# clear ip bgp 1.1.1.1
```

To RESET THE BGP CONNECTION USING DYNAMIC INBOUND SOFT RESET

If the BGP neighbor supports the route refresh capability, you can use the dynamic soft reset method for resetting the inbound BGP table. The **'clear ip bgp'** command with the **soft in** option allows you to perform a dynamic soft reset of the inbound BGP table.

Command (in SUM)	Description
clear ip bgp {* <neighbor-address>/<peer-group-name>} soft in	Performs a dynamic soft reset on the connection specified in the command.

To CONFIGURE BGP SOFT RESET USING STORED ROUTING POLICY INFORMATION

For BGP neighbors who do not support the route refresh capability, previously stored information can be used to generate a new set of BGP table updates. This could potentially have higher memory overhead since additional routing information needs to be stored.

The router needs to be configured to store the routing information it needs for this kind of inbound soft reset as shown below:

Command (in RCM)	Description
neighbor {<ip-address>/<peer-group-name>} soft-reconfiguration inbound	Configures the router to start storing updates.

The **'clear ip bgp'** command can be used to initiate a soft reset which will generate a new set of inbound BGP table updates based on the stored information.

Command (in SUM)	Description
clear ip bgp {* <neighbor-address>/<peer-group-name>} soft in	Performs a soft reset on the connection specified in the command, using the stored routing table information for that connection.

To RESET A ROUTER USING BGP OUTBOUND SOFT RESET

To perform an outbound soft reset, no pre-configuration is required. Enter this command in the Super User Mode and Configuration Mode as follows:

Command (in SUM)	Description
<code>clear ip bgp {* <neighbor-address>/<peer-group-name>} soft out</code>	Performs a outbound soft reset on the connection specified in the command.

A TYPICAL BGP EXAMPLE USING OA-700

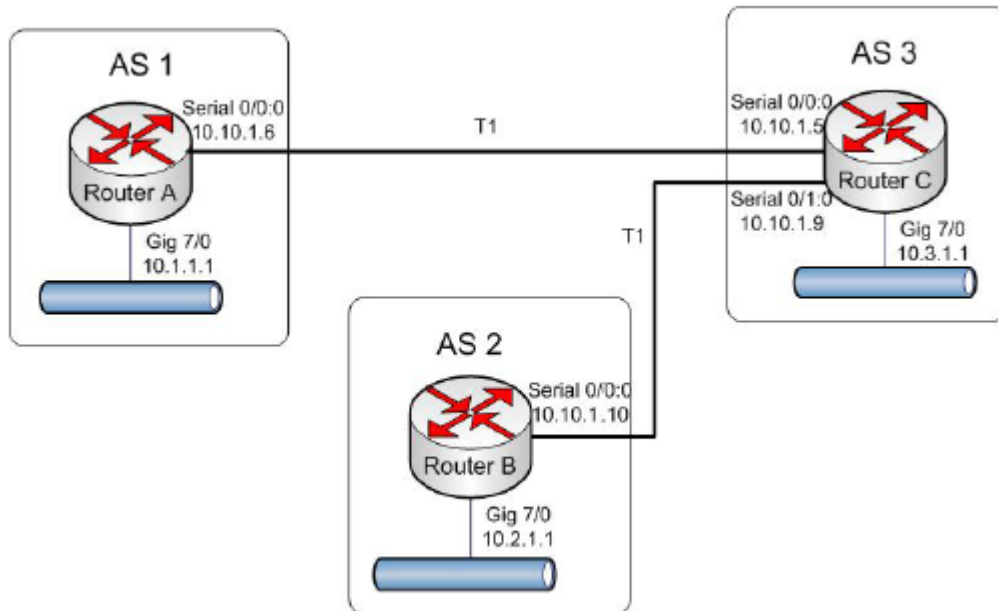


Figure 41: BGP Configuration Scenario

ROUTER A:

```
hostname RouterA
!
interface Serial0/0:0
  ip address 10.10.1.6/30
  encapsulation ppp
!
interface GigabitEthernet7/0
  ip address 10.1.1.1/24
!
router bgp 1
  neighbor 10.10.1.5 remote-as 3
!
address-family ipv4 unicast
  network 10.1.1.0/24
  neighbor 10.10.1.5 activate
```

ROUTER B:

```
hostname RouterB
!
interface Serial0/0:0
  ip address 10.10.1.10/30
  encapsulation ppp
!
interface GigabitEthernet7/0
  ip address 10.2.1.1/24
!
router bgp 2
  neighbor 10.10.1.9 remote-as 3
!
address-family ipv4 unicast
  network 10.2.1.0/24
  neighbor 10.10.1.9 activate
```

ROUTER C:

```
hostname RouterC
!
interface Serial0/0:0
  ip address 10.1.1.5/30
  encapsulation ppp
!
interface Serial0/1:0
  ip address 10.1.1.9/30
  encapsulation ppp
!
interface GigabitEthernet7/0
  ip address 10.3.1.1/24

router bgp 3
  neighbor 10.10.1.6 remote-as 1
  neighbor 10.10.1.10 remote-as 2
!
address-family ipv4 unicast
  neighbor 10.10.1.6 activate
  neighbor 10.10.1.10 activate
```


CHAPTER 22 OPEN SHORTEST PATH FIRST

This chapter covers the Open Shortest Path First (OSPF) configuration for the OA-700.

The “[OSPF Overview](#)” section serves as an additional information for Open Shortest Path First Protocol. You can skip this section, and directly go to the configuration section of this chapter.

CHAPTER CONVENTIONS

Acronym	Description
ABR	Area Border Router
ASBR	Autonomous System Border Router
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
LSA	Link State Advertisement
NSSA	Not-So-Stubby Areas
OSPF	Open Shortest Path First
RCM	Router Configuration Mode - ALU (config-router ospf)#
SUM	Super User Mode - ALU #
TSA	Totally Stubby Areas

OSPF OVERVIEW

OSPF is an IGP (Interior Gateway Protocol) developed by the OSPF working group of the IETF (Internet Engineering Task Force). RIP (Routing Information Protocol), an older routing protocol is also used by several corporate networks. Like RIP, OSPF is designated by the IETF as one of the several IGPs. OSPF is replacing RIP as the favoured router protocol in larger autonomous system networks.

OSPF was designed expressly for the IP networks. OSPF supports IP subnetting and tagging of externally derived routing information. Packet authentication and sending and receiving packets using IP multicast are also supported in OSPF.

Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. Unlike RIP, in which the entire routing table is sent, the host using OSPF sends only the part that has changed. With RIP, the routing table is sent to a neighbor host every 30 seconds. OSPF multicasts the updated information only when a change has taken place.

Instead of counting the number of hops, OSPF bases its path descriptions on "link states" that take into account additional network information. OSPF also lets the user assign cost metrics to a given host router so that some paths are given preference. OSPF supports a variable network subnet mask so that a network can be subdivided.

OSPF CONFIGURATION

This chapter includes the following sections:

- [“OSPF Configuration Steps”](#)
- [“OSPF Configuration Flow”](#)
- [“OSPF Configuration Commands”](#)
- [“OSPF Configuration on OA-700”](#)

OSPF CONFIGURATION STEPS

The steps given below helps in configuring and running basic OSPF on the OA-700.

Step 1 to Step 5 are the minimum configuration requirements for enabling OSPF. Step 6 describes other important but optional configuration commands for OSPF.

Step 1: Configure an interface. Enter Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```



Note: OSPF can be configured on GigabitEthernet, Serial, Tunnel, VLAN, Loopback interfaces.

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Enable OSPF. See [“To Enable OSPF”](#)

Step 5: Configure OSPF network. See [“To Configure OSPF Network”](#)

Step 6: Configure the following OSPF optional parameters. See “[OSPF Optional Parameters](#)”

- Configure Passive Interfaces. See “[To Configure Passive Interfaces](#)”
- Configure OSPF Area Parameters. See “[To Configure OSPF Area Parameters](#)”
- Configure OSPF Interface Parameters. See “[To Configure OSPF Interface Parameters](#)”
- LSA Group Pacing. See “[LSA Group Pacing](#)”
- Configure OSPF for Non-broadcast Networks. See “[To Configure OSPF for Non-broadcast Networks](#)”
- Configure Route Summarization. See “[To Configure Route Summarization](#)”
- Generate a Default Route. See “[To Generate a Default Route](#)”
- Control Default Metrics. See “[To Control Default Metrics](#)”
- Configure OSPF Administrative Distances. See “[To Configure OSPF Administrative Distances](#)”
- Configure Route Calculation Timers. See “[To Configure Route Calculation Timers](#)”
- Log Adjacency Changes. See “[To Log Adjacency Changes](#)”

OSPF CONFIGURATION FLOW

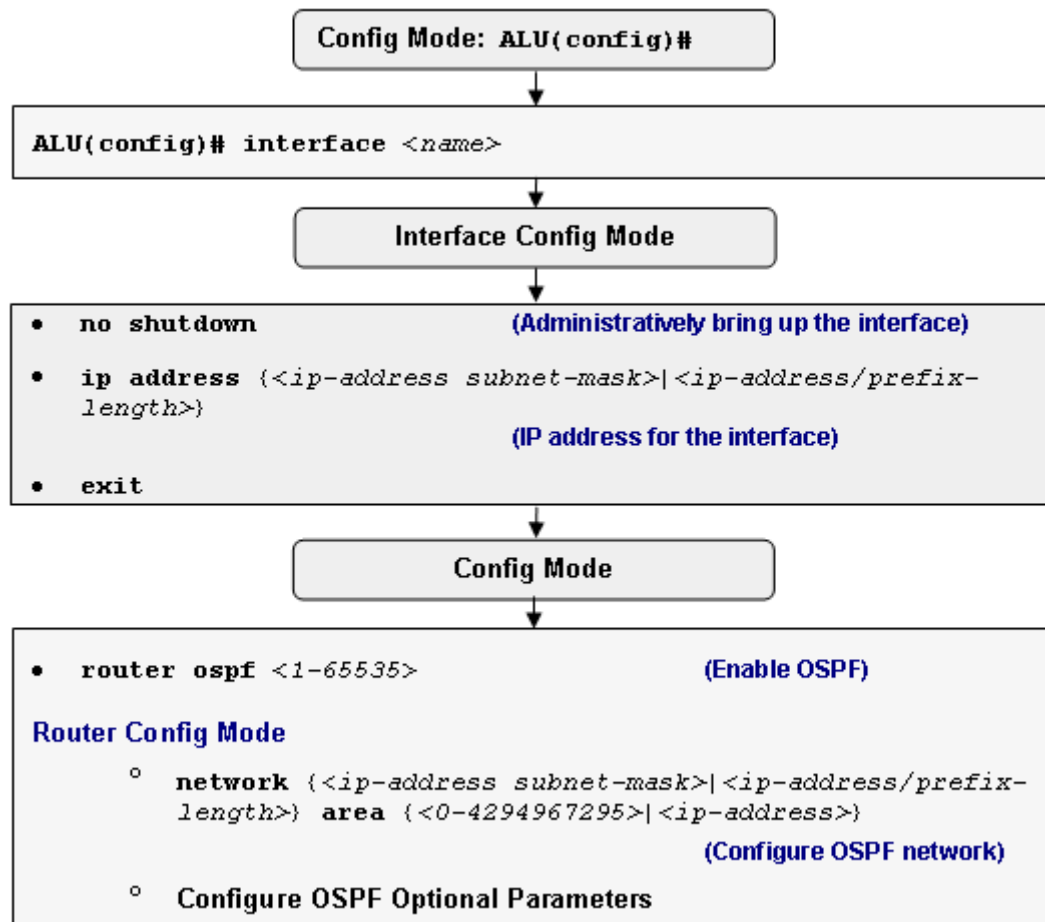


Figure 42: OSPF Configuration Flow

OSPF CONFIGURATION COMMANDS

To configure OSPF, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional, but might be required for your network.

To ENABLE OSPF

The OSPF process ID is not an autonomous system number. The process ID can be any positive integer and has no significance outside the router on which it is configured. The process ID merely distinguishes one process from another within the device. You can configure maximum of 30 OSPF instances.

As with other routing protocols, enabling OSPF requires you to create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses. Use the following commands for this purpose:

Command (in CM)	Description
<code>router ospf <1-65535></code>	Enables OSPF routing, which places you in Router Configuration Mode.

EXAMPLE

```
ALU(config)# router ospf 1
```

To CONFIGURE OSPF NETWORK

Specify the interfaces on which to run OSPF, and their areas, with the "**network area**" command. This command is flexible, reflecting the fully classless nature of OSPF. Any address range can be specified with an address, inverse mask pair. The area can be specified in decimal or dotted decimal [0 or 0.0.0.0].

Command (in RCM)	Description
<code>network {<ip-address subnet-mask> <ip-address/prefix-length>} area {<0-4294967295> <ip-address>}</code>	Enables routing on an IP network and the area ID for that interface.



Note: Area '0' is called the backbone area.

EXAMPLE

```
ALU(config-router ospf 1)# network 10.0.0.0/8 area 1
```

OSPF OPTIONAL PARAMETERS

To CONFIGURE PASSIVE INTERFACES

If some of the interfaces within the network should not run the routing protocol, the “**passive-interface**” command has to be used with these protocols.

Command (in RCM)	Description
passive-interface { GigabitEthernet Serial } <slot/ port> Loopback <0-14487> default }}	Suppresses sending of routing updates packets and OSPF hello packets through the specified interface.
no passive-interface { GigabitEthernet Serial } <slot/ port> Loopback <0-14487> default }}	The “ no passive-interface ” command enables sending of hello packets and routing updates on a specified interface.

EXAMPLE

```
ALU(config-router ospf 1)#passive-interface GigabitEthernet 7/0

ALU(config-router ospf 1)# no passive-interface GigabitEthernet
7/0
```

To CONFIGURE OSPF AREA PARAMETERS

The OSPF software allows you to configure several area parameters. These area parameters, described below, include authentication, defining stub areas, and assigning costs to the default summary route. Authentication allows password-based protection against unauthorized access to an area.

Information about external routes are not sent to the stub areas. Instead, a default external route is generated by the ABR, to provide information to the stub areas regarding the destinations outside the autonomous system. To take advantage of the OSPF stub area support, default routing must be used in the stub area. To further reduce the number of LSAs sent to a stub area, configure the “**no-summary**” keyword of the area stub router configuration command on the ABR. This prevents it from sending summary link advertisement (LSAs type 3) into the stub area.

To specify an area parameter for your network, use the following commands:

To ENABLE AREA AUTHENTICATION

Command (in RCM)	Description
area {<0-4294967295>/<ip-address>} authentication [message-digest]	Enables authentication for an OSPF area. Use ' message-digest ' keyword to enable MD5 authentication. The default authentication is Plain Text authentication.
no area {<0-4294967295>/<ip-address>} authentication [message-digest]	Disables authentication for an OSPF area.

EXAMPLE

```
ALU(config-router ospf 1)# area 1 authentication message-digest
```

To CONFIGURE DEFAULT COST

Command (in RCM)	Description
area {<0-4294967295>/<ip-address>} default-cost <0-16777215>	Assigns a specific cost to the default summary route used for the stub area/NSSA.
no area {<0-4294967295>/<ip-address>} default-cost <0-16777215>	Removes the specific cost assigned to the default summary route used for the stub area/NSSA.

EXAMPLE

```
ALU(config-router ospf 1)# area 1 default-cost 100
```

To CONFIGURE OSPF NSSA

NSSA does not flood type 5 external LSAs from the core into the area, but can import autonomous system external routes in a limited fashion within the area. NSSA allows importing of type 7 autonomous system external routes within NSSA area by redistribution. These type 7 LSAs are translated into type 5 LSAs by NSSA ABRs, which are flooded throughout the whole routing domain. Summarization and filtering are supported during the translation.

To specify area parameters to configure OSPF NSSA, enter the following command:

Command (in RCM)	Description
<code>area {<0-4294967295>/<ip-address>} nssa [default-information-originate] [no-summary] [no-redistribution]</code>	Defines an area to be NSSA. The TSAs are configured by placing the keyword " no summary ". This step is necessary only at the ABR.
<code>no area {<0-4294967295>/<ip-address>} nssa [default-information-originate] [no-summary] [no-redistribution]</code>	The 'no' command sets area to default.

You can set a type 7 default route that can be used to reach external destinations. When configured, the router generates a type 7 default route into the NSSA.

Every router within the same area must agree that the area is NSSA; otherwise, the routers will not form adjacency.

EXAMPLE

```
ALU(config-router ospf 1)# area 1 nssa
```

TO CONFIGURE AREA RANGE

The 'range' command consolidates and summarizes routes at an area boundary. Route summarization is the consolidation of advertised addresses.

If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range. To specify an address range, enter the following command:

Command (in RCM)	Description
<code>area {<0-4294967295>/<ip-address>} range {<ip-address subnet-mask/<ip-address/prefix-length>} [not-advertise]</code>	Specifies an address range for which a single route will be advertised. If ' not advertise ' keyword is used, the Type 3 summary LSA is suppressed, and the networks remain hidden from other networks.
<code>no area {<0-4294967295>/<ip-address>} range {<ip-address subnet-mask/<ip-address/prefix-length>} [not-advertise]</code>	Removes an address range for which a single route is to be advertised.

EXAMPLE

```
ALU(config-router ospf 1)# area 1 range 10.0.0.0/8 not-advertise
```

To CONFIGURE STUB-AREAS

Command (in RCM)	Description
<code>area {<0-4294967295>/<ip-address>} stub [no-summary]</code>	Defines an area to be a stub area. If 'no-summary' keyword is used, then ABR does not send summary link advertisements into the stub area.
<code>no area {<0-4294967295>/<ip-address>} stub [no-summary]</code>	The 'no' command sets area to default.



Note: The area '0' cannot be configured as a stub as it forms the backbone of the network.

EXAMPLE

```
ALU(config-router ospf 1)# area 1 stub no-summary
```

To CREATE VIRTUAL LINKS

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a virtual link. The two endpoints of a virtual link are ABRs.

The virtual link must be configured on both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR) and the non backbone area that the two routers have in common (called the transit area). Virtual links cannot be configured through stub areas.

Command (in RCM)	Description
<pre> area {<0-4294967295>/<ip-address>} virtual-link <router-id> [authentication [message- digest null] [[hello- interval retransmit-interval retransmit-interval transmit- delay dead-interval] <1-8192>] authentication-key <0-0> <key>] message-digest-key <1-255> md5 <key>]] </pre>	Establishes a virtual link with neighbor specified by router ID.
<pre> no area {<0-4294967295>/<ip- address>} virtual-link <router-id> [authentication [message- digest null] [[hello- interval retransmit-interval retransmit-interval transmit- delay dead-interval] <1-8192>] authentication-key <0-0> <key>] message-digest-key <1-255> md5 <key>]] </pre>	Removes the virtual link with neighbor specified by router ID.

To display information about virtual links, use the '**show ip ospf virtual-links**' command. To display the router ID of an OSPF router, use the '**show ip ospf**' command.

EXAMPLE

```
ALU(config-router ospf 1)# area 1 virtual-link 202.202.202.5
```

To CONFIGURE OSPF INTERFACE PARAMETERS

The OSPF implementation allows you to alter certain interface-specific OSPF parameters.

Some interface parameters like **'ip ospf hello-interval'**, **'ip ospf dead-interval'**, and **'ip ospf authentication-key'** must be consistent across all routers in an attached network. If you configure any of these parameters, make sure that the configurations for all the routers on the network should have compatible values.

To specify the interface parameters for the network, enter the following commands in the Interface Configuration Mode:

Command (in ICM)	Description
<code>ip ospf cost <1-65535></code>	Specifies the cost of sending a packet on an OSPF interface. The value set by the 'ip ospf cost' command overrides the cost resulting from the auto-cost command.
<code>ip ospf retransmit-interval <1-65535></code>	Specifies the time (in seconds) between LSA retransmissions for adjacencies belonging to an OSPF interface. The default retransmit-interval is 5 seconds.
<code>ip ospf transmit-delay <1-65535></code>	Sets the estimated time in seconds required to send a link-state update packet on an OSPF interface. The default transmit-delay is 1 second.
<code>ip ospf priority <0-255></code>	Sets the priority to help determine the OSPF designated router for a network. The default OSPF interface priority is 1.
<code>ip ospf hello-interval <1-65535></code>	Specifies the length of time (in seconds) between the hello packets that OSPF sends on an interface. On broadcast network, the default hello-interval is 10 seconds.
<code>ip ospf dead-interval <1-65535></code>	Sets the number of seconds that a device must wait before it declares a neighbor OSPF router dead because it has not received a hello packet. On broadcast network, the dead-interval is 40 seconds.

Command (in ICM)	Description
<code>ip ospf mtu-ignore</code>	Disables detection of OSPF MTU mismatch in Database Description Packets. By default, MTU mismatch detection is enabled.
<code>ip ospf database-filter all out</code>	Enables filtering of outgoing LSAs on OSPF interface. By default, database-filtering is not enabled.

EXAMPLE

```

ALU(config-if GigabitEthernet7/0)# ip ospf cost 100

ALU(config-if GigabitEthernet7/0)# ip ospf retransmit-interval
6

ALU(config-if GigabitEthernet7/0)# ip ospf transmit-delay 2

ALU(config-if GigabitEthernet7/0)# ip ospf priority 2

ALU(config-if GigabitEthernet7/0)# ip ospf hello-interval 20

ALU(config-if GigabitEthernet7/0)# ip ospf dead-interval 50

ALU(config-if GigabitEthernet7/0)# ip ospf mtu-ignore

ALU(config-if GigabitEthernet7/0)# ip ospf database-filter all
out

```

To CONFIGURE AUTHENTICATION FOR AN INTERFACE

OSPF packets can be authenticated to prevent inadvertent or intentional introduction of bad routing information. OSPF authentication on OA-700 supports both clear text as well as MD5 cryptographic checksum.

Command (in ICM)	Description
<code>ip ospf authentication [message-digest null]</code>	<p>This command is used to enable authentication for OSPF.</p> <p>Use 'message-digest' keyword to enable MD5 authentication.</p> <p>The default authentication mode is Plain Text authentication.</p> <p>If 'null' keyword is used, then no authentication is used. It is used to override authentication configured for an area.</p>
<code>ip ospf authentication-key {<0-0>/<password-key>}</code>	<p>This command assigns an authentication password to be used by OSPF routers on a network segment.</p> <p>Password need not be the same throughout the area but needs to be the same between neighbors.</p>
<code>ip ospf message-digest-key <1-255> md5 <key></code>	<p>Enables OSPF MD5 authentication. The values for the key-id and key arguments must match the values specified for other neighbors on a network segment.</p>

The **"no"** form of these commands negates the configured authentication.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip ospf authentication
```

```
ALU(config-if GigabitEthernet7/0)# ip ospf authentication-key  
passwordtest
```

```
ALU(config-if GigabitEthernet7/0)# ip ospf authentication  
message-digest
```

```
ALU(config-if GigabitEthernet7/0)# ip ospf message-digest-key  
100 md5 passwordline
```

To CONFIGURE OSPF NETWORK TYPE

By default, OSPF classifies different media into the following three types of network:

- Broadcast networks: Ethernet, Token Ring and FDDI
- NBMA (Non-Broadcast Multiple Access) networks: SMDS (Switched Multimegabit Data Service), Frame Relay and X.25
- Point-to-point networks: (HDLC) High-Level Data Link Control and PPP

You have the choice of modifying interface type regardless of the default media type.

Command (in ICM)	Description
<code>ip ospf network {broadcast non-broadcast point-to-point}</code>	Configures the OSPF network type for a specified interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip ospf network non-  
broadcast
```

LSA GROUP PACING

The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, checksumming, and aging functions. Group pacing results in more efficient use of the router. Group pacing avoids sudden increases in the CPU usage and network resources. This feature is most beneficial to large OSPF networks. By default, the OSPF LSA group pacing is enabled.

Original LSA Behavior

Each OSPF LSA has an age, which indicates the validity of the LSA. Once LSA reaches the maximum age (1 hour), it is discarded. During the aging process, the originating router sends a refresh packet every 30 minutes to refresh the LSA. Refresh packets are sent to keep the LSA from expiring, whether there has been a change in the network topology or not. Checksumming is performed on all LSAs every 10 minutes. The router keeps track of the LSAs it generates and the LSAs it receives from other routers. The router refreshes the LSAs it generated and ages the LSAs it received from other routers.

LSA GROUP PACING WITH MULTIPLE TIMERS

This problem is solved by configuring each LSA to have its own timer. For example, each LSA gets refreshed every 30 minutes, independent of other LSAs; so the CPU is used only when necessary.

Refreshing LSAs at frequent, random intervals requires the router to send many packets, which uses up the bandwidth. Therefore, the router delays the LSA refresh function for an interval of time. The accumulated LSAs constitute a group, which is then refreshed and sent out in one packet or more. Thus, the refresh packets are paced, as are the checksumming and aging.

Command (in RCM)	Description
<code>timers lsa-group-pacing <10-1800></code>	Changes the group pacing of LSAs. The default lsa-group pacing interval is 60 seconds.

EXAMPLE

```
ALU(config-router ospf 1)# timers lsa-group-pacing 100
```

TO REDUCE LSA FLOODING

By design, OSPF requires LSAs to be refreshed as they expire after 3600 seconds. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 minutes to about 50 minutes.

This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires. The OSPF flooding reduction solution works by reducing unnecessary refreshing and flooding of already known and unchanged information.

Command (in ICM)	Description
<code>ip ospf flood-reduction</code>	Suppresses the unnecessary flooding of LSAs in stable topologies.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# ip ospf flood-reduction
```

To CONFIGURE OSPF FOR NON-BROADCAST NETWORKS

Special configuration parameters are needed in the designated router selection if broadcast capability is not configured.

To configure routers, that interconnect to non-broadcast networks, you need to configure static neighbors.

Command (in RCM)	Description
<code>neighbor <ip-address> [cost <1-65535> database-filter all out priority <0-255> poll-interval <0-4294967295>]</code>	This command is used to configure a neighbor router. Use this command only if the network type is 'non-broadcast'.

You can specify the following neighbor parameters, as required:

- **Priority:** Indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0.
- **Poll Interval:** The router sends unicast hello packets every poll interval to the neighbor from which hello packets have not been received within the dead interval.
- **Cost:** Assigns a cost to the neighbor. Neighbors with no specific cost configured will assume the cost of the interface.
- **Database-filter all:** Filters the outgoing LSAs to an OSPF neighbor.

EXAMPLE

```
ALU(config-router ospf 1)# neighbor 10.0.0.1 priority 1 poll-
interval 130
```

To CONFIGURE ROUTE SUMMARIZATION

Though the stub areas conserve resources within non-backbone areas by preventing certain LSA's from entering, these areas do nothing to conserve resources on the backbone. Address Summarization conserves resources by reducing the number of LSA's being flooded and by hiding instabilities. An ABR can be configured to advertise a summary address either into backbone or into a non-backbone area. The best practice is that a non-backbone area address should be summarized into backbone by its own ABR as opposed to having all other ABR's summarize the area address into their areas.

When routes from other protocols are redistributed into OSPF, each route is advertised individually in an external LSA. However, you can configure OA-700 to advertise a single route for all the redistributed routes that are covered by a specified network address and mask. This helps decrease the size of the OSPF link-state database.

To advertise one summary route for all redistributed routes covered by a network address and mask, enter the following command:

Command (in RCM)	Description
summary-address {<ip-address subnet-mask/> <ip-address/prefix-length>} [not-advertise tag <0-4294967295>]	Specifies an address and mask that covers redistributed routes, so only one summary route is advertised. Use the optional not-advertise keyword to filter out a set of routes.

EXAMPLE

```
ALU(config-router ospf 1)# summary-address 20.0.0.0/8 tag 20
```

```
ALU(config-router ospf 1)# summary-address 10.0.0.0/8 not
advertise
```


To GENERATE A DEFAULT ROUTE

You can force an ASBR to generate a default route into an OSPF routing domain. When redistribution of routes is specifically configured into an OSPF routing domain, the router automatically becomes an ASBR.

However, an ASBR does not, generate a default route into the OSPF routing domain, by default. To force the ASBR to generate a default route, enter the following command:

Command (in RCM)	Description
default-information originate [always] [metric <0-16777214>] [metric-type <1-2>] [route-map <route-map name>]	Forces the autonomous system boundary router to distribute a default route into the OSPF routing domain.

EXAMPLE

```
ALU(config-router ospf 1)# default-information originate always
metric 100
```

To CONFIGURE REDISTRIBUTION

Command (RCM)	Description
redistribute { connected static bgp <1-65535> ospf <1-65535>} [metric <0-16777214> metric-type <1-2> route-map <map-name> tag <0-4294967295> subnets]	This command is used redistribute routes to OSPF.

EXAMPLE

```
ALU(config-router ospf 1)#redistribute static metric 19 metric-
type 1
```

To CONTROL DEFAULT METRICS

By default, OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface.

The OSPF metric is calculated as the reference bandwidth value divided by the bandwidth value, with the reference bandwidth value equal to 10^8 by default, and the bandwidth value determined by the bandwidth interface configuration command. If you have multiple links with high bandwidth, you might want to specify a larger number to differentiate the cost on those links. To do so, enter the following command:

Command (in RCM)	Description
<code>auto-cost [reference-bandwidth <1-4294967>]</code>	<p>This command is used to calculate the interface cost based on the reference bandwidth.</p> <p>Default value for reference bandwidth is 100.</p> <p>The OSPF metric is calculated as the reference bandwidth value divided by the bandwidth, with reference bandwidth equal to 10^8 by default.</p>

EXAMPLE

```
ALU(config-router ospf 1)# auto-cost reference-bandwidth 100
```

To CONFIGURE OSPF ADMINISTRATIVE DISTANCES

An administrative distance is an integer from 1 to 255. '0' administrative distance is used for connected routes to give a high preference to these routes. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

OSPF uses three different administrative distances: intra-area, inter-area, and external. Routes within an area are intra-area; routes to another area are inter-area; and routes from another routing domain learned via redistribution are external. The default distance for each type of route is 110. To change any of the OSPF distance values, enter the following command:

Command (in RCM)	Description
<code>distance {<1-255> [<ip-address subnet-mask/<ip-address/prefix-length>][<1-99>] [<1300-1999>]}</code>	This command is used to change the administrative distance for a given network.
<code>distance ospf {external inter-area intra-area} <1-255>}}</code>	This command performs the same function as the distance command used with an access list. However, the 'distance ospf' command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

'Distance ospf' command is used when we have multiple OSPF instance and we want prefer routes of one OSPF instance over routes of other instance.

EXAMPLE

```
ALU(config-router ospf 1)# distance 60 10.0.0.0/8
```

```
ALU(config-router ospf 1)# distance ospf external 10
```

To CONFIGURE ROUTE CALCULATION TIMERS

You can configure the delay in the time when OSPF receives a topology change and when it starts a SPF (Shortest Path First) calculation. You can also configure the hold time between two consecutive SPF calculations. To do so, use the following command:

Command (in RCM)	Description
<code>timers spf {<0-65535> <0-65535>}</code>	<p>Configures the delay time and hold time for Shortest Path First (SPF) calculation.</p> <p>spf delay: Delay time (in seconds) between when OSPF receives a topology change and when it starts an SPF calculation. The default time is 5 seconds.</p> <p>A value of '0' means that there is no delay; that is, the SPF calculation starts immediately.</p> <p>spf hold: Minimum time (in seconds) between two consecutive SPF calculations. The default time is 10 seconds.</p> <p>A value of '0' means two consecutive SPF calculations can be done one immediately after the other.</p>

EXAMPLE

```
ALU(config-router ospf 1)# timers spf 20 10
```

To LOG ADJACENCY CHANGES

By default, the system sends a notification when an OSPF neighbor comes up or goes down.

Command (in RCM)	Description
<code>log-adjacency-changes [detail]</code>	<p>This command is used to enable logging of adjacency changes.</p> <p>Use 'detail' keyword to log the messages for all state changes.</p>
<code>no log-adjacency-changes</code>	<p>This command is used to disable logging.</p>

EXAMPLE

```
ALU(config-router ospf 1)# log-adjacency-changes detail
```

```
ALU(config-router ospf 1)# no log-adjacency-changes
```

To CONFIGURE ALTERNATE ABR (RFC 3509)

Command (in RCM)	Description
<code>alt-abr [cisco ibm]</code>	This command enables OSPF router behavior specified in RFC 3509. By default, OSPF router follows ABR behavior specified in RFC 2328.

EXAMPLE

```
ALU(config-router ospf 1)# alt-abr
```

COMPATIBLE RFC1583

This command restores the method used to calculate summary route costs per RFC 1583. To minimize the chance of routing loops, all OSPF routers in an OSPF routing domain should have RFC compatibility set identically. Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the `no compatible rfc1583` command to enable the calculation method used per RFC 2328.

Command (in RCM)	Description
<code>compatible rfc1583</code>	This command restores the method used to calculate summary route costs per RFC 1583.

EXAMPLE

```
ALU(config-router ospf 1)# compatible rfc1583
```

To CONFIGURE DEFAULT METRIC

Command (in RCM)	Description
<code>default-metric <1-4294967295></code>	This command sets the default metric values for the OSPF routing protocol. The default metric is 20.

EXAMPLE

```
ALU(config-router ospf 30)#default-metric 60000
```

To CONFIGURE ROUTER-ID

Command (in RCM)	Description
<code>router-id <ip-address></code>	This command configures the OSPF router ID.

EXAMPLE

```
ALU(config-router ospf 30)#router-id 35.0.0.1
```

To VIEW OSPF RUNNING CONFIGURATION

Command (in RCM)	Description
<code>write ospf</code>	This command is used to view the OSPF running configuration.

EXAMPLE

```
ALU(config-router ospf 30)#write ospf
```

SHOW COMMANDS IN OSPF

OSPF show commands display specific statistics, databases, neighbor information, OSPF routing table information.

DISPLAY OSPF UPDATE PACKET PACING

While sending update packets, some packets may not reach **antilabor** in the first attempt. OSPF protocol adds those packets in re-transmission lists.

To view list of LSAs waiting to be flooded over a specified interface, use the following command:

Command (in SUM)	Description
<code>show ip ospf flood-list</code> [<code>{GigabitEthernet Serial}</code> <code><slot/port></code> <code>Loopback <0-14487></code>]	Displays a list of LSAs waiting to be flooded over an interface.

EXAMPLE

```
ALU# show ip ospf flood-list
```

```
OSPF Router with ID (1.1.1.2) (Process ID 1)
```

```
Interface GigabitEthernet 7/0, Queue length 1
```

```

Type  LS ID   ADV RTR   Seq NO      Age      Checksum
  1   1.1.1.2  1.1.1.2   0x8000001D  0        0x04EA
ALU#
```

To Display Various Routing Statistics

To display various routing statistics, use the following commands in the Super User Mode:

Command (in SUM)	Description
<code>show ip ospf [<1-65535>]</code>	Displays general information about all the OSPF routing processes. If the process ID is specified, displays information about that process.
<code>show ip ospf [<1-65535>] border-routers</code>	Displays the internal OSPF routing table entries to an ABR and ASBR.
<code>show ip ospf [<1-65535>] database [{adv-router <ip-address> asbr-summary database-summary external network nssa-external router summary } [adv-router <ip-address> self-originate ip-address] self-originate]]</code>	Displays lists of information related to the OSPF database.
<code>show ip ospf [<1-65535>] flood-list [{GigabitEthernet Serial } <slot/port> Loopback <0-14487>]]</code>	Displays a list of LSAs waiting to be flooded over an interface.
<code>show ip ospf [<1-65535>] interface [{GigabitEthernet Serial } <slot/port> Loopback <0-14487> statistics]]</code>	Displays OSPF-related interface information.
<code>show ip ospf [<1-65535>] neighbor [neighbor-router-id] [{GigabitEthernet Serial } <slot/port> Loopback <0-14487>] [detail]</code>	Displays OSPF neighbor information on a per-interface basis.
<code>show ip ospf process-interface</code>	Displays the process interface table.
<code>show ip ospf interface-process [{GigabitEthernet Serial } <slot/port> Loopback <0-14487>]]</code>	Displays the interface-process table.
<code>show ip ospf [<1-65535>] request-list [neighbor-router-id] [{GigabitEthernet Serial } <slot/port> Loopback <0-14487>]]</code>	Displays a list of all LSAs requested by a router.
<code>show ip ospf [<1-65535>] retransmission-list [neighbor-router-id] [{GigabitEthernet Serial } <slot/port> Loopback <0-14487>]]</code>	Displays a list of all LSAs waiting to be resent.

Command (in SUM)	Description
<code>show ip ospf [<1-65535>] route</code>	Displays the OSPF internal routing table.
<code>show ip ospf [<1-65535>] summary-address</code>	Displays a list of all summary address redistribution information configured under an OSPF process.
<code>show ip ospf [<1-65535>] virtual-links</code>	Displays virtual link adjacency information.

EXAMPLES**Ex 1:**

```
ALU# show ip ospf
```

```
Routing Process "ospf 1" with ID 1.1.1.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an area border and autonomous system boundary router
  Redistributing External Routes from:
    connected route-map permit

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 4. Checksum Sum 0x1c8fd
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
Full neighbors 2
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    Area has message digest authentication
    SPF algorithm executed 36 times
    Area ranges are
    Number of LSA 6. Checksum Sum 0x35E53
    Number of opaque link LSA 0. Checksum Sum 0x0
    Flood list length 0
  Area 1
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 8 times
    Area ranges are
    Number of LSA 5. Checksum Sum 0x234A3
    Number of opaque link LSA 0. Checksum Sum 0x0
    Flood list length 0
```

Ex 2:

ALU# show ip ospf border-routers

OSPF Process 1 internal Routing Table

Codes : i - Intra-area route, I - Inter-area route

i 6.6.6.6 [100] via 2.2.2.1, GigabitEthernet 7/1, ABR, Area 1,
SPF 5
ALU#

Ex 3:**ALU# show ip ospf database**

OSPF Router with ID (1.1.1.2) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	
Link count					
1.1.1.1	1.1.1.1	957	0x800000FC	0xAE6C	1
1.1.1.2	1.1.1.2	96	0x80000019	0xF2F0	1
6.6.6.6	6.6.6.6	2430	0x80000008	0xC20B	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
2.2.2.1	6.6.6.6	2430	0x80000006	0xB91F
1.1.1.2	1.1.1.2	1121	0x80000004	0xBD46

Summary Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
2.2.2.0	1.1.1.2	96	0x80000002	0x43CC

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum	
Link count					
1.1.1.2	1.1.1.2	1744	0x80000005	0x579A	1
6.6.6.6	6.6.6.6	1745	0x80000002	0xD8F9	1

Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
2.2.2.2	1.1.1.2	1747	0x80000001	0x4AA5

Summary Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
1.1.1.0	1.1.1.2	96	0x80000003	0x65AC

Summary ASBR Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
1.1.1.1	1.1.1.2	96	0x80000002	0x4FC1

Type-5 AS External Link States

Link ID Tag	ADV Router	Age	Seq#	Checksum
1.1.1.0	1.1.1.2	1664	0x80000003	0x9F10 0
2.2.2.0	1.1.1.2	639	0x80000004	0x9D0B 0
3.3.3.0	1.1.1.1	131	0x80000001	0x5D36 0
45.5.5.0	1.1.1.2	1603	0x80000003	0xC4BB 0

Ex 4:**ALU# show ip ospf flood-list**

OSPF Router with ID (1.1.1.2) (Process ID 1)

Interface GigabitEthernet 7/0, Queue length 1

Type	LS ID	ADV RTR	Seq NO	Age	Checksum
1	1.1.1.2	1.1.1.2	0x03000080	0	0x9109

Ex 5:**ALU# show ip ospf interface**

```
GigabitEthernet7/0 is up, line protocol is up
  Internet Address 1.1.1.2/24, Area 0
  Process ID 1, Router ID 1.1.1.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.2, Intf address 1.1.1.2
  Backup Designated router (ID) 1.1.1.1, Intf address 1.1.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
GigabitEthernet7/1 is up, line protocol is up
  Internet Address 2.2.2.2/24, Area 1
  Process ID 1, Router ID 1.1.1.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 6.6.6.6, Intf address 2.2.2.1
  Backup Designated router (ID) 1.1.1.2, Intf address 2.2.2.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 6.6.6.6 (Designated Router)
```

```
Supress hello for 0 neighbor(s)
ALU#
```

```
ALU# show ip ospf interface GigabitEthernet 7/0
```

```
GigabitEthernet7/0 is up, line protocol is up
Internet Address 1.1.1.2/24, Area 0
Process ID 1, Router ID 1.1.1.2, Network Type BROADCAST, Cost: 100
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.2, Intf address 1.1.1.2
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Neighbor Count is 0, Adjacent neighbor count is 0
Supress hello for 0 neighbor(s)
Message digest authentication enabled
ALU#
```

```
ALU# show ip ospf interface statistics
```

```
GigabitEthernet7/0
Internet Address 1.1.1.2/24, ProcessID 1, Area 0
Hello Packets Received 516, Hello Packets Sent 508
Database Description Packets Received 11, Database
Description Packets Sent 9
LS Request Packets Received 1, LS Request Packets Sent 2
LS Update Packets Received 22, LS Update Packets Sent 11
LS Acknowledgment Packets Received 7, LS Acknowledgment
Packets Sent 15
Errors 0, Events 0
GigabitEthernet7/1
Internet Address 2.2.2.2/24, ProcessID 1, Area 1
Hello Packets Received 506, Hello Packets Sent 507
Database Description Packets Received 6, Database Description
Packets Sent 7
LS Request Packets Received 0, LS Request Packets Sent 2
LS Update Packets Received 14, LS Update Packets Sent 38
LS Acknowledgment Packets Received 19, LS Acknowledgment
Packets Sent 8
Errors 1, Events 0
ALU#
```

Ex 6:**ALU# show ip ospf neighbor**

```

Process ID 1
Neighbor ID   Pri   State           Dead Time   Address
Interface
1.1.1.1      1    FULL/BDR       00:00:33   1.1.1.1
GigabitEthernet7/0
6.6.6.6      1    FULL/BDR       00:00:37   2.2.2.1
GigabitEthernet7/1
ALU#

```

ALU# show ip ospf neighbor GigabitEthernet 7/1

```

Process ID 1
Neighbor ID   Pri   State   Dead Time   Address   Interface
6.6.6.6      1    FULL/DR  00:00:35   2.2.2.1  GigabitEthernet7/1

```

ALU#

ALU# show ip ospf neighbor detail

```

Neighbor 1.1.1.1, interface address 1.1.1.1
  In the area 0 via interface GigabitEthernet7/0
  Neighbor priority is 1, State is FULL, 19 state changes
  DR is 1.1.1.2 BDR is 1.1.1.1
  Options is 0x42
  Dead timer due in 00:00:31
  Neighbor is up for 00:49:28
  retransmission queue length 0, number of retransmissions 1
Neighbor 6.6.6.6, interface address 2.2.2.1
  In the area 1 via interface GigabitEthernet7/1
  Neighbor priority is 1, State is FULL, 10 state changes
  DR is 2.2.2.2 BDR is 2.2.2.1
  Options is 0x42
  Dead timer due in 00:00:35
  Neighbor is up for 00:31:32
  retransmission queue length 0, number of retransmissions 0

```

Ex 7:**ALU# show ip ospf process-interface**

Process-Interface Table:

Process-Id	Interfaces
20	GigabitEthernet7/0, GigabitEthernet3/0

Ex 8:**ALU# show ip ospf interface-process**

Interface-Process Table:

Interface	Attached Process	Waiting Process
GigabitEthernet7/0	20	-
GigabitEthernet7/0	20	-
loopback 9	-	-
loopback1	-	-

Ex 9:**ALU# show ip ospf request-list**

OSPF Router with ID (1.1.1.2) (Process ID 1)

Neighbor 6.6.6.6, interface GigabitEthernet 7/1 address 2.2.2.2

Type	LS ID	ADV RTR	Seq NO	Age
Checksum				
1280	192.175.142.0	1.1.1.1	0x80000003	774 0x9FFB
1280	192.175.206.0	1.1.1.1	0x80000003	774 0xDC7E
1280	192.175.15.0	1.1.1.1	0x80000003	774 0x1A01

ALU#

Ex 10:**ALU# show ip ospf retransmission-list**

```

OSPF Router with ID (1.1.1.2) (Process ID 1)

Neighbor 1.1.1.1, interface GigabitEthernet 7/0 address 1.1.1.2
Link state retransmission due in 4 sec, Queue length 0

Type  LS ID          ADV RTR          Seq NO          Age          Checksum
Neighbor 6.6.6.6, interface GigabitEthernet 7/1 address 2.2.2.2
Link state retransmission due in 0 sec, Queue length 1

Type  LS ID          ADV RTR          Seq NO          Age          Checksum
  3    1.1.1.0        1.1.1.2          0x80000001      2            0x69AA
ALU#

```

Ex 11:**ALU# show ip ospf route**

```

OSPF Router with ID (1.1.1.2) (Process ID 1)

Dest/Mask      Type  Adv-Rtr  Cost  Area/tag  NextHop
2.0.0.0/8      Summ  1.1.1.2  20    0         0.0.0.0
1.1.1.0/24     Ext-2 0.0.0.0  20    0         1.1.1.2
2.0.0.0/8      Summ  1.1.1.2  20    0         0.0.0.0
2.2.2.0/24     Ext-2 0.0.0.0  20    0         2.2.2.2
45.5.5.0/24    Ext-2 0.0.0.0  20    0         0.0.0.0
ALU#

```

Ex 12:**ALU# show ip ospf summary-address**

```

OSPF Process 1, Summary-address

192.175.0.0/255.255.0.0 Metric -1, Type 2, Tag 4 2.0.0.0/
255.0.0.0 Metric 20, Type 2, Tag 0 router-2(config)#

```

Ex 13:

```
ALU# show ip ospf virtual-links
```

```
Virtual Link VLINK to router 6.6.6.6 is up
  Run as demand circuit
  DoNotAge LSA not allowed
  Transit area 1, via interface GigabitEthernet7/1, Cost of
using 1
  Transmit Delay is 1 sec, State POINT-TO-POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Hello due in 00:00:04
  Adjacency state FULL
  Retransmission queue length 2, number of retransmission 0
ALU#
```

CLEAR COMMANDS IN OSPF**To RESTART AN OSPF PROCESS**

To restart an OSPF process, use the following command:

Command (in SUM)	Description
<pre>clear ip ospf [[<1-65535> process redistribution counters [neighbor] [neighbor-id] [interface-name] interface statistics [hello ddp lsupd lsack lsreq][interface-name]]</pre>	<p>Restarts OSPF router if only process ID is specified.</p> <p>For other parameters, it restarts the specified counters/feature.</p>

OSPF CONFIGURATION ON OA-700

EXAMPLE 1

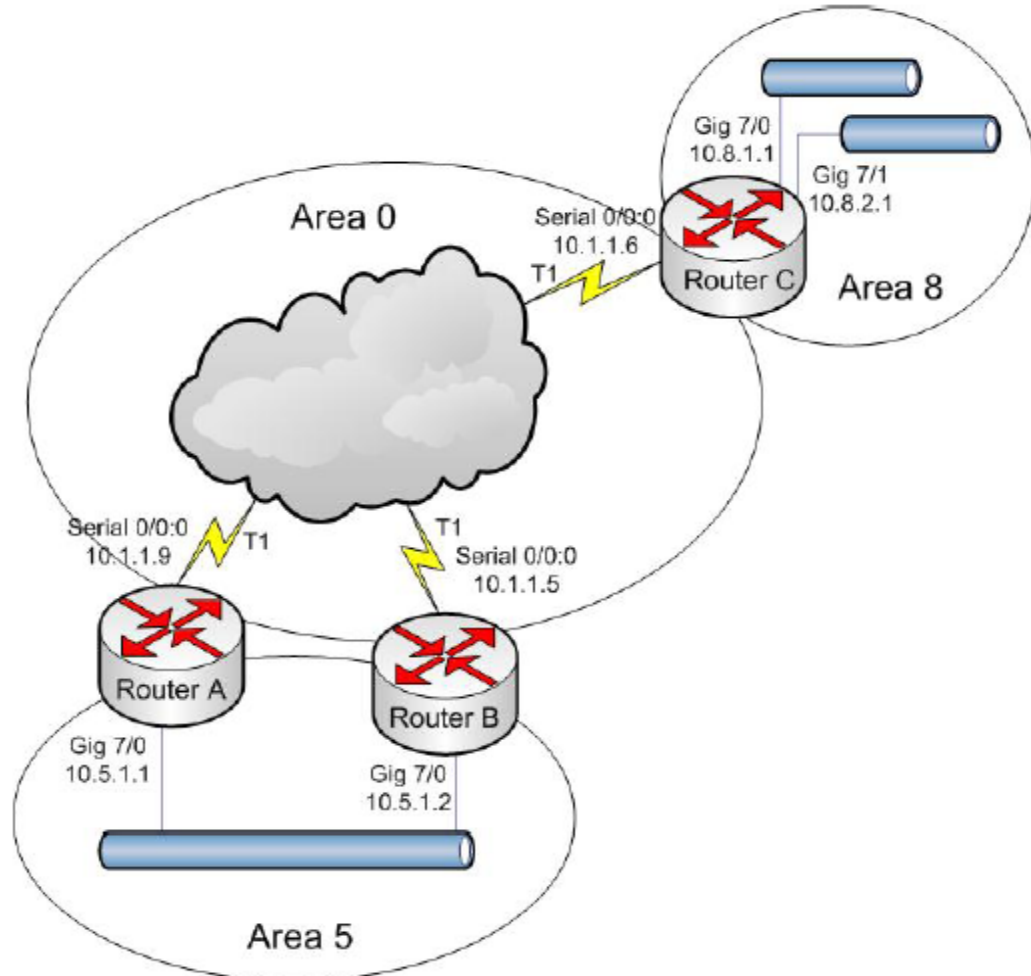


Figure 43: OSPF Configuration Scenario

ROUTER A:

```
hostname RouterA
!
interface Serial0/0:0
 ip address 10.1.1.9/30
 encapsulation ppp
!
interface GigabitEthernet7/0
 ip address 10.5.1.1/24
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0/24 area 0
 network 10.5.0.0/16 area 5
```

ROUTER B:

```
hostname RouterB
!
interface Serial0/0:0
 ip address 10.1.1.5/30
 encapsulation ppp
!
interface GigabitEthernet7/0
 ip address 10.5.1.2/24
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0/24 area 0
 network 10.5.0.0/16 area 5
```

ROUTER C:

```
hostname RouterC
!
interface Serial0/0:0
 ip address 10.1.1.6/30
 encapsulation ppp
!
interface GigabitEthernet7/0
 ip address 10.8.1.1/24
!
interface GigabitEthernet7/1
 ip address 10.8.2.1/24
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0/24 area 0
 network 10.8.0.0/16 area 8
```

CHAPTER 23 MULTICAST ROUTING

This chapter covers the Multicast routing configuration for the OA-700.

The “**Multicast Overview**” section serves as an additional information on the Routing Information Protocol. You can skip this section, and directly go to the configuration section of this chapter.

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
IGMP	Internet Group Multicast Protocol
DR	Designated Router
RIB	Routing Information Base
RP	Rendezvous Point
BSR	Bootstrap Router Mechanism
RPF	Reverse Path Forwarding
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast Sparse Mode
FIB	Forwarding Information Base

MULTICAST OVERVIEW

Multicast is an efficient way to deliver traffic from one sender to many potential receivers.

The varied multicast protocols in use today range from host protocols (IGMP, MLD) to routing protocols (MOSPF, DVMRP, PIM-DM, and PIM-SM/SSM). Earlier versions of multicast routing protocols suffered from limitations and scalability issues of one type or another. For these and other reasons, the PIM-SM/SSM has emerged as the most popular multicast routing protocol for most service providers today. OA-700 supports PIM and IGMP.

The OA-700 software supports the following multicast forwarding features:

- Packet forwarding based on (S, G) entry
- Packet forwarding based on (*, G) entry
- RPF checks for all multicast data traffic
- Acts as DR for directly connected sources
- Acts as DR for directly connected receivers
- Acts as a RP.

PROTOCOL INDEPENDENT MULTICAST (PIM)

PIM-SM is described in RFC 4601.

The PIM sparse mode is optimized for internetworks with many data streams but relatively few LANs. It defines a Rendezvous Point (RP) that is then used as a registration point to facilitate the proper routing of packets. When a sender wants to transmit data, the first-hop router (with respect to the source) node sends data to the RP. When a receiver wants to receive data, the last-hop router (with respect to the receiver) registers with the RP. A data stream then can flow from the sender to the RP and to the receiver. Routers in the path optimize the path and automatically remove any unnecessary hops, even at the rendezvous point.

Protocol Overview

PIM-SM is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a RP per group, and optionally creates shortest-path trees per source.

PIM-SM protocol is for efficiently routing multicast groups that may span wide-area (and inter-domain) internets. This protocol is called Protocol Independent Multicast - Sparse Mode (PIM-SM) because, although it may use the underlying unicast routing to provide reverse-path information for multicast tree building, it is not dependent on any particular unicast routing protocol.

PIM relies on an underlying topology-gathering protocol to populate a routing table with routes. PIM protocol uses multicast/unicast routing table to get RPF neighbor. PIM sends Join/Prune messages to RPF neighbor. Data flows along the reverse path of the Join messages. Thus, in contrast to the unicast RIB, which specifies the next hop that a data packet would take to get to some subnet, the MRIB gives reverse-path information and indicates the path that a multicast data packet would take from its origin subnet to the router that has the MRIB.

A multicast receiver expresses its interest in receiving traffic destined for a multicast group. Typically, it does this using IGMP.

One of the receiver's local routers is elected as the Designated Router (DR) for that subnet. On receiving the receiver's expression of interest, the DR sends a PIM Join message towards the RP for that multicast group. All the receivers DR router sends join message towards RP.

This is known as the RPTree (RPT), and is also known as the shared tree because it is shared by all sources sending to that group. Join messages are resent periodically so long as the receiver remains in the group. When all receivers on a leaf-network leave the group, the DR will send a PIM Prune message towards the RP for that multicast group.

A multicast data sender just starts sending data destined for a multicast group. The sender's local router (DR) takes those data packets, unicast-encapsulates them, and sends them directly to the RP. The RP receives these encapsulated data packets, decapsulates them, and forwards them onto the shared tree. The packets then follow the RPTree, being replicated wherever the RP Tree branches, and eventually reaching all the receivers for that multicast group. The process of encapsulating data packets to the RP is called registering, and the encapsulated packets are known as PIM Register packets.

After receiving packets from source RP sends join message towards source and this forms source specific Shortest Path Tree (SPT). This is to reduce the encapsulation and decapsulation overhead. For many receivers, the route to source via the RP may not be shortest. To obtain lower latencies, router on receiver LAN joins SPT once it receives some packets over RPTree. This is called as switching to SPT from RPT.

INTERNET GROUP MANAGEMENT PROTOCOL (IGMP)

The IGMP version 2 is described in RFC 2236.

IGMP is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers. Multicast routers use IGMP to learn which groups have members on each of their attached physical networks.

Routers periodically (Query Interval) send a General Query on each attached network for which this router is the Querier to solicit the membership information. A General Query is sent to the all-systems multicast group (224.0.0.1)

When a host receives a General Query, it sets delay timers for each group (excluding the all-systems group) of which it is a member on the interface from which it received the query. This delay timer is set to value selected in the range (0, max response time of query).

When a host receives a Group-Specific Query, it sets a delay timer to a random value selected from the range (0, Max Response Time) for the group being queried if it is a member on the interface from which it received the query.

When a group's timer expires, the host multicasts a version 2 Membership Report to the group, with IP TTL of 1. If the host receives another host's Report (version 1 or 2) while it has a timer running, it stops its timer for the specified group and does not send a Report, in order to suppress duplicate Reports.

When a router receives a Report, it adds the group being reported to the list of multicast group memberships on the network on which it received the Report and sets the timer for the membership (Group Membership Interval). Repeated Reports refresh the timer. If no Reports are received for a particular group before this timer has expired, the router assumes that the group has no local members and that it need not forward remotely-originated multicasts for that group onto the attached network.

When host joins multicast group, it transmit IGMPv2 report message. Host sends this report 2-3 times to avoid membership report being lost. IGMPv2 host sends group leave message before leaving group.

When a Querier receives a Leave Group message for a group that has group members on the reception interface, it sends (Last Member Query Count) Group-Specific Queries every (Last Member Query Interval) to the group being left. If no Reports are received after the response time of the last query expires, the routers assume that the group has no local members. IGMPv2 is compatible with IGMPv1 routers.

The OA-700 supports IGMPv2 as default IGMP version. As IGMPv2 is backward compatible, it works well with IGMPv1 host as well.

RFCs

- PIM-SM: Supported RFC 4601
- IGMP: Supported version 2. RFC 2236

PIM CONFIGURATION

This chapter includes the following sections:

- [“PIM Configuration Steps”](#)
- [“PIM Configuration Flow”](#)
- [“PIM Configuration Commands”](#)
- [“Multicast Configuration on OA-700”](#)

PIM CONFIGURATION STEPS

The steps given below helps in configuring PIM routing on the OA-700.

Step 1: Configure an interface. Enter Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet3/0
ALU(config-if GigabitEthernet3/0)#
```



Note: PIM can be configured on Layer 3 interfaces.

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet3/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet3/0)# ip address
20.20.20.20/24
```

Step 4: Enable Multicast routing. See [“To Enable Multicast Routing”](#)

Step 5: Enable PIM on an interface:. See [“To Enable PIM on an Interface”](#)

Step 6: Configure PIM Static RP. See [“To Configure PIM Static RP”](#)

Or

Configure PIM RP candidate using BSR. See [“To Configure PIM RP Candidate”](#)

Step 7: Configure the following PIM optional parameters. See “[PIM Optional Parameters](#)”

- Configure PIM Interface Parameters. See “[To Configure PIM Interface Parameters](#)”
- Configure message interval for PIM. See “[To Configure Message Interval](#)”
- Configure Source-tree Switching Threshold. See “[To Configure Source-tree Switching Threshold](#)”
- Configure PIM as BSR. See “[To Configure PIM as BSR](#)”
- Configure RP candidate priority. See “[To Configure RP Candidate Priority](#)”

Step 8: View PIM configuration. See “[Show Commands in PIM](#)”

PIM CONFIGURATION FLOW

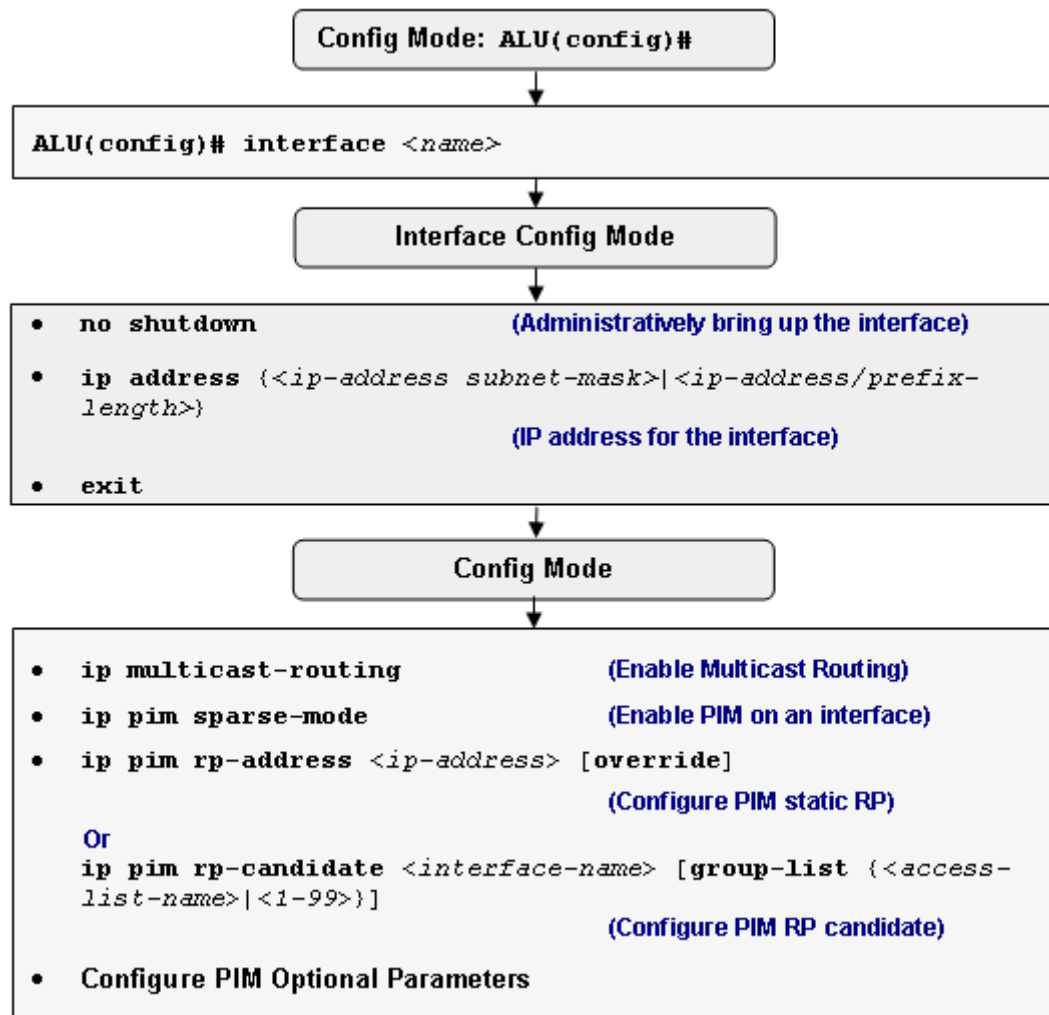


Figure 44: PIM Configuration Flow

PIM CONFIGURATION COMMANDS

To configure PIM, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional, but might be required for your network.

To ENABLE MULTICAST ROUTING

Command (in CM)	Description
<code>ip multicast-routing</code>	This command enables multicast routing and forwarding on OA-700. Multicast routing is disabled by default.

EXAMPLE

```
ALU(config)# ip multicast-routing
```

To ENABLE PIM ON AN INTERFACE

Command (in ICM)	Description
<code>ip pim sparse-mode</code>	Enter this command in the Interface Configuration Mode. This command is used to enable PIM on an interface. After enabling this command, PIM starts sending hello packets to form neighborhood.
<code>no ip pim sparse-mode</code>	This command is used to disable PIM on an interface.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip pim sparse-mode
```

To CONFIGURE RP

RP is the root of shared tree. Data flows from source to RP on SPT, and RP sends data on RPT. Each group can have different RP. There are various ways to learn/configure RP for a group.

OA-700 supports static RP and dynamic RP (learning RP using BSR protocol).

To CONFIGURE PIM STATIC RP

Command (in CM)	Description
<code>ip pim rp-address <ip-address> [override]</code>	This command is used to configure the RP router address for all multicast groups. Override keyword can be used to give preference to static RP over dynamic RP.

EXAMPLE

```
ALU(config)# ip pim rp-address 11.0.0.3
```

To CONFIGURE PIM RP CANDIDATE

Command (in CM)	Description
<code>ip pim rp-candidate <interface-name> [group-list {<access-list-name> <1-99>}]</code>	This command is used to configure the PIM router as RP candidate. RP uses specified interface address. Group list is used to specify access-list, which contains the multicast group for which RP candidate is being configured. BSR selects the RP with the highest priority. If multiple routers are candidate RP for same group and having same priority, then BSR calculates the hash value, and with the highest hash value becomes RP. If more than one RP has the same hash value, the RP with the highest IP address is chosen.

EXAMPLE

```
ALU(config)# ip pim rp-candidate GigabitEthernet3/0 group-list 30
```



Note: All routers in the PIM domain should have same RP address for a multicast group.

PIM OPTIONAL PARAMETERS

TO CONFIGURE PIM INTERFACE PARAMETERS

The DR priority command is used to allow a particular router to win the DR election process by giving a numerically larger DR election priority. The DR priority option should be included in every hello messages, even if no DR priority is explicitly configured on that interface. This is necessary because priority-based DR election is only enabled when all neighbors on an interface advertise that they are capable of using the DR priority option.

Default priority is 1. The router with the highest priority becomes the DR for the subnet. The router with the highest IP address becomes DR if there is a tie in DR priority, the DR priority is not configured, or the DR option is not present. Priority based DR election is only enabled when all neighbors on an interface advertise they are capable of using DR priority option. DR is responsible for sending register packets to RP.

Command (in ICM)	Description
<code>ip pim dr-priority <0-4294967294></code>	Specifies PIM router DR priority on an interface. This DR priority is used in the DR election algorithm. Default DR-priority is 1.
<code>ip pim query-interval <0-65535></code>	PIM router sends periodic hello messages on all PIM enabled interfaces. Use this command to configure this interval (in seconds). The default query-interval is 30 seconds.
<code>ip pim neighbor-filter {<1-99> <standard access-list-name>}</code>	Enter this command in the Interface Configuration Mode. This command is used to prevent PIM router from forming neighborhood with other router. Using access-list, you can specify permitted neighbors. By default, PIM router forms neighborhood with all the routers on an interface.
<code>show ip pim rp-hash <group-address></code>	This command is used to see group to RP mapping. If RP information for the given group does not exist then command gives error else output shows the RP information for the given group.

EXAMPLE

```

ALU(config-if GigabitEthernet3/0)# ip pim dr-priority 2

ALU(config-if GigabitEthernet3/0)# ip pim query-interval 50

ALU(config-if Serial0/0:0)# ip pim neighbor-filter acc-list1

```

To CONFIGURE MESSAGE INTERVAL

PIM router sends Join/Prune messages towards source or RP. This message is periodic to keep the states in upstream router active.

Command (in CM)	Description
<code>ip pim message-interval <1-65535></code>	PIM router sends periodic join and prune messages on interfaces over which it has at least one neighbor. Use this command to configure this interval (in seconds). The default message-interval is 60 seconds.

EXAMPLE

```
ALU(config)# ip pim message-interval 30
```

To CONFIGURE SOURCE-TREE SWITCHING THRESHOLD

PIM router joins SPT once the configured policy is satisfied. This command is used to configure the policy to control switching traffic from shared Tree (RPT) to Shortest Path Tree (SPT).

Command (in CM)	Description
<code>ip pim spt-threshold {<0-4294967>/infinity} [group-list {<1-99> <1300-1999> <standard access-list-name>}]</code>	This command is used to configure the the SPT threshold value. The value can be specified in the range 0-4294967 or infinity, which means never to switch-over from RPT to SPT. In case, the access-list is specified, this threshold value is used only for the groups, which matches the access-list. The default spt-threshold is 0 Kbps.

EXAMPLE

```
ALU(config)# ip pim spt-threshold 100 group-list 10
```

To CONFIGURE PIM AS BSR

Command (in CM)	Description
ip pim bsr-candidate <interface-name> [<0-30>] [<0-255>]	This command is used to configure the PIM router as BSR candidate. BSR uses specified interface address. 0-30: Indicates the hash length. This value is used to select one RP. 0-255: Indicates the priority of the BSR router.

EXAMPLE

```
ALU(config)# ip pim bsr-candidate GigabitEthernet3/0 1 10
```

To CONFIGURE RP CANDIDATE PRIORITY

Command (in CM)	Description
ip pim rp-candidate-priority <0-255>	This command is used to configure the priority of the RP candidate.

EXAMPLE

```
ALU(config)# ip pim rp-candidate-priority 10
```

SHOW COMMANDS IN PIM

TO VIEW PIM INTERFACE INFORMATION

Command (in SUM/CM)	Description
show ip pim interface [<interface-name>]	This command shows the interfaces on which PIM is enabled, and details like interface DR priority and current DR on the interface is displayed.

EXAMPLE

```
ALU# show ip pim interface
```

```
Address          Interface          Ver/ Nbr   Query DR      DR
Mode Count Intvl Prior
3.3.3.4          GigabitEthernet3/0 v2/S 0      30    1      3.3.3.4
4.4.4.4          GigabitEthernet3/1 v2/S 0      30    1      4.4.4.4
8.8.8.7          Serial0/0:0        v2/S 1      30    1      8.8.8.8
6.6.6.6          Serial0/1:0        v2/S 1      30    1      6.6.6.7
ALU#
```

```
ALU# show ip pim interface GigabitEthernet 3/0
```

```
Address          Interface          Ver/ Nbr   Query DR      DR
Mode Count Intvl Prior
3.3.3.4          GigabitEthernet3/0 v2/S 0      30    1      3.3.3.4
ALU#
```

TO VIEW PIM NEIGHBOR INFORMATION

Command (in SUM/CM)	Description
show ip pim neighbor [<interface-name>]	This command displays PIM neighbors on all interfaces. To see neighbors on a specific interface, use the interface name.

EXAMPLE

```
ALU#show ip pim neighbor
```

```
PIM Neighbor Table
Neighbor  Interface    Uptime/Expires    Ver  DR Address  Prio/Mode
8.8.8.8   Serial0/0:0  00:09:37/00:01:39 v2   1/ DR
6.6.6.7   Serial0/1:0  00:09:45/00:01:33 v2   1/ DR
ALU#
```

ALU# show ip pim neighbor Serial 0/0:0

```
PIM Neighbor Table
Neighbor   Interface   Uptime/Expires   Ver   DRAddress   Prio/Mode
8.8.8.8    Serial0/0:0 00:09:43/00:01:33 v2    1/ DR
ALU#
```

To VIEW RP INFORMATION

Command (in SUM/CM)	Description
show ip pim rp-hash [<group-address>]	This command is used to see group-to-RP mapping
show ip pim rp [mapping][<group-address>]	This command displays the group-to-RP mapping table of PIM.

EXAMPLE

```
ALU(config)# show ip pim rp-hash 227.0.0.1
RP 1.1.1.1(?)Priority - 0 Holdtime - 150, v2
Info source:1.1.1.1(?), via bootstrap
Uptime: 00:00:32, expires 00:01:58
ALU(config)#
```

ALU(config)# show ip pim rp mapping

```
PIM Group-to-RP Mappings
Group(s) 225.0.0.0/8
RP 1.1.1.1 (?) v2
Info source: 1.1.1.1 (?), via bootstrap, priority 0, holdtime = 53760
Uptime: 00:00:45, expires 14:55:15
Group(s) 228.0.0.0/8
RP 2.2.2.1 (?) v2
Info source: 2.2.2.1 (?), via bootstrap, priority 0, holdtime = 38400
Uptime: 00:03:55, expires 10:39:05
ALU(config)#
```


To VIEW BSR INFORMATION

Command (in SUM/CM)	Description
<code>show ip pim bsr-router</code>	This command displays the BSR information.

EXAMPLE

```
ALU(config)# show ip pim bsr-router
```

```
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR Address: 1.1.1.2 (?)
Uptime:      00:04:24, BSR Priority: 0, Hash Mask Length: 30
Next Bootstrap Message in 00:00:46 seconds
```

```
Candidate RP: 2.2.2.1 (GigabitEthernet7/0), Group Acl: test
Next Cand_RP_Advertisement in 00:00:35 seconds
```

```
ALU(config)#
```

To VIEW SG STATE INFORMATION

Command (in SUM/CM)	Description
<code>show ip pim state-info</code> [<i><group-address></i>] [<i><source-address></i>] [<i>summary</i>]	This command displays the PIM upstream (towards RP/Source) and downstream (towards Receivers) state information.

EXAMPLE

```
ALU# show ip pim state-info
```

```
PIMv2 State information
Flags: M - Nexthop from Mroute, T - Terminating
       K - KeepAlive Timer Running, S - SPT bit set

(*,224.1.1.1), JOINED 00:00:55/00:00:05, RP 5.5.5.5, flags:
  Incoming interface: GigabitEthernet3/1, RPF neighbor 5.5.5.5
  Downstream interface state:
    GigabitEthernet3/0, 00:00:55, flags:A
  inherited_olist: GigabitEthernet3/0
```

CLEAR COMMANDS IN PIM

To CLEAR SG STATE INFORMATION

Command (in SUM/CM)	Description
<code>clear ip pim state-info [<group-address>] [<source-address>]</code>	This command clears the PIM SG State information.

EXAMPLE

```
ALU# clear ip pim state-info
```

To CLEAR NEIGHBOR INFORMATION

Command (in SUM/CM)	Description
<code>clear ip pim neighbor {* <interface-name> {[neighbor-address] *}}</code>	This command clears the neighbor information on an interface.

EXAMPLE

```
ALU# clear ip pim neighbor GigabitEthernet 3/0 1.1.1.1
```

To CLEAR IP PIM RP MAPPING

Command (in SUM/CM)	Description
<code>clear ip pim rp-mapping [<rp-address>]</code>	This command clears the mulitcast group addresses mapped to the RP.

EXAMPLE

```
ALU# clear ip pim rp-mapping
```

To CLEAR IP PIM BSR

Command (in SUM/CM)	Description
<code>clear ip pim bsr [<bsr-address>]</code>	This command clears the BSR address.

EXAMPLE

```
ALU# clear ip pim bsr
```

IGMP CONFIGURATION

This chapter includes the following sections:

- [“IGMP Configuration Steps”](#)
- [“IGMP Configuration Flow”](#)
- [“IGMP Configuration Commands”](#)
- [“Multicast Configuration on OA-700”](#)

IGMP CONFIGURATION STEPS

The steps given below helps in configuring IGMP routing on the OA-700.

Step 1: Configure an interface. Enter Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet3/0
ALU(config-if GigabitEthernet3/0)#
```



Note: IGMP can be configured on Layer 3 interfaces.

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet3/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet3/0)# ip address
20.20.20.20/24
```

Step 4: Enable Multicast routing. See [“To Enable Multicast Routing”](#)

Step 5: Enable IGMP on an interface:. See [“To Enable IGMP on an Interface”](#)

Step 6: Configure the following IGMP Interface optional parameters. See “IGMP Interface Optional Parameters”

- Configure last member query count. See “[To Configure IGMP Last Member Query Count](#)”
- Configure last member query interval. See “[To Configure IGMP Last Member Query Interval](#)”
- Configure querier time-out. See “[To Configure IGMP Querier Time-out](#)”
- Configure query interval. See “[To Configure IGMP Query Interval](#)”
- Configure query max response time. See “[To Configure IGMP Query Max Response Time](#)”
- Configure IGMP join-group. See “[To Join Multicast Group](#)”
- Configure IGMP access group. See “[To Configure IGMP Access Group](#)”

Step 7: View IGMP configuration. See “[Show Commands in IGMP](#)”

Step 8: View Multicast configuration. See “[Show Commands in Multicast](#)”

IGMP CONFIGURATION FLOW

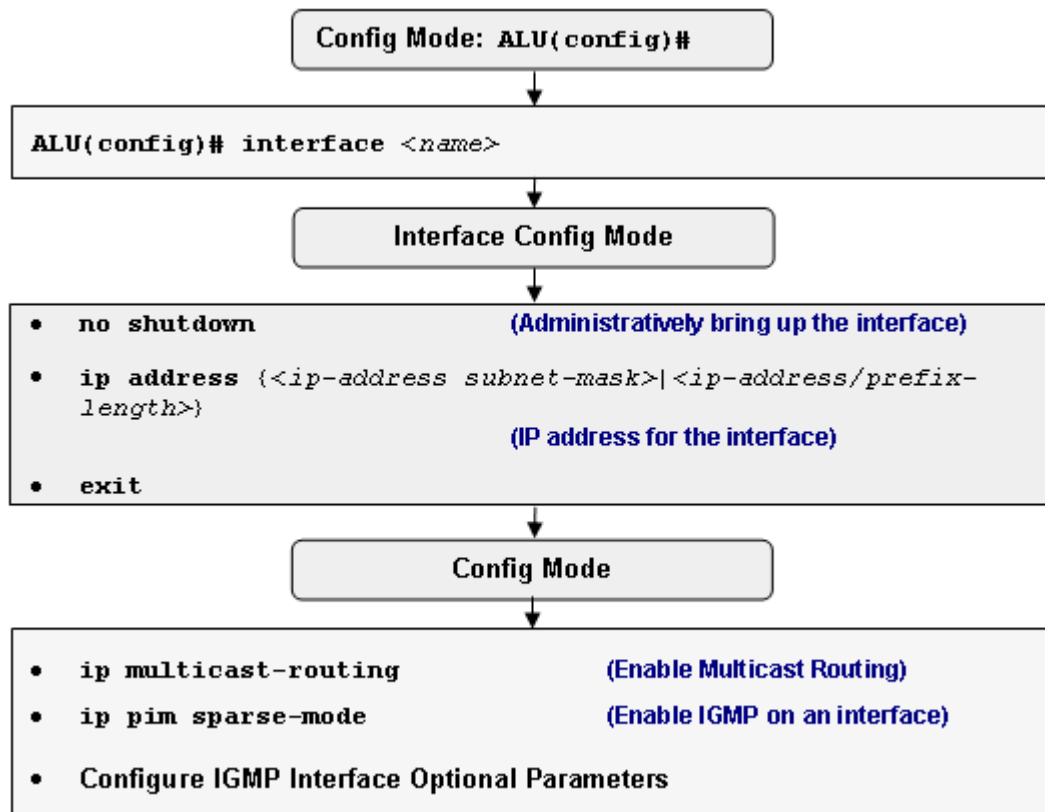


Figure 45: IGMP Configuration Flow

IGMP CONFIGURATION COMMANDS

To configure IGMP, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional, but might be required for your network.

To ENABLE MULTICAST ROUTING

Command (in CM)	Description
<code>ip multicast-routing</code>	This command enables multicast routing and forwarding on OA-700. Multicast routing is disabled by default.

EXAMPLE

```
ALU(config)# ip multicast-routing
```

To ENABLE IGMP ON AN INTERFACE

Command (in ICM)	Description
<code>ip pim sparse-mode</code>	Enter this command in the Interface Configuration Mode. This command is used to enable IGMP on an interface. After enabling this command, IGMP learns the multicast host information on given interface.
<code>no ip pim sparse-mode</code>	This command is used to disable IGMP on an interface.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip pim sparse-mode
```

IGMP INTERFACE OPTIONAL PARAMETERS

To specify the interface parameters, enter the following commands in the Interface Configuration Mode:

To CONFIGURE IGMP LAST MEMBER QUERY COUNT

When a router receives an IGMP version 2 leave group message, router sends last-member-query-count group-specific IGMP query messages at intervals of igmp-last-member-interval milliseconds.

Command (in ICM)	Description
<code>ip igmp last-member-query-count <1-7></code>	Use this command to configure the number of retransmission of group-specific queries. The default last-member-query-count is 2.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip igmp last-member-query-count 3
```

To CONFIGURE IGMP LAST MEMBER QUERY INTERVAL

When a multicast host leaves a group, the host sends an IGMP leave group message. To check if this host is the last to leave the group, IGMP router sends an IGMP group specific query message. If no reports are received before the configured last member query interval, routers assumes that no receiver is interested in this group.

Command (in ICM)	Description
<code>ip igmp last-member-query-interval <100-65535></code>	Use this command to configure the last-member query interval (in milliseconds) for the IGMP. The default last-member-query-interval is 1000 milliseconds.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip igmp last-member-query-interval 2000
```

To CONFIGURE IGMP QUERIER TIME-OUT

IGMP enabled router may assume one of two roles Querier or Non-Querier on an interface. There is normally only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a Query message from a router with a lower IP address, it become a Non-Querier on that network. If a router has not heard a Query message from another router for Querier time-out, it resumes the role of Querier. Routers periodically send a General Query on each attached network for which this router is the Querier.

Command (in ICM)	Description
<code>ip igmp querier-timeout <60-300></code>	This command configures the time-out value (in seconds) after which the router assumes itself to be the querier on the interface. Default IGMP querier-timeout is 305.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip igmp querier-timeout 100
```



Note: Make sure that all IGMP routers on LAN have same querier time-out. Else, router with less querier time-out will always become querier.

To CONFIGURE IGMP QUERY INTERVAL

Command (in ICM)	Description
<code>ip igmp query-interval <1-65535></code>	This command is used to configure the interval (in seconds) at which the IGMP router sends query messages on an interface. The default query-interval is 125 seconds.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip igmp query-interval 100
```


TO CONFIGURE IGMP QUERY MAX RESPONSE TIME

Command (in ICM)	Description
<code>ip igmp query-max-response-time <1-25></code>	This command configures the maximum response time (in seconds) advertised in IGMP queries. The default query-max-response-time is 10 seconds.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip igmp query-max-response-time 20
```

TO JOIN MULTICAST GROUP

Router can join a group by using this command. This helps in keeping PIM states always active even if no host is interested in the group. This command also helps in debugging multicast routing.

Command (in ICM)	Description
<code>ip igmp join-group <group-address></code>	This command is used to join specified multicast group.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip igmp join-group 226.2.2.2
```

TO CONFIGURE IGMP ACCESS GROUP

Command (in ICM)	Description
<code>ip igmp access-group {<1-99> <access-list-name>}</code>	This command is used to deny groups, which are not permitted by access-lists. This restricts the host on a subnet joining only multicast groups that are permitted by access-lists.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip igmp access-group 10
```

SHOW COMMANDS IN IGMP

TO VIEW IGMP GROUP INTERFACE INFORMATION

Command (in SUM/CM)	Description
<code>show ip igmp groups</code> [<i><group-address></i>] [<i><interface-name></i>]	This command displays all the multicast groups joined. You can enter the interface name to see multicast groups on that interface.

EXAMPLE

```
ALU# show ip igmp groups
```

```
Interface          Group-Address Last-Reporter Uptime Expires(sec:msec)
GigabitEthernet3/0 224.1.1.1      3.3.3.4       0:0:51 217:89
GigabitEthernet3/1 224.0.1.40     5.5.5.5       4:12:42 147:509
GigabitEthernet3/1 225.5.5.5     5.5.5.5       0:0:7 252:620
```

TO VIEW IGMP INTERFACE INFORMATION

Command (in SUM/CM)	Description
<code>show ip igmp interface</code> [<i><interface-name></i>]	This command displays all interfaces on which the IGMP is enabled, and displays configured/default values of the IGMP interface parameters.

EXAMPLE

```
ALU# show ip igmp interface
```

```
GigabitEthernet3/0 Internet address 7.7.7.3 Mask 255.255.255.0
Host version 2 Router Version 2
Query Interval = 125
Querier Timeout = 255
Max query response time = 10
Last member query count = 2
Last member query response time = 1000
Access Group set = 0
Number of joins on this interface = 84
Number of leave message on this interface = 7
Querier on this interface = 7.7.7.3
Interface DR is 7.7.7.3
Total groups on this interface 1
Group 1 224.1.1.1
```

SHOW COMMANDS IN MULTICAST

TO VIEW FORWARDING INFORMATION BASE (FIB) INFORMATION

Command (in SUM/CM)	Description
<code>show ip mroute [<group-address>] [<interface-name>]</code>	This command displays the multicast routing table.

EXAMPLE

```
ALU# show ip mroute
```

```
IP Multicast Forwarding Information Base
```

```
Flags: T - SPT-bit set
```

```
(*, 224.1.1.1), uptime 0:10:21, flags:
```

```
Rates: Waiting for latest...
```

```
Incoming Interface: GigabitEthernet3/1, RPF failures 0
```

```
Outgoing Interfaces (1):
```

```
GigabitEthernet7/0
```

```
(4.4.4.4, 224.1.1.1), uptime 0:30:20, expired, flags:
```

```
Rates: Waiting for latest...
```

```
Incoming Interface: Serial0/0:0, RPF failures 0
```

```
Outgoing Interfaces (1):
```

```
GigabitEthernet3/0
```

```
(*, 225.5.5.5), uptime 0:09:37, flags:
```

```
Rates: Waiting for latest...
```

```
Incoming Interface: GigabitEthernet3/1, RPF failures 0
```

```
Outgoing Interfaces (0):
```

TO VIEW IP MULTICAST TRAFFIC STATISTICS

Command (in SUM/CM)	Description
<code>show ip multicast traffic</code>	This command displays the statistics of the multicast packets.

EXAMPLE

```
ALU# show ip multicast traffic
```

```
IP Multicast statistics:
```

```
Rcvd: 4449 total, 838 link local
```

```
Sent: 3334 forwarded, 0 send register
```

```
0 send assert, 3 first data pkt notice
```

```
Errors: 1 rpf failure, 1 drop
```

CLEAR COMMANDS IN MULTICAST

TO CLEAR MULTICAST ROUTING INFORMATION

Command (in SUM/CM)	Description
<code>clear ip mroute</code>	This command clears multicast routing information.

EXAMPLE

```
ALU# clear ip mroute
```

TO CLEAR MULTICAST TRAFFIC

Command (in SUM/CM)	Description
<code>clear ip multicast traffic</code>	This command resets the multicast traffic counters.

EXAMPLE

```
ALU# clear ip multicast traffic
```

MULTICAST CONFIGURATION ON OA-700

EXAMPLE 1

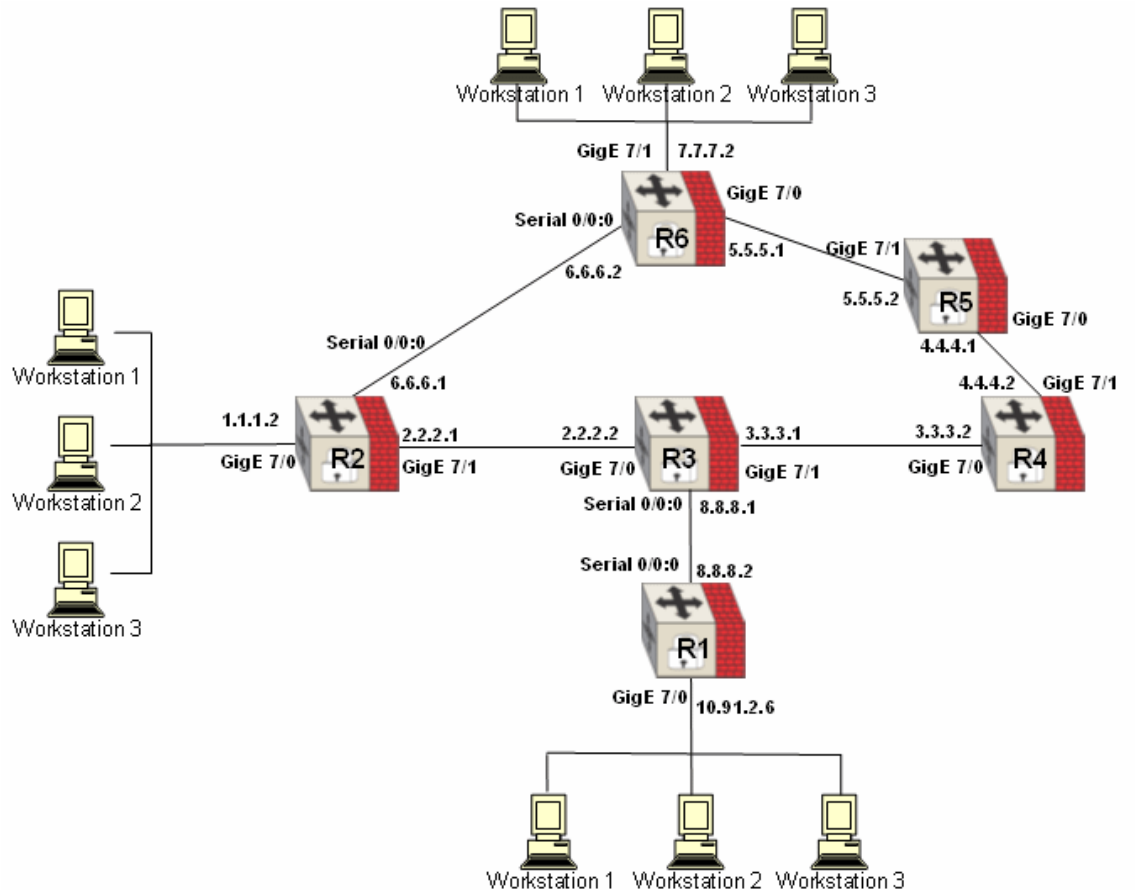


Figure 46: Multicast Configuration Scenario

In the above scenario, multicast receivers connected to router R2 is joined to multicast group 227.7.7.7, and receivers connected to Router R1 are joined to multicast groups 225.5.5.5 and 227.7.7.7.

Router R4 is configured as RP for all the multicast groups. All the routers have static RP configuration with RP address as 3.3.3.2.

OSPF routing is used in this topology to make sure that all routers are reachable.

Multicast sender for group 225.5.5.5 and 227.7.7.7 is connected to router R6.

In the given scenario, you can see the multicast routing table entries on routers to verify multicast routing. Show command outputs on router R3 is given.

ROUTER 1 CONFIGURATION

```
ip multicast-routing

interface GigabitEthernet7/0
 ip address 10.91.2.6/24
 ip pim sparse-mode

interface Serial0/0:0
 ip address 8.8.8.2/24
 encapsulation hdlc
 ip pim sparse-mode

router ospf 1
 log-adjacency-changes
 network 8.0.0.0/8 area 0
 network 10.91.0.0/16 area 0

ip pim rp-address 3.3.3.2
```

ROUTER 2 CONFIGURATION

```
ip multicast-routing

interface GigabitEthernet7/0
 ip address 1.1.1.2 255.255.255.0
 ip pim sparse-mode

interface Serial0/0:0
 ip address 6.6.6.1 255.255.255.0
 ip pim sparse-mode

interface GigabitEthernet7/1
 ip address 2.2.2.1 255.255.255.0
 ip pim sparse-mode

router ospf 1
 log-adjacency-changes
 network 1.0.0.0/8 area 0
 network 2.0.0.0/8 area 0
 network 6.0.0.0/8 area 0
!
ip pim rp-address 3.3.3.2

ip pim spt-threshold infinity
```

ROUTER 3 CONFIGURATION

```
ip multicast-routing

interface GigabitEthernet7/0
 ip address 2.2.2.2/24
 ip pim sparse-mode
!
interface GigabitEthernet7/1
 ip address 3.3.3.1/24
 ip pim sparse-mode
!
interface Serial0/0:0
 ip address 8.8.8.1/24
 encapsulation hdlc
 ip pim sparse-mode

router ospf 1
 log-adjacency-changes
 network 2.0.0.0/8 area 0
 network 3.0.0.0/8 area 0
 network 8.0.0.0/8 area 0
!
!
ip pim rp-address 3.3.3.2
```

ROUTER 4 CONFIGURATION

```
ip multicast-routing

interface GigabitEthernet7/0
 ip address 3.3.3.2 255.255.255.0
 ip pim sparse-mode

interface GigabitEthernet7/1
 ip address 4.4.4.2 255.255.255.0
 ip pim sparse-mode

router ospf 1
 log-adjacency-changes
 network 3.0.0.0/8 area 0
 network 4.0.0.0/8 area 0

ip pim rp-address 3.3.3.2
```

ROUTER 5 CONFIGURATION

```
ip multicast-routing

interface GigabitEthernet7/0
 ip address 4.4.4.1/24
 ip pim sparse-mode

interface GigabitEthernet7/1
 ip address 5.5.5.2/24
 ip pim sparse-mode

router ospf 1
 log-adjacency-changes
 network 4.0.0.0/8 area 0
 network 5.0.0.0/8 area 0

ip pim rp-address 3.3.3.2
```

ROUTER 6 CONFIGURATION

```
ip multicast-routing

interface Loopback0
 ip address 99.99.99.1 255.255.255.0

interface GigabitEthernet7/0
 ip address 5.5.5.1 255.255.255.0
 ip pim sparse-mode

interface Serial0/0:0
 ip address 6.6.6.2 255.255.255.0
 ip pim sparse-mode

interface GigabitEthernet7/1
 ip address 7.7.7.2 255.255.255.0
 ip pim sparse-mode

router ospf 1
 network 5.0.0.0/8 area 0
 network 6.0.0.0/8 area 0
 network 7.0.0.0/8 area 0

ip pim rp-address 3.3.3.2
```


VERIFYING MULTICAST ROUTING

Show command outputs on router R3 is given. It shows the outgoing interface list for each (*,G) entry. You can use "show ip multicast traffic" command to verify the packet reception and forwarding.

```
R3(config)# show ip pim state-info
```

```
PIMv2 State information
Flags: M - Nexthop from Mroute, T - Terminating, A - Reported by IGMP
      K - KeepAlive Timer Running, S - SPT bit set

(*,225.5.5.5), JOINED 00:01:10/00:00:49, RP 3.3.3.2, flags:
  Incoming interface: GigabitEthernet7/1, RPF neighbor 3.3.3.2
  Downstream interface state:
    Serial0/0:0, 00:01:10, flags:
      (*,G): JOIN ET:00:03:20 PPT:00:00:00
    inherited_olist: Serial0/0:0

(*,227.7.7.7), JOINED 00:09:26/00:00:34, RP 3.3.3.2, flags:
  Incoming interface: GigabitEthernet7/1, RPF neighbor 3.3.3.2
  Downstream interface state:
    GigabitEthernet7/0, 00:09:26, flags:
      (*,G): JOIN ET:00:03:02 PPT:00:00:00
    Serial0/0:0, 00:00:16, flags:
      (*,G): JOIN ET:00:03:14 PPT:00:00:00
    inherited_olist: GigabitEthernet7/0 Serial0/0:0
R3(config)#
```

```
R3(config)# show ip mroute
```

```
IP Multicast Forwarding Information Base
Flags: R - RP-bit set, T - SPT-bit set
      F - Register flag, J - Joined

(*, 225.5.5.5), uptime 0:01:59, flags:
  Incoming Interface: GigabitEthernet7/1, RPF failures 0
  Outgoing Interfaces (1):
    Serial0/0:0

(*, 227.7.7.7), uptime 0:10:15, flags:
  Incoming Interface: GigabitEthernet7/1, RPF failures 0
  Outgoing Interfaces (2):
    GigabitEthernet7/0
    Serial0/0:0
R3(config)#
```

```
R3(config)# show ip multicast traffic
```

```
IP Multicast statistics:
  Rcvd: 11134 total, 4802 link local
  Sent: 5973 forwarded, 0 send register
       5 send assert, 1 first data pkt notice
  Errors: 5 rpf failure, 5 drop
R3(config)#
```

R3(config)# show ip pim neighbor

PIM Neighbor Table

Neighbor	Interface	Uptime/Expires	Ver	DR Address	Prio/Mode
2.2.2.1	GigabitEthernet7/0	02:59:10/00:01:33	v2	1/ Not DR	
3.3.3.2	GigabitEthernet7/1	02:58:43/00:01:30	v2	1/ DR	
8.8.8.2	Serial0/0:0	00:02:36/00:01:44	v2	1/ DR	

R3(config)#

R3(config)# show ip pim interface

Address	Interface	Ver/ Mode	Nbr Count	Query Intvl	DR Prior	DR
2.2.2.2	GigabitEthernet7/0	v2/S	1	30	1	2.2.2.2
3.3.3.1	GigabitEthernet7/1	v2/S	1	30	1	3.3.3.2
8.8.8.1	Serial0/0:0	v2/S	1	30	1	8.8.8.2

R3(config)#

CHAPTER 24 POLICY BASED ROUTING

This chapter covers the Policy Based Routing (PBR) configuration for the OA-700.

The “[PBR Overview](#)” section serves as an additional information on the PBR. You can skip this section, and directly go to the configuration section of this chapter.

CHAPTER CONVENTIONS

Acronym	Description
PBR	Policy Based Routing
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
IP Policy-CM	IP Policy Sub Configuration Mode - ALU (config-ip-policy-name)#
SUM	Super User Mode - ALU #

PBR OVERVIEW

Branch offices need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional forwarding and routing algorithms. PBR is useful in deployments, where administrative issues dictate that traffic be routed through specific paths. By using PBR, customers can implement policies that selectively cause packets to take different paths.

PBR provides the ability to route traffic based on attributes other than the destination IP address. Attributes like source IP address, protocol type can be used to define policies and apply them to an interface.

ALCATEL-LUCENT SPECIFIC OVERVIEW

- OA-700 supports PBR that allows routing of packets based on policies (match-lists) to a specified egress interface/next hop.
- OA-700 shall support PBR as an infrastructure for other software components to add system PBR rules. This shall enable the applications to treat certain traffic in a special way.

PBR CONFIGURATION

This chapter includes the following sections:

- [“PBR Configuration Steps”](#)
- [“PBR Configuration Flow”](#)
- [“PBR Configuration Commands”](#)

PBR CONFIGURATION STEPS

This section lists the steps for configuring policy based routing on OA-700.

Step 1: Configure the **match-lists** using the common classifiers syntax. (Refer to the chapter on [“Common Classifiers”](#) in this guide).

Step 2: Configure an IP policy. See [“To Configure an IP Policy”](#)

- Configure a Rule inside an IP policy. See [“To Configure a Rule for an IP Policy”](#)

Attach an IP Policy to an Interface

Step 3: Enter into Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet3/0
ALU(config-if GigabitEthernet3/0)#
```



Note: IP policy can be configured on any interface.

Step 4: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet3/0)# no shutdown
```

Step 5: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet3/0)# ip address
20.20.20.20/24
```

Step 6: Attach the configured IP policy to an appropriate interface. See [“To Attach / Detach an IP Policy to an Interface”](#)



Note: An interface can have only one IP policy applied on it at any time.

Step 7: Use the show commands to view PBR configuration. See [“Show Commands in PBR”](#)

PBR CONFIGURATION FLOW

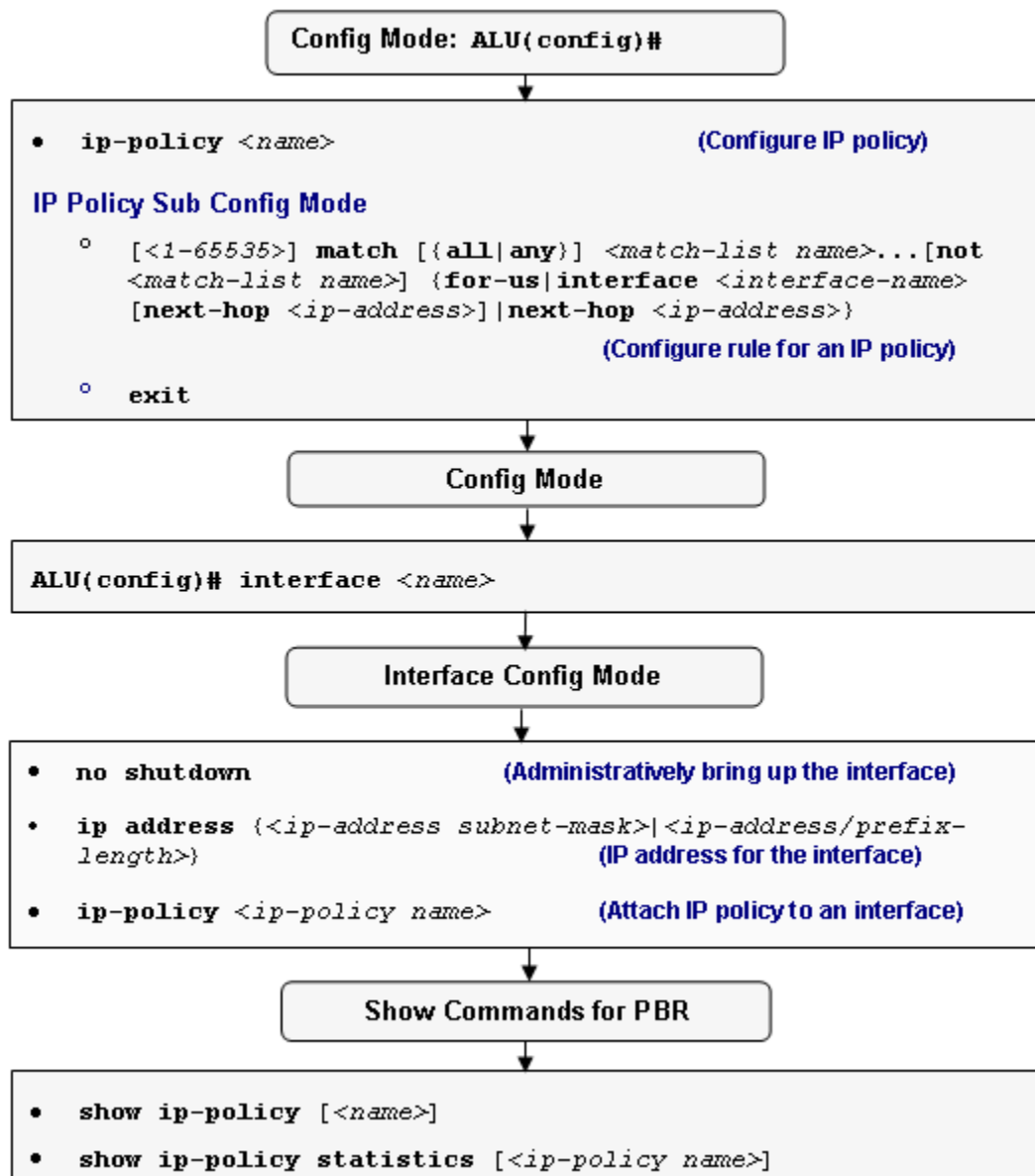


Figure 47: PBR Configuration Flow

PBR CONFIGURATION COMMANDS

The following steps are used to configure a PBR on the OA-700.

TO CONFIGURE AN IP POLICY

Command (in CM)	Description
<code>ip-policy <name></code>	This command is used to create an IP policy.
<code>no ip-policy <name> [force]</code>	This command is used to delete an IP policy. If the policy is attached to any of the interfaces, it cannot be deleted. The " force " keyword will automatically detach the specified policy from respective interfaces, and deletes the IP policy. This command when used also deletes all the rules configured under this policy.

EXAMPLE

```
ALU(config)# ip-policy pbr1
ALU(config-ip-policy-pbr1)#

ALU(config)# no ip-policy pbr1
```

TO CONFIGURE A RULE FOR AN IP POLICY

This command specifies the match conditions and forwarding action.

- Rule can have multiple match-lists along with the option of any/all.
- Rule can also have one match-list with NOT option. Match-list with NOT option can only be specified as the last match-list and only one match-list can have NOT option.
- The interface-name and/or next-hop shall specify the egress path of the packet.
- The 'for-us' keyword redirects the packet to the management plane of the OA-700.
- Only one of next-hop and/or interface or for-us shall be in effect at any time.
- If the interface and next-hop are specified together, then the packet shall be forwarded to the specified next-hop on the specified interface.



Note: When the interface option is chosen as Ethernet/VLAN, it is mandatory to specify the next hop.

- The range for the rule is 1-65535. This rule number signifies the priority of a rule.


Command (in IP Policy CM)	Description
<pre>[<1-65535>] match [{all any}] <match-list name>...[not <match-list name>] {for- us interface <interface-name> [next-hop <ip-address>] next- hop <ip-address>}</pre>	<p>This command is used to configure rules (associate match-lists and set priority for the rule) for an IP policy.</p> <p>The range for the rule number is 1-65535. This rule number signifies the priority of a rule. By default, the numbering pattern for rule number is the next multiple of ten to the highest existing rule number.</p>
<pre>no rule <1-65535></pre>	<p>The command deletes a rule corresponding to the rule number.</p>

EXAMPLE

```
ALU(config-ip-policy-pbr1)# 10 match m1 m2 not m3 interface
GigabitEthernet 3/0 next-hop 1.2.2.1
```

```
ALU(config-ip-policy-pbr1)# 20 match m1 m2 next-hop 1.2.2.2
```

To ATTACH / DETACH AN IP POLICY TO AN INTERFACE

Command (in ICM)	Description
<code>ip-policy <ip-policy name></code>	<p>This command is used to attach an IP policy to an interface.</p>  <p>Note: An interface can have only one IP policy applied on it at any time.</p> <p>‘Transparent-forwarding’ command, if in effect, shall be cleaned up before this command takes effect.</p>
<code>no ip-policy <ip-policy name></code>	This command detaches the IP policy attached to an interface.

EXAMPLE

The following example binds the IP policy ‘pbr1’ to interface GigabitEthernet3/1:

```
ALU(config)# interface GigabitEthernet3/1
ALU(config-if GigabitEthernet3/1)# ip-policy pbr1
```

If the IP policy pbr1 is attached to the GigabitEthernet3/1, the following command detaches it from the interface:

```
ALU(config)# interface GigabitEthernet3/1
ALU(config-if GigabitEthernet3/1)# no ip-policy pbr1
```

SHOW COMMANDS IN PBR

TO VIEW IP POLICY DETAILS

Command (in SUM/CM)	Description
show ip-policy [<i><name></i>]	This command is used to view all the IP policies configured in the system. This command is also used to view the details of a specific IP policy. This command also displays interfaces on which these policies are applied.

EXAMPLE

```
ALU(config)# show ip-policy
!
! IP-Policy configuration
!
ip-policy pbr1
    10 match any m1 m2 interface GigabitEthernet3/0 next-hop
1.2.2.1
exit
!
interface GigabitEthernet3/1
    ip-policy pbr1
exit
```

TO VIEW IP POLICY STATISTICS

Command (in SUM/CM)	Description
show ip-policy statistics [<i><ip-policy name></i>]	This command is used to display the statistics of all the IP policies configured in the system. If a policy-name is specified, then the statistics for the specified IP policy are displayed. This displays the number of packets that hit the rules in the IP policy, and number of packets dropped.

EXAMPLE

```
ALU(config)# show ip-policy statistics
PBR - Policy Based Routed, Drop - Dropped

0 packets forwarded by best effort IP forwarding

ip-policy pbr1 : PBR - 0 Drop - 0
    0 hits on : 1 match any m1 next-hop 1.1.1.1
```

CLEAR COMMANDS

To CLEAR IP POLICY STATISTICS

Command (in SUM/CM)	Description
<code>clear ip-policy statistics [<ip-policy name>]</code>	This command clears the statistics of all the IP policies configured in the system. If a policy-name is specified, then the statistics for the specified IP policy are cleared.

EXAMPLE

```
ALU(config)# clear ip-policy statistics
```

PBR CONFIGURATION EXAMPLE

Consider a scenario, a corporate XYZ with two departments - Finance and Engineering.

XYZ would like to send finance department's traffic on to the next-hop 203.121.10.1 and send engineering department's traffic on 150.23.221.50. Its internal LAN is connected on one of the L2GE ports (configured as VLAN 10).

In order to achieve this, you need to configure a routing policy and the following match conditions and forwarding action:

CONFIGURATION STEPS

Quick Steps

1. Create match-list specific to finance department and engineering department.
2. Create an IP policy.
3. Attach the IP policy to an interface.

Detailed Steps

Step 1: Create a match-list for finance department and engineering department.

```
ALU(config)# match-list fin-dept
ALU(config-match-list-fin-dept)# 10 ip prefix 10.1.1.0/24
any
ALU(config-match-list-fin-dept)# exit

ALU(config)# match-list engg-dept
ALU(config-match-list-engg-dept)# 10 ip prefix 10.1.2.0/
24 any
ALU(config-match-list-engg-dept)# exit
ALU(config)#
```

Step 2: Create a routing policy to route the traffic originating from finance department to the next hop 203.121.10, and route all traffic from engineering department to the next hop 150.23.221.50.

```
ALU(config)# ip-policy xyz-corporate-policy
ALU(config-ip-policy-xyz-corporate-poli)# 10 match fin-
dept next-hop 203.121.10.1
ALU(config-ip-policy-xyz-corporate-poli)# 20 match engg-
dept next-hop 150.23.221.50

ALU(config-ip-policy-corporate-policy)# exit
ALU(config)#
```

Step 3: Apply the IP policy on the interface.

```
ALU(config)# interface vlan 10
ALU(config-if Vlan10)# ip-policy xyz-corporate-policy
ALU(config-if Vlan10)# exit
ALU(config)#
```

SHOW COMMANDS

Verify the IP policy configuration by using the following show command:

```
ALU(config)# show ip-policy xyz-corporate-policy
!
! IP-Policy configuration
!
ip-policy xyz-corporate-policy
    10 match any fin-dept next-hop 203.121.10.1
    20 match any engg-dept next-hop 150.23.221.50
exit
!
interface Vlan10
    ip-policy xyz-corporate-policy
exit
```

Part 6 Network Security

CHAPTER 25 NETWORK ADDRESS TRANSLATION

After you install the OA-700, use the CLI to configure the system for Network Address Translation (NAT). This chapter includes steps for configuring the Source NAT (SNAT) and Destination NAT (DNAT).

For instructions on using the NAT commands and descriptions on each of their parameters, refer to the “**NAT CLI Commands**” in the *OmniAccess 700 CLI Command Reference Guide*.

This chapter includes the following sections:

- “**NAT Overview**”
- “**Source NAT Configuration**”
- “**Destination NAT Configuration**”
- “**Bypass IPsec Traffic**”
- “**Modifying NAT Configuration**”

CHAPTER CONVENTIONS

Acronym	Description
UM	User Mode - ALU >
SUM	Super User Mode - ALU #
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
NAT	Network Address Translation
NAPT	Network Address Port Translation
NCM	NAT Configuration Mode - ALU (config-nat name)#
PAT	Port Address Translation

NAT OVERVIEW

Scarcity of registered IP addresses and related address management issues in connecting a private network to the Internet created a need for a mechanism such as NAT.

NAT mechanism translates un-registered "private" IP addresses used in an internal network to a real "registered" IP on external networks such as the Internet. When using NAT, only a single unique IP address is required to represent an entire group of computers.

By configuring NAT on the network gateway, home users and small businesses can connect their network to the Internet inexpensively and efficiently. As a fringe benefit, NAT automatically hides internal IP addresses and hence offers protection from exposing hosts on the private network to the Internet.

Refer the following section for more details on NAT:

- [“Types of NAT”](#)
- [“Benefits of NAT”](#)
- [“Before You Configure NAT”](#)
- [“Alcatel-Lucent Specific Overview”](#)

TYPES OF NAT

This section describes following types of NAT:

- [“Network Address Port Translation”](#)
- [“Static NAT”](#)
- [“Dynamic NAT”](#)

NETWORK ADDRESS PORT TRANSLATION

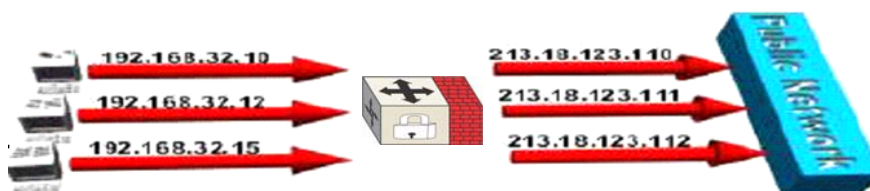
Network Address Port Translation (NAPT) is an extension to the basic NAT. In this, many network addresses and their TCP/UDP ports are translated to a single network address and its TCP/UDP ports. This involves mapping ports for requests within a network to an external address via a Public IP to free ports so that incoming replies on those connections can be uniquely identified to specific systems within the network.

STATIC NAT

Static NAT allows systems in a private network with unregistered IP address appear to have a registered IP address with a one-to-one mapping. It is particularly useful when a device needs to be accessible from outside the network. In specific circumstances, Static NAT, also called inbound mapping, allows external devices to initiate connections to computers on the private domain.



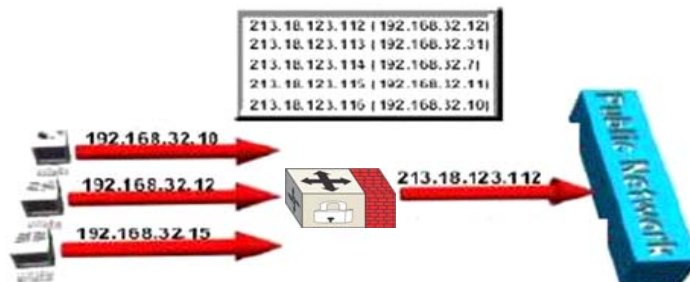
Note: In case of a firewall being used in conjunction with Static NAT, a filter or policy on the firewall must exist for each address map to allow inbound traffic.



Static NAT: Mapping an unregistered IP address to a registered IP address on a one-to-one basis.

DYNAMIC NAT

Allow hosts on the private network to start 'conversation' to the external network with the inbound replies being automatically forwarded to the initiating host. The NAT device achieves this by building a mapping table between the internal and external hosts on the fly based on the traffic flow.



Dynamic NAT: Maps an unregistered IP address to a registered IP address from a group of registered IP addresses

BENEFITS OF NAT

- Connection to the Internet: NAT is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address.
- Transparent Proxying.
- Security considerations: NAT automatically provides firewall-style protection without any special setup.
- Traffic logging: Since all the traffic to and from the Internet has to pass through a NAT gateway, it can record all the traffic to a log file.
- Ease and flexibility of network administration: The smaller parts expose only one IP address to the outside, which means that computers can be added or removed, or their addresses changed, without impacting external networks.

BEFORE YOU CONFIGURE NAT

1. Before you configure NAT, you must decide whether NAT has to be configured on an internal or external interface.
2. You should also be sure that you have a basic understanding of the IP protocol, port numbers, host address mapping; specifically, you should know how to configure dynamic NATs.
3. Configure the common classifiers to decide on the match-list. (Refer to the [“Common Classifiers”](#) of this guide, to configure the match-lists).

ALCATEL-LUCENT SPECIFIC OVERVIEW

- In OA-700, NAT is applied to an interface.
- Configuration allows for load-balancing in DNAT if a pool of IP addresses are used.
- Port ranges used for translation can be explicitly specified.
- Command "**ip nat name**" enters the sub-configuration mode. Hence, you can have multiple match-lists with different NAT IP pool or host address.
- In OA-700, the default for NAT configuration is dynamic mapping. The keyword "**static**" has to be used to convert this setting to static.
- OA-700 supports reflexive/stateful inspection.
- For Source NAT, if no IP pool or host address is specified, the default is the box's IP address of the egress interface on which the NAT policy is applied.

SOURCE NAT CONFIGURATION

Source NAT (SNAT) is mainly used for changing the source address of packets. A good example would be that of a network behind a firewall, which interacts with the external world. For the hosts behind the firewall to interact with the external world, the local network's IP addresses have to be substituted with that of the firewall.

With this target, the firewall will automatically SNAT and De-SNAT the packets, hence making it possible to make connections from the LAN to the Internet.

Refer the following section to configure SNAT on your system:

- [“SNAT Configuration Steps”](#)
- [“SNAT Configuration Flow”](#)
- [“SNAT Configuration Commands”](#)

SNAT CONFIGURATION STEPS

This section lists the steps to be followed while configuring SNAT.

Step 1: Configure the match-lists with the common classifiers pre-configured. (Refer the [“Common Classifiers”](#) in this guide)

Step 2: Enter the NAT Configuration Mode. See [“To Enter NAT Configuration Mode”](#)

Step 3: Configure SNAT. See [“To Configure SNAT”](#)

Step 4: Configure SNAT optional parameters.

- Configure SNAT with host IP address. See [“To Configure SNAT with Host IP Address”](#)
- Configure address pool. See [“To Configure SNAT with an IP Address Pool”](#)
- Configure port range. See [“To Configure SNAT with Port Range”](#)
- Configure Static SNAT. See [“To Configure Static SNAT”](#)
- Reorder the rules in the match-list for the configured SNAT. See [“To Reorder the Rules in SNAT”](#)

Attach configured SNAT to an Interface

Step 5: Enter into Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 6: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 7: Configure IP address for the interface.

```
ALU(config-if <interface-name>)# ip address {<ip-  
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address  
20.20.20.20/24
```

Step 8: Attach the configured SNATs to appropriate interfaces as per the desired direction i.e, either "IN/OUT". See ["To Attach a NAT Policy to an Interface"](#)

Step 9: Turn On /Turn Off the statistics on an Interface ["To Turn On/Off Statistics on an Interface"](#) (Optional)

Step 10: View NAT configuration. See ["NAT Show Commands"](#).

SNAT CONFIGURATION FLOW

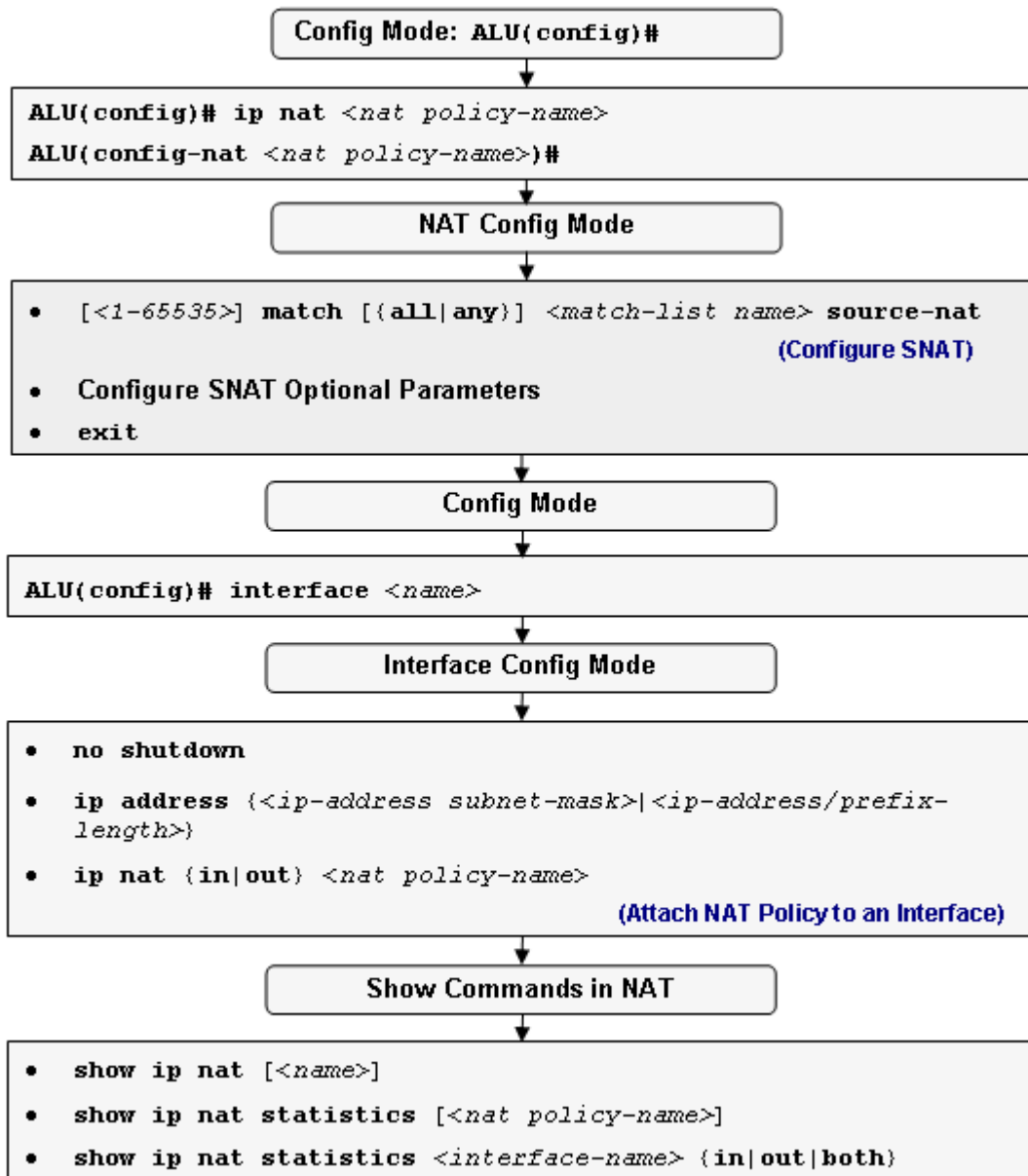


Figure 48: SNAT Configuration Flow

SNAT CONFIGURATION COMMANDS

This section details the commands that are used in configuring SNAT.

For SNAT, you have an option to enter either the “address pool” or single host address. Even if no address is configured, the IP address of the egress interface on which the NAT policy is applied will be used.

TO ENTER NAT CONFIGURATION MODE

Command (in CM)	Description
<code>ip nat <nat policy-name></code>	This command is used to configure a NAT policy. This command enters the NAT configuration mode.

EXAMPLE

```
ALU(config)# ip nat N1
ALU(config-nat-N1)#
```

TO CONFIGURE SNAT

Command (in NCM)	Description
<code>[<1-65535>] match [{all any}] <match-list name> source-nat</code>	This command is used to configure a SNAT, and configure one or more rule (associate match-lists and set priority for the rule) for the configured SNAT. The range for the rule number is 1-65535. This rule number signifies the priority of a rule. By default, the numbering pattern for rule number is the next multiple of ten to the highest existing rule number.



Note:


1. Currently, multiple match-lists cannot be associated to a firewall policy rule for NAT. To configure more than one match-list within a firewall policy, add multiple rules with different match-lists.

2. When you configure a SNAT without any IP address, the address used for natting is taken as the IP address of the interface to which the NAT policy is bound.

EXAMPLE

```
ALU(config-nat-N1)# 10 match m1 source-nat
```

To CONFIGURE SNAT WITH HOST IP ADDRESS

Command (in NCM)	Description
<pre>[<1-65535>] match [{all any}] <match-list name> source-nat host {<ip-address/host-name>} [port- range {<2048-65535> <2048- 65535>} static]</pre>	<p>This command is used to configure a SNAT with host IP address.</p>  <p>Note: If no address is configured, the IP address of the egress interface on which the NAT policy is applied will be used.</p>




Note: Currently, 'Hostname' option is not supported. Only host IP address can be configured.

EXAMPLE

```
ALU(config-nat-N1)# match m1 source-nat host 192.168.10.91
```

To CONFIGURE SNAT WITH AN IP ADDRESS POOL

Command (in NCM)	Description
<pre>[<1-65535>] match [{all any}] <match-list name> source-nat pool <list-name> [port-range {<2048-65535> <2048- 65535>} static]</pre>	<p>This command is used to configure SNAT with an IP address pool.</p>  <p>Note: If no address is configured, the IP address of the egress interface on which the NAT policy is applied will be used.</p>




Note: If a SNAT policy with the pool configuration is attached to an interface, and at any given point of time, the list is modified, you need to reapply the NAT policy on the interface.

EXAMPLE

```
ALU(config-nat-N1)# match m1 source-nat pool 11
```


To CONFIGURE SNAT WITH PORT RANGE

Command (in NCM)	Description
<pre>[<1-65535>] match [{all any}] <match-list name> source-nat port-range <2048-65535> <2048- 65535></pre>	<p>This command is used to configure SNAT with a port range.</p>  <p>Note: If no port range is specified, a default port range of 2048 – 65535 is used.</p>

EXAMPLE

```
ALU(config-nat-N1)# match m1 source-nat port-range 2048 6000
```

To CONFIGURE STATIC SNAT

Command (in NCM)	Description
<pre>[<1-65535>] match [{all any}] <match-list name> source-nat static</pre>	<p>This command is used to configure a static SNAT that uses one-to-one address mapping without port translation.</p> <p>By default, NAT enables dynamic mapping.</p>  <p>Note: If no address is configured, the IP address of the egress interface on which the NAT policy is applied will be used.</p>

EXAMPLE

```
ALU(config-nat-N1)# match m1 source-nat static
```

To REORDER THE RULES IN SNAT

Note: Rule/line numbers will not be shown unless you specifically type them in. Also, the line numbers can be seen only in the “**show**” command.

Command (in NCM)	Description
renumber	Use this command to generate a numbering scheme for the SNAT rules configured.
change <1-65535> <1-65535>	Use this command to change the priority/order of a specific SNAT rule configured.



Note: Refer to the “**Updates**” section to know more on the “change” and “renumber” keywords.

EXAMPLE

```
ALU(config-nat-N1)# renumber
```

```
ALU(config-nat-N1)# change 10 20
```

To ATTACH A NAT POLICY TO AN INTERFACE

Command (in ICM)	Description
<code>ip nat {in out} <nat policy-name></code>	<p>Enter this command in the Interface Configuration Mode.</p> <p>This command is used to attach a NAT policy to an interface in 'in' or 'out' direction.</p> <p>The keyword "in" signifies that ingress traffic is subjected to the NAT, only if all classifiers in this NAT object are matched.</p> <p>The keyword "out" denotes that egress traffic is subjected to the NAT, if all classifiers in this NAT object are matched.</p>



Note: Each interface can have only one ingress and one egress NAT policy.

EXAMPLE

In the example below, HTTP requests initiated from internal network will be translated and sent to external network. Returning HTTP responses are automatically allowed and translated even if there is a filter to block:

```

ALU(config)# match-list m1
ALU2(config-match-list m1)# ip any any type ftp
ALU(config)# exit

ALU(config)# ip filter f1
ALU(config-filter f1)# match m1 deny
ALU(config)# exit

ALU(config)# ip nat n1
ALU(config-nat n1)# match m1 source-nat
ALU(config)# exit

ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# ip filter in f1
ALU(config-if GigabitEthernet7/0)# ip nat out n1

```

To TURN ON/OFF STATISTICS ON AN INTERFACE

Command (in ICM)	Description
<code>ip nat statistics {in out both}</code>	This command turns on statistics for a given interface. By default the NAT statistics on an interface is turned off.
<code>no ip nat statistics {in out both}</code>	This command turns off the statistics for a given interface.

EXAMPLE

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# ip nat statistics out

ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# no ip nat statistics out
```

SAMPLE CONFIGURATIONS OF SNAT ON OA-700

EXAMPLE 1

```
list zone1 prefix 10.1.1.0/24 prefix 10.2.2.0/24
list p1 host 192.168.24.1 host 192.168.24.2

match-list m1
    ip zone1 any type ftp

match-list m2
    ip host 11.1.1.1 any type ftp

ip nat n1
    match m2 source-nat host 174.35.8.1 static
    match m1 source-nat pool p1

interface GigabitEthernet7/0
ip nat out n1
```

EXAMPLE 2

Single address translation with no port translation.

```
list p1 prefix 192.168.56.0/24
match-list host1
    ip host 10.1.1.1 any type ftp

match-list host2
    ip host 10.1.1.2 any type ftp
match-list net11
    ip prefix 11.1.1.0/24 any type ftp

ip nat n2
    match host1 source-nat host 192.168.10.1 static
    match host2 source-nat host 192.168.10.2 static
    match net11 source-nat pool p1 static

interface GigabitEthernet7/0
ip nat out n2
```

DESTINATION NAT CONFIGURATION

Destination NAT (DNAT) is commonly used to publish a service from an internal network to a publicly accessible IP. The destination address of the packet is changed and rerouted to the host.

For DNAT, you can specify a single internal target to connect the external service requests (such as HTTP) to one or several targets for load balancing.

For DNAT, IP pool or host address must be specified.

Refer the following sections to configure DNAT on your system:

- [“DNAT Configuration Steps”](#)
- [“DNAT Configuration Flow”](#)
- [“DNAT Configuration Commands”](#)
- [“NAT Show Commands”](#)

DNAT CONFIGURATION STEPS

This section lists the steps to be followed while configuring DNAT.

Step 1: Configure the match-lists with the common classifiers pre-configured. (Refer the **“Common Classifiers”** in this guide.)

Step 2: Enter the NAT Configuration Mode. See [“To Enter NAT Configuration Mode”](#)

Step 3: Configure DNAT with host IP address or address pool See [“To Configure DNAT”](#)

Step 4: Configure DNAT optional parameters.

- Configure port number for DNAT. See [“To Configure Port Number for DNAT”](#)
- Configure Static DNAT. See [“To Configure Static DNAT”](#)
- Reorder the rules in the match-list for the configured DNAT. See [“To Reorder the Rules in DNAT”](#)

Attach configured DNAT to an Interface

Step 5: Enter into Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 6: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 7: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 8: Attach the configured DNATs to appropriate interfaces as per the desired direction i.e, either "IN/OUT". See ["To Attach a NAT Policy to an Interface"](#)

Step 9: Turn On /Turn Off the statistics on an Interface ["To Turn On Statistics on an Interface"](#) (Optional)

Step 10: View NAT configuration. See ["NAT Show Commands"](#).

DNAT CONFIGURATION FLOW

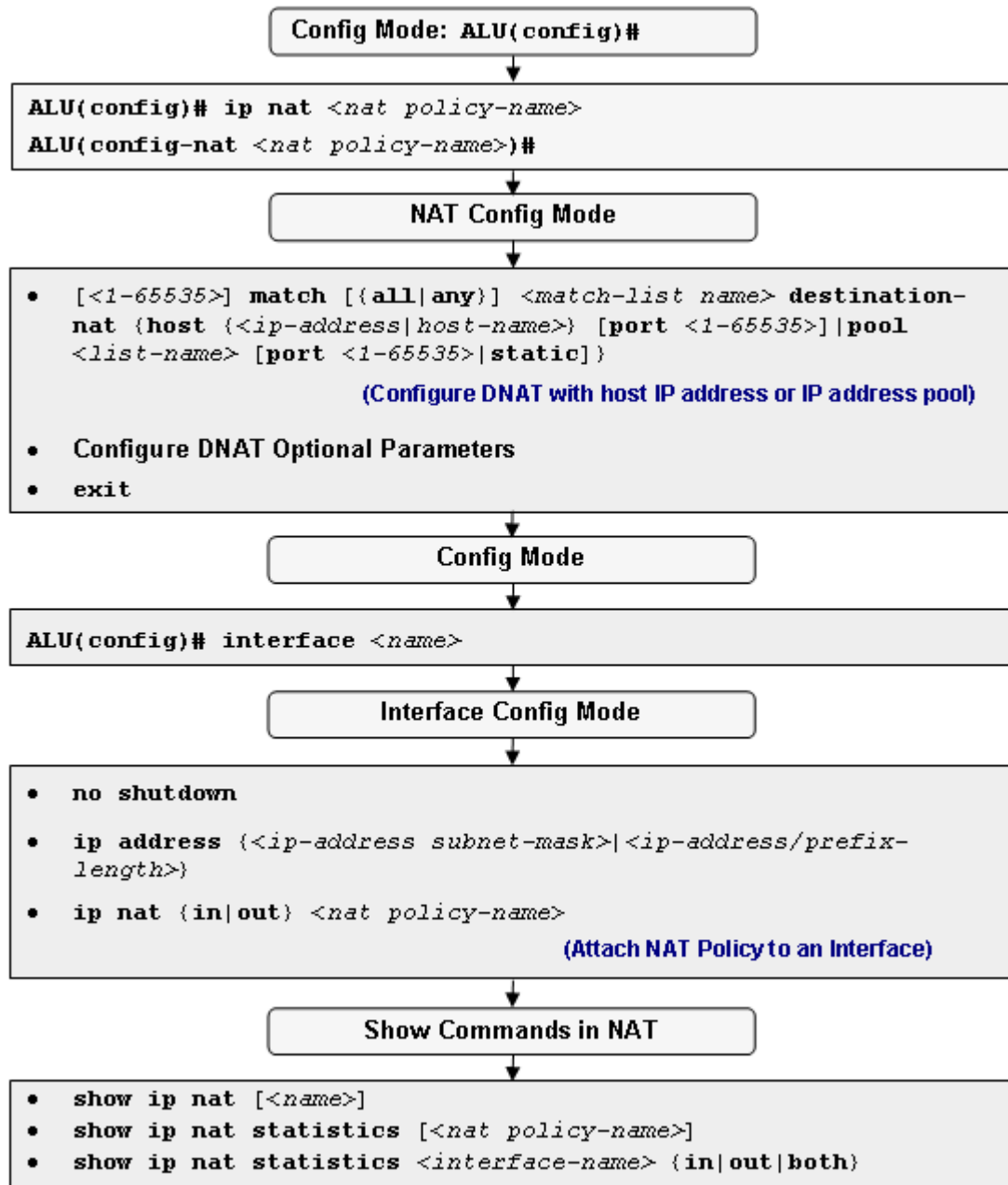


Figure 49: DNAT Configuration Flow

DNAT CONFIGURATION COMMANDS

This section provides details about the commands that are used in configuring DNAT.


To ENTER NAT CONFIGURATION MODE

Command (in CM)	Description
<code>ip nat <nat policy-name></code>	This command is used to configure a NAT policy. This command enters the NAT configuration mode.

EXAMPLE

```
ALU(config)# ip nat N2
ALU(config-nat-N2)#
```

To CONFIGURE DNAT

Command (in NCM)	Description
<code>[<1-65535>] match [{all any}] <match-list name> destination-nat {host {<ip-address/host-name>} [port <1-65535>] pool <list-name> [port <1-65535> static]}</code>	<p>This command is used to configure a DNAT with one or more rules (associate match-lists and set priority for the rule) for the configured DNAT.</p> <p>The range for the rule number is 1-65535. This rule number signifies the priority of a rule. By default, the numbering pattern for rule number is the next multiple of ten to the highest existing rule number.</p> <p>And, this command is used to configure a DNAT with host IP address or an IP address pool.</p> <div style="display: flex; align-items: flex-start;">  <p>Note: Presently, 'Hostname' option is not supported. Only host IP address can be configured.</p> </div>



Note: Currently, multiple match-lists cannot be associated to a firewall policy rule for NAT. To configure more than one match-list within a firewall policy, add multiple rules with different match-lists.

If a DNAT policy with the pool configuration is attached to an interface, and at any given point of time, the list is modified, you need to reapply the NAT policy on the interface.

EXAMPLE

```
ALU(config-nat-N2)# match m1 destination-nat host 192.168.10.91
ALU(config-nat-N2)# match m1 destination-nat pool l1
```

To CONFIGURE PORT NUMBER FOR DNAT

Command (in NCM)	Description
[<1-65535>] match [{ all any }] <match-list name> destination-nat { host {<ip-address/host-name>} pool <list-name>} port <1-65535>	This command is used to configure port number for a DNAT.

EXAMPLE

```
ALU(config-nat-N2)# match m1 destination-nat host 192.168.10.91
port 100
ALU(config-nat-N2)# match m1 destination-nat pool l1 port 100
```

To CONFIGURE STATIC DNAT

Command (in NCM)	Description
[<1-65535>] match [{ all any }] <match-list name> destination-nat pool <list-name> static	This command is used to configure a static DNAT that uses one-to-one address mapping without port translation.

EXAMPLE

```
ALU(config-nat-N2)# match m1 destination-nat pool l1 static
```

To REORDER THE RULES IN DNAT

Command (in NCM)	Description
<code>renumber</code>	Use this command to generate a numbering scheme for the DNAT rules configured.
<code>change <1-65535> <1-65535></code>	Use this command to change the priority/order of a specific DNAT rule configured.



Note: Refer to the **“Updates”** section to know more on the “change” and “renumber” keywords.

EXAMPLE

```
ALU(config-nat-N2)# renumber
ALU(config-nat-N2)# change 10 20
```

To ATTACH A NAT POLICY TO AN INTERFACE

Command (in ICM)	Description
<code>ip nat {in out} <nat policy-name></code>	<p>Enter this command in the Interface Configuration Mode.</p> <p>This command is used to attach a NAT policy to an interface in ‘in’ or ‘out’ direction.</p> <p>The keyword "in" signifies that ingress traffic is subjected to the NAT, only if all classifiers in this NAT object are matched.</p> <p>The keyword "out" denotes that egress traffic is subjected to the NAT, if all classifiers in this NAT object are matched.</p>

EXAMPLE

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# ip nat in N2
```



Note: Each interface can have only one ingress and one egress NAT policy.

To Turn On Statistics on an Interface

Command (in ICM)	Description
<code>ip nat statistics {in out both}</code>	This command turns on statistics for a given interface. By default, the interface statistics is 'off'.

EXAMPLE

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# ip nat statistics out
```

SAMPLE CONFIGURATION EXAMPLE OF DNAT ON OA-700

The following DNAT example illustrates that any ingress HTTP traffic at the external interface GigabitEthernet7/0 with destination IP address 201.176.18.1 will have that destination address translated to 14.1.1.1 or 14.1.1.2, and destination port translated to 8080. This is used in a typical web server farm load balancing situation:

```
list p1 host 14.1.1.1 host 14.1.1.2
match-list m1
    tcp any host 201.176.18.1 service http

ip nat N1
    10 match M1 destination-nat pool p1

    match m1 destination-nat pool p1 port 8080

ALU(config-if GigabitEthernet7/0) ip nat in n1
```

BYPASS IPSEC TRAFFIC

TO BYPASS THE IPSEC TRAFFIC

Command (in CM)	Description
[<1-65535>] match [{ all any }] <match-list name> bypass	This command is used in conjunction with the SNAT or DNAT commands to bypass the traffic.

EXAMPLE

```
ALU(config)# ip nat snat
ALU(config-nat-snat)# match m1 bypass
```


NAT SHOW COMMANDS

Use the following show commands to display the configuration setting for NAT on the OA-700.

To VIEW NAT

Command (in SUM)	Description
<code>show ip nat</code>	Displays details of all the configured NATs.
<code>show ip nat [<name>]</code>	This command displays the configuration details for a specific NAT.

EXAMPLE

- The following example displays the details of all the NATs configured:

```
ALU# show ip nat

ip nat n1
  10 match all m1 source-nat
ip nat n2
  10 match m2 source-nat
```

- The following example shows the configuration details of a specific NAT:

```
ALU# show ip nat n1

ip nat n1
  10 match all m1 source-nat
```

To VIEW NAT STATISTICS

Command (in SUM)	Description
<code>show ip nat statistics [<nat policy-name>]</code>	This command displays detailed statistics for the NATs configured or for a specific NAT policy.

EXAMPLE

- The following example shows detailed statistics for the NAT policy 'n1':

```
ALU# show ip nat statistics n1

ip nat n1
  Dropped: 0, Bypassed: 0, Enqueued: 0
  10 match any m1 source-nat host 1.1.1.1
  Translated: 0, Bypassed: 0, PORTS Allocated: 0, Released: 0
  20 match any m2 source-nat host 1.1.1.2
  Translated: 0, Bypassed: 0, PORTS Allocated: 0, Released: 0
interface GigabitEthernet7/0 Out
```

To View the NAT Statistics on an Interface

Command (in SUM)	Description
<code>show ip nat statistics <interface-name> {in out both}</code>	This command displays NAT statistics for a specific interface.

First turn ON the interface statistics and view the interface statistics.

EXAMPLE

The following example shows NAT statistics on a specified interface:

```
ALU# show ip nat statistics GigabitEthernet7/0 Out
```

```
ip nat n1
Dropped: 0, Bypassed: 0, Enqueued: 0
 10 match any m1 source-nat host 1.1.1.1
   NATted Packets: 0
 20 match any m2 source-nat host 1.1.1.2
   NATted Packets: 0
   interface GigabitEthernet7/0 out
```

NAT CLEAR COMMANDS

To CLEAR NAT DETAILS

Command (in SUM)	Description
<code>clear ip nat statistics <nat policy-name></code>	This command clears the statistics of a specific NAT policy.
<code>clear ip nat statistics <interface-name> {in out both}</code>	This command is used to clear the statistics of a NAT Policy on a particular interface.

EXAMPLE

The following example clears the counters of NAT 'n1'.

```
ALU# clear ip nat statistics n1
ALU#
```

The following example clears the statistics of the NAT for interface 'GigabitEthernet7/0'.

```
ALU# clear ip nat statistics GigabitEthernet7/0 in
ALU#
```

NAT DEBUG COMMANDS

This section lists the debug commands in NAT.

To ENABLE/DISABLE DEBUGGING ON NAT

Command (in SUM)	Description
<pre>debug firewall {session filter nat attack alg intrusion selector [saddr <ip-address> daddr <ip- address> protocol <number> sport <number> dport <number>][output permanent] all [detail-level]}</pre>	<p>This command turns on the debugging functionality for NAT on OA-700.</p>
<pre>no debug firewall {session filter nat attack alg intrusion selector [saddr <ip-address> daddr <ip- address> protocol <number> sport <number> dport <number>][output permanent] all [detail-level]}</pre>	<p>Use this command to turn off the debugging functionality for NAT.</p>

Notes:

1. **saddr** == source address
2. **daddr** == destination address
3. **sport** == source port
4. **dport** == destination port

EXAMPLE

```
ALU# debug firewall nat
```

MODIFYING NAT CONFIGURATION

This section deals with the method to modify NAT configuration on the OA-700.

- “Insertions”
- “Updates”
- “NAT Deletion Commands”

INSERTIONS

This section explains how to insert a rule in the NAT.

TO INSERT A RULE IN NAT

The need for insertion of match-lists becomes inevitable when you wish to include one or a group of match-lists after you have already configured the match-lists for a particular application.

The following example depicts the way to accomplish this.



Note: Rule numbers are displayed only in “show” command.

EXAMPLE

Consider the following example for inserting another rule in NAT:

```
ip nat N1
  10 match m1 source-nat pool p1
  20 match m2 source-nat pool p2
  30 match m3 source-nat pool p3

interface GigabitEthernet3/0
  ip nat out N1
```

If m4 is the match that has its priority in between m1 and m2, then to insert it in the NAT N1’s configuration, use the following syntax:

```
ip nat N1
  15 match m4 source-nat pool p4
```

View NAT N1’s configuration to recheck if the match has been added in the list:

```
show ip nat N1
```

The output will be:

```
ip nat N1
  10 match m1 source-nat pool p1
  15 match m4 source-nat pool p4
  20 match m2 source-nat pool p2
  30 match m3 source-nat pool p3

interface GigabitEthernet3/0
  ip nat out N1
```

UPDATES

This section explains how to update a NAT rule.

To RENUMBER THE LIST

By default, the numbering pattern used in OA-700 is multiples of ten. If a new match-list is to be included in-between two existing match-lists without actually changing the sequence of numbering, use the “**renumber**” keyword.

This command normalizes the line numbers of each rule, and sets them to the consecutive multiples of 10.

EXAMPLE

Consider the following example:

```
ip nat N1
  10 match M1 source-nat
  20 match M2 source-nat
  30 match M3 source-nat
  25 match M4 source-nat
```

This generates a numbering scheme without a proper order. The output of the show command will be:

```
ip nat N1
  10 match M1 source-nat
  20 match M2 source-nat
  25 match M4 source-nat
  30 match M3 source-nat
```

The keyword “**renumber**” is used to re-order the numbers to the original scheme.

```
ALU(config-nat-N1)# renumber
```

The output of the show command would now be:

```
ip nat N1
  10 match M1 source-nat
  20 match M2 source-nat
  30 match M4 source-nat
  40 match M3 source-nat
```

To Change the Rule/Line Numbers

To change the rule/line number of a pre-defined match-list, use the “**change**” keyword. This allows you to just change the line number and not to swap between two numbers. This command changes the order of a rule to the new number position.

EXAMPLE

Consider the following example:

```
ip nat N1
  10 match M1 source-nat
  20 match M2 source-nat
  30 match M3 source-nat
  40 match M4 source-nat
```

In the above sequence, if m4 has a priority 40. Use the “change” keyword to change the priority of m4.

```
ALU(config-nat-N1)# change 40 25
```

To view the NAT configuration after changing the priority, use the show command. The output appears as shown:

```
ip nat N1
  10 match M1 source-nat
  20 match M2 source-nat
  25 match M4 source-nat
  30 match M3 source-nat
```

Now to generate a numbering scheme with a proper order, use the keyword “**renumber**” as explained in the section [“To Renumber the List”](#).

NAT DELETION COMMANDS

This section explain how to delete NAT configurations.

TO DELETE A NAT POLICY

Command (in CM)	Description
<code>no ip nat <name></code>	This command is used to delete a specific NAT policy when it is not attached to any interface.

EXAMPLE

If the NAT 'N1' is to be deleted, use the following command:

```
ALU(config)# no ip nat N1
```

If a NAT policy is attached to an interface, first detach it before deleting.

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# no ip nat out nat1
```

TO ENFORCE DELETION OF NAT GLOBALLY

Command (in CM)	Description
<code>no ip nat <name> force</code>	The "force" keyword will automatically detach the specified NAT policy from respective interfaces, and deletes the policy. This command when used also deletes all the associated NAT policy rules.

EXAMPLE

To force deletion of the NAT N1:

```
ALU(config)# no ip nat N1 force
```


To DETACH A NAT POLICY FROM AN INTERFACE

Command (in ICM)	Description
<code>no ip nat {in out} <nat-name></code>	<p>This command detaches a NAT policy attached to an interface.</p> <p>This command does not delete the NAT policy definition in its entirety. It only detaches it from its interface.</p> <p>If the command "no ip nat <policy name>" is issued at the top level and if this NAT policy is not bound to any interface, it deletes the NAT policy definition.</p>

EXAMPLE

In the following example, NAT 'N1' is detached from its interface GigabitEthernet7/0.

Ex 1:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# no ip nat in nat1
```

Ex 2:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# no ip nat out nat1
```

To TURN OFF STATISTICS ON AN INTERFACE

Command (in ICM)	Description
<code>no ip nat statistics {in out both}</code>	This command turns off the statistics for a given interface.

EXAMPLE

```
ALU(config-if GigabitEthernet7/0)# no ip nat statistics out
```

To DELETE A NAT RULE

Command (in NCM)	Description
<code>no rule <1-65535></code>	This deletes only the rule in the NAT policy corresponding to the line number.

EXAMPLE

In the example below, the component or action corresponding to the rule 30 is deleted.

```
ALU(config-nat-N1)# no rule 30
```


CHAPTER 26 FILTER AND FIREWALL

After installing the OA-700, use the CLI to configure the OA-700 for security. This chapter provides the CLI commands for configuring the filters, firewall policies, and DoS attack prevention.

For instructions on using the commands and to get a detailed description on each of their parameters, refer to the “**Filter and Firewall**” section in the ***OmniAccess 700 CLI Command Reference Guide***.

This chapter includes the following sections:

- “**Network Security - An overview**”
- “**Network Attacks - An Overview**”
- “**Zone Configuration**”
- “**Security - Best Practices**”
- “**Customized-service Rule Based ALG Configuration**”

CHAPTER CONVENTIONS

Acronym	Description
ALG	Application Level Gateway
CLI	Command Line Interface
DoS	Denial-of-Service
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
FCM	Filter Configuration Mode - ALU (config-filter name)#
FwCM	Firewall Configuration Mode - ALU (config-firewall)#
F-PCM	Firewall-Policy Sub Configuration Mode - ALU (config-firewall-policy name)#
F-ACM	Firewall-Attack Sub Configuration Mode - ALU (config-firewall-attack name)#
TCM	Time-range Sub Configuration Mode - ALU (config-time-range name)#
ICM	Interface Configuration Mode - ALU (config-interface name)#

NETWORK SECURITY - AN OVERVIEW

With Internet access provided to most private networks, many become reachable for anyone wanting to gain access to such a private network. Besides legitimate access being made available for conducting business, this also opens the door for malicious access into private networks.

To circumvent such access, it is imperative for a network administrator to secure his network perimeter and guard access to areas of the network containing sensitive information, while not hampering applications such as e-mail and web server access. Since, network routers connecting a private network to the Internet are the entry points into the private network, these devices need to be included in securing the network perimeter.

Computing systems belonging to a single organization or department that allow complete unrestricted sharing of information, where the users are authorized and identified, are said to belong to a "**Trusted Zone**". In the interest of network security, all the other networks and users outside of the "trusted zone" are said to belong to an "**Untrusted Zone**". Most corporate networks need to access the Internet for retrieving information and the Internet is treated as an "untrusted zone".

Communication between the trusted and untrusted zones needs to be authorized, controlled, and monitored in effective yet transparent ways, so that malevolent entities do not have access to the information that is privileged and sensitive. Mechanisms that allow administrators to enforce such a regulation are called Firewalls.

A firewall is a network element that uses a combination of hardware and software intelligence to filter traffic between this trusted and untrusted zones. Firewalls can monitor the flow of traffic, and decide to either permit or deny the communication that is being attempted. Administrators define what are called access "**policies**" on Firewalls, where policies are a set of rules defining the types of traffic that may be permitted or denied. The policy specifies a packet-matching criteria to be based on the source IP address of the packet, the destination IP address, the source port number, the destination port number (for protocols which support ports) or even the packet type (UDP, TCP, ICMP, etc.). These fields are called "**Classifier fields**".

These security policies envisage the use of firewalls in different topologies. Before looking at these topologies, it is imperative to familiarize with some important firewall terminologies described below.

- [“Network Security Terminologies”](#)
- [“Firewall Mechanisms”](#)
- [“Before You Configure Filters and Firewalls”](#)
- [“OA-700 Specific Overview”](#)

NETWORK SECURITY TERMINOLOGIES

This section explains the Network Security Terminologies.

- “Gateway”
- “Application Level Gateway (ALG)”

GATEWAY

A gateway is an internetworking system used to connect two disparate network technologies and achieve seamless interconnectivity. Gateways typically operate on one or more layers of the OSI data model. Depending on the function intended for, they can operate from the application layer to link layer. A common type is a protocol gateway used to connect networks running different network or application protocols (e.g. TCP/IP, IPX). Because a network gateway can appear at the edge of the network, it is likely to implement related functions like firewalling on the gateway.

APPLICATION LEVEL GATEWAY (ALG)

An ALG has the capability to conduct stringent packet inspection and thereby augment the security infrastructure. Besides using a specialized program for each type of application or service that needs to pass through the firewall, ALGs look for altered data, potentially harmful traffic, data appropriateness, and also have the capability to log these.

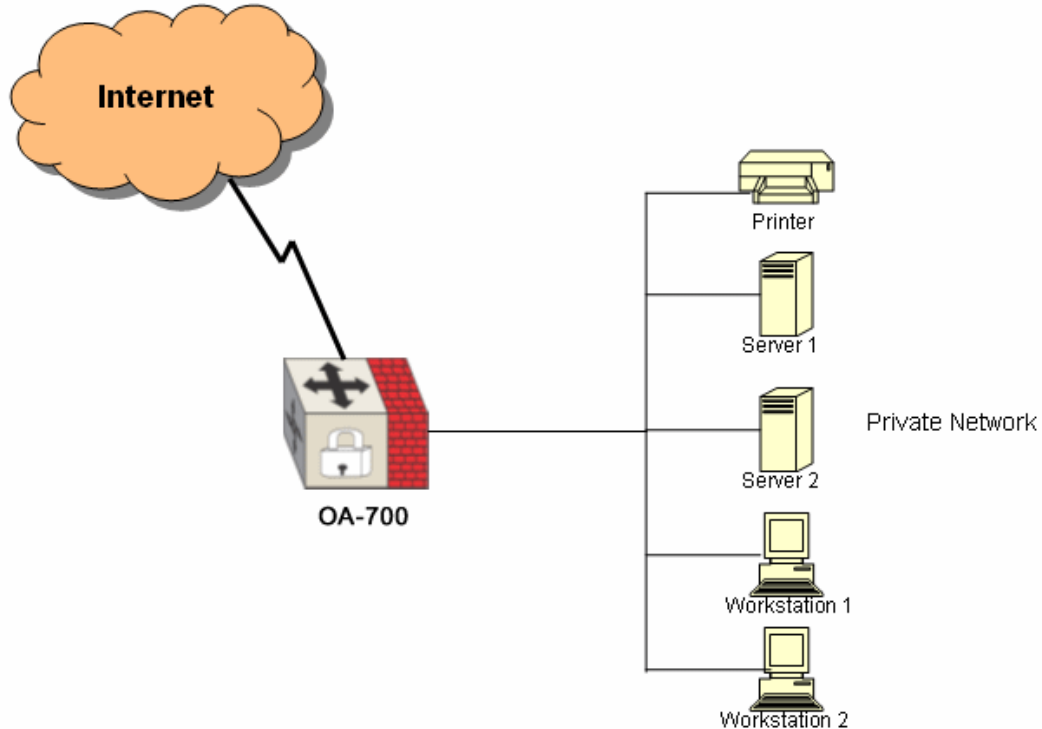


Figure 50: Depicting ALG Scenario

FIREWALL MECHANISMS

This section provides details about firewall mechanisms.

- [“Packet Filtering”](#)
- [“Stateful Inspection”](#)

PACKET FILTERING

This is a simple firewall solution that is usually implemented on devices like routers that filter packets. The packet-headers are inspected when going through the firewall. Packets are analyzed against a set of rules. Depending on these rules, the packet is either accepted or denied.

Once a match is found, the rule action is obeyed. The rule action could be to drop the packet, to forward the packet, or even to send an ICMP message back to the originator. Only the first match counts, as the rules are searched in order. Hence, the list of rules can be referred to as a “rule chain”. On match, the specified action is taken. Typical actions are deny/ allow / drop/ reject packets or reset connection.

STATEFUL INSPECTION

This is an advanced implementation of packet filtering that inspects packets at higher network layers, up to the application layer. Such filters interpret transport-level information (such as TCP and UDP headers) to analyze and record all current connections. This process is known as stateful inspection.

A stateful packet filter records the status of all connections and allows only those packets that are associated with a current connection. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics. The incoming information is then compared to these defining characteristics and upon a reasonable match, the information is permitted, else it is denied.

When a computer in the protected network initiates a connection with an external server, the stateful packet filter allows the server's response packets into the protected network. When the original connection is closed, however, the packet filter will block all further unsolicited packets from the untrusted zone. Stateful firewalls are also known as “dynamic” packet filters.



Note: OA-700 supports stateful and stateless inspection. By default, OA-700 firewall is ‘stateful’.

BEFORE YOU CONFIGURE FILTERS AND FIREWALLS

1. The identification of the risk level and the type of access required of each network system forms the basis before setting up the firewall.
2. Create Usage Policy Statements: Create Usage Policy Statements that outline users' roles and responsibilities with regard to security. Start with a general policy that covers all network systems and data.
3. Before you configure firewall, keep in mind to maintain a workable balance between security and required network access.
4. You should also be sure that you have a thorough understanding of the IP protocol, port numbers, host address mapping, and other related basic firewall technologies.
5. Configure the common classifiers first based on the usage policy statements. (Refer to the “**Common Classifiers**” chapter in this guide).
6. Configure the firewall with necessary parameters for scheduling, policy statements, stateful inspection, session management, etc.

OA-700 SPECIFIC OVERVIEW

- For OA-700, the default action for a filter is “**deny**”. However, you can change this option by using the keyword “**permit**”.
- OA-700, by default, supports “**stateful inspection**”. To convert it to a stateless inspection firewall, use the keyword “**stateless**”.
- If no rules (match cases) are defined, the **default** keyword can be used to just configure a **permit** or **deny** on all incoming and outgoing traffic.
- Filtering takes place only when filters are bound to interfaces - physical and virtual. If a virtual interface is created, the rules attached to the real interface is copied to the ruleset for the virtual interface. This can be modified. In the packet filter sequence, only the virtual interface ruleset will be used for the packets exiting from a virtual interface. The physical interface rules will have no effect on these packets.
- In contrast to other products, OA-700 differentiates between the classification and the actions. The classification on OA-700 is done by the use of match-lists and the actions are done by the use of filters.
- Our product is not a “**pure**” firewall appliance. In fact, it is a unified device of routing, Firewall, IDS/IPS, and voice. Firewall is only one component in the system, and is not enabled by default. So the “proper installation” to **enable** firewall is for you to create a default ACL policy, and bind it to untrusted interfaces to deny all traffic, such as the following commands:

FILTER CONFIGURATION

Refer to the following sections to configure filter:

- [“Filter Configuration Steps”](#)
- [“Filter Configuration Flow”](#)
- [“Filter Configuration Commands”](#)
- [“Filter Show Commands”](#)
- [“Filter Deletion Commands”](#)
- [“Filter Debug Commands”](#)

FILTER CONFIGURATION STEPS

This section lists the steps to be followed while configuring a filter.

Step 1: Configure the **match-lists** using the common classifiers syntax. (Refer to the chapter on [“Common Classifiers”](#) in this guide).

Step 2: Configure a filter. See [“To Create a Filter”](#)

- Configure Rule for a filter. See [“To Configure a Rule for a Filter”](#)

Step 3: Configure Filter Optional Parameters.

- Configure a stateless filter. See [“To Configure a Stateless Filter”](#)
- Reorder the rules in the filter. See [“To Reorder the Rules in the Filter”](#)

Step 4: Enter into Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```



Note: Filter can be configured on Gigabit Ethernet, Loopback, Serial, Tunnel, VLAN interfaces.

Step 5: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```


Step 6: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-  
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address  
20.20.20.20/24
```

Step 7: Interface Binding - Attach the configured filters to the appropriate interfaces as per the desired direction i.e, either "IN/OUT". See ["To Attach / Detach a Filter to an Interface"](#)



Note: An interface can have only one ingress and one egress filter.

Step 8: Use the show commands to view the configured filters. See ["Filter Show Commands"](#).

FILTER CONFIGURATION FLOW

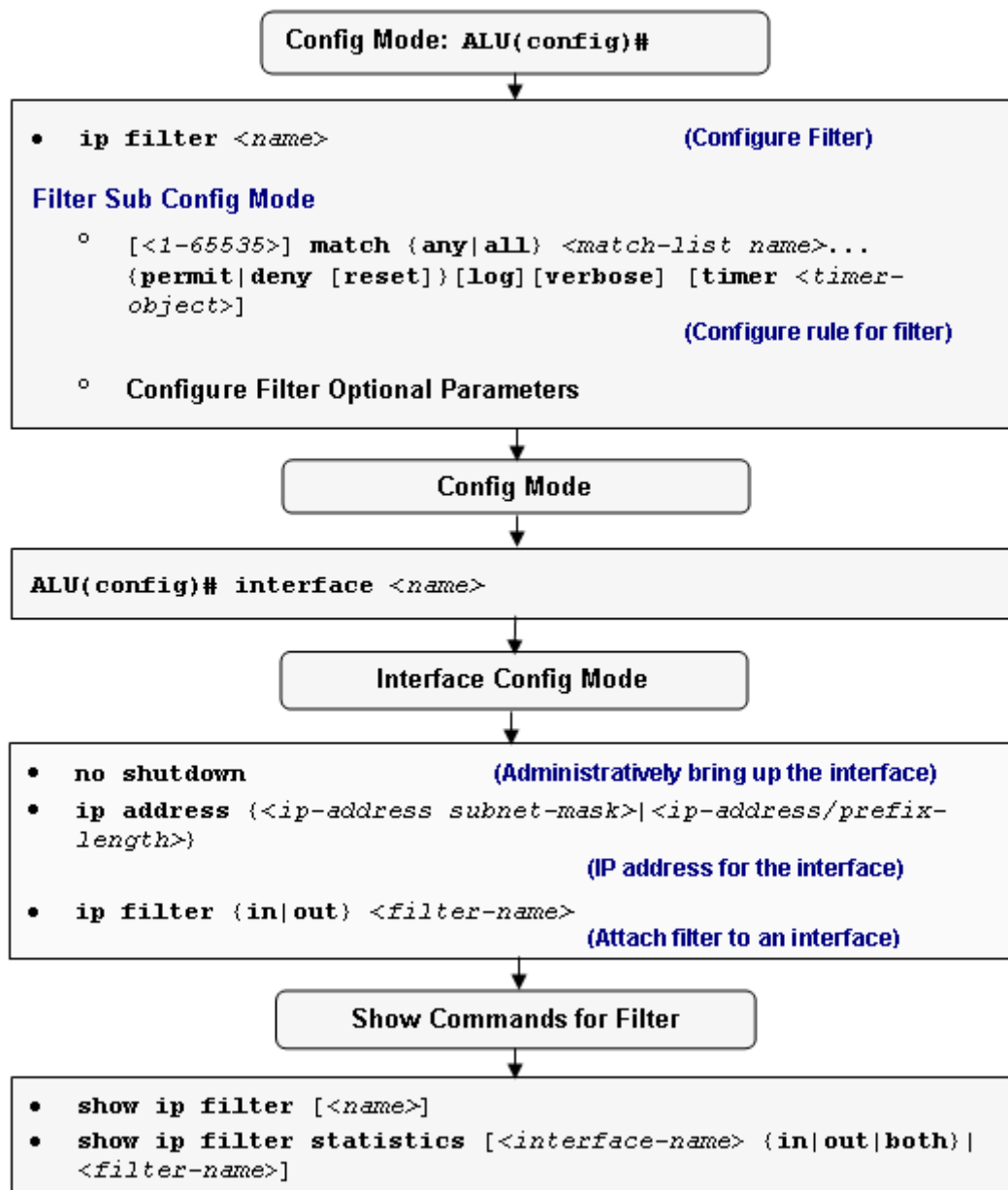


Figure 51: Filter Configuration Flow

FILTER CONFIGURATION COMMANDS

The following steps are used to configure a filter on the OA-700:

TO CREATE A FILTER

Command (in CM)	Description
<code>ip filter <name></code>	This command configures a filter.

EXAMPLE

```
ALU(config)# ip filter f1
ALU(config-filter-f1)#
```

TO CONFIGURE A RULE FOR A FILTER

Command (in FCM)	Description
<pre>[<1-65535>] match [any all] <match-list name>... {permit deny [reset]} [log] [verbose] [timer <timer- object>]</pre>	<p>This command is used to configure rules (associate match-lists and set priority for the rule) for a filter, and also set the action deny or permit for the configured rules.</p> <p>By default, 'any' keyword is used.</p> <p>The range for the rule number is 1-65535. This rule number signifies the priority of a rule. By default, the numbering pattern for rule number is the next multiple of ten to the highest existing rule number.</p> <p>Reset: Use this keyword to send a reset packet to the sender.</p> <p>Log: Use this keyword to log the packet information.</p> <p>Verbose: This logs all packets of a session.</p> <p>Timer object: The name of the time range.</p>
<pre>default {deny permit} [log] [verbose]</pre>	<p>This command sets an action of either permit or deny on the filter.</p> <p>The default action for a filter is "deny".</p>



Note: The 'reset' keyword can be used in conjunction only with the "deny" keyword.

In filtering, packets are analyzed against a set of rules. Only those which satisfy these conditions and have a “**permit**” flag attached are allowed through the filters and sent to the requesting system. The permit traffic can also be logged. The rest are discarded and can optionally be logged.

EXAMPLE

The example below sets a permit rule on all IP traffic across the filter.

```
ALU(config)# ip filter f1
ALU(config-filter-f1)# 10 match m1 permit log
```

The example below configures a deny rule with reset option on all the IP traffic on the filter configured.

```
ALU(config-filter-f1)# 10 match m1 deny reset
```

TO CONFIGURE A STATELESS FILTER

Command (in FCM)	Description
stateless	Use this command to set the filter behavior to stateless.
no stateless	The 'no' command changes the stateless option configured on the filter to the default state which is stateful or reflexive.



Note: The filters on **OA-700** are by default stateful. This behavior can be overridden by the keyword “**stateless**”.

EXAMPLE

The following example sets the filter to stateless.

```
ALU(config-filter-f1)# stateless
```

In the example below, the filter f1 is changed to stateful/reflexive mode.

```
ALU(config)# filter f1
ALU(config-filter-f1)# no stateless
```

TO REORDER THE RULES IN THE FILTER

Command (in FCM)	Description
renumber	Use this command to generate a numbering scheme for the filter rules configured.
change <1-65535> <1-65535>	Use this command to change the priority of a specific filter rule configured.

EXAMPLE

Consider the following configuration:

```
ALU(config)# ip filter f1
ALU(config-filter-f1)#
 10 match m1 deny
 20 match m2 deny
 30 match m3 deny log
 40 match m4 deny reset
default permit
```

In the above example, m4 has a priority 40. Use the “change” keyword to change the priority of m4.

```
ALU(config)# ip filter f1
ALU(config-filter-f1)# change 40 15
```

To view the filter configuration after changing the priority, give the show command. The output appears as shown:

```
show ip filter f1
ip filter f1
 10 match m1 deny
 15 match m4 deny reset
 20 match m2 deny log
 30 match m3 deny
default permit
```

Now, to generate a numbering scheme with a proper order, use the keyword “renumber”, as follows:

```
ALU(config)# ip filter f1
ALU(config-filter-f1)# renumber
```

To view the filter configuration after renumbering, give the show command. The output appears as shown:

```
show ip filter f1
ip filter f1
 10 match m1 deny
 20 match m4 deny reset
 30 match m2 deny log
 40 match m3 deny
default permit
```

TO ATTACH / DETACH A FILTER TO AN INTERFACE

Command (in ICM)	Description
<code>ip filter {in out} <filter-name></code>	<p>This command is used to attach a filter to an interface in 'in' or 'out' direction.</p> <p>Filter is applied to the ingress (incoming) traffic if "in" keyword is used.</p> <p>Filter is applied to the egress (outgoing) traffic if "out" keyword is used.</p>
<code>no ip filter {in out} <filter-name></code>	<p>This command detaches the filter attached to an interface.</p> <p>This does not delete the filter definition in its entirety. It only detaches it from its interface.</p> <p>If the command "no ip filter name" is issued at the top level and if this filter is not bound to any interface, it deletes the filter definition.</p>



Note: Each interface can have one ingress and one egress filter.

EXAMPLE

The following example binds the filter f1 to interface Gigabit Ethernet7/0:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# ip filter in f1
```

If the filter f1 is interfaced to GigabitEthernet7/0, the following example detaches it from Gigabit Ethernet7/0:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# no ip filter in f1
```

FILTER SHOW COMMANDS

Use the following show commands to monitor and troubleshoot filter performance on the OA-700.

TO VIEW FILTERS CONFIGURED

Command (in SUM)	Description
<code>show ip filter [<name>]</code>	This command displays the details of all the filters configured on the system. If filter name is specified, it displays the details for the specified filter.

EXAMPLE

a) The following syntax displays the all the filters configured in the system:

```
ALU# show ip filter
```

```
ip filter f1
 10 match any m1 permit
 20 match any m1 permit
 default deny
 interface GigabitEthernet7/0 In, Stats Off
```

```
ip filter f2
 10 match any m2 deny
 default deny
 interface GigabitEthernet7/0 In, Stats Off
```

b) The following syntax displays the filter f1's details:

```
ALU(config-filter-f1)# show ip filter f1
```

```
ip filter f1
 10 match any m1 permit
 20 match any m1 permit
 default deny
 interface GigabitEthernet7/0 In, Stats Off
```

To VIEW THE FILTER STATISTICS ON AN INTERFACE

Command (in SUM/ICM)	Description
<code>show ip filter statistics</code> [<interface-name> {in out both} <filter-name>]	This command displays the statistics of a filter on a particular interface.

EXAMPLE

The following command displays the filter statistics:

```
ALU(config)# show ip filter statistics GigabitEthernet 7/0
in

ip filter f1
 20 match any m1 permit   Hits 0
 10 match any m1 permit   Hits 2
 default deny
interface GigabitEthernet7/0 In, Stats On

ip filter f2
 20 match any m2 deny     Hits 0
 default deny             Hits 0
interface GigabitEthernet7/0 In, Stats Off
```


FILTER DELETION COMMANDS

TO DELETE A FILTER GLOBALLY WHEN NOT ATTACHED TO ANY INTERFACE

Command (in CM)	Description
<code>no ip filter <name></code>	This command is used to delete the filter when it is not attached to any interface.

EXAMPLE

If the filter f1 has to be deleted, use the following command:

```
ALU(config)# no ip filter f1
```

If a filter is attached to an interface, first detach it before deleting.

```
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# no ip filter out f1
```

TO DELETE A FILTER GLOBALLY WHEN ATTACHED TO AN INTERFACE

Command (in CM)	Description
<code>no ip filter <name> force</code>	This command is used to delete the filter when it is attached to an interface.

If the filter is attached to any of the interfaces, it cannot be deleted. In such a case, to force deletion of a filter, use the “**force**” command from the configuration mode itself.

This gives the flexibility in deleting a filter even without detaching it from its interfaces. As a result, it reduces the complexity and time.

EXAMPLE

If the filter f1 has to be deleted when attached to a an interface, apply the following syntax:

```
ALU(config)# no ip filter f1 force
```

TO DELETE A COMPONENT IN THE FILTER

Command (in FCM)	Description
<code>no rule <1-65535></code>	This command deletes a single component in the filter with respect to the corresponding line number.

EXAMPLE

The example below deletes the match corresponding to the line number 10 from the F1 filter.

```
ALU(config-filter-f1)# no rule 10
```

FILTER CLEAR COMMANDS

TO CLEAR FILTER STATISTICS

Command (in SUM)	Description
<code>clear ip filter statistics</code> [<interface-name> {in out both} <filter-name>]	This command is used to clear the statistics of a filter on a particular interface.

EXAMPLE

```
ALU# clear ip filter statistics GigabitEthernet7/0 in
ALU#
```

```
ALU# clear ip filter statistics GigabitEthernet3/0 out
ALU#
```

FILTER DEBUG COMMANDS

This section details the debug commands used in Filter configuration.

TO ENABLE/DISABLE DEBUGGING ON FILTER

Command (in SUM)	Description
<pre>debug firewall {session filter nat attack alg intrusion selector [saddr <ip- address> daddr <ip- address> protocol <number> sport <number> dport <number>] [output permanent] all [detail-level]}</pre>	<p>This command turns on debugging for the filter statistics configured.</p> <p>The “selector” keyword is used to debug only selected traffic.</p>
<pre>no debug firewall {session filter nat attack alg intrusion selector [saddr <ip- address> daddr <ip- address> protocol <number> sport <number> dport <number>] [output permanent] all [detail-level]}</pre>	<p>This command turns off the debugging functionality.</p> <p>The “selector” keyword is used to turn off debugging only for selected traffic.</p>

Notes:

1. **saddr** == source address
2. **daddr** == destination address
3. **sport** == source port
4. **dport** == destination port

EXAMPLE

The example below enables debugging for the source IP 10.91.0.52

```
ALU# debug firewall selector saddr 10.91.0.52
```

The example below disables debugging for the source IP 10.91.0.52

```
ALU# no debug firewall selector saddr 10.91.0.52
```

SAMPLE EXAMPLES OF CONFIGURING FILTERS ON OA-700

EXAMPLE 1:

If GigabitEthernet7/0 is the interface positioned to be the outside gateway, the configuration shown below allows traffic initiated from inside and corresponding response coming from outside. It also denies all traffic initiated from outside.

```
match-list m1
  ip any any

ip filter f1
  10 match m1 deny

ip filter f2
  10 match m1 permit

interface GigabitEthernet7/0
  ip filter in f1
  ip filter out f2
```

EXAMPLE 2:

Consider the following example where filter f2 is regarded as stateless. Now, the return traffic will be dropped. For example, HTTP requests from internal network matches m1 in f2, they will be passed to external network. But the HTTP response coming back will be blocked by filter "f1" since previously allowed traffic is stateless (non-reflexive).

```
ip filter f2
  10 match m1 permit
  default deny
  stateless
```

EXAMPLE 3:

If you need to give access from the network 192.168.1.0/24 to 192.168.2.0/24, the CLI would be as follows:

```
match-list m1
  ip prefix 192.168.1.0/24 prefix 192.168.2.0/24 type ftp

ip filter f1
  10 match m1 permit
  default deny
```

MANAGING SECURITY CONFIGURATION

This chapter gives an overview of adding and updating the security configuration. This gives enough flexibility to configure the desired rules with appropriate priorities at any stage.

Refer the following sections on how to update and modify firewall configurations:

- “Insertions”
- “Updates”

INSERTIONS

The following section comprehends with an example as to how a new rule can be inserted within a filter configuration.

TO INSERT A NEW RULE

The need for insertion of match-lists become inevitable when you wish to include one or a group of rules after you have configured the match-lists for a particular application. The following example depicts the way to accomplish this.



Note: Line numbers will not be shown unless you specifically enter it. The line numbers are displayed only in the “**show**” command-view.

EXAMPLE

Consider the following example for inserting another rule in the filter:

```
ip filter f1
  10 match m1 permit
  20 match m2 deny log
  30 match m3 permit

stateless
```

Now to insert another rule, 15 which has its priority in between 10 and 20, use the following syntax:

```
ip filter f1
  15 match m4 deny reset
```

To view the filter f1’s configuration:

```
show ip filter f1
ip filter f1
  10 match m1 permit
  15 match m4 deny reset
  20 match m2 deny log
  30 match m3 permit

stateless
```

UPDATES

The numbering pattern employed by default in the OA-700 is multiples of ten. If a new rule has to be included in between two existing rules, without actually changing the sequence of numbering, use the “**renumber**” keyword.

To change the line number of a pre-defined rule, use the “**change**” keyword. This allows you to just change the line number and not to swap between two numbers.



Note: Line numbers will not be shown unless you specifically type them in. You can view the line numbers only in “**show**” commands.

To NORMALIZE LINE NUMBERS

Use the keyword “renumber” to normalize the line numbers of each rule and set them to the consecutive multiples of 10.

EXAMPLE

Consider the following configuration:

```
ip filter f1
  10 match m1 permit
  15 match m4 deny reset
  20 match m2 deny log
  30 match m3 permit

stateless
```

Here the numbers does not follow the specified order. This becomes more complex when you try to enter another match in between 10 and 15. This creates ambiguity in the flow and in prioritizing the rules. Hence after the insertion of any specific rule, the ordering can be set back to its original manner with the help of the keyword “**renumber**”.

```
ip filter f1
renumber
```

To view the filter configuration after renumbering, give the show command.

```
show ip filter f1
ip filter f1
  10 match m1 permit
  20 match m4 deny reset
  30 match m2 deny log
  40 match m3 permit

stateless
```

To Change the Order of a Rule

Use the keyword “change” to change the order of a rule to the new number position.

EXAMPLE

Consider the following configuration:

```
ip filter f1
  10 match m1 permit
  20 match m2 deny log
  30 match m3 permit
  40 match m4 deny reset
```

In the above sequence, if m4 has a priority 40. Use the “change “ keyword to change the priority of m4.

```
ALU(config)# ip filter f1
ALU(config-filter-f1)# change 40 15
```

To view the filter configuration after changing the priority, use the show command. The output appears as shown:

```
show ip filter f1
ip filter f1
  10 match m1 permit
  15 match m4 deny reset
  20 match m2 deny log
  30 match m3 permit
```

Now, to generate a numbering scheme with a proper order, use the keyword “**renumber**”, as explained in the previous section.

NETWORK ATTACKS - AN OVERVIEW

A Denial-of-service (DoS) attack is a malicious attempt by one or many users to limit or completely disable the availability of a service.

They cost businesses millions of dollars each year and are a serious threat to any system or a network. These costs are related to system downtime, lost revenues and the labour involved in identifying and reacting to such attacks.

Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack. Illegitimate use of resources may also result in denial of service.

For example, an intruder may use anonymous FTP area as a place to store illegal copies of commercial software, consuming disk space and generating network traffic. Denial-of-service attacks come in a variety of forms and aim at a variety of services.

There are three basic types of attacks:

- Consumption of scarce, limited, or non-renewable resources.
- Destruction or alteration of configuration information.
- Physical destruction or alteration of network components.

The OA-700 provides an effective way to prevent these attacks against their networks. The OA-700 employs rate limiting and rule based filtering to prevent these attacks. The following sections describe usage guidelines to configure the system to protect against these attacks.

TYPES OF NETWORK ATTACKS

The following sections give a concise overview on all the rate-limiting and non-rate-limiting attacks that can be prevented by the OA-700. The attacks are further classified into:

- **“Default Attacks (Rate-limiting / Stateful)”**
- **“Default Attacks (Non-rate Limiting / Stateless)”**
- **“Optional Attacks”**

The **Default Attacks** are the ones that are present in the default attack prevention list of the OA-700. These attacks can be either manually turned on for detection or filters can be applied to block them. [“To Configure Default Attacks \(Rate Limiting / Non-rate Limiting\) for an Attack Object”](#)

The **Optional Attacks** are the ones that are not present in the default attack prevention list of the OA-700. These attacks too can be either manually turned on for detection or filters can be applied to block them. [“To Configure Individual Attack for an Attack Object”](#)

DEFAULT ATTACKS (RATE-LIMITING / STATEFUL)

ICMP-DEST-UNRCH-STORM

```
icmp-dest-unrch-storm [ threshold <1-4294967295> <1-4294967295> ]
```

This attack is implicitly a part of the default attack prevention list. However, if you do not want to use these default lists, you can turn on only a selected number of attacks by using their respective keywords with parameters.

ICMP-IP-ADDRESS-SWEEP

```
icmp-ip-address-sweep [ threshold <1-4294967295> <1-4294967295> ]
```

An address sweep attack occurs when one source IP address sends number of ICMP echo requests (or pings) to different hosts within a defined interval. The purpose of this scheme is to ping several hosts in the hope that one will reply, thus uncovering an address to target, resulting in system failure. This command is included in the Alcatel-Lucent's default attack prevention list.

ICMP-PING-FLOOD

```
icmp-ping-flood [ threshold <1-4294967295> <1-4294967295> ]
```

A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to the broadcast addresses performs the IP broadcast to another broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. To secure system from this kind of ping flooding, this command is included in the default attack prevention list.

PORT-SCAN

```
port-scan [ threshold <1-4294967295> <1-4294967295> ]
```

A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

TCP-FIN-SCAN

```
tcp-fin-scan
```

TCP FIN flooding. To secure system from this kind of flooding, this command also forms a part of the default list.

TCP-HEADER-FRAG**tcp-header-frag**

In this attack, a TCP header is split into multiple frames in an attempt to bypass firewalls or intrusion detection systems. This could lead to secure information also being passed through the filter. To retain security, this command is included in the DoS prevention list.

TCP-SYN-FLOOD

```
tcp-syn-flood [ { threshold <1-4294967295> <1-4294967295>
| timeout <1-4294967295> } ]
```

The server builds in its system memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-open connections. Systems providing TCP-based services to the Internet community may be unable to provide services while under this attack and for some time after this attack ceases. To protect the system from this attack, this command is also included in the default attack prevention list.

UDP-FLOOD

```
udp-flood [ threshold <1-4294967295> <1-4294967295> ]
```

A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

UDP-PORT-LOOPBACK

```
udp-port-loopback [ threshold <1-4294967295> <1-4294967295> ]
```

An UDP packet travels between two "echoing" ports. Such packets can bounce infinite number of times, using up network bandwidth and CPU. An intruder can cause problems by spoofing a packet from one machine and send it to another. The malicious intruder could generate lots of these packets in order to totally overwhelm the systems and network. This keyword is included with appropriate parameters in the default list.

DEFAULT ATTACKS (NON-RATE LIMITING / STATELESS)

ICMP-PING-OF-DEATH

```
icmp-ping-of-death [ {max-frag-num|max-total-length} <1-4294967295> ]
```

The TCP/IP specification requires a specific packet size for datagram transmission. Many ping implementations allow you to specify a larger packet size if desired. A grossly oversized ICMP packet can trigger a range of adverse system reactions such as denial of service (DoS), crashing, freezing, and rebooting. This command is included in the default attack prevention list to secure the system from this attack.

IP-LAND-ATTACK

```
ip-land-attack
```

A LAND attack consists of a stream of TCP SYN packets that have the source IP address and TCP port number set to the same value as the destination address and port number (i.e., that of the attacked host).

IP-TEAR-DROP

```
ip-tear-drop
```

Teardrop attack tool attacks the vulnerability of the TCP/IP IP fragmentation re-assembly codes which do not properly handle the overlapping IP fragments.

IP-TINY-FRAG

```
ip-tiny-frag [ {max-frag-num|min-frag-size} <1-4294967295> ]
```

If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn't hit a match in the filter. The above keyword is also turned on by default. If you wish to disable this, you can override this keyword and then turn it on when necessary with a specified minimum fragment size in the user-defined attack prevention list.

IP-ZERO-LENGTH

```
ip-zero-length
```

This kind of denial of service attack is caused when a 0-length IP fragment is received as the first fragment in the list.

A series of such IP fragments of 0 length being the first in the fragment list, makes it impossible for the kernel to deallocate the destination entry and remove it from the cache, resulting in a Denial -of Service. To avoid the attack, this keyword is also placed in the default list.

TCP-FIN-NO-ACK**tcp-fin-no-ack**

TCP packets without ACK set for FIN. This leads to system crashing at times. To avoid this mishap, the above command is also present in the default DoS prevention list.

TCP-INVALID-URGENT-OFFSET**tcp-invalid-urgent-offset**

The intruder sends a TCP frame with an Urgent pointer which points past the end of the data. This may cause some TCP/IP implementations to become unstable or crash. Some TCP/IP implementations will hang when receiving many such frames. Inclusion of this command avoids such attacks.

TCP-NULL-SCAN**tcp-null-scan**

TCP packets w/o any flag set. Leads to inability to scan such packets. This attack is avoided since it is also included in the default DoS prevention list.

TCP-SYN-FIN**tcp-syn-fin**

This has TCP packets with both SYN and FIN flag set, causing a denial of service. This attack is prevented by using the "default" keyword or can be inserted in the user-defined list.

TCP-XMAS-SCAN**tcp-xmas-scan**

This frame should never be seen in normal TCP operation. Sometimes this is done in preparation for a future attack, or sometimes it is done to see if the system has a service which is susceptible to attack. A TCP frame has been seen with a sequence number of zero and the FIN, URG, and PUSH bits all set. To avoid this attack the above command is placed in the default DoS prevention list.

UDP-FRAGGLE-ATTACK**udp-fraggle-attack**

When a perpetrator sends a large number of UDP echo (ping) traffic at IP broadcast addresses, all of it having a fake source address, it causes system crash or denial of service. This command is implicitly included in the default attack prevention list to secure the system from this attack.

OPTIONAL ATTACKS

The following four DoS attacks are not set for prevention by default. These attacks too can be either manually turned on for detection or filters can be applied to block them.

ICMP-BLOCK-TRACE-ROUTE

`icmp-block-trace-route`

This command is not a default DoS setting. The square brackets around the whole command denotes its only optional. This means that this attack is not set for protection by default in the *OA-700*, but you can turn it on by explicitly adding the above keyword in the user-defined attack prevention list.

ICMP-ROUTER-ADVERTISEMENT

`icmp-router-advertisement`

Remote attackers can spoof these ICMP packets and remotely add bad default-route entries into a victims routing table. Since the victim's system would be forwarding the frames to the wrong address, it will be unable to reach other networks. This attack can be prevented by adding this command in the DoS prevention list.

ICMP-REDIRECT

`icmp-redirect`

This command is not a default DoS setting. The square brackets around the whole command denotes its only optional. However the above command can be included in the DoS prevention list to avoid this kind of attacks.

IP-SOURCE-ROUTING

`ip-source-routing`

Source routing is a technique whereby the sender of a packet can specify the route that a packet should take through the network. Attackers can use source routing to probe the network by forcing packets into specific parts of the network. Using source routing, an attacker can collect information about a networks topology, or other information that could be useful in performing an attack. During an attack, an attacker could use source routing to direct packets to bypass existing security restrictions. This command is included in the default attack protection list to secure the network from this attack.

IP-SPOOFING

ip-spoofing

To gain access, intruders create packets with spoofed source IP addresses. This exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall. After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts. This command is not included in the default attack list. Can be explicitly included to secure the network from this attack.

UDP-SNORK-ATTACK

udp-snork-attack

This is an attempt to connect two services which, if enabled, will engage in an indefinite communication with each other.

This will cause many frames to be unnecessarily transmitted, and dramatically reduce the performance of the network and the systems involved. To avoid this Denial of Service overload attempt, this command is placed in the default prevention list.

NETWORK ATTACK PREVENTION CONFIGURATION

Refer the following section to prevent network attack:

- [“Network Attack Prevention Configuration Steps”](#)
- [“Network Attack Prevention Configuration Flow”](#)

NETWORK ATTACK PREVENTION CONFIGURATION STEPS

This section lists the steps to be followed to prevent network attacks.

Step 1: Configure the match-lists with the common classifiers pre-configured. (Refer to the chapter [“Common Classifiers”](#) in this guide).

Step 2: Enter the Firewall Sub Configuration Mode. See [“To Enter Firewall Configuration Mode”](#)

Step 3: Configure DoS attack Object. This enters the Attack Sub Configuration Mode. See [“To Configure DoS Attack Object”](#)

Step 4: Configure attacks to the configured attack object. See [“To Configure Default Attacks \(Rate Limiting / Non-rate Limiting\) for an Attack Object”](#)

OR

[“To Configure All Attacks for an Attack Object \(Including Default / Optional\)”](#)

OR

[“To Configure Individual Attack for an Attack Object”](#)

Step 5: Exit from the Attack Sub Configuration Mode

Step 6: Configure Firewall Policy. See [“To Configure Firewall Policy”](#)

- To create a DoS Rule inside a Firewall Policy. See [“To Create a DoS Rule Inside a Firewall Policy”](#)

Attach a Firewall Policy to an Interface

Step 7: Enter into Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 8: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 9: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-  
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address  
20.20.20.20/24
```

Step 10: Attach the configured firewall policies to appropriate interfaces as per the desired direction i.e, either "IN/OUT". See ["To Attach a Firewall Policy to an Interface"](#)

Step 11: View the firewall configuration. See ["Firewall Show Commands"](#)

Step 12: Delete the firewall configuration. See ["Firewall Deletion Commands"](#)

NETWORK ATTACK PREVENTION CONFIGURATION FLOW

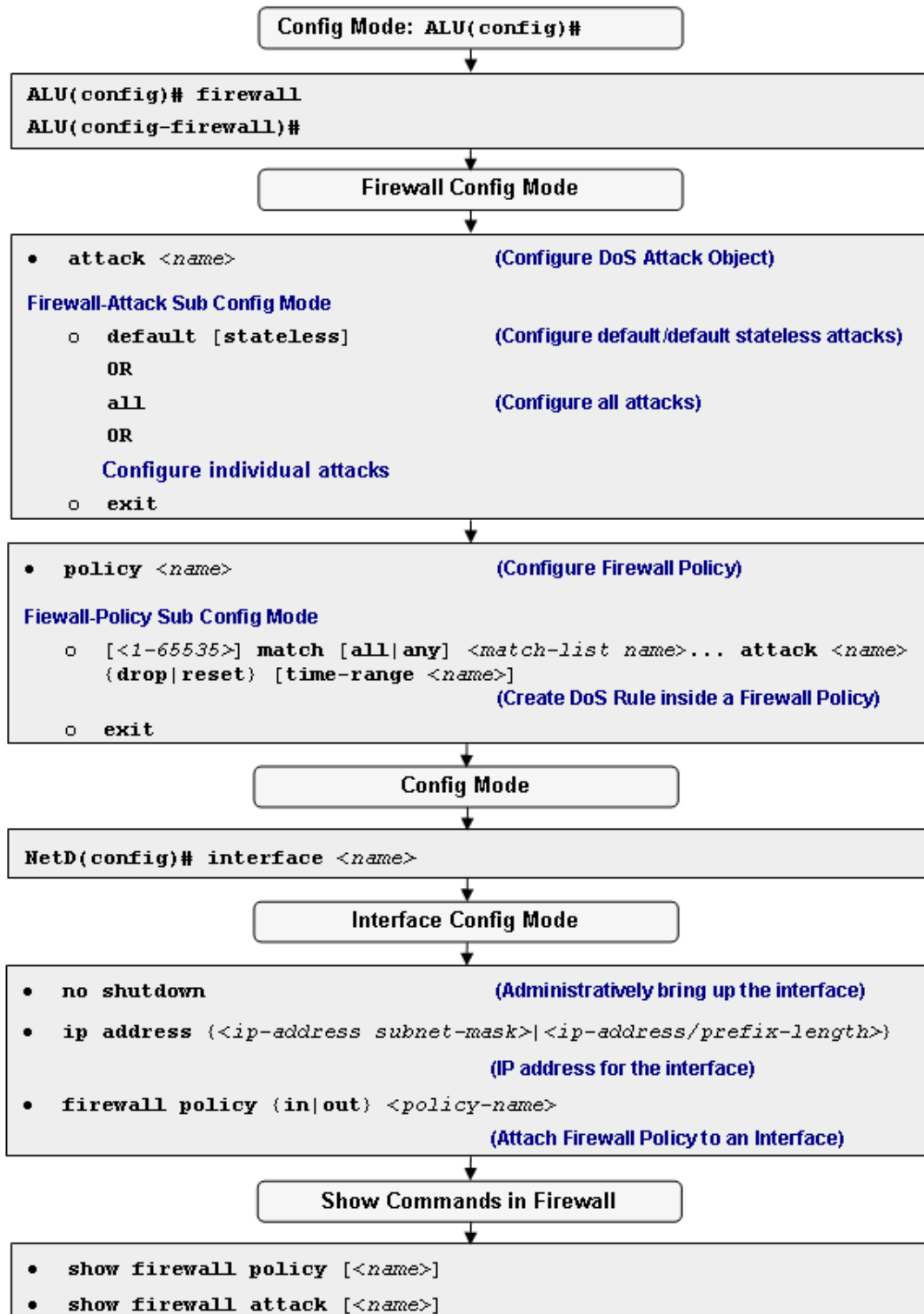


Figure 52: Network Attack Prevention Flowchart

NETWORK ATTACK PREVENTION CONFIGURATION COMMANDS

This section provides the commands used to prevent network attacks.

TO ENTER FIREWALL CONFIGURATION MODE

Command (in CM)	Description
<code>firewall</code>	This command enters the firewall configuration mode.

EXAMPLE

```
ALU(config)# firewall
ALU(config-firewall)#
```

TO CONFIGURE DoS ATTACK OBJECT

Command (in FwCM)	Description
<code>attack <name></code>	This command is used to configure an attack object to be attached to a firewall policy.

EXAMPLE

```
ALU(config-firewall)# attack A1
ALU(config-firewall-attack-A1)#
```

TO CONFIGURE DEFAULT ATTACKS (RATE LIMITING / NON-RATE LIMITING) FOR AN ATTACK OBJECT

During system bootup, an attack object and a policy map is created by the system. These are the **System-default Attack Object** and the **System-default Policy**. This system-default policy is attached to the system-default attack object, and by default is attached to the system traffic.

Note:

1. You can only modify the system default attack object but cannot delete it.
2. You cannot modify/delete the system default policy.
3. You can modify/delete the user created attack objects and the attack policies associated to it.

Command (in F-ACM)	Description
default [stateless]	This command is used to configure all the default attacks for an attack object. <ul style="list-style-type: none"> • Default keyword configures all the Default Rate Limiting attacks (i.e., both Stateful and Stateless attacks) • Stateless keyword configures only the Default Non-rate Limiting (i.e., only Stateless attacks.)
no default [stateless]	The 'no' command disables all the default attacks configured for an attack object. Stateless keyword disables only the stateless default attacks.

EXAMPLE

```

ALU(config-firewall-attack-A1)# default

ALU(config-firewall-attack-A1)# default stateless

ALU(config-firewall-attack-A1)# no default

ALU(config-firewall-attack-A1)# no default stateless

```

You can create a “**default**” attack setting to check default attacks on ingress traffic to all interfaces.

In the OA-700, the default DoS attack is configured for the prevention of all attacks and their default settings except "**icmp-block-trace-route**", "**icmp-router-advertisement**", "**icmp-redirect**" and "**ip-rate-threshold**". These attacks too can be either manually turned on for detection or filters can be applied to block them. The minimum time resolution you can enter is 5 milliseconds.

The following attacks are the Default attacks (Rate Limiting attacks, which includes both Stateful and Stateless attacks):

tcp_header_frag	-	-
udp_header_frag	-	-
tcp_fin_scan	-	-
tcp_syn_flood	100	1000 5
icmp_ping_flood	100	1000
icmp_dest_unrch_storm	10	1000
icmp_ip_address_sweep	100	1000
port_scan	5	1000
udp_flood	200	1000
udp-port-loopback	10	1000
ip-tear-drop	-	-
ip-tiny-frag	50	64
icmp-ping-of-death	50	65507
ip-zero-length	-	-
ip-land-attack	-	-
tcp-xmas-scan	-	-
tcp_-invalid-urgent-offset	-	-
tcp-null-scan	-	-
tcp-syn-fin	-	-
tcp-fin-no-ack	-	-
udp-fraggle-attack	-	-

You can create a “**default**” attack setting to check only the stateless attacks by using the keyword “**default stateless**”.

The following attacks are the Default Stateless (Default Non-Rate Limiting) attacks:

ip-tear-drop	-	-
ip-tiny-frag	50	64
icmp-ping-of-death	50	65507
ip-zero-length	-	-
ip-land-attack	-	-
tcp-xmas-scan	-	-
tcp_-invalid-urgent-offset	-	-
tcp-null-scan	-	-
tcp-syn-fin	-	-
tcp-fin-no-ack	-	-
udp-fraggle-attack	-	-



Note: Some of the fragmentation attacks, in particular teardrop attack, tiny fragment attack, and TCP header fragment attacks are detected by the fragment handling code even if the corresponding attacks have not been configured. This will happen for any traffic that is subject to any firewall configuration, i.e., either filter, NAT or DoS configuration. This is why you can see these attacks in the “**show**” output even when you have not configured them.

To CONFIGURE ALL ATTACKS FOR AN ATTACK OBJECT (INCLUDING DEFAULT / OPTIONAL)

Command (in F-ACM)	Description
all	This command is used to configure all the attacks (including all Default and Optional attacks) for an attack object.
no all	The 'no' command disables all the attacks configured for an attack object.

EXAMPLE

```
ALU(config-firewall-attack-A1)# all
```

```
ALU(config-firewall-attack-A1)# no all
```

The following are the Optional attacks that are not present in the default attack prevention list of the OA-700:

```
icmp_router_advertisement
icmp_redirect
ip_spoofing
icmp_block_trace_route
ip_source_routing
udp_snork_attack
```

To CONFIGURE INDIVIDUAL ATTACK FOR AN ATTACK OBJECT

The following command enables you to configure attacks (both Default - stateful and stateless and Optional attacks) individually for an attack object.

Command (in F-ACM)	Description
udp-port-loopback [threshold <1-4294967295> <1-4294967295>]	This command is used to configure udp-port-loopback attack for an attack object.
udp-flood [threshold <1-4294967295> <1-4294967295>]	This command is used to configure udp-flood attack for an attack object.
port-scan [threshold <1-4294967295> <1-4294967295>]	This command is used to configure port-scan attack for an attack object.
tcp-fin-scan	This command is used to configure tcp-fin-scan attack for an attack object.
icmp-ip-address-sweep [threshold <1-4294967295> <1-4294967295>]	This command is used to configure icmp-ip-address-sweep attack for an attack object.
icmp-dest-unrch-storm [threshold <1-4294967295> <1-4294967295>]	This command is used to configure icmp-dest-unrch-storm attack for an attack object.

Command (in F-ACM)	Description
<code>icmp-ping-flood [threshold <1-4294967295> <1-4294967295>]</code>	This command is used to configure icmp-ping-flood attack for an attack object.
<code>tcp-syn-flood [{threshold <1-4294967295> <1-4294967295> timeout <1-4294967295>}]</code>	This command is used to configure tcp-syn-flood attack for an attack object.
<code>udp-fraggle-attack</code>	This command is used to configure udp-fraggle-attack for an attack object.
<code>udp-snork-attack</code>	This command is used to configure udp-snork-attack for an attack object.
<code>tcp-fin-no-ack</code>	This command is used to configure tcp-fin-no-ack attack for an attack object.
<code>tcp-syn-fin</code>	This command is used to configure tcp-syn-fin attack for an attack object.
<code>tcp-null-scan</code>	This command is used to configure tcp-null-scan attack for an attack object.
<code>tcp-invalid-urgent-offset</code>	This command is used to configure tcp-invalid-urgent-offset attack for an attack object.
<code>tcp-xmas-scan</code>	This command is used to configure tcp-xmas-scan attack for an attack object.
<code>ip-land-attack</code>	This command is used to configure ip-land-attack for an attack object.
<code>ip-source-routing</code>	This command is used to configure ip-source-routing attack for an attack object.
<code>icmp-block-trace-route</code>	This command is used to configure icmp-block-trace-route attack for an attack object.
<code>ip-spoofing</code>	This command is used to configure ip-spoofing attack for an attack object.
<code>icmp-redirect</code>	This command is used to configure icmp-redirect attack for an attack object.
<code>icmp-router-advertisement</code>	This command is used to configure icmp-router-advertisement attack for an attack object.
<code>tcp-header-frag</code>	This command is used to configure tcp-header-frag attack for an attack object.
<code>ip-zero-length</code>	This command is used to configure ip-zero-length attack for an attack object.

Command (in F-ACM)	Description
<code>ip-tiny-frag [{max-frag-num min-frag-size} <1-4294967295>]</code>	This command is used to configure ip-tiny-frag attack for an attack object.
<code>icmp-ping-of-death [{max-frag-num max-total-length} <1-4294967295>]</code>	This command is used to configure icmp-ping-of-death attack for an attack object.
<code>ip-tear-drop</code>	This command is used to configure ip-tear-drop attack for an attack object.

EXAMPLE

```
ALU(config-firewall-attack-A1)# ip-tear-drop
```



Note: The 'no' command disables the individual attack configured for an attack object.
Example:

```
ALU(config-firewall-attack-A1)# no ip-tear-drop
```



Note: You can also modify the System Default Attack Object by entering into the system-default attack object.

E.g.

```
ALU(config-firewall)# attack system-default
```

```
ALU(config-firewall-attack-system-default)# all
```

TO LOG ALL THE ATTACKS

Command (in F-ACM)	Description
<code>log</code>	This command logs all the attacks in the log server.
<code>no log</code>	This 'no' command disables logging of the attacks.

EXAMPLE

```
ALU(config-firewall-attack-A1)# log
```

```
ALU(config-firewall-attack-A1)# no log
```

To CONFIGURE FIREWALL POLICY

Command (in FwCM)	Description
<code>policy <name></code>	Enter this command in the Firewall Configuration Mode. This command is used to configure a firewall policy. This enters the firewall policy sub-configuration mode

EXAMPLE

The following example depicts firewall policy configuration:

```
ALU(config-firewall)# policy P1
ALU(config-firewall-P1)#
```

To CREATE A DoS RULE INSIDE A FIREWALL POLICY

Command (in F-PCM)	Description
<code>[<1-65535>] match {any all} <match-list name>... attack <name> {drop reset} [time-range <name>]</code>	Enter this command in the Firewall Policy Configuration Mode. This command is used to attach an attack object to a firewall policy, and create rules (associate match-lists and set priority for the rule) for a firewall policy, and also set the action drop or reset for the configured rules. The range for the rule number is 1-65535. This rule number signifies the priority of a rule. By default, the numbering pattern for rule number is the next multiple of ten to the highest existing rule number. The keyword “ drop ” drops the packets, and “ reset ” also drops the packets but sends an error message or an acknowledgement to the sender.



Note: Currently, multiple match-lists cannot be associated to a firewall policy rule. To configure more than one match-list within a firewall policy, add multiple rules with different match-lists.

EXAMPLE

In the following example, the attack object **atk** is configured to drop all the attacks:

```
ALU(config-firewall-P1)# 10 match m1 attack atk drop
```

In the following example, the attack object **atk** is configured to drop all the attacks and send acknowledgement such as an error report.

```
ALU(config-firewall-P1)# match m1 attack atk reset
```

TO REORDER THE RULES IN THE FIREWALL POLICY

Command (in F-PCM)	Description
renumber	Use this command to generate a numbering scheme for the firewall policy rules configured.
change {<1-65535> <1-65535>}	Use this command to change the priority of a specific firewall policy rule configured.

EXAMPLE

Consider the following configuration:

```
ALU(config)# firewall
ALU(config-firewall)# policy P1
ALU(config-firewall-P1)#
  10 match m1 permit
  20 match m2 deny log
  30 match m3 permit
  40 match m4 deny reset
```

In the above sequence, if m4 has a priority 40. Use the “change “ keyword to change the priority of m4.

```
ALU(config-firewall)# policy P1
ALU(config-firewall-P1)# change 40 15
```

To view the policy configuration after changing the priority, give the show command. The output appears as shown:

```
show firewall policy P1
ip policy P1
  10 match m1 permit
  15 match m4 deny reset
  20 match m2 deny log
  30 match m3 permit
```

Now, to generate a numbering scheme with a proper order, use the keyword “**renumber**” as follows:

```
ALU(config-firewall)# policy P1
ALU(config-firewall-P1)# renumber
```

To view the filter configuration after renumbering, use the show command. The output appears as shown:

```
show firewall policy p1
ip policy P1
  10 match m1 permit
  20 match m4 deny reset
  30 match m2 deny log
  40 match m3 permit
```

TO ATTACH A FIREWALL POLICY TO AN INTERFACE

Command (in ICM)	Description
<code>firewall policy {in out} <policy-name></code>	<p>This command is used to attach a firewall policy to an interface in 'in' or 'out' direction.</p> <p>Firewall policy is applied to the ingress (incoming) traffic if "in" keyword is used.</p> <p>Firewall policy is applied to the egress (outgoing) traffic if "out" keyword is used.</p>



Note: Firewall policy will take into effect once it is attached to an interface.

EXAMPLE

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# firewall policy in P1
```

FIREWALL SESSION COMMANDS

To MODIFY DEFAULT TIME-OUT VALUES

Command (in Firewall Session Mode)	Description
<code>default timeout {icmp tcp udp}</code> <code><0-2147483648></code>	Enter this command in the Firewall Session Configuration Mode. Firewall session table has a periodic timer to age out inactive entries. To change these default values, use this command. Timeout value '0' stands for infinity.

- Default TCP value is 15 minutes
- Default UDP value is 5 minutes.
- Default ICMP value is 30 seconds.

EXAMPLE

```
ALU(config-firewall)# session
ALU(config-firewall-session)# default timeout tcp 10
```

FIREWALL SHOW COMMANDS

Use the following show commands to monitor and troubleshoot firewall on your OA-700.



Note: Show commands can be issued either in the Super User Mode or in the firewall sub-configuration mode.

TO VIEW FIREWALL POLICY DETAILS

Command (in SUM)	Description
<code>show firewall policy [<name>]</code>	This command is used to view all the firewall policy details configured. This command is also used to view the details of a specific firewall policy.

EXAMPLE

To view the firewall policy details, use the following syntax:

```
ALU# show firewall policy P1

policy P1
  10 match any dos attack P1 drop
interface GigabitEthernet7/0 In
```

TO VIEW THE ATTACK COMPONENTS

Command (in SUM)	Description
<code>show firewall attack [<name>]</code>	This command is used to view all the DoS attacks details. This command can also be used to view the details of a specific attack object

EXAMPLE

The following syntax is used to view the details of attack A1:

```
ALU# show firewall attack A1

attack A1
  udp-port-loopback          10 1000
  udp-flood                   200 1000
  tcp-fin-scan                 - -
  icmp-ip-address-sweep       2 10
  icmp-dest-unrch-storm       2 10
  icmp-ping-flood             2 10
  tcp-syn-flood               100 1000 5
  udp-fraggle-attack          - -
```

```

udp-snork-attack          -   -
tcp-fin-no-ack            -   -
tcp-syn-fin              -   -
tcp-null-scan            -   -
tcp-invalid-urgent-offset -   -
tcp-xmas-scan            -   -
ip-land-attack           -   -
ip-source-routing        -   -
icmp-block-trace-route   -   -
ip-spoofing              -   -
icmp-redirect            -   -
icmp-router-advertisement -   -
tcp-header-frag          -   -
ip-zero-length           -   -
ip-tiny-frag             50  64
icmp-ping-of-death       50  65507
ip-tear-drop             -   -

```

To View the Firewall Session Details

Command (in SUM)	Description
<code>show firewall session</code>	This command is used to view all the firewall sessions used by the system.
<code>show firewall session detail</code>	This command is used to view all the firewall sessions in a detailed format.

EXAMPLE

To view the firewall session, use the following syntax:

```
ALU# show firewall session
```

```

TCP Sessions      : 0
UDP Sessions      : 0
ICMP Sessions     : 1
GRE Sessions      : 0
Total Sessions    : 1
Free Sessions     : 127999

```

The following syntax is used to view the details of firewall session

```
ALU(config)# show firewall session detail
```

```

ID 70 ICMP timeout 28 secs, used by NAT
Initiator: (10.91.1.108:13)=>(10.91.0.1:13)
Responder: (10.91.0.1:34416)=>(10.91.1.108:34416)

```

To VIEW THE SESSION PROTOCOL

Command (in SUM)	Description
<code>show firewall session [proto {tcp udp icmp}]</code>	This command displays the firewall sessions with respect to the protocol type.

EXAMPLE

The following syntax is used to view the details of firewall session with respect to TCP protocol:

```
ALU(config)# show firewall session proto icmp
```

```
ID 70 ICMP timeout 19 secs, used by NAT
Initiator: (10.91.1.108:13)=>(10.91.0.1:13)
Responder: (10.91.0.1:34416)=>(10.91.1.108:34416)
```

To VIEW SESSION DETAILS WITH SOURCE - DESTINATION GIVEN

Command (in SUM)	Description
<code>show firewall session [source {<ip-address> <ip-address/prefix-length>} [<1-65535>]]</code>	This command is used to view the firewall session details given the source address.
<code>show firewall session [destination {<ip-address> <ip-address/prefix-length>} [{<1-65535>}/proto {gre icmp tcp udp}]</code>	This command is used to view the firewall session details given the destination address.

EXAMPLE

```
ALU(config-if GigabitEthernet7/1)# show firewall session source
10.91.1.108
```

```
ID 70 ICMP timeout 25 secs, used by NAT
Initiator: (10.91.1.108:13)=>(10.91.0.1:13)
Responder: (10.91.0.1:34416)=>(10.91.1.108:34416)
```

```
ALU(config-if GigabitEthernet7/1)#show firewall session
destination ip 10.91.0.1
```

```
ID 70 ICMP timeout 25 secs, used by NAT
Initiator: (10.91.1.108:13)=>(10.91.0.1:13)
Responder: (10.91.0.1:34416)=>(10.91.1.108:34416)
```

FIREWALL DELETION COMMANDS

This section lists the firewall deletion commands.

TO DETACH A FIREWALL POLICY FROM AN INTERFACE

Command (in ICM)	Description
<code>no firewall policy {in out} <name></code>	<p>This command detaches a firewall policy attached to an interface.</p> <p>This command does not delete the firewall policy definition in its entirety. It only detaches it from its interface.</p> <p>If the command "no firewall policy name" is issued at the top level and if this firewall policy is not bound to any interface, it deletes the firewall policy definition.</p>

EXAMPLE

The following syntax detaches the firewall policy "P1":

```
ALU(config-if GigabitEthernet7/0)# no firewall policy in P1
```

TO DELETE A FIREWALL POLICY

Command (in FwCM)	Description
<code>no policy <name> force</code>	<p>Enter this command in the Firewall Configuration Mode.</p> <p>The "force" keyword will automatically detach the specified policy from respective interfaces, and deletes the firewall policy. This command when used also deletes all policy rules.</p>

EXAMPLE

```
ALU(config)# no policy P1 force
```

TO DELETE A SPECIFIC FIREWALL POLICY RULE

Command (in F-PCM)	Description
<code>no rule <1-65535></code>	This deletes only the rule in the firewall policy corresponding to the line number.

EXAMPLE

```
ALU(config-firewall-P1)# no rule 30
```

TO DELETE A DoS ATTACK OBJECT

Command (in FCM)	Description
<code>no attack <name></code>	This deletes the specified DoS attack object and its configuration. You cannot delete an attack object if it is attached to an interface.

EXAMPLE

```
ALU(config-firewall)# no attack A1
```

TO GLOBALLY DELETE AN ATTACK OBJECT

Command (in CM)	Description
<code>no attack <name> force</code>	This deletes a specified DoS attack object from the global level.

EXAMPLE

```
ALU(config)# no attack A1 force
```

TO VIEW THE SYSTEM DEFAULT POLICY

Command (in SUM)	Description
<code>show firewall policy system-default</code>	This command is used to view the system default policy configuration.

EXAMPLE

```
ALU# show firewall policy system-default

policy system-default
    10 match all attack system-default drop
system-traffic firewall policy system-default
```


To View System Default Attacks

Command (in SUM)	Description
<code>show firewall attack system-default</code>	This command is used to view the attacks configured for the system default attack object.

EXAMPLE

ALU# `show firewall attack system-default`

```

attack system-default
  udp-port-loopback          10 1000
  udp-flood                  200 1000
  port-scan                  5 1000
  tcp-fin-scan                - -
  icmp-ip-address-sweep     100 1000
  icmp-dest-unrch-storm     10 1000
  icmp-ping-flood           100 1000
  tcp-syn-flood              100 1000 5
  udp-fraggle-attack        - -
  tcp-fin-no-ack             - -
  tcp-syn-fin                - -
  tcp-null-scan              - -
  tcp-invalid-urgent-offset - -
  tcp-xmas-scan              - -
  ip-land-attack             - -
  icmp-echo-storm-attack    - -
  udp-short-header           - -
  tcp-header-frag           - -
  ip-zero-length             - -
  ip-tiny-frag               50 64
  icmp-ping-of-death         50 65506
  ip-tear-drop               - -

```

Note:

1. The “show running configuration” command does not display the system default policy.
2. The “show running configuration” command displays only the newly created/non default attacks for the system default attack object. The deleted default attacks are displayed with a prefix “no”, and the modified default attacks are displayed with the modified parameters.

FIREWALL DEBUG COMMANDS

This section lists the debug commands in firewall.

To ENABLE/DISABLE DEBUGGING ON FIREWALL

Command (in SUM)	Description
<pre>debug firewall {session filter nat attack alg intrusion selector [saddr <ip-address> daddr <ip- address> protocol <number> sport <number> dport <number>][output permanent] all [detail-level]}</pre>	<p>Use this command to turn on debugging for specified firewall features.</p> <p>The “selector” keyword allows you to debug only selected traffic.</p>
<pre>no debug firewall {session filter nat attack alg intrusion selector [saddr <ip-address> daddr <ip- address> protocol <number> sport <number> dport <number>][output permanent] all [detail-level]}</pre>	<p>Use this command to turn off the debugging functionality.</p> <p>The “selector” keyword allows you to turn off debugging only for selected traffic.</p>

- Notes:**
1. **saddr** == source address
 2. **daddr** == destination address
 3. **sport** == source port
 4. **dport** == destination port

EXAMPLE

The example below enables debugging for the source IP 10.91.0.52

```
ALU# debug firewall selector saddr 10.91.0.52
```

The example below disables debugging for the source IP 10.91.0.52

```
ALU# no debug firewall selector saddr 10.91.0.52
```

SAMPLE FIREWALL POLICY CONFIGURATIONS ON OA-700

EXAMPLE 1

As the default setting, detection of all stateless attacks with logging is applied at the ingress path of all interfaces. To be exact, the following is the default setting for a brand new box out of factory:

```
match-list everything
ip any any type any

firewall
  attack a1
  default stateless

policy p1
  match everything attack a1 reset

interface GigabitEthernet7/0
  firewall policy in p1
```

EXAMPLE 2

This example checks traffic from outside-zone to inside-zone for attacks defined in "d1". If found, TCP RST will be sent to both source and destination for TCP traffic. Packets will be dropped for non-TCP traffic.

```
list outside-zone interface GigabitEthernet7/0
GigabitEthernet3/0
list inside-zone interface GigabitEthernet7/1

match-list m1
  tcp list outside-zone list inside-zone type ftp

firewall
  attack d1
  default

policy p1
  match m1 attack d1 reset

interface GigabitEthernet7/0
  firewall policy in p1
```

EXAMPLE 3

The following configuration selectively checks traffic from GigabitEthernet3/0 to subnet 10.0.0.0/8 for all default attacks:

```
match-list m2
  ip any prefix 10.0.0.0/8 type any

firewall
  attack a2
  default

policy p2
  match m2 attack a2 reset

interface GigabitEthernet3/0
  firewall policy in p2
```

ZONE CONFIGURATION

Refer to following sections for detailed spectrum on configuring zones:

- [“Trusted Zone Configuration” on page 623](#)
- [“Untrusted Zone Configuration” on page 623](#)
- [“Semi-trusted Zone or Demilitarized Zone” on page 624](#)

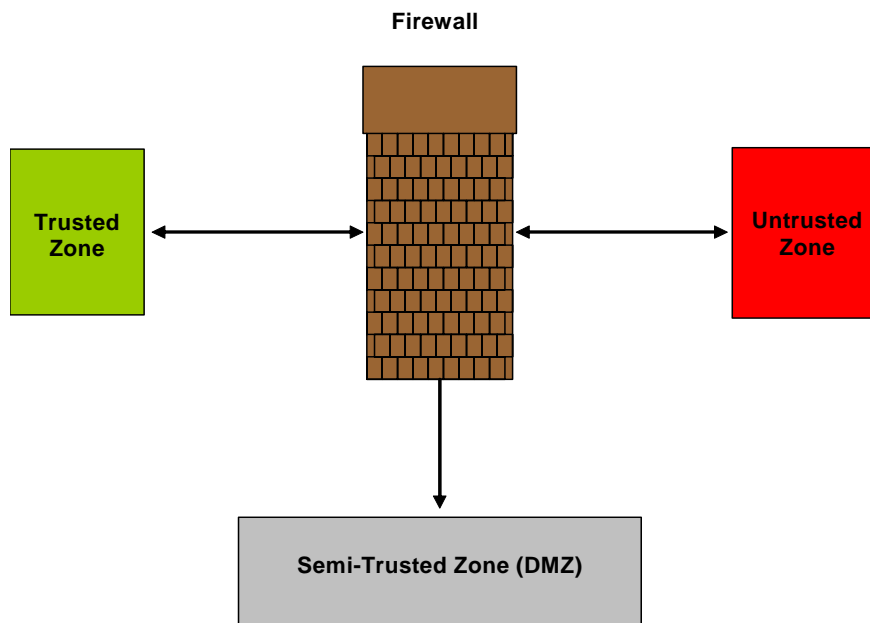


Figure 53: Figure Depicting Three Zones

TRUSTED ZONE CONFIGURATION

The "Trusted Zone" is a network domain in which the users and systems are known entities and hence, communication between the known entities is conducted in an environment of integrity. Hence, data presented from resulting communication is not checked for malicious content or intent. In a corporate network, all systems within the domain of the company is considered to be within a "trusted zone".

UNTRUSTED ZONE CONFIGURATION

The domain falling outside the "trusted zone" is the "untrusted zone". Hence, external networks which comprise traffic or systems that are not within the administrative purview of a private network, such as the Internet, is an example of "untrusted zone".

SEMI-TRUSTED ZONE OR DEMILITARIZED ZONE

A Demilitarized Zone (DMZ) is a network attached to an internetworking device on the border of a "trusted" and "untrusted" zones. This network typically comprises the servers and related network resources that need exposure to the "untrusted" zone without compromising security of a "trusted" zone.

A DMZ creates a buffer space between the Internet and the private network which is accessed by both Internet and the internal network. A DMZ typically contains the following:

- Web Server
- Mail Server
- Application Gateway
- E-Commerce Systems

Example of systems to place on a DMZ include Web servers and FTP servers.

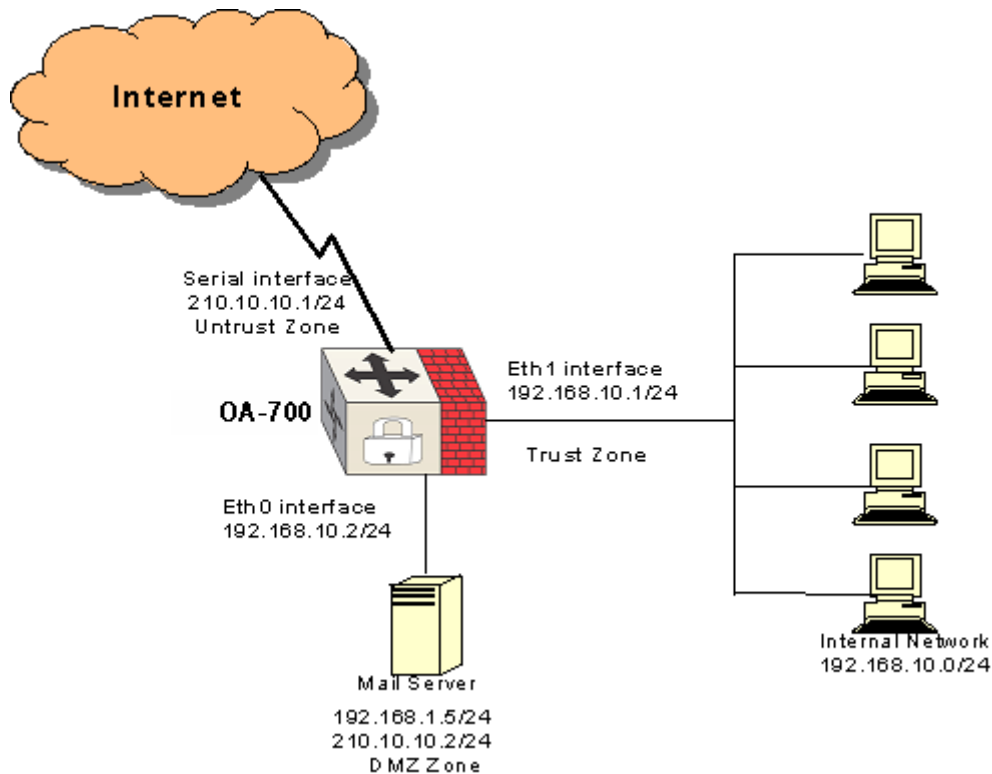


Figure 54: Three - Zone Network Topology

THREE ZONE FIREWALL EXAMPLE

SCENARIO

1. The network has a network of nodes, a mail server, a web server, and access to the internet using a leased line with a static IP.
2. The LAN nodes are designated and placed in the trusted zone.
3. The mail server and web server need to be accessed from the Internet and the local LAN. Since these servers are exposed in some form to the Internet, they are placed in the DMZ.
4. All traffic going out to the Internet is subject to NAT.

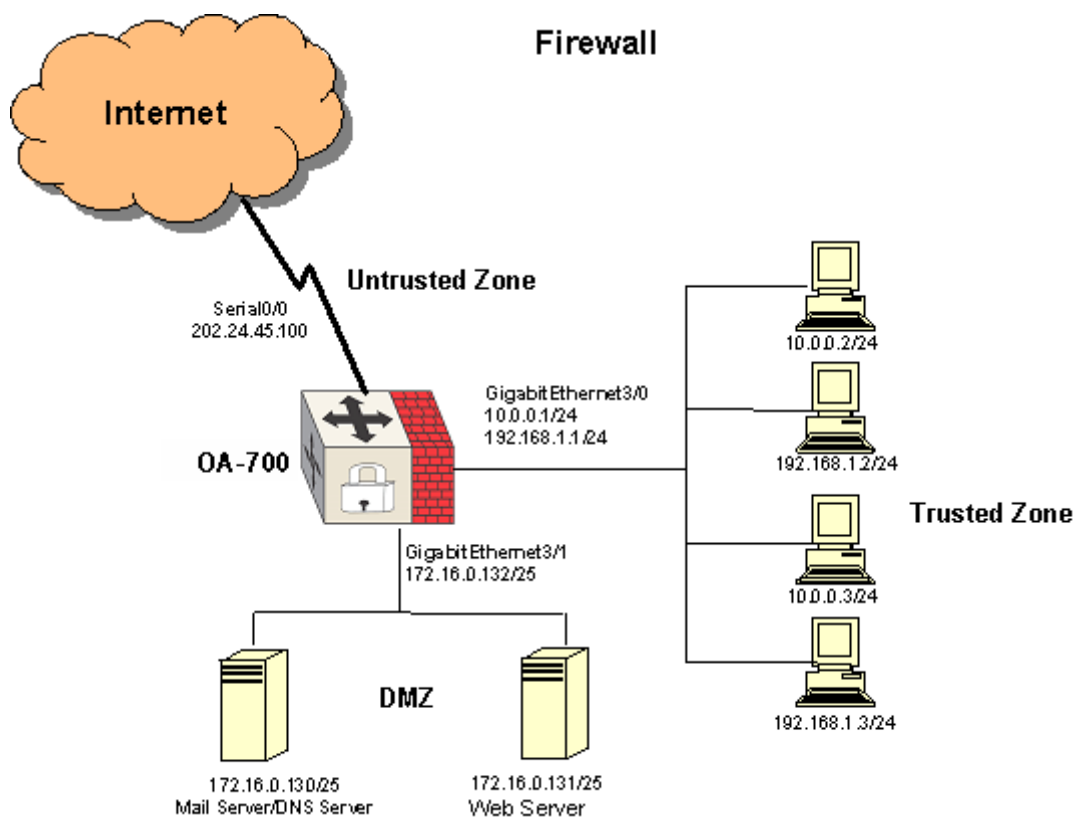


Figure 55: Three Zone Firewall Network Topology

POLICIES THAT NEED TO BE FORMULATED

Serial Number	From	To	Allow
1.	Trusted/LAN	DMZ	All services
2.	Untrusted/Internet	Mail server in DMZ	SMTP, POP, IMAP, HTTP, HTTPS, DNS.
3.	Untrusted/Internet	Web server in DMZ	HTTP, HTTPS, DNS, FTP.
4.	Trusted/LAN	Internet	All services
5.	DMZ	Internet/Untrusted	SMTP, DNS
6.	DMZ/Internet	Trusted/LAN	Nil

- Apart from this, the DMZ has to be protected from DoS attacks.
- Checks have to be done on LAN ports for traffic from valid IP addresses. RFC1918 addresses from the Internet have to be discarded.
- ICMP rate limiting to be applied to 2/second.

IP ADDRESSING SCHEME

1. LAN addresses fall in 3 subnets
 - 10.0.0.0/24
 - 192.168.0.0/24
 - 172.16.0.0/25
2. The Public IP of the link is 202.24.45.100. This is forwarded to Mail Server and Web Server using NAT.

OA-700 CONFIGURATION FOR THE ABOVE SCENARIO

1. CONFIGURE IP ADDRESSES ON THE SPECIFIC INTERFACES

```

ALU#configure
ALU(config)#interface GigabitEthernet 3/0
ALU(config-if GigabitEthernet3/0)#no shutdown
ALU(config-if GigabitEthernet3/0)#ip address 10.0.0.1/24
ALU(config-if GigabitEthernet3/0)#ip address 192.168.1.1/24
secondary
ALU(config-if GigabitEthernet3/0)#ip address 172.16.0.1/25
secondary

ALU(config-if GigabitEthernet3/0)#interface GigabitEthernet
3/1
ALU(config-if GigabitEthernet3/1)#no shutdown
ALU(config-if GigabitEthernet3/1)#ip address 172.16.0.132/28

ALU(config-if GigabitEthernet3/1)#interface Serial 0:0
ALU(config-if Serial0:0)#no shutdown
ALU(config-if Serial0:0)#ip address 202.24.45.100/30
ALU(config-if Serial0:0)#exit
ALU(config)#

```

2. PUT A DEFAULT ROUTE GOING TOWARDS THE INTERNET

```

ALU(config)# ip route 0.0.0.0/0 Serial0:0

```

3. THE THREE ZONES ARE CONFIGURED BY USING LISTS AND ATTACHING THE INTERFACES TO THESE LISTS. IT IS ALSO POSSIBLE TO DEFINE THE NETWORKS WITHIN THE LISTS.

```

ALU(config)# list Trust interface GigabitEthernet 3/0
ALU(config)# list Untrust interface Serial 0:0
ALU(config)# list DMZ interface GigabitEthernet 3/1
or
ALU(config)# list Trust prefix 10.0.0.0/24 prefix
192.168.0.0/24 prefix 172.16.0.0/25
ALU(config)# list Untrust prefix 202.24.45.100/30
ALU(config)# list DMZ host 172.16.0.130 host 172.16.0.131
ALU(config)# list SG8 host 172.16.0.130 host 192.168.1.1
host 202.24.45.100 host 10.0.0.1 host 172.16.0.1

```



Note: Configuring Lists with IP addresses rather than interfaces lead to the more efficient system operation, as it does not have to a lookup to determine egress interface and then apply filter.

4. CONFIGURING THE RULES AS PER THE SCENARIO

(i) Trusted to Internet - All services

```
ALU(config)# match-list Internet-access
ALU(config-match-list-Internet-access)# ip list Trust list
Untrust
```

(ii) Trust to DMZ -All services

```
ALU(config)# match-list trust-DMZ-access
ALU(config-match-list-DMZ access)# ip list Trust list DMZ
```

(iii) Mailserver access from the Internet

```
ALU(config)# match-list Internet-mail-access
ALU(config-match-list-Internet mail-access)# 1 tcp list
Untrust host 172.16.0.130 service smtp
ALU(config-match-list-Internet mail-access)# 2 tcp list
Untrust host 202.24.45.100/30 service pop
ALU(config-match-list-Internet mail-access)# 3 tcp list
Untrust host 202.24.45.100/30 service imap
ALU(config-match-list-Internet mail-access)# 4 tcp list
Untrust host 202.24.45.100/30 service http
ALU(config-match-list-Internet mail-access)# 5 tcp list
Untrust host 202.24.45.100/30 service 443
```

(iv) Webserver access from the internet

```
ALU(config)# match-list webserver-access
ALU(config-match-list-webserver-access)# 1 tcp list Untrust
host 202.24.45.100/30 service http
ALU(config-match-list-webserver-access)# 2 tcp list Untrust
host 202.24.45.100/30 service https
ALU(config-match-list-webserver-access)# 3 tcp list Untrust
host 202.24.45.100/30 service dns
ALU(config-match-list-webserver-access)# 4 udp list Untrust
host 202.24.45.100/30 service dns
```

(v) DMZ access to the Internet

```
ALU(config)# match-list untrust-DMZ-access
ALU(config-match-list-DMZ-access)# 1 tcp list DMZ list
Untrust service smtp
ALU(config-match-list-DMZ-access)# 2 tcp list DMZ list
Untrust service dns
ALU(config-match-list-DMZ-access)# 3 udp list DMZ list
Untrust service dns
```

(vi) Internet access to Trust

```
ALU(config)# match-list Internet-Trust
ALU(config-match-list-Internet-Trust)# ip any any
```

(vii) Managing the box

```

ALU(config)# match-list trust-manage
ALU(config-match-list-trust-manage)# 1 tcp list trust list
SG8 service ssh
ALU(config-match-list-trust-manage)# 2 tcp list trust list
SG8 service telnet

```

(viii) DMZ

```

ALU(config)# match-list DMZ-Trust
ALU(config-match-list-DMZ-Trust)# ip any any

```

5. RFC 1918 COMPLIANCE RULES

```

ALU(config)# list 1918 prefix 10.0.0.0/8 prefix 172.16.0.0/
12 prefix 192.168.0.0/16 prefix 0.0.0.0/8 prefix 14.0.0.0/8
prefix 127.0.0.0/8
ALU(config)# match-list RFC-1918
ALU(config-match-list-RFC-1918)# 1 ip list 1918 list Trust
ALU(config-match-list-RFC-1918)# 2 ip list 1918 list DMZ

```

6. RULES FOR MANAGING THE BOX FROM UNTRUST, DMZ AND TRUST ZONE THROUGH SSH AND TELNET.

```

ALU(config)# list untrust-manage host 202.24.45.100
ALU(config)# list dmz-manage host 172.16.0.132
ALU(config)# list trust-mange host 10.0.0.1 host
192.168.1.1 host 172.16.0.1/25

```

7. CONFIGURING THE MATCH-LISTS FOR INBAND MANAGEMENT THROUGH SSH AND TELNET.

```

ALU(config)# match-list manage-untrust
ALU(config-match-list-manage-untrust)# tcp any list untrust-
manage service telnet
ALU(config-match-list-manage-untrust)# tcp any list untrust-
manage service ssh

```

8. CONFIGURING RULES FOR DoS PROTECTION

```

ALU(config)# match-list DoS
ALU(config-match-list-DoS)# 1 ip any list trust
ALU(config-match-list-DoS)# 2 ip any list DMZ

```

9. CONFIGURING RULE FOR SNATING THE TRUSTED AND DMZ NETWORK

```

ALU(config)# match-list source-nat
ALU(config-match-list-source-nat)# 1 ip list Trust any
ALU(config-match-list-source-nat)# 2 ip list DMZ any

```

10. CONFIGURING THE DoS ATTACKS FROM WHICH PROTECTION IS REQUIRED. IN THIS CASE, WE CONFIGURE ALL THE AVAILABLE ATTACKS PRESENT ON THE OA-700.

```
ALU(config)# firewall
ALU(config-firewall)# attack atk1
ALU(config-firewall-attack-atk1)# tcp-fin-no-ack
ALU(config-firewall-attack-atk1)# tcp-fin-scan
ALU(config-firewall-attack-atk1)# tcp-header-frag
ALU(config-firewall-attack-atk1)# tcp-invalid-urgent-offset
ALU(config-firewall-attack-atk1)# tcp-null-scan
ALU(config-firewall-attack-atk1)# tcp-syn-fin
ALU(config-firewall-attack-atk1)# tcp-syn-flood
ALU(config-firewall-attack-atk1)# tcp-xmas-scan
ALU(config-firewall-attack-atk1)# udp-flood
ALU(config-firewall-attack-atk1)# udp-fraggle-attack
ALU(config-firewall-attack-atk1)# udp-port-loopback
ALU(config-firewall-attack-atk1)# udp-snork-attack
ALU(config-firewall-attack-atk1)# icmp-block-trace-route
ALU(config-firewall-attack-atk1)# icmp-dest-unrch-storm
ALU(config-firewall-attack-atk1)# icmp-ip-address-sweep
ALU(config-firewall-attack-atk1)# icmp-ping-flood threshold
2 10
ALU(config-firewall-attack-atk1)# icmp-ping-of-death
ALU(config-firewall-attack-atk1)# icmp-ping-of-death max-
total-length 64
ALU(config-firewall-attack-atk1)# icmp-redirect
ALU(config-firewall-attack-atk1)# icmp-router-advertisement
ALU(config-firewall-attack-atk1)# ip-land-attack
ALU(config-firewall-attack-atk1)# ip-source-routing
ALU(config-firewall-attack-atk1)# ip-spoofing
ALU(config-firewall-attack-atk1)# ip-tear-drop
ALU(config-firewall-attack-atk1)# ip-tiny-frag
ALU(config-firewall-attack-atk1)# ip-zero-length
```

11. CONFIGURING THE FILTERS MATCHING THE ABOVE SCENARIO

A) FILTERS FOR UN-TRUST ZONE

```
ALU(config)# ip filter untrust-traffic
ALU(config-filter-trust)#10 match any Internet-access permit
ALU(config-filter-trust)#20 match any trust-DMZ-access
permit
ALU(config-filter-trust)#30 match any trust-manage permit
ALU(config-filter-trust traffic)#default deny
```

Applying this filter as "IN" filter on the un-trust Interface

```
ALU(config-if GigabitEthernet3/0)#ip filter in untrust-
traffic
ALU(config)#ip filter in-untrust
ALU(config-filter-out-trust)#10 match any Internet-Trust
permit
ALU(config-filter-out-trust)#20 match any trust-manage
permit
ALU(config-filter-out-trust)#default deny
```

Applying this filter as "out" on the un-trust interface

```
ALU(config-if GigabitEthernet3/0)#ip filter out in-untrust
```

B) FILTERS FOR DMZ ZONE

```
ALU(config)# ip filter DMZ-traffic
ALU(config-filter-DMZ)#match any Internet-mail-access permit
ALU(config-filter-DMZ)#match any trust-DMZ-access permit
ALU(config-filter-DMZ traffic)#default deny
```

Applying the filter DMZ as a "IN" filter on the DMZ interface

```
ALU(config-if GigabitEthernet3/1)#ip filter in DMZ-traffic
ALU(config)#ip filter DMZ-out
ALU(config-filter-DMZ-out)#10 match any DMZ-Trust
ALU(config-filter-DMZ-out)#default deny
```

Applying the filter as "out" on the DMZ interface

```
ALU(config-if GigabitEthernet3/1)#ip filter out DMZ-out
```

C) FILTERS FOR TRAFFIC COMING FROM THE INTERNET

```
ALU(config)# ip filter untrust-traffic
ALU(config-filter-untrust-traffic)#match any Internet-mail-
access permit
ALU(config-filter-untrust-traffic)#match any webserver-
access permit
ALU(config-filter-untrust-traffic)#match any RFC-1918 deny
log
ALU(config-filter-untrust-traffic)#match any manage-untrust
permit
ALU(config-filter-untrust-traffic)#default deny
```

Applying this filter as 'in' on Untrust interface

```
ALU(config-if Serial0:0)#ip filter in untrust-traffic
ALU(config)# ip filter out-untrust
ALU(config-filter-out-untrust)#10 match any Internet-access
permit
ALU(config-filter-out-untrust)#20 match any untrust-DMZ-
access permit
ALU(config-filter-out-untrust)#default deny
```

This filter is applied as "out" filter

```
ALU(config-if Serial0:0)#ip filter out out-untrust
```

12. CONFIGURING SOURCE NAT FOR ALL TRAFFIC GOING TOWARDS INTERNET

```
ALU(config)# ip nat source-nat
ALU(config-nat-source-nat)# match any source-nat source-nat
```

Applying the Source NAT on the serial interface as out NAT policy so that all the internal traffic gets NAT ed to the public IP of the Serial Interface.

```
ALU(config-if Serial0:0)#ip nat out source-nat
```

13. CONFIGURING THE DNAT RULES FOR THE DMZ

```
ALU(config)# ip nat DNAT
ALU(config-nat-DNAT)#match any Internet-mail-access
destination-nat host 172.16.0.130
ALU(config-nat-DNAT)#match any webserver-access
destination-nat host 172.16.0.131
```

Applying this DNAT rule as a IN nat policy for the mail and webserver access.

```
ALU(config-if Serial0:0)#ip nat in DNAT
```

14. CONFIGURING THE FIREWALL POLICY TO PROTECT AGAINST THE DoS ATTACK.

```

ALU(config)#firewall
ALU(config-firewall)# policy prevent
ALU(config-firewall-prevent)# match any DoS attack atkl
drop

```

Applying this firewall policy to the trust and DMZ as an IN policy to protect the network against the Dos attacks.

```

ALU(config-if Serial0:0)#firewall policy in prevent

```

EXAMPLE 2: SIMPLE ZONE CONFIGURATION IN OA-700

In OA-700, you can define classification for trusted/untrusted/dmz traffic in ACL, NAT, or DoS policies, and further apply these policies to the interfaces:

```

Match-list trusted
  Ip 10.1.1.0/24 any

Match-list dmz
  Ip 148.64.4.0/24 any

Match-list any-ip
  Ip any any

Ip nat nat-policy
  Match trusted source-nat

Ip filter permit-dmz-policy
  Match dmz permit

Ip filter deny-untrusted-policy
  Match any-ip deny

```

Suppose Gigabit Ethernet 7/1 is facing external networks, you will need to apply these NAT and Filter policies to this interface:

```

Interface GigabitEthernet7/1 //Physical i/f to untrusted networks

Ip nat out nat-policy //This will NAT internal traffic

Ip filter out permit-dmz-policy //This will permit DMZ traffic without
translation

Ip filter in deny-untrusted-policy //This will deny all untrusted
traffic originated from outside.

Exit //Done

```

If you prefer, you can use interface based classification:

```
Match-list trusted
    Ip interface GigabitEthernet7/0 any

Match-list untrusted
    Ip interface GigabitEthernet7/1 any

Match-list dmz
    Ip interface GigabitEthernet3/0 any
```

Suppose Gigabit Ethernet 7/1 is facing external networks, you will need to bind these NAT and Filter policies to this interface:

```
Interface GigabitEthernet7/1 //Physical i/f to untrusted networks

Ip nat out nat-policy //This will NAT internal traffic

Ip filter out permit-dmz-policy //This will permit DMZ traffic without
translation

Ip filter in deny-untrusted-policy //This will deny all untrusted
traffic originated from outside

Exit //Done
```


TIME-RANGE/TIMER CONFIGURATION

This section describes configuration of the time-range/timer across various applications. It is divided into the following sections:

- “Time-range Configuration Commands” on page 635
- “Time-range Show Command” on page 636

TIME-RANGE CONFIGURATION COMMANDS

This section lists the commands used in configuring time-range.

TO CONFIGURE A TIME-RANGE

Command (in CM)	Description
<code>time-range <name></code>	This command is used to configure a time-range object that can be used across applications.
<code>no time-range <name></code>	This command is used to delete a specific time-range.

Time-range enters the Time-range sub-configuration mode. Here, the time configured for scheduling is the local time and not the GMT time. Therefore, it has the option to permit automatic changing to/from daylight savings time.



Note: User must issue “clock” command to set the clock in OA-700, so that the time-range configuration can take effect precisely.

EXAMPLE

```
ALU(config)# time-range t1
ALU(config-time-range-t1)#

ALU(config)# no time-range t1
```

TO CONFIGURE ABSOLUTE/PERIODIC TIME-RANGE

Command (in Time-range Mode)	Description
<pre>absolute <hh:mm:ss> <mm/dd/yyyy> [to <hh:mm:ss> <mm/dd/yyyy>] periodic {daily weekly {sunday monday ...} weekend } <hh:mm:ss> to <hh:mm:ss>}]</pre>	This command is used to configure an absolute or periodic time-range object.

EXAMPLE

```
ALU(config-time-range-t1)# absolute 10:20:00 12/20/2003 to
13:15:00 4/15/2004
```

```
ALU(config-time-range t2)# periodic daily 08:00:00 to 19:00:00
```

```
ALU(config-time-range t3)# periodic weekly wednesday 10:00:00
to 13:30:00
```

TIME-RANGE SHOW COMMAND

Command (in SUM)	Description
<pre>show time-range [<name>]</pre>	This command is used to view information of all the time-range configured on the system or a specific time-range.

EXAMPLE

If "t1" is a schedule, then to view the particulars in it, use the following command:

```
ALU# show time-range
time-range t1
absolute 10:10:10 5/6/2006
time-range t2
absolute 10:10:10 2/5/2006
```

ALGS SUPPORTED IN OA-700

These ALGs (Application Level Gateway) can be used only in conjunction with NAT. The ALGs supported in OA-700 are listed below.

SIP

The Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify, and terminate multimedia sessions such as Internet telephony calls. SIP can also invite participants to already existing sessions. Media can be added to or removed from an existing session.

A SIP network consists of proxy servers, redirect servers, registration servers and user agents (UA). For the UA which initiates the session, we call it user agent client (UAC). The party which accepts the invitation from UAC, we call it user agent server (UAS). For the purpose of discussion, we call redirect, registration and proxy servers "SIP servers". SIP is actually a signaling protocol for setting up sessions between clients over the network. These sessions do not necessarily have to be Internet telephony sessions.

OmniAccess supports SIP as a service and can screen SIP traffic, allowing and denying it based on a policy that you configure. SIP is a predefined service in OA-700 and uses port 5060 as the destination port.

DNS

Domain Name System (or Service or Server) (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might translate to `198.105.232.4`.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

FTP

File Transfer Protocol (FTP) is the protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer.

FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server).

NFS

Network File System (NFS) is a client/server application designed by Sun Microsystems that allows all network users to access shared files stored on computers of different types. NFS provides access to shared files through an interface called the Virtual File System (VFS) that runs on top of TCP/IP. Users can manipulate shared files as if they were stored locally on the user's own hard disk.

With NFS, computers connected to a network operate as clients while accessing remote files, and as servers while providing remote users access to local shared files. The NFS standards are publicly available and widely used.

RTSP

Real Time Streaming Protocol (RTSP) is a standard for controlling streaming data over the World Wide Web.

RTSP uses RTP (Real-Time Transport Protocol) to format packets of multimedia content. But whereas H.323 is designed for video conferences of moderately-sized groups, RTSP is designed to efficiently broadcast audio-visual data to large groups.

TFTP

Trivial File Transfer Protocol (TFTP) a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

UA

Universal Alcatel (UA) is a VoIP signaling protocol proprietary of Alcatel.

ALG CONFIGURATION COMMANDS

This section lists the commands used in configuring an ALG.



Note: Configuring match-lists is a pre-requisite for configuring ALG. (For details, refer to the chapter “[Common Classifiers](#)” in this guide).

To CONFIGURE ALG

Command (in Match-list Mode)	Description
<code>udp any any service {dns nfs rpc-portmap sip tftp}</code>	This command is used to enable DNS, NFS, RPC-Portmap, TFTP, or SIP ALG.
<code>tcp any any service {dns ftp nfs rpc-portmap rtsp sip}</code>	This command is used to enable DNS, FTP, NFS, RPC-Portmap, RTSP or SIP ALG.

EXAMPLE

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# udp any any service sip
```

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# tcp any any service dns
```



Note: Use the port number to configure any other standard ALG service apart from those given in the above commands.

FIREWALL ALG SHOW COMMANDS**To VIEW DNS ALG STATISTICS**

Command (in CM)	Description
<code>show firewall alg dns statistics</code>	This command is used to view the DNS ALG statistics.

EXAMPLE

```
ALU(config)# show firewall alg dns statistics
```

```
Total DNAT Ordinary Queries           : 0
Total DNAT Inverse Queries             : 0
Total DNAT Ordinary Query Responses    : 0
Total DNAT Inverse Query Responses     : 0
Total non-translated Packets           : 0
```

To VIEW FTP ALG STATISTICS

Command (in CM)	Description
<code>show firewall alg ftp statistics</code>	This command is used to view the FTP ALG statistics.

EXAMPLE

```
ALU(config)# show firewall alg ftp statistics
```

```
Total SNAT Port commands               : 0
Total DNAT Port commands                : 0
Total Filter Port commands              : 0
Total SNAT Pasv Response commands       : 0
Total DNAT Pasv Response commands       : 0
Total Filter Pasv Response commands     : 0
Total Pinholes created                  : 0
Total Pinholes matched                   : 0
Total Pinholes timed out                 : 0
Total Pinholes failed                    : 0
```

To VIEW TFTP ALG STATISTICS

Command (in CM)	Description
<code>show firewall alg tftp statistics</code>	This command is used to view the TFTP ALG statistics.

EXAMPLE

```
ALU(config)# show firewall alg tftp statistics
```

```
Total SNAT Write commands           : 0
Total DNAT Write commands           : 0
Total Filter Write Commands         : 0
Total SNAT Read Commands            : 0
Total DNAT Read Commands            : 0
Total Filter Read commands          : 0
Total Pinholes created               : 0
Total Pinholes matched              : 0
Total Pinholes timed out            : 0
Total Pinholes failed               : 0
```

To VIEW RPC-PORTMAP ALG STATISTICS

Command (in CM)	Description
<code>show firewall alg rpc statistics</code>	This command is used to view the RPC-Portmap ALG statistics.

EXAMPLE

```
ALU(config)# show firewall alg rpc statistics
```

```
Total SNAT RPC CALL Packets        : 0
Total DNAT RPC REPLY Packets        : 0
Total DNAT DUMP REPLY Packets       : 0
Total Pinholes created               : 0
Total Pinholes matched              : 0
Total Pinholes failed               : 0
Total Pinholes removed              : 0
```

To VIEW RTSP ALG STATISTICS

Command (in CM)	Description
<code>show firewall alg rtsp statistics</code>	This command is used to view the RTSP ALG statistics.

EXAMPLE

```
ALU(config)# show firewall alg rtsp statistics
```

```
Total RTSP sessions           : 0
Total RTP sessions            : 0
Total RTCP sessions           : 0
Total RTP Pinholes created    : 0
Total RTP Pinholes matched    : 0
Total RTP Pinholes timed-out  : 0
Total RTCP Pinholes created   : 0
Total RTCP Pinholes matched   : 0
Total RTCP Pinholes timed-out : 0
```

To VIEW SIP ALG STATISTICS

Command (in CM)	Description
<code>show firewall alg sip statistics</code>	This command is used to view the SIP ALG statistics.

EXAMPLE

```
ALU(config)# show firewall alg sip statistics
```

```
Total SIP Connections           : 1
Total allocated SIP Call Sessions : 1
Total SIP Call Sessions freed    : 0
Total RTP Sessions              : 0
Total RTCP Sessions             : 0
Total RTP Pinholes created      : 2
Total RTP Pinholes freed        : 1
Total RTP Pinholes matched     : 1
Total RTP Pinholes timeout     : 0
Total RTCP Pinholes created     : 2
Total RTCP Pinholes freed       : 0
Total RTCP Pinholes matched    : 0
Total RTCP Pinholes timeout    : 0
Total SIP Packets with Non-SDP message body : 0
Total SIP Packets with invalidate payload : 0
Total SIP Packets with invalidate SDP payload : 0
Total SIP Packets out of order  : 0
```


FIREWALL ALG DEBUG COMMANDS

To VIEW DNS DEBUG COUNTERS

Command (in CM)	Description
<code>show firewall alg dns debug counters</code>	This command is used to view the DNS ALG debug counters.

EXAMPLE

```
ALU(config)# show firewall alg dns debug counters
```

```
Total malloc operations           : 0
Total failed malloc operations     : 0
Total memory release operations   : 0
```

To VIEW FTP ALG DEBUG COUNTERS

Command (in CM)	Description
<code>show firewall alg ftp debug counters</code>	This command is used to view the FTP ALG debug counters.

EXAMPLE

```
ALU(config)# show firewall alg ftp debug counters
```

```
Total malloc operations           : 0
Total failed malloc operations     : 0
Total memory release operations   : 0
```

To VIEW TFTP ALG DEBUG COUNTERS

Command (in CM)	Description
<code>show firewall alg tftp debug counters</code>	This command is used to view the TFTP ALG debug counters.

EXAMPLE

```
ALU(config)# show firewall alg tftp debug counters
```

```
Total malloc operations           : 0
Total failed malloc operations     : 0
Total memory release operations   : 0
```

To VIEW RPC-PORTMAP ALG DEBUG COUNTERS

Command (in CM)	Description
<code>show firewall alg rpc debug counters</code>	This command is used to view the RPC-Portmap ALG debug counters.

EXAMPLE

```
ALU(config)# show firewall alg rpc debug counters
```

```
Total malloc passed           : 0
Total malloc failed           : 0
Total memory free count       : 0
```

To VIEW RTSP ALG DEBUG COUNTERS

Command (in CM)	Description
<code>show firewall alg rtsp debug counters</code>	This command is used to view the RTSP ALG debug counters.

EXAMPLE

```
ALU(config)# show firewall alg rtsp debug counters
```

```
Currently registered RTSP families : 0
```

To VIEW SIP ALG DEBUG COUNTERS

Command (in CM)	Description
<code>show firewall alg sip debug counters</code>	This command is used to view the SIP ALG debug counters.

EXAMPLE

```
ALU(config)# show firewall alg sip debug counters
```

```
Total malloc passed, sip sessions and calls : 0
Total malloc failed                          : 0
Total memory free count, sip sessions and calls : 0
Total sip packets translated                 : 0
Total sdp packets translated                 : 0
Total sip packets retransmitted              : 0
```

FIREWALL ALG CLEAR COMMANDS**To CLEAR FIREWALL ALG SIP STATISTICS**

Command (in CM)	Description
<code>clear firewall alg sip statistics</code>	This command is used to clear the the ALG SIP statistics.

EXAMPLE

```
ALU(config)# clear firewall alg sip statistics
```

CUSTOMIZED-SERVICE RULE BASED ALG CONFIGURATION

The OA-700 now supports the customized-service rule based ALG (Application Level Gateway) configuration. By definition, the ALGs operate on well known ports or standard ports. The customized service gives an additional point of invocation of the ALG and the capability to remove or disable the invocation from well-known ports.

You also have the flexibility to use ALG based on the rules defining specific service configuration apart from those on well-known ports.

If you do not want to use ALG for a particular service, configure “service-none”.

This customization of invoking ALG on user configured ports is an enhancement specific to OA-700 and is not available on other systems.



Note: ALG configuration is system wide firewall configuration and is not specific to any interface.

CUSTOMIZING ALG COMMANDS

To CONFIGURE CUSTOMIZED SERVICE

Command (in CM)	Description
<code>customized-service</code>	This command is used to configure ALG rule. This also enters into customized service configuration mode.

EXAMPLE

```
ALU(config)# customized-service
```

To CREATE A CUSTOMIZED SERVICE ALG RULE

Command (in Customized Service Mode)	Description
<pre>[<1-65535>] match [any all] <match-list name.> service {service-name alcatel-tftp dns ftp none rpc rtsp sip tftp}</pre>	<p>This command creates a rule for mapping ALG action for a well known service to a non-standard port or disable a well known service on its well known port.</p> <p>The range for the rule number is 1-65535. This rule number signifies the priority of a rule. By default, the numbering pattern for rule number is the next multiple of ten to the highest existing rule number.</p>

EXAMPLE

The following example shows that if the packet is intended for the server with address 20.1.1.1 comes to port 100, then the service is recognized as FTP and the ALG is invoked accordingly. The standard port invocation of ALG is also active here.

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# tcp any host 20.1.1.1 to 100
ALU(config-customized-service)# match all m1 service ftp
```

To MODIFY AN EXISTING ALG RULE

Command (in Customized Service Mode)	Description
<pre>[<1-65535>] match [any all] <match-list name>... service {service-name alcatel-tftp dns ftp none rpc rtsp sip tftp}</pre>	<p>This command modifies a rule that has been configured for mapping ALG action to a non-standard port.</p>

EXAMPLE

The following example modifies a rule:

```
ALU(config-customized-service)# 10 match any m2 service none
```

TO MODIFY PRIORITY OF AN EXISTING ALG RULE

Command (in Customized Service Mode)	Description
<code>change {<1-65535> <1-65535>}</code>	Use this command to change the priority of a specific ALG rule configured.

EXAMPLE

The following example shows how to change the priority of a rule;
 ALU(config-customized-service)# change 10 1

TO DELETE AN EXISTING ALG RULE

Command (in Customized Service Mode)	Description
<code>no rule {<1-65535>}</code>	This command deletes an existing ALG rule.

EXAMPLE

ALU(config-customized-service)# no rule 10

TO VIEW THE DETAILS OF A ALG RULE BASED SERVICE

Command (in CM)	Description
<code>show customized-service</code>	This command shows the ALG rule based service details.

EXAMPLE

ALU(config)# show customized-service

20 match any m2 service none

UA ALG CONFIGURATION

Universal Alcatel (UA) is a VoIP signaling protocol proprietary of Alcatel.

UA ALG is a software module, which works with firewallfilter to adjust the data packets on-the-fly. The UA ALG Processing involves:

- Register UA ALG Constructor (based on Packet type classification, filter/firewall Policies)
- Install UA ALG vectors
- Create Pinhole and monitor UA data traffic
- ALG inspection and translation
- Release of Pinhole and Call ALG Destructor.

ALG also gives user an option to configure firewall policies to precisely classify, permit only UA/RTP/RTCP traffic between phones, Call Server, Media Gateway, and drop other types of traffic between these devices. These features will prevent attacks coming from internal networks through VPN. Another benefit from UA ALG is to precisely identify RTP and RTCP so user can apply QoS on voice traffic.

UA ALG COMMANDS

To CONFIGURE UA ALG

Follow the steps to enable UA ALG:

- Configure a match-list.
- Enable TFTP and define UA traffic in Customized Service Mode.
- Classify UA traffic.
- Configure a rule to deny/permit UA traffic in a filter/firewall policy and attach it to an interface.

Command (in Match-list Mode)	Description
<code>udp any any service tftp</code>	This command is to enable TFTP.

Command (in Customized Service Mode)	Description
<code>[<1-65535>] match [any all] <match-list name>... service alcatel-tftp</code>	Configure this command in the customized-service mode. Use this command to define UA traffic, so that ALG knows which addresses and ports that UA is running on, and how to translate the TFTP configuration files.

Command (in Match-list Mode)	Description
<code>udp any any type alcatel-ua</code>	Configure this command in the match-list mode. Use this command to classify the UA traffic.

You can also apply QoS to UA traffic by using "type alcatel-ua" match-lists in the QoS policies.

EXAMPLE

Enable UA ALG service and define UA traffic.

```
ALU(config)# match-list m1-filter
ALU(config-match-list-m1-filter)# udp any any service tftp
ALU(config-customized-service)# 10 match any m1-filter service
alcatel-tftp
```

Classify UA traffic.

```
ALU(config-match-list-m2-qos)# udp any any type alcatel-ua
```

Configure a rule to permit UA traffic in a filter and attach it to an interface.

```
ALU(config)# ip filter f1
ALU(config-filter-f1)# 10 match m1-filter permit
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# ip filter in f1
```

TO VIEW UA ALG STATISTICS

Command (in CM)	Description
<code>show firewall alg alcatel-ua statistics</code>	This command is used to view the Alcatel-UA ALG statistics.

EXAMPLE

```
ALU(config)# show firewall alg alcatel-ua statistics
```

```
UA pinholes outstanding           : 1
UA sessions created              : 10
UA sessions released             : 10
UA sessions timed out           : 12
RTP pinholes outstanding         : 2
RTP sessions created            : 10
RTP sessions released           : 10
RTP sessions terminated from UA time-outs : 0
RTCP pinholes outstanding       : 2
RTCP sessions created           : 10
RTCP sessions released         : 10
RTCP sessions terminated from UA time-outs: 0
```


To VIEW UA ALG DEBUG COUNTERS

Command (in CM)	Description
<code>show firewall alg alcatel-ua debug-counters</code>	This command is used to view the Alcatel-UA ALG debug counters.

EXAMPLE

```
ALU(config)# show firewall alg alcatel-ua debug-counters
```

```
Total malloc passed, UA sessions and calls      : 2951
Total malloc failed                               : 0
Total memory free count, UA sessions and calls   : 0
Total UA packets translated                       : 7690
Total sdp packets translated                     : 26
Total UA packets retransmitted                   : 330
```

TYPICAL RULE BASED ALG AND DNAT EXAMPLE USING OA-700

When there are multiple internal FTP servers inside the DMZ and sufficient Public IP addresses are not available, these multiple FTP servers should run on different ports so that they can be accessed from outside using DNAT. As a standard service, FTP ALG is registered only on port 21 so outsiders will not be able to access internal servers. To allow outside access to internal FTP Servers, FTP ALG should be registered on those ports where FTP Server is listening for a control connection.

The following example illustrates how rule based ALG solves this problem by mapping the non-standard ports to standard service so that FTP ALG can be invoked on these non-standard ports.

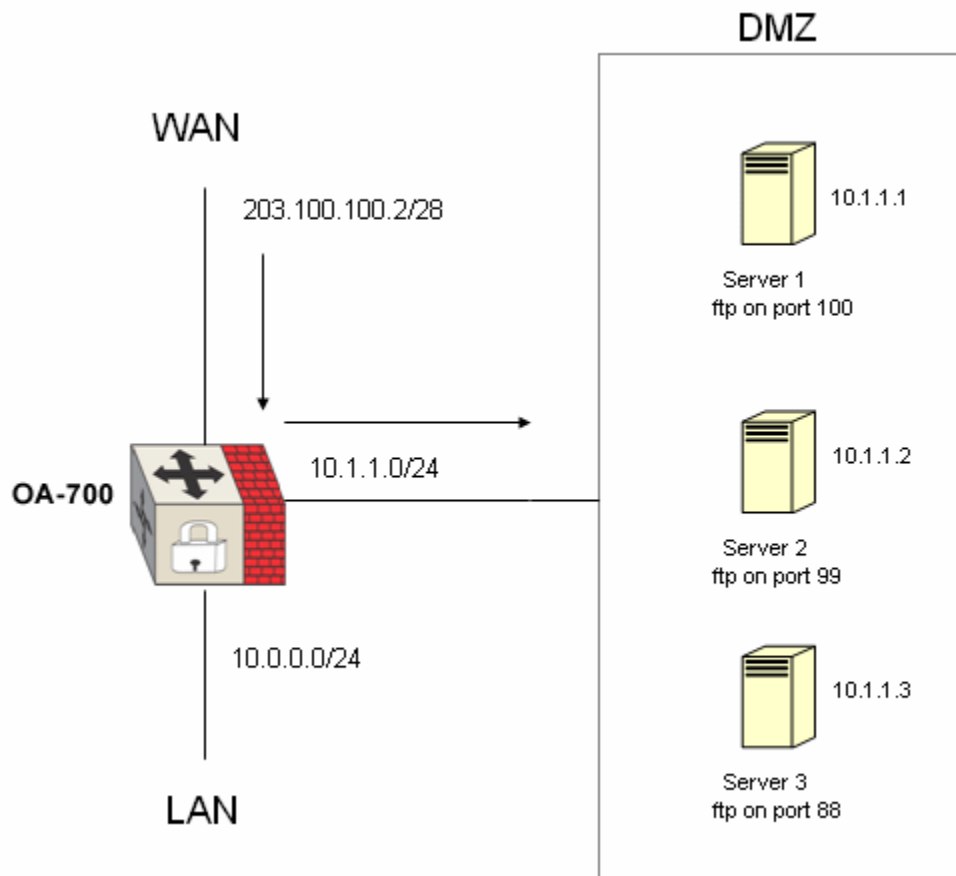


Figure 56: ALG Configuration Scenario

Match-list configuration:

```
ALU(config)# match-list m1
ALU(config-match-list-m1)# tcp any host 203.100.100.2/28
service 100
ALU(config-match-list-m1)# match-list m2
ALU(config-match-list-m2)# tcp any host 203.100.100.2/28
service 99
ALU(config-match-list-m1)# match-list m3
ALU(config-match-list-m3)# tcp any host 203.100.100.2/28
service 98
ALU(config-match-list-m1)# match-list m4
ALU(config-match-list-m4)# tcp any host 203.100.100.2/28
service 21
```

DNAT Configuration

```
ALU(config-match-list-m3)#ip nat dnat
ALU(config-nat-dnat)# match m1 destination-nat host 10.1.1.1
ALU(config-nat-dnat)# match m2 destination-nat host 10.1.1.2
ALU(config-nat-dnat)# match m3 destination-nat host 10.1.1.3
```

Customized-Service Configuration

```
ALU(config)customized-service
ALU(config-customized-service)#match m1 service ftp
ALU(config-customized-service)#match m2 service ftp
ALU(config-customized-service)#match m3 service ftp
ALU(config-customized-service)#match m4 service none
```

Show Customized-Service Configuration

```
ALU(config)# show customized service
10 match m1 service ftp
20 match m2 service ftp
30 match m3 service ftp
40 match m4 service none
```

SECURITY - BEST PRACTICES

"Security is not a product, it's a process". This is a very famous saying by Bruce Schneier. Nothing in security is "set it and forget it!" Security cannot be achieved with point products-it is an ongoing process that never ends. A firewall is a very important part of security, but it is a small part. There are instances where one has the best firewall product installed but poorly configured one. This is same as not having one.

It becomes imperative, hence to know what are the best practices to follow when configuring a firewall. The below said discussion gives a broad guideline to configure a firewall which protects the network against the hackers as well as the Denial-of -Service attacks. Below are some rules, procedures and restrictions you may use to provide level of security in the network.

The following are some general procedures, which needs to be kept in mind. (These are independent of Firewall configuration).

- Keeping network user accounts off the Internet service computers such as web servers. FTP servers and firewall. Having separate administrative accounts with different passwords for these devices.
- Regularly scan the system logs for failed logon attempts to network services and failed connection attempts to web servers, FTP servers, etc.
- Regularly scan system user accounts for unauthorized addition or modification of user accounts for network services
- Performing regular backups.

RULES FOR CONFIGURING PACKET FILTERS

A packet filter will not stop a concentrated network attack from exploiting service protocol weaknesses, but it will stop the simplest Denial -of- service attacks. These rules control the flow of several different kinds of packet through the firewall. The point to be noted here is that rules are evaluated by firewall from first to last.

The rules are:

- [ICMP Rules](#)
- [IP Rules](#)
- [UDP Rules](#)
- [TCP Rules](#)

ICMP RULES

ICMP packets can be forged to trick computers into re-directing their communications, stopping all communications or even crashing. Following rules should be kept in mind when creating policies for ICMP:

- Allow source quench: This tells external host when the local network is saturated
- Allow echo request outbound
- Allow echo reply inbound
- Allow destination unreachable inbound
- Allow service unavailable inbound
- Allow TTL exceeded inbound
- Drop echo request inbound
- Drop and log redirect inbound
- Drop destination unreachable outbound
- Drop service unavailable outbound
- Drop TTL exceeded outbound
- Drop all other ICMP packets.

IP RULES

These are some rules that you would want to configure for all packets regardless of whether they contain TCP or UDP traffic inside them.

- Drop all packets arriving on the internal interface that have source field indicating that the packet came from outside the network.
- Drop all incoming packets to interior computers that have no externally accessible service.
- Drop and log all private addresses coming on the external interface. As per RFC 1918, the address blocks 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.16.31.255 and 192.168.0.0 to 192.168.255.255 are reserved for private allocation. Hence, any packet arriving with any of the said IP's on the interface which is connected to the internet should be dropped and logged. If there is occurrence of the same, it might be because some hacking taking place.

UDP RULES

Once the rules for generic IP traffic are put in place, it is better to have some UDP rules to block egregious security holes, such as X-windows. Each of these UDP rules specifically denies a port or range of ports:

- Drop packets using ports below 21: There are no services below port 21 that an average Internet user finds useful.
- Drop X-Windows (packets using ports 600-6003). It is possible for a hacker to control mouse and keyboard for a host inside the network.
- Drop SNMP (packets using ports 161 and 162).

TCP RULES

The TCP rules are like UDP rules but with one difference - ACK bit can be used to stop connections from being initiated from one direction or the other. Blocking inbound packets with ACK bit cleared for a particular port allows only outbound connections to be initiated, but allows subsequent data traffic for that connection- all of which will have the ACK bit set. Some of the important rules are listed below:

- Drop packets using ports below 21; same as the rule like UDP.
- Drop X-Window: same as UDP.
- Disallow incoming telnet connections (incoming packets with port 23). It is worth using SSH (port 22) which is more secure than telnet.
- Specifically allow any internal services that use ports greater than 1023; This way subsequent rule can be used to stop backdoor software like Back Orifice, which opens port internally for remote unauthorized control of computers.
- Drop syn packets from outside to internal ports >1023; Most legitimate services are configured on ports <1024.
- Disallow incoming FTP data connections thus allowing passive FTP only.
- Disallow SMTP connections (port 25) from the outside to other than mail server.
- Establish service destinations rules for other services such as HTTP.

Many of the users feel that above mentioned rules are not enough; A dedicated hacker with time and resources can find a way around these rules. Some of the advanced methods that you can use are:

NETWORK ADDRESS TRANSLATION

This feature allows to expose just a handful of IP addresses to the outside world. The firewall keeps a track of connections and re-writes packet source and destination and port values on the fly.

FRAGMENTATION

Fragmented packet should be disallowed into the network. It is wise to reassemble fragmented packet at the firewall or just drop since the fragmentation feature is largely obsolete.

RATE-LIMITING

Rate limiting is a good method of prevention against Denial -of -service attack. Most common of them are:

SYN ATTACK

Knowing traffic pattern for the site helps in preventing this type of attack. For a e-business site, it may be 20,000 syn packets/second. For a smaller site, it might be 20 syn packets/sec.

Hence, depending upon the traffic pattern, the threshold can be set. If the threshold is crossed, it might be pointer to a syn attack. One can configure the threshold as:

```
dos p1
tcp syn flood threshold 40 packets per msec
```

PORT SCAN ATTACKS

This attacks happens whereby one source IP address sends IP packets to 10 different ports at the same destination IP address within a defined interval. This is again can be prevented by setting a threshold (.005 seconds is the default). This can be shown as:

```
dos p1
udp port scan threshold 10 per 0.005 seconds
```


CHAPTER 27 IP SECURITY - VIRTUAL PRIVATE NETWORK

After installing the OA-700, use the Command Line Interface (CLI) to configure IPsec VPN. This chapter gives a fundamental understanding and the steps involved in configuring the IPsec VPN, its components, tunneling, and security. To get a succinct knowledge on the parameters and default values, refer to the VPN section in ***OmniAccess 700 CLI Command Reference Guide***.

This chapter includes instructions for configuring the IPsec through the CLI. It includes the following sections:

- **“IPsec VPN Overview”**
- **“IPsec VPN Configuration”**
- **“IPsec Scenarios on OA-700”**
- **“Best Practices For Deploying IPsec VPN”**
- **“IPsec NAT-Traversal”**
- **“Scenarios Depicting IPsec Nat-traversal”**
- **“IPsec Tunnel Interface”**
- **“IPsec Tunnel Configuration Scenarios using OA-700”**

CHAPTER CONVENTIONS

Acronym	Description
CA	Certificate Authority
CM	Configuration Mode - ALU (config)#
Crypto Map Mode	Crypto Map Configuration Mode - ALU (config-crypto-map name)#
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DPD	Dead Peer Detection
ESP	Encapsulating Security Payload
ICM	Interface Configuration Mode - ALU (config-interface name)#
IKE	Internet Key Exchange
IKE Policy Mode	IKE Policy Configuration Mode - ALU (config-IKE policy name)#
ISAKMP	Internet Security Association and Key Management Protocol
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
SA	Security Association
SPD	Security Policy Database
SUM	Super User Mode - ALU#

IPSEC VPN OVERVIEW

VPN is basically a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

With the rapid growth of Internet access and bandwidth availability across the globe, the need for security has almost become inevitable. But now, with the evolution of security through VPN's, this is possible and gives the capability to connect the private offices and users to use any untrusted IP network for secure interconnections through this "virtual" mode. This medium of communication also worked out to be highly attractive as a replacement to the private leased circuits.

Using VPN, corporates will be able to leverage on an ISP's service, providing cost-effective:

- Office to office connectivity
- Road warrior connectivity access
- Extranets with service agents, partners, etc.
- Secure connectivity from home to the office network.

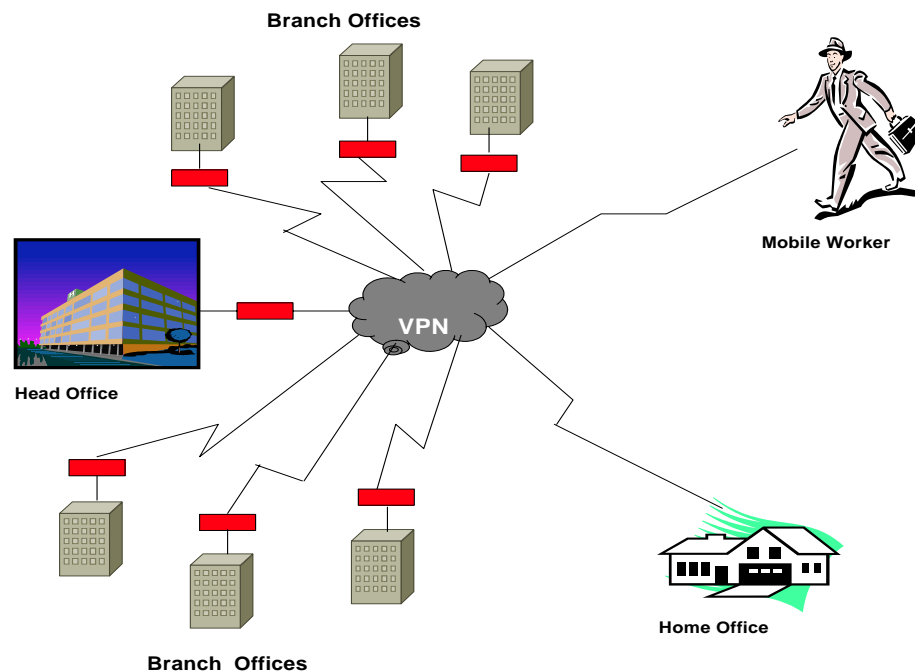


Figure 57: General VPN Usage

VPNs may be implemented using any of the several protocols such as PPTP, L2TP, and IPsec, to name a few. This chapter primarily focuses on the implementation of 'secure' VPNs with IPsec.

In a TCP/IP network, the packet is routed based on the network layer information while the actual data is held in the IP layer. Hence, by securing the IP layer, it is possible to secure the network.

The following sections provide a conceptual overview of IPsec VPN:

- [“IPsec Enabled VPN”](#)
- [“IPsec Connection Types”](#)
- [“IPsec Concepts”](#)
- [“Benefits of IPsec Enabled VPN”](#)
- [“Default Configuration Setting on OA-700”](#)

IPSEC ENABLED VPN

Internet Protocol Security (IPsec) provides enhanced security features, such as confidentiality and more comprehensive authentication. IPsec has two encryption modes: tunnel and transport. Tunnel mode encrypts the header and the payload of each packet while the transport mode encrypts only the payload. Systems that are IPsec compliant can take advantage of this protocol.

IPSEC CONNECTION TYPES

This section lists various types of IPsec connections:

- "NAT-pass-through"
- "Host to Host"
- "Host to Subnet"
- "Subnet to Subnet"

NAT-PASS-THROUGH

This connection is for an individual computer behind a firewall to make a connection to a remote computer or network. The firewall that is protecting the individual computer does not participate in the VPN connection or authenticate it, but rather allows the connection "through" the firewall. A home connection that is connected to a company network is an example of this type of connection.

HOST TO HOST

This connection is for connecting two computers together. The subnet declaration is not used in the connection configuration. This is commonly used as a second tunnel between subnet-to-subnet gateway for WINS and/or DNS services that are impossible for the gateway machines to participate in through the subnet tunnel.

HOST TO SUBNET

This connection is for a single computer to connect to a remote network. This is typically known as the "Road Warrior" connection and the remote computer is not behind a firewall. The IP address that the remote computer will be using is normally not known for configuration.

SUBNET TO SUBNET

This connection is for remote offices to connect their respective private networks to each other. The tunnel is formed between respective networks to forward the traffic between the locations.

The figure below depicts a general scenario of IPsec -VPN. Tunnel 2 is the secured VPN channel that connects the Finance department and Accounts department of two geographically displaced locations. Tunnel 1 users have no access to this path.

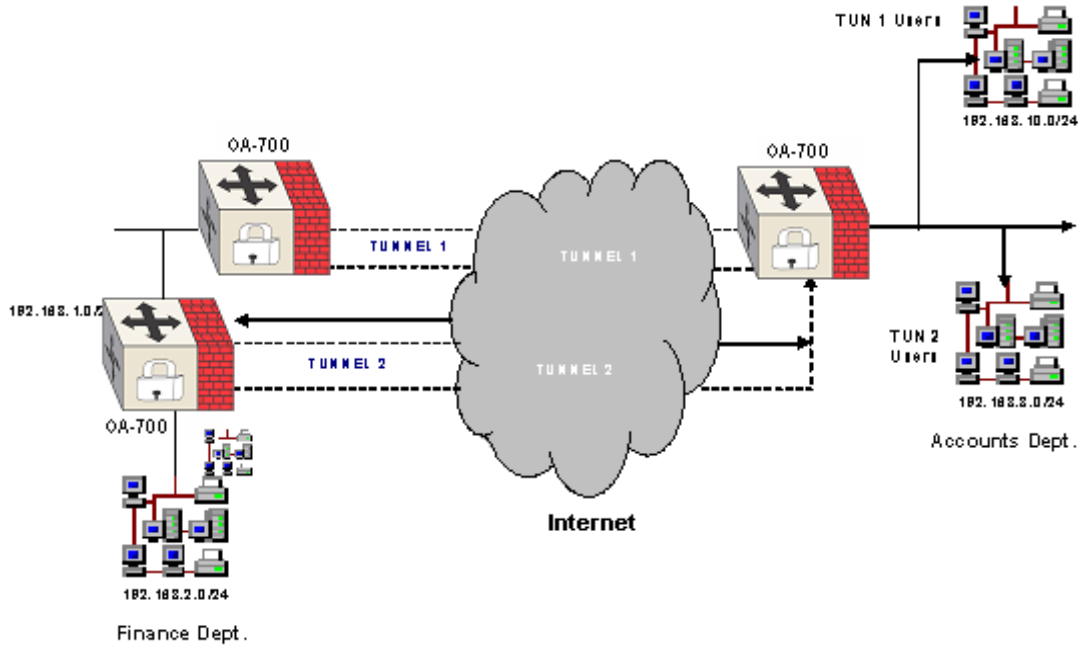


Figure 58: A General Scenario of IPsec - VPN

IPSEC CONCEPTS

The following section comprehends a conceptual overview of IPsec:

- “IPsec Modes Of Operation”
- “IPsec Protocols”
- “Encryption Algorithms”
- “Internet Key Exchange”
- “Security Association (SA)”

IPSEC MODES OF OPERATION

IPsec provides two different modes to exchange protected data across the different kinds of VPNs:

TRANSPORT MODE

This mode is applicable for only host-to-host security. For example, this mode can be used to create a secure association between two personal workstations each of which has a public address. The protection here is extended to the payload of IP data.

TUNNEL MODE

This mode is used to provide data security between two networks. It provides protection for the entire IP packet and is sent by adding an outer IP header which corresponds to the two tunnel endpoints. The unprotected packets generated by the hosts travel through the protected “tunnel” created by gateways on both the ends. The outer IP header corresponds to these gateways. Since the tunnel mode hides the original IP header, it facilitates security of the networks with private IP address space.

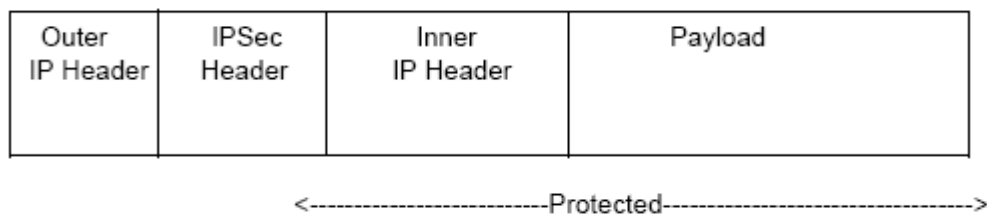


Figure 59: Tunnel Mode



Note: The OA-700 supports only Tunnel Mode.

IPSEC PROTOCOLS

The IPsec protocol suite consists of two protocols:

- “**Authentication Header (AH)**”
- “**Encapsulating Security Payload (ESP)**”

AUTHENTICATION HEADER (AH)

An **Authentication Header (AH)** for an IP permits communicating parties to verify that data was not modified in transit and that it was genuinely transmitted from the apparent source.

This protocol provides a means to verify the authenticity/integrity of the content and origin of a packet. A packet can be authenticated by the checksum calculated via hash-based message authentication code (HMAC) using a secret key and either MD-5 or SHA-1 hash functions.

- **Message Digest version 5 (MD5)** - An algorithm that produces a 128-bit hash (also called a digital signature or message digest) from a message of arbitrary length and a 16-byte key. The resulting hash is used, like a fingerprint of the input, to verify content and source authenticity and integrity.
- **Secure Hash Algorithm-1 (SHA-1)** - An algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces.

ENCAPSULATING SECURITY PAYLOAD (ESP)

An **Encapsulation Security Payload (ESP)** format for IP is applied to encrypt the data. This provides for enhanced security of the data packet and protects it against eavesdropping during transit.

The ESP protocol provides a means to ensure privacy (encryption), source authentication, and content integrity (authentication). In tunnel mode it encapsulates the entire IP packet (header and payload), and then appends a new IP header to the now encrypted packet. This new IP header contains the destination address needed to route the protected data through the network.



Note: The OA-700 supports the ESP protocol, which also provides AH functionality.

ENCRYPTION ALGORITHMS

There are several different encryption algorithms that can be used for closed source versions of IPsec. However, the most commonly used algorithms are “3DES” and “AES”. These algorithms are used for encrypting IP packets.

- **Data Encryption Standard (DES)** - A cryptographic block algorithm with a 64-bit key.
- **Triple DES (3DES)** - A more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 192-bit key.
- **Advanced Encryption Standard (AES)** - AES uses a 128-bit, 192-bit, and 256-bit keys.

INTERNET KEY EXCHANGE

Internet Key Exchange (IKE) defines the mechanism to establish SA's (Security Association) requirements to secure packets between the two IPsec peers.

The tunnel negotiation happens using IKE protocol. IKE uses Internet Security Association and Key Management Protocol (ISAKMP) as the framework to send the messages. IKE messages are sent using UDP port number 500. For secure communication, both ISAKMP SA and IPsec SA have to be established.

The system decides which packets are to be processed by IPsec using a policy, based on the IP addresses, ports, etc. With each policy, a [Security Association \(SA\)](#) is associated. You should mainly configure the encryption algorithm and authentication algorithm that should be used. The cryptographic key should be configured.

SECURITY ASSOCIATION (SA)

SA is an unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. Full bidirectional communication requires at least two SAs, one for each direction. The main components of SA are the transform details that are used to protect the data.

The tunnel negotiation happens in two phases.

PHASE 1

Phase 1 is also called as the "**Main Mode**". The objective of "Phase 1" is to establish a secure channel, authenticate the negotiating parties, and generate shared keys to protect IKE protocol messages.

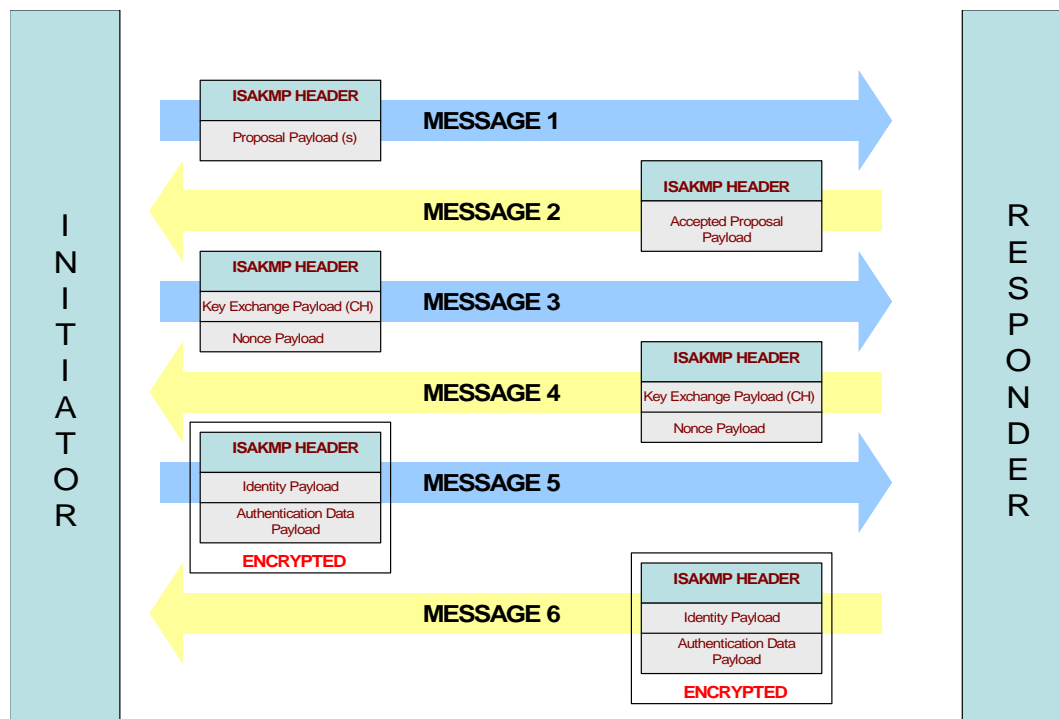


Figure 60: Phase 1 Negotiation - Main Mode

The above figure shows the basic Main mode message exchanges. In the main mode, the negotiating parties use six messages. The first two messages to negotiate the security policy that will be used to protect the phase II messages. The next two messages perform a Diffie-Hellman key exchange and pass nonces (random numbers sent for signing) to each other. The last two messages are used to authenticate the peers. To authenticate peers, the following can be used:

- **Pre-shared keys (PSK)** - A shared secret is distributed out-of-band to the peers. The peers use this information and nonce parameters to create a hash that is used to authenticate messages. PSK is a secret alpha-numeric key that is created by the person configuring the IPsec configuration. This "secret password" is exactly the same on all the computers authenticating the connection and is case-sensitive.
- **Digital Signatures (RSA or DSS)**- Certificates of the peers are exchanged in the last two messages and hashes are calculated over these certificates to authenticate each other. A "**RSA Key**" is an authentication method that uses a program to generate a set of authentication keys. This program is built into IPsec.

PHASE II

This phase is also called "**Quick Mode**". It is used to establish the IPsec SA and generate the new keying material. The figure below shows the Quick mode message exchanges:

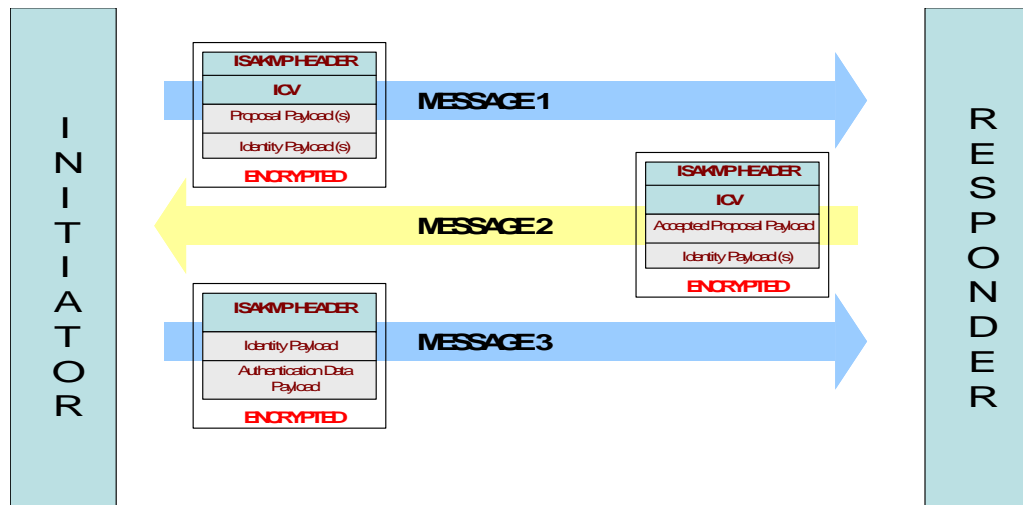


Figure 61: Phase 2 Negotiation - Quick Mode

A full Diffie-Hellman key exchange may be done to provide Perfect Forward Secrecy (PFS).

BENEFITS OF IPSEC ENABLED VPN

The following are the benefits of using IPsec - VPN:

- Connects machines inside two private-address cloud (For e.g., India branch and California headquarters).
- Reduces the operational costs versus traditional WAN since VPN works over the public network (Internet).
- Extended geographic connectivity.
- Reduces transit time and transportation costs for remote users.
- Improves productivity.
- Simplifies network topology.
- Provides global networking opportunities.
- Provides telecommuter support.

DEFAULT CONFIGURATION SETTING ON OA-700

To ease the setup of IPsec tunnel, OA-700 provides the following default configurations:

- If an IKE policy is not configured, the '**default**' ike policy is applied to the crypto map. Following are the default values for IKE policy:
 - i. Default proposal in ike policy: **sha1-aes128**
 - ii. Default PFS group in ike policy: **pfs group2**
 - iii. Default IPsec security-association lifetime in seconds: **28800**
 - iv. Default IKE lifetime in seconds: **86400**
- Default authentication mechanism: **Pre-shared Keys (PSK)**
- If a transform set is not configured, the '**default**' transform set is applied to the crypto map. Following are the default values for transform-set:
 - i. esp-sha1-aes256
 - ii. esp-sha1-3des
 - iii. esp-md5-aes256
 - iv. esp-md5-3des
- If a crypto map is not configured, you can attach the '**default**' crypto map to an interface. Following are the default values within a crypto map:
 - i. Default IKE policy in crypto map: '**default**' ike policy
 - ii. Default transform set in crypto map: '**default**' transform set
 - iii. Default PFS group in crypto map: **pfs group2**.
 - iv. Default lifetime in Seconds for a crypto map: **28800**

IPSEC VPN CONFIGURATION

Refer to the following sections for configuring IPsec:

- [“IPsec VPN Configuration Steps”](#)
- [“IPsec VPN Configuration Flow”](#)
- [“IPsec Configuration Commands”](#)
- [“IPsec VPN Show Commands”](#)

IPSEC VPN CONFIGURATION STEPS

The following are the steps to configure IPsec VPN on the OA-700:

Step 1: Configure the **match-lists** with the pre-configured common classifiers. (Refer to the [“Common Classifiers”](#) chapter in this guide).

Step 2: Configure a pre-shared key. See [“IPsec Configuration with Pre-shared Key”](#)

OR

Configure X.509 certificates. See [“IPsec Configuration with X.509 Certificates”](#)

Step 3: Configure IKE policy. See [“To Configure an IKE Policy”](#)

Step 4: Configure a Transform Set. See [“To Configure Transform-set in IPsec”](#)

Step 5: Configure Crypto Map. See [“To Configure IPsec Crypto Map”](#)

Step 6: Enter the Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0  
ALU(config-if GigabitEthernet7/0)#
```

Step 7: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 8: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-  
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address  
20.20.20.20/24
```

Step 9: Attach the configured crypto map to an interface. See [“To Attach Crypto Map to an Interface”](#)

Step 10: Configure Dead Peer Detection. See [“Dead Peer Detection \(DPD\)”](#) (Optional)

Step 11: Know the default values allowed by the OA-700. See [“Default Configuration Setting on OA-700”](#)

Step 12: View the IPsec configuration. See [“IPsec VPN Show Commands”](#).

IPSEC VPN CONFIGURATION FLOW

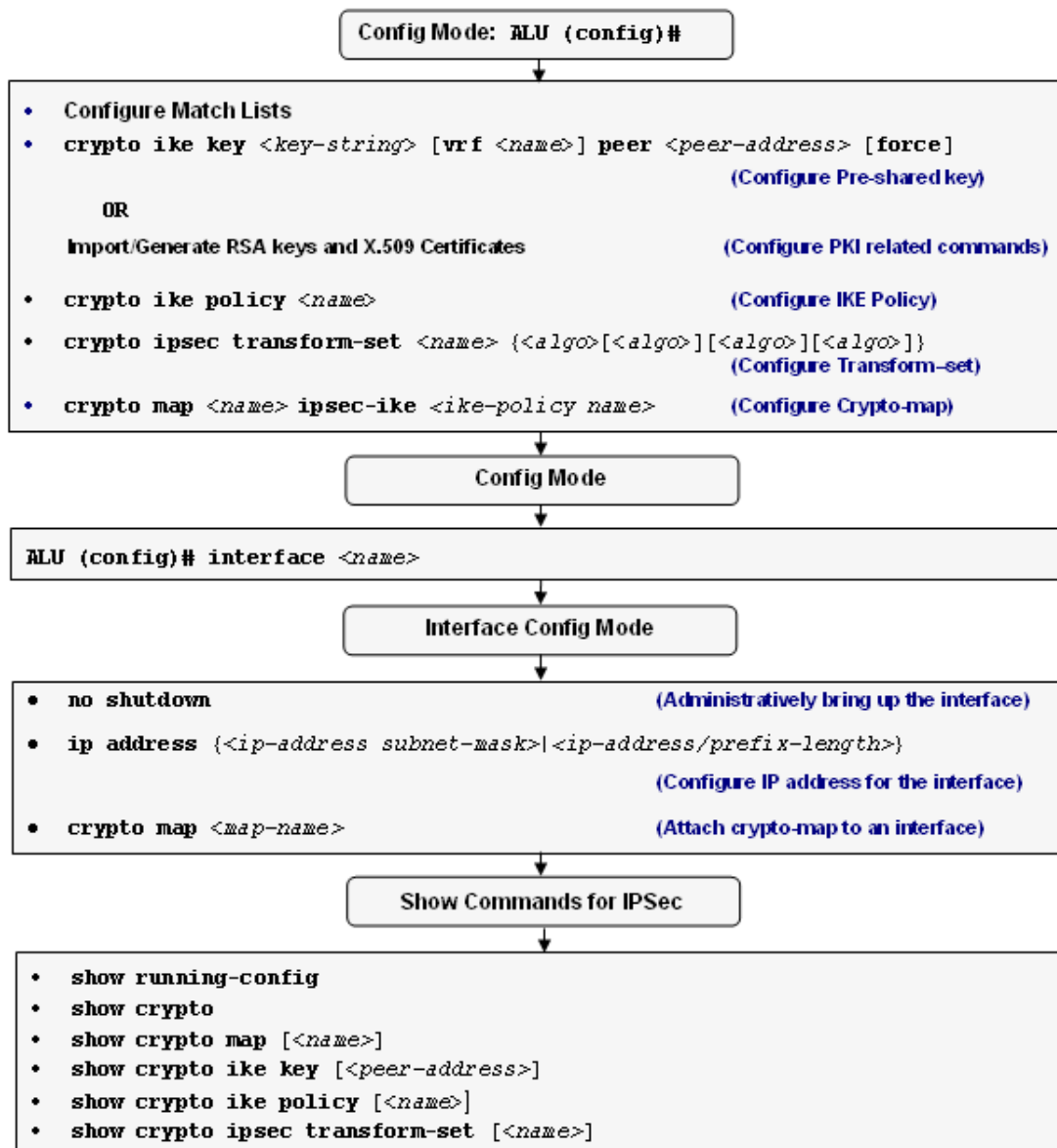


Figure 62: IPsec Configuration Flowchart

IPSEC CONFIGURATION COMMANDS

This section details the commands used in configuring IPsec VPN.

TO CONFIGURE THE MATCH-LISTS

To get a concise and terse outlook on the methods to configure the match-lists, please refer “**Common Classifiers**” chapter in this guide.

To specify the subnets, which need to communicate with each other, match-list (access-list) needs to be configured. This match-list is called by the crypto map command.

In the OA-700, a wide variety of match-lists can be defined. However, a well-defined subset of match-lists can be used for IPsec tunnel (a match-list should not have ‘any any’ option). The match-list should not contain multiple rules or another nested match-list/list. A rule should not have the ‘port range’ or ‘interfaces’ keywords.

However, these constraints can be overcome by applying multiple crypto maps to the same interface.

For Example:

```
match-list m1
  ip prefix 10.0.0.0/8 prefix 9.0.0.0/8
```

IPSEC CONFIGURATION WITH PRE-SHARED KEY

Command (in CM)	Description
<code>crypto ike key <key-string> [vrf <name>] peer <peer-address> [force]</code>	This command is used to configure a pre-shared key.
<code>no crypto ike key <key-string> [vrf <name>] peer <peer-address></code>	This ‘no’ command removes the configured pre-shared key.

The Pre-shared key is used to authenticate peers. This key is same on both the IPsec gateways. It is denoted in the form of a key-string. The “**force**” keyword edits or modifies the IKE keys, which are already configured.



Note: The IKE key is given by means of a key-string. Currently, the pre-shared-key length is restricted to 128 characters, and the minimum length is 8 characters.

EXAMPLE

```
ALU(config)#crypto ike key top_secret1612 peer 10.10.1.2
```

```
ALU(config)#crypto ike key "!netsecret!" peer 202.54.30.100
```

IPSEC CONFIGURATION WITH X.509 CERTIFICATES

Public Key Infrastructure (PKI) will manage all the certificates for authentication in the ALU domain. PKI provides a framework to verify the identity of each entity in a given domain. It includes the requesting, issuing, signing and validating of the public key certificate. The purpose of a public key infrastructure is to manage keys and certificates. By managing keys and certificates through a PKI, an organization establishes and maintains a trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

TO GENERATE A RSA KEY PAIR

Command (in CM)	Description
<code>crypto key generate rsa <512-4096> <name> [bg]</code>	This command generates an RSA key pair


If the key modulus is greater than 2000, it can take few minutes to generate the keys. **[bg]** will generate the keys in the background and free the CLI. Use "bg" to generate the keys in the background and proceed with other configurations that do not depend on the key generation.

EXAMPLE

```
ALU(config)#crypto key generate rsa 1024 exampleKey
```

TO IMPORT A RSA KEY

The RSA keys can be imported instead of generating them on the OA-700.

Command (in CM)	Description
<code>crypto key import rsa <name> [fpkey <file-path> ftp: http: https: scp: tftp:]</code>	This command imports an RSA key pair from a remote location.  Note: Currently, SCP option is not supported.

EXAMPLE

```
ALU(config)#crypto key import rsa testKey ftp:
```

To CONFIGURE A CA IDENTITY

Command (in CM)	Description
<code>crypto ca identity <name></code>	This command configures a CA identity with the name specified.




Note: Entering this command changes the mode to ca-identity mode.

EXAMPLE

```
ALU(config)#crypto ca identity ALUCA
```

To IMPORT A CA CERTIFICATE

Command (in CA Identity CM)	Description
<code>import ca-cert [fpkey <file-path> ftp: tftp: http: https: scp:]</code>	This command imports a CA certificate.  Note: Currently, SCP option is not supported.

EXAMPLE

```
ALU(ca-ALUCA)#import ca-cert ftp:
```



Note: X.509 certificates received during the IKE negotiation are automatically authenticated by going up the trust chain until a self-signed root CA certificate is reached.


To CONFIGURE THE SUBJECT-NAME FOR A CERTIFICATE SIGNING REQUEST (CSR)

Command (in CA Identity CM)	Description
<code>subject-name <subject-name></code>	This command specifies the subject distinguished name that would appear in the certificate request for this CSR, if generated on the OA-700.

EXAMPLE

```
ALU(ca-ALUCA)#subject-name /CN=Bart Simpson/O=ALU/C=US
```


To Import A CRL

Command (in CA Identity CM)	Description
<code>import crl [fpkey <file-path> ftp: tftp: http: https: scp:]</code>	<p>This command imports a CRL from the remote location.</p>  <p>Note: Currently, SCP option is not supported.</p>

EXAMPLE

```
ALU(ca-ALUCA)# import crl ftp:
```

To Import A SIGNED CERTIFICATE

Command (in CA Identity CM)	Description
<code>import signed-cert <name> [fpkey <file-path> ftp: tftp: http: https: scp:]</code>	<p>This command imports an X.509 certificate signed by the CA from a remote location.</p>  <p>Note: Currently, SCP option is not supported.</p>

EXAMPLE

```
ALU(ca-ALUCA)#import signed-cert cert_Simpson ftp:
```

**Note:**

Generate a CSR ([“To Generate a CSR”](#)) and export the CSR ([“To Export a CSR”](#)) from the OA-700 to a remote location to generate the X.509 signed certificate on the OA-700.


To Generate A CSR

Command (in CM)	Description
<code>crypto certificate-request <name> generate key-name <name> ca <name></code>	This command generates a CSR for the specified CA.

EXAMPLE

```
ALU(config)# crypto certificate-request req_Simpson generate
key-name exampleKey ca ALUCA
```


To EXPORT A CSR

Command (in CM)	Description
<code>crypto certificate-request <name> export [fpkey <file-path> ftp: tftp: scp:]</code>	<p>This command exports the CSR from the OA-700 to a remote location.</p> <p>If none of the optional arguments are specified, then the command will have the same effect as the “To View CSR Details” command.</p> <p> Note: Currently, SCP option is not supported.</p>

EXAMPLE

```
ALU(config)# crypto certificate-request req_Simpson export ftp:
```

To ADD THE IMPORTED CERTIFICATE/KEY TO IPSEC DATABASE

Command (in CM)	Description
<code>crypto certificate-database refresh</code>	<p>This command adds the imported certificate or key to the IPsec database.</p> <p>This operation need not be performed after every certificate/key import, but once all the certificates/keys are imported.</p> <p> Note: The crypto certificates will take into effect only after issuing the ‘refresh’ command.</p>

EXAMPLE

```
ALU(config)# crypto certificate-database refresh
```

To Configure a Strict CRL Policy

By default, the OA-700 has a lenient CRL policy, i.e., even if the CRL is not present (not imported) or expired, the peer's certificate will be accepted. There is an option of making this CRL policy strict.


Command (in CM)	Description
<code>crypto crl-check strict</code>	This command makes the CRL policy strict. It ensures that if no CRL is present or if the CRL is already expired, then no negotiation takes place until a new CRL is imported.
<code>no crypto crl-check strict</code>	This command makes the CRL policy lenient.

EXAMPLE

```
ALU(config)# crypto crl-check strict
ALU(config)# no crypto crl-check strict
```

To Import a Peer's Self-Signed Certificate

The peer's self-signed certificate can be imported to override the CA check. This can be done if the peer is not enrolled with any of the trusted CAs and if the peer is trusted. Thus one does not have to rely on the certificate to be transmitted by the peer as part of the IKE protocol.

Command (in CM)	Description
<code>crypto peer-certificate <name></code> <code>import [fpkey <file-path></code> <code> ftp: tftp: http: https: scp:]</code>	This command imports trusted peer certificates in the OA-700.  Note: Currently, SCP option is not supported.

EXAMPLE

```
ALU(config)# crypto peer-certificate cert_Bouvier import ftp:
```

To CONFIGURE AN IKE IDENTITY

Command (in CM)	Description
<code>crypto ike identity <name></code> <code>[force]</code>	This command configures an IKE identity. Entering this command changes the mode to ike-identity mode.

EXAMPLE

```
ALU(config)# crypto ike identity exampleIdentity
```



Note: The “force” keyword is used to modify or edit the IKE policy in use.

To CONFIGURE PEER IDENTITY

Command (in IKE Identity CM)	Description
<code>peer-id {dn fqdn user-fqdn}</code> <code><name> address <ip-address></code>	This command configures an ID for the peer.

EXAMPLE

```
ALU(ike-identity-exampleidentity)# peer-id user-fqdn  
selma_bouvier@alcatel-lucent.com
```

To SPECIFY THE ISSUER (CA) OF THE PEER'S CERTIFICATE

Command (in IKE Identity CM)	Description
<code>peer-ca <name></code>	This command specifies the issuer (CA) of the peer's certificate.

EXAMPLE

```
ALU(ike-identity-exampleidentity)# peer-ca CN=ALU,  
OU=Certificate Authority, C=US
```

To CONFIGURE SELF IDENTITY

Command (in IKE Identity CM)	Description
<code>my-id {dn fqdn user-fqdn} <name> address <ip-address></code>	This command configures self identity.

EXAMPLE

```
ALU(ike-identity-exampleidentity)# my-id dn /CN=Bart Simpson/
O=ALU/C=US
```

To SPECIFY THE ISSUER (CA) OF THE USER'S CERTIFICATE

Command (in IKE Identity CM)	Description
<code>my-ca <name></code>	This command specifies the issuer (CA) of the user's certificate. This is an optional command.

EXAMPLE

```
ALU(ike-identity-exampleidentity)# my-ca CN=ALU, OU=Certificate
Authority, C=US
```

To SPECIFY THE CERTIFICATE TO BE USED

Command (in IKE Identity CM)	Description
<code>my-cert <name></code>	This command specifies the imported signed certificate to be used during IKE negotiation. This should be one among the certificates imported under the "To Import a Signed Certificate" command.

EXAMPLE

```
ALU(ike-identity-exampleidentity)# my-cert cert_Simpson
```



To SPECIFY THE PEER'S PUBLIC KEY

Command (in IKE Identity CM)	Description
<code>peer-cert <name></code>	This command specifies the self signed peer's certificate. This can be used if a trusted peer is not enrolled to any of the CAs.

EXAMPLE

```
ALU(ike-identity-exampleidentity)# peer-cert cert_robert
```

To EXPORT RSA KEYS

Command (in CM)	Description
<code>crypto key export rsa <name> [fpkey <file-path> ftp: tftp: scp:]</code>	<p>This command exports the RSA keys from the OA-700. If none of the optional arguments are used, it works like a show command.</p>  <p>Note: Currently, SCP option is not supported.</p>

EXAMPLE

```
ALU(config)# crypto key export rsa examplekey tftp:
```

To DELETE A CA CERTIFICATE

Command (in CM)	Description
<code>crypto ca-cert <name> delete</code>	This command deletes the specified CA certificate.

EXAMPLE

```
ALU(config)# crypto ca-cert ALUca delete
```

TO DELETE A SIGNED CERTIFICATE

Command (in CM)	Description
<code>crypto signed-cert <name> delete</code>	This command deletes the specified signed certificate.

EXAMPLE

```
ALU(config)# crypto signed-cert cert_Simpson delete
```

TO DELETE A PEER CERTIFICATE

Command (in CM)	Description
<code>crypto peer-certificate <name> delete</code>	This command deletes the specified peer certificate.

EXAMPLE

```
ALU(config)# crypto peer-certificate cert_Bouvier delete
```

TO DELETE AN RSA KEY PAIR

Command (in CM)	Description
<code>crypto rsa-key <name> delete</code>	This command deletes the specified RSA key pair.


EXAMPLE

```
ALU(config)# crypto rsa-key examplekey delete
```

INTERNET KEY EXCHANGE (IKE) POLICY

The purpose of IKE is to establish a secure channel. The security is based on an exchange, where a safe key is negotiated without being transmitted. For instance, the use of a pre-shared key to set up a secure communication channel. IKE uses this secure channel to negotiate the final keys. The more often the key is changed, the more a channel is secure.

TO CONFIGURE AN IKE POLICY

Command (in CM)	Description
<code>crypto ike policy <name></code> <code>[force]</code>	Use this command to configure a IKE policy. The policy name can be a maximum of 128 characters.
<code>no crypto ike policy <name></code>	This command deletes the IKE policy.  Note: An ike policy cannot be deleted if it is used by a crypto map. The ike policy has to be first removed from the crypto map and then deleted.


EXAMPLE

```
ALU(config)# crypto ike policy P1
ALU(config-crypto-ike-policy-P1)#
```



Note: The “force” keyword is used to modify or edit an IKE policy in use.

To CONFIGURE AN IKE PROPOSAL

Command (in IKE Policy CM)	Description
<pre>proposal {<algo>[<algo>][<algo>] [<algo>]...}</pre>  <p>Note: Options for algo are: md5-aes128 md5-aes192 md5- aes256 md5-des md5-3des sha1-aes128 sha1-aes192 sha1-aes256 sha1-des sha1- 3des</p>	<p>Use this command to configure an IKE proposal.</p> <p>You can configure a maximum of 4 proposals.</p>
<pre>no proposal</pre>	<p>This command deletes the proposal configured for the IKE policy.</p> <p>The 'no' command resets the IKE policy to its default.</p>



Note: If no proposal is configured for an IKE policy, **sha1-AES-128** is taken as the default proposal.

EXAMPLE

```
ALU(config-crypto-ike-policy-P1)# proposal md5-aes-128
```

```
ALU(config-crypto-ike-policy-P1)# no proposal
```

To CONFIGURE IPSEC SA LIFETIME

IKE is used for SA negotiation. It requires a proposal to be configured so that a secure channel can be established to authenticate the negotiating parties. When both lifetime in kilobytes and lifetime in seconds is set, re-negotiation of new SA is triggered depending on which lifetime expires first. When re-keying happens, both lifetimes get reset.

Command (in IKE Policy CM)	Description
<code>ipsec security-association lifetime {kilobytes <512-2147483647>/seconds <540-86400>}</code>	This command is used to configure the SA lifetime in kilobytes/seconds.
<code>no ipsec security-association lifetime {kilobytes/seconds}</code>	The 'no' command resets the IPsec SA lifetime in seconds value to its default. The 'no' command removes the IPsec security-association lifetime in kilobytes value.



Note: IPsec security lifetime associations has a default value of **28800** seconds.

There is no default value for IPsec security-association lifetime in Kilobytes.

EXAMPLE

```
ALU(config-crypto-ike-policy-P1)# ipsec security-association
lifetime kilobytes 5400
```

```
ALU(config-crypto-ike-policy-P1)# ipsec security-association
lifetime seconds 5400
```

```
ALU(config-crypto-ike-policy-P1)# no ipsec security-association
lifetime kilobytes
```

```
ALU(config-crypto-ike-policy-P1)# no ipsec security-association
lifetime seconds
```

To CONFIGURE IKE LIFETIME

Command (in IKE Policy CM)	Description
<code>lifetime seconds <540-86400></code>	This command is used to configure a IKE lifetime.
<code>no lifetime seconds</code>	The 'no' command resets the IKE lifetime to its default.




Note: Default IKE lifetime = 86400 seconds.

EXAMPLE

```
ALU(config-crypto-ike-policy-P1)# lifetime seconds 4096
```

```
ALU(config-crypto-ike-policy-P1)# no lifetime seconds
```

To CONFIGURE PFS (PERFECT FORWARD SECRECY) GROUP

Command (in IKE Policy CM)	Description
<code>pfs {group1 group2 group5}</code>	This command is used to configure a PFS group.  Note: If the PFS group is not explicitly configured, group2 is used as the default PFS.
<code>no pfs</code>	The 'no' command resets the PFS group to default.

EXAMPLE

```
ALU(config-crypto-ike-policy-P1)# pfs group1
```

```
ALU(config-crypto-ike-policy-P1)# no pfs
```

TO CONFIGURE AUTHENTICATION TYPE

Command (in IKE Policy CM)	Description
<code>authentication {pre-shared rsa-sig}</code>	This command configures the authentication type to be used during IKE negotiation.

EXAMPLE

```
ALU(config-crypto-ike-policy-P1)# authentication pre-shared
```



Note: If the Authentication type is not explicitly configured, default **pre-shared** is used.

TO CONFIGURE TRANSFORM-SET IN IPSEC

A transform set represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.



Note: You can specify a maximum of **4 values** in a transform set.

Command (in CM)	Description
<code>crypto ipsec transform-set <name> {<algo>[<algo>][<algo>] [<algo>]} [force]</code>	This command creates a transform-set.



Note: The “force” keyword is used to modify or edit the transform-set in use.

Options for proposal under transform-set:

- `esp-md5-3des` encapsulation with MD5 and 3DES encryption
- `esp-md5-aes128` encapsulation with MD5 and 128 bit AES encryption
- `esp-md5-aes192` encapsulation with MD5 and 192 bit AES encryption
- `esp-md5-aes256` encapsulation with MD5 and 256 bit AES encryption
- `esp-md5-des` encapsulation with MD5 and 56 bit DES encryption
- `esp-sha1-3des` encapsulation with SHA1 and 3DES encryption
- `esp-sha1-aes128` encapsulation with SHA1 and 128 bit AES encryption
- `esp-sha1-aes192` encapsulation with SHA1 and 192 bit AES encryption
- `esp-sha1-aes256` encapsulation with SHA1 and 256 bit AES encryption
- `esp-sha1-des` encapsulation with SHA1 and 56 bit DES encryption



Note: The OA-700 will have a default transform-set configuration with parameters **esp-sha1-aes256 esp-sha1-3des esp-md5-aes256 esp-md5-3des**.

EXAMPLE

```
ALU(config)# crypto ipsec transform-set netset esp-sha1-aes256
ALU(config)# crypto ipsec transform-set myset esp-md5-3des esp-
md5-aes128 esp-md5-aes192
```

TO DELETE A TRANSFORM-SET GLOBALLY

This command deletes the transform-set from the global configuration mode. If a transform-set is being used by any crypto map, it is prohibited from deletion. Hence, the transform-set must be first disabled from the crypto map and then deleted.

Command (in CM)	Description
<code>no crypto ipsec transform-set <name></code>	This command deletes a transform-set.

EXAMPLE

```
ALU(config)# no crypto ipsec transform-set netset
```


To CONFIGURE IPSEC CRYPTO MAP

Crypto map entries created for IPsec pull together various parts used to set up IPsec security associations that include:

- Which traffic should be protected by IPsec (as defined by match-list earlier)
- Where the IPsec-protected traffic should be sent (remote IPsec peer).
- What kind of IPsec security to be applied to this traffic (as configured by the transform-set)
- Security associations established via IKE.

Command (in CM)	Description
<code>crypto map <name> ipsec-ike <ike-policy name> } [force]</code>	This command creates a crypto map, and attaches an IKE policy to it. Enter the IKE policy name as 'default' to use the default IKE policy.



Note: The crypto map name can have a maximum of 32 characters.
Force - This option is used to modify a crypto map when it is applied to an interface.

EXAMPLE

```
ALU(config)# crypto map exampleMap ipsec-ike examplePolicy
ALU(config-crypto-map-exampleMap)#
```

To ATTACH MATCH-LIST TO A CRYPTO MAP

Command (in Crypto Map CM)	Description
<code>match <match-list name></code>	This command attaches a match-list to a crypto map.
<code>no match <match-list name></code>	The 'no' command detaches the specified match-list attached to a crypto map.





Note: If you try to attach a match-list to a crypto map that already has one, it overrides the existing match-list.

EXAMPLE

```
ALU(config-crypto-map-exampleMap)# match matchlist1
ALU(config-crypto-map-exampleMap)# no match matchlist1
```

To Attach a Peer to a Crypto Map


Command (in Crypto Map CM)	Description
<code>peer <ipaddress></code>	<p>This command attaches a peer to a crypto map.</p>  <p>Note: You can attach a maximum of four peers to a crypto map.</p>
<code>no peer <ipaddress></code>	<p>The 'no' command detaches the specified peer attached to a crypto map.</p>  <p>Note: You cannot delete a peer from the crypto map if the crypto map is attached to an interface.</p>

EXAMPLE

```
ALU(config-crypto-map-exampleMap)# peer 100.10.61.20
```

```
ALU(config-crypto-map-exampleMap)# no peer 100.10.61.20
```

To Attach a Transform Set to a Crypto Map

Command (in Crypto Map CM)	Description
<code>transform-set <name></code>	<p>This command attaches a transform-set to a crypto map.</p>
<code>no transform-set</code>	<p>The 'no' command detaches the specified transform-set attached to a crypto map.</p>  <p>Note: A transform-set must be first detached from the crypto map to delete it globally.</p>




Note: If no transform set is attached to a crypto map, **Default** transform set is used.

EXAMPLE

```
ALU(config-crypto-map-exampleMap)# transform-set netset
```

```
ALU(config-crypto-map-exampleMap)# no transform-set
```

To ATTACH PFS GROUP TO A CRYPTO MAP

Command (in Crypto Map CM)	Description
<code>pfs [group1 group2 group5]</code>	<p>This command attaches a PFS group to a crypto map.</p>  <p>Note: If no PFS group is attached to a crypto map, group2 PFS is used.</p>
<code>no pfs</code>	The 'no' command disables PFS completely.

EXAMPLE

```
ALU(config-crypto-map-exampleMap)# pfs group1
```

```
ALU(config-crypto-map-exampleMap)# no pfs
```

To CONFIGURE LIFETIME FOR A CRYPTO MAP

Command (in Crypto Map CM)	Description
<code>lifetime {kilobytes <512-2147483647>/seconds <540-86400>}</code>	This command configures lifetime for a crypto map. Use Kilobytes keyword to configure lifetime in kilobytes, and use Seconds keyword to configure lifetime in seconds for a crypto map.
<code>no lifetime {kilobytes/seconds}</code>	The 'no' command resets the seconds lifetime to default. If set in kilobytes, the 'no' command removes the kilobytes lifetime value.



Note: Lifetime has a default value of **28800** seconds.

There is no default value for lifetime in Kilobytes.

EXAMPLE

```
ALU(config-crypto-map-exampleMap)# lifetime seconds 1000
```

```
ALU(config-crypto-map-exampleMap)# lifetime kilobytes 1005236
```

```
ALU(config-crypto-map-exampleMap)# no lifetime seconds
```

```
ALU(config-crypto-map-exampleMap)# no lifetime kilobytes
```

To Attach an IKE Identity to a Crypto Map

Command (in Crypto Map CM)	Description
<code>ike-identity <name></code>	This command attaches an IKE identity to a crypto map.
<code>no ike-identity</code>	The 'no' command detaches the specified IKE identity attached to a crypto map.



Note: IKE identity should only be attached to a crypto map if the Authentication type is 'rsa-sig'.

EXAMPLE

```
ALU(config-crypto-map-exampleMap)# ike-identity exampleIdentity
ALU(config-crypto-map-exampleMap)# no ike-identity
```

To Attach Crypto Map to an Interface

Crypto map needs to be applied to an interface through which the IPsec traffic flows. Binding a crypto map to an interface instructs the system to evaluate all the interface traffic against the crypto map, and to use the specified policy during connection or security association negotiation.

Command (in ICM)	Description
<code>crypto map <map-name></code>	Enter this command in the Interface Configuration Mode. This command attach a crypto map to an interface.
<code>no crypto map <map-name></code>	This command is used to detach the crypto map attached to an interface. <div data-bbox="915 1459 990 1528" data-label="Image"> </div> <p>Note: You cannot delete a crypto map that is applied to an interface. To delete, first detach the crypto map from the interface.</p>

EXAMPLE

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# crypto map exampleMap
ALU(config-if GigabitEthernet7/0)# no crypto map exampleMap
```

DEAD PEER DETECTION (DPD)

DPD enables IPsec to identify the loss of peer connectivity. It helps to recognize black holes as soon as possible and recover lost resources.

By default, DPD is turned off. A global configuration is available so that all connections follow the same DPD configuration. Each connection can override the global DPD configuration by specifying its own DPD policy in its crypto map.

TO CONFIGURE DPD GLOBALLY

Command (in CM)	Description
<code>crypto ike dpd interval <5-3600> [timeout <5-72000>]</code>	This command configures the DPD globally with the interval in seconds for which the keep-alive messages will be sent, and the time-out in seconds after which the peer will be declared to be dead. The default value for DPD time-out is three times that of the DPD interval specified.
<code>no crypto ike dpd</code>	This command disables DPD for IPsec globally.

EXAMPLE

```
ALU(config)# crypto ike dpd interval 10 timeout 35
```

```
ALU(config)# no crypto ike dpd
```

To CONFIGURE DPD LOCALLY

Command (in Crypto Map CM)	Description
<code>dpd {interval <5-3600> [timeout <5-72000>]/none}</code>	<p>This command configures a DPD at the crypto map mode.</p> <p>This command allows all connections associated with a crypto map to use a DPD policy that is different from the global policy.</p> <p>The keyword 'none' disables DPD for all the connections associated with a crypto map. These connections will not detect Dead Peer.</p> <p>The local DPD configuration is given higher priority than the global DPD configuration.</p>
<code>no dpd</code>	This command removes the local DPD and switches to the global policy.



Note: The default value for DPD time-out is three times that of the DPD interval specified.

EXAMPLE

```
ALU(crypto-map-map1)# dpd delay 15 timeout 60
```

```
ALU(crypto-map-map1)# dpd NONE
```

```
ALU(crypto-map-map1)# no dpd
```



Note: If there is no global DPD defined, both the **dpd none** command and **no dpd** command produce the same result.

IPSEC VPN SHOW COMMANDS

TO VIEW THE RUNNING CONFIGURATION

Command (in SUM/CM)	Description
<code>show running-config</code>	This command displays the running configuration. The output of this command does not show the default configurations.

EXAMPLE

The following example displays the output of the running configuration:

```
ALU# show running-config
```

```
Current Configuration:
!
! NVRAM config last updated at 05:26:39 GMT  Tue Jan 18 2005
from line 0 ! Statlog Configuration !
logging on
logging console debugging
logging os messages informational
logging buffered priority 7
logging buffered size 131072
service timestamps log
!
interface GigabitEthernet7/0
 ip address 2.2.2.2/8
 mac-addr 0000.4567.6789
 no shutdown
!
interface GigabitEthernet7/1
 ip address 1.1.1.2/8
 mac-addr 0000.3456.4567
 no shutdown
!
ip route 3.0.0.0/8 2.2.2.1
!
match-list m1
1 ip prefix 1.0.0.0/8 prefix 3.0.0.0/8
!
! ipsec Policy configuration
!
crypto ike key linux peer 2.2.2.1
! Key in Use (by 1 cryptomap/s)
crypto ike policy ike
 proposal md5-3des
 pfs group2
 ipsec security-association lifetime seconds 590
 lifetime seconds 1500
! Policy in Use (by 1 cryptomap/s)
crypto ipsec transform-set myset esp-md5-3des
```



```

! Transform-Set in Use (by 1 cryptomap/s)

crypto map ALU2 ipsec-ike ike
    peer 2.2.2.1
    match m1
    transform-set myset
    pfs group2
! Applied to : GigabitEthernet7/1
interface GigabitEthernet7/1
    crypto map ALU2
top
!
line vty 4
    transport input none
!
line con 0
!
end
ALU#

```

To View the Crypto Configuration on OA-700

Command (in SUM/CM)	Description
show crypto	This command displays all the configuration details related to IPsec including the default configurations.

EXAMPLE

```

ALU(config)# show crypto

crypto ike identity exampleIdentity
    peer-id user-fqdn fred@flintstones.com
    my-id fqdn @flintstones.com
    my-cert cert_flintstones
crypto ike key topSecret peer 100.1.200.4
crypto ike key anotherTopSecret peer 126.2.34.68
crypto ike dpd interval 15 timeout 60
!crypto ike policy default
!    proposal sha1-aes128
!    ipsec security-association lifetime seconds 28800
!    lifetime seconds 86400
!    pfs group2
crypto ike policy examplePolicy
    proposal sha1-aes256
    ipsec security-association lifetime seconds 28800
    lifetime seconds 7200
    pfs group5
    authentication pre-shared
! Policy in Use (by 1 cryptomap/s)
!crypto ipsec transform-set default
!    esp-sha1-aes256 esp-sha1-3des esp-md5-aes256 esp-md5-3des

```

```

crypto ipsec transform-set exampleT-set esp-shal-aes192 esp-md5-aes192
! Transform-Set in Use (by 1 cryptomap/s) crypto map exampleMap ipsec-
ike examplePolicy
    peer 100.1.200.4
    match exampleMatchList
    transform-set exampleT-set
    pfs group5
    lifetime seconds 3600
    lifetime kilobytes 4096
! Applied to : GigabitEthernet3/1
interface GigabitEthernet3/1
    crypto map exampleMap
!crypto ipsec profile default
!    ike-policy default
!    transform-set default
!    pfs group2
!    lifetime seconds 28800
! Not Applied to Any Interface

```

To VIEW CRYPTO MAP

Command (in SUM/CM)	Description
show crypto map [<name>]	This command displays the details of all the crypto maps configured. If a crypto map is specified, then the details of the specified crypto map is displayed.

EXAMPLE

```

ALU(config)# show crypto map
crypto map ALU2 ipsec-ike ike
    peer 202.192.192.1
    match m1
    transform-set default
    pfs group2
! Applied to : GigabitEthernet7/1
interface GigabitEthernet7/1
    crypto map ALU2

```

The following example displays a the details for a specified crypto map:

```
ALU# show crypto map india
```

```

crypto map india ipsec-ike panchsheel
    peer 202.192.192.2
! default transform set
    pfs group2
    lifetime seconds 86400

```

To VIEW CRYPTO IKE KEY

Command (in SUM/CM)	Description
show crypto ike key [<i><peer-address></i>]	This command displays the details of all the IKE keys configured.

EXAMPLE

```
ALU(config)# show crypto ike key

crypto ike key top_secret1612 peer 10.10.1.2

ALU(config)# show crypto ike key 3.3.3.3

crypto ike key linux123 peer 3.3.3.3
```

To VIEW CRYPTO IKE POLICY

Command (in SUM/CM)	Description
show crypto ike policy [<i><name></i>]	This command displays the details of all the IKE policies configured. If the IKE policy name is specified, the details of the specified IKE policy is displayed.

EXAMPLE

```
ALU(config)# show crypto ike policy
crypto ike policy ALU1
    proposal md5-3des
    ipsec security-association lifetime seconds 28800
    lifetime seconds 3600
    pfs group2

crypto ike policy ALU2
    proposal md5-3des
    ipsec security-association lifetime seconds 28600
    lifetime seconds 2500
    pfs group5
```

The following is an example of the crypto policy with default values:

```
ALU(config)# show crypto ike policy

crypto ike policy sample
! proposal sha1-aes128
! ipsec security-association lifetime seconds 28800
! lifetime seconds 3600
! pfs group2
```

```
ALU(config)# show crypto ike policy ALU1
```

```
crypto ike policy ALU1
  proposal md5-3des
  pfs group2
  ipsec security-association lifetime seconds 28800
  lifetime seconds 3600
```

To View Crypto IPsec Transform Set

Command (in SUM/CM)	Description
show crypto ipsec transform-set [<name>]	This command displays all the transform-sets configured. If the Transform-set name is specified, it displays the details of the specified transform-set.

EXAMPLE

```
ALU# show crypto ipsec transform-set
```

```
crypto ipsec transform-set myset
  esp-md5-3des
! Transform-Set in Use (by 1 cryptomap/s)
```

```
ALU# show crypto ipsec transform-set myset
```

```
crypto ipsec transform-set myset esp-md5-3des
```

To VIEW IPSEC SECURITY ASSOCIATION

Command (in SUM/CM)	Description
<pre>show crypto ipsec sa [interface <name> map <name> peer <ip-address>]</pre>	<p>This command displays IPsec SA details, the encryption and authentication algorithms used in negotiating SAs.</p> <p>It also displays dynamic information like SPI's and SA-ID's, information/statistics about all the VPN tunnels that are active and in use.</p>

EXAMPLE

```
ALU# show crypto ipsec sa

GigabitEthernet3/1
  Crypto Map: ALU Match m1
  Peer 60.60.60.2

*****INBOUND*****

  ESP Algo:crypt:DES-CBC len:64 auth:SHA1-HMAC len:160
  TUNNEL MODE Replay Detection Enabled: Yes
  ESP spi:0xc3fb59c time-left:28793secs/0kb esp-sa-id:12
  Decaps:7 Decrypt:7 Auth:7 Errors:0

*****OUTBOUND*****

  ESP Algo:crypt:DES-CBC len:64 auth:SHA1-HMAC len:160
  TUNNEL MODE Replay Detection Enabled: Yes
  ESP spi:0x541a7498 time-left:28793secs/0kb esp-sa-id:16
  Encaps:7 Encrypt:7 Auth:7 Errors:0
```

SHOW COMMANDS FOR PKI**TO VIEW PUBLIC KEYS GENERATED**

Command (in SUM/CM)	Description
<code>show crypto rsa-key</code>	Displays the list of all rsa-keys generated on the OA-700 or imported. It does not display the keys but only the names.
<code>show crypto rsa-key <name></code>	Displays the details of the key specified.
<code>show crypto rsa-key [<name> <public-key>]</code>	Displays the details of the public key.

EXAMPLE

```
ALU(config)# show crypto rsa-key
```

```
KEY NAME                LENGTH
-----                -
exampleKey              512
key_Bruns               1024
```

```
ALU(config)# show crypto rsa-key exampleKey
```

```
# LENGTH = 512
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBALrZr88JSfTvE9+n4+4oMrXvBuL4yTFtRESB0j9JgslrWtFz0Huv
P16CNBVUSafTXmkpxHJXJWruAvgs3VkvA60CAwEAAQJATCC1Q6p1qj68qgOU5kMK
01mlRUGns+/Zr8fplInbrybL7aUyw0ZbOxwR47nhv2cPJmBEVYBgD3MJBpmoCoQ3
JQIhAPQF4cc793YnqQjDmMZlrU5EgW0+iTv7tZhBfu9Be6hzAiEAXCC2wzozczYb
Vu34ghDwp8Bcr5dyRH1qqKXAWfhj018CIHy5W0o1a01YAhY5pKebJpZ/i0ukeA65
m9qjdlaguKyjAiEAsZOVJsppjyUsN9cbLfi+LITE5s9OzKhpi+0Xbd6xqi0CIQCR
p2uSbE2LoC4r3XovZoVF1mLzZLrC3WZcMKRk0qe00Q==
-----END RSA PRIVATE KEY-----
```

```
ALU(config)# show crypto rsa-key exampleKey public-key
```

```
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALrZr88JSfTvE9+n4+4oMrXvBuL4yTFt
RESB0j9JgslrWtFz0HuvP16CNBVUSafTXmkpxHJXJWruAvgs3VkvA60CAwEAAQ==
-----END PUBLIC KEY-----
```

To VIEW CA IDENTITY

Command (in SUM/CM)	Description
<code>show crypto ca identity</code>	Displays all CA identities
<code>show crypto ca identity <name></code>	Displays the CA identity specified

EXAMPLE

```
ALU(config)# show crypto ca identity
```

```
crypto ca identity SomeOtherCA
      subject-name /O=ALU/C=IN/CN=CM Burns
crypto ca identity ALUCA
      subject-name /CN=Bart Simpson/O=ALU/C=US
```

```
ALU(config)# show crypto ca identity ALUCA
```

```
crypto ca identity ALUCA
      subject-name /CN=Bart Simpson/O=ALU/C=US
```

To VIEW IKE IDENTITY

Command (in SUM/CM)	Description
<code>show crypto ike identity</code>	Displays the details of the all IKE identities configured.
<code>show crypto ike identity <name></code>	Displays the details of the specified IKE identity.

EXAMPLE

```
ALU(config)# show crypto ike identity
```

```
crypto ike identity someOtherIdentity
      peer-id fqdn @www.simpsons.com
      my-id DN /CN=CM Burns/O=ALU/C=IN
      my-cert cert_Burns
crypto ike identity exampleIdentity
      peer-id user-fqdn selma_bouvier@ALU.com
      peer-ca CN=ALU, OU=Certificate Authority, C=US
      my-id DN /CN=Bart Simpson/O=ALU/C=US
      my-cert cert_Simpson
```

```
ALU(config)# show crypto ike identity exampleIdentity
```

```
crypto ike identity exampleIdentity
      peer-id user-fqdn selma_bouvier@ALU.com
      peer-ca CN=ALU, OU=Certificate Authority, C=US
      my-id DN /CN=Bart Simpson/O=ALU/C=US
      my-cert cert_Simpson
```

To VIEW SIGNED CERTIFICATE

Command (in SUM/CM)	Description
<code>show crypto signed-cert</code>	Displays the names of all the signed certificates.
<code>show crypto signed-cert <name></code>	Displays the details of the signed certificate specified in a readable format.
<code>show crypto signed-cert [<name> [pem]]</code>	Displays the details of the signed certificate specified in the base64 pem format.

EXAMPLE

```
ALU(config)# show crypto signed-cert
```

```
cert_Simpson
cert_Burn
```

```
ALU(config)# show crypto signed-cert cert_Simpson
```

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 8 (0x8)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: CN=CA_0x01, O=ALU
    Validity
      Not Before: Jan 27 09:22:03 2006 GMT
      Not After : Jan 27 09:22:03 2007 GMT
    Subject: C=US, O=ALU, CN=Bart Simpson
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (512 bit)
      Modulus (512 bit):
        00:ba:f3:af:cf:09:49:f4:ef:13:df:a7:e3:ee:28:
        32:b5:ef:06:e2:f8:c9:31:6d:44:44:81:d2:3f:49:
        82:c9:6b:5a:d1:73:d0:7b:af:3f:5e:82:34:15:54:
        49:a7:d3:5e:69:29:c4:72:57:25:6a:ee:02:f8:2c:
        dd:59:2f:03:ad
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Comment:
        OpenSSL Generated Certificate
      X509v3 Subject Key Identifier:
        88:75:2D:47:AC:E8:AB:C3:5F:9F:E1:93:6B:7E:07:9C:A3:B0:24:CB
      X509v3 Authority Key Identifier:
        keyid:05:98:D2:25:D3:18:12:A1:C7:4B:7A:98:D2:D8:25:73:2B:6B:AE:B1
        DirName:/CN=CA_0x01/O=ALU
        serial:00

    Signature Algorithm: md5WithRSAEncryption
```



```

0c:30:3a:96:bb:2a:be:6c:53:47:b9:5d:b4:40:1d:0e:4a:85:
f3:99:57:82:07:58:a1:bf:f6:36:3a:03:9b:81:7a:3d:6c:fa:
b7:24:70:78:c4:15:75:4a:58:69:ad:aa:3d:82:f1:ae:1a:76:
82:79:b9:43:05:26:b8:34:cc:59:ee:b6:0b:82:4b:a2:70:2a:
2a:72:4c:1a:c7:a8:74:30:fb:24:52:21:b9:2f:ef:b9:56:ae:
f1:45:75:0b:46:2f:e4:94:ec:8c:b6:99:47:a8:68:c3:a8:0c:
e3:56:f0:bc:54:53:02:ed:c0:17:1e:72:be:7b:fd:11:76:91:
05:db

```

```
ALU(config)# show crypto signed-cert cert_Simpson pem
```

```

-----BEGIN CERTIFICATE-----
MIICLTCCAzagAwIBAgIBCDANBgkqhkiG9w0BAQQFADAhMRAwDgYDVQQDFAdDQV8w
eDAXMQ0wCwYDVQQKEwROZXRkMB4XDTA2MDEyNzA5MjIwM1oXDTA3MDEyNzA5MjIw
M1owMzELMAkGA1UEBhMCVVMxDTALBgNVBAoTBEE5ldEQxFTATBgNVBAMTDEJhcnQg
U2ltcHNvbWJcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC686/PCUn07xPfp+PuKDK1
7wbi+MkxbUREgdI/SYLJa1rRc9B7rz9egjQVVEmn015pKcRyVyVq7gL4LN1ZLwOt
AgMBAAGjggaYwgaMwCQYDVR0TBAIwADAsBg1ghkgBhvhCAQ0EHzYdTB3BlblNTTCBH
ZW5lcmF0ZWQgQ2VydG1maWNhdGUwHQYDVR0OBBYEFih1LUes6KvDX5/hk2t+B5yj
sCTLMEkGA1UdIwRCMECAFAWY0iXTGBKhx0t6mNLYJXMra66xoSWkIzAhMRAwDgYD
VQQDFAdDQV8weDAXMQ0wCwYDVQQKEwROZXRkkgEAMA0GCSqGSIb3DQEBAQUAA4GB
AAwwOpa7Kr5sU0e5XbRAHQ5KhfOZV4IHWKG/9jY6A5uBejls+rckcHjEFXVKWgmt
qj2C8a4adoJ5uUMFJrg0zFnutguCS6JwKipyTBrHqHQw+yRSIbkv771WrvFFdQtG
L+SU7Iy2mUeoMoDONW8LxUUwLtwBcecr57/RF2kQXb
-----END CERTIFICATE-----

```

To VIEW PEER CERTIFICATE

Command (in SUM/CM)	Description
<code>show crypto peer-certificate</code>	Displays the names of all the peer certificates.
<code>show crypto peer-certificate <name></code>	Displays the details of the specified peer certificate in a readable format.
<code>show crypto peer-certificate [<name> [pem]]</code>	Displays the details of the specified peer certificate in the base64 pem format.

EXAMPLE

```
ALU(config)# show crypto peer-certificate
```

```

cert_fred
cert_barney
cert_wilma

```

ALU(config)# show crypto peer-certificate cert_fred

Certificate:

Data:

```

Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=Bedrock, CN=Fred Flintstone/
emailAddress=fred@flintstones.com
Validity
  Not Before: Jun 22 06:56:13 2006 GMT
  Not After : Jul 22 06:56:13 2006 GMT
Subject: C=US, ST=Bedrock, CN=Fred Flintstone/
emailAddress=fred@flintstones.com
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
  Modulus (1024 bit):
    00:cc:77:33:35:10:2c:90:6a:7d:ba:08:5b:97:68:
    eb:ea:91:bb:e2:b7:ac:9d:42:95:36:3a:db:ab:d3:
    38:04:38:9b:34:18:31:22:69:78:de:11:37:7f:1e:
    7f:10:9b:ba:96:60:e3:dd:bd:74:93:cf:dc:ad:c5:
    a7:ca:69:7f:d1:77:33:38:6a:66:89:07:66:d2:08:
    d4:b8:98:3f:e0:99:11:f8:3f:78:9b:27:51:8d:ee:
    5e:e7:2a:5a:3a:d2:dc:dc:f7:45:b9:1e:8e:c2:ed:
    2a:5e:a5:29:03:3d:ab:6e:2d:fd:6c:eb:c5:72:a8:
    54:44:a6:03:70:4e:d0:38:33
  Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier:
A8:80:7E:54:63:61:76:66:DE:E0:98:6C:10:31:6D:EB:1E:9D:4C:46
  X509v3 Authority Key Identifier:
keyid:A8:80:7E:54:63:61:76:66:DE:E0:98:6C:10:31:6D:EB:1E:9D:4C:46
  DirName:/C=US/ST=Bedrock/CN=Fred Flintstone/
emailAddress=fred@flintstones.com
  serial:00
X509v3 Basic Constraints:
  CA:TRUE
Signature Algorithm: md5WithRSAEncryption
2d:b4:af:ef:cb:25:79:fe:11:9a:85:2e:a5:ef:27:9c:87:21:
00:c8:19:89:19:05:ae:6a:2f:d0:02:df:ba:70:e9:ac:81:29:
f2:ff:dc:da:35:e4:d0:43:ec:ec:7c:73:24:c9:52:d8:c9:0a:
90:40:6f:64:df:0d:65:16:bf:96:22:fb:06:fb:6b:0b:17:24:
c2:2e:33:0b:2d:f6:76:ec:8e:e7:9e:cc:4e:c6:fa:25:a2:7f:
4a:79:c9:ba:55:67:a9:74:4e:5e:30:ff:37:13:94:cd:db:47:
26:30:c6:19:38:31:62:12:70:5f:00:e7:80:01:2c:8a:da:d5:
e0:e5

```

```
ALU(config)# show crypto peer-certificate cert_fred pem
```

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAlWgAwIBAgIBADANBgkqhkiG9w0BAQQFADBEMQswCQYDVQQGEwJVUzEQ
MA4GA1UECBMHQmVkcml9jzEYMBYGA1UEAxMPrnJlZCBGbgGluDHNB25lMSMwIQYJ
KoZIHvcNAQkBFhRmcmVkcGZsaW50c3RvbmVzLmNvbTAeFw0wNjA2MjIwNjU2MTNa
Fw0wNjA3MjIwNjU2MTNaMF4xCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdCZWRYb2Nr
MRgwFgYDVQQDEw9GcmVkieZsaW50c3RvbmUxIzAhBgkqhkiG9w0BCQEFWFGZyZWRA
ZmxpbmRzdG9uZXMuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMdzM1
ECyQan26CFuXaOvqkbvit6ydQpU20tur0zgEOJs0GDEiaXjeETd/Hn8Qm7qWYOPd
vXSTz9ytxafKaX/RdzM4amaJB2bSCNS4mD/gmRH4P3ibJlGN7l7nKlo60tzc90W5
Ho7C7SpepSkDPatUlf1s68VyqFREpgNwTtA4MwIDAQABo4G5MIG2MB0GA1UdDgQW
BBSogH5UY2F2Zt7gmGwQMW3rHp1MRjCBhgYDVR0jBH8wfYAUqIB+VGNhdmb4Jhs
EDft6x6dTEahYqRgMF4xCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdCZWRYb2NrMRgw
FgYDVQQDEw9GcmVkieZsaW50c3RvbmUxIzAhBgkqhkiG9w0BCQEFWFGZyZWRAZmxp
bnRzdG9uZXMuY29tggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEA
LbSv78slef4RmoUupe8nnIchAMgZiRkFrmov0ALfundprIEp8v/c2jXk0EPs7Hxz
Jm1S2MkKkEBvZN8NZRa/liL7BvtrCxckwi4zCy32duyO557MTsb6JaJ/SnnJulVn
qXROXjD/NxOUzdtHJjDGGTgxYhJwXwDngAEsitrV40U=
-----END CERTIFICATE-----
```

To VIEW CRL

Command (in SUM/CM)	Description
<code>show crypto crl ca <name></code>	Displays the details of the specified CRL in a readable format.
<code>show crypto crl ca [<name> [pem]]</code>	Displays the details of the specified CRL in the base64 pem format.

EXAMPLE

```
ALU(config)# show crypto crl ca ALUCA
```

```
Certificate Revocation List (CRL):
  Version 1 (0x0)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: /CN=CA_0x01/O=ALU
  Last Update: Jan  9 11:46:37 2006 GMT
  Next Update: Feb  8 11:46:37 2006 GMT
Revoked Certificates:
  Serial Number: 01
    Revocation Date: Jan  9 11:46:12 2006 GMT
  Serial Number: 02
    Revocation Date: Jan  9 11:46:16 2006 GMT
Signature Algorithm: md5WithRSAEncryption
45:6b:da:5f:10:09:77:7c:16:1e:a4:c2:aa:b6:3c:04:d1:ca:
4c:bc:9c:74:07:a7:a4:8a:09:cc:ad:e0:8b:9c:34:9d:05:c0:
63:3b:d7:01:9c:e0:29:44:38:e4:f8:e9:81:69:13:92:f4:14:
f2:a6:7a:75:35:96:f5:12:3f:77:32:ef:c2:a7:28:4b:81:69:
10:a5:05:0d:dd:2f:73:20:70:58:b5:d9:2f:d9:13:c8:c1:20:
c6:f7:34:c9:c0:23:06:b4:32:6c:65:48:06:78:18:48:fe:78:
ab:ba:5c:a3:f5:0b:c8:64:95:5b:a6:27:c1:43:ca:d9:f5:d0:
bd:5c
```

EXAMPLE

```
ALU(config)# show crypto crl ca ALUCA pem
```

```
-----BEGIN X509 CRL-----
MIIBDzB6MA0GCSqGSIb3DQEBAUMCExEDAOBgNVBAMUB0NBXzB4MDExDALBgNV
BAoTBE5ldGQXDTA2MDEwOTExNDYzN1oXDTA2MDIwODExNDYzN1owKDASAgEBFw0w
NjAxMDkxMTQ2MTJAMBICAQIXDTA2MDEwOTExNDYxN1owDQYJKoZIhvcNAQEEBQAD
gYEARWvaXxAJd3wWHqTCqrY8BNHKTLycaAenpIoJzK3gi5w0nQXAYzvXAZzgKUQ4
5PjjpgWkTkVQU8qZ6dTWw9RI/dzLvwqcoS4FpEKUFDd0vcyBwWLXZL9kTyMEgxvc0
ycAjBrQybGVIBngYSP54q7pco/ULyGSVW6YnwUPK2fXQvVw=
-----END X509 CRL-----
```

To VIEW CA CERTIFICATE

Command (in SUM/CM)	Description
<code>show crypto ca-cert <name></code>	Displays the details of the specified CA certificate in a readable format.
<code>show crypto ca-cert [<name> [pem]]</code>	Displays the details of the specified CA certificate in the base64 pem format.

EXAMPLE

```
ALU(config)# show crypto ca-cert ALUCA
```

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 0 (0x0)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: CN=CA_0x01, O=ALU
  Validity
    Not Before: Dec 28 12:30:49 2005 GMT
    Not After : Jan 27 12:30:49 2006 GMT
  Subject: CN=CA_0x01, O=ALU
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:b2:bf:d4:a9:46:f0:d3:38:3c:46:e1:52:0e:e4:
        31:1c:0c:81:70:90:1a:95:dd:79:44:c6:e3:1b:c6:
        a3:ec:d7:d5:18:9e:c2:d0:14:a3:8c:35:c0:34:e1:
        9f:ff:2c:ae:fd:0e:b2:6f:5a:59:3e:c8:67:e8:f8:
        a7:a2:ba:84:d9:e5:0a:cc:af:e0:cf:67:36:a4:e6:
        f5:22:d5:88:72:3c:aa:85:be:92:06:87:78:6a:6e:
        69:3b:ab:73:bd:c0:5c:eb:85:1d:18:76:c4:f8:aa:
        a9:c1:bb:14:1f:15:38:cc:8f:8c:e6:5c:3c:a1:b8:
        10:4b:1a:98:c2:7d:b4:d0:cd
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      05:98:D2:25:D3:18:12:A1:C7:4B:7A:98:D2:D8:25:73:2B:6B:AE:B1
    X509v3 Authority Key Identifier:

keyid:05:98:D2:25:D3:18:12:A1:C7:4B:7A:98:D2:D8:25:73:2B:6B:AE:B1
  DirName:/CN=CA_0x01/O=ALU
  serial:00

  X509v3 Basic Constraints:
    CA:TRUE
  Signature Algorithm: md5WithRSAEncryption
    0c:0b:92:9c:1d:60:ac:62:e0:7f:f3:1d:9c:7b:e8:de:67:09:
    43:a1:2e:47:d1:78:c1:17:f6:0c:aa:ef:51:55:e2:9b:5f:8a:
    0e:9f:ba:51:55:57:48:2b:4c:8f:f7:6b:7c:65:4b:cf:99:b2:
    dc:83:2d:da:99:63:0c:ad:6b:33:66:19:91:ef:35:cb:dd:d8:
    74:48:34:a6:40:c2:f0:8d:b6:8a:32:63:8c:f0:82:14:14:5a:
    a3:56:de:b1:50:42:6f:b3:0f:ea:f1:26:be:2e:ce:9e:61:f5:
    24:c3:88:ab:13:42:70:82:80:f9:f1:d2:8f:02:d5:5b:62:ff:
    3e:cc
```

```
ALU(config)# show crypto ca-cert ALUCA pem
```

```
-----BEGIN CERTIFICATE-----
MIICMjCCAZugAwIBAgIBADANBgkqhkiG9w0BAQQFADAhMRAwDgYDVQQDFAdDQV8w
eDAXMQ0wCwYDVQQKEwROZXRkMB4XDTA1MTIyODEyMzA0OVoXDTA2MDEyNzEyMzA0
OVowITEQMA4GA1UEAxQHQ0FfMHgwMTENMASGA1UEChMETmV0ZDZCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAser/UqUbw0zg8RuFSduQxHAYBcJAald15RMbjG8aj
7NfVGJ7C0BSjjDXANOGf/yyu/Q6yblpZPshn6PinorqE2eUKzK/gz2c2pOb1ItWI
cjyqhb6SBod4am5p06tzvcBc64UdGHbE+KqpwsUHxU4zI+M51w8obgQSxqYwn20
0M0CAwEAAaAN6MHgwHQYDVR0OBBYEFAYW0iXTGBKx0t6mNLYJXMra66xMEkGA1Ud
IwRCMECAFAYW0iXTGBKx0t6mNLYJXMra66xoSWkIzAhMRAwDgYDVQQDFAdDQV8w
eDAXMQ0wCwYDVQQKEwROZXRkkgEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEE
BQADgYEADAuSnBlgrGLgf/MdnHvo3mcJQ6EuR9F4wRf2DKrvUVXim1+Kdp+6UUVX
SctMj/drfgVLz5my3IMt2pljDK1rM2YZke81y93YdEg0pkDC8I22ijJjjPCCFBra
olbesVBCb7MP6vEmvi7OnmH1JMOIqxNCcIKA+fHSjwLVW2L/Psw=
-----END CERTIFICATE-----
```

To VIEW CSR DETAILS

Command (in SUM/CM)	Description
<code>show crypto certificate-request</code>	Displays the names of all the CSR.
<code>show crypto certificate-request <name></code>	Displays the details of the specified CSR in a readable format.
<code>show crypto certificate-request [<name> [pem]]</code>	Displays the details of the specified CSR in the base64 pem format.

EXAMPLE

```
ALU(config)# show crypto certificate-request
```

```
req_Simpson
req_Burns
```

```
ALU(config)# show crypto certificate-request req_Simpson
```

```
Certificate Request:
```

```
Data:
```

```
Version: 0 (0x0)
```

```
Subject: CN=Bart Simpson, O=ALU, C=US
```

```
Subject Public Key Info:
```

```
Public Key Algorithm: rsaEncryption
```

```
RSA Public Key: (512 bit)
```

```
Modulus (512 bit):
```

```
00:ba:f3:af:cf:09:49:f4:ef:13:df:a7:e3:ee:28:
```

```
32:b5:ef:06:e2:f8:c9:31:6d:44:44:81:d2:3f:49:
```

```
82:c9:6b:5a:d1:73:d0:7b:af:3f:5e:82:34:15:54:
```

```
49:a7:d3:5e:69:29:c4:72:57:25:6a:ee:02:f8:2c:
```

```
dd:59:2f:03:ad
```

```
Exponent: 65537 (0x10001)
```

```
Attributes:
```

```
a0:00
```

```
Signature Algorithm: md5WithRSAEncryption
```

```
57:7b:73:45:07:37:a3:c6:a3:fc:46:5d:a6:c7:00:b1:2c:c8:
```

```
15:00:8f:ef:47:c5:0d:fa:81:a3:82:90:15:76:ad:10:42:ef:
```

```
68:a5:58:5a:e8:7b:17:85:d3:2b:f5:c5:ca:ca:db:c1:f0:d5:
```

```
a6:87:b6:0b:13:a2:35:2f:91:cb
```

```
ALU(config)# show crypto certificate-request req_Simpson pem
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIHtMIGYAgEAMDMxFTATBgNVBAMTDEJhcnQgU2l0cHNvbWVjENMAsGAlUEChMETmV0
RDELMAkGAlUEBhMCVVMwXDANBgkqhkiG9w0BAQEFAANLADBIakeAuvOvzwlJ908T
36fj7igyte8G4vjJMW1ERIHSP0mCyWta0XPQe68/XoI0FVRJp9NeaSnEclclau4C
+CzdWS8DrQIDAQABoAAwdQYJKoZIhvcNAQEEBQADQQBXe3NFBzejxqP8Rl2mxwCx
LMgVAI/vR8UN+oGjgpAVdq0QQu9opVha6HsXhdMr9cXKytvB8NWmh7YLE6I1L5HL
-----END CERTIFICATE REQUEST-----
```

CLEAR COMMANDS IN IPSEC

TO CLEAR CRYPTO IPSEC COUNTERS

Command (in SUM/CM)	Description
<code>clear crypto ipsec counters</code>	This command is used to reset the IPsec SA related counters for Encapsulation, Encryption, Authentication, and Error.

EXAMPLE

```
ALU# clear crypto ipsec counters
ALU#
```

TO CLEAR CRYPTO IPSEC SA

Command (in SUM/CM)	Description
<code>clear crypto ipsec sa</code> {all <sa_index>}	This command is used to clear all the IPsec SAs or IPsec SAs corresponding to a specific SA index. As a result, the SA pair will be cleared and the tunnel will be brought down.



Note: The sa-index must be a valid sa-index of an outbound SA.

EXAMPLE

```
ALU# clear crypto ipsec sa all
ALU#

ALU# clear crypto ipsec sa 16
ALU#
```


IPSEC SCENARIOS ON OA-700

CONFIGURING IPSEC WITH ONLY A PRE-SHARED KEY

```
ALU(config)# show crypto
```

```
! No Key Set
!crypto ike policy default
!      proposal sha1-aes128
!      ipsec security-association lifetime seconds 28800
!      lifetime seconds 3600
!      pfs group2
!crypto ipsec transform-set default
! esp-sha1-aes256 esp-sha1-3des esp-md5-aes256 esp-md5-3des
```

```
! No Cryptomap Defined
!
```

```
ALU(config)# crypto ike key rtalukdar peer 10.0.0.1
ALU(config)# match-list m1
ALU(config-match-list-m1)# ip prefix 20.0.0.0/24      prefix
10.0.0.0/24
ALU(config-match-list-m1)# top
```

```
ALU(config)# crypto map demomap ipsec-ike default
ALU(config-crypto-map-demomap)# match m1
ALU(config-crypto-map-demomap)# peer 10.0.0.1
ALU(config-crypto-map-demomap)# top
```

```
ALU(config)# show crypto
```

```
crypto ike key rtalukdar peer 10.0.0.1
!crypto ike policy default
!      proposal sha1-aes128
!      ipsec security-association lifetime seconds 28800
!      lifetime seconds 3600
!      pfs group2
!crypto ipsec transform-set default
!      esp-sha1-aes256 esp-sha1-3des esp-md5-aes256
      esp-md5-3des

crypto map demomap ipsec-ike default
      peer 10.0.0.1
      match m1
      transform-set default
      pfs group2
! Not Applied to Any Interface
```

COMPARATIVE STUDY BETWEEN OA-700 AND OTHER SYSTEMS

This same thing in other systems would involve:

1. Defining a Preshared key.
2. Defining an ike policy - 3 sub-commands minimum (OA-700 has a default IKE policy).
3. Defining a transform-set (in our case, we have a default transform-set).
4. Defining a crypto map - 4 sub-commands (in our case, only 2 sub-commands).

Further, when a show crypto is done, the defaults assumed are shown with a "!" at the beginning of the line. This would help in knowing whether the value was set or assumed.

Another point to note is that the OA-700 does not support AH in IPsec. AH is a very weak mechanism and hence is not used in most modern systems.

EDITING A MATCH-LIST ATTACHED TO THE CRYPTO MAP

```
ALU(config)# match-list tunnel
ALU(config-match-list-tunnel)# 1 ip prefix 10.91.0.0/24 prefix
10.0.0.0/24
```

```
ALU(config)# crypto map cryp-tunnel ipsec-ike default
ALU(config-crypto-map-cryp-tunnel)# match tunnel
```

Now, if we want to tunnel traffic from 192.168.0.0/24 to 10.0.0.0/24

```
ALU(config)# match-list tunnel
ALU(config-match-list-tunnel)# 1 ip prefix 10.91.0.0/24
prefix 10.0.0.0/24
ALU(config-match-list-tunnel)# 2 ip prefix 192.168.0.0/24
prefix 10.0.0.0/24
```

This will not work as the crypto map accepts only the first configured rule in the match-list. Hence, you should configure another match-list with the new rule and configure this into a new crypto map.

Alternatively, you can modify the same rule.

```
ALU(config)# match-list tunnel
ALU(config-match-list-tunnel)# 1 ip prefix 10.91.0.0/24
prefix 10.0.0.0/24
ALU(config-match-list-tunnel)# 1 ip prefix 192.168.0.0/24
prefix 10.0.0.0/24
```



Note: The crypto map supports only one rule in a match-list.

The above can be achieved in the following way:

```
ALU(config)# match-list tunnel
ALU(config-match-list tunnel)# 1 ip prefix 10.91.0.0/24
prefix 10.0.0.0/24
```

```
ALU(config)# crypto map cryp-tunnel ipsec-ike default
ALU(config-crypto-map-cryp-tunnel)# match tunnel
```

```
ALU(config)# match-list nxt-tunnel
ALU(config-match-list tunnel)# 2 ip prefix 192.168.0.0/24
prefix 10.0.0.0/24
```

```
ALU(config)# crypto map cryp-nxt-tunnel ipsec-ike default
ALU(config-crypto-map-cryp-nxt-tunnel)# match nxt-tunnel
```

With respect to editing a match-list within a crypto map, consider the following scenarios:

CASE(I) DELETION OF THE MATCH-LIST USED BY A CRYPTO MAP

Match-list cannot be deleted if it is attached to a crypto map.

CASE(II) DELETION OF THE RULE IN A MATCH-LIST USED BY A CRYPTO MAP

A rule in the match-list cannot be deleted if the match-list is attached to a crypto map.

CASE(III) MODIFYING THE RULE WITHIN THE MATCH-LIST USED BY A CRYPTO MAP

If a rule in the match-list which is connected to the crypto map is modified, the tunnel goes down and the SPD is modified. Tunnel will come up again for the modified SPD. The modified rule should satisfy IPsec match-list criteria.

CASE(IV) ADDING AN EXTRA RULE TO THE MATCH-LIST USED BY A CRYPTO MAP

An extra rule cannot be added to a match-list if it is attached to a crypto map.

BEST PRACTICES FOR DEPLOYING IPSEC VPN

Virtual Private Networks are convenient, but they can also create gaping security holes in the network. The following sections discuss general guidelines that need to be kept in mind but are independent of VPN configuration.

The following sections provide information on best practices for deploying IPsec VPN:

- “Identity”
- “IPsec Access Control”
- “IPsec”
- “Network Address Translation”
- “Network Access Control”
- “Interoperability”

IDENTITY

It is important that the devices are identified in a secure and manageable manner. Device authentication uses either a pre-shared key or digital certificates to provide the device authentication.

PRE-SHARED KEY

Pre-shared keys are of three types:

- Unique—Unique pre-shared keys are tied to a specific IP address.
- Group—Group pre-shared keys are tied to a group-name identity
- Wild card—These keys are not associated with any factor unique information to determine a peer's identity.

Since, a Wild Card Key is not tied to a specific IP address, it should not be used when deploying site-to-site VPN tunnels. When using Wild Card keys, every single device uses the same key. Hence, if a single device in the network has been compromised and the wild card key has been determined, all the devices in the network are compromised.

Using Unique Pre-shared key is advisable. But the drawback of using pre-shared key is that it would not scale in large networks. Providing strong device authentication also would depend upon how often the keys are changed and the key length. Most devices provide a maximum key length of 127 characters strong. It is up to you to decide upon the key length. It is recommended to use a minimum key length of 16 characters.



Note: The OA-700 supports only unique pre-shared key to provide better security.

IPSEC ACCESS CONTROL

IPsec access control happens after the device Authentication. As defined by the IPsec standard, the networks, host, and ports that are allowed to traverse the network are defined in the Security Policy Database or SPD. It is advisable to have an inbound control list when configuring VPN for site-to-site traffic.

IPSEC

IPsec provides numerous security features. The following are some features that can be configured:

- Device Authentication and credentials
- Data Encryption
- Data Integrity
- SA aging

IPsec standard requires the use of either data integrity or data encryption. It is recommended to have both data integrity and data encryption.

Data encryption is brought about by using algorithms, such as DES, 3-DES, AES-128, AES-192, and AES-256. Most common deployments use 3-DES in place of DES. The drawback of using 3-DES is the loss of performance. It is recommended to use AES-128 than 3-DES as it improves upon the performance. AES-128 is also widely accepted by the federal government of U.S. Reference to the same can be found at the following site: http://www.nist.gov/public_affairs/releases/g01-111.htm

Data Integrity is brought about using HASH algorithms like MD5 and SHA-1. SHA-1 is considered to be more secure than MD5 because of its greater bit strength. SHA-1 uses 160-bit hash algorithm while MD5 uses only 128-bit. It is recommended to use SHA-1 instead of MD-5.

Both the IPsec phases offer the ability to change the lifetime of a Security Association. Lesser the lifetime more secure is the connection. But it has to be kept in mind that if the lifetime is too small i.e for a few seconds, tunnel negotiation would keep on happening without the tunnel being setup for the flow of data traffic. Hence, it is recommended that SA lifetime is kept in the magnitude of minutes/hours instead of seconds so that the data traffic is more than the control traffic.

Perfect Forward Secrecy (PFS) generates a new key based on new seed material altogether by carrying out DH group exponentiation every time a new quick-mode SA needs new key generation. This option increases the level of the security but also increases the processor overhead. Some of the VPN devices do provide an option of not configuring PFS due to this reason. Enabling of PFS also depends upon the sensitivity of the data being tunneled. If the data mandates higher security, PFS can be enabled. The strength of Diffie-Hellman exponentiation is configurable.



Note: It is recommended to use Diffie-Hellmann PFS Group 5.

- group1: Use Diffie-Hellman Group 1: 768 bits
- group2: Use Diffie-Hellman Group 2: 1024 bits
- group5: Use Diffie-Hellman Group 5: 1536 bits

NETWORK ADDRESS TRANSLATION

NAT can occur after or before IPsec. NAT interferes with IPsec by blocking tunnel establishment or traffic flow through the tunnel due to change in IP headers. It is a best practice to avoid application of NAT and IPsec traffic on the same interface. If they are applied on the same interface until and unless it is absolutely necessary, appropriate NAT bypass must be configured.

Generally NAT and IPsec are applied on same interface (public). From a performance perspective, this is not a good conjunction. Hence the OA-700 allows you to use the bypass command, to **bypass** all the NAT traffic and allow only the IPsec traffic. This can be achieved in the following ways.



Note: The match-list used in IPsec should be applied as bypass rule in NAT with higher priority as compared to the match-list specifying traffic for which NAT is intended.

NETWORK ACCESS CONTROL

Filtering inbound traffic is recommended to allow only IKE and ESP on the particular interface from where the IPsec tunnels is initiated.

INTEROPERABILITY

Although IPsec is a documented standard, it has still left a room for interpretation. In addition, Internet Drafts such as IKE mode-configuration and vendor proprietary features increase the likelihood of interoperability challenges. For these reasons, check should be made with the vendor of the products for interoperability informations.

ROUTING ENTRY

For IPsec tunnel to come up, you must have a routing entry for the destination address in the match-list.

For example:

```
match-list m1
  ip prefix 10.0.0.0/8 prefix 9.0.0.0/8
```

This is applied to the crypto map attached to interface gig3/1.

Then, you should have a routing entry

```
ip route 9.0.0.0/8 gig3/1
```

Otherwise the tunnel will not come up.

IPSEC NAT-TRAVERSAL

NAT can occur before or after IPsec. If NAT occurs before the IPsec packet is encrypted, NAT and IPsec can work together. If the packet is encrypted before being sent to NAT, the address is changed by NAT. Since the packet is modified, it fails the integrity check at the receiving end. The packet is discarded and the VPN tunnel cannot be created. In such a scenario, NAT and IPsec cannot be applied on the same interface.

NAT-Traversal (NAT-T) was created to enable IPsec VPNs to work with NAT. It makes it easier to deploy NAT and IPsec together by resolving these issues. NAT-T uses UDP (User Datagram Protocol) encapsulation. This enables NAT devices to change IP or port addresses without modifying the IPsec packet. Additionally, to prevent an IKE-aware NAT from modifying IKE packets, IPsec NAT-T peers change the IKE UDP port of 500 to the UDP port 4500 during IKE negotiation.

There is no configuration required as NAT-T is detected automatically by VPN devices. Both the VPN devices must be NAT-T capable.



Note: IPsec NAT-T is only defined for ESP (Encapsulating Security Payload) traffic.

TO ENABLE/DISABLE NAT TRAVERSAL

Command (in CM)	Description
<code>crypto nat-traversal {enable disable}</code>	This command is used to enable or disable NAT traversal for IPsec on the OA-700. By default, NAT Traversal is enabled.

EXAMPLE

```
ALU(config)# crypto nat-traversal disable
```


SCENARIOS DEPICTING IPSEC NAT-TRAVERSAL

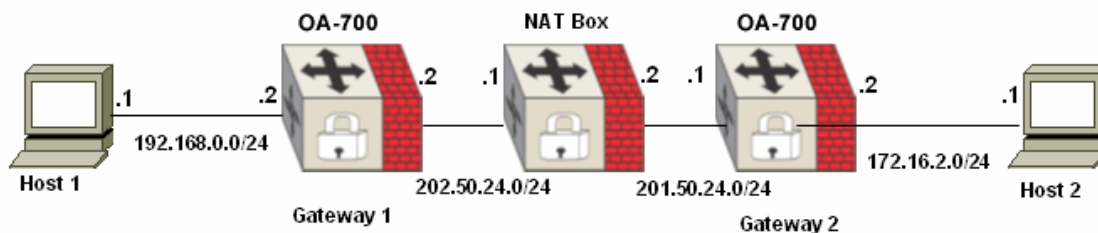


Figure 63: IPsec Scenario with NAT-Traversal

When both the IPsec peers Host 1 and Host 2 are behind NAT. Both peers being NAT-T capable detect NAT during the main mode negotiation and peers switch to port 4500.

OA700-1

```

ALU(config)# show match-list
match-list m1
1 ip prefix 10.0.0.0/24 prefix 10.91.0.0/24

!

ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)#ip address 202.50.24.2/24
ALU(config-if GigabitEthernet7/0)#crypto-map map1

ALU(config-if GigabitEthernet7/0)#show crypto

crypto ike key secret peer 202.50.24.1
!crypto ike policy default
!   proposal shal-aes128
!   ipsec security-association lifetime seconds 28800
!   lifetime seconds 86400
!   pfs group2
!crypto ipsec transform-set default
!   esp-shal-aes256 esp-shal-3des esp-md5-aes256 esp-md5-3des
crypto map map1 ipsec-ike default
      peer 202.50.24.1
      match m1
      transform-set default
      pfs group2
! Applied to : GigabitEthernet7/0
interface GigabitEthernet7/0
  crypto map map1
top

```

OA700-2

```
ALU(config)# show match-list
match-list m1
1 ip prefix 10.91.0.0/24 prefix 10.0.0.0/24
```

```
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)#ip address 201.50.24.1/24
ALU(config-if GigabitEthernet7/0)#crypto map map1
```

```
ALU(config)# show crypto
```

```
crypto ike key secret peer 202.50.24.2
!crypto ike policy default
!      proposal sha1-aes128
!      ipsec security-association lifetime seconds 28800
!      lifetime seconds 86400
!      pfs group2
!crypto ipsec transform-set default
!      esp-sha1-aes256 esp-sha1-3des esp-md5-aes256 esp-md5-
3des
crypto map map1 ipsec-ike default
      peer 202.50.24.2
      match m1
      transform-set default
      pfs group2
! Applied to : GigabitEthernet7/0
interface GigabitEthernet7/0
      crypto map map1
top
```

IPSEC TUNNEL INTERFACE

Alcatel-Lucent provides support for IPsec in a tunnel mode with encryption, intended for secure site-to-site communications over an untrusted network.

Currently IPsec can be configured through a crypto map and applied to a interface. In addition, IPsec as a tunnel interface is required so that,

- Pre, post encryption or decryption policies for QoS, Filters, and ACL can be applied.
- Traffic classifier will be routed based rather than policy based, which means that routing can control what traffic needs to be secure.
- Tunnel fail over can be handled by having traffic routed through another tunnel interface.
- Allows to run dynamic routing protocols over the tunnel.

BEFORE YOU CONFIGURE IPSEC TUNNEL INTERFACE

Here are a few guidelines that you need to pay attention to when configuring the OA-700 for the IPsec Tunnel interface.

1. Routing setup must be in ordinance.
2. The interface must be a configurable interface, i.e., associated with an IP address.
3. Tunnel endpoints (source and destination) should be specified. The source address could be a configured IP address or another interface address (thus deriving its IP address). The destination address is the address of the peer with which IKE negotiation will take place.
4. Parameters required in tunnel negotiation should be configured. These parameters are IPsec transform set, IKE policy, SA lifetime, PFS, and IKE Identity.

DEFAULT CONFIGURATION

The OA-700 provides the following default configurations:

- If an IKE policy is not configured, the '**default**' ike policy is applied to the profile. Following are the default values for IKE policy:
 - i. Default proposal in ike policy: **sha1-aes128**
 - ii. Default PFS group in ike policy: **pfs group2**
 - iii. Default IPsec security-association lifetime in seconds: **28800**
 - iv. Default IKE lifetime in seconds: **86400**
- Default authentication mechanism: **Pre-shared Keys (PSK)**
- If a transform set is not configured, the '**default**' transform set is applied to the profile. Following are the default values for transform-set:
 - i. esp-sha1-aes256
 - ii. esp-sha1-3des
 - iii. esp-md5-aes256
 - iv. esp-md5-3des
- If a crypto map is not configured, you can attach the '**default**' profile to an interface. Following are the default values within a profile:
 - i. Default IKE policy in crypto map: '**default**' ike policy
 - ii. Default transform set in crypto map: '**default**' transform set
 - iii. Default PFS group in crypto map: **pfs group2**.
 - iv. Default lifetime in Seconds for a crypto map: **28800**

IPSEC TUNNEL INTERFACE CONFIGURATION

Refer to the following sections for configuring IPsec tunnel interface:

- [“IPsec Tunnel Interface Configuration Commands”](#)
- [“IPsec VPN Configuration Flow”](#)
- [“IPsec Configuration Commands”](#)
- [“IPsec VPN Show Commands”](#)

IPSEC TUNNEL INTERFACE CONFIGURATION STEPS

The following are the steps to configure IPsec tunnel interface on the OA-700:

Step 1: Following IPsec VPN configuration is pre-requisite for IPsec tunnel configuration. These are mandatory for IPsec tunnel functioning.

The configurations for all these parameters (pre-shared key/X.509 certificates, IKE policy, Transform Set) are already given in the earlier sections of the document; hence it is not repeated in this section. Use the links to see the specific commands.

- Configure a pre-shared key using. See [“IPsec Configuration with Pre-shared Key”](#)



Note: While configuring Pre-shared key for IPsec Tunnel interface, the peer address should be the destination IP address configured on the tunnel interface.

OR

Configure X.509 certificates. See [“IPsec Configuration with X.509 Certificates”](#)

- Configure IKE policy. See [“To Configure an IKE Policy”](#)
- Configure a Transform Set. See [“To Configure Transform-set in IPsec”](#)

Step 2: Configure IPsec Profile. See [“To Configure IPsec Profile”](#). And, configure Profile related commands.

Step 3: Enter Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 4: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 5: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-  
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address 2.2.2.1/  
24
```

Step 6: Configure a Tunnel interface. See [“To Configure a Tunnel Interface”](#)

- Administratively bring up the tunnel interface. See [“To Administratively Bring Up/Shutdown the Tunnel Interface”](#)
- Configure IP address for the tunnel interface. See [“To Configure IP Address on a Tunnel Interface”](#)
- Set the mode on the tunnel interface. See [“To Configure Mode on a Tunnel Interface”](#)
- Configure the tunnel source for the tunnel interface. See [“To Configure Source IP Address for the Tunnel”](#)
- Configure the tunnel destination on the tunnel interface. See [“To Configure Destination IP Address for the Tunnel”](#)
- Attach the configured IPsec Profile to the tunnel interface. See [“To Attach an IPsec Profile to the Tunnel Interface”](#)

Step 7: View the IPsec tunnel configuration. See [“To View the IPsec Profile Configuration”](#)**Note:**

All the IPsec parameters related show commands are valid for this section also. For more details, see [“IPsec VPN Show Commands”](#)

IPSEC TUNNEL INTERFACE CONFIGURATION FLOW

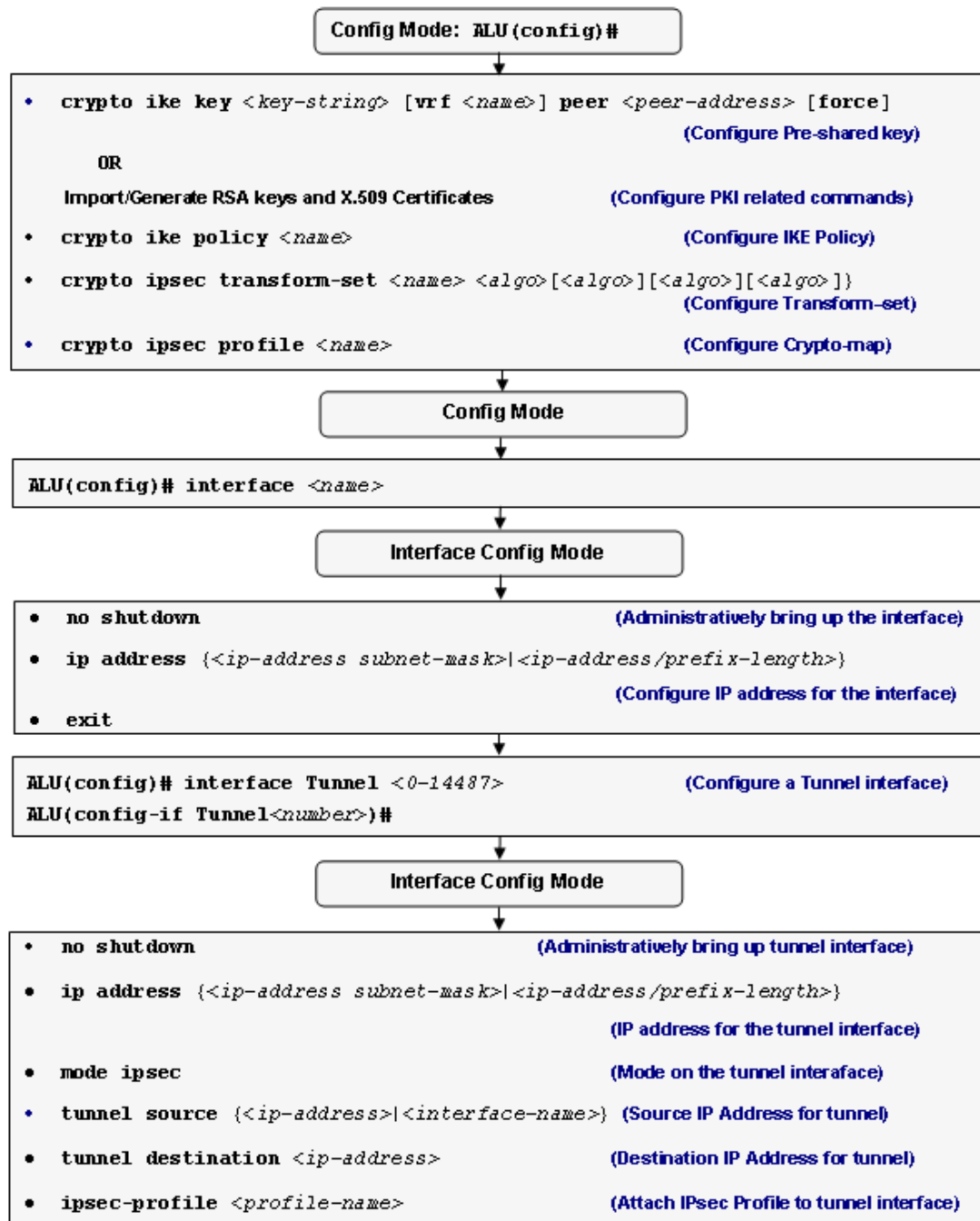


Figure 64: IPsec Tunnel Interface Configuration Flowchart

IPSEC TUNNEL INTERFACE CONFIGURATION COMMANDS

This section details the commands used in configuring the IPsec tunnel interface.

To CONFIGURE IPSEC PROFILE

IPsec Profile entries created for the IPsec tunnel interface pull together various parts used to set up IPsec security associations that include:

- Where the IPsec-protected traffic should be sent (remote IPsec peer).
- What kind of IPsec security should be applied to this traffic (as configured by the transform-set)
- Security associations established via IKE.

Command (in CM)	Description
<code>crypto ipsec profile <name></code> <code>[force]</code>	This command is used to configure an IPsec Profile.



Note: **Force** - This option is used to modify a IPsec profile when it is applied to an interface.

EXAMPLE

```
ALU(config)# crypto ipsec profile PF1
ALU(ipsec-profile-PF1)#
```

To ATTACH AN IKE POLICY TO AN IPSEC PROFILE

Command (in IPsec Profile CM)	Description
<code>ike-policy <name></code>	This command is used to attach an already configured IKE policy to an IPsec profile.
<code>no ike-policy</code>	The 'no' command detaches the specified IKE policy attached to the profile. <div data-bbox="831 1419 906 1486" data-label="Image"> </div> <p>Note: An IKE policy must be first detached from the profile to delete it globally.</p>




Note: If no IKE policy is attached to an IPsec profile, **'default'** IKE policy is used.

EXAMPLE

```
ALU(ipsec-profile-PF1)# ike-policy IKE1

ALU(ipsec-profile-PF1)# no ike-policy
Alcatel-Lucent
```


TO ATTACH A TRANSFORM SET TO AN IPSEC PROFILE

Command (in IPsec Profile CM)	Description
<code>transform-set <name></code>	This command is used to attach an already configured transform-set to an IPsec profile.
<code>no transform-set</code>	The 'no' command detaches the specified transform-set attached to the profile.  Note: A transform-set must be first detached from the profile to delete it globally.




Note: If no transform-set is attached to an IPsec profile, **'default'** transform set is used.

EXAMPLE

```
ALU(ipsec-profile-PF1)# transform-set TS1
```

```
ALU(ipsec-profile-PF1)# no transform-set
```

TO ATTACH PFS GROUP TO AN IPSEC PROFILE

Command (in IPsec Profile CM)	Description
<code>pfs {group1 group2 group5}</code>	This command is used to attach a PFS group to an IPsec profile.  Note: If no PFS group is attached to an IPsec profile, group2 PFS is used.
<code>no pfs</code>	The 'no' command disables PFS completely.

EXAMPLE

```
ALU(ipsec-profile-PF1)# pfs group2
```

```
ALU(ipsec-profile-PF1)# no pfs
```

To CONFIGURE LIFETIME FOR AN IPSEC PROFILE

Command (in IPsec Profile CM)	Description
<code>lifetime {kilobytes <512-2147483647>/seconds <540-86400>}</code>	This command configures lifetime for an IPsec profile. Use 'kilobytes' keyword to configure lifetime in kilobytes, and use 'seconds' keyword to configure lifetime in seconds for a profile.
<code>no lifetime {kilobytes/seconds}</code>	The 'no' command resets the seconds lifetime to default. If set in kilobytes, the 'no' command removes the kilobytes lifetime value.



Note: Lifetime has a default value of **28800** seconds.

There is no default value for lifetime in kilobytes.

EXAMPLE

```
ALU(ipsec-profile-PF1)# lifetime seconds 1000
ALU(ipsec-profile-PF1)# lifetime kilobytes 1005236
```

```
ALU(ipsec-profile-PF1)# no lifetime seconds
ALU(ipsec-profile-PF1)# no lifetime kilobytes
```

To ATTACH AN IKE IDENTITY TO AN IPSEC PROFILE

Command (in IPsec Profile CM)	Description
<code>ike-identity <name></code>	This command attaches an IKE identity to an IPsec profile.
<code>no ike-identity</code>	The 'no' command detaches the specified IKE identity attached to a profile.



Note: IKE identity should only be attached to an IPsec profile if the Authentication type is **'rsa-sig'**

EXAMPLE

```
ALU(ipsec-profile-PF1)# ike-identity ID01
```

```
ALU(ipsec-profile-PF1)# no ike-identity
```

To CONFIGURE A TUNNEL INTERFACE

Command (in CM)	Description
interface Tunnel <0-14487>	This command is used to configure a tunnel interface.

EXAMPLE

```
ALU(config)# interface Tunnel 1
ALU(config-if Tunnel1)#
```

To ADMINISTRATIVELY BRING UP/SHUTDOWN THE TUNNEL INTERFACE

Command (in ICM)	Description
no shutdown	This command is used to administratively bring up the tunnel interface.
shutdown	This command is used to administratively bring down the tunnel interface.

EXAMPLE

```
ALU(config-if Tunnel1)# no shutdown

ALU(config-if Tunnel1)# shutdown
```

To CONFIGURE IP ADDRESS ON A TUNNEL INTERFACE


Command (in ICM)	Description
ip address {<ip-address subnet-mask>/<ip-address/ prefix-length>}	This command is used to assign an IP address and subnet mask to the tunnel interface.

EXAMPLE

```
ALU(config-if Tunnel1)# ip address 20.20.20.20/24

ALU(config-if Tunnel1)# ip address 192.168.0.1 255.255.255.255
```

To CONFIGURE MODE ON A TUNNEL INTERFACE

Command (in ICM)	Description
<code>mode {gre ipsec}</code>	<p>This command is used to set the mode on tunnel interface.</p> <p>To configure IPsec tunnel interface, set the mode to IPsec.</p>  <p>Note: By default, tunnel is configured in GRE mode.</p>

EXAMPLE

```
ALU(config-if Tunnel1)# mode ipsec
```

To CONFIGURE SOURCE IP ADDRESS FOR THE TUNNEL

Command (in ICM)	Description
<code>tunnel source {<ip-address>/<interface-name>}</code>	This command sets the source IP address of the tunnel.
<code>no tunnel source {<ip-address>/<interface-name>}</code>	The “no” command removes the configured source IP address of the tunnel.

EXAMPLE

```
ALU(config-if Tunnel1)# tunnel source 2.2.2.1
```

or

```
ALU(config-if Tunnel1)# tunnel source GigabitEthernet7/0
```

```
ALU(config-if Tunnel1)# no tunnel source 2.2.2.1
```

or

```
ALU(config-if Tunnel1)# no tunnel source GigabitEthernet7/0
```

TO CONFIGURE DESTINATION IP ADDRESS FOR THE TUNNEL

Command (in ICM)	Description
<code>tunnel destination <ip-address></code>	This command sets the destination IP address of the tunnel at the remote end.
<code>no tunnel destination <ip-address></code>	The “no” command removes the configured destination IP address.

EXAMPLE


```
ALU(config-if Tunnel1)# tunnel destination 2.2.2.3
```

```
ALU(config-if Tunnel1)# no tunnel destination 2.2.2.3
```

TO ATTACH AN IPSEC PROFILE TO THE TUNNEL INTERFACE

IPsec Profile needs to be applied to the IPsec tunnel interface through which the IPsec traffic flows.

Binding an IPsec profile to an interface instructs the system to evaluate all the interface traffic against the IPsec profile, and to use the specified policy during connection or security association negotiation.

Command (in ICM)	Description
<code>ipsec-profile <profile-name></code>	Enter this command in the Tunnel Interface Configuration Mode. This command is used to attach the configured IPsec profile to the tunnel interface.
<code>no ipsec-profile <profile-name></code>	This command is used to detach the IPsec profile attached to the interface.  Note: You cannot delete an IPsec profile that is applied to the interface. To delete, first detach the IPsec profile from the tunnel interface.

EXAMPLE

```
ALU(config-if Tunnel1)# ipsec-profile PF1
```

```
ALU(config-if Tunnel1)# no ipsec-profile PF1
```

To VIEW THE IPSEC PROFILE CONFIGURATION

Command (in SUM/CM)	Description
<code>show crypto ipsec profile</code> [<profile-name>]	This command displays the IPsec profile details.

EXAMPLE

```
ALU(config)# show crypto ipsec profile

crypto ipsec profile PF1
    ike-policy secret
    transform-set transet1
    ike-identity ID01
    pfs group2
!     lifetime seconds 28800
! Applied to:
interface Tunnell
    ipsec-profile PF1
ALU(config)#
```

IPSEC TUNNEL CONFIGURATION SCENARIOS USING OA-700

The OA-700 topology below consists of the following components:

- 1 OA-700
- 1 Cisco

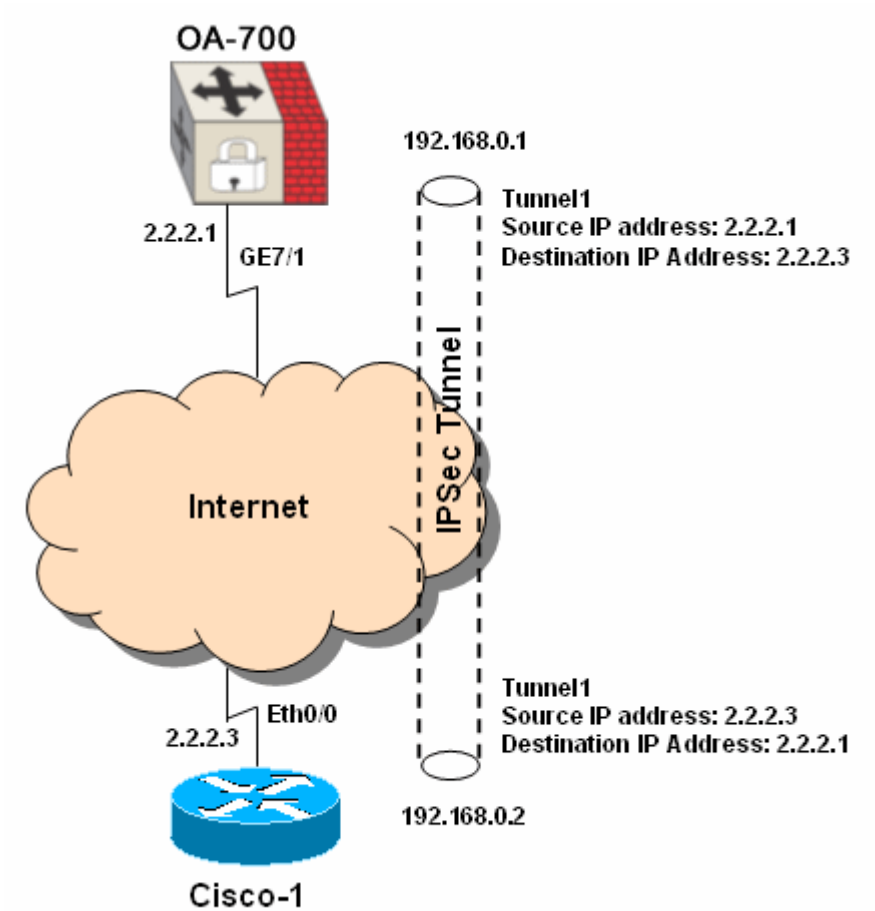


Figure 65: IPsec Tunnel Interface Configuration Topology

ON OA700-1

- a) IPsec VPN configuration: Configure pre-shared key, IKE policy, Transform Set,
ALU-1(config)# crypto ike key top_secret1612 peer 2.2.2.3
ALU-1(config)# crypto ike policy IKE1
ALU-1(config)# crypto ipsec transform-set TS1
- b) Configure IPsec Profile
ALU(config)# crypto ipsec profile PF1
ALU(ipsec-profile-PF1)# ike-policy IKE1
ALU(ipsec-profile-PF1)# transform-set TS1
- c) Configure an interface
ALU-1(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# no shutdown
ALU(config-if GigabitEthernet7/0)# ip address 2.2.2.1
- d) Configure a tunnel interface
ALU-1(config)# interface Tunnel 1
ALU-1(config-if Tunnel1)# no shutdown
ALU-1(config-if Tunnel1)# ip address 192.168.0.1
255.255.255.255
ALU-1(config-if Tunnel1)# mode ipsec
- e) Specify tunnel end-points, and attach IPsec Profile to the tunnel interface.
ALU-1(config-if Tunnel1)# mode ipsec
ALU-1(config-if Tunnel1)# tunnel source 2.2.2.1
ALU-1(config-if Tunnel1)# tunnel destination 2.2.2.3
ALU-1(config-if Tunnel1)# ipsec-profile PF1

ON CISCO-1

Consider a cisco router -Cisco-1 with specific IPsec tunnel configuration with tunnel source being 2.2.2.3 and tunnel destination as 2.2.2.1.

VERIFICATION WITH SHOW COMMANDS

```
ALU(config)# show crypto ipsec profile

crypto ipsec profile PF1
    ike-policy secret
    transform-set transet1
    ike-identity ID01
    pfs group2
!     lifetime seconds 28800
! Applied to:
interface Tunnel1
    ipsec-profile PF1
ALU(config)#
```

CHAPTER 28 GENERIC ROUTING ENCAPSULATION

This chapter documents the commands for GRE (Generic Routing Encapsulation) configuration. For more detailed information on the parameter descriptions and their corresponding default values, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

This chapter includes the configuration steps, CLI syntax with its description, and configuration examples. The commands are described in the sequential order of configuration.

CHAPTER ORGANIZATION

- “GRE Overview”
- “GRE Tunnel Configuration”
- “GRE Configuration Scenarios using OA-700”

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
GRE	Generic Routing Encapsulation
ICM	Interface Configuration Mode - ALU (config-interface name)#

GRE OVERVIEW

GRE is a simple, stateless protocol that allows for the tunneling of traffic. IP is used as transport for GRE. GRE tunnels can be used to form VPNs, connecting remote sites using private IP addresses via a public network. Typically, GRE tunnel is run between the customer edge routers and are transparent to the rest of the network. GRE tunnels are used to carry non-IP traffic (like IPX, Appletalk, DECnet from legacy networks) over an IP backbone.

GRE TUNNEL SETUP

A GRE tunnel is configured by specifying two endpoints, one local and the other remote. In order to establish a tunnel, a GRE tunnel must be configured from the remote endpoint. No intermediary routers need to be configured, and the tunnel rides on top of the standard IP. The only requirement is that the tunnel must be configured in a context where the remote endpoint is reachable.

If the remote address of a GRE tunnel is not reachable then any circuit associated with that tunnel is brought down. Any interface bound to a GRE circuit is also marked in a down state, and any route to the tunnel interface is withdrawn. This prevents the “blackholing” of traffic caused by network instability, where traffic is sent through a tunnel that can no longer reach the remote endpoint.

Public addresses must be used for tunnel endpoint addresses. It is possible to use private IP addresses as the GRE tunnel interface IP address allowing a private address VPN to be carried over a public network.

GRE TUNNEL FEATURES

In addition to the above concepts, some important features should be highlighted:

TOPOLOGY AND SCALABILITY FEATURES

Due to the flexible nature of GRE, tunnels can be established in different topologies.

The use of different topologies also allows GRE tunnels to be scaled appropriately. Specifically, a hierarchical structure allows a core to be constructed by connecting core routers together with GRE tunnels. From that core, additional tunnels can be provisioned to the provider edge routers.

SEPARATION OF CUSTOMER AND PROVIDER ROUTING

In the OS-700, OSPF protocol instances operate upon their own instance of the routing table. Routes from one routing table instance are not visible to the other routing table instance unless it is explicitly redistributed. Therefore, even though customer routes are present in our routing table, they will not be picked up by the provider OSPF instance.

Therefore, it is possible for us to have independent OSPF routing instances for the VPN going over the tunnel, and the connectivity to the provider network.

In terms of BGP, it is possible to run BGP over the VPN by specifying a peer IP address that is reachable over the tunnel. This will guarantee that all the BGP messages to the peer will go over the tunnel.

FILTERS ON GRE TUNNELS

Filters are packet filters which determine whether packets are forwarded or dropped. They are useful for security or policy purposes. The header in each packet is examined and the relevant criteria include source and destination address, source and destination port, or other information. Filters can be applied to GRE tunnel interfaces, which means that packet filtering with its corresponding benefits can be offered for GRE tunnels.

SUMMARY

GRE tunnels are a flexible and powerful tool on any Router for offering a VPN service. Contexts and interfaces are used in combination with GRE tunneling to create a VPN service complete with private addressing, routing, user authentication, debugging, and logging.

- GRE tunnels may also be used by providers who wish to offer a VPN service before transitioning to MPLS.
- GRE protocol is defined in RFC-2784
- Provides a means of encapsulating IP and non IP packets inside GRE header and transport the payload over the GRE tunnel.
- GRE protocol header size (minimum without any options) is 4 bytes.
- GRE header format is as follows:

```
-----
| Reserved0 = 0 (13 bits) | Ver=0 (bits) | Protocol (16bits) |
-----
```

- GRE uses the ethernet protocol identifiers (from RFC-1700) to identify the type of protocol packet that is being tunnelled.
- GRE packet is encapsulated using an outer IP header.
- Outer IP header's protocol value = 47
- Support for GRE keepalive feature to monitor tunnel state.

ALCATEL-LUCENT SPECIFIC OVERVIEW

- The source IP address of the tunnel must be of either a loopback interface or one of the physical interfaces.



Note: Non IP Packets are not supported in the standard release. But it is available as a part of the component upgrade.

- By default, when a tunnel is configured for a destination address, the mode is GRE.

GRE TUNNEL CONFIGURATION

Refer to the following sections to configure GRE on the OA-700:

- [“GRE Configuration Steps”](#)
- [“GRE Configuration Flow”](#)
- [“GRE CLI Commands”](#)
- [“GRE Configuration Scenarios using OA-700”](#)

GRE CONFIGURATION STEPS

This section lists the steps for GRE tunnel configuration.

Step 1: Enter Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Configure a Tunnel interface. See [“To Configure a Tunnel Interface”](#)

- Administratively bring up the tunnel interface. See [“To Administratively Bring Up/Shutdown the Tunnel Interface”](#)
- Configure IP address for the tunnel interface. See [“To Configure IP Address on a Tunnel Interface”](#)
- Set the mode on the tunnel interface. See [“To Configure Mode on a Tunnel Interface” \(Optional\)](#)

- Configure the tunnel source for the tunnel interface. See [“To Configure Source IP Address for the Tunnel”](#)
- Configure the tunnel destination on the tunnel interface. See [“To Configure Destination IP Address for the Tunnel”](#)
- Set the Tunnel DF-BIT. See [“To Set the Tunnel DF-BIT” \(Optional\)](#)

GRE CONFIGURATION FLOW

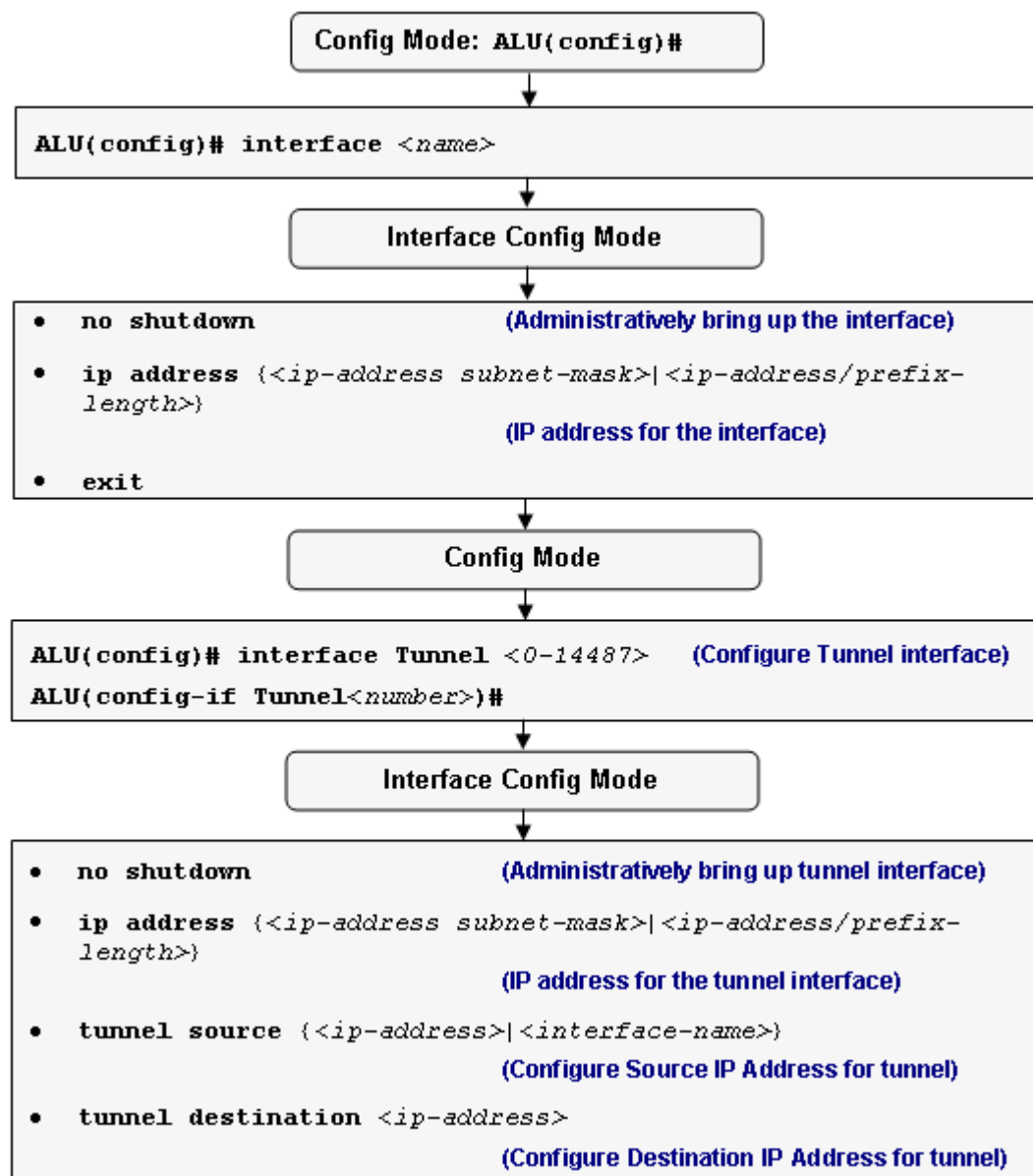


Figure 66: GRE Configuration Flow

GRE CLI COMMANDS

This section details the commands that are used in configuring GRE.

TO CONFIGURE A TUNNEL INTERFACE

Command (in CM)	Description
interface Tunnel <0-14487>	This command is used to create a tunnel interface.

EXAMPLE

```
ALU(config)# interface tunnel 7
ALU(config-if Tunnel7)#
```

TO ADMINISTRATIVELY BRING UP/SHUTDOWN THE TUNNEL INTERFACE

Command (in ICM)	Description
no shutdown	This command is used to administratively bring up the tunnel interface.
shutdown	This command is used to administratively bring down the tunnel interface.

EXAMPLE

```
ALU(config-if Tunnel7)# no shutdown

ALU(config-if Tunnel7)# shutdown
```


TO CONFIGURE IP ADDRESS ON A TUNNEL INTERFACE

Command (in ICM)	Description
ip address {<ip-address subnet-mask> <ip-address/ prefix-length>}	This command is used to assign an IP address and subnet mask to the tunnel interface.

EXAMPLE

```
ALU(config-if Tunnel7)# ip address 20.20.20.20/24
```


TO CONFIGURE MODE ON A TUNNEL INTERFACE

Command (in ICM)	Description
<code>mode {gre ipsec}</code>	<p>This command is used to set the mode on tunnel interface.</p>  <p>Note: By default, tunnel is configured in the GRE mode.</p>

EXAMPLE

```
ALU(config-if Tunnel7)# mode gre
```

TO CONFIGURE SOURCE IP ADDRESS FOR THE TUNNEL



Note: The source IP address of the tunnel must be of either a loopback interface or one of the physical interfaces.

Command (in ICM)	Description
<code>tunnel source {<ip-address>/<interface-name>}</code>	This command sets the source IP address of the tunnel.
<code>no tunnel source {<ip-address>/<interface-name>}</code>	The “no” command removes the configured source IP address of the tunnel.

EXAMPLE

```
ALU(config-if Tunnel7)# tunnel source 10.91.0.7
```

or

```
ALU(config-if Tunnel7)# tunnel source GigabitEthernet7/0
```

```
ALU(config-if Tunnel7)# no tunnel source 10.91.0.7
```

or

```
ALU(config-if Tunnel7)# no tunnel source GigabitEthernet7/0
```

To CONFIGURE DESTINATION IP ADDRESS FOR THE TUNNEL

Command (in ICM)	Description
<code>tunnel destination <ip-address></code>	This command sets the destination IP address of the tunnel at the remote end.
<code>no tunnel destination <ip-address></code>	The “no” command removes the configured destination IP address.

EXAMPLE

```
ALU(config-if Tunnel7)# tunnel destination 10.1.0.5
```

```
ALU(config-if Tunnel7)# no tunnel destination 10.1.0.5
```

To SET THE TUNNEL DF-BIT

Command (in ICM)	Description
<code>tunnel df-bit {clear set copy-from-inner-ip}</code>	This command sets the value of the DF-bit for the Outer-IP header. The default DF-BIT value is ‘clear’.

EXAMPLE

```
ALU(config-if Tunnel7)# tunnel df-bit clear
```

GRE CONFIGURATION SCENARIOS USING OA-700

GRE protocol is used to tunnel either IP or non-IP packets across an IP cloud. In the legacy applications, GRE was used to transport non-routable protocols like SNA and non-IP protocols like IPX, Appletalk, and DECnet since normal IP Security (IPsec) configurations could not transfer routing protocols, such as OSPF.

In current applications, IPsec provides security by encrypting packets sent over GRE tunnels.

The following features can be configured on a GRE Tunnel:

- GRE
- GRE + IP Filters + DoS
- GRE over IPsec

1. GRE CONFIGURATION

The OA-700 topology below consists of the following components:

- 2 OA-700 - OA700-1 and OA700-2

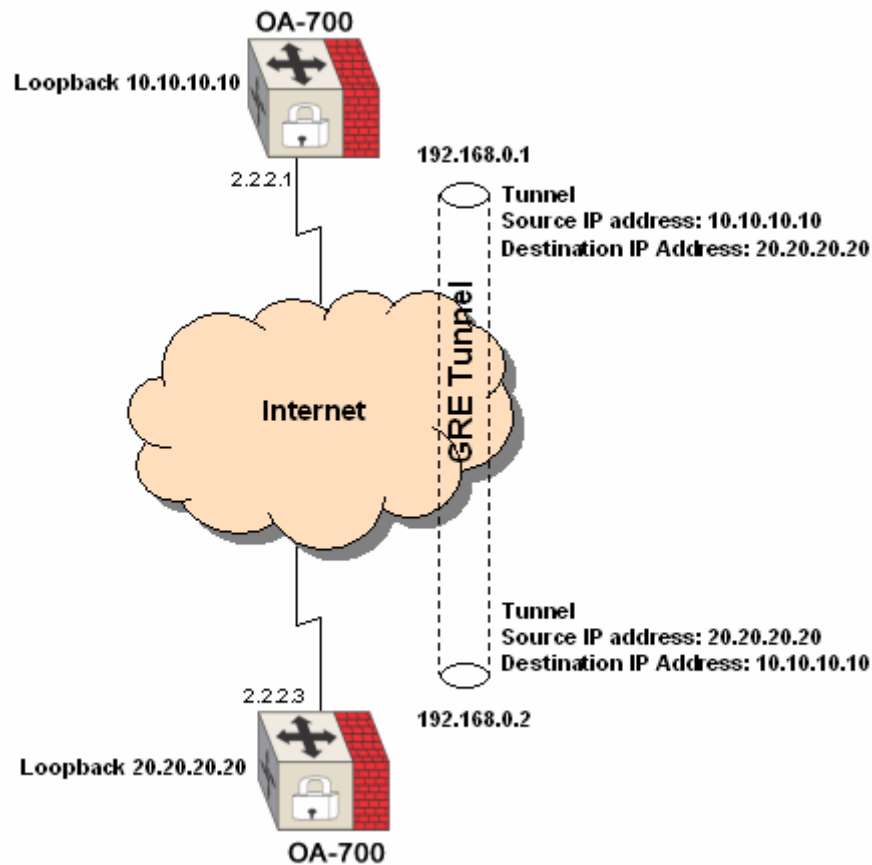


Figure 67: GRE Configuration Topology

ON OA700-1

a) Configure an interface

```
ALU-1(config)# interface loopback 1
ALU-1(config-if loopback1)# ip address 10.10.10.10/24
ALU-1(config-if loopback1)# no shutdown
```

b) Configure a tunnel interface

```
ALU-1(config)#interface tunnel1
ALU-1(config-if tunnel1)#ip address 192.168.0.1/24
ALU-1(config-if tunnel1)#no shutdown
```

c) Specify tunnel end-points

```
ALU-1(config-if tunnel1)#tunnel source 10.10.10.10
ALU-1(config-if tunnel1)#tunnel destination 20.20.20.20
ALU-1(config-if tunnel1)#no shutdown
```

ON OA700-2

a) Configure an interface

```
ALU-2(config)# interface loopback 1
ALU-2(config-if loopback1)# ip address 20.20.20.20
255.255.255.0
```

b) Configure a tunnel interface

```
ALU-2(config)#interface tunnel 1
ALU-2(config-if tunnel1)#ip address 192.168.0.2
255.255.255.0
```

c) Specify tunnel end-points

```
ALU-2(config-if tunnel1)#tunnel source 20.20.20.20
ALU-2(config-if tunnel1)#tunnel destination 10.10.10.10
ALU-2(config-if tunnel1)#no shutdown
```

VERIFICATION WITH SHOW COMMANDS**show ip route**

Shows all routes including routes on the remote end of the tunnel.

ALU-1(config)# show ip route

```
Codes: R - RIP, O - OSPF, C - connected
       S - static, M - mcstatic, B - BGP, I - IS-IS
       IA - OSPF inter area route,
       E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route,
       N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
       V - VRRP route
       * - candidate default route
```

ISIS route display notation:

First character

```
I - int route/int metric
E - ext route/int metric
i - int route/ext metric
e - ext route/ext metric
```

Second character:

```
1 - level 1
2 - level 2
u - level 1 with up/down set
U - level 2 with up/down set
```

Gateway of last resort is not set

2.0.0.0/24 is subnetted, 1 subnet

2.2.2.0 [0/0] is directly connected, GigabitEthernet7/1

192.168.0.0/24 [0/0] is directly connected, tunnell

ALU-1(config)#

10.10.10.10 is directly connected, Loopback0

2. GRE + IP FILTERS + DoS CONFIGURATION

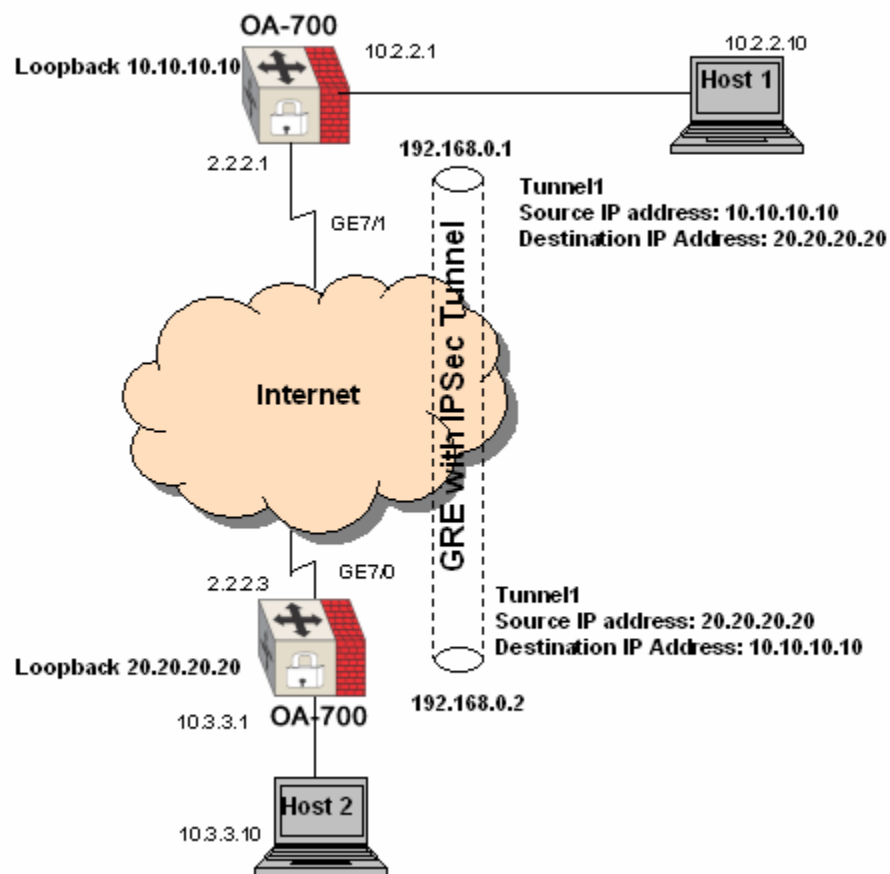


Figure 68: GRE+ IP Filters + DoS Configuration Topology

GRE + IP filters + Dos can be configured to deny/permit specific traffic through the GRE tunnel.

ON OA700-1

In conjunction with above configuration, define the filters as follows:

1. Configure rule using match-list to permit all traffic only from 10.3.3.1/24 network.
2. Configure filter by performing actions of permit/deny on the rules configured above.
3. Apply filters configured to the tunnel interface.

CONFIGURE RULES

```
ALU-1(config)#match-list permit-traffic
ALU-1(config-match-list-permit-traffic)#ip 10.3.3.1/24 any
ALU-1(config-match-list-permit-traffic)#exit
```

CONFIGURE FILTER

```
ALU-1(config)#ip filter tr-access
ALU-1(config-filter-tr-access)#match any permit-traffic
permit log
ALU-1(config-filter-tr-access)#exit
```

APPLY THE FILTER TO INGRESS OF TUNNEL INTERFACE

```
ALU-1(config)#interface tunnel1
ALU-1(config-if tunnel1)#ip filter in tr-access
ALU-1(config-if tunnel1)#exit
```

CREATE FIREWALL POLICY FOR PROTECTING THE NETWORK AGAINST 27 DOS ATTACKS

1. Configure a rule using match-list for any packet that matches classification.
2. Create an attack policy, which includes the signature against DoS attack.
3. Create a firewall policy, which uses the rule and attack policy created earlier.
4. Apply the firewall policy to the tunnel interface.

CONFIGURE A RULE FOR PROTECTING THE NETWORK AGAINST DoS ATTACK

```
ALU-1(config)#match-list dos
ALU-1(config-match-list-dos)#ip any any
ALU-1(config-match-list-dos)#exit
```

CREATE ATTACK POLICY

```
ALU-1(config)#firewall
ALU-1(config-firewall)#attack atk1
ALU-1(config-firewall-attack-atk1)#all
ALU-1(config-firewall-attack-atk1)#exit
```

CREATE FIREWALL POLICY

```
ALU-1(config)#policy p1
ALU-1(config-fiewall-p1)#match dos attack atk1 drop
ALU-1(config-fiewall-p1)#exit
```

APPLY THE FIREWALL POLICY TO INGRESS OF TUNNEL INTERFACE

```
ALU-1(config)#interface tunnel 1
ALU-1(config-if tunnel1)#firewall policy in p1
ALU-1(config-if tunnel1)#exit
```

3. GRE OVER IPSEC CONFIGURATION

The following figure displays a typical scenario to configure GRE over IPsec:

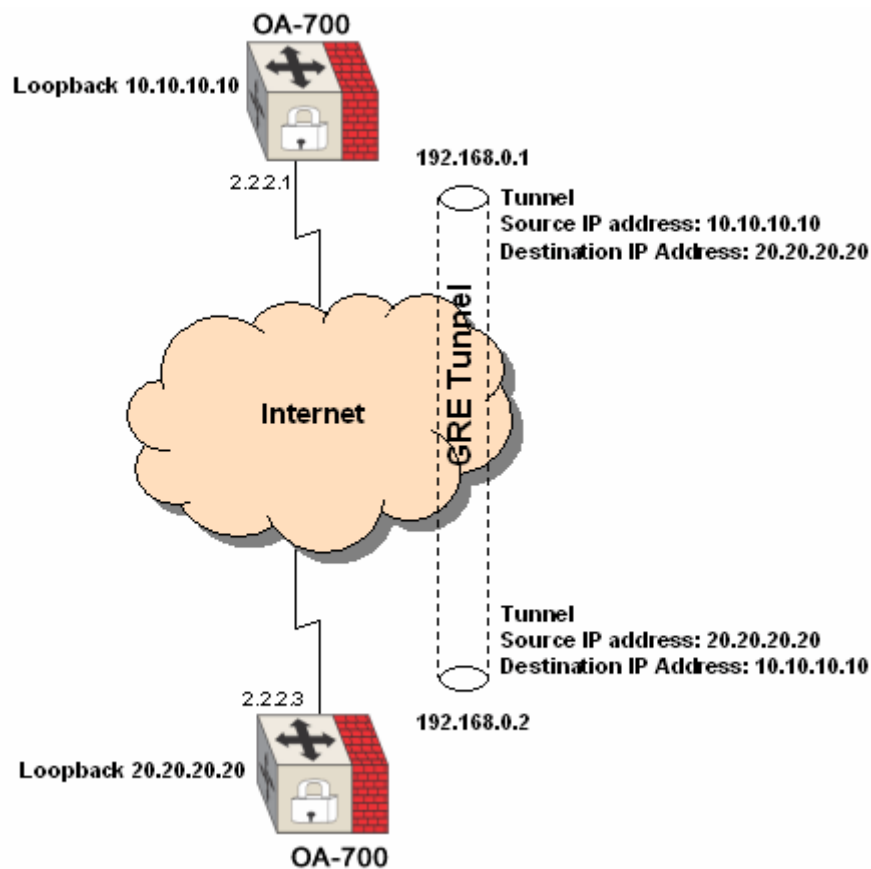


Figure 69: GRE + IPsec Configuration Topology

IPsec is used for transport mode encryption for tunneled traffic only. Ensure tunnel end-point reachability from OA700-1.

IPSEC VPN CONFIGURATION PROCESS**ON OA700-1**

a) Configure an interface

```
ALU-1(config)# interface loopback 1
ALU-1(config-if loopback1)# ip address 10.10.10.10/24
ALU-1(config-if loopback1)# no shutdown
```

b) Configure a tunnel interface

```
ALU-1(config)#interface tunnel1
ALU-1(config-if tunnel1)#ip address 192.168.0.1/24
ALU-1(config-if tunnel1)#no shutdown
```

c) Specify tunnel end-points

```
ALU-1(config-if tunnel1)#tunnel source 10.10.10.10
ALU-1(config-if tunnel1)#tunnel destination 20.20.20.20
ALU-1(config-if tunnel1)#no shutdown
```

IPSEC POLICY CONFIGURATION ON OA700-1

a) Configure a match-list

```
ALU-1(config)# match-list tunnel-traffic
ALU-1(config-match-list-tunnel-traffic)#1 protocol 47 host
2.2.2.1 host 2.2.2.3
```

b) Configure an IKE policy

```
ALU-1(config)# crypto ike policy test
ALU-1(config-ike-pollicy-test)#proposal md5-des
ALU-1(config-ike-pollicy-test)#ipsec security-association
lifetime seconds 28800
ALU-1(config-ike-pollicy-test)#lifetime seconds 86400
ALU-1(config-ike-pollicy-test)#pfs group2
```

c) Configure an IKE Key

```
ALU-1(config)#crypto ike key test peer 2.2.2.3
```

d) Configure a transform set

```
ALU-1(config)# crypto ipsec transform-set test esp-md5-des
```

e) Configure a crypto map

```
ALU-1(config)#crypto map test ipsec-ike test
ALU-1(config-crypto-map-test)#peer 2.2.2.3
ALU-1(config)#match tunnel-traffic
ALU-1(config)#transform-set test
ALU-1(config)#pfs group2
```

f) Bind the crypto map to a tunnel interface

```
ALU-1(config)#interface tunnel 1
ALU-1(config-if tunnel1)#crypto map test
```

ON OA700-2

a) Configure an interface

```
ALU-2(config)# interface loopback 1
ALU-2(config-if loopback1)# ip address 20.20.20.20/24
ALU-2(config-if loopback1)# no shutdown
```

b) Configure a tunnel interface

```
ALU-2(config)#interface tunnell
ALU-2(config-if tunnell)#ip address 192.168.0.2
255.255.255.0
ALU-2(config-if tunnell)#no shutdown
```

c) Specify tunnel end-points

```
ALU-2(config-if tunnell)#tunnel source 20.20.20.20
ALU-2(config-if tunnell)#tunnel destination 10.10.10.10
ALU-2(config-if tunnell)#no shutdown
```

IPSEC POLICY CONFIGURATION ON CISCO-2

a) Configure an access-list

```
access-list 101 permit gre host 2.2.2.3 host 2.2.2.1
```

b) Configure an IKE policy

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
```

c) Configure an IKE Key

```
crypto isakmp key test address 2.2.2.1
```

d) Configure a transform set

```
crypto ipsec transform-set test esp-des esp-md5-hmac
```

e) Configure a crypto map

```
crypto map test 1 ipsec-isakmp
 set peer 2.2.2.1
 set transform-set test
 set pfs group2
 match address 101
```

f) Bind the crypto map to an interface

```
interface Ethernet0/0
 ip address 2.2.2.3 255.255.255.0
 crypto map test
```

g) Bind the crypto map to a tunnel interface

```
interface tunnel 1
 crypto map test
```

CHAPTER 29 TRANSPARENT FIREWALL

This chapter covers the Transparent Firewall (TF) configuration for the OA-700.

The “**TF Overview**” section serves as an additional information on the Transparent Firewall. You can skip this section, and directly go to the configuration section of this chapter.

CHAPTER CONVENTIONS

Acronym	Description
TF	Transparent Firewall
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
TF-CM	Transparent Firewall Sub Configuration Mode - ALU (config-transparent-forward-name)#
SUM	Super User Mode - ALU#

TF OVERVIEW

The Transparent Firewall (Forwarding) feature allows the users to "drop" the OA-700 in their existing network without changing configuration of their network-connected devices. Thus, users can allow selected devices from a subnet to traverse the firewall while access to other devices on the same subnet is denied.

OA-700 SPECIFIC OVERVIEW

- OA-700 supports TF between two Ethernet interfaces (Services Engine Gigabit Ethernet).
- IP packets on the TF is subjected to L3 filters that can be applied on the ingress / egress path on an interface.
- The TF framework allows ARP packets and IP packets to be bridged across the TF'ed interfaces.
- The TF framework provides configuration for non-IP packets to be transparently bridged across the TF'ed interfaces.

TF CONFIGURATION

This chapter includes the following sections:

- [“TF Configuration Steps”](#)
- [“TF Configuration Flow”](#)
- [“TF Configuration Commands”](#)
- [“TF Configuration on OA-700”](#)

TF CONFIGURATION STEPS

This section lists the steps for configuring TF on the OA-700.

Configure TF on an Interface

Step 1: Enter into Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet3/0  
ALU(config-if GigabitEthernet3/0)#
```

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet3/0)# no shutdown
```

Step 3: Configure TF on an interface, and optionally attach TF policy (**See Step 4**) on the interface. See [“To Configure TF on an Interface”](#)



Note: An interface can have only one TF policy applied on it at any time.

Step 4: Configure TF policy (**Optional**)

- Configure a TF policy. See [“To Configure a TF Policy”](#)
- Configure pass through protocol. See [“To Configure Pass Through Protocol”](#)

Step 5: Use the show commands to view TF configuration. See [“Show Commands in TF”](#)

TF CONFIGURATION FLOW

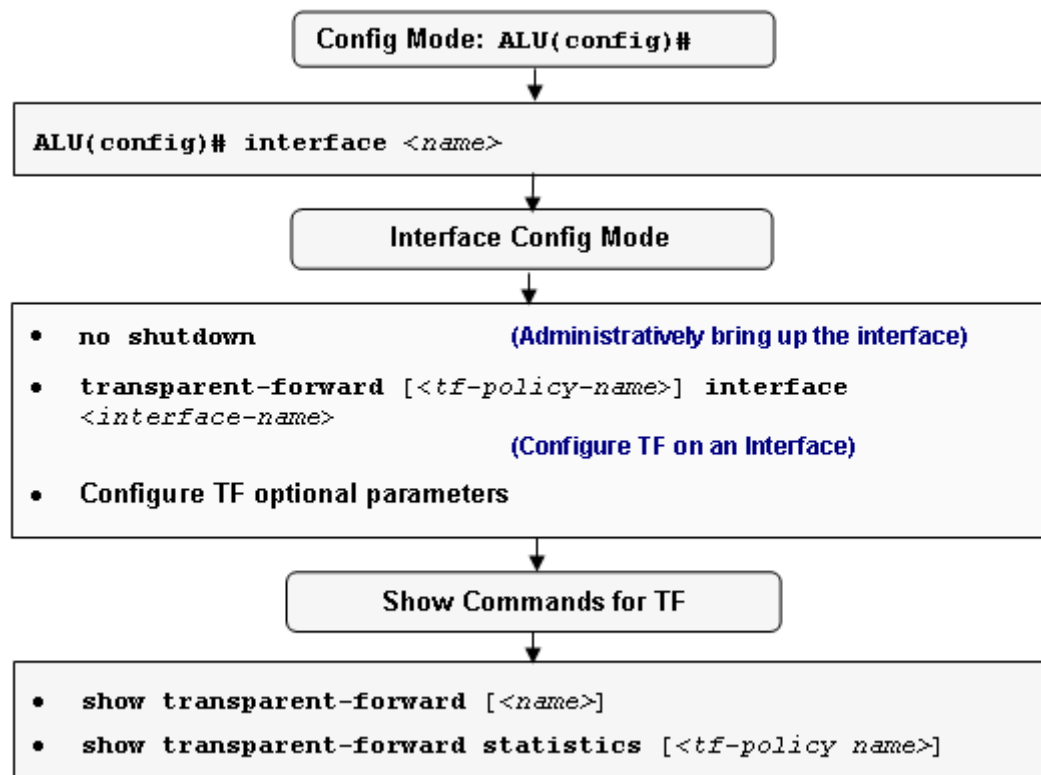



Figure 70: TF Configuration Flow

TF CONFIGURATION COMMANDS

The following steps are used for TF configuration:

To CONFIGURE TF ON AN INTERFACE

Command (in ICM)	Description
<code>transparent-forward</code> [<i><tf-policy-name></i>] interface <i><interface-name></i>	<p>This command is entered in the Interface Configuration mode.</p> <p>This command is used to configure TF feature on an interface (incoming interface). Use the interface keyword to configure the outgoing interface.</p> <p>You can optionally apply a TF policy (that defines the treatment of non-IP and non-ARP packets) on the interface.</p>  <p>Note: The 'IP Policy' command, if in effect, shall be cleaned up before this command takes effect.</p>
<code>no transparent-forward</code> [<i><tf-policy-name></i>]	<p>This command removes the TF feature on the interface, and detaches the TF policy attached to an interface, if specified.</p>



Note: The outgoing interface cannot be the same as incoming interface.

You can configure an IP address on an interface for management purpose.

EXAMPLE

The following configures TF feature and binds the TF policy 'TF1' on the interface GigabitEthernet3/0 with outgoing interface as VLAN 10.

```
ALU(config)# interface GigabitEthernet3/0
ALU(config-if GigabitEthernet3/0)# transparent-forward TF1
interface Vlan 10
```

If the TF policy 'TF1' is attached to the GigabitEthernet3/0, the following command detaches it from the interface:

```
ALU(config)# interface GigabitEthernet3/0
ALU(config-if GigabitEthernet3/0)# no transparent-forward
TF1
```

TO CONFIGURE A TF POLICY


Command (in CM)	Description
<code>transparent-forward <name></code>	This command is used to configure a TF policy.
<code>no transparent-forward <name> [force]</code>	This command is used to delete a TF policy. If the policy is attached to any of the interfaces, it cannot be deleted. The "force" keyword will automatically detach the specified policy from respective interfaces, and deletes the TF policy.

EXAMPLE

```
ALU(config)# transparent-forward TF1
ALU(config-transparent-forward-TF1)#

ALU(config)# no transparent-forward TF1
```

TO CONFIGURE PASS THROUGH PROTOCOL

Command (in TF-CM)	Description
<code>pass-through protocol {<1-65535> appletalk ipx nonip}</code>	This command is used to define how the non-IP packets should be treated in a TF configuration. Using this command, other protocols like IPX, Apple-talk can be configured to be bridged across the transparent firewalling interfaces. Using this command more than once will add the protocol to existing configured protocols.  Note: By default, IP and ARP protocols are configured as passthrough protocols.
<code>no pass-through protocol {<1-65535> appletalk ipx nonip}</code>	The command removes the pass through configuration.

EXAMPLE

```
ALU(config-transparent-forward-TF1)# pass-through protocol
nonip
ALU(config-transparent-forward-TF1)# no pass-through protocol
nonip
```


SHOW COMMANDS IN TF

TO VIEW TF POLICY DETAILS

Command (in SUM/CM)	Description
show transparent-forward [<name>]	This command is used to view all the TF policies configured in the system. If a TF policy is specified then the details of the specific TF policy is displayed. This command also displays the interfaces on which these policies are applied.

EXAMPLE

```

ALU(config)# show transparent-forward
!
! Transparent-forward configuration
!
interface GigabitEthernet7/1
    transparent-forward interface GigabitEthernet7/0
exit
!
transparent-forward tf
    pass-through protocol ipx
exit
!
interface GigabitEthernet7/0
    transparent-forward tf interface GigabitEthernet7/1
exit
!
ALU(config)#

```

To VIEW TF POLICY STATISTICS

Command (in SUM/CM)	Description
show transparent-forward statistics [<i><tf-policy name></i>]	<p>This command is used to display the statistics of all the TF policies configured in the system.</p> <p>If a policy-name is specified, then the statistics for the specified TF policy are displayed.</p> <p>This displays the number of IP, ARP, IPX Appletalk, 'other protocol' packets (excluding the above) forwarded by TF, and number of packets dropped.</p>

EXAMPLE

```

ALU(config)# show transparent-forward statistics
!
! Transparent-forward Statistics
!
interface GigabitEthernet7/1 :
IP 0, ARP 0, IPX 0, AppleTalk 0, Others 0,Dropped 0

interface GigabitEthernet7/0 : tf
IP 0, ARP 0, IPX 0, AppleTalk 0, Others 0,Dropped 0

ALU(config)#

```

CLEAR COMMANDS**To CLEAR TF POLICY STATISTICS**

Command (in SUM/CM)	Description
clear transparent-forward statistics [<i><tf-policy name></i>]	<p>This command clears the statistics of all the TF policies configured in the system.</p> <p>If a TF policy is specified, then the statistics for the specified TF policy are cleared.</p>

EXAMPLE

```

ALU(config)# clear transparent-forward statistics

```

TF CONFIGURATION ON OA-700

Consider a scenario, a corporate XYZ with LAN (GigE 3/1) is connected to the internal network of XYZ and the WAN (GigE 3/0) is facing the external gateway. Other than IP and ARP traffic, XYZ intends the IPX traffic to be bridged across the TF'ed ports.

In order to achieve this, you need to configure TF on an interface, and attach the TF policy with pass through protocol as IPX on the interface.

CONFIGURATION STEPS

Quick Steps

1. Create a TF policy, and configure the pass through protocol
2. Configure TF on an interface.

Detailed Steps

Step 1: Create a TF policy for bridging IPX packets transparently

```
ALU(config)# transparent-forward TF1
ALU(config-transparent-forward-TF1)# pass-through
protocol ipx
```

Step 2: Configure an interface, apply the TF policy for forwarding IP, ARP and IPX packets coming in on GigE 3/1 to GigE 3/0

```
ALU(config)# interface GigabitEthernet3/1
ALU(config-if GigabitEthernet3/1)# transparent-forward
TF1 interface GigabitEthernet 3/0
```

SHOW COMMANDS

Verify the TF policy configuration by using the following show command:

```
ALU(config)# show transparent-forward
!
transparent-forward TF1
    pass-through protocol ipx
exit
!
interface GigabitEthernet3/1
    transparent-forward TF1 interface GigabitEthernet3/0
exit
!
```


Part 7 Quality of Service

CHAPTER 30 QUALITY OF SERVICE

This chapter documents the commands for QoS (Quality of Service) configuration. QoS refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantee on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.

This chapter includes the following sections:

- [“QoS Overview”](#)
- [“Generic terms used in QoS”](#)
- [“Alcatel-Lucent Specific Overview on QoS”](#)
- [“QoS Configuration Steps”](#)
- [“QoS Show Commands”](#)
- [“QoS Clear Commands”](#)
- [“QoS Test Scenarios on OA-780”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
ICM	Interface Configuration Mode - ALU (config-interface name)#
Class-map Mode	Class Map configured - ALU (config-class-map)#
Policy-map Mode	Policy Map configured - ALU (config-policy-map)#
Class Mode	Traffic-class inside a policy-map- ALU (config-policy-map-class)#
DSCP	Differentiated Services Code Point
RED	Random Early Detection
WRED	Weighted Random Early Detection

QoS OVERVIEW

The term QoS commonly refers to the management of link bandwidth and the preferential treatment of certain traffic over others. The mechanisms to support this are many, some are complicated and for most of these mechanisms, no standards exist.

There are, however, fairly standard algorithms that can be applied to some of the mechanisms. Several of the QoS mechanisms have been in use for years, for example to limit the bandwidth usage to conform to the Service Level Agreements (SLAs). The ISP commonly makes sure this contract is honored by dropping all traffic above the rate the customer pays for.

QoS generally involves prioritization, queuing, and shaping of network traffic. QoS can be defined in terms of the total network "pipe" being queued and shaped to the performance of a given server or router, or in terms of specific applications like the source, destination, TOS, control information, and data. A network monitoring system must typically be deployed as a part of QoS to insure that networks are performing at the desired level.

QoS supports voice and data service simultaneously on the OA-700. This include controlled resource sharing by providing bandwidth guarantee for different classes. It also provides features that make QoS configuration simpler by means of Auto QoS commands.

GENERIC TERMS USED IN QoS

QoS

QoS is a term commonly used to describe a policy or a set of mechanisms used to manage bandwidth or give certain types of traffic preferential treatment over others.

DSCP

The DSCP (Differentiated Services Code Point) value refers to 6 bits in the TOS byte in the IP header that can be used to mark the IP datagram with a certain value. This value can be interpreted by devices. This packet passes through on the way to its destination.

IP PRECEDENCE

It has become common to use 3 bits in the TOS byte in the IP header to mark the packet for QoS treatment. We can use IP Precedence to assign values from 0 to 7 to classify and prioritize types of traffic.

RED

RED (Random Early Detection) is a congestion avoidance technique.

WRED

WRED (Weighted Random Early Detection) is also a congestion avoidance technique.

POLICING

Dropping or marking packets in order to make traffic stay below a configured bandwidth. Thus defined, a traffic policing do not remove traffic burst, but controls the size of the peak.

SHAPING

The process of delaying packets before they go out, to make the traffic conform to a configured maximum rate. The main intention of shaping the traffic is to define the traffic to flow within an envelop.

SCHEDULING

The process of identifying which packet is to be selected for further action.

QUEUEING

An algorithm that manage the queue of an interface/sub-interface. Queue algorithm could be a passive (drop tail, drop-head, etc.) or active (RED, WRED etc.)

DIFF-SERV

Diff-serv is a class-based mechanism for specifying and controlling network traffic. It differentiates IP traffic so that the traffic's relative priority could be determined on a per-hop basis. It helps certain types of traffic (like voice) get precedence over others.

DIFFERENTIATED SERVICES FIELD (DS FIELD)

Defines the packets class (or type) in a Diff-serve domain. The classical TOS field in the IP header is renamed as DS field. Six bits of the DS field are used as a code point (DSCP) to select the Per-Hop Behavior (PHB) a packet experiences at each node.

PHB (PER HOP BEHAVIOR)

In a diff-serv approach of providing QoS for IP flow, each packet is treated in a specific manner in each node. This treatment of packet at each hop is defined as Per Hop Behavior.

ASSURED FORWARDING (AF)

Is a type of Per-Hop Behavior (PHB) group that provides delivery of IP packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence.

EXPEDITED FORWARDING (EF)

The intent of the EF Per-Hop Behavior (PHB) is to provide a building block for low loss, low delay and low jitter services.

ALCATEL-LUCENT SPECIFIC OVERVIEW ON QoS

QoS functionality and features supported are implemented at two stages - ingress QoS processing and egress QoS processing. Ingress QoS processing deals with features that are applicable while the packet gets into the OA-700. For e.g., policing is a feature that admits packets into the system only if they arrive at a committed rate. Policing functionality is normally applied at the ingress QoS processing stage. Egress QoS processing deals with features that are applicable to packets that leaves the OA-700. For e.g., shaping that fits the outgoing traffic in to a committed rate envelope, is implemented at the egress QoS processing stage.

Packets at the ingress are classified using common classifier, and exploits the one-pass classification feature on the OA-700. These packets, based on classification are grouped into a class. QoS is applied on each flow.

FEATURES SUPPORTED BY OA-700

1. Traffic policy definition and policy management
2. Packet Classification
 - Multi-field packet classification
 - Behavior Aggregate (BA) classification
 - TOS/Precedence based classification
3. Packet Queuing
 - Per interface queuing
 - Weighted Fair Queuing
 - CBQ (Class Based Queuing)
 - Strict priority scheduling
 - DSCP to queue mapping, user configurable
 - A policy map can have a maximum of **16 classes** including the default traffic class - 'class-default'.
 - One can be a default class 'class-default' and another one can be a network-control class.
 - 14 classes are used for shaping.
 - The class-default traffic class is a non-priority class.
 - Priority and network-control commands are not applicable for class-default traffic class.
4. Congestion Management
 - Tail Drop
 - Active queuing using WRED
 - Ingress traffic conditioning

5. Metering/Policing
 - Single Rate Three Color policer
 - Two Rate Three Color Marker

6. Packet Marking
 - Marking router generated packets, user configurable
 - Marking routed/forwarded packets, user configurable
 - DSCP to Queue Mapping (Static)

7. DiffServ EF/AF
 - Expedited Forwarding PHB
 - Assured Forwarding PHB
 - Architecture for Differentiated Service

8. Egress queues configurable at interface or sub-interface level
 - Queuing per Interface (LAN/WAN)
 - Queuing per Virtual Circuit (FR/T1E1)
 - Queuing per Tunnel
 - Hierarchical up to 4 levels.

9. Bandwidth Management
 - Priority Queuing (Bandwidth Allocation)
 - Weighted Fair Queuing
 - CBQ (Class Based Queuing)

10. Management Support
 - CLI
 - Support for simple configuration (Auto QoS)
 - Web GUI

TRAFFIC WITHOUT POLICING AND SHAPING

The following diagram depicts the traffic flow before implementing the QoS:

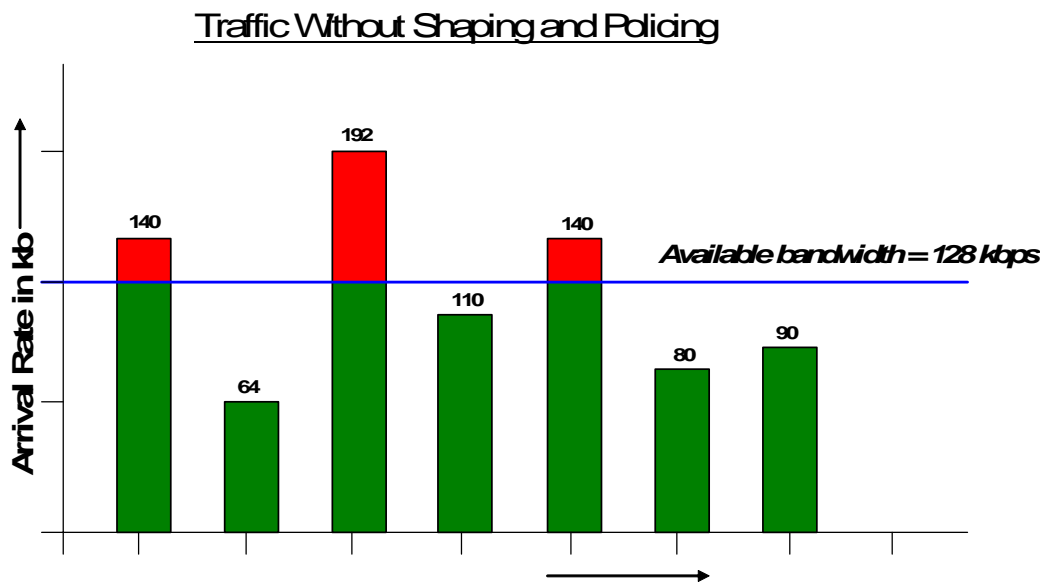


Figure 71: Data Traffic before Policing And Shaping

In the above diagram, the portion marked **red** implies the packet flow exceeding the allowed bandwidth level. If QoS is not implemented, all these packets are dropped.

TRAFFIC WITH POLICING

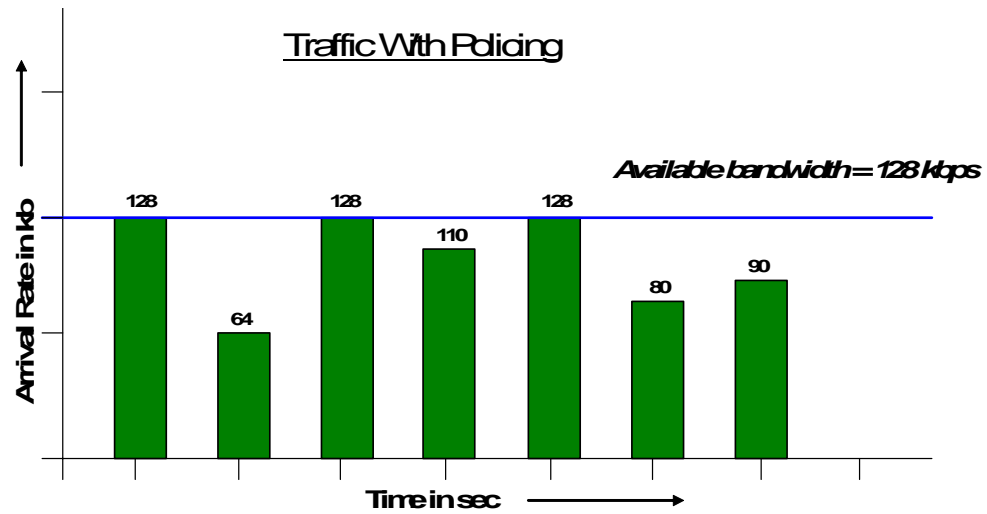


Figure 72: Data Traffic with Policing

The diagram above depicts the traffic flow after implementing Policing. Here, the packets exceeding the available bandwidth are all dropped. This provides for a decent flow of traffic.

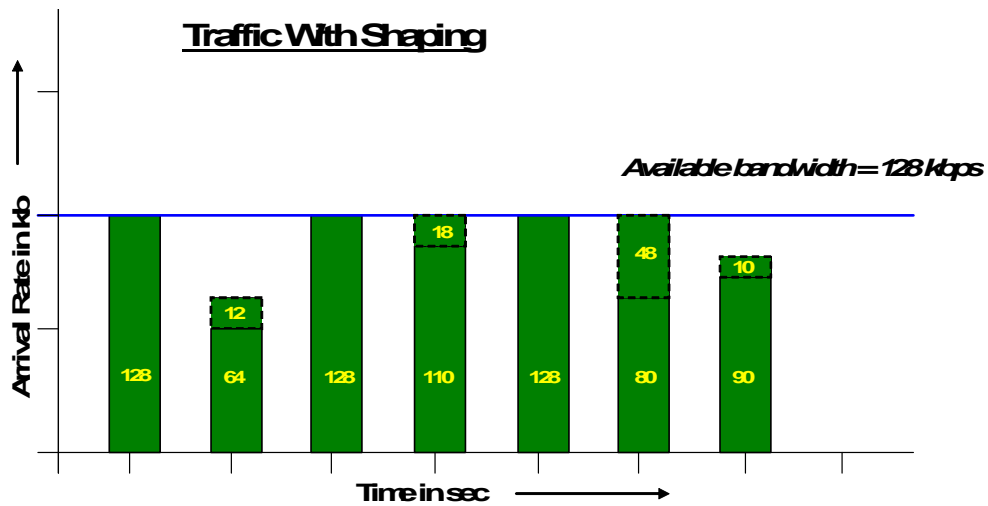
TRAFFIC WITH SHAPING

Figure 73: Data Traffic with Shaping

The above diagram depicts the traffic flow after implementing Shaping. Here, the packets are all shaped and queued. The packets exceeding the available bandwidth, is queued up and there is no loss of data.

HIERARCHICAL QUEUEING

Hierarchical Queuing provides a mechanism of controlled sharing of excess bandwidth in a hierarchical fashion. The requirement of hierarchical queuing is illustrated below.

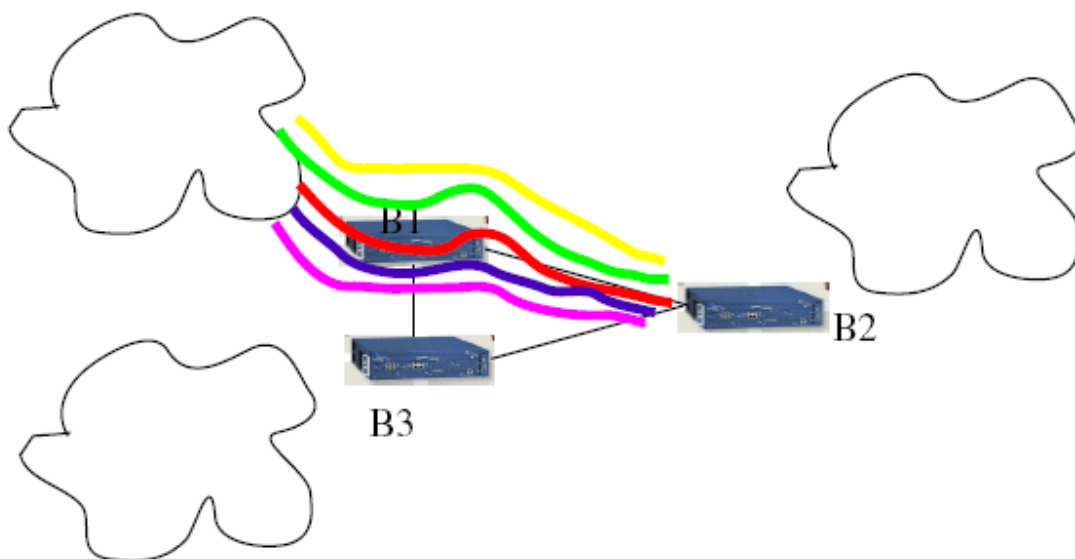


Figure 74: Link Sharing Requirement Example

Two branch offices are linked with 2Mbps link (as shown in the above figure). Five different type of traffic require an efficient way of sharing the link between, voice, VPN tunnel and public Internet access.

One possible solution:

Voice: 128, no one else should use this, also high priority.

VPN traffic: Total of 768 Kbps to be shared between SMTP and CVS.

Public Internet: Total of 1 MBPS, to be shared between web and SMTP.

A Link sharing scheme to suite this is deployed on the OA-780 with the help of hierarchical link sharing feature on the 2Mbps link (as shown in the figure below).

Class in tree structure will be typically of three kinds: Leaf class, Case class, and root class. Leaf class will have a destination queue associated with it. Depending on the need of organization, leaf might indicate a flow of certain application or IP address in a subnet. Case class will have more than two branches, for e.g., it could be specific IP source address with all the TCP ports as a leaf nodes. Root class is the tree root.

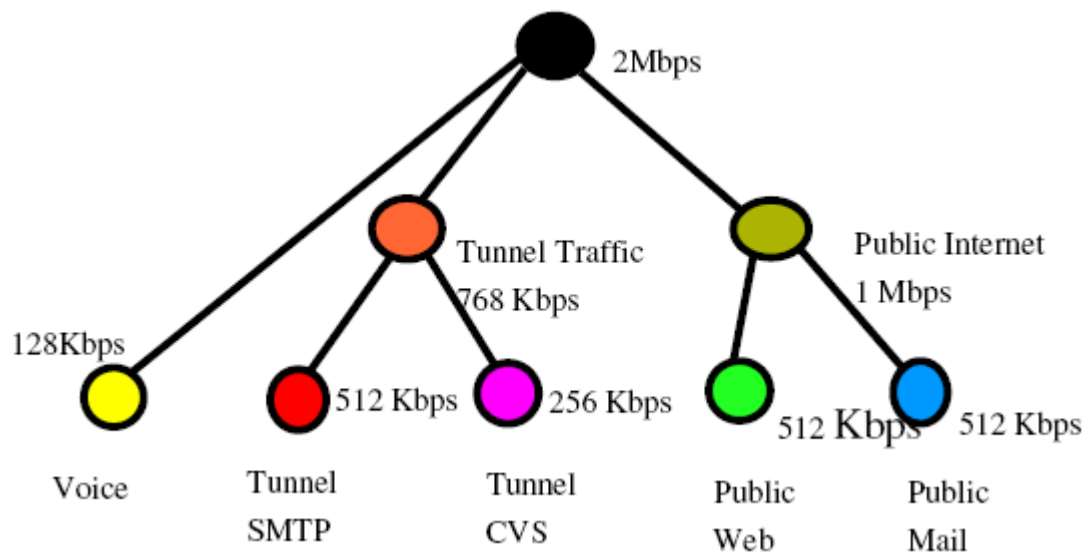


Figure 75: Link Sharing Solution

Hierarchical queues are configured using 'service-policy' command within a policy. Thus policy-in-a-policy configuration provides hierarchal link sharing structure.

BANDWIDTH SHARING IN TUNNELS

A typical requirement of a service edge router is to support VPN tunnels to corporate office. Over these VPN tunnel, bandwidth sharing and other QoS functionalities (marking/classification/police, etc.) are expected.

The example of link bandwidth sharing requirements over VPN tunnels is depicted in the figure below. This type of link sharing is achieved using regular hierarchical link sharing algorithm.

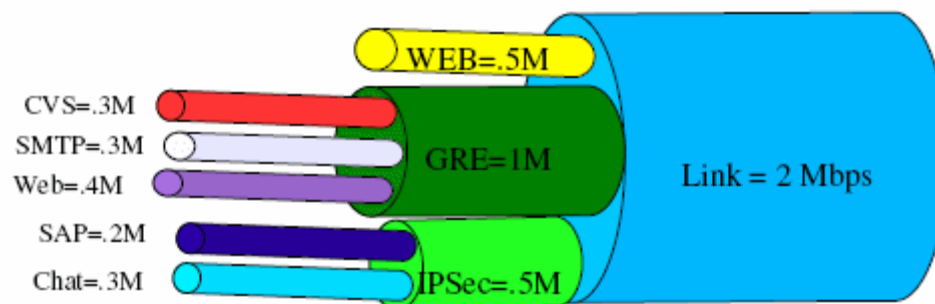


Figure 76: Link Bandwidth sharing requirements over VPN tunnels

In order to provide classification, a pre-classify command is introduced. For the purpose of providing service-policy in the tunnel, each of the tunnel (IPSec or GRE) must support interface abstraction. QoS policy is applied on this interface similar to service-policy on the physical interface. Also, in order to manage congestion on the physical interface, a policy has to be created on the physical interface, and this policy must include tunnel policy as child policy.

QoS CONFIGURATION

This chapter includes the following sections:

- [“QoS Configuration Steps”](#)
- [“QoS Configuration Flow”](#)
- [“QoS Configuration Commands”](#)
- [“QoS Test Scenarios on OA-780”](#)

QoS CONFIGURATION STEPS

You can configure QoS on OA-700 by any of the following procedures:

- **Auto QoS procedure**
- **Standard procedure**

Auto QoS Procedure:

Step 1: Enter into the Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```



Note: Auto QoS can be configured on Gigabit Ethernet, Serial, Tunnel, and Switchport interfaces.

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Configure Auto QoS. See [“Auto QoS Configuration”](#)

Standard Procedure

Step 1: Configure the **match-lists** using the common classifiers syntax. (Refer to the chapter "**Common Classifiers**" on page 359 in this guide).

Step 2: Configure Class-map. See "[To Configure a Class Map](#)"

Step 3: Configure Rule for the Class-map. See "[To Configure a Rule for a Class-map](#)"

Step 4: Configure Policy-map. See "[To Configure a Policy Map](#)"

Step 5: Configure Traffic Class, i.e., associate a class-map to a policy-map. See "[To Configure a Traffic Class](#)"

Attach Policy Map to an interface

Step 6: Enter into the Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```



Note: QoS can be configured on Gigabit Ethernet, Serial, Tunnel, Switchport and ISDN-Dialer interfaces.

Step 7: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 8: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 9: Interface Binding - Attach a configured policy map to an interface as per the desired direction i.e, either "IN/OUT. See ["To Attach a Policy Map to an Interface"](#)



Note: An interface can have only one policy map attached in a direction.

Step 10: View the Policy-map details using the respective "show" commands. See ["QoS Show Commands"](#)

Step 11: Clear the queuing interface statistics. See ["QoS Clear Commands"](#)

QoS Optional Parameters

- Configure attributes of a Traffic Class. See ["Traffic Class Attributes Configuration"](#)
- Configure Hierarchical Policy. See ["Hierarchical Policy Configuration"](#)
- Configure QoS over Tunnel Interface. See ["QoS over Tunnel Interface"](#)

QoS CONFIGURATION FLOW

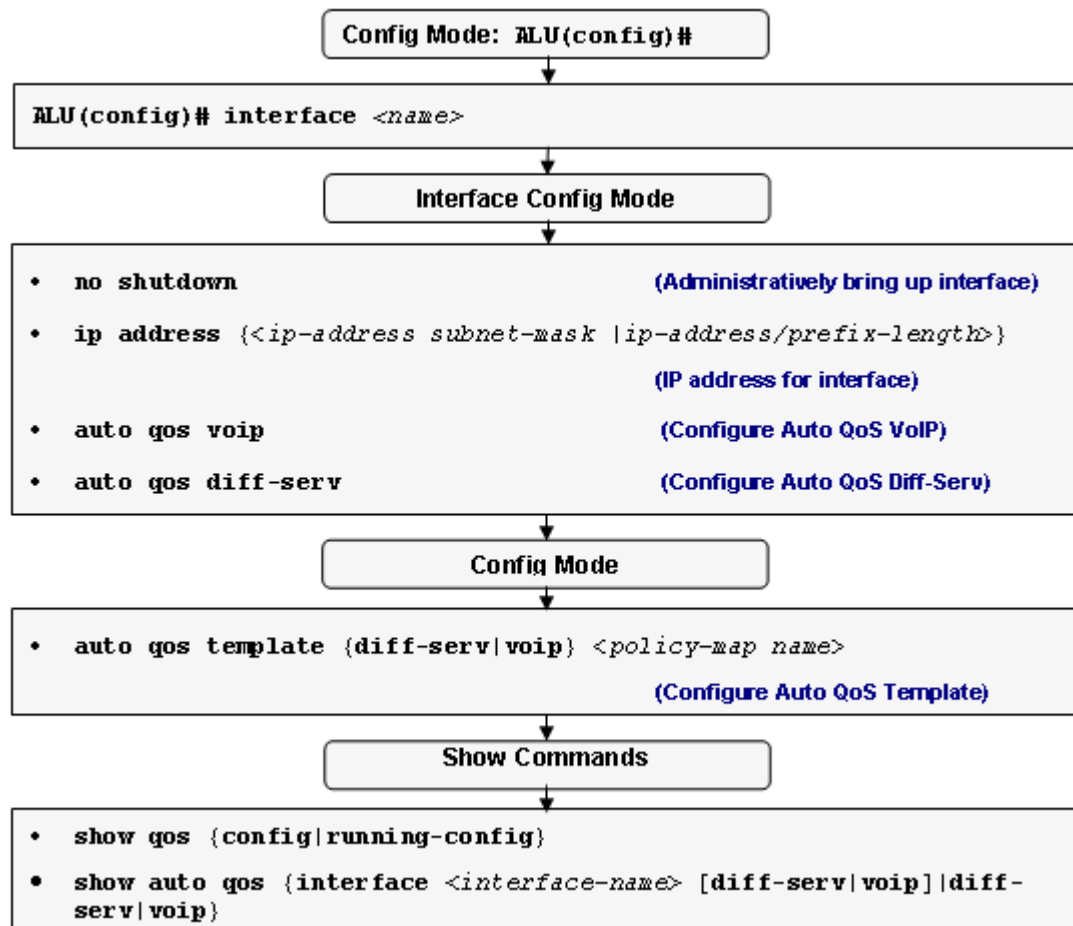


Figure 77: QoS Configuration Flow - Auto QoS Procedure

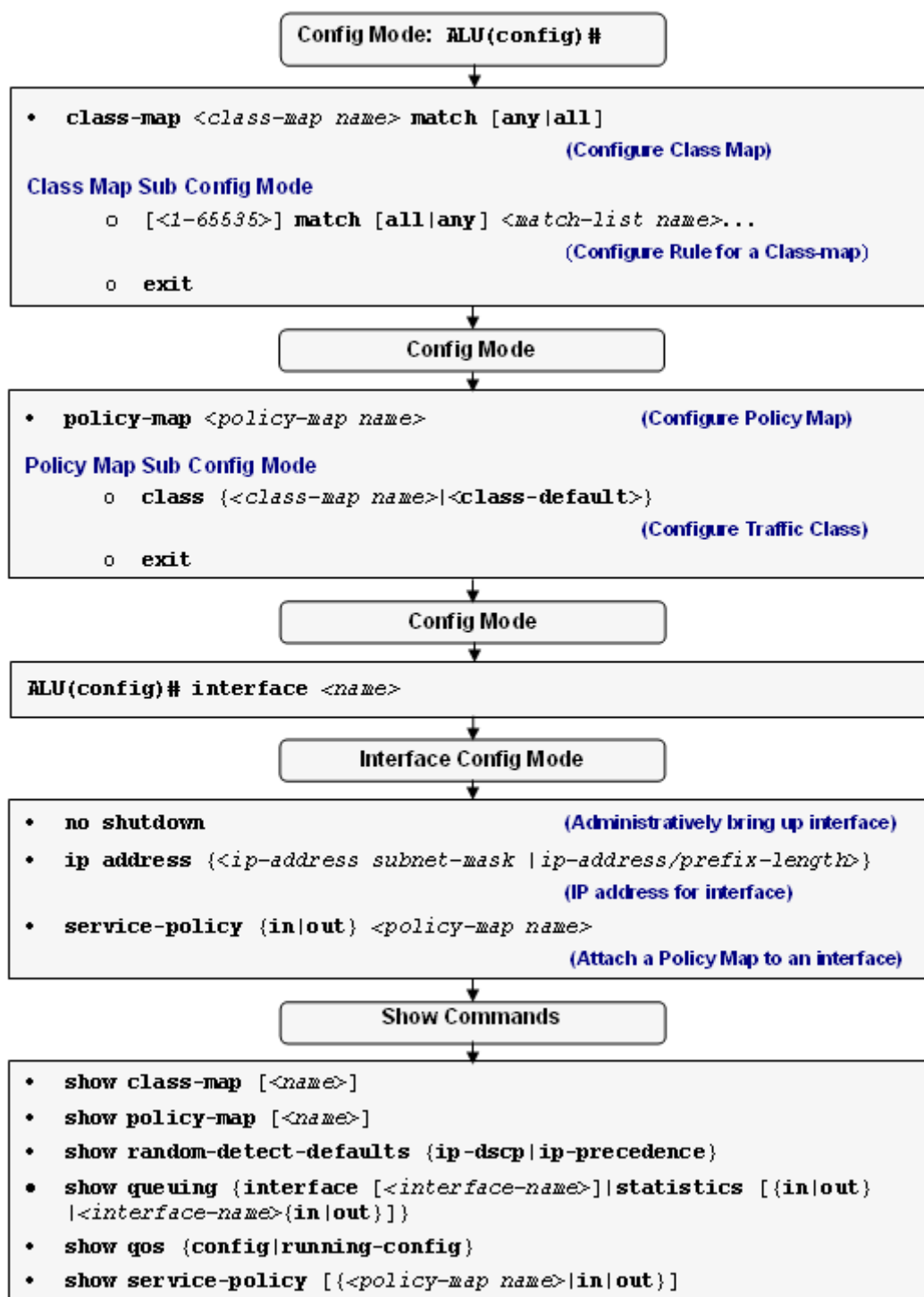


Figure 78: QoS Configuration Flow - Standard Procedure

QoS CONFIGURATION COMMANDS

This section details the commands used to configure QoS on the OA-700.

CLASS MAP CONFIGURATION

Notes:

1. You can define match-all or match-any for all the match-lists configured within a class map.
2. There can be any number of match commands within the class-map mode. A match command within a class map can have any number of match-list names.
3. The match-list-name is an alphanumeric string. You can configure any number of match-lists.
4. There is no priority among the different match statements. It is just a logical OR among them.

TO CONFIGURE A CLASS MAP

Command (in CM)	Description
class-map <class-map name> match [any all]	This command is used to configure a class map, and define the relationship between all the match-lists configured within the class map. This command enters the class-map sub-configuration mode. Default match-list relationship of a class-map is ' match-any '.
no class-map <class-map name>	Deletes a configured class-map.

EXAMPLE

```

ALU(config)# class-map C1 match-all
ALU(config-qos-C1)#

ALU(config)# no class-map C1
Class-Map C1 removed.

```

To CONFIGURE A RULE FOR A CLASS-MAP

Command (in Class-map Mode)	Description
[<1-65535>] match [all any] <match-list name>...	This command is used to configure rules (associate match-lists and set priority for the rule) for a class map. The range for the rule is 1-65535. This rule number signifies the priority of a rule.

EXAMPLE


```
ALU(config-qos-C1)# match all m1 m3
```

```
ALU(config-qos-C1)# match any m2 m4 m5
```

POLICY MAP CONFIGURATION**Notes:**

1. A policy map can have a maximum of 16 traffic classes including the default class. By default, the default-class exists for a policy map.
2. A Traffic Class is defined by using the 'class' command. 'Class' command takes an already defined class map or the keyword 'class-default' (to configure the default class) as an argument.
3. Within a policy map, only one traffic class can be configured as either priority or network-control class. A class cannot be both priority and network control class at the same time.
4. Priority and network-control commands are not applicable for the 'class-default'.
5. All the attributes of a traffic class are optional. By default, policing and shaping are not enabled on any traffic class. Queue limit is the only parameter which has a default argument set.
6. To configure another traffic class as either priority or network control, delete the earlier configured traffic class.

To CONFIGURE A POLICY MAP

Command (in CM)	Description
policy-map <policy-map name>	This command is used to configure a policy map.
no policy-map <policy-map name>	This removes a user configured policy-map.  Note: You cannot remove a policy map if it has been attached to an interface either in ingress or egress direction.

EXAMPLE

```

ALU(config)# policy-map P1
ALU(config-qos-P1)#

ALU(config-qos-P1)# no policy-map P1
Policy-map P1 deleted.

```

To CONFIGURE A POLICY MAP DESCRIPTION

Command (in Policy-map Mode)	Description
description <line>	The description for the policy map configured.

EXAMPLE


```

ALU(config-qos-P1)# description P1 is the name of the policy-
map

ALU(config-qos-P1)# show policy-map P1
policy-map P1
  description P1 is the name of the Policy Map

```

To CONFIGURE A TRAFFIC CLASS

Command (in Policy-map Mode)	Description
<pre>class {<class-map name> <class-default>}</pre>	<p>This command is used to configure a traffic class, i.e., associate a user-defined class map to the policy map.</p> <p>Use class-default keyword to configure the default traffic class to the policy map.</p> <p>This command enters the Class sub-configuration mode inside the Policy-map Mode.</p> <div style="text-align: center;">  </div> <p>Note: If no rule is associated with a class-map and if you try to configure a class on that class-map, a warning is displayed.</p> <p>Example:</p> <pre>ALU (config-qos-P1)# class C1 No rule in class-map C1. It will not match any traffic.</pre>
<pre>no class <class-map name></pre>	<p>This command removes a traffic class associated with the policy map.</p>

EXAMPLE

```
ALU(config-qos-P1)# class C1
ALU(config-qos-P1-C1)#
```

```
ALU(config-qos-P1-C1)# class class-default
ALU(config-qos-P1-class-default)#
```

```
ALU(config-qos-P1)# no class C1
Class C1 removed.
```

ATTACHING A POLICY MAP TO AN INTERFACE

Notes:

1. An interface can have only one policy map attached in a direction.
 2. It is possible to attach a policy map to any of the Layer 3 physical interfaces.
 3. When a policy map is attached in the ingress direction on an interface, then only policy and mark attributes will be used.
 4. When a policy map is attached in the egress direction on an interface, then shape, priority, mark, and queue-limit attributes will be used.
-

TO ATTACH A POLICY MAP TO AN INTERFACE



Note: An empty policy can be attached to the interface as a policy-map will have a default traffic class associated with it, by default.

But, while attaching an empty policy-map to the interface, the system gives a warning: "Policy map() is empty. It should contain at least one traffic class or the class-default with some configuration."

This is just a warning, you can proceed with the configuration.

Command (in ICM)	Description
service-policy {in out} <policy-map name>	This command is entered in the Interface Configuration mode. This command is used to attach a policy-map to an interface either in ingress or egress direction.
no service-policy {in out} <policy-map name>	This command detaches the policy map from the interface it has been bound.

EXAMPLE

```
ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# service-policy in P1

ALU(config)# interface GigabitEthernet 7/0
ALU(config-if GigabitEthernet7/0)# no service-policy in P1
```

TRAFFIC CLASS ATTRIBUTES CONFIGURATION

To CONFIGURE POLICE

Policing is done using Token Bucket Algorithm. A token bucket is a formal definition of a rate of transfer. It has two mandatory parameters like burst size, mean rate and can have optional parameter of excess burst size.

The traffic received on a flow that is to be policed is examined. The rate of the traffic is compared to a configured token bucket and action is taken based on the result.

When sufficient number of tokens is available then the arriving traffic is said to confirm and then the corresponding number of tokens are removed from the bucket. If there are not enough tokens, then the traffic is said to exceed.

Policer does not do any smoothing or shaping of traffic, and therefore does no buffering and adds no delay. The rate limit define which packets confirm to or exceed the defined rate based on the following three parameters:

- Committed rate – Determines the long term average transmission rate, the traffic that falls under this rate will always conform.
- Committed burst size (Bc) – Determines how large traffic bursts can be before some traffic exceeds the rate limit.
- Excess burst size (Be) – Determines how large traffic bursts can be before all traffic exceeds the rate limit.


The maximum number of tokens a bucket can ever contain is determined by the normal burst size configured for the token bucket. Excess Burst (Be) is set to value higher than the normal burst value.

When rate limit is applied, Policer will remove tokens that are equivalent in number to the byte size of the packet from the bucket. If a packet arrives and there are fewer tokens that are available in the token bucket than that is required by the packet's byte size, then Excess Burst is utilized if configured. If packet cannot be transmitted (due to lack of tokens), packet is dropped and no tokens are removed from the bucket.

Two Rate Three Color Marker (trTCM) meters an IP Packet stream and marks its packets based on two rates, Peak Information Rate (PIR) and Committed Information Rate (CIR), and their associated burst sizes to be red (exceeds PIR), yellow (exceeds CIR) or green (does not exceed CIR).

This command is used to apply policing on the traffic class. The **committed-rate** keyword is compulsory. The **excess-burst** keyword must be given if **exceed-action** parameter is set. Action could be any one of the following:

1. Drop
2. Transmit
3. Set (marks the packet either in IP-precedence or IP-DSCP fields)

Command (in Class Mode)	Description
<pre> police {committed-rate <8000-10000000>} [commit-action {drop set {ecn-ce ip-dscp {<0-63> <dscp-mnemonics>}} ip- precedence {<0-7> <precedence-mnemonics>}} tos {<0-15> <tos-mnemonics>}} transmit}] [committed-burst {<40- 150000> exceed-action {drop set {ecn-ce ip-dscp {<0-63> <dscp-mnemonics>}} ip-precedence {<0-7> <precedence-mnemonics>}} tos {<0-15> <tos-mnemonics>}} transmit}] [excess-burst {<40-150000> violate-action {drop set {ecn-ce ip-dscp {<0-63> <dscp-mnemonics>}} ip- precedence {<0-7> <precedence-mnemonics>}} tos {<0-15> <tos-mnemonics>}} transmit}] [peak-rate <8000-2000000>] </pre>	<p>This command sets the QoS traffic policing parameters on the traffic class.</p>  <p>Note: Excess-Burst cannot be less than Committed-Burst.</p> <p>Exceed-Action will be of no effect if Commit-Action is set to 'drop'.</p> <p>Violate-Action will be of no effect if Exceed-Action is set to 'drop'.</p> <p>Peak rate cannot be less than the Committed-rate.</p> <p>Policing is allowed at leaf class only.</p> <p>If Shaper is already configured, policer is not allowed in the same class.</p>
<pre> no police </pre>	<p>This command removes the configured police on the traffic class of the policy map.</p>

Refer '**Appendix B - QoS Values and Mnemonics**' for IP-DSCP, IP-Precedence, and ToS mnemonics.

EXAMPLE

```

ALU(config-qos-P1-C1)# police committed-rate 9600 commit-action
transmit committed-burst 1500 exceed-action drop

```

```

ALU(config-qos-P1-C1)# no police

```

TO CONFIGURE THE TYPE OF CLASS FOR A TRAFFIC CLASS

TO CONFIGURE TRAFFIC CLASS AS A PRIORITY CLASS

Command (in Class Mode)	Description
<code>priority</code>	This command configures the traffic class as a priority class.
<code>no priority</code>	This command removes the priority attribute of the traffic-class.

EXAMPLE

```
ALU(config-qos-P1-C1)# priority
```

TO CONFIGURE TRAFFIC CLASS AS A NETWORK-CONTROL CLASS

Sets the class priority to network control.

Command (in Class Mode)	Description
<code>network-control</code>	This command configures the traffic class as a network control class.
<code>no network-control</code>	This command removes the network-control attribute of the traffic-class.



- Note:**
- Network-control class will have the highest priority among all the traffic classes.
 - Priority class will have the next priority.
 - Default class has the least priority.

EXAMPLE

```
ALU(config-qos-P1-C1)# network-control
```

```
ALU(config-pmap-P1-C1)# no network-control
```

To SET TRAFFIC SHAPING

The main objective of the traffic shaper is to allow the traffic in to the network at a controlled rate from different sources so that the network resources are optimally utilized for better performance. Typically this is achieved by applying a Token Bucket Filter at the egress of an interface. Tokens will be generated per each flow at a sustained rate (configured as CIR) and are emptied as and when the packets are transmitted.



Note: If shape is configured on a priority class, the system gives a warning message.

Command (in Class Mode)	Description
<code>shape committed-rate <8000-10000000> committed-burst <40-150000></code>	This command sets QoS shaping parameters on the policy map's traffic class.
<code>no shape</code>	This command removes the configured shaping parameters.

EXAMPLE

```
ALU(config-qos-P1-C1)# shape committed-rate 90000
committed-burst 6000
```

```
ALU(config-qos-P1-C1)# no shape
```

To CONFIGURE QUEUE-LIMIT

Command (in Class Mode)	Description
<code>queue-limit <10-3500></code>	This command sets a queue-limit for the scheduler for the traffic class.
<code>no queue-limit</code>	This command deletes the configured queue-limit. By default, a traffic class will have a queue limit of 150.

EXAMPLE

```
ALU(config-qos-P1-C1)# queue-limit 155
```

```
ALU(config-qos-P1-C1)# no queue-limit
```

To CONFIGURE RANDOM DETECT

- RED (Random Early Detection)


RED is designed for a network where a single marked or dropped packet is sufficient to signal the presence of congestion to the transport layer protocol. It aims to control the average queue size by indicating to the end hosts when they should temporarily slow down transmission of packets. RED congestion control mechanisms monitor the average queue size for each output queue and using randomization, choose connections to notify of that connection.


RED actually takes advantage of the congestion control mechanism of TCP, packets are randomly dropped prior to periods of congestion. This causes RED to inform the packet source to decrease its transmission rate.

- WRED (Weighted Random Early Detection)

WRED combines the capabilities of the RED algorithm with the IP precedence feature to provide preferential traffic handling of higher priority packets. It can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service.

WRED can also be configured to ignore the IP precedence when making drop decisions so that non weighted RED behavior is achieved. WRED can provide separate thresholds and weights for different IP precedences, which can provide different quality of service with regard to packet dropping for different packet types.

Command (in Class Mode)	Description
<code>random-detect</code>	This command enables RED.
<code>random-detect ip-dscp</code>	This command enables ip-dscp based WRED, with the default values.
<code>random-detect ip-precedence</code>	This command enables ip-precedence based WRED, with the default values.
<code>random-detect ip-dscp <0-63> min-thresh <50-750> max-thresh <150-950></code>	Use this command to change the default ip-dscp based WRED values. This command populates the WRED values but does not enable the features. To enable this, use 'random-detect ip-dscp' command.  <p>Note: The queue limit of the traffic class should be greater than the max thresh value.</p>

Command (in Class Mode)	Description
<pre>random-detect ip-precedence <0-7> min-thresh <50-750> max-thresh <150-950></pre>	<p>Use this command to change the default ip-precedence based WRED values. This command populates the WRED values but does not enable the feature. To enable this, use 'random-detect ip-precedence' command.</p>  <p>Note: The queue limit of the traffic class should be greater than the max thresh value.</p>
<pre>no random-detect [ip-dscp ip-dscp-values ip-precedence ip-precedence-values values]</pre>	<p>This command resets/disables the random-detect on ip-dscp and ip-precedence. The command also deletes all ip-dscp, ip-precedence configuration, or all random-detect configuration.</p>

Refer '**Appendix - QoS Values and Mnemonics**' for IP-precedence and IP-dscp default values.

EXAMPLE

```
ALU(config-qos-P1-C1)#random-detect ip-precedence
ALU(config-qos-P1-C1)# random-detect ip-dscp 5 min-thresh 60
max-thresh max-thresh 600
```

```
ALU(config-qos-P1-C1)# no random-detect
ALU(config-qos-P1-C1)# no random-detect ip-precedence
ALU(config-qos-P1-C1)# no random-detect values
```

To SET MARKING

Sets the IP Precedence/IP DSCP/ToS flags on the matched packet.

Command (in Class Mode)	Description
set { ecn-ce ip-dscp {<0-63>/<dscp-mnemonics>} ip-precedence {<0-7>/<precedence-mnemonics>} tos {<0-15>/<tos-mnemonics>}}	This command sets the IP packet marking and the value to mark.
no set { ecn-ce ip-dscp ip-precedence / tos }	This command removes the packet marking configuration.

Refer 'Appendix - QoS Values and Mnemonics' for IP-DSCP, IP-Precedence, and ToS mnemonics.

EXAMPLE

```
ALU(config-qos-P1-C1)# set ip dscp af11
```

```
ALU(config-pmap-c)# no set ip dscp
Deleted ip-dscp marking.
```

To CONFIGURE BANDWIDTH FOR A TRAFFIC CLASS

This command provides a mechanism for bandwidth sharing of the link.

Command (in Class Mode)	Description
bandwidth {<101-700000000> percent <1-100>}	This command is used to configure the bandwidth for a traffic class. 0-750000000 - the absolute bandwidth (bps) value. 1-100 - bandwidth in percentage.
no bandwidth	This command removes the bandwidth configuration.



Note: You cannot mix the absolute bandwidth command with percentage bandwidth command across sibling classes.

EXAMPLE

```
ALU(config-pmap-P1-C1)# bandwidth 101
```

```
ALU(config-pmap-P1-C1)# no bandwidth
```

To CONFIGURE BANDWIDTH FOR A PRIORITY CLASS

This command provides a mechanism for bandwidth sharing of the link.

Command (in Class Mode)	Description
<code>priority bandwidth {<101-700000000> percent <1-100>}</code>	This command is used to set the traffic class as a priority class and configure bandwidth for the same. 0-750000000 - the absolute bandwidth (bps) value. 1-100 - bandwidth in percentage.
<code>no priority</code>	This command removes the priority attribute of the traffic-class and the configured bandwidth.



Note: You cannot mix the absolute bandwidth command with percentage bandwidth command across sibling classes.

EXAMPLE

```
ALU(config-pmap-P1-C1)# priority bandwidth 101
```

```
ALU(config-pmap-P1-C1)# no priority
```

AUTO QoS CONFIGURATION

AutoQoS is a feature that enables user to configure QoS on the OA-700 with minimal effort. Normally, QoS configuration involve definition of class, match list association with the class, definition of policy, class association with the policy and defining class traffic attributes like bandwidth, police, shape, etc. This entire configuration might be cumbersome for user to configure.

Auto QoS commands creates QoS configuration - automatically classifies traffic, applies the required traffic attributes for each of the classes based on the class needs. Auto QoS configuration also automatically applies the policy on to the interface. These configurations are not editable.



Note: Auto QoS commands are available only in the Interface Configuration mode.

VoIP AUTO QoS CONFIGURATION

Auto QoS VoIP create policies and classes as required by VoIP application.

VoIP Auto QoS is typically configured on the Serial Interface (that has HDLC and PPP encapsulation). This is to achieve low-latency on the serial interfaces or Point to Point link.



Note: Auto VoIP configurations are applied only in the egress direction of the interface as queuing is involved.

TO CONFIGURE AUTO QoS VoIP

Command (in ICM)	Description
<code>auto qos voip</code>	This command enables Auto QoS VoIP on an interface.
<code>no auto qos voip</code>	This command disables Auto QoS VoIP on an interface.

EXAMPLE

```
ALU(config-if Serial0/1:3)# auto qos voip
```

```
ALU(config-if Serial0/1:3)# no auto qos
```

AUTO QoS DIFF-SERV CONFIGURATION

Auto QoS Diff-serv create policies and classes as required by standard Diff-serv application.



Note: Auto Diff-serv is applied only in the egress direction of an interface as RED and marking of outgoing packets are involved.

TO CONFIGURE AUTO QoS DIFF-SERV

Command (in ICM)	Description
<code>auto qos diff-serv</code>	This command enables Auto QoS Diff-Serv on an interface (assured forwarding and expedited forwarding).
<code>no auto qos diff-serv</code>	This command disables Auto QoS Diff-Serv on an interface.

EXAMPLE

```
ALU(config-if Serial0/1:3)# auto qos diff-serv
```

```
ALU(config-if Serial0/1:3)# no auto qos diff-serv
```

AUTO QoS TEMPLATE

Auto-QoS template command creates a set of match-lists, traffic classes and a policy map automatically. You can **edit** or **modify** these match lists and class - maps.

The policy is not applied on to the interface automatically - you have to explicitly apply this template on an interface.

TO CONFIGURE AUTO QoS TEMPLATE

Command (in CM)	Description
<code>auto qos template {diff-serv voip} <policy-map name></code>	This command creates an Auto QoS VoIP/Diff-serv template policy. This policy is to be attached to an interface using the ' service policy command '. See " To Attach a Policy Map to an Interface ".
<code>no auto qos template {diff-serv voip} <policy-map name></code>	This command removes the specified Auto QoS template.

EXAMPLE

```
ALU(config)# auto qos template voip p1
```

```
ALU(config)# no auto qos template voip p1
Auto-QoS template removed
```


HIERARCHICAL POLICY CONFIGURATION

In order to achieve Hierarchical classification and link sharing, user can configure the hierarchical policy.

Hierarchical policy is configured by attaching a policy map (child policy) on to a traffic class of the parent policy.



Note: We support four levels of hierarchy of the policy.

Command (in Class Mode)	Description
service-policy <child policy-map name>	This command sets a policy-map as a child policy.  Note: Direction parameter is not required here.
no service-policy <child policy-map name>	This command deletes a policy-map as the child policy.

EXAMPLE 1

Create policies p1 and p2 and configure traffic class c1 and c2 in each of the policy.

```
ALU(conifg)# policy-map p1
ALU(config-qos-p1)# class c1
ALU(config-qos-p1-c1)#
```

```
ALU(conifg)# policy-map p2
ALU(config-qos-p1)# class c2
ALU(config-qos-p1-c2)#
```

Now, policy p2 can be included in the policy p1 using the '**service-policy**' command.

```
ALU(conifg)# policy-map p1
ALU(config-qos-p1)# class c1
ALU(config-qos-p1-c1)# service-policy p2
```

EXAMPLE 2

Peer classes refers to the traffic classes in a policy map at same level. If a parent is not having the bandwidth, its child may have the bandwidth configured.

```
ALU(config)# policy-map p1
ALU(config-qos-p1)# class c1
ALU(config-qos-p1-c1)# service-policy p2

ALU(config)# policy-map p2
ALU(config-qos-p2)# class c2
ALU(config-qos-p2-c2)# bandwidth percent 10
```

In the above example, policy p1 is having child policy p2 inside the class c1. Traffic class c1 is not having bandwidth configured, but the child class is having the bandwidth configured. In this particular case (only one Traffic) whole bandwidth is available for the traffic c1.

EXAMPLE 3

When a parent policy is having more than one traffic class and some of the class is having the bandwidth configured.

Consider a policy p1 with two classes c12 and c13 with bandwidth 30 and 70 respectively, and policy p2 included in p1 under class c12:

```
ALU(config)# policy-map p1
ALU(config-qos-p1)# class c12
ALU(config-qos-p1-c12)# service-policy p2
ALU(config-qos-p1-c12)# bandwidth percent 30

ALU(config)# policy-map p1
ALU(config-qos-p1)# class c13
ALU(config-qos-p1-c13)# bandwidth percent 70
```

Consider the policy p2 with class c2 having bandwidth 10.

```
ALU(config)# policy-map p2
ALU(config-qos-p2)# class c2
ALU(config-qos-p2-c2)# bandwidth percent 10
```

In this case, the class c2 will get 10% of the zero (class c11 share is 0). It is the time of the congestion but if the bandwidth is unused by the other classes, then c2 can have some bandwidth (10% of available bandwidth).

BANDWIDTH

You cannot mix the absolute bandwidth command with percentage bandwidth command across the siblings at a same hierarchical level.

SHAPE

This command is available for the leaf class. User cannot shape the class_full_class (non leaf class). Leaf class can have both bandwidth and shape commands.

PRIORITY

You can put a class as a priority if its parent is a priority class, else you cannot make this class as priority. At a level, only one class can be a priority class.

RANDOM DETECT

If ancestor/parent of a class is not RED/WRED, then you can make it RED/WRED enable. If a class is RED/WRED enabled, then you cannot enable the RED/WRED for its children as the children inherit the property (RED/WRED) from its parent.

Example 1

Consider a policy p1 with class c1 and random detect enabled. And, policy p2 (without random detect) included in p1:

```
ALU(config)# policy-map p1
ALU(config-qos-p1)# class c1
ALU(config-qos-p1-c1)# random detect

ALU(config)# policy-map p2
ALU(config-qos-p2)# class c2
ALU(config-qos-p2-c2)#

ALU(config-qos-p1-c1)# service-policy p2
```

In the above example, class c2 is child of the class c1. c1 is random-detect enable, it implies that c2 is also random-detect enable.

Example 2

Consider another case with policy p1 with class c1 without random detect. And, policy p2 with class c2 and random detect enabled included in p1:

```

ALU(config)# policy-map p1
ALU(config-qos-p1)# class c1
ALU(config-qos-p1-c1)#

ALU(config)# policy-map p2
ALU(config-qos-p2)# class c2
ALU(config-qos-p2-c2)# random detect

ALU(config-qos-p1-c1)# service-policy p2

```

In the above example, class c2 is random-detect enable but c1 is not.

SET (MARKING)

The concept of the RED/WRED is applied here also.

If marking is not configured at the parent level of a class, then you can configure the marking for that class. If a marking is configured for a class, then you cannot configure the marking for its children.

QUEUE LIMIT

Queue limit can be configured at every level. But if the parent class is having queue limit, then all its children will have the same queue limit. You cannot configure the queue limit for its child classes.

Example 1

Consider a policy p1 with class c1 and queue limit 150 enabled. And, policy p2 (without queue limit) included in p1:

```

ALU(config)# policy-map p1
ALU(config-qos-p1)# class c1
ALU(config-qos-p1-c1)# queue-limit 150

ALU(config)# policy-map p2
ALU(config-qos-p2)# class c2
ALU(config-qos-p2-c2)#

ALU(config-qos-p1-c1)# service-policy p2

```

In the above example, class c2 will also have queue limit 150, which is inherited from its parent class.

Example 2

Consider another case with policy p1 with class c1 without queue limit. And, policy p2 with classes c21 and c22 with queue limit 150 and 250 respectively included in p1:

```
ALU(config)# policy-map p1
ALU(config-qos-p1)# class c1
ALU(config-qos-p1-c1)#
```

```
ALU(config)# policy-map p2
ALU(config-qos-p2)# class c21
ALU(config-qos-p2-c21)# queue-limit 150
ALU(config-qos-p2)# class c22
ALU(config-qos-p2-c22)# queue-limit 250
```

```
ALU(config-qos-p1-c1)# service-policy p2
```

In the above example, parent class c1 does not have any queue limit but its child classes (c21, c22) are having the queue limits 150 and 250 respectively.

The queue limit of the parent is calculated by this following formula.

Parent's class queue-limit = (Sum of queue-limit)/ No of children)

Queue limit for class c11 = (150+ 250)/2

Queue limit for class c11 = 200

You are not allowed to configure the queue limit of a parent class if one of its child is having the queue limit configured.

QoS OVER TUNNEL INTERFACE

QoS can be provided over tunnel (IPsec/GRE) interfaces.

Tunnel command is available in the policy map mode. When you attach a policy to the tunnel interface, you have to explicitly attach a policy (root – policy) to the physical interface to which the tunnel is associated. You can then use the tunnel command to attach the tunnel-policy.

Tunnel command automatically creates a class map in the root policy and will apply the policy that is applied over the tunnel interface.

Notes:

1. You are not allowed to use the tunnel command in a policy map that is attached to some tunnel interface.
 2. The service-policy command is not allowed in the tunnel mode (policy-map tunnel).
 3. The maximum level of the policy is three. When an interface is having the tunnel over it, then it may have four level of policy. But you are not allowed to configure more than three level.
 4. Qos-pre-classify command is used in the interface mode to store the classification index.
-

Command (in Policy-map Mode)	Description
tunnel < tunnel-interface-name >	This command is used to configure QoS over a tunnel interface.

Tunnel command is just like a class command in a policy map. The only difference is that service-policy command is not allowed in this mode. The commands like bandwidth, priority, shape, random-detect is allowed in this mode.

EXAMPLE

```
ALU(config-pmap)# tunnel tunnel1
```

TO CONFIGURE BANDWIDTH FOR THE TUNNEL INTERFACE

Command (in Policy-map Mode)	Description
tunnel < tunnel-interface-name > bandwidth percent < 1-100 >	This command is used to configure bandwidth for the tunnel interface.
no tunnel < tunnel-interface-name > bandwidth	This command removes the bandwidth configured for the tunnel interface.

EXAMPLE

```
ALU(config-pmap)# tunnel tunnel1 bandwidth percent 10
```

```
ALU(config-pmap)# no tunnel tunnel1 bandwidth
```

QoS SHOW COMMANDS

The QoS show command displays the following details:

1. Number of packets dropped from a queue.
2. Number of packets transmitted through a queue.
3. Number of packets currently in the queue (queue length).
4. Total amount of bytes transmitted from a queue.

TO VIEW THE CLASS-MAP CONFIGURATION

Command (in SUM/CM)	Description
show class-map [<i><name></i>]	This command shows all or specified class map along with its match-lists.

EXAMPLE

```
ALU# show class-map cmap1
```

```
class-map c1 match-any
1 match any m1 m2
2 match any m2 m4 m5
```

TO VIEW THE POLICY MAP CONFIGURATION

Command (in SUM/CM)	Description
show policy-map [<i><name></i>]	This command shows the details of all or specified policy map configured in the system.

EXAMPLE

```
ALU# show policy-map P1
```

```
policy-map p1
interface serial0/0:0 EGRESS
 10 class cm_ef
  random-detect ip-dscp
 20 class cm_af11
65535 class class-default
```

TO VIEW THE RANDOM DETECT DEFAULT PARAMETERS

Command (in SUM/CM)	Description
<code>show random-detect-defaults {ip-dscp ip-precedence}</code>	This command displays Random Detect default parameters.

EXAMPLE

```
ALU(config)# show random-detect-defaults ip-dscp
```

```
ip-dscp  Min-Thresh  Max-Thresh  Drop-Probability
be        50           150         10
af11     100           150         10
af12     75           150         10
af13     50           150         10
af21     100           150         10
af22     75           150         10
af23     50           150         10
af31     100           150         10
af32     75           150         10
af33     50           150         10
af41     100           150         10
af42     75           150         10
af43     50           150         10
ef       125           150         10
```

```
ALU(config)# show random-detect-defaults ip-precedence
```

```
ip-precedence  Min-Thresh  Max-Thresh  Drop-Probability
0              50          150         10
1              60          160         10
2              70          170         10
3              80          180         10
4              90          190         10
5             100          200         10
6             110          210         10
7             120          220         10
```

TO VIEW SERVICE-POLICY STATISTICS

Command (in SUM/CM)	Description
show service-policy [{<policy-map name> in/out}]	This command displays the statistics for Policing/Shaping, being used in a policy.

EXAMPLE

```
ALU(config-qos-p2-cm_ef)# show service-policy p2 out
```

```
interface Serial0/0:0
service-policy out p2
  Class class-default
    0 packets total,           0 bytes total,
    0 packets transmitted,    0 bytes transmitted,
    0 packets dropped,        0 bytes dropped,
  Class cm_ef match-any
  match any ml_ef
    0 packets total,           0 bytes total,
    0 packets transmitted,    0 bytes transmitted,
    0 packets dropped,        0 bytes dropped,
  RED:
  Class Random drops Tail drops Min.Th. Max.Th. Mark Prob.
  be      0             0           50     150     1/10
  af11    0             0          100     150     1/10
  af12    0             0           75     150     1/10
  af13    0             0           50     150     1/10
  af21    0             0          100     150     1/10
  af22    0             0           75     150     1/10
  af23    0             0           50     150     1/10
  af31    0             0          100     150     1/10
  af32    0             0           75     150     1/10
  af33    0             0           50     150     1/10
  af41    0             0          100     150     1/10
  af42    0             0           75     150     1/10
  af43    0             0           50     150     1/10
  ef      0             0          125     150     1/10
  Class cm_af11 match-any
  match any ml_af11
    0 packets total,           0 bytes total,
    0 packets transmitted,    0 bytes transmitted,
    0 packets dropped,        0 bytes dropped,
  Class L2-network-control
    0 packets total,           0 bytes total,
    0 packets transmitted,    0 bytes transmitted,
    0 packets dropped,        0 bytes dropped,
```

To VIEW THE INTERFACE QUEUEING STATISTICS

Command (in SUM/CM)	Description
show queuing interface [<interface-name>]	This command shows all the interfaces to which the QoS service policy is attached and the name/direction of the policy.

EXAMPLE

ALU(config)# show queuing interface GigabitEthernet 7/0

```
interface GigabitEthernet7/0
  service-policy in p1
    description p1 is the name of the policy map
    class c1
      priority
      shape committed-rate 90000 committed-burst 6000
    police committed-rate 9600 commit-action drop committed-burst 1500 exceed-a
      queue-limit 155
      random-detect ip-dscp 0 min-thresh 50 max-thresh 150
```

To VIEW THE QUEUEING STATISTICS

Command (in SUM/CM)	Description
show queuing statistics [{in/out} <interface-name> {in out}]	This command shows the statistics of all or specified interfaces and traffic classes in both in and out, or for the specified direction.

EXAMPLE

ALU(config)# show queuing statistics

```
interface GigabitEthernet7/0
  service-policy in p1
    class class-default
      Packets dropped 0
      Packets dequeued 0
      Bytes dequeued 0
    class c1
      Packets dropped 0
      Packets dequeued 0
      Bytes dequeued 0
interface GigabitEthernet7/1
  service-policy out p1
    class class-default
      Packets dropped 0
      Packets dequeued 0
      Bytes dequeued 0
      Queue length (Packets) 0
```

Alcatel-Lucent

```
class network-control
  Packets dropped 0
  Packets dequeued 0
  Bytes dequeued 0
  Queue length (Packets) 0
class c1
  Packets dropped 0
  Packets dequeued 0
  Bytes dequeued 0
  Queue length (Packets) 0
```


To VIEW QoS CONFIGURATION

This command shows all class-maps, policy-maps and interfaces to which a policy is attached (if any).

Command (in SUM/CM)	Description
<code>show qos config</code>	This command shows the configuration related to QoS.

EXAMPLE

ALU# show qos config

```

class-map c1 match-any
  1 match any m1 m2
class-map c2 match-any
  1 match any m1
class-map 3 match-any
class-map c5 match-any
  3 match any m1

policy-map p1
  description p1 is the name of the policy map
  class c1
    priority
    shape committed-rate 90000 committed-burst 6000
    police committed-rate 9600 commit-action drop committed-burst 1500
  exceed-action drop excess-burst 2000 violate-action transmit
    queue-limit 155
    random-detect ip-dscp 0 min-thresh 50 max-thresh 150
policy-map p2
  class c2
    police committed-rate 1000000 commit-action transmit committed-
burst 1600 exceed-action drop excess-burst 2600 violate-action drop
interface GigabitEthernet7/0
  service-policy in p1
interface GigabitEthernet7/1
  service-policy out p1

```

To VIEW QoS RUNNING CONFIGURATION

This command shows the configurations related to QoS if only attached to interface(s). In particular, this command shows the following:

- Policy-maps attached to interface(s).
- Class-maps attached to the above list of policy-maps.
- Match-lists attached to the above list of class-maps.
- All the interfaces where the QoS policy has been attached.

The order of display of running configuration is as follows:

- Match-lists
- Class-maps
- Policy-maps
- Interfaces where the QoS policy has been attached.

Command (in SUM/CM)	Description
<code>show qos running-config</code>	This command shows the configurations related to QoS if only attached to interface(s).

EXAMPLE

```
ALU# show qos running-config
```

```
!Qos Configurations
!
! Use "show match-list [NAME]" to expand the match-lists
match-list m1
match-list m2

class-map c1 match-any
1 match any m1 m2

policy-map p1
  description p1 is the name of the policy map
  class c1
    priority
    shape committed-rate 90000 committed-burst 6000
    police committed-rate 9600 commit-action drop committed-burst 1500
  exceed-action drop excess-burst 2000 violate-action transmit
  queue-limit 155
  random-detect ip-dscp 0 min-thresh 50 max-thresh 150

interface GigabitEthernet7/0
  service-policy in p1
interface GigabitEthernet7/1
  service-policy out p1
!
```

To VIEW AUTO QoS CONFIGURATION

Command (in SUM/CM)	Description
<code>show auto qos {interface <interface-name> [diff-serv voip] diff-serv voip}</code>	<p>This command displays all/any Auto QoS configuration.</p> <p>You can also view the Auto QoS configuration for a specific interface.</p> <p>The output of this command is a list of all the Auto QoS policies, and traffic classes.</p>

EXAMPLE

ALU(config)# show auto qos diff-serv

```

auto qos diff-serv
  class autoqos-class-af1
    match ip any any dscp af11
    match ip any any dscp af12
    match ip any any dscp af13
    bandwidth percent 20
    queue-limit 350
    random detect ip-dscp af11 min-threshold 200 max-threshold 300
    random detect ip-dscp af12 min-threshold 150 max-threshold 300
    random detect ip-dscp af13 min-threshold 100 max-threshold 300
    random-detect ip-dscp
  class autoqos-class-af2
    match ip any any dscp af21
    match ip any any dscp af22
    match ip any any dscp af23
    bandwidth percent 20
    queue-limit 350
    random detect ip-dscp af21 min-threshold 200 max-threshold 300
    random detect ip-dscp af22 min-threshold 150 max-threshold 300
    random detect ip-dscp af23 min-threshold 100 max-threshold 300
    random-detect ip-dscp
  class autoqos-class-af3
    match ip any any dscp af31
    match ip any any dscp af32
    match ip any any dscp af33
    bandwidth percent 20
    queue-limit 350
    random detect ip-dscp af31 min-threshold 200 max-threshold 300
    random detect ip-dscp af32 min-threshold 150 max-threshold 300
    random detect ip-dscp af33 min-threshold 100 max-threshold 300
    random-detect ip-dscp
  class autoqos-class-af4
    match ip any any dscp af41
    match ip any any dscp af42
    match ip any any dscp af43
    bandwidth percent 20
    queue-limit 350
    random detect ip-dscp af41 min-threshold 200 max-threshold 300
    random detect ip-dscp af42 min-threshold 150 max-threshold 300
    random detect ip-dscp af43 min-threshold 100 max-threshold 300
    random-detect ip-dscp

```

```
class autoqos-class-ef
  match ip any any dscp ef
  priority
  police committed-rate 350000 committed-burst 30000
exceed-action drop violate-action drop
class class-default
  fair-queue
```

ALU(config)# show auto qos voip

```
auto qos voip
class autoqos-voip-control-class
  match any
    tcp any any service range 1719 1720
    tcp any any service range 2427 2428
    tcp any any service rtsp
    udp any any service range 2000 2002
    udp any any service 5060
  bandwidth percent 10
  set ip-dscp af31
class autoqos-voip-data-class
  match any
    udp any any type rtp
    udp any any type rtcp
  priority
  bandwidth percent 70
  set ip-dscp ef
class-default
fair-queue
  set ip-dscp default
```

QoS CLEAR COMMANDS

TO CLEAR QUEUING STATISTICS

Command (in SUM/CM)	Description
<code>clear queuing statistics</code> [{<interface-name> {in/out} in out}]	This command clears the QoS statistics on that particular interface.

EXAMPLE

```
ALU# clear queuing statistics
```

```
Success : Cleared ingress stats for interface GigabitEthernet 7/0.  
Success : Cleared egress stats for interface GigabitEthernet 7/0.
```

QoS TEST SCENARIOS ON OA-780

TRAFFIC SHAPING

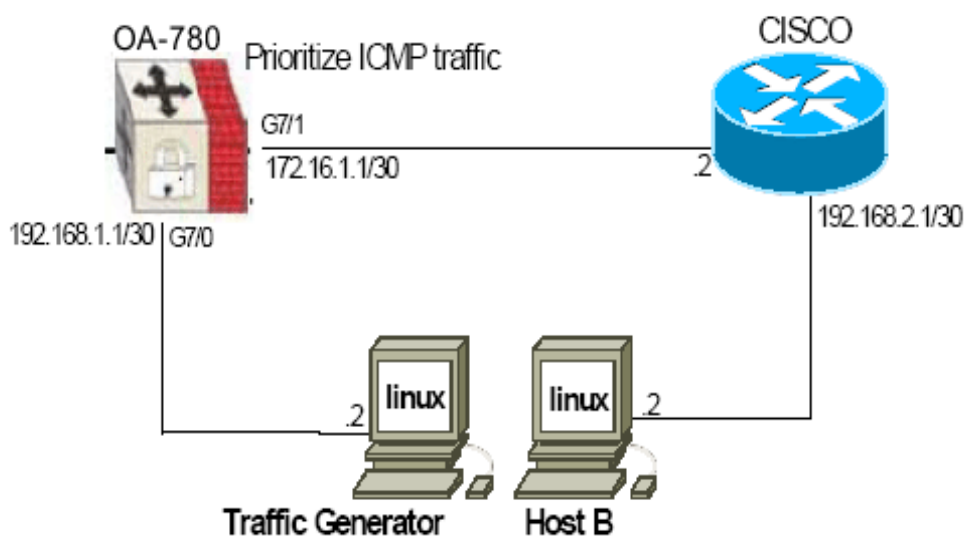


Figure 79: QoS Traffic Shaping Using OA-780

From the Traffic Generator, send Internet mix (IMIX) traffic of varying packet sizes: 64 bytes, 256 bytes, 512 bytes, 1024 bytes, 1518 bytes at 10 Mbps in the direction of the OA-780. On OA-780, configure QoS policy to shape the traffic to 5 Mbps using shape command on interesting traffic.

1. DEFINE CLASS-MAPS TO MATCH EGRESS TRAFFIC

```
ALU(config)#match-list allow-traffic
ALU(config-match-list-allow-traffic)#ip host 192.168.1.2 host
192.168.2.2
```

```
ALU(config)#class-map class1
ALU(config-cmap)#match any allow-traffic
ALU(config-cmap)#exit
```

2. DEFINE POLICY-MAP WITH CLASS-NAMES

```
ALU(config)#policy-map flow-policy
ALU(config-qos-flow-policy)#class class1
ALU(config-qos-flow-policy-class1)#shape committed-rate 5000000
committed-burst 1600
ALU(config-qos-flow-policy-class1)#exit
```

3. ATTACH POLICY TO OUTGOING INTERFACE

```
ALU(config)#interface GigabitEthernet 7/1
ALU(config-if GigabitEthernet7/1)# service-policy out flow-
policy
```

We can verify from IPTraf, that traffic has been rate-limited to 5Mbps after applying QoS.

PRIORITY QUEUING

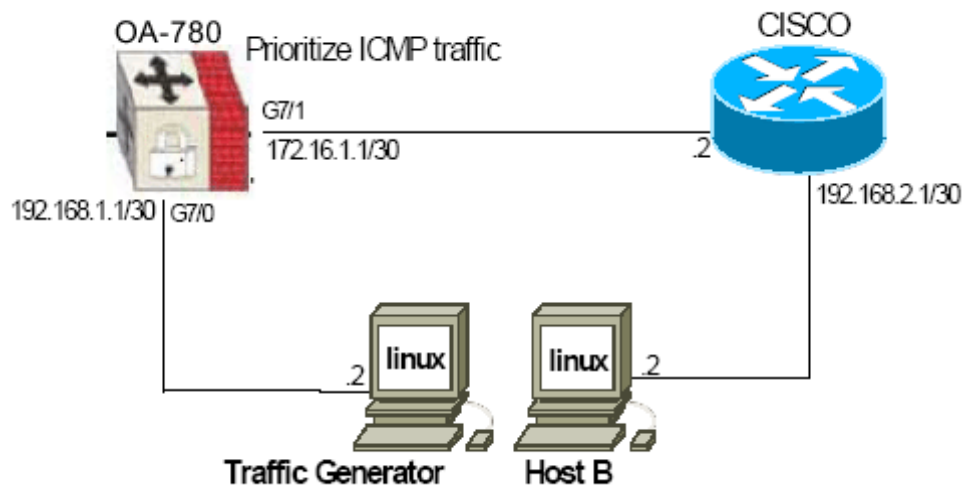


Figure 80: QoS Priority Queuing Using OA-780

Send continuous ping from Traffic Generator to Host B. On the OA-780, configure QoS policy to prioritize traffic (ICMP - as given in the above example). Generate additional traffic (IP) on the Traffic Generator. Increase the rate of this secondary (IP) traffic to exceed line (10 Mbps) capacity. Since ICMP is given higher precedence (by virtue of its high priority), ping will still go through even though IP traffic is dropped.

1. DEFINE CLASS-MAPS TO MATCH ICMP EGRESS TRAFFIC

```
ALU(config)#match-list icmp-traffic
ALU(config-match-list-icmp-traffic)#icmp any any

ALU(config)#class-map priority-traffic
ALU(config-class-map priority-traffic)#match any icmp-traffic
ALU(config-class-map priority-traffic)#exit
```

2. ADD CLASS-MAP TO POLICY-MAP

```
ALU(config)#policy-map flow-policy
ALU(config-qos-flow-policy)#class priority-traffic
ALU(config-qos-flow-policy-priority-traffic)#priority
ALU(config-qos-flow-policy-priority-traffic)#exit
```

3. VERIFYING QoS PRIORITY

1. Without configuring QoS on OA-780, send both ping and IP traffic exceeding egress line capacity. Since all egress traffic are given same treatment by OA-780, ping gets dropped randomly along with IP traffic.
2. By configuring Priority on OA-780, we can verify that IP traffic gets dropped without compromising ICMP.

CHAPTER 31 INTRUSION DETECTION SYSTEM

This chapter documents the Command Line Interface (CLI) commands for configuring IDS (Intrusion Detection System) on an interface.

For instructions on using the commands and to get a detailed description on each of their parameters, refer to the “IDS” chapter in the ***OmniAccess 700 CLI Command Reference Guide***.

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU (config)#
SUM	Super User Mode - ALU#
FwCM	Firewall Configuration Mode - ALU (config-firewall)#
F-PCM	Firewall-Policy Sub Configuration Mode - ALU (config-firewall-policy name)#
ICM	Intrusion Configuration Mode - ALU (config-firewall-intrusion)#

IDS OVERVIEW

Intrusion Detection System (IDS) is a network security system designed to identify intrusive or malicious behavior via monitoring of network activity. The IDS identifies suspicious patterns that may indicate an attempt to attack, break in, or otherwise compromise a system. IDS can be network-based or host-based, passive or reactive, and can rely on either misuse detection or anomaly detection.

ALCATEL-LUCENT SPECIFIC OVERVIEW

The OA-700 supports Snort engine for IDS functionality.

IDS CONFIGURATION

Refer to the following sections to configure IDS:

- [“IDS Configuration Steps”](#)
- [“IDS Configuration Flow”](#)
- [“IDS Configuration Commands”](#)
- [“IDS Configuration Scenario Using OA-700”](#)

IDS CONFIGURATION STEPS

This section lists the step-by-step instructions to be followed while configuring IDS.

Step 1: Configure rule using match-list for any packet that matches classification. (Refer to the chapter on [“Common Classifiers”](#) in this document.)

Step 2: Enter Firewall Configuration Mode.

```
ALU(config)# firewall
ALU(config-firewall)#
```

Step 3: Configure intrusion sensor. See [“To Configure an IDS Sensor”](#)

Step 4: Optional configuration commands.

- Update Snort Rule. See [“To Update Snort Rule”](#)
- Rollback Snort Rule Database. See [“To Rollback Snort Rule Database”](#)
- Manually Rebuild Signature Database. See [“To Manually Rebuild Signature Database”](#)
- Modifying Snort Rule for detecting intrusion. See [“To Modify Group Level Detection”](#)
- Enable/Disable Snort Rule. See [“To Enable/Disable Snort Rule”](#)
- Modify Snort Rule. See [“To Modify Snort Rule”](#)
- Prevent Snort Rule Modification. See [“To Modify Group Level Prevention”](#)

Step 5: Configure Firewall Policy.

```
ALU(config)# policy <name>
ALU(config-firewall-policy<name>)#
```

Example:

```
ALU(config-firewall)# policy P1
ALU(config-firewall-policy-P1)#
```

(For a detailed information on firewall, refer [“Filter and Firewall”](#) chapter.)

Step 6: Attach the configured intrusion sensors to the firewall policy. See [“To Create a Intrusion Rule Inside a Firewall Policy”](#)

Step 7: Enter the Interface Configuration Mode

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 8: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 9: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 10: Attach the configured firewall policy to appropriate interfaces in the ingress direction of the interface. See [“To Attach a Firewall Policy to an Interface”](#)

Step 11: View the intrusion sensor configuration using show commands. See [“Show Commands”](#)

IDS CONFIGURATION FLOW

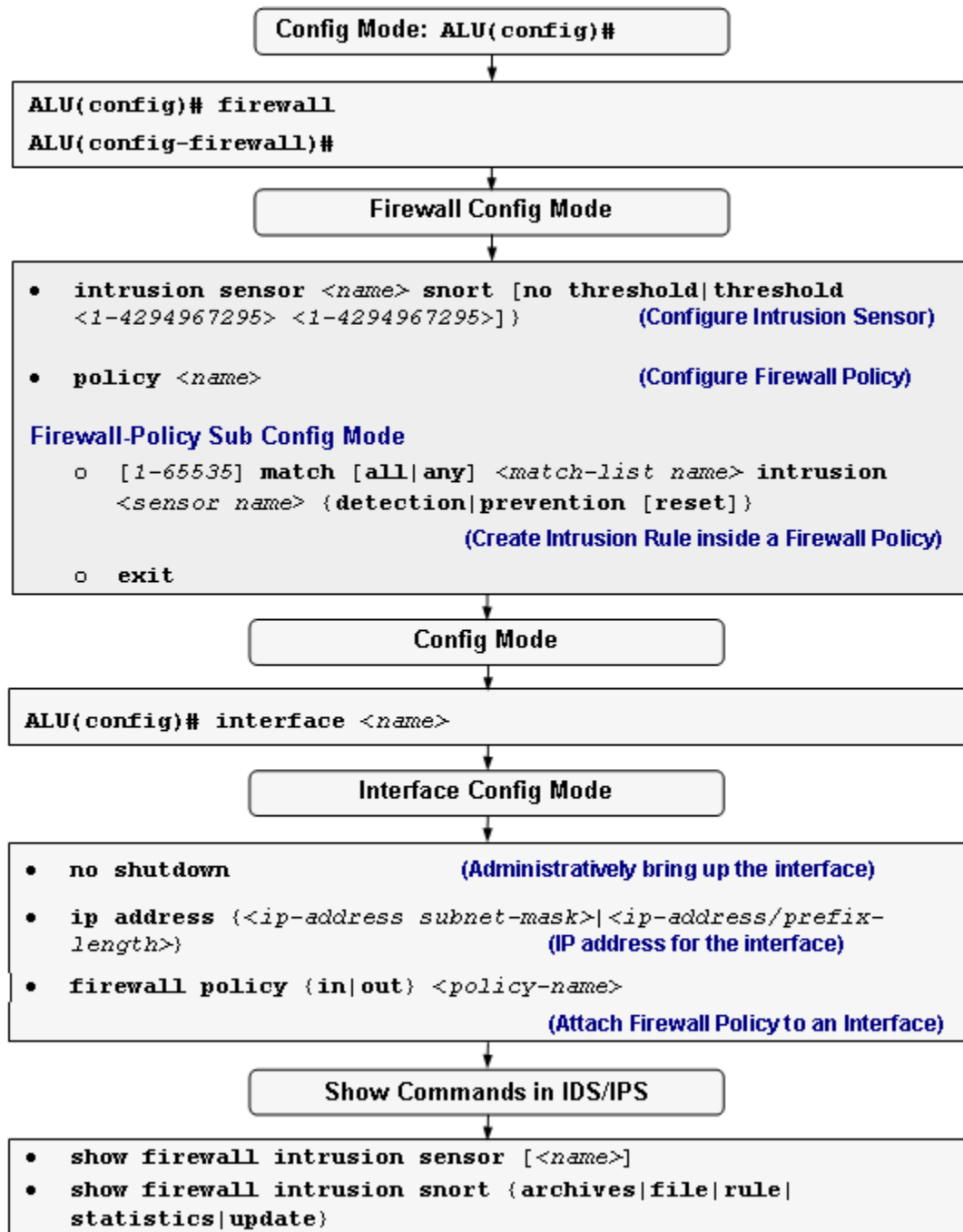


Figure 81: IDS Configuration Flow


IDS CONFIGURATION COMMANDS

The following commands are used to configure IDS on the OA-700.

To CONFIGURE AN IDS SENSOR



Note: The OA-700 supports Snort based sensors.

Command (in FwCM)	Description
<pre>intrusion sensor <name> snort [no threshold threshold <1-4294967295> <1-4294967295>]}</pre>	<p>Use this command to create an intrusion sensor based on snort. Enter this command in the Firewall configuration mode.</p> <p>Use the 'threshold' keyword to configure the threshold for the sensor.</p> <p>Use the 'no threshold' keyword to remove threshold configured for the sensor.</p>
<pre>no intrusion sensor <name> snort</pre>	<p>Use this command to delete an intrusion sensor.</p> <div style="margin-top: 10px;">  <p>Note: You cannot delete the intrusion sensor if it is attached to a firewall policy. Detach the sensor from the firewall policy before deleting it.</p> </div>

EXAMPLE

```
ALU(config)#firewall
ALU(config-firewall)# intrusion sensor sensor1 snort threshold
10 1000
ALU(config-firewall-intrusion-sensor-sensor1)#
```

```
ALU(config-firewall)# intrusion sensor sensor1 snort no
threshold
```

```
ALU(config-firewall)# no intrusion sensor sensor1 snort
```

INTRUSION SENSOR OPTIONAL CONFIGURATION COMMANDS

This section lists the commands for modifying/updating the Snort database to be used by the sensor.

TO ENTER SNORT CONFIGURATION MODE

Command (in FwCM)	Description
<code>intrusion snort</code>	This command enters the snort configuration mode.

EXAMPLE

```
ALU(config)# firewall
ALU(config-firewall)# intrusion snort
ALU(config-firewall-intrusion-snort)#
```

TO UPDATE SNORT RULE

Command (in Intrusion Snort CM)	Description
<code>update</code> { <code>instant</code> <code>scheduled</code> { <code>daily</code> <hh:mm:ss> <code>monthly</code> <1-31> <hh:mm:ss> <code>weekly</code> { <code>Sunday</code> <code>Monday</code> . . }<hh:mm:ss>} <code>delta</code> <1-300>} <code>https</code> <url> { <code>passive</code> <code>rebuild</code> }}	Use this command to update the Snort rule database through the HTTP server. This command gives the option to update the Snort rule immediately or regularly on the scheduled date and time.
<code>no update</code> { <code>passive</code> <code>rebuild</code> }	Use this command to remove the scheduled Snort rule database update.

EXAMPLE

```
ALU(config-firewall-intrusion-snort)# update instant https
https://<uid:pwd>@ids.alu.com/signature.tar.gz rebuild
```

TO ROLLBACK SNORT RULE DATABASE

Command (in Intrusion Snort CM)	Description
<code>rollback</code> <version-number>	Use this command to rollback to different versions of the Snort rule database.

EXAMPLE

```
ALU(config-firewall-intrusion-snort)#rollback 2.3.1
```

TO MANUALLY REBUILD SIGNATURE DATABASE

Command (in Intrusion Snort CM)	Description
<code>rebuild <version-number></code>	Use this command to manually rebuild the signature database.

EXAMPLE

```
ALU(config-firewall-intrusion-snort)# rebuild 2.3.0
```

TO MODIFY GROUP LEVEL DETECTION

Command (in Intrusion Snort CM)	Description
<code>rule detection {{category <name>.. classtype <name>.. priority {high low medium}}}</code>	This command enables you to modify the group level detection.

EXAMPLE

```
ALU(config-farewell-intrusion-snort)# rule detection category
attack-responses
```

TO ENABLE/DISABLE SNORT RULE

Command (in Intrusion Snort CM)	Description
<code>rule enable {{category <name>... classtype <name>... priority {high low medium} sid <1-4294967295...>}}</code>	Use this command to enable Snort rules by Snort Rule ID (SID), class type, priority, or category.
<code>rule disable {{category <name>... classtype <name>... priority {high low medium} sid <1-4294967295...>}}</code>	Use this command to disable Snort rules by Snort rule ID (SID), class type, priority, or category.

EXAMPLE

To enable Snort rule:

```
ALU(config-firewall-intrusion-snort)# rule enable classtype
attempted-dos
```

To disable Snort rule:

```
ALU(config-firewall-intrusion-snort)# rule disable classtype
attempted-dos
```


To MODIFY SNORT RULE

Command (in Intrusion Snort CM)	Description
<code>rule modify <1-4294967295> content <rule-content></code>	Use this command to modify Snort rule.

EXAMPLE

To modify the rule given below, use the rule modify command:

Original rule:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ATTACK-RESPONSES directory listing"; flow:from_server,established; content:"Volume Serial Number"; classtype:bad-unknown; sid:1292; rev:8;)
```

Modification of rule to \$EXTERNAL_NET is shown below:

```
ALU(config-firewall-intrusion-snort)# rule modify 1292  
content alert tcp $EXTERNAL_NET any -> $EXTERNAL_NET any  
(msg:"ATTACK-RESPONSES directory listing";  
flow:from_server,established; content:"Volume Serial  
Number"; classtype:bad-unknown; sid:1292; rev:8;)
```

To MODIFY GROUP LEVEL PREVENTION

Command (in Intrusion Snort CM)	Description
<code>rule prevention {{{category <name> classtype <name> priority {high low medium} reset {category <name> classtype <name> priority {high low medium}}}}</code>	This command enables you to modify the group level prevention.

EXAMPLE

```
ALU(config-firewall-intrusion-snort)# rule prevention category  
attack-responses
```

TO CREATE A INTRUSION RULE INSIDE A FIREWALL POLICY

Command (in F-PCM)	Description
<pre>[<1-65535>] match [all any] <match-list name> intrusion <sensor name> {detection prevention [reset]}</pre>	<p>Enter this command in the Firewall Policy Configuration mode.</p> <p>This command is used to attach an intrusion sensor to a firewall policy, and create rules (associate match-list and set priority for the rule) for a firewall policy.</p> <p>This command also sets the action - detection or prevention for the configured rule.</p> <p>The range for the rule number is 1-65535. This rule number signifies the priority of a rule. By default, the numbering pattern for rule number is the next multiple of ten to the highest existing rule number.</p> <p>The keyword “detection” detects the intrusion, and “prevention” detects and also prevents the intrusion.</p>



Note: Currently, multiple match-lists cannot be associated to a firewall policy rule. To configure more than one match-list within a firewall policy, add multiple rules with different match-lists.

EXAMPLE

```
ALU(config)#firewall
ALU(config-firewall)#policy policy1
ALU(config-firewall-policy1)#1 match m1 intrusion sensor1
detection
```

To ATTACH A FIREWALL POLICY TO AN INTERFACE

Command (in ICM)	Description
<pre>firewall policy {in out} <policy-name></pre>	<p>This command is used to attach a firewall policy (to which an intrusion sensor is attached) to an interface in 'in' or 'out' direction.</p> <p>Firewall policy is applied to the ingress (incoming) traffic if the "in" keyword is used.</p> <p>Firewall policy is applied to the egress (outgoing) traffic if the "out" keyword is used.</p>



Note: The Firewall policy will take effect once it is attached to an interface.

EXAMPLE

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# firewall policy in P1
```

IDS SHOW COMMANDS

This section lists the show commands in IDS.

To VIEW AN IDS SENSOR DETAILS

Command (in SUM)	Description
<code>show firewall intrusion sensor</code> [<name>]	Use this command to view intrusion sensor configuration details.

EXAMPLE

```
ALU# show firewall intrusion sensor
firewall
  intrusion sensor sensor1 snort
  intrusion sensor sensor4 snort
  intrusion sensor s1 snort
exit
```

To VIEW ARCHIVES

Command (in SUM)	Description
<code>show firewall intrusion snort</code> <code>archives</code>	Use this command to display snort signature archives.

EXAMPLE

```
ALU#show firewall intrusion snort archives
Version no |   Details   |   Date of Download   |Time of Downl-
2.3.0      |   Current   |         initial      |
```

To VIEW FILE LIST

Command (in SUM)	Description
<code>show firewall intrusion snort file {<filename>/list}</code>	Use this command to display the contents of a specific snort rule file or list all the rule files.

EXAMPLE

```

ALU#show firewall intrusion snort file policy.rules
C) Copyright 2001-2004, Martin Roesch, Brian Caswell, et al.
All rights reserved.
$Id: policy.rules,v 1.1 2005/03/18 11:27:51 ppote Exp $
-----
POLICY RULES
-----

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"POLICY FTP anonymous
login at)

alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"POLICY WinGate
telnet server )

# we have started to see multiple versions of this beyond 003.003, so
we have
# expanded this signature to take that into account.
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"POLICY VNC server
response";)
--More--

```

To VIEW SNORT RULES

Command (in SUM)	Description
<pre>show firewall intrusion snort rule {category <name> classtype <name> disable{category classtype pri ority sid} priority {high low medium} sid <1- 4294967295>...}</pre>	Use this command to display the contents of a specific Snort rule.

EXAMPLE

```
ALU#show firewall intrusion snort rule category dos
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS Jolt
attack"; dsize:408; fragbits:M; reference:cve,1999-0345;
classtype:attempted-dos; sid:268; rev:4;)

alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"DOS Teardrop
attack"; fragbits:M; id:242; reference:bugtraq,124;
reference:cve,1999-0015; reference:nessu)

alert udp any 19 <> any 7 (msg:"DOS UDP echo+chargen bomb";
reference:cve,1999-0103; reference:cve,1999-0635;
classtype:attempted-dos; sid:271; rev:4;)
```

To VIEW DISABLED RULES/GROUPS

Command (in FwCM)	Description
<pre>show firewall intrusion snort rule disable {category classtype priority sid}</pre>	Use this command to display the information of group of rules that are disabled.

EXAMPLE

```
ALU#show firewall intrusion snort rule disable SID
```

To VIEW SNORT STATISTICS

Command (in SUM)	Description
<code>show firewall intrusion snort statistics [<interface name>]</code>	Use this command to display Snort statistics on a specified interface.

EXAMPLE

```
ALU#show firewall intrusion snort statistics
Pkt Received : 20
Pkt Passed : 16
Pkt Dropped : 4
Pkt Queued : 0
Pkt Detected : 0
```

To VIEW SNORT PRE-PROCESSOR STATISTICS

Command (in SUM)	Description
<code>show firewall intrusion snort statistics preprocessor [{back-orifice http-inspect rpc stream4}]</code>	Use this command to display statistics for a specific Snort pre-processor.

EXAMPLE

```
ALU#show firewall intrusion snort statistics preprocessor http-inspect
```

To VIEW SNORT RULE STATISTICS

Command (in SUM)	Description
<code>show firewall intrusion snort statistics rule {<1-4294967295..> all category <name> classtype <name> priority {high low medium}}</code>	Use this command to display Snort rule statistics based on rule ID, category, class type, or priority.

EXAMPLE

```
ALU#show firewall intrusion snort statistics rule all
```

TO VIEW REPORTS AND STATUS OF SNORT SIGNATURE UPDATE

Command (in SUM)	Description
<code>show firewall intrusion snort update [(report status)]</code>	Use this command to display the status of the Snort signature database update.

EXAMPLE

```
ALU#show firewall intrusion snort update report
```


IDS CLEAR COMMANDS

To CLEAR SNORT STATISTICS

Command (in SUM)	Description
<code>clear firewall intrusion snort statistics</code>	Use this command to clear Snort statistics.

EXAMPLE

```
ALU#clear firewall intrusion snort statistics
Pkt Received : 10
Pkt Passed   : 8
Pkt Dropped  : 2
Pkt Queued   : 0
Pkt Detected : 0
```

To CLEAR SNORT PREPROCESSOR STATISTICS

Command (in SUM)	Description
<code>clear firewall intrusion snort statistics preprocessor</code> <code>[{back-orifice http-inspect rpc stream4}]</code>	Use this command to clear the Snort preprocessor statistics.

EXAMPLE

```
ALU#clear firewall intrusion snort statistics preprocessor
http-inspect
```

To CLEAR GROUP LEVEL SNORT STATISTICS

Command (in SUM)	Description
<code>clear firewall intrusion snort statistics rule</code> {<1-4294967295..> all category <name> classtype <name> priority {high low medium}}	Use this command to clear group level Snort statistics.

EXAMPLE

```
ALU#clear firewall intrusion snort statistics rule all num
class-type class-type1
```

IDS DEBUG COMMANDS

This section lists the debug commands in IDS.

To ENABLE / DISABLE DEBUGGING ON FIREWALL

Command (in SUM)	Description
<pre>debug firewall {session filter nat attack alg intrusion selector [saddr <ip-address> daddr <ip- address> protocol <number> sport <number> dport <number>][output permanent] all [detail-level]}</pre>	<p>This command turns on the debugging functionality for IDS on the OA-700.</p> <p>The “selector” keyword allows you to debug only selected traffic.</p>
<pre>no debug firewall {session filter nat attack alg intrusion selector [saddr <ip-address> daddr <ip- address> protocol <number> sport <number> dport <number>][output permanent] all [detail-level]}</pre>	<p>Use this command to turn off the debugging functionality for IDS.</p> <p>The “selector” keyword allows you to turn off debugging only for selected traffic.</p>

Notes:

1. **saddr** == source address
2. **daddr** == destination address
3. **sport** == source port
4. **dport** == destination port

EXAMPLE

```
ALU# debug firewall intrusion
```

```
ALU# no debug firewall intrusion
```

IDS CONFIGURATION SCENARIO USING OA-700

The step-by-step procedure to configure IDS using the OA-700 is given below.

CONFIGURATION STEPS

QUICK STEPS

1. Create match-list.
2. Create intrusion sensor.
3. Create firewall policy.
4. Attach match-list and intrusion sensor to the firewall policy.
5. Attach firewall policy to an interface.

DETAILED STEPS

Step 1: Configure rule using match-list for any packet that matches classification.

```
ALU(config)#match-list m1
ALU(config-match-list-m1)#ip any any
ALU(config-match-list-m1)#exit
```

Step 2: Create an intrusion sensor.

```
ALU(config)#firewall
ALU(config-firewall)#intrusion sensor ids1 snort
ALU(config-intrusion-sensor-ids1)#exit
```

Step 3: Create a firewall policy.

```
ALU(config)#firewall
ALU(config-firewall)#policy p1
ALU(config-firewall-p1)#
```

Step 4: Attach match-list and intrusion sensor to the firewall policy and specify the action (detection or prevention).

```
ALU(config-firewall-p1)#match m1 intrusion ids1 prevention
```

Step 5: Apply the firewall policy to ingress of WAN interface.

```
ALU(config)#interface GigabitEthernet 7/1
ALU(config-if GigabitEthernet7/1)#firewall policy in p1
ALU(config-if GigabitEthernet7/1)#exit
```

SHOW COMMANDS

1. To check firewall policy with IDS sensor information


```
ALU#show firewall policy p1
ALU#show firewall intrusion sensor ids1
```
2. To verify firewall intrusion statistics and counters when device detects the intrusion


```
ALU#show firewall intrusion snort statistics
```

IDS TOPOLOGY

The topology consists of the following components:

- OA-780
- 3 PCs - with 2 PCs running Nessus

TEST CASE

In the topology given below, OA-780 is configured in the Prevention mode. Attacks from PC-1 and PC-2 running application Nessus is intercepted by the OA-780 and dropped.

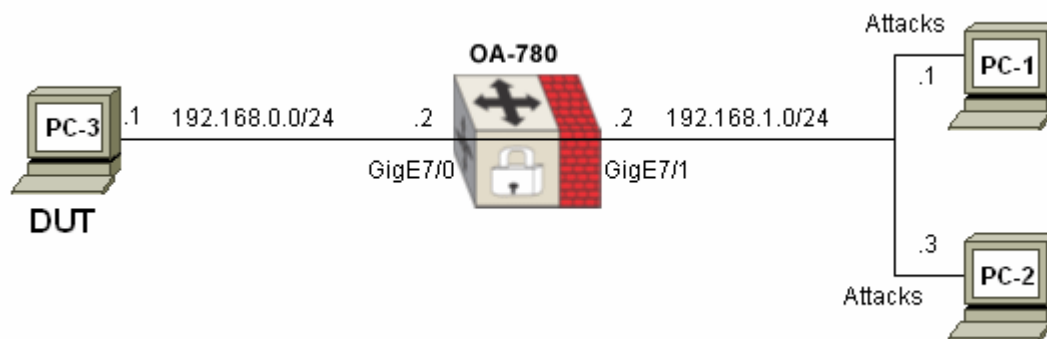


Figure 82: IDS Topology

Part 8 TCP/IP Services



CHAPTER 32 DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) SERVER

This chapter documents the commands for DHCP Server configuration.

For instructions on using the DHCP Server commands and descriptions on each of their parameters with the corresponding default values for each, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

This chapter includes the following sections:

- [“DHCP Server Overview”](#)
- [“DHCP Server Configuration”](#)
- [“DHCP Server Test Scenarios using OA-780”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#

DHCP SERVER OVERVIEW

DHCP is a protocol for dynamically assigning IP addresses to the devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs (Internet Service Providers) use dynamic IP addressing for dial-up users.

ALCATEL-LUCENT SPECIFIC OVERVIEW

By default, the DHCP service is disabled and you should 'enable' the DHCP server explicitly for the service to become available.

The DHCP server in the OA-700 provides DHCP clients with an IP address along with other network and boot information, based on the DHCP request received from the client.

The major configurable objects in the DHCP component are the pools and options. There is a global set of options and each pool can have its own set of options configured. While processing a client's DHCP request the options will be looked up in the pool to which the request is matched. If the pool specific options are not configured, the global options will be checked if both of them are not configured then the particular option will not be returned in the response message.

DHCP SERVER CONFIGURATION

This chapter includes the following sections:

- [“DHCP Server Configuration Steps”](#)
- [“DHCP Server Configuration Flow”](#)
- [“DHCP Server Configuration Commands”](#)
- [“DHCP Server Test Scenarios using OA-780”](#)

DHCP SERVER CONFIGURATION STEPS

The following steps details the procedure to configure DHCP server on OA-700:

Step 1: Configure an interface. Enter the Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Enable DHCP service. See [“To Enable DHCP Service”](#)

Step 5: Configure DHCP pool. See [“To Configure DHCP Pool”](#)

- Configure network pool. See [“To Configure a Network Pool”](#)
- Configure Network range for the pool. See [“To Configure a Network Range”](#)

Step 6: Configure DHCP server optional parameters.

- Exclude IP address from a network range. See [“To Exclude IP Address from a Network Range”](#)
- Configure host pool for manual binding. See [“To Configure a Host Pool”](#)
- Configure DHCP Options. See [“To Configure DHCP Options”](#)

Step 7: View the DHCP server configuration by using the show commands. See [“DHCP Server Show Commands”](#)

DHCP SERVER CONFIGURATION FLOW

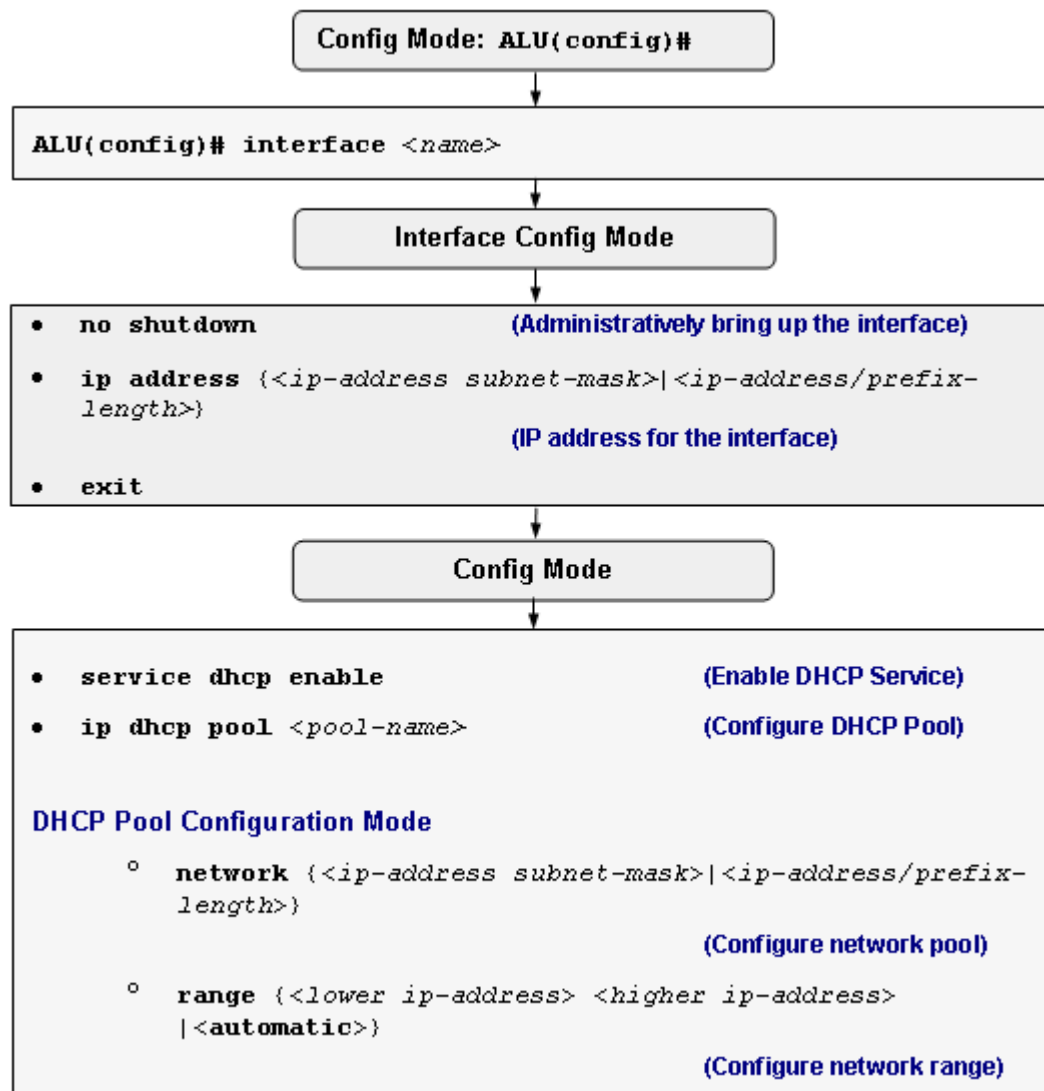


Figure 83: DHCP Server Configuration Flow

DHCP SERVER CONFIGURATION COMMANDS

To ENABLE DHCP SERVICE

Command (in CM)	Description
<code>service dhcp enable</code>	This command is used to enable the DHCP service on the OA-700. By default, DHCP service is disabled.
<code>service dhcp disable</code>	This command is used to disable the DHCP service on the OA-700.

EXAMPLE

```
ALU(config)# service dhcp enable
```

```
ALU(config)# service dhcp disable
```

To CONFIGURE DHCP POOL

A pool is a collection of IP addresses maintained by the DHCP server for assignment to DHCP clients. A pool can have only a single network or host configured inside it, and is accordingly called a network or a host pool.

Command (in CM)	Description
<code>ip dhcp pool <pool-name></code>	This command is used to configure a DHCP pool. This command enters the DHCP pool sub-configuration mode.
<code>no ip dhcp pool <pool-name></code>	Deletes a configured DHCP pool.

EXAMPLE

```
ALU(config)# ip dhcp pool p1
```

```
ALU(config-dhcp-pool-p1)#
```

```
ALU(config)# no ip dhcp pool p1
```

```
Pool Deleted
```

TO CONFIGURE A NETWORK POOL

Command (in DHCP Pool CM)	Description
network {<ip-address subnet-mask> <ip-address/prefix-length>}	This command is used to specify the network to which the pool belongs to.
no network {<ip-address subnet-mask> <ip-address/prefix-length>}	Deletes a configured network pool.

EXAMPLE

```
ALU(config-dhcp-pool-p1)# network 1.2.3.0/24
```

```
ALU(config-dhcp-pool-p1)# no network 1.2.3.0/24
```



Note: Network mask configurable for a DHCP network is limited to /16 or 255.255.0.0. You cannot give a mask < 16 or <255.255.0.0. That is, a single network can have maximum of 65534 hosts.

TO CONFIGURE A NETWORK RANGE

Command (in DHCP Pool CM)	Description
range {<lower ip-address> <higher ip-address> <automatic>}	<p>This command is used to configure the range of IP addresses within the network of the pool, which are used to service DHCP requests from the clients.</p> <p>You can specify the lower and the upper addresses of the network range.</p> <p>You can also use 'automatic' keyword to specify the entire network addresses to be available to the client.</p> <p>Specification of range is mandatory for a network pool. The range cannot include the network address and the broadcast address of the network.</p>
no range {<lower ip-address> <higher ip-address> <automatic>}	Deletes a configured network range.



Note: The network configuration for a pool must exist before a range can be specified.

EXAMPLE

```
ALU(config-dhcp-pool-p1)# range 1.2.3.50 1.2.3.100
```

```
ALU(config-dhcp-pool-p1)# range automatic
```

```
ALU(config-dhcp-pool-p1)# no range automatic
```

TO EXCLUDE IP ADDRESS FROM A NETWORK RANGE

After having a specified range, you can exclude certain IP addresses of that range from the pool. The exclude command is used for this.

Command (in DHCP Pool CM)	Description
exclude ip <ip-address>	This command is used to exclude an IP address of the range from the pool. The excluded IP address should exist within the configured range.

EXAMPLE

```
ALU(config-dhcp-pool-p2)# exclude ip 1.2.3.65
```

TO CONFIGURE A HOST POOL

Command (in DHCP Pool CM)	Description
host <ip-address> <mac-address>	This command is used to statically bind an IP address with a hardware (MAC) address. The IP address should exist within the configured network.
no host <ip-address> <mac-address>	Deletes the manual binding between the host and IP address specified for it.

EXAMPLE

```
ALU(config-dhcp-pool-p2)# host 1.2.3.66 1122.aabb.55ff
```

```
ALU(config-dhcp-pool-p2)# no host 1.2.3.66 1122.aabb.55ff
```

To CONFIGURE DHCP OPTIONS

There are two types of DHCP options - Global Options and Pool Options. The global options are applicable to all pools. In case the option is re-specified in a pool, then the pool-specific (per-pool) option overrides the global option for that pool. The global options need to be configured in the **Configuration Mode**, whereas, the pool options need to be configured in the **DHCP Pool Configuration Mode**.

Whenever a DHCP request with a parameter list comes, first the option will be searched in the pool to which the request maps to, and then if it is not configured there, it is looked for in the list of global options. If it is not configured in either places, then it is not supplied.



Note: For a detailed reference on DHCP options, refer RFC 2132.

To CONFIGURE DHCP GLOBAL OPTIONS

Command (in CM)	Description
<code>[no] ip dhcp option bootfile-name <file-name></code>	This command is used to configure the boot file for a host.
<code>[no] ip dhcp option dns-server <ip-address></code>	This command is used to configure the DNS server IP address to be used by the clients.
<code>[no] ip dhcp option domain-name <name></code>	This command is used to configure the domain name to be used by the clients.
<code>[no] ip dhcp option lease-time <1-4294967295></code>	This command is used to configure the time for which the clients can use the IP address assigned to them.
<code>[no] ip dhcp option log-server <ip-address></code>	This command is used to configure the MIT-LCS UDP log server IP address to be used by the clients.
<code>[no] ip dhcp option ntp-server <ip-address></code>	This command is used to configure the IP address of the Network Time Protocol server to be used by the clients.
<code>[no] ip dhcp option rebinding-time <1-4294967295></code>	This command is used to set the time the client has to wait before trying to obtain an IP address from any available DHCP server. Typically this is used if the renewal request fails. Default value of the rebinding time is 87.5% of the lease time.

Command (in CM)	Description
<code>[no] ip dhcp option renewal-time <1-4294967295></code>	This command is used to set the time after which the client has to renew the IP address. Default value for the renewal time is 50% of the lease time.
<code>[no] ip dhcp option routers <ip-address></code>	This command is used to configure the router in the subnet for which the DHCP has been configured.
<code>[no] ip dhcp option subnet-mask <subnet-mask></code>	This command is used to configure the client's subnet mask.
<code>[no] ip dhcp option tftp-server <string></code>	This command is used to configure the IP address/domain name of the TFTP server.
<code>[no] ip dhcp option time-offset <1-4294967295></code>	This command is used to determine the time variation from GMT (in seconds).

EXAMPLE

```

ALU(config)# ip dhcp option bootfile-name boot_image

ALU(config)# ip dhcp option dns server 1.2.2.2

ALU(config)# ip dhcp option domain-name ALU

ALU(config)# ip dhcp option lease-time 1000250

ALU(config)# ip dhcp option log-server 1.1.1.1

ALU(config)# ip dhcp option ntp-server 1.1.1.1

ALU(config)# ip dhcp option rebinding-time 50000

ALU(config)# ip dhcp option renewal-time 86400

ALU(config)# ip dhcp option routers 1.1.1.1

ALU(config)# ip dhcp option subnet-mask 255.255.255.0

ALU(config)# ip dhcp option tftp-server 3.2.2.1

ALU(config)# ip dhcp option time-offset 100

```


To CONFIGURE DHCP POOL OPTIONS

These commands are to configure DHCP options for a specific pool. These commands are entered in the DHCP Pool Configuration mode.

Command (in DHCP Pool CM)	Description
<code>[no] option bootfile-name <file-name></code>	This command is used to configure the boot file for a host.
<code>[no] option dns-server <ip-address></code>	This command is used to configure the DNS server IP address to be used by the clients.
<code>[no] option domain-name <name></code>	This command is used to configure the domain name to be used by the clients.
<code>[no] option lease-time <1-4294967295></code>	This command is used to configure the time for which a client can use the IP address assigned to it.
<code>[no] option log-server <ip-address></code>	This command is used to configure the MIT-LCS UDP log server IP address to be used by the clients.
<code>[no] option ntp-server <ip-address></code>	This command is used to configure the IP address of the Network Time Protocol server to be used by the clients.
<code>[no] option rebinding-time <1-4294967295></code>	This command is used to set the time the client has to wait before trying to obtain an IP address from any available DHCP server. Typically this is used if the renewal request fails.
<code>[no] option renewal-time <1-4294967295></code>	This command is used to set the time after which the client has to renew the IP address.
<code>[no] option routers <ip-address></code>	This command is used to configure the router in the subnet for which the DHCP has been configured.
<code>[no] option subnet-mask <subnet-mask></code>	This command is used to configure the client's subnet mask.
<code>[no] option tftp-server <string></code>	This command is used to configure the IP address/domain name of the TFTP server.
<code>[no] option time-offset <1-4294967295></code>	This command is used to determine the time variation from GMT (in seconds).

EXAMPLE

```
ALU(config-dhcp-pool-p1)# option bootfile-name boot_image
ALU(config-dhcp-pool-p1)# option dns server 1.2.2.2
ALU(config-dhcp-pool-p1)# option domain-name ALU
ALU(config-dhcp-pool-p1)# option lease-time 106400
ALU(config-dhcp-pool-p1)# option log-server 1.1.1.1
ALU(config-dhcp-pool-p1)# option ntp-server 1.1.1.1
ALU(config-dhcp-pool-p1)# option rebinding-time 50000
ALU(config-dhcp-pool-p1)# option renewal-time 86400
ALU(config-dhcp-pool-p1)# option routers 1.1.1.1
ALU(config-dhcp-pool-p1)# option subnet-mask 255.255.255.0
ALU(config-dhcp-pool-p1)# option tftp-server 3.2.2.1
ALU(config-dhcp-pool-p1)# option time-offset 100
```

DHCP SERVER SHOW COMMANDS

To VIEW DHCP GLOBAL OPTIONS

Command (in SUM/CM)	Description
<code>show ip dhcp options</code>	This command shows all the DHCP global options configured.

EXAMPLE

```
ALU(config)# show ip dhcp options

Routers                : 1.1.1.1
Domain Name Server     : 1.2.2.2
Log Server              : 1.1.1.1
NTP Server              : 1.1.1.1
ALU(config)#
```

To VIEW THE DHCP POOL CONFIGURATION

Command (in SUM/CM)	Description
<code>show ip dhcp pools [<pool-name>]</code>	This command shows all the pools and their options configured. You can also view the details of only a single pool by specifying the pool name.

EXAMPLE

```
ALU(config)# show ip dhcp pools

Pool Name                : p2
Pool Host Address        : 1.2.3.66
Pool Host Mac Address    : 11:22:aa:bb:55:ff

Pool Name                : p1
Pool Network Number      : 1.2.3.0
Pool Network Mask        : 255.255.255.0
Number of leases         : 50
Pool Range                : 1.2.3.50 / 1.2.3.100
Boot-File Name           : boot_image

ALU(config)# show ip dhcp pools p2

Pool Name                : p2
Pool Host Address        : 1.2.3.66
Pool Host Mac Address    : 11:22:aa:bb:55:ff
```

To VIEW THE BINDING CONFIGURATION

Command (in SUM/CM)	Description
<pre>show ip dhcp bindings [{dynamic manual pool <name> }]</pre>	<p>This command shows all the assigned leases (the IP addresses allocated to the hosts).</p> <p>Dynamic: This keyword shows all the dynamically assigned leases of all the pools.</p> <p>Manual: This keyword shows all the manually linked leases of all the pools.</p> <p>Pool: This keyword shows all the assigned leases for a specific pool (dynamic/manual).</p>

EXAMPLE

```
ALU(config)# show ip dhcp bindings
```

IP Address	Hardware Address	Lease Expiration	Type	Pool
=====	=====	=====	=====	=====
10.91.2.87	00:0f:fe:3a:63:da	Wed Jan 17 23:38:11 2007	DYNAMIC	p1
203.196.196.74	00:0f:ef:3b:63:de	INFINITE	MANUAL	p2

```
ALU(config)# show ip dhcp bindings dynamic
```

IP Address	Hardware Address	Lease Expiration	Type	Pool
=====	=====	=====	=====	=====
10.91.2.87	00:0f:fe:3a:63:da	Wed Jan 17 23:38:11 2007	DYNAMIC	p1

To VIEW DHCP SERVER STATISTICS

Command (in SUM/CM)	Description
<code>show ip dhcp server statistics</code>	This command shows the DHCP server statistics.

EXAMPLE

```
ALU(config)# show ip dhcp server statistics
```

```
Message                Received
DHCPDISCOVER           0
DHCPREQUEST            14
DHCPCDECLINE           0
DHCPRELEASE            0
DHCPINFORM             8
```

```
Message                Sent
DHCPPOFFER             0
DHCPACK                0
DHCPNAK                0
```

DHCP SERVER TEST SCENARIOS USING OA-780

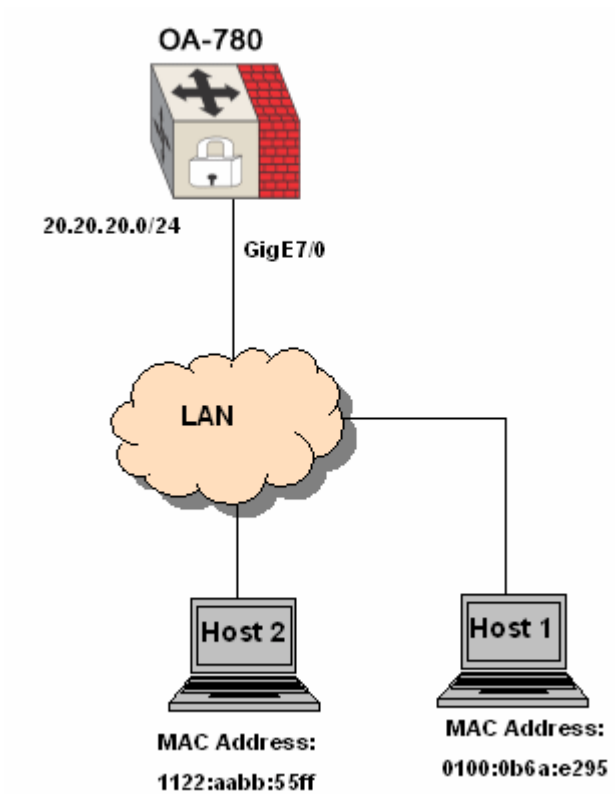


Figure 84: DHCP Server Test Scenario using OA-780

Consider a scenario with OA-780 as a DHCP Server, with two hosts Host 1 and Host 2 connected to LAN, with MAC address 0100:0b6a:e295 and 1122:aabb:55ff respectively.

CONFIGURATION STEPS

Step 1: Configure a GigE interface, IP address for the interface and administratively bring it up.

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)# no shutdown
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 2: Enable DHCP Service on the OA-780

```
ALU(config)# service dhcp enable
```

Step 3: Configure DHCP pool

```
ALU(config)# ip dhcp pool p1
ALU(config-dhcp-pool-p1)#
```

Step 4: Configure a Network Pool, and Network Range for the pool

```
ALU(config-dhcp-pool-p1)# network 20.20.20.0/24
ALU(config-dhcp-pool-p1)# range 20.20.20.50 20.20.20.100
```

When the host 1 and host 2 sends broadcast request to the DHCP server, the DHCP server assigns the IP addresses within the network range configured for the pool p1. This can be verified by giving the show command '**show ip dhcp bindings** [{dynamic|manual|pool <name>}]'

CHAPTER 33 TFTP (TRIVIAL FILE TRANSFER PROTOCOL) SERVER

This chapter documents the TFTP Server configuration commands.

For instructions on using the TFTP Server commands and descriptions on each of their parameters with the corresponding default values for each, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

This chapter includes the following sections:

- [“TFTP Server Overview”](#)
- [“TFTP Server Configuration”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
TFTP	Trivial File Transfer Protocol

TFTP SERVER OVERVIEW

TFTP (Trivial File Transfer Protocol) is a simplified version of FTP without authentication and many other basic features.

TFTP is normally used only for booting diskless workstations. TFTP provides very little security, and should not be enabled unless it is expressly needed. The tftp-server package allows users to download files from the OA-700 using TFTP.

ALCATEL-LUCENT SPECIFIC OVERVIEW

- The TFTP Server is based on the Open BSD (tftp-hpa version 1.3) version of the code.
- TFTP services implemented on the OA-700 platform allows you to configure/download files from User area of USB. For the ease of use, each file can be added with an alias associated with it and you can get the file referring to the alias name.
- Only 'tftp get' option is allowed and the 'tftp put' requests are silently discarded.
- You can copy the files onto the USB using the copy command framework and then add it to the list of files allowed for download through the TFTP server.
(To know more about the copy commands, refer to the [“System Configuration and Monitoring”](#) chapter.)
- By default, the TFTP service is disabled and you should 'enable' the TFTP server explicitly for the service to become available.

TFTP SERVER CONFIGURATION

This chapter includes the following sections:

- [“TFTP Configuration Steps”](#)
- [“TFTP Configuration Flow”](#)
- [“TFTP Configuration Commands”](#)

TFTP CONFIGURATION STEPS

The following steps details the procedure to configure TFTP server on the OA-700:

Step 1: Enable TFTP service. See [“To Enable/Disable TFTP Service”](#)

Step 2: Copy files for download through TFTP and optionally configure alias for easy access. See [“To Configure Files for Download Through TFTP and to Create File Alias”](#)

Step 3: View the TFTP files using the show command. See [“To View TFTP Files”](#)

TFTP CONFIGURATION FLOW

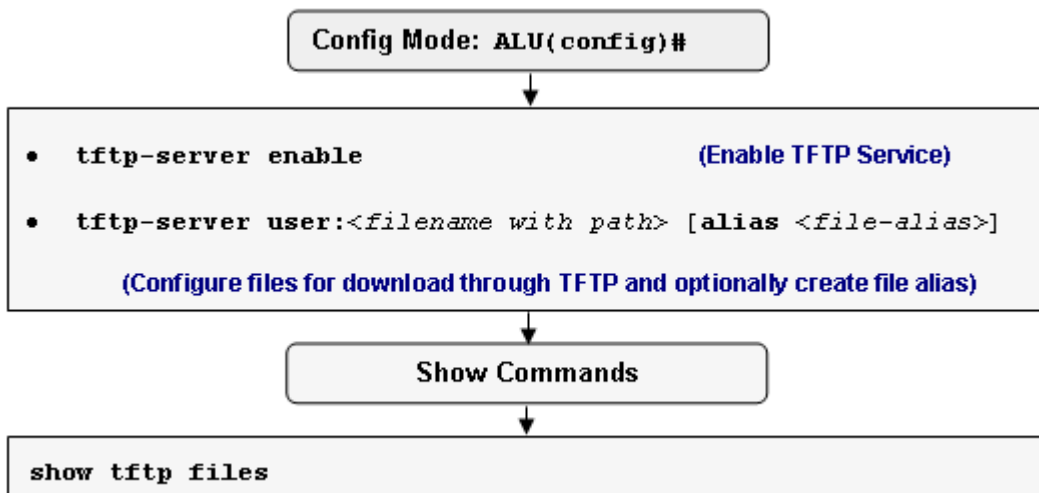


Figure 85: TFTP Configuration Flow

TFTP CONFIGURATION COMMANDS

To ENABLE/DISABLE TFTP SERVICE


Command (in CM)	Description
<code>tftp-server enable</code>	This command is used to enable TFTP service on the OA-700. By default, TFTP service is disabled.
<code>tftp-server disable</code>	This command is used to disable TFTP service on the OA-700.

EXAMPLE

```
ALU(config)# tftp-server enable
```

```
ALU(config)# tftp-server disable
```

To CONFIGURE FILES FOR DOWNLOAD THROUGH TFTP AND TO CREATE FILE ALIAS

Command (in CM)	Description
<code>tftp-server user:<filename with path> [alias <file-alias>]</code>	<p>This command is used to specify files allowed for download through the TFTP server.</p> <p>Using the 'alias' keyword, you can create an alias for the file. You can then download the file through this alias, instead of its actual path. This could be useful if the file's name or path is tedious. A file can have multiple aliases.</p>  <p>Note: Alias must be a unique name and no two files can have the same aliases.</p> <p>Enter the file name with the path after user: keyword without any space.</p>
<code>no tftp-server {user:<filename with path> alias <file-alias>}</code>	<p>This command is used to remove the file from the tftp file-list.</p> <p>If a file is removed from the tftp-file list, then all its aliases are also removed.</p>

EXAMPLE

```
ALU(config)# tftp-server user:/voip/www/voip/update.php alias
voiptest
```

```
ALU(config)# no tftp-server user:/voip/www/voip/update.php
```

```
ALU(config)# no tftp-server alias voiptest
```

TFTP SHOW COMMANDS**TO VIEW TFTP FILES**

Command (in SUM/CM)	Description
<code>show tftp files</code>	This command shows the list of files configured for download through the TFTP server.

EXAMPLE

```
ALU(config)# show tftp files
```

```
TFTP-File                                     Alias
-----
/a                                             N.A.
/tftpd                                        N.A.
/voip/www/voip/update.php                    N.A.
/voip/www/voip/update.php                    voiptest
```

CHAPTER 34 DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) RELAY

This chapter documents the commands for DHCP Relay configuration.

For instructions on using the DHCP Relay commands and descriptions on each of their parameters with the corresponding default values for each, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

This chapter includes the following sections:

- [“DHCP Relay Overview”](#)
- [“DHCP Relay Configuration”](#)
- [“DHCP Relay Test Scenarios using OA-780”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU#
CM	Configuration Mode - ALU (config)#
DHCP	Dynamic Host Configuration Protocol

DHCP RELAY OVERVIEW

DHCP Relay Agent acts as an intermediary between clients and servers by listening for client DHCP broadcast requests and forwarding them on to the server. In addition, the Relay Agent receives the server's response and passes the response back to the client.

The relay agent allows the client and server to reside on different subnets.

ALCATEL-LUCENT SPECIFIC OVERVIEW

DHCP Relay forwarding to the DHCP server is implemented directly or via rebroadcast on another interface on the OA-780.

DHCP RELAY CONFIGURATION

This chapter includes the following sections:

- [“DHCP Relay Configuration Steps”](#)
- [“DHCP Relay Configuration Flow”](#)
- [“DHCP Relay Configuration Commands”](#)
- [“DHCP Relay Test Scenarios using OA-780”](#)

DHCP RELAY CONFIGURATION STEPS

The following steps details the procedure to configure DHCP Relay on the OA-700:

Step 1: Configure an interface. Enter Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>|<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Configure the DHCP server to which the DHCP requests are to be forwarded. Alternatively you can also configure the interface through which the relay requests are to be broadcast. See [“To Relay DHCP Packets to Server”](#), [“To Relay Requests to Interface”](#).

Step 5: View the DHCP Relay configuration by using the show commands. See [“To View DHCP Relay Configuration”](#).

DHCP RELAY CONFIGURATION FLOW

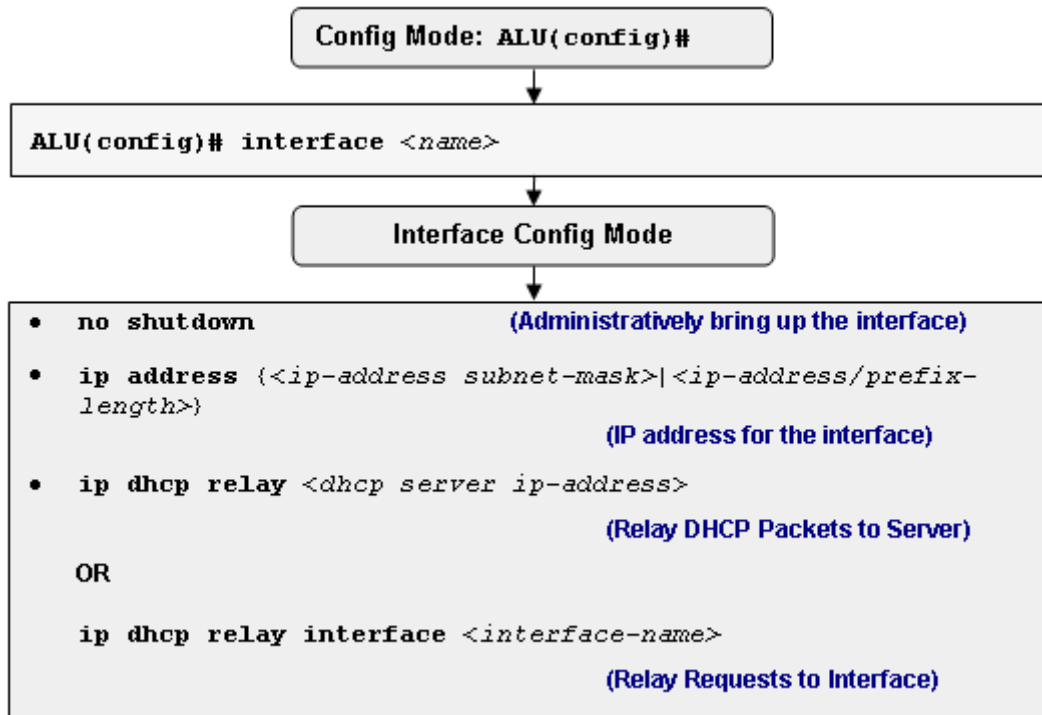



Figure 86: DHCP Relay Configuration Flow

DHCP RELAY CONFIGURATION COMMANDS

TO RELAY DHCP PACKETS TO SERVER

Command (in ICM)	Description
<code>ip dhcp relay <dhcp server ip-address></code>	<p>This command is entered in the Interface Configuration mode.</p> <p>This command is used to configure the DHCP server to which the DHCP requests are to be forwarded.</p>  <p>Note: A maximum of four DHCP relays can be configured on an interface.</p>
<code>no ip dhcp relay [<dhcp server ip-address>]</code>	This command is used to disable all/a specific relay configured on an interface.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip dhcp relay 192.168.1.1
ALU(config-if GigabitEthernet3/0)# no ip dhcp relay 192.168.1.1
```

TO RELAY REQUESTS TO INTERFACE

Command (in ICM)	Description
<code>ip dhcp relay interface <interface-name></code>	<p>This command is entered in the Interface Configuration Mode.</p> <p>This command is used to configure the interface through which the DHCP relay requests have to be rebroadcasted.</p>
<code>no ip dhcp relay interface <interface-name></code>	This command is used to disable relay of DHCP requests to the specified interface.

EXAMPLE

```
ALU(config-if GigabitEthernet3/0)# ip dhcp relay interface
GigabitEthernet 3/1
ALU(config-if GigabitEthernet3/0)# no ip dhcp relay interface
GigabitEthernet 3/1
```

To VIEW DHCP RELAY CONFIGURATION

Command (in SUM/CM)	Description
<code>show ip dhcp relay</code> [<interface-name>]	This command shows the DHCP Relay configuration of all/an interface.

EXAMPLE

```
ALU(config)# show ip dhcp relay
```

```
Interface                Relay destination
GigabitEthernet3/0       192.168.1.1
GigabitEthernet3/0       GigabitEthernet3/1
```

DHCP RELAY TEST SCENARIOS USING OA-780

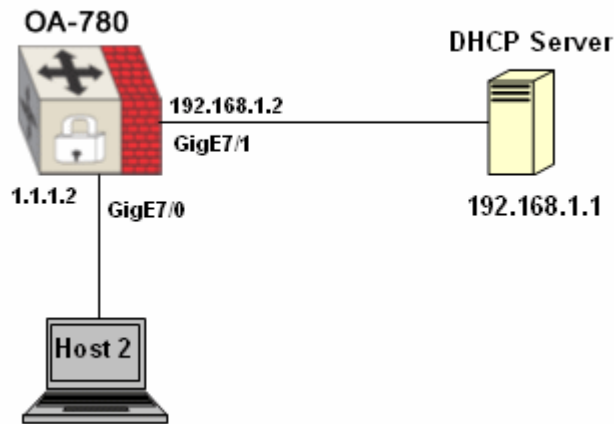


Figure 87: DHCP Relay Test Scenario using OA-780

CONFIGURATION STEPS

Step 1: Configure the DHCP server to which the DHCP requests are to be forwarded.

```
ALU(config-if GigabitEthernet7/0)# ip dhcp relay
192.168.1.1
```

OR

Configure the interface through which the DHCP relay requests have to be rebroadcasted.

```
ALU(config-if GigabitEthernet7/0)# ip dhcp relay
interface GigabitEthernet 7/1
```

When the host 2 sends broadcast requests, the DHCP Relay listens to them and forwards to the DHCP server. The DHCP client receives the server's response and passes the response back to the client.



Note: If you configure relay via IP address and interface, preferred method of relaying DHCP would be via "relay to address" as it reduces broadcast load.

CHAPTER 35 DNS (DOMAIN NAME SERVICE) CLIENT

This chapter documents the commands for DNS Client configuration.

For instructions on using the DNS Client commands and descriptions on each of their parameters with the corresponding default values for each, refer to the ***OmniAccess 700 CLI Command Reference Guide***.

This chapter includes the following sections:

- [“DNS Client Overview”](#)
- [“DNS Client Configuration”](#)
- [“DNS Client Test Scenario using OA-780”](#)

CHAPTER CONVENTIONS

Acronym	Description
SUM	Super User Mode - ALU #
CM	Configuration Mode - ALU (config)#

DNS CLIENT OVERVIEW

The DNS Client functionality on the OA-700 allows for resolution of host names to IP addresses, and vice-versa.

DNS CLIENT CONFIGURATION

This chapter includes the following sections:

- [“DNS Client Configuration Steps”](#)
- [“DNS Client Configuration Flow”](#)
- [“DNS Client Configuration Commands”](#)

DNS CLIENT CONFIGURATION STEPS

The following steps details the procedure to configure DNS Client on OA-700:

Step 1: Configure an interface. Enter Interface Configuration Mode.

```
ALU(config)# interface <name>
```

Example:

```
ALU(config)# interface GigabitEthernet7/0
ALU(config-if GigabitEthernet7/0)#
```

Step 2: Administratively bring up the interface

```
ALU(config-if <interface-name>)# no shutdown
```

Example:

```
ALU(config-if GigabitEthernet7/0)# no shutdown
```

Step 3: Configure IP address for the interface

```
ALU(config-if <interface-name>)# ip address {<ip-
address subnet-mask>/<ip-address/prefix-length>}
```

Example:

```
ALU(config-if GigabitEthernet7/0)# ip address
20.20.20.20/24
```

Step 4: Enable domain lookup. See [“To Enable/Disable IP Domain Lookup”](#)

Step 5: Specify DNS server to which the requests are to be sent. See [“To Specify DNS Server”](#)

Step 6: Configure DNS Client optional parameters.

- Configure default domain name. See [“To Configure Default Domain Name”](#)
- Configure domain list. See [“To Configure Domain List”](#)
- Add a static address mapping for hosts. See [“To Add a Static Address Mapping”](#)
- Configure Host-max-age. See [“To Configure Host-max-age”](#)

Step 7: View the DNS Client by using the show commands. See [“To View DNS Client Configuration”](#)

DNS CLIENT CONFIGURATION FLOW

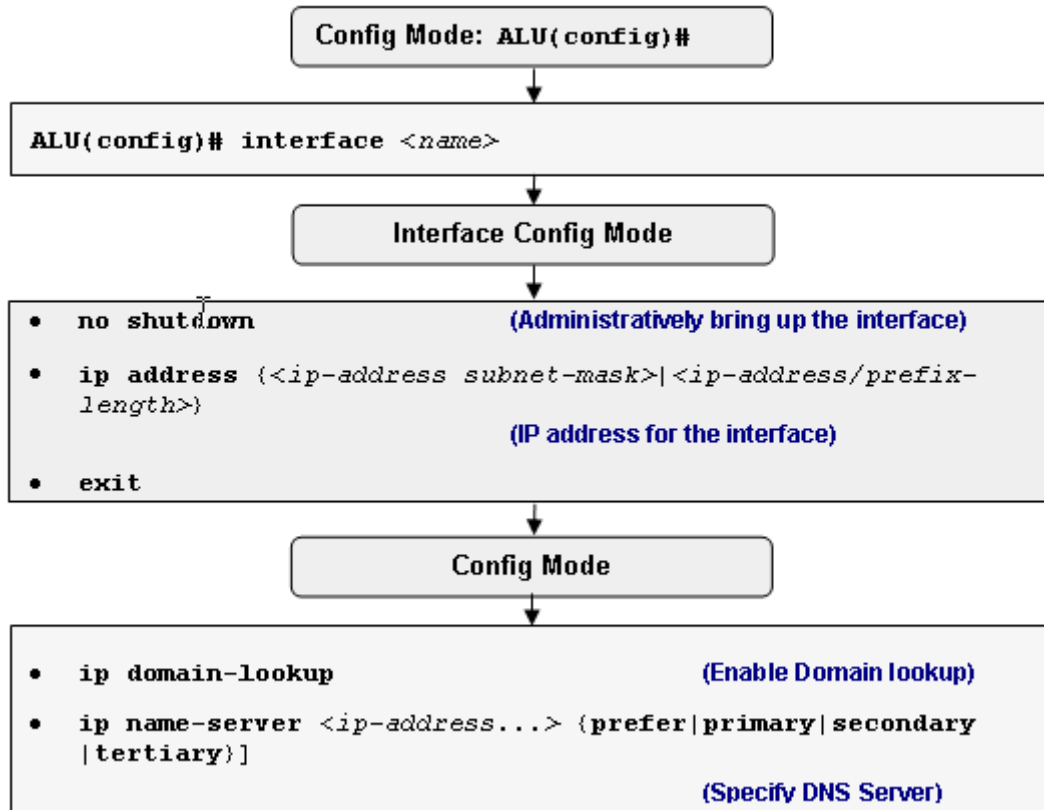


Figure 88: DNS Client Configuration Flow

DNS CLIENT CONFIGURATION COMMANDS

To ENABLE/DISABLE IP DOMAIN LOOKUP

Command (in CM)	Description
<code>ip domain-lookup</code>	This command is used to enable the system to query the DNS server (s) for name/address translation. By default, domain lookup is enabled.
<code>no ip domain-lookup</code>	This command is used to disable the domain lookup.

EXAMPLE

```
ALU(config)# ip domain-lookup
ALU(config)# no ip domain-lookup
```

To SPECIFY DNS SERVER

Command (in CM)	Description
<code>ip name-server <ip-address...> [{prefer primary secondary tertiary}]</code>	This command is used to add DNS server to which the resolution requests are be sent. You can add maximum of three DNS servers, and specify the order of preference to them individually - Primary, Secondary, Tertiary. Primary is tried first, then the Secondary, and lastly Tertiary. Secondary and tertiary name servers are tried only the query sent to the primary server is not successful. "Prefer" is the same as "primary".
<code>no ip name-server <ip-address...> [{prefer primary secondary tertiary}]</code>	This command is used to remove a name server. If the ordinal is specified, the removal is only successful if the given address is in that ordinal location.

EXAMPLE

```
ALU(config)# ip name-server 1.1.1.1 1.1.1.2 1.1.1.3
ALU(config)# ip name-server 1.1.1.1 primary
ALU(config)# ip name-server 1.1.1.2 secondary
ALU(config)# no ip name-server 1.1.1.1
```

DNS CLIENT OPTIONAL PARAMETERS

TO CONFIGURE DEFAULT DOMAIN NAME

Command (in CM)	Description
<code>ip domain-name <name></code>	This command is used to configure the default domain name, which is used in domain lookup.
<code>no ip domain-name [<name>]</code>	This command is used to remove the default domain name.

EXAMPLE

```
ALU(config)# ip domain-name abc.com
```

```
ALU(config)# no ip domain-name
```

TO CONFIGURE DOMAIN LIST

Command (in CM)	Description
<code>ip domain-list <name></code>	This command is used to add domain names to the domain-list. These are the domain names, which are to be appended to the host names while lookup. By default, the default domain-name is used. The domain names added in the list are probed in order.
<code>no ip domain-list [<name>]</code>	This command is used to delete an entire domain list or a specific domain name from the domain list.

EXAMPLE

```
ALU(config)# ip domain-list test
```

```
ALU(config)# no ip domain-list
```

To ADD A STATIC ADDRESS MAPPING

Command (in CM)	Description
<code>ip host <name> <ip-address></code>	This command is used to add a static address mapping for a specific host.
<code>no ip host <name> [<ip-address>]</code>	This command is used to remove a static address mapping for a host. If the address is specified, the removal is successful only if the exact mapping exists.

EXAMPLE

```
ALU(config)# ip host google.com 64.233.187.99
```

```
ALU(config)# no ip host google.com
```

To CONFIGURE HOST-MAX-AGE

Command (in CM)	Description
<code>ip host-max-age <30-31556952></code>	This command is used to configure the maximum time (in seconds) for which the dynamic host entries will be stored in DNS client cache. Host entries will be stored for a time, which is the minimum of the configured host-max-age or the DNS TTL received from the DNS server. If the DNS TTL is 100 seconds, and the host-max-age is 300 seconds, the entries are stored only for 100 seconds.
<code>no ip host-max-age</code>	This command deletes the configured host-max-age, and resets to its default. The default host-max-age is 300 seconds.

EXAMPLE

```
ALU(config)# ip host-max-age 100
```

```
ALU(config)# no ip host-max-age
```

To VIEW DNS CLIENT CONFIGURATION

Command (in SUM/CM)	Description
show hosts	This command shows all the configuration parameters, and all learned name/address mappings.

EXAMPLE

```
ALU(config)# show hosts
```

```
Default domain is abc.com
Domain list: test1, test
Name/address lookup uses domain service
Name server(s): 1.1.1.1, 1.1.1.2, 1.1.1.3
Dynamic host maximum age (seconds): 300
```

Address	Type	TTL	Name
64.233.187.99	static		www.google.com
216.109.112.135	dynamic	294	yahoo.com

To CLEAR DYNAMIC HOST INFORMATION

Command (in SUM/CM)	Description
clear host { * <host-name> }	This command clears the dynamically learnt name/address mapping, or all such mappings if "*" is specified.

EXAMPLE

```
ALU(config)# clear host *
```

DNS CLIENT TEST SCENARIO USING OA-780

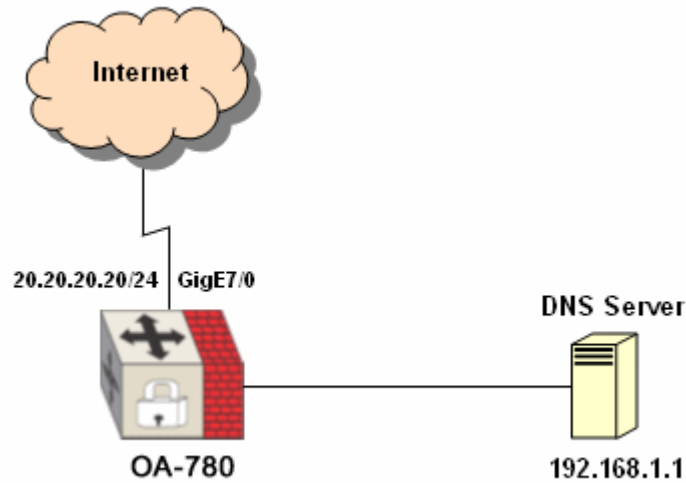


Figure 89: DNS Client Test Scenario using OA-780

Consider a scenario with the OA-780 as a DNS Client connected to the Internet and DNS Server.

CONFIGURATION STEPS

Step 1: Enable domain lookup on the OA-780.

```
ALU(config)# ip domain-lookup
```

Step 2: Specify DNS name server to which the requests are to be sent.

```
ALU(config)# ip name-server 192.168.1.1 primary
```

When user tries to ping to a host by issuing the command "ping <URL>", a DNS query request is sent by OA-780 to the DNS server. When the OA-780 gets a valid response with the IP address for the URL, it sends an echo request to that IP. If the query fails or the DNS server does not have any entry, the user is shown an error "% Unrecognized host or address."

Part 9 Lifeline (Dedicated Management Framework)

CHAPTER 36 LIFELINE

This chapter describes the Lifeline management framework, which is a key architectural aspect of the OA-780. The intent of Lifeline is to deliver a facility by which the system can be reached remotely by at least one method in the event of most severe failures, except power outages. This management framework has been built to facilitate centralized management of a network of the OA-780 systems from a NOC (Network Operations Center) and deliver high levels of manageability and serviceability to these networks. As a part from this, the Lifeline framework also comprises health monitoring of various system components - both hardware and software, with automated recovery procedures. When a drastic failure condition occurs, the system switches to the Lifeline Mode, which allows only management of the OA-780.

When the automated recovery procedures fail, the component is turned off and flagged for attention to the system administrator.

The key success factors for a unified services platform or gateway to address the emerging new needs of branch infrastructure are:

- Access always available to all system management functions, independent of the state of the system.
- 100% remote manageability, with ability to troubleshoot, fix, upgrade, and re-configure services remotely.
- Ability to roll out applications to all non-HQ employees on an as-needed basis.
- Efficient, unified management of all services.

The Lifeline framework addresses the first two propositions listed above.



Note: Currently, Lifeline management framework is supported only on the OA-780.

This chapter includes the configuration steps, CLI syntax with its description and configuration examples. The commands are described in sequential order of configuration.

This chapter describes why the system switches to the Lifeline Mode, its behavior under various scenarios, and commands with their syntax specific to the Lifeline Mode.

CHAPTER CONVENTIONS

Acronym	Description
CM	Configuration Mode - ALU(config)#
NOC	Network Operations Center

LIFELINE OVERVIEW

The Lifeline feature provides remote accessibility for management of the OA-780 under failure conditions. Through the Lifeline management framework, the OA-780 provides remote access to system management, independent of the state of the system. It provides the ability to manage the system, diagnose the failure, and recover from the failure.

The salient features of the Lifeline management framework are a separate management plane with dedicated processors, N+1 dedicated architecture, multiple access mechanisms to reach the system and unified management of all services.

TERMS USED IN LIFELINE

- **Lifeline Mode**
A state of the OA-780 system. When the system experiences a critical hardware or software failure, it discontinues control/data plane functions but continues to provide remote access for management purposes only.
- **Normal Mode**
The state of the system in regular operation when all functions are available and the system is capable of data forwarding.
- **In-Band**
Where the management functions of the system may be accessed directly via the network interfaces of the system used by pass-through data.
- **Data Plane**
Software architectural unit responsible for packet inspection and forwarding.
- **Management Plane**
Software architectural unit responsible for system and services management functions.

LIFELINE FEATURES

SEPARATE MANAGEMENT PLANE WITH DEDICATED RESOURCES

The foundation of the Lifeline management framework is a dedicated management plane that is separate from the data and control planes as shown below.

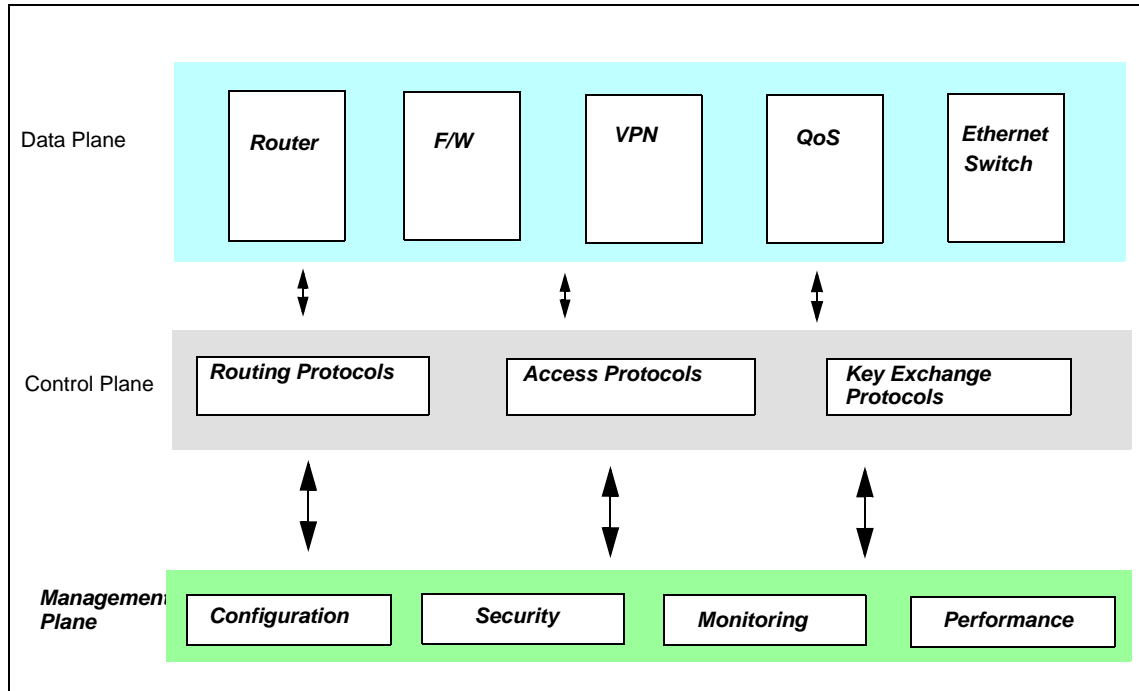


Figure 90: Separate Management Plane

The separate management plane plays a critical role in ensuring uninterrupted access to system management even under the most adverse conditions. The management plane is equipped with dedicated resources, including a separate bus architecture, dedicated processors, dedicated switching fabric and separate management software processes. This enables complete isolation of system management functions from packet processing and control plane functions. As a result, management access to the system is unaffected under conditions such as failure of a data plane function (like routing or firewall), or high main processor utilization caused by high load or Denial of Service (DoS) attack. In contrast, with traditional solutions, there is no guarantee of being able to access the device when the main processing resource is unavailable.

N+1 REDUNDANT MANAGEMENT PROCESSORS

Under the Lifeline management framework, there are multiple active instances of the management process running on each line card, powered by its own management processor. The management plane portion of each line card is connected to a separate management plane switch in the switching card, while the data plane portion is connected to a data plane switch in the switching card. Additionally, a second switching card can be provided for redundancy, with a parallel set of redundant connections between each line card and the second switching card. This concept is illustrated below:

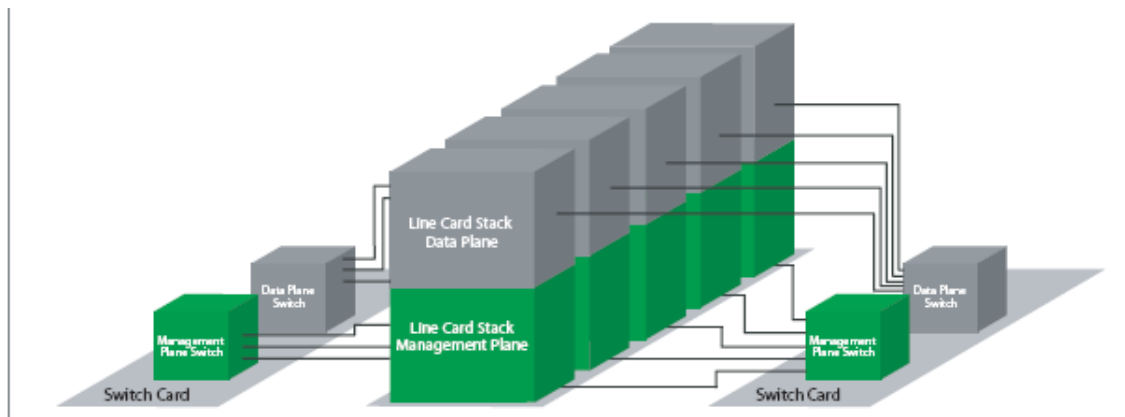


Figure 91: N+1 Redundant Management Architecture

It plays a critical role in ensuring that access to system management functions through the management plane is always available. This will be elaborated further in the following section using a few example scenarios:

LIFELINE SOFTWARE

- **Lifeline Manager**

Lifeline Manager is a Lifeline software architecture unit responsible for detecting and responding to system failures. This manages the system transition to Lifeline Mode and back to Normal Mode.

- **Lifeline Agent**

Lifeline Agent is a Lifeline software architectural unit running on each line card, which is responsible for lifeline framework functions. When the system is running in the normal mode, Lifeline Agent caches all the configuration information. It also caches all the dynamic/static routing configuration.

When the system goes in to the Lifeline Mode, the Lifeline Agent uses this configuration information to set up a minimal data plane to support management access, thus providing remote access to the system.

FAILURE MODES SUPPORTED BY LIFELINE

FAILURE OF THE SERVICES ENGINE

Typically all packets, including management data packets are forwarded through the Services Engine (SE). As noted earlier, under the Lifeline management framework, there are multiple active instances of the management process running on each line card. Hence, if there is a problem with the SE, this is detected by the Lifeline Manager and a special "lifeline" mode of operation is automatically initiated to ensure uninterrupted access through management plane processes running on a different line card as illustrated below.

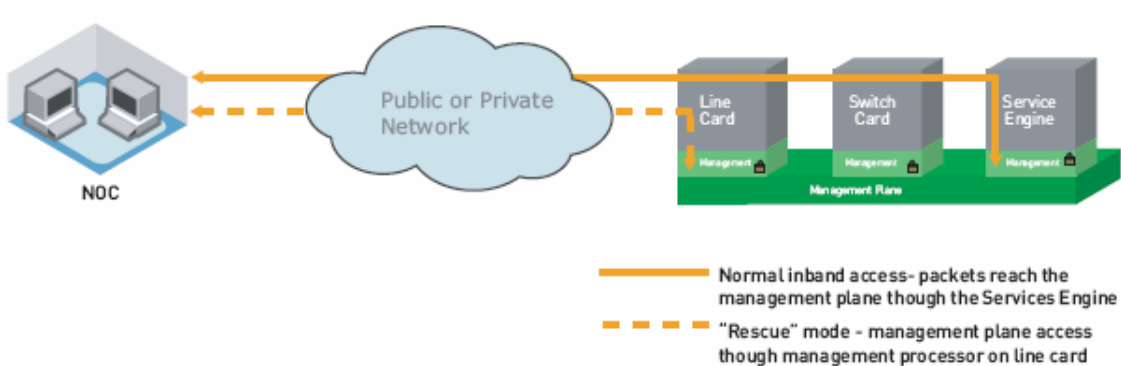


Figure 92: Uninterrupted Access to System Management

As a result, full management functionality is available for rapid troubleshooting and corrective action. In traditional solutions, such a scenario would have led to a complete loss of management access and functionality.

The SE failures could be categorized as:

- SE card failures: This includes hardware failures, including card removal from slot, card power down, overheating shutdown, component failure, etc.
- SE processor failures: This includes software failures, etc.
- This failure is detected by the Lifeline software, which monitors the health of the chassis components and software components.

FAILURE OF THE LINE CARD

If there is a problem with just the data plane functionality on the line card, this will be detected by the management process on that card. The data plane can be re-initialized (automatically) or re-configured to fix the problem through the management plane processor on that card. On the other hand, if there is a failure of the line card itself, full management access to the card is still available through the management plane, which can be used to remotely power off/power on the card or do further trouble-shooting.

FAILURE OF A SOFTWARE COMPONENT

The feature health monitor in the management plane detects the failure of a software component and automatically initiates a restart of the process. In most cases, a restart of the feature will resolve the issue and the problem is fixed without any manual intervention. If there is an extended failure within a very short interval of time (typically two minutes), an alarm is raised to trigger manual intervention for troubleshooting and restart of the feature. The Lifeline management framework ensures that remote management access is always available for rapid efficient manual intervention.

FAILURE OF DATA PLANE SERVICE

In traditional solutions, when there is a failure in the data plane, all access from a remote terminal will be lost. However, lifeline ensures that remote management access is always available.

OTHER FAILURES

Other failures will be handled by a mechanism called auto inband packet path test. This mechanism checks for the health of the inband-management path. When the test fails, the OA-780 moves in to the Lifeline Mode.

FAILURE DETECTION

When there is any failure on the OA-780, Lifeline software detects the same, and switches to Lifeline Mode. The Lifeline ensures that remote management access is always available.

FAILURE NOTIFICATION

When there is a failure on the OA-780, and it switches to the Lifeline mode, a notification is sent out via Syslog and SNMP.

SYSLOG

The failures which cause the OA-780 to switch to Lifeline are critical, and appropriate high level syslog messages are generated. If syslog is configured for remote notification, then activation of Lifeline Mode will be indicated to remote system administrator within a few seconds. This notification is repeated periodically and contains detailed information about the failure.

SNMP

When Lifeline Mode is enabled, SNMP traps are sent, according to configuration, indicating the failure.

INTERFACE CARDS THAT ARE CURRENTLY SUPPORTED

T1 or E1 line cards - all L2 encapsulation protocols available on the T1 or E1 ports in Normal Mode are supported in Lifeline Mode viz. HDLC, PPP and Frame Relay, and L2-GE (Layer 2) line cards.

FUNCTIONALITY AVAILABLE IN LIFELINE MODE

The following functions are available when OA-780 is operating in the Lifeline Mode:

- System access to the management interface
- Diagnosis of failure that caused activation of Lifeline Mode
- Edit/Save system configuration
- Package Manager functionality: Software upgrade/downgrade, etc.
- System recovery and restart commands.

No control plane functions such as routing protocols, and no data plane functions such as packet forwarding and firewall are available when the OA-780 is operating in the Lifeline Mode.

ROUTING CONSIDERATIONS IN LIFELINE MODE

All dynamic routing information is lost when there is a failure on the OA-780.

In this environment, it may be impossible to reach the system remotely from multiple hops away in the network. The Lifeline Agent caches the dynamic/static routing information during the Normal Mode of operation and uses this to provide reachability in Lifeline Mode. However, static routing or additional configuration may be required on the next hop router from the OA-780 system or other routers on the path to the remote administrator. The Command Line Interface (CLI) allows the configuration of additional routing information, that can be used when the system goes to the Lifeline mode.

OPERATION OF OA-780 IN LIFELINE MODE

When there is a failure on the OA-780 and it switches to the Lifeline Mode, remote **in-band access** of the system is possible. This is an exclusive feature of the OA-780. It enables the administrator to access the system using the same network interface and the same IP address, which is in use when the system was operating normally.

In addition to this, **out-of-band access** is also provided through the analog modem built into the front panel of the OA-780 system. This feature is also not available on most devices as they do not have dedicated hardware resources to manage the device. In those that have separate control plane and data plane, external modems are used on the console port - innately reducing the reliability of out-of-band access drastically; an aspect that is crucial in times of emergency.

CLI COMMANDS

CLI ENHANCEMENTS

All existing CLI functions are available in Lifeline Mode. Thus all configure, show and action (such as clear) commands will be available. However, the success of these commands execution will vary widely depending upon the failed vs running software components.

The configuration commands will allow you to update and save the running and startup configuration of the system (potentially with the intention of repairing the failure that caused the system to go in to Lifeline Mode).

SPECIAL LIFELINE PROMPT

When the OA-780 is in the Lifeline Mode, the CLI prompt changes from

```
hostname#
```

to

```
Lifeline hostname#
```

TO ENABLE/DISABLE LIFELINE

Command (in CM)	Description
<code>lifeline {enable disable}</code>	This command is used to enable or disable Lifeline functionality. By default, this is enabled.

EXAMPLE

```
ALU(config)# lifeline enable
```

```
ALU(config)# lifeline disable
```

To CONFIGURE A STATIC ROUTE FOR LIFELINE MANAGEMENT STATION ACCESSIBILITY

This command adds a special Lifeline static route, which allows you to configure a route to a management station well-known to you. This is used during Lifeline only. When the OA-780 is in Lifeline mode, the Lifeline Agent will add this route to its local **RIB**, which ensures that a route exists to the management station.

Command (in CM)	Description
<pre>lifeline ip route <destination ip-address subnet-mask> <destination ip-address/ prefix-length> <next-hop-ip- address> <interface-name> <slot/port> [<1-255>]</pre>	This command is used to add a pre-configured route for Lifeline Mode.



Note: You must ensure that this route is reasonable and correct, and that other routers along the route path chosen are willing to handle the routing as well. This route is similar to a default static route. The interface used for forwarding packets via this route must be one of the line cards that support lifeline. See [“Interface Cards that are Currently Supported”](#)

EXAMPLE

```
ALU(config)# lifeline ip route 20.20.20.20/24 192.168.0.1
255.255.255.255 203.121.10.1 Serial 0/0:0 10
```

LIFELINE SHOW COMMANDS

Command (in Lifeline Mode)	Description
<code>show lifeline</code>	This command displays the following: <ul style="list-style-type: none"> • Failure that caused the OA-780 to switch to Lifeline Mode. • Static Lifeline routes configured.
<code>show lifeline ip route slot <0-7></code>	This command displays all the routes that are cached by the Lifeline Agent for the card in the slot specified.

EXAMPLE

```
Lifeline ALU(config)# show lifeline
```

```
Currently in Lifeline because: Services Engine removed from slot 7
```

```
Lifeline routes configured:
```

Destination	Mask	Gateway	Interface	Wt
10.91.2.0	255.255.255.0	0.0.0.0	Serial4/0:2	1

```
Lifeline ALU(config)# show lifeline ip route slot 4
```

```
Showing Lifeline IP routes for slot 4/0:2
```

```
Codes: R - RIP, O - OSPF, C - connected
```

```
S - static, M - mcstatic, B - BGP, A - ASE
```

```
IA - OSPF inter area route, E1 - OSPF external type 1 route,
```

```
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
```

```
N2 - OSPF NSSA external type 2 route
```

```
* - candidate default route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/22 is subnetted, 1 subnet 10.91.0.0 [0/0] is directly connected,
GigabitEthernet7/1
```

To Exit Lifeline Mode

Command (in Lifeline Mode)	Description
<code>lifeline exit</code>	This command is used to exit Lifeline Mode.

EXAMPLE

```
Lifeline ALU# lifeline exit
```

RECOVERY FROM LIFELINE MODE TO NORMAL MODE

The first indication of the OA 780 Lifeline mode is the change in CLI prompt.

```
Lifeline hostname#
```

On seeing this prompt, you should issue the '**show lifeline**' command, which will display the reason for the failure.

Based on the failure in the OA-780, which caused it to go into the Lifeline Mode, specific action has to be taken to repair corresponding to the faults so the OA-780 can be restored to Normal Mode.

LIFELINE CONFIGURATION SCENARIO

Connect the equipment according to the diagram show below. The IP addresses shown are representative and could be changed, however they must match the configuration on the OA-780 and PE router devices.

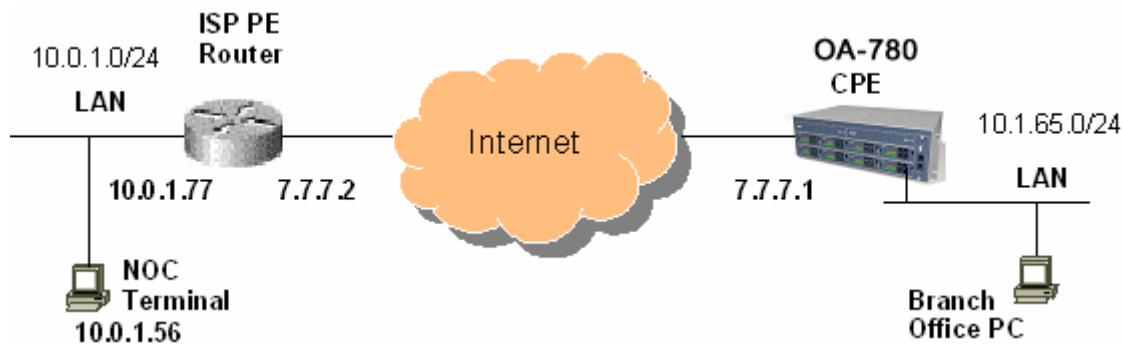


Figure 93: Lifeline Configuration Scenario

The following startup-configuration corresponds to the IP addresses shown in the equipment connection diagram above.

OA-780 (CPE Router):

```
!
! NVRAM config last updated at 06:31:57 GMT Tue Nov 15 2005
from line 0
!
! Statlog Configuration
!
logging on
logging buffered priority 6
logging buffered size 128
logging console 6
logging system 6
logging remote 10.0.1.56 port 514 priority 5 - (Syslog to NOC
terminal)

service timestamps log
!
! Chassis manager configuration
!
http enable
ssh enable
telnet enable - (telnet is enabled for remote access)
!
! SNMP Configurations
!
snmp system contact user1 user1@alcatel-lucent.com
snmp system location Alcatel-Lucent, Calabasas
```



```

!
aludb enable
aludb user user1 password encrypted
202cb962ac59075b964b07152d234b70
aludb usb address 10.1.1.254/24
!
aaa services
!
username user1 password 5 7d077f716c9a40f5660456534922464f
!
controller T1 4/0 - (T1 card is in slot 4 here)
no shutdown
channel-group 0 timeslots 1-24 -(T1 Interface defined)
top
!
controller T1 4/1
top
!
controller T1 4/2
top
!
controller T1 4/3
top
!
!
interface Serial4/0:0
!Note: Any PPP/Frame-Relay configuration currently does not
apply
ip address 7.7.7.1/24 - (IP address of T1 WAN interface)
encapsulation hdlc - (Encapsulation is set to HDLC)
no shutdown
top
!
interface GigabitEthernet7/0
ip address 172.16.0.3/16 (Branch office LAN (optional))
no shutdown
top
!
interface GigabitEthernet7/1
shutdown
top
!
!
ip route 0.0.0.0/0 7.7.7.2 (Routing to NOC terminal via PE)
!
!
! Filter Policy configuration
!
!

!QoS Configuration
!
line vty 4
transport input none

```

```
!  
line con 0  
!  
end
```

Part 10 Appendices



Appendix A Well Defined Port Numbers for Services

Sl. No.	Name	Protocol Type	Description	RFCs/References
1	tcpmux	1/tcp/udp	TCP port service multiplexer	
2	rje	5/tcp/udp	Remote Job Entry	
3	echo	7/tcp/udp	Echo	347
4	discard	9/tcp/udp	Discard	348
5	systat	11/tcp/udp		
6	daytime	13/tcp/udp	Daytime	867
7	qotd	17/tcp/udp	Quote	
8	msh	18/tcp/udp	Message Send Protocol	
9	chargen	19/tcp/udp	Character Generator	364
10	ftp-data	20/tcp/udp	File Transfer Protocol - Data for passive connection	959
11	ftp	21/tcp/udp	FTP (control)	959
12	ssh	22/tcp/udp	SSH remote login protocol	Internet Drafts
13	telnet	23/tcp/udp	Telnet	854
14	smtp	25/tcp/udp	Simple Mail Transfer Protocol	821
15	time	37/tcp/udp	Timeserver	
16	rlp	39/tcp/udp	Resource Location	
17	name server	42/tcp/udp	Name Server	
18	nic name	43/tcp/udp	whois	
19	tacacs	49/tcp/udp	TACACS	
20	re-mail-chk	50/tcp/udp	Remote Mail Checking Protocol	
21	DNS	53/tcp/udp	Domain Name Server	1035, 1183, 2535, 1712, 1886, 1876, 2065, 2053, 2538, 2671
22	whois++	63/tcp/udp		

Sl. No.	Name	Protocol Type	Description	RFCs/ References
23	bootps	67/tcp/udp	Bootstrap Protocol Server	
24	bootpc	68/tcp/udp	Bootstrap Protocol Client	
25	tftp	69/tcp/udp	Trivial File Transfer	783, 1350
26	gopher	70/tcp/udp	Gopher	1436
27	netrjs-1	71/tcp/udp	Remote Job Service	
28	netrjs-2	72/tcp/udp	Remote Job Service	
29	netrjs-3	73/tcp/udp	Remote Job Service	
30	netrjs-4	74/tcp/udp	Remote Job Service	
31	finger	79/tcp/udp	Finger	742,1288
32	HTTP	80/tcp/udp	www HTTP	2616
33	kerberos	88/tcp/udp	Kerberos v5	
34	supdup	95/tcp/udp		
35	hostname	101/tcp/udp	Usually from sri-nic	
36	iso-tsap	102/tcp	Part of ISODE.	
37	csnet-ns	105/tcp/udp	Also used by CSO name server	
38	3com-tsmux	106/tcp/udp	Poppassd	
39	rtelnet	107/tcp/udp	Remote Telnet	
40	pop2	109/tcp/udp	POP version 2	
41	POP3	tcp/110	Post Office Protocol V3	1939,1957
42	sunrpc	111/tcp/udp	RPC 4.0 portmapper TCP	
43	auth	113/tcp/udp	Authentication tap ident	
44	sftp	115/tcp/udp		
45	uucp-path	117/tcp/udp		
46	nntp	119/tcp/udp		
47	ntp	123/tcp	Network Time Protocol	
48	netbios-ns	137/tcp/udp	NETBIOS Name Service	
49	netbios-dgm	138/tcp/udp	NETBIOS Datagram Service	
50	SMB/Netbios	139/tcp/udp	NETBIOS	Internet Drafts
51	imap2	143/tcp/udp	Interim Mail Access Proto v2	
52	snmp	161/udp	Simple Network Mgmt Protocol	Internet Drafts

Sl. No.	Name	Protocol Type	Description	RFCs/ References
53	snmp-trap	162/udp	SNMP-Trap	Internet Drafts
54	cmip-man	163/tcp/udp	ISO mgmt over IP (CMOT)	
55	cmip-agent	164/tcp/udp		
56	mailq	174/tcp/udp	MAILQ	
57	xdmcp	177/tcp/udp	X Display Mgr. Control Proto	
58	nextstep	178/tcp/udp	NeXTStep window / NextStep server	
59	bgp	179/tcp	Border Gateway Protocol	
60	prospero	191/tcp/udp	Cliff Neuman's Prospero	
61	irc	194/tcp/udp	Internet Relay Chat	
62	smux	199/tcp/udp	SNMP Unix Multiplexer	
63	at-rtmp	201/tcp/udp	AppleTalk routing	
64	at-nbp	202/tcp/udp	AppleTalk name binding	
65	at-echo	204/tcp/udp	AppleTalk echo	
66	at-zis	206/tcp/udp	AppleTalk zone information	
67	qmtip	209/tcp/udp	Quick Mail Transfer Protocol	
68	z39.50210	210/tcp/udp	NISO Z39.50 database	
69	ipx	213/tcp/udp	IPX	
70	imap3	220/tcp/udp	Interactive Mail Access	
71	link	245/tcp/udp	ttylink	
72	fatserv	347/tcp/udp	Fatmen Server	
73	rsvp_tunnel	363/tcp/udp		
74	rpc2portmap	369/tcp/udp	Coda portmapper	
75	codaaauth2	370/tcp/udp	Coda authentication server	
76	ulistproc	372/tcp/udp	UNIX Listserv	
77	ldap	389/tcp/udp		
78	svrloc	427/tcp/udp	Server Location Protocol	
79	mobile ip-agent	434/tcp/udp		
80	mobile ip-agent	435/tcp/udp		
81	https	443/tcp/udp	MCom	

Sl. No.	Name	Protocol Type	Description	RFCs/ References
82	snpp	444/tcp/udp	Simple Network Paging Protocol	
83	microsoft-ds	445/tcp/udp	SMB	Internet Drafts
84	kpasswd	464/tcp/udp	Kerberos "passwd"	
85	photuris	468/tcp/udp		
86	saft	487/tcp/udp	Simple Asynchronous File Transfer	
87	gss-http	488/tcp/udp		
88	pim-rp-disc	496/tcp/udp		
89	isakmp	500/tcp/udp		
90	iiop	535/tcp/udp		
91	gdomap	538/tcp/udp	GNUstep distributed objects	
92	dhcpv6-client	546/tcp/udp		
93	dhcpv6-server	547/tcp/udp		
94	rtsp	554/tcp/udp	Real Time Stream Control Protocol	
95	nntps	563/tcp/udp	NNTP over SSL	
96	whoami	565/tcp/udp		
97	submission	587/tcp/udp	mail message submission	
98	npmp-local	610/tcp/udp	npmp-local / DQS	
99	npmp-gui	611/tcp/udp	npmp-gui / DQS	
100	hmmp-ind	612/tcp/udp	HMMP Indication / DQS	
101	ipp	631/tcp/udp	Internet Printing Protocol	
102	ldaps	636/tcp/udp	LDAP over SSL	
103	acap	674/tcp/udp		
104	ha-cluster	694/tcp/udp	Heartbeat HA-cluster	
105	kerberos-adm	749/tcp/udp	Kerberos 'kadmin' (v5)	
106	kerberos-iv	750/tcp/udp	kerberos4 kerberos-sec kdc	
107	webster	765/tcp/udp	Network dictionary	
108	phonebook	767/tcp/udp	Network phonebook	
109	rsync	873/tcp/udp	rsync	

Sl. No.	Name	Protocol Type	Description	RFCs/ References
110	telnets	992/tcp/udp		
111	imaps	993/tcp/udp	IMAP over SSL	
112	ircs	994/tcp/udp		
113	pop3s	995/tcp/udp	POP-3 over SSL	
114	socks	1080/tcp/udp	socks proxy server	
115	bvcontrol	1236/tcp/udp	Daniel J. Walsh, Gracilis Packeten remote config server	
116	h323hostcalls c	1300/tcp/udp	H323 Host Call Secure	
117	ms-sql-s	1433/tcp/udp	Microsoft-SQL-Server	
118	ms-sql-m	1434/tcp/udp	Microsoft-SQL-Monitor	
119	ica	1494/tcp/udp	Citrix ICA Client	
120	wins	1512/tcp/udp	Microsoft's Windows Internet Name Service	
121	ingreslock	1524/tcp/udp		
122	prospero-np	1525/tcp/udp	Prospero non-privileged	
123	datametrics	1645/tcp/udp	Old radius entry	
124	sa-msg-port	1646/tcp/udp	sa-msg-port / old radacct entry	
125	kermit	1649/tcp/udp		
126	l2tp	1701/tcp/udp	l2f	
127	h323gatedisc	1718/tcp/udp		
128	h323gatestat	1719/tcp/udp		
129	h323hostcall	1720/tcp/udp		
130	tftp-mcast	1758/tcp/udp		
131	mtftp	1759 udp		
132	hello	1789/tcp/udp		
133	radius	1812/tcp/udp	Radius	
134	radius-acct	1813/tcp/udp	Radius Accounting	
135	mtp	1911/tcp/udp		

Sl. No.	Name	Protocol Type	Description	RFCs/ References
136	hsrp	1985/tcp/udp	Cisco Hot Standby Router Protocol	
137	license daemon	1986/tcp/udp		
138	gdp-port	1997/tcp/udp	Cisco Gateway Discovery Protocol	
139	nfs	2049/tcp/udp	nfsd	
140	zephyr-srv	2102/tcp/udp	Zephyr server	
141	zephyr-clt	2103/tcp/udp	Zephyr serv-hm connection	
142	zephyr-hm	2104/tcp/udp	Zephyr hostmanager	
143	cvspserver	2401/tcp/udp	CVS client/server operations	
144	venus	2430/tcp/udp	Venus callback/wbc interface	
145	venus-se	2431/tcp/udp	udp sftp side effect	
146	codasrv	2432/tcp/udp	server port	
147	codasrv-se	2433/tcp/udp	udp sftp side effectQ	
148	hpstgmgr	2600/tcp/udp	HPSTGMGR	
149	discp-client	2601/tcp/udp	discp client	
150	discp-server	2602/tcp/udp	discp server	
151	servicemeter	2603/tcp/udp	Service Meter	
152	nsc-ccs	2604/tcp/udp	NSC CCS	
153	nsc-posa	2605/tcp/udp	NSC POSA	
154	netmon	2606/tcp/udp	Dell Netmon	
155	corbaloc	2809/tcp	CORBA naming service locator	
156	icpv2	3130/tcp/udp	Internet Cache Protocol V2 (Squid)	
157	mysql	3306/tcp/udp	MySQL	
158	trnsprntproxy	3346/tcp/udp	Transparent Proxy	
159	pxe	4011/udp	PXE server	
160	rwhois	4321/tcp/udp	Remote Who Is	
161	krb52	4444/tcp/udp	Kerberos 5 to 4 ticket xlator	
162	rfe	5002/tcp/udp	Radio Free Ethernet	

Sl. No.	Name	Protocol Type	Description	RFCs/ References
163	cfengine	5308/tcp/udp	CFEngine	
164	cvsup	5999/tcp/udp	CVSup file transfer/John Polstra/FreeBSD	
165	x11	6000/tcp	The X Window System	
166	afs3- fileserver	7000/tcp/udp	File server itself	
167	afs3-callback	7001/tcp/udp	Callbacks to cache managers	
168	afs3-prserver	7002/tcp/udp	Users and groups database	
169	afs3-vlserver	7003/tcp/udp	Volume location database	
170	afs3-kaserver	7004/tcp/udp	AFS/Kerberos authentication service	
171	afs3-volser	7005/tcp/udp	Volume management server	
172	afs3-errors	7006/tcp/udp	Error interpretation service	
173	afs3-bos	7007/tcp/udp	Basic overseer process	
174	afs3-update	7008/tcp/udp	Server-to-server updater	
175	afs3-rmtsys	7009/tcp/udp	Remote cache manager service	
176	sd	9876/tcp/udp	Session Director	
177	amanda	10080/tcp/udp	amanda backup services	
178	pgpkeyserver	11371/tcp/udp	PGP/GPG public keyserver	
179	h323callsigalt	11720/tcp/udp	H323 Call Signal Alternate	
180	bprd	13720/tcp/udp	BPRD (VERITAS NetBackup)	
181	bpdbm	13721/tcp/udp	BPDBM (VERITAS NetBackup)	
182	bpjava-msvc	13722/tcp/udp	BP Java MSVC Protocol	
183	vALU	13724/tcp/udp	Veritas Network Utility	
184	bpcd	13782/tcp/udp	VERITAS NetBackup	
185	vopied	13783/tcp/udp	VOPIED Protocol	
186	wnn6	22273/tcp/udp	wnn4	
187	quake	26000/tcp/udp		
188	wnn6-ds	26208/tcp/udp		
189	traceroute	33434/tcp/udp		

Sl. No.	Name	Protocol Type	Description	RFCs/ References
190	tfido	60177/tcp/udp	lfmail	
200	fido	60179/tcp/udp	lfmail	

Appendix B RFCs Supported by OA-700

AAA AUTHENTICATION

RFC 2865 Remote Authentication Dial-in User Service (RADIUS)
RFC 3579 Dot1x extensions to RADIUS

SNMP

SNMPv1 is defined in RFC 1157
SNMPv2c is defined in several RFC's. RFC 2578-2580, 3416-3418
SNMPv3 is defined by several RFC's in RFC 2576, 3410-3415

MANAGEMENT

SSH V3 compliance
RFC 4250 RFC 4251
RFC 4252 RFC 4253
RFC 4254 RFC 4256
RFC 4335 RFC 4344
RFC 4345
RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol

VRRP

RFC 3768

LAN

802.1D-2004 - Spanning Tree
802.1X - Port Based Network Access Control
802.1Q - Virtual LANs

WAN

RFC 1990 The PPP Multilink Protocol
RFC 2427 - Multiprotocol Interconnect over Frame Relay
RFC 2570 (FRF.16) UNI/NNI Multilink Frame Relay Interworking Implementation Agreement

LAYER-2 PROTOCOLS

PPP

RFC 1661: PPP
RFC 1662: PPP in HDLC-like framing
RFC 1332: IPCP
RFC 1334: PAP
RFC 1994: CHAP
RFC 3748: EAP

ROUTING

RIP

RFC 1058 (RIPv1)
RFC 2453 (RIPv2)

OSPF

RFC 2328: OSPFv2
RFC 1587: OSPF NSSA Option
RFC 1583: OSPF
RFC 3509: OSPF

BGP-4

- RFC 1771 BGP-4 Standard RFC
- RFC 2858 Multiprotocol Extensions to BGP-4
- RFC 2385 Protection of BGP Sessions via TCP MD5 Signature Option
- RFC 2439 BGP Route Flap Damping
- RFC 1997 BGP Communities Attribute
- RFC 1965 Autonomous Confederations for BGP [obsoleted by rfc3065]
- RFC 1745 BGP4/IDRP for IP – OSPF Interaction
- RFC 1657 Definitions of Managed Objects for BGP-4 using SMIv2
- RFC 2796 BGP Route Reflection An Alternative to full mesh IBGP
- RFC 2842 Capabilities Advertisement with BGP-4 [obsoleted by rfc3392]

IPSEC VPN

VPN

- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2411 IP Security Document Roadmap

Basic Protocols

- RFC 2402 IP Authentication Header
- RFC 2406 IP Encapsulating Security Payload (ESP)

Key Management

- RFC 2367 PF_KEY Key Management API, Version 2
- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 3706 - A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 2412 The OAKLEY Key Determination Protocol

- RFC 3715 - IPsec-Network Address Translation (NAT) Compatibility Requirements
- RFC 3947 - Negotiation of NAT-Traversal in the IKE
- RFC 3948 - UDP Encapsulation of IPsec ESP Packets

GRE

RFC 2784

QoS

RFC 2475 Architecture for Differentiated Service

RFC 2597 Assured Forwarding PHB Group

RFC 2598 Expedited Forwarding PHB

RFC 2697 Single Rate Three Color Marker

RFC 2698 Two Rate Three Color Marker



Note: All the above listed RFCs are applicable to both OA-780 and OA-740.

Appendix C Failure Scenarios While Installing OA-700 Software Package

FAILURE SCENARIOS WHILE INSTALLING

The OA-700 package install operation can fail in certain scenarios.

In case the package is being downloaded from a remote host, the download itself may fail with following error messages:

1. Unable to connect to remote host - This means that there is no route to remote host.
2. Access denied - When you do not have proper access permissions to access the package.
3. User name/Password incorrect - When you enter an incorrect user name or password.
4. Write Error in local file system - The package is transferred temporarily into the 'user area'. If there is no space in the user-area or if the USB is corrupted, then this error message is displayed.
5. Error in Connection Establishment - The connection to server timed-out. Maybe the remote server is not running.

In case the package is being taken from 'user area' or 'fpkey',

1. The error "<package> does not exist." is displayed if the package is not really there.
2. In case of fpkey, if it could not be mounted, then "Failed to mount Fpkey" is displayed.

The installation can also fail in the verification stage because of the following reasons:

1. If the package is not of proper format, then an error "Unrecognized format" is displayed. This can occur if you are using any other type of file (maybe a text file or a binary file, etc.). This can also occur if the package is corrupted.
2. The space required for the new package is calculated now. If it is not enough then, "Insufficient space to install new package" is displayed.
3. If the package set as default is already the default package then a message "<package> is already the default package" is displayed.
4. If you try to remove the default package, an error message "package is in use as default" is displayed.

Local backups can fail due to these reasons.

1. If the backup is being taken into fpkey and it cannot be mounted, then "Failed to mount Fpkey" is displayed.

2. If the file being backed-up already exists, then error message "File <backup-file> is already present" is displayed.

In case of remote backups, these errors can occur.

1. Unable to connect to remote host - This means that there is no route to remote host.
2. Access denied - This means that you do not have proper access permissions to backup the package in the given location.
3. User name/Password incorrect - Incorrect user name and password.
4. Write error at server side - There has been a write error at the remote site. Probably there was no space left.
5. Error in Connection Establishment - The connection to server timed-out. Maybe the remote server is not running.

Appendix D QoS Values and Mnemonics

DEFAULT VALUES FOR RANDOM-DETECT IP-PRECEDENCE

ip-precedence	Min-Threshold	Max-Threshold	Drop-Probability
0	50	150	10
1	60	160	10
2	70	170	10
3	80	180	10
4	90	190	10
5	100	200	10
6	110	210	10
7	120	220	10

DEFAULT VALUES FOR RANDOM-DETECT IP-DSCP

ip-precedence	Min-Threshold	Max-Threshold	Drop-Probability
0	50	150	10
1	50	150	10
2	50	150	10
3	50	150	10
4	50	150	10
5	50	150	10
6	50	150	10
7	50	150	10
8	50	150	10
9	50	150	10
10	50	150	10
11	50	150	10
12	40	120	10

ip-precedence	Min-Threshold	Max-Threshold	Drop-Probability
13	50	150	10
14	32	96	10
15	50	150	10
16	50	150	10
17	50	150	10
18	50	150	10
19	50	150	10
20	40	120	10
21	50	150	10
22	32	96	10
23	50	150	10
24	50	150	10
25	50	150	10
26	50	150	10
27	50	150	10
28	40	120	10
29	50	150	10
30	32	96	10
31	50	150	10
32	50	150	10
33	50	150	10
34	50	150	10
35	50	150	10
36	40	120	10
37	50	150	10
38	32	96	10
39	50	150	10
40	50	150	10
41	50	150	10
42	50	150	10
43	50	150	10

ip-precedence	Min-Threshold	Max-Threshold	Drop-Probability
44	50	150	10
45	50	150	10
46	50	150	10
47	50	150	10
48	50	150	10
49	50	150	10
50	50	150	10
51	50	150	10
52	50	150	10
53	50	150	10
54	50	150	10
55	50	150	10
56	50	150	10
57	50	150	10
58	50	150	10
59	50	150	10
60	50	150	10
61	50	150	10
62	50	150	10
63	50	150	10

IP-DSCP MNEMONICS

DSCP Mnemonics	Values
default	0
cs1	8
cs2	16
cs3	24
cs4	32
cs5	40
cs6	48
cs7	56
ef	46
af11	10
af12	12
af13	14
af21	18
af22	20
af23	22
af31	26
af32	28
af33	30
af41	34
af42	36
af43	38

IP-PRECEDENCE MNEMONICS

IP-Precedence Mnemonics	Values
routine	0
priority	1
immediate	2
flash	3
flash-override	4
critical	5
internet	6
network	7

ToS MNEMONICS

TOS Mnemonics	Values
min-delay	8
max-tput	4
max-reli	2
flash	1
normal	0

Appendix E IP Security Interoperability of OA-700

CONFIGURING IPSEC TUNNEL BETWEEN OA-700 AND CISCO 2621

The following scenario explains how to establish a IPsec tunnel between the OA-700 and Cisco 2621 router.

Topology:

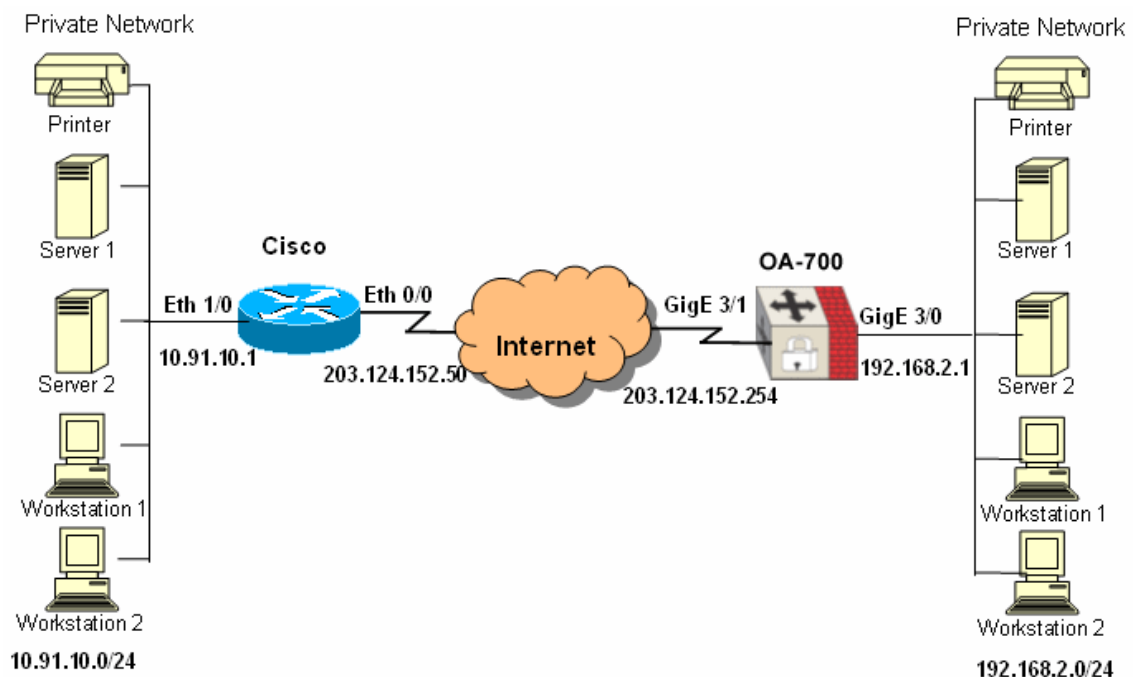


Figure 94: IPsec Interoperability Between OA-700 and Cisco 2621

The test network consists of router Cisco 2621 running a crypto image c2600-ik2s-mz.121-2.bin. The IPsec tunnel is created for the network 10.91.10.0/24 and 192.168.2.0/24 to communicate in a secure manner.

CONFIGURATION

CONFIGURING OA-700

Current Configuration:

```
!  
! Statlog Configuration  
!  
logging on  
logging console debugging  
logging os messages informational  
logging buffered priority 7  
logging buffered size 131072  
service timestamps log  
hostname ALU  
  
! Port Based VLAN Global Configurations!  
!  
! VLAN Table Static Configurations!  
!  
! Bridge Configuration  
!
```

IP address configured on the interface pointing the internal network:

```
interface GigabitEthernet3/0  
ip address 192.168.2.1/24  
no shutdown  
top  
!
```

IP address configured on the interface pointing the external network:

```
interface GigabitEthernet3/1  
ip address 203.124.152.254/24  
no shutdown  
top  
!
```

Default route pointing to the next hop:

```
ip route 0.0.0.0/0 203.124.152.50  
!
```

Match-list rule configured for selecting the local and remote network, which need to communicate:

```

match-list m1
 1 ip prefix 192.168.2.0/24 prefix 10.91.10.0/24
!
```

IKE key created for the remote peer:

```

crypto ike key Ty#$cH peer 203.124.152.50
```

IKE policy created for defining the proposal set:

```

crypto ike policy ALU1
  proposal md5-3des md5-des sha1-des sha1-3des
  pfs group2
  ipsec security-association lifetime seconds 28800
  lifetime seconds 3600
! Policy in Use (by 1 cryptomap/s)
```

Transform-set created for defining the proposal to be used for encryption:

```

crypto ipsec transform-set myset esp-md5-3des
! Transform-Set in Use (by 1 cryptomap/s)
```

Crypto map created pointing to the remote peer:

```

crypto map ALU ipsec-ike ALU1
  peer 203.124.152.50
  match m1
  transform-set myset
  pfs group2
! Applied to : GigabitEthernet3/1
!
```

Crypto map applied on the interface pointing to the external network:

```

interface GigabitEthernet3/1
  crypto map ALU
top
!
line vty 4
transport input none
!
line con 0
!
end
```

CONFIGURING CISCO 2621 ROUTER**Current Configuration:**

```
!  
version 12.1  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname Cisco  
!  
boot system flash c2600-ik2s-mz.121-2.bin  
enable secret 5 $1$N8vA$D65vf69j1Z1DokDLYJttX.  
enable password cisco  
!  
!  
memory-size iomem 15  
ip subnet-zero  
!  
lane client flush  
!
```

ISAKMP policy created, which confirms to the OA-700 IKE policy:

```
crypto isakmp policy 10  
encr 3des  
hash md5  
authentication pre-share  
group 2
```

ISAKMP key created, which is same as the IKE key in the OA-700:

```
crypto isakmp key Ty#$cH address 203.124.152.254  
!  
!  
!
```

Transform set created, which is used for data encryption:

```
crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

Crypto map applied pointing to the external IP address of the OA-700:

```

crypto map test 10 ipsec-isakmp
set peer 203.124.152.254
set transform-set myset
set pfs group2
match address 100
!
!
interface Ethernet0/0
ip address 203.124.152.50 255.255.255.0
no ip mroute-cache
crypto map test
!
interface Serial0/0
no ip address
no ip mroute-cache
no shutdown
no fair-queue
!
interface Ethernet1/0
ip address 10.91.10.1 255.255.255.0
no ip mroute-cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.124.152.254
no ip http server
!

```

Access-list created for allowing subnet-to-subnet communication through IPsec tunnel:

```

access-list 100 permit ip 10.91.10.0 0.0.0.255 192.168.2.0
0.0.0.255
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0
exec-timeout 0 0
password cisco
login
line vty 1 4
password cisco
login
!
end

```

VERIFICATION

On the OA-700, the tunnel can be verified by giving the command '**show crypto ipsec sa**'.

On the Cisco 2621 router, the same can be observed by issuing the following commands:

1. **show crypto isakmp sa**
2. **show crypto ipsec sa**
3. **show crypto engine**
4. **show crypto**

CONFIGURING IPSEC BETWEEN OA-700 AND SONICWALL (PRO 3060)

The following scenario explains how to establish a IPsec tunnel between the OA-700 system and Sonicwall.

Topology:

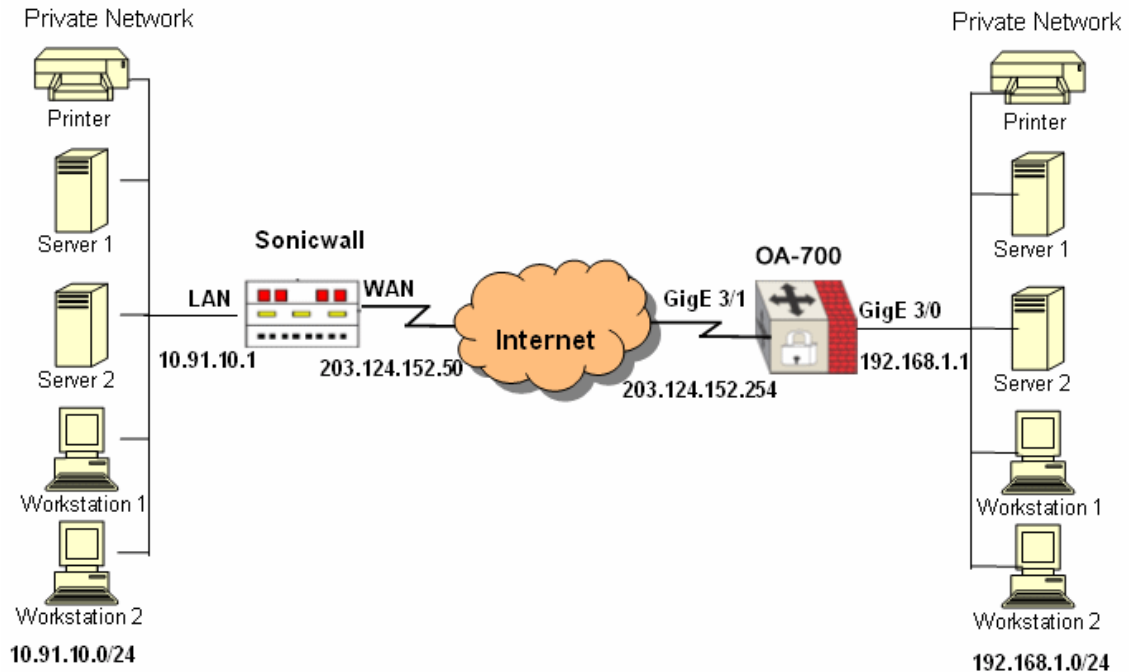


Figure 95: IPsec Interoperability Between OA-700 and Sonicwall PRO 3060

The above network shows the setup used to create a tunnel between Sonicwall and OA-700.

The tunnel is built to allow network behind the OA-700 gateway (192.168.1.0) to communicate with network behind Sonicwall (10.91.10.0). The IPsec tunnel hence built allows the networks to communicate with each other in a secure manner.

CONFIGURATION

CONFIGURING OA-700

Current Configuration:

```
!  
! NVRAM config last updated at 15:42:46 GMT Mon Jan 24 2000  
from line 0  
!  
  Statlog Configuration  
!  
statlog logging: enabled  
  console logging: level debugging  
  monitor logging: level debugging  
  os logging: level informational  
  buffer logging: level debugging  
  external server logging: level informational  
  
log buffer size:   (131072 bytes)  
  
log timestamp enabled  
!  
! Port Based VLAN Global Configurations!  
!  
! VLAN Table Static Configurations!  
!  
!  
! Bridge Configuration  
!  
!  
interface GigabitEthernet3/0  
  ip address 192.168.1.1/24  
!  
! Port Based VLAN Interface Configurations!  
  no shutdown  
!  
interface GigabitEthernet3/1  
  ip address 203.124.152.254/24  
!  
! Port Based VLAN Interface Configurations!  
  no shutdown  
!  
!  
ip route 0.0.0.0/0 203.124.152.50  
!  
!  
!
```

Match-list created for the two subnets to communicate with each other:

```
match-list m1  
1 ip prefix 192.168.1.0/24 prefix 10.91.10.0/24  
!
```


IKE policy configured:

```
crypto ike policy test
  proposal md5-des
  pfs group2
  ipsec security-association lifetime seconds 28800
  lifetime seconds 3600
```

IKE key created:

```
crypto ike key Ty#$cH peer 203.124.152.50
```

Transform-set created for encryption:

```
! Policy in Use (by 1 cryptomap/s)
crypto ipsec transform-set myset esp-md5-des
! Transform-Set in Use (by 1 cryptomap/s)
!
```

Crypto map created calling the IKE policy configured earlier:

```
crypto map mymap ipsec-ike test
  peer 203.124.152.50
  match m1
  transform-set myset
  pfs group1
```

Crypto map applied to the interface connected to public network:

```
! Applied to : GigabitEthernet3/1
interface GigabitEthernet3/1
  crypto map mymap
top
!
line vty 4
  transport input none
!
line con 0
!
end
```

CONFIGURING SONICWALL (PRO 3060)

Sonicwall software offers a Web Graphical User Interface (GUI), which enables you to configure the site-to-site IPsec tunnel. The steps are as given below.

Creating local network behind Sonicwall:

- Select **Network > Settings > Configure icon for LAN** to configure the internal network IP address. This internal network is called "localnet" behind the Sonicwall.

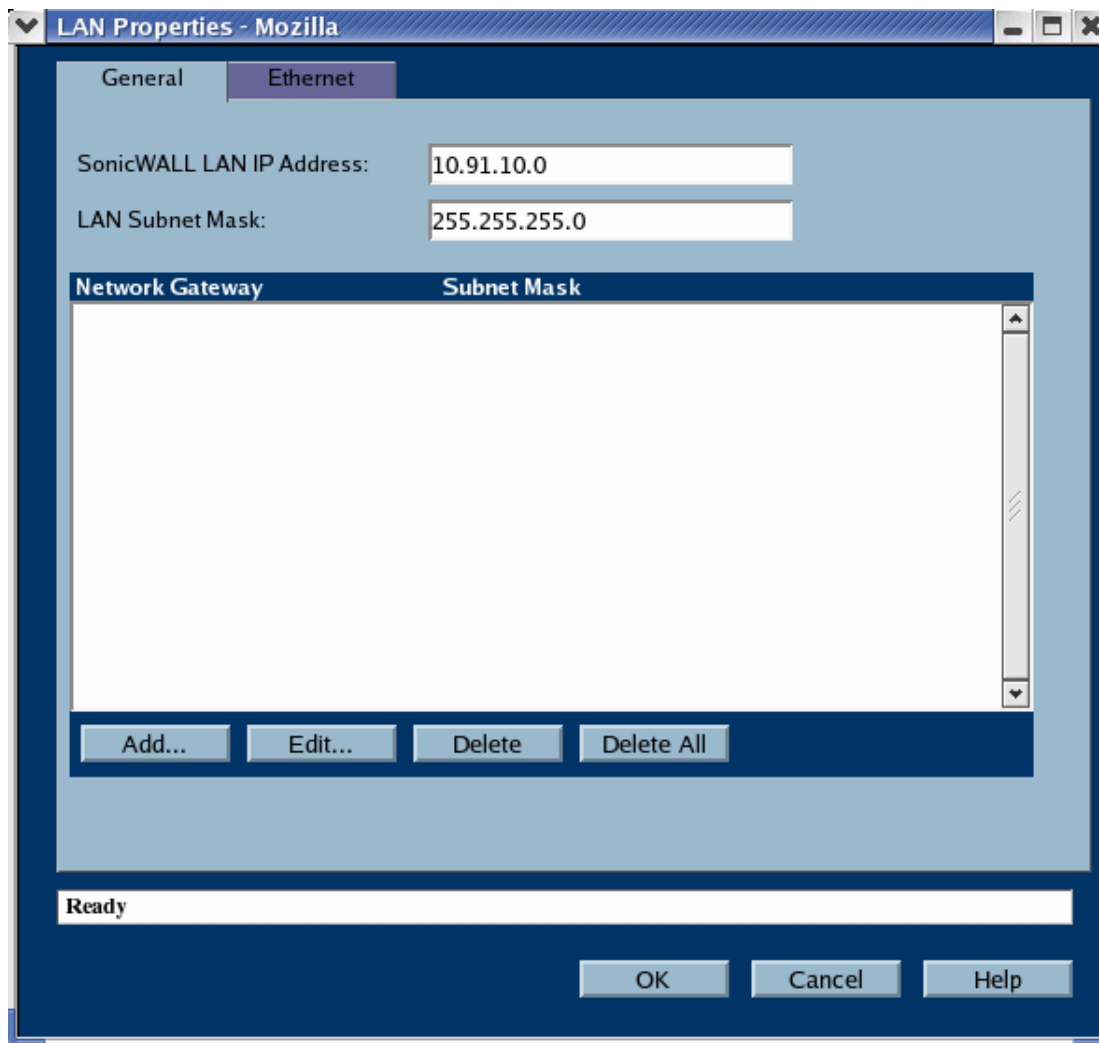


Figure 96: Configuring Local network behind Sonicwall

- Enter the local IP address and the Subnet Mask.

Creating External IP address for Sonicwall:

- Select **Network > Settings > Configure icon for WAN** to configure the external network IP address.

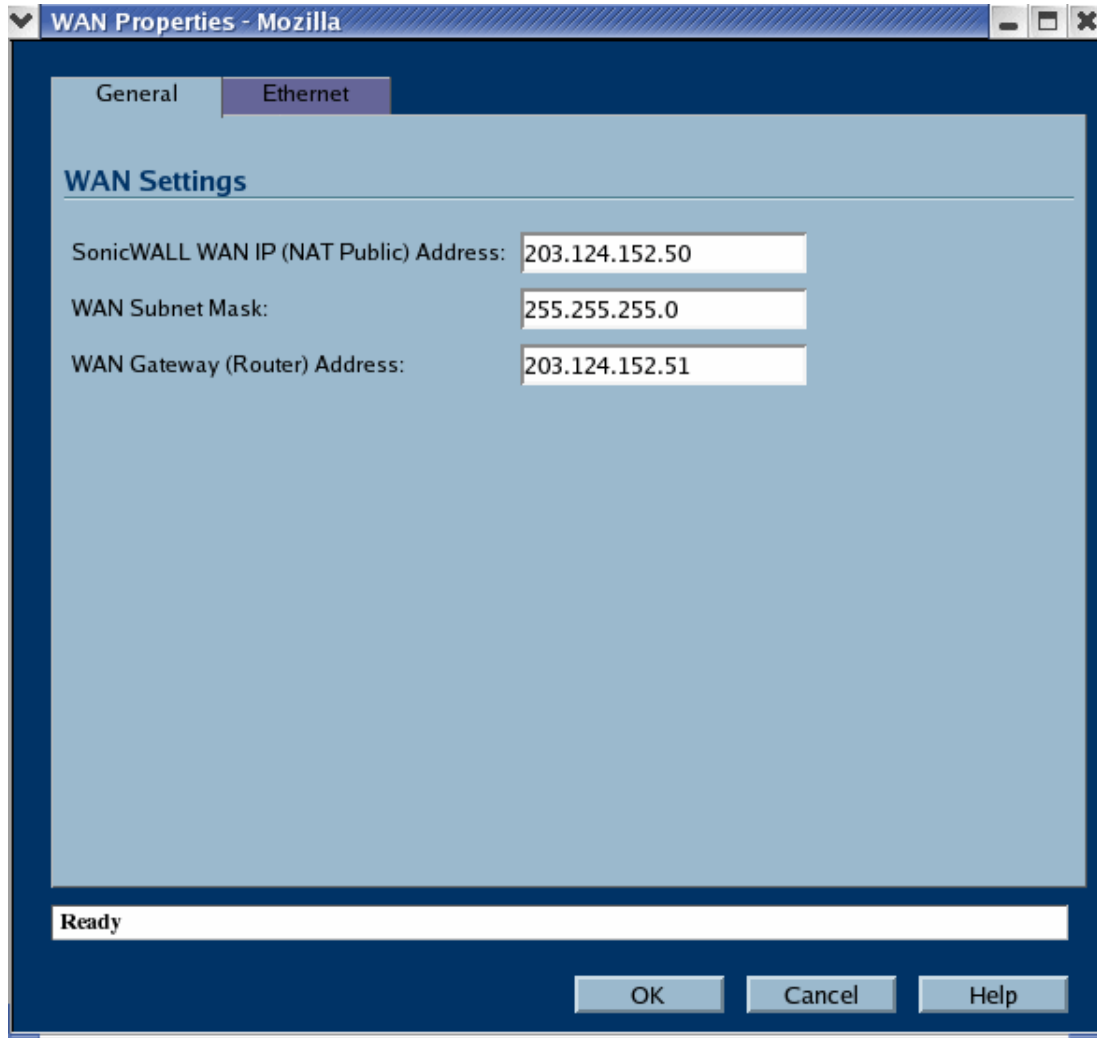


Figure 97: Configuring External IP Address for Sonicwall

- Enter the WAN IP address and the Subnet Mask.



Note: Reboot Sonicwall for the configured IP address to come into effect.

Configuring IPsec Tunnel on Sonicwall:

- Select **VPN > Settings > Add > General** to configure IPsec policy.

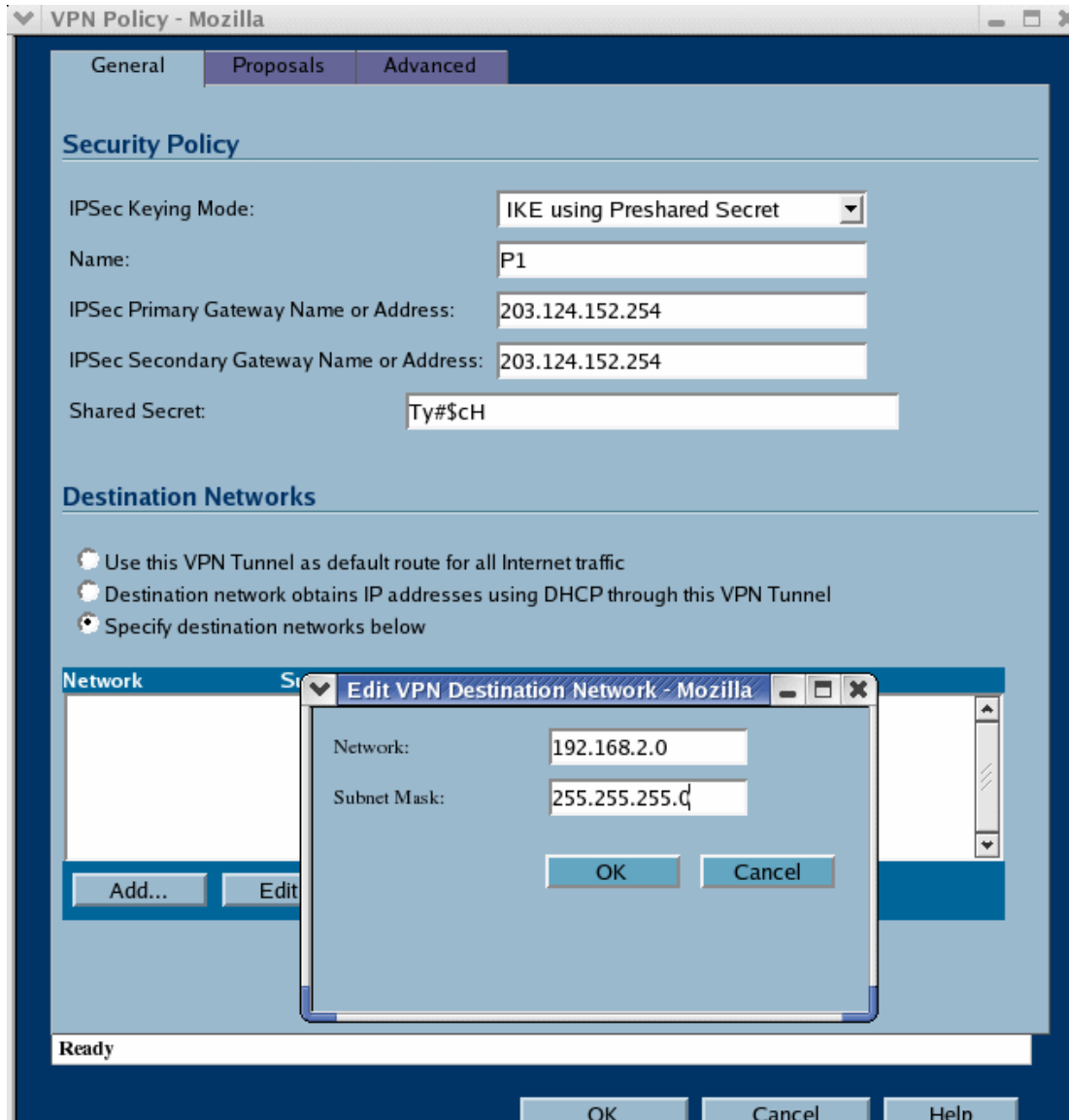


Figure 98: Configuring IPsec Policy and Destination Network

- Select the IPsec keying mode. Enter the policy name, peer IP address, key, and destination network.

- Select **VPN > Settings > Add > Proposals** to configure IPsec proposal.

The screenshot shows a web browser window titled "VPN Policy - Mozilla" with three tabs: "General", "Proposals", and "Advanced". The "Proposals" tab is active, and the "IKE (Phase 1) Proposal" section is expanded. Below it, the "IPsec (Phase 2) Proposal" section is also expanded. The configuration fields are as follows:

Section	Field	Value
IKE (Phase 1) Proposal	Exchange:	Main Mode
	DH Group:	Group 2
	Encryption:	3DES
	Authentication:	MD5
	Life Time (seconds):	28800
IPsec (Phase 2) Proposal	Protocol:	ESP
	Encryption:	3DES
	Authentication:	MD5
	<input checked="" type="checkbox"/> Enable Perfect Forward Secrecy	
	DH Group:	Group 2
	Life Time (seconds):	28800

At the bottom of the window, there is a status bar that says "Ready" and three buttons: "OK", "Cancel", and "Help".

Figure 99: Configuring IPsec Phase 1 and Phase 2 Proposals

- Select the appropriate algorithms for Phase 1 and Phase 2 Proposals.
- Enable PFS Group and enter the lifetime.

VERIFYING THE CONFIGURATION

The VPN configuration on the OA-700 can be verified by using the commands **'show crypto map'** and **'show crypto'**.

The tunnel setup on Sonicwall can be verified by viewing the Log page.

Appendix F Software Licenses and Acknowledgements

This section lists licenses for the public domain software used by this product:

- [Linux Kernel](#)
- [Intel Linux Device Driver Software](#)
- [PMC-Sierra Linux Device Driver Software](#)
- [Mindspeed Linux Device Driver Software](#)
- [eCos](#)
- [U-Boot](#)
- [Linux STP](#)
- [Paul's PPP Package](#)
- [DHCP](#)
- [tftp-hpa](#)
- [Net-SNMP](#)
- [OpenSSH](#)
- [ZEBRA CLI](#)
- [GNU Pth - The GNU Portable Threads](#)
- [TCP Proxy and Reassembly](#)
- [Strongswan IKE](#)
- [FreeBSD Crypto Library](#)
- [Snort](#)
- [Mbedthis AppWeb](#)
- [libxslt](#)
- [BusyBox](#)
- [iputils](#)
- [e2fsprogs](#)
- [InetUtils, gawk, GDB](#)
- [cURL](#)
- [PCRE](#)
- [MD5](#)

Licenses

- [GNU General Public License](#)
- [GNU Lesser General Public License](#)

LINUX KERNEL

Copyright (c) Linus Torvalds and others

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation version 2 of the License.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

INTEL LINUX DEVICE DRIVER SOFTWARE

Copyright(c) 1999 - 2004 Intel Corporation. All rights reserved.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

PMC-SIERRA LINUX DEVICE DRIVER SOFTWARE

COPYRIGHT (C) 2003 PMC-SIERRA, INC. ALL RIGHTS RESERVED.

Copyright (c) 1999 SBS Technologies Communications Products
(Formerly SciTech Inc.) All Rights Reserved

Unpublished Proprietary Source Code

This software embodies materials and concepts which are proprietary and confidential to PMC-Sierra, Inc.

PMC-Sierra distributes this software to its customers pursuant to the terms and conditions of the Device Driver Software License Agreement contained in the text file software.lic that is distributed along with the device driver software. This software can only be utilized if all terms and conditions of the Device Driver Software License Agreement are accepted. If there are any questions, concerns, or if the Device Driver Software License Agreement text file, software.lic, is missing please contact PMC-Sierra for assistance.

SBS Technologies Communications Products grants permission to copy and modify this software provided this copyright notice appears in all copies. SBS Technologies Communications Products does not warrant, guarantee and is not responsible for any results due to the use of this software. SBS Technologies Communications Products is not responsible for the accuracy, reliability or correctness of this software and any use of this software is solely at your own risk.

MINDSPEED LINUX DEVICE DRIVER SOFTWARE

Copyright (c) 1999 SBS Technologies Communications Products. (Formerly SciTech Inc.) All Rights Reserved. Unpublished Proprietary Source Code.

SBS Technologies Communications Products grants permission to copy and modify this software provided this copyright notice appears in all copies. SBS Technologies Communications Products does not warrant, guarantee and is not responsible for any results due to the use of this software. SBS Technologies Communications Products is not responsible for the accuracy, reliability or correctness of this software and any use of this software is solely at your own risk.

eCos

Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003 Red Hat, Inc.

Copyright (C) 2002, 2003 John Dallaway

Copyright (C) 2002, 2003 Nick Garnett

Copyright (C) 2002, 2003 Jonathan Larmour

Copyright (C) 2002, 2003 Andrew Lunn

Copyright (C) 2002, 2003 Gary Thomas

Copyright (C) 2002, 2003 Bart Veer

eCos is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 or (at your option) any later version.

eCos is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

U-BOOT

Copyright(C) 2000 - 2005 Wolfgang Denk, DENX Software Engineering, wd@denx.de.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

Note: The CREDIT file distributed with uboot source acknowledges all other Authors who have contributed to uboot source and have copyright on specific files.

LINUX STP

Authors: Lennert Buytenhek <buytenh@gnu.org>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

PAUL'S PPP PACKAGE

Paul's PPP Package is obtained from <http://ppp.samba.org>.

This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>), Paul Mackerras <paulus@samba.org>, and Gregory M. Christy. The MD5 implementation used in this product is based on RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

Office of Technology Transfer

Carnegie Mellon University

5000 Forbes Avenue

Alcatel-Lucent

Pittsburgh, PA 15213-3890
(412) 268-4387, fax: (412) 268-7395
tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>).

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1993-2002 Paul Mackerras. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment:

This product includes software developed by Paul Mackerras <paulus@samba.org>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1991 Gregory M. Christy. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Gregory M. Christy. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message- Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

DHCP

Copyright (c) 2004-2005 Internet Systems Consortium, Inc. ("ISC")

Copyright (c) 1995-2003 Internet Software Consortium. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of ISC, ISC DHCP, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY INTERNET SYSTEMS CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ISC OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

TFTP-HPA

Copyright (c) 1983, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION).

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NET-SNMP

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1988, 1989 by Carnegie Mellon University. All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1990 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1988, 1989, 1990 by Carnegie Mellon University

Copyright 1989 TGV, Incorporated

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and TGV not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU AND TGV DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU OR TGV BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OPENSSSH

OpenSSH is developed by the OpenBSD project. It contains components that are under a BSD license or a license more free than that. OpenSSH contains no GPL code.

The creator of SSH is Tau Ylonen ylo@cs.hut.fi

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland. All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

The 32-bit CRC compensation attack detector was contributed by CORE SDI S.A. under a BSD-style license.

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com> <<http://www.core-sdi.com>>

ssh-keyscan was contributed by David Mazieres under a BSD style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

One component of ssh source code is pulled from the original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some components of the software are provided under a standard 2-term BSD license with the copyright holders listed in each source file.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium. Todd C. Miller, Reyk Floeter, Chad Mynhier

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN

ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

Note: The CREDIT file distributed with OpenSSH source acknowledges all other Authors who have contributed to source and have copyright on specific files.

ZEBRA CLI

The CLI core module in this product uses the parser code from GNU Zebra.

Copyright (C) 1989 - 2002 Free Software Foundation, Inc.

Copyright (C) 1998 - 2000 Kunihiro Ishiguro

Copyright (C) 2003 Paul Jakma.

GNU Zebra is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2, or (at your option) any later version.

GNU Zebra is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

GNU PTH - THE GNU PORTABLE THREADS

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

A copy of the GNU Lesser General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/copyleft/lgpl.html>

TCP PROXY AND REASSEMBLY

Copyright (c) 1982, 1986, 1988, 1990, 1993, 1994, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

STRONGSWAN IKE

Copyright (C) 1997 Angelos D. Keromytis.

Copyright (C) 1998-2001 D. Hugh Redelmeier.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. See <<http://www.fsf.org/copyleft/gpl.txt>>.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

FREEBSD CRYPTO LIBRARY

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related:-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license including the GNU Public license.

SNORT

Copyright (C) 1998-2002 Martin Roesch <roesch@sourcefire.com>

Copyright (C) 2002-2003, Sourcefire, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

MBEDTHIS APPWEB

Copyright (c) 2003-2005 Mbedthis Software, LLC. All Rights Reserved.

Mbedthis and AppWeb are trademarks of Mbedthis Software, LLC. Other brands and their products are trademarks of their respective holders.

This software is licensed according to the provisions of GNU General Public License.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

Portions Copyright (c) The Apache Software Foundation, 2000-2003. This copyright applies to some documentation and portions of the URL security validation code in url.cpp. See the Apache HTTP Server license for details.

Portions Copyright (c) GoAhead Software Inc, 1995-2000. This copyright applies to portions of the Embedded Javascript Engine.

Portions Copyright (c) RSA Data Security, Inc. This copyright applies to the MD5 transformation routines.

LIBXSLT

Libxslt except Libxslt Copyright (C) 2001-2002 Daniel Veillard. All Rights Reserved.

Libxslt Copyright (C) 2001-2002 Thomas Broyer, Charlie Bozeman and Daniel Veillard.

All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the authors shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

BusyBox

BusyBox contains code contributed by many people in open source community. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License Version 2 only as published by the Free Software Foundation.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

Note: The AUTHORS file distributed with BusyBox source acknowledges all authors who have contributed to BusyBox source and have copyright on specific files.

IPUTILS

iputils is a collection of basic networking utilities.

Some files have the following license:

Copyright (c) Alexey Kuznetsov and others.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

Some files have the following license.

Copyright (c) 1983 Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some files have the following license:

Rdisc (this program) was developed by Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Rdisc without charge, and they may freely distribute it.

RDISC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Rdisc is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY RDISC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

E2FSPROGS

Copyright (c) Theodore Ts'o and others.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

Files under lib/uid directory have the following BSD style license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

INETUTILS, GAWK, GDB

Copyright (c) Free Software Foundation, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is provided at the end of this chapter, and also available from <http://www.gnu.org/licenses/gpl.html>

cURL

Copyright (c) 1996 - 2007, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

PCRE

Copyright (c) 1997-2003 University of Cambridge

Written by: Philip Hazel <ph10@cam.ac.uk>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MD5

RSA Data Security, Inc., MD5 message-digest algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based

on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept

this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
```

```
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program  
`Gnomovision' (which makes passes at compilers) written by James Hacker.
```

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

* a) The modified work must itself be a software library.

* b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

* c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

* d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- * a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- * b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

- * c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

- * d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- * e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- * a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

- * b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this.

Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

