OmniAccess 700 Web GUI Users 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

Part No: 060222-00, Rev A

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.

Not withstanding 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

List of Figures

CHAPTER 1

PREFACE

ABOUT THIS GUIDE

This chapter describes how to perform the basic configuration of the OmniAccess 700 (OA-700 - OA 740/OA 780) using the Web Graphical User Interface (GUI) tool - Unified Services Gateway Configuration Manager (USGM).

The guide contains procedures for configuring interfaces, routing parameters, SNMP, syslog parameters, time range, lists and match lists, traffic classification, filter and firewall, IPSec policy, QoS, and various other features.

CHAPTER DESCRIPTION

This section explains the objectives, intended audience, and organization of the USGM Web GUI User Guide.

AUDIENCE

This book is intended for networking professionals who are responsible for designing, implementing, and managing enterprise networks. This book aims to provide unique technologies and effective practices that deliver value on the networking perspective.

The user is expected to have, at minimum, an introductory understanding of the following:

- Networking applications
- Telecommunication networks
- Hardware configuration

DOCUMENT ORGANIZATION

This user guide is organized into the following chapters:

Chapter 1 Preface provides a brief introdcution on the Web GUI Users Guide.

Chapter 2 GUI Layout provides a brief description of the GUI layout and its components.

Chapter 3 Configure allows you to perform configurations for Interfaces, Firewalls, VPNs, Routing, and other tasks.

Chapter 4 Maintenance allows you to perform system maintenance tasks like Software and Flash OS upgrade, Lifeline, among others.

Chapter 5 Monitor lets you view statistics of various features configured on the OA-700 system.

DOCUMENT CONVENTIONS

Item	Convention
Selecting a menu item	Configure > System Information
Menu items, button names, and field names	**Boldface** font
Arguments for which the user has to supply values	*Italics* font

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

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 CLI Configuration 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 comments about this book, please enter them through the feedback link on the Alcatel-Lucent Website. We will use your feedback in our plans to improve the documentation.

CHAPTER 2

GUI LAYOUT AND LOGGING ON TO USGM

This chapter provides a brief description of the USGM (Unified Services Gateway Configuration Manager) Web GUI layout and its components.

USGM WEB GUI TOOL

The USGM Web GUI tool is an easy-to-use interface that helps you configure your OA-700 system without using the Command Line Interface (CLI). You can configure the following features, among others, using this tool:

- Interfaces
- Routing
- Firewall (NAT, Filters)
- IPSec VPN
- IDS/IPS
- QoS
- Software Upgrade

You can also view statistics pertaining various features configured on the system.

For quick and easy configuration of some of the features like Firewalls, VPN IPSec, and Quality of Service, USGM provides wizards based configuration - sequenced screens that enables you to complete a task in defined steps.

SYSTEM REQUIREMENTS

The USGM tool is supported on following browsers:

- Internet Explorer 6.0 or later
- Netscape 7.0 or later
- Mozilla 1.7 or later
- Mozilla Firefox 1.0 or later

LAUNCHING THE GUI

Follow the procedure given below to access and configure the OA-700 system through the USGM.

Step 1: Enable HTTP/HTTPS to access the OA-700 using HTT/HTTPSP through a web browser after being authenticated. By default, the access is disabled.

Note: To enable HTTP service on your system, enter the following command in the configuration mode.

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

To enable HTTPS service on your system, enter the following command in the configuration mode.

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

Step 2: Configure IP address for an interface.

Note: To configure IP address for a given interface, follow Step 1 through Step 10 detailed in the **"Accessing OA-780/OA-740 System Through CLI"** section of the OA-780/ OA-740 Hardware Installation Guide.

Step 3: Open a web browser in your PC.

Step 4: In the address bar/field, type the IP address of the interface and press the **Enter**.

This launches the USGM with the login page.

LOGON TO USGM

The web interface is launched with the login page.

Step 1: Enter the user name and the password in the **Username** and **Password** fields.
Use the default '**superadmin**' user account or use the AAA user name and password configured using the CLI to login to USGM.
(For more information on configuring AAA user name and password, refer the note below.)

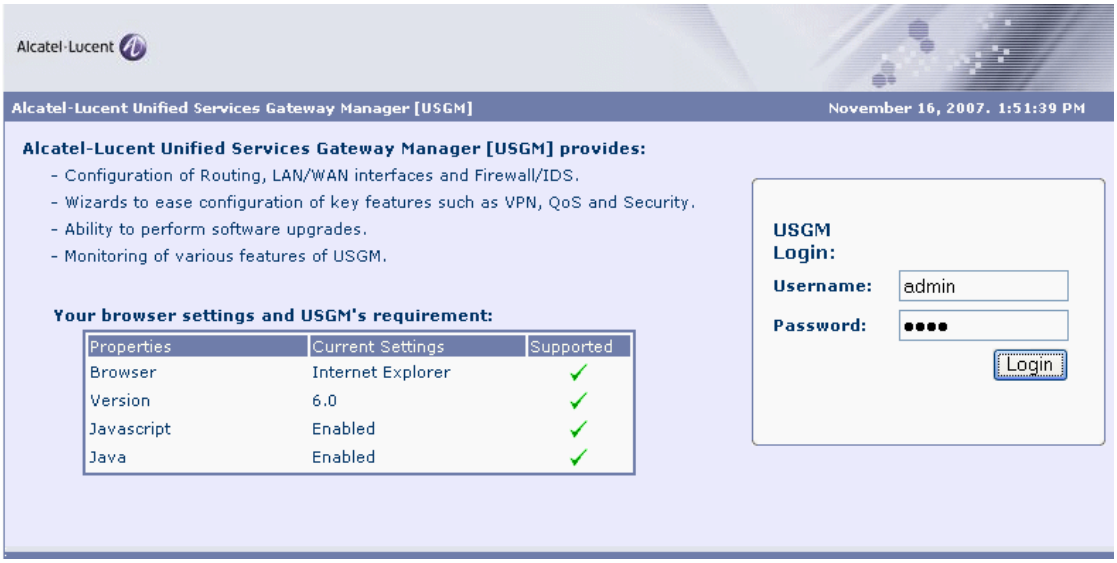


Figure 1: Logon to USGM

Note: To enable AAA services on your system, enter the command **aaa services** in configuration mode.

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

Establish authentication to new users by configuring new user accounts. To configure new user account, use the following command:

username <*user-name*> {**password** [**5**] <*password*>|**nopassword**|
secret [**5**] <*password*>}

Example:

```
ALU (config)# username user1 password pass1
```

Step 2: Click **Login**.

Step 3: On successful login, the USGM main page is displayed.

Figure 2: USGM Home Page

Top Panel

The Top Panel of the USGM home page has the following standard buttons: Device, Tools, Help and Logout. Device and Tools enable you to perform some activities. They are described in detail in the later sections of this guide. Help gives information on ‘About USGM’. It gives the details about the USGM tool like the version number, model name, and so on.

The Top Panel of the USGM home page also has a menu bar. The menu bar consists of menu items. Each menu item and their respective sub menu items are described in the later sections of this guide.

Center Panel

The Center Panel displays the front panel view of the system chassis (Services Gateway - OA-780/OA-740) that houses all the hardware components. This displays all those line cards that are installed in the system. Mouse-over a particular card name to view additional information like serial number, slot number.

The center panel also displays four tabs: the **System Information**, **Service Availability**, **Security Alerts** and **IPSec VPN Tunnels**.

- **System Information** panel provides basic information about the OA-700 (Services Gateway - OA-780/OA-740), its hardware and software configuration.
- **Service Availability** panel displays the list of all the services available on the system. The green icon indicates that the service is available and is running on the system. The red icon indicates that the service is not currently available.
- **Security Alerts** panel displays a graphical representation of the security alerts. This gives a real time update on the number of DoS and IDS attacks.
- **IPSec VPN Tunnels** displays a graphical representation of the number of IPSec tunnels configured on the system, and number of tunnels that are active. This is updated real time.

The **Bottom Panel** has the Status bar, which displays the statlog counts for the top three priority statlog (Critical, Error, and Warning - categorized by the severity level). This number is updated real time. These logs enable you to take appropriate action for smooth functioning of the system.

Click on these buttons to view the details of the respective log messages.

DESCRIPTION OF STANDARD BUTTONS ON THE GUI

Majority of the screens have consistent look and feel. They have the same buttons to take certain actions. To avoid repetition of description of the usage of these buttons and hyperlinks on every screen shot, they are described here. Any deviation from these standard buttons and links are described in the specific section.

ADD

This button is used to enter a new record. If certain fields have default values, it populates these. The user can enter data for the new record being created.

EDIT

This button is used to edit a record.

DELETE

This button deletes a record.

RESET

Resets the values entered in the fields. After updating the entries for an existing record, if you want go back to the old values (before saving them), you could hit the reset values button. This button discards the updates that are being entered and reverts to the latest saved information from the database.

SAVE

This button saves all the configured data.

Note: * indicates a mandatory field.

ICONS AND LABELS

The following table lists the icons and labels used in the OA-700 Web GUI tool.

Table 1: Icons, Labels in the OA-700 Web GUI Tool

Icon/Label	Description
	Configure/Edit the selected item.
	Delete. Click this icon to delete the selected item.
	Attach. Click this icon to attach an interface.
	Detach. Click this icon to detach an interface.
	Activate. Click this icon to activate the interface.
	Shutdown. Click this icon to shutdown the interface.
	Select. Click this icon to select an item from the available list.
	View. Click this icon to view details of the selected item.
	View Statistics. Click this icon to view statistics.
	Disable Statistics. Click this icon to disable statistics.

Icon/Label	Description
	Enable Statistics. Click this icon to enable viewing statistics.
	Log out.

LOGOUT

To logout from the USGM, click **Logout** button on the Top Panel. Confirm at the prompt to logout.

Note: The system automatically logs you out of the tool if there is no activity for 15 minutes. When you perform any activity after 15 minutes of inactivity, the system prompts you to login again.

CHAPTER 3

CONFIGURE

This chapter provides procedure to configure various features like interfaces, routing, traffic classification, filters, IPSec policy, and QoS.

CONFIGURE

From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below, which allows you to perform configurations for Interfaces, Firewalls, VPNs, Routing, and other tasks.

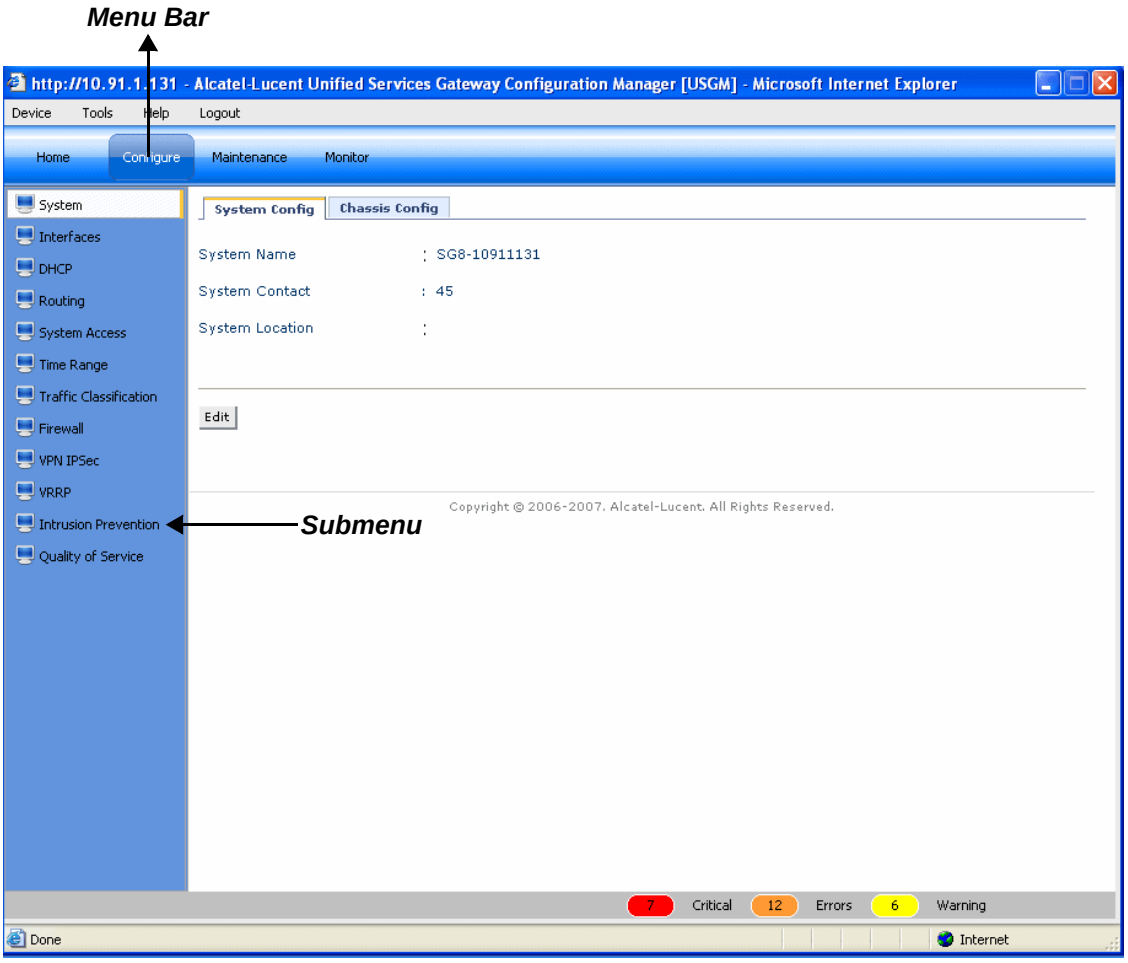


Figure 3: USGM - Configure Main Page

By default, **System** is selected and its details are displayed in the Center Panel.

SYSTEM

The System sub-menu allows to view and/or edit system parameters, and view chassis configuration.

SYSTEM CONFIGURATION

The page allows you to view and/or edit system parameters.

VIEWING SYSTEM CONFIGURATION

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: By default, **System** sub-menu is selected. System page has two tabs: **System Config** and **Chassis Config**. By default, **System Config** page is displayed in the center panel.

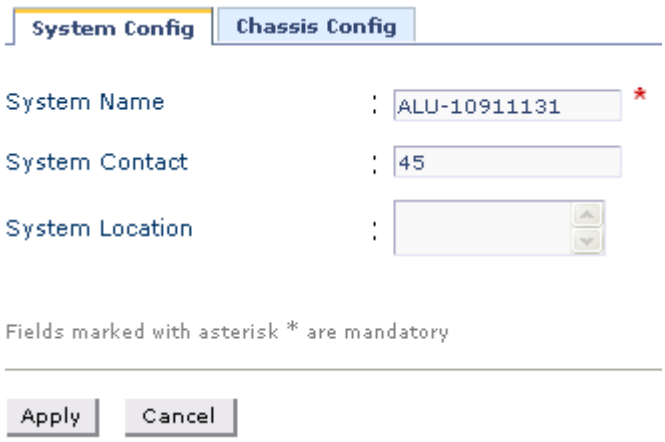


Figure 4: System Config

The table below provides description of all the fields in the System Config page.

Table 2: System Config Field Description

Field	Description
SYSTEM CONFIG	
System Name	Name given to the system.
System Contact	Contact details.
System Location	Place where the system is located.
Edit	Edit system parameters.

EDIT SYSTEM PARAMETERS

Step 1: From the **System Config** page, click **Edit** to edit the system parameters. The following page is displayed:

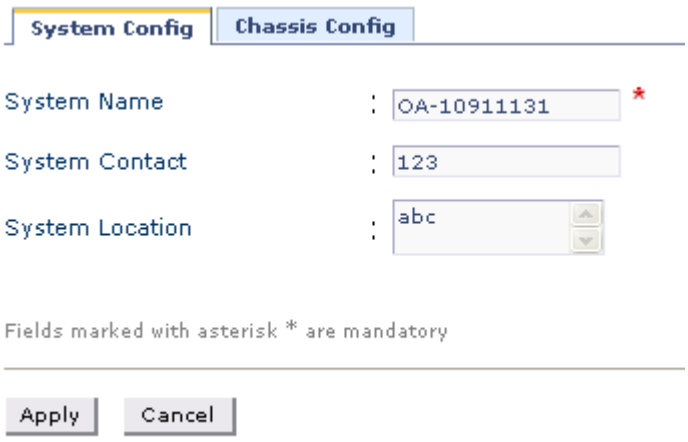


Figure 5: Edit System Configuration

Step 2: Enter or edit the system name, system contact, and system location in the respective fields. (System Name is mandatory.)

Step 3: Click **Apply** to save the changes or click **Cancel** to cancel the operation.

CHASSIS CONFIGURATION

This page lists the respective slot numbers and the line cards associated with it that are installed in the system.

This also displays the details of the OA-700 base system that includes the following components: OA-700 Chassis, Switch Fabric, Services Engine, Fan Tray and Power Tray.

VIEWING CHASSIS CONFIGURATION

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: By default, **System** sub-menu is selected.

System page has two tabs: **System Config** and **Chassis Config**. Click **Chassis Config** tab. The following page is displayed in the center panel.

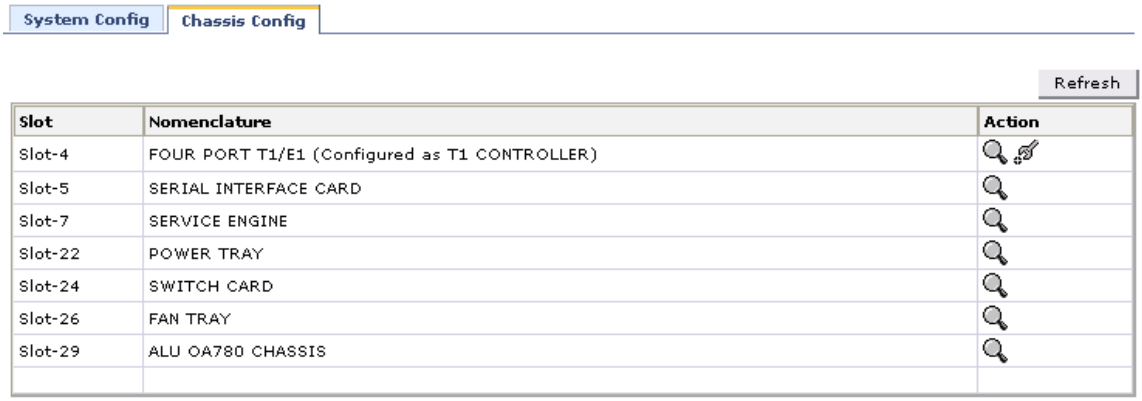


Figure 6: Chassis Config

The table below provides description of all the fields in the Chassis Config page.

Table 3: System Config Field Description

Field	Description
Slot	The slot number of the line card
Nomenclature	The name of the line card/system component
Action	Provides an option to view the details of the respective card. **Note:** Provides an option to set the card type to T1 or E1.

VIEWING CARD DETAILS

This enables you to view the details of the respective card.

1. Click **View** icon in the **Action** column corresponding to the line card whose details is to be viewed. The following pop up window is displayed:

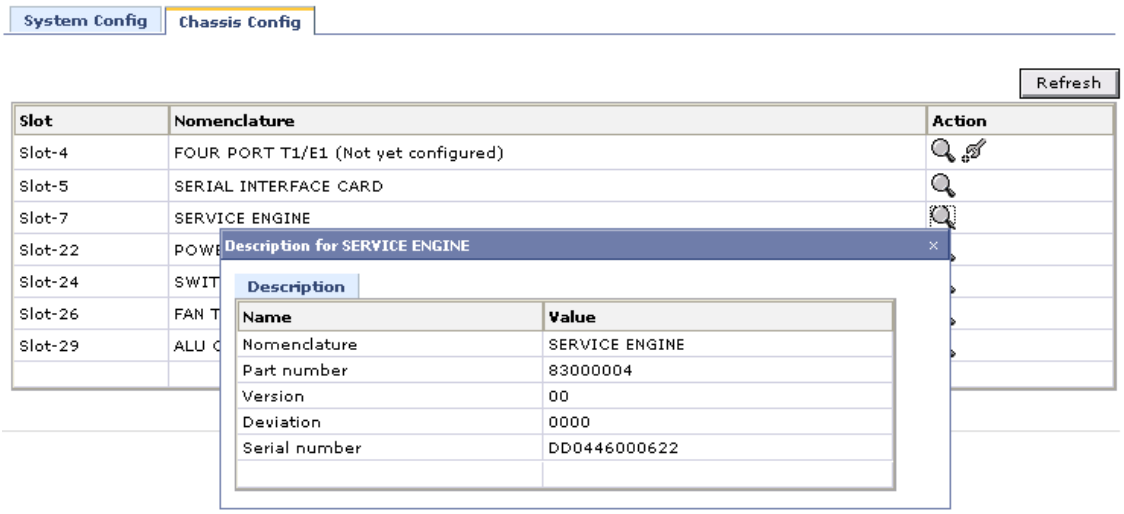


Figure 7: Chassis Config - View

SETTING CARD TYPE TO T1 OR E1

This enables you to set the T1/E1 line card type to T1 or E1 for the first time.

1. Click **Configure** icon in the **Action** column against the T1E1 line card.
2. The following message box is displayed prompting you to set the line card type to T1 or E1:

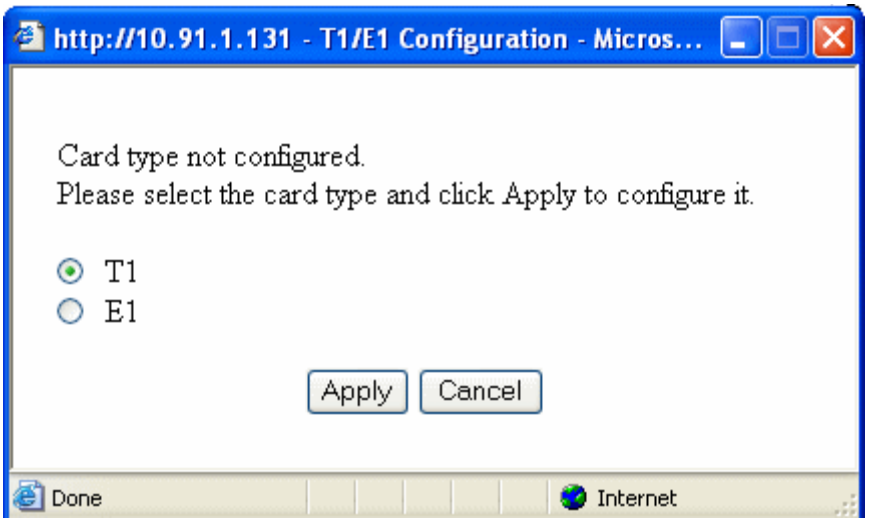


Figure 8: Chassis Config - Setting Card Type to T1 or E1

3. Select the card type and click **Apply** or click **Cancel** to cancel the operation.

CHANGING CARD TYPE

This enables you to change the already configured card type to T1 to E1.

1. Click **Configure** icon in the **Action** column against the T1E1 line card.
2. The following message box is displayed:

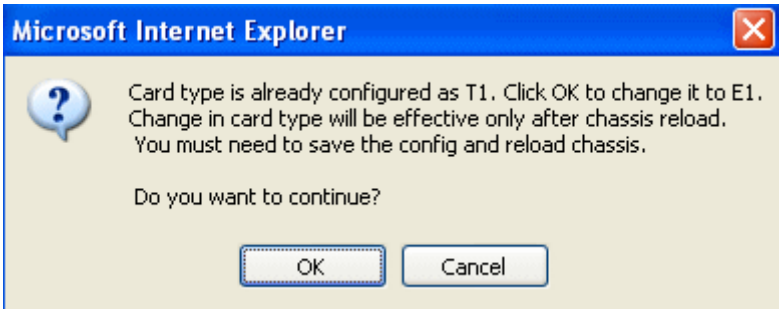


Figure 9: Chassis Config - Changing Card Type

3. Click **OK** to continue.

INTERFACES

The Interfaces page allows you to configure the interfaces supported by OA-700.

The page lists the interfaces based on the line cards installed on your system. The list also includes those interfaces that have already been configured through CLI.

This section explains on how to configure the following interfaces:

- Configure Gigabit Ethernet (GigE) Interface
- Configure T1 Controller
- Configure E1 Controller
- Configure Encapsulation on a Channelized Serial Interface
- Configure Serial Interface (V.35/ X.21)
- Configure Logical Interface
  i. Virtual LAN (VLAN)
  ii. Configure Tunnel Interface
  iii. Configure Loopback Interface

Note: The interfaces page displays the MLFR and MLPPP interfaces configured through CLI. Currently, these interfaces cannot be configured through GUI.

VIEWING INTERFACES

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Interfaces** sub-menu. The Interfaces page is displayed with the list of all the interfaces available on your system.

The list also displays those interfaces configured using the CLI commands.

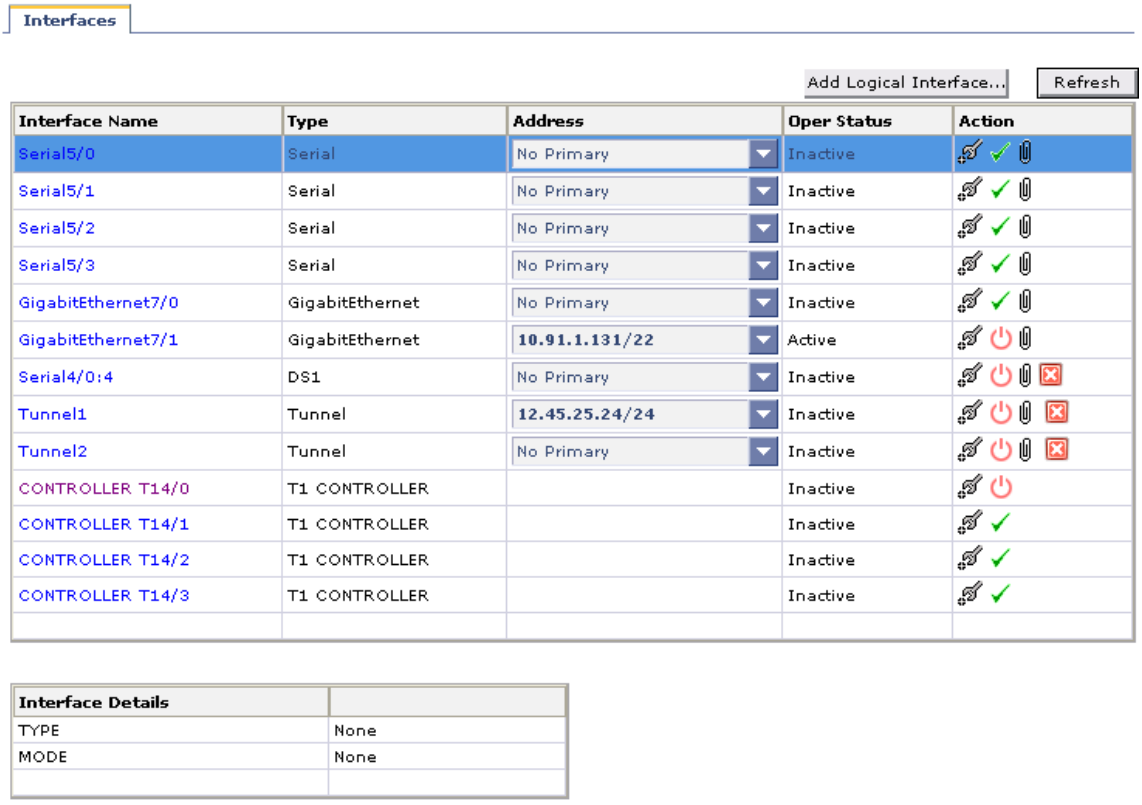


Figure 10: Interfaces

The table below provides field description for the Interfaces page.

Table 4: Interface Field Description

Field	Description
INTERFACES	
Interface Name	Name of the interface configured on the system.
Type	Interface type configured such as GigabitEthernet, loopback, serial interface, etc.
Address	IP address of the interface
Operational Status	Shows if the interface is operationally active or inactive.
Action	Provides option to edit, activate/ shutdown the interface, and associate policy/ies to the interface
Refresh	Update the interface page
Interface Details	This table displays the details of the selected interface.

CONFIGURE GIGABIT ETHERNET (GIGE) INTERFACE

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.

Follow the procedure below to configure Gigabit Ethernet interface through the Web GUI.

Step 1: On the **Interfaces** page, click **Configure** icon against the Gigabit Ethernet interface that is to be configured.

This displays the **Interface Configuration** page in the Center Panel. Interface Configuration page contains basic and advanced details and secondary address details table.

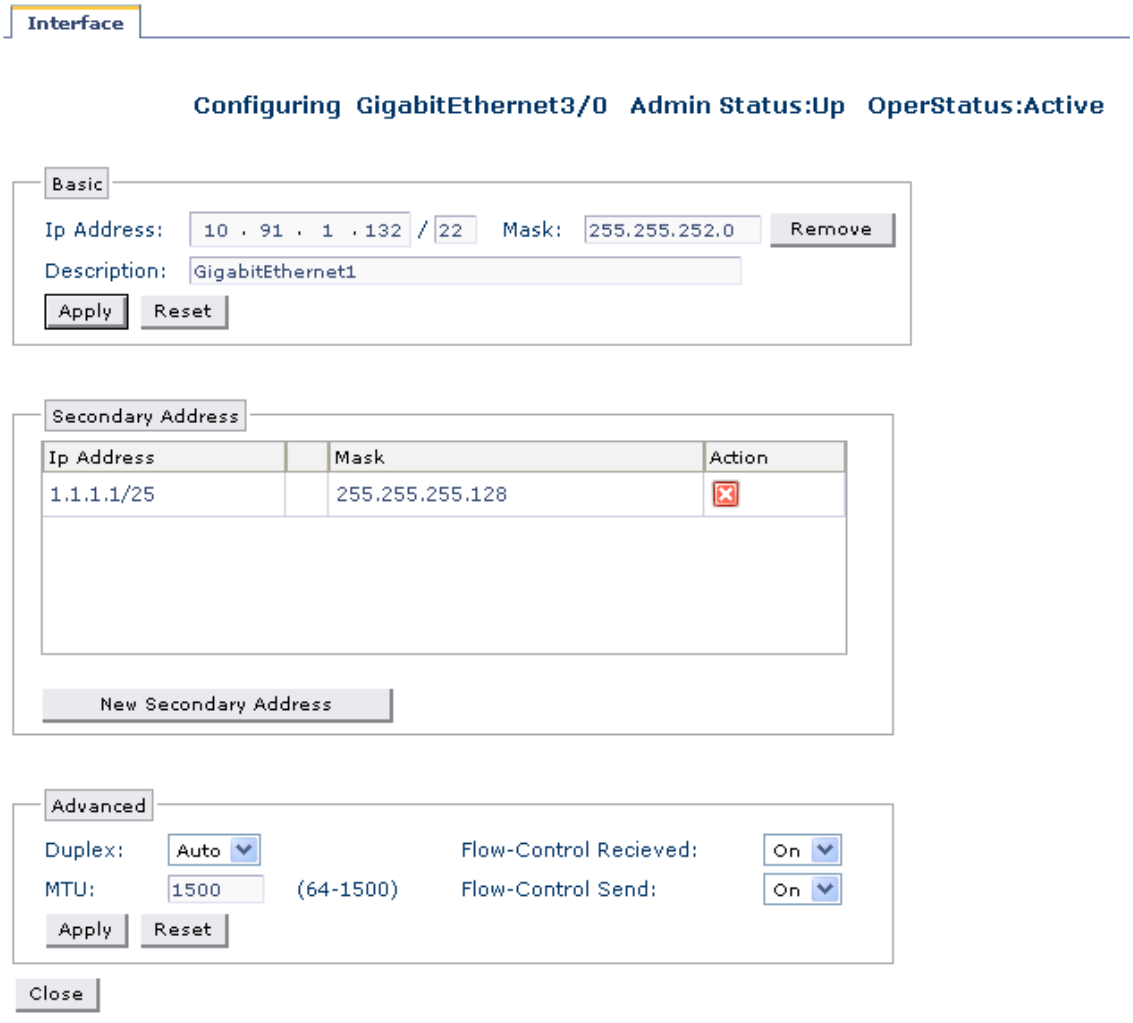


Figure 11: Interfaces - Configuring GigE Interface Details

Step 2: Configure primary IP address in the **Basic** table.

1. Enter the IP address and subnet mask for the interface in the **IP Address** and **Mask** field.
2. Enter description for the interface in the **Description** field.
3. Click **Apply** to add the details, or **Reset** to retain the original details.
4. Click **Remove** to delete the configured IP address.

Step 3: Configure secondary IP address for the interface in the **Secondary** table.

Click **New Secondary Address** to add a new secondary address to the selected interface. Fields to enter the IP address is populated.

1. Enter the secondary IP address and subnet mask for the interface in the **IP Address** and **Mask** column.
2. Click **Apply** to add the secondary IP address, or click **Cancel** to cancel adding secondary IP address.
3. Click **Delete** icon in the Action column to delete the secondary address.

Step 4: Configure advanced details in the **Advanced** table. The table displays the default values. You can retain the same or configure as required.

1. Select the required Duplex operation to be configured on the interface from the **Duplex** drop down list: **Auto/Full/Half.**

   Full-duplex refers to the ability of a network, to send and receive data at the same time.
2. Select the flow control option for the incoming traffic from the **Flow-Control Received** drop-down list: **On**/**Off**
3. Enter the MTU value (Maximum Transmission Unit) of the interface, i.e., the maximum packet size that the interface can accept in the **MTU** field (in the range 64 - 1500).
4. Select the flow control option for the outgoing traffic from the **Flow-Control Send** drop-down list: **On**/**Off**
5. Click **Apply** to add the set values, or click **Reset** to retain the original values.

Step 5: Click **Close** at the bottom of the interface configuration page to save the GigE interface configuration.

CONFIGURE T1 CONTROLLER

The interface page allows you to configure the T1 Controller.

Also, this page allows you to configure the Serial Interfaces from the T1 or E1 page.

The T1 and E1 interfaces are two different, independent standardized Time Division Multiplexing (TDM) technologies. These technologies enable the transmission of several (multiplexed) voice/data channels simultaneously on the same transmission facility.

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 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 time slots plus 1 framing bit added to them. Each time slot is regarded as a channel of 64kbps bandwidth. The frame length is 193 bits (24*8 + 1) A framing bit creates a channel of 8kbps and is used for messages, synchronization and alarms.

Follow the procedure below to configure the T1 Controller.

Step 1: On the **Interfaces** page, click **Configure** icon against the T1 Controller that is to be configured. The following page is displayed:

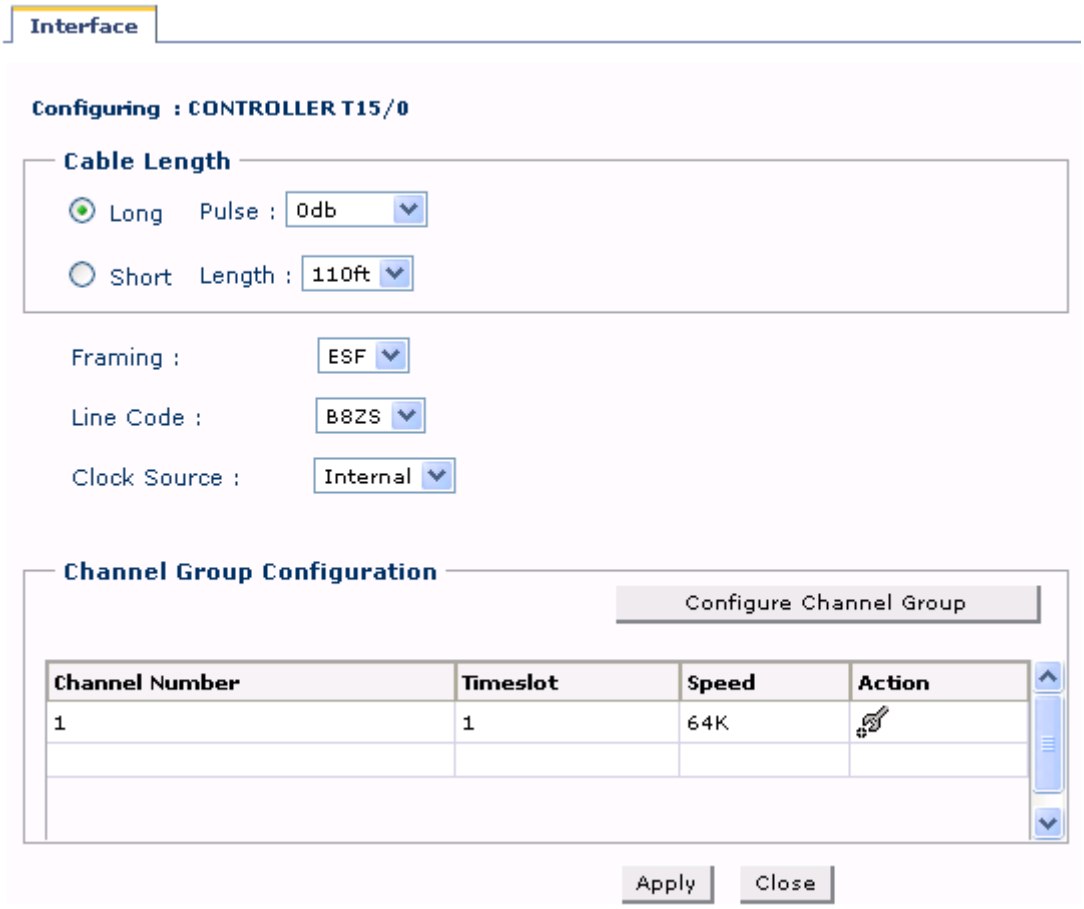


Figure 12: Interfaces - Configuring T1 Controller

Step 2: Specify the cable length parameters in the **Cable Length** box. The cable length can be of the type **Short** or **Long**.

- Select the **Long** radio button, and select the pulse value from the **Pulse** drop-down list.

  Long option configures the transmit and receive levels for a cable length (line build-out) longer than 660 ft for a T1 trunk. The default length of the cable for a T1 is Long 0db.

- Select the **Short** radio button, and select the length from the **Length** drop-down list.

  Short option sets the transmit attenuation for a cable length (line build-out) of 660 feet or shorter for a T1 trunk.

Step 3: Select the framing, line code, and clock source from the **Framing, Line Code,** and **Clock Source** drop down lists.

- **Framing**: Select the framing option: **esf/sf** to determine which framing type is required for the T1 circuit.

  Framing is configured where the router or access server is intended to communicate with t1 fractional data lines.

  i. **esf** (Extended Super Frame) - Type of frame format used. Also known as D5 or Fe. Each extended superframe consists of 24 frames.

  ii. **sf** (Super Frame): Type of frame format used. A Superframe is a structure constructed of 12 Frames, numbered: 1 - 12. It is also called as the D4 frame.

- **Line Code**: Select the line option: **ami/b8zs** to set the line code for T1.

  Line Code is configured where the router or access server is intended to communicate with T1 fractional data lines.

  i. **ami**: Alternate Mark Inversion (AMI) line-code type.

  AMI is a line encoding technique (line code) for T1s. This three-level system uses positive, negative, and grounded pulses (e.g. -5V, 0V, 5V) to represent logical values. A logical 0 is represented with a grounded or absent pulse, and a logical 1 by pulses of alternating polarity.

  ii. **b8zs**: Binary 8 Zeros Substitution (b8zs) line code type.

  b8zs is an encoding method in T1 and E1 transmission that substitutes a special bit pattern for 8 consecutive zeros in order to maintain ones density.

- **Clock Source**: Select the clock source option: **Internal/Line** to set the clock source for T1. Clock source is used to transmit clock signals. The default value for clock source is internal.

  i. **Internal**: The controller synchronizes itself to the internal (system) clock.

  ii. **Line**: The controller recovers external clock from the line and provides the recovered clock to the internal (system) clock generator.

Step 4: Configure channel groups on the controller. This creates a channel-group that will form a channelized serial interface. Click **Configure Channel Group** to configure channel group. **Channel Group Configuring** pop up window is displayed.

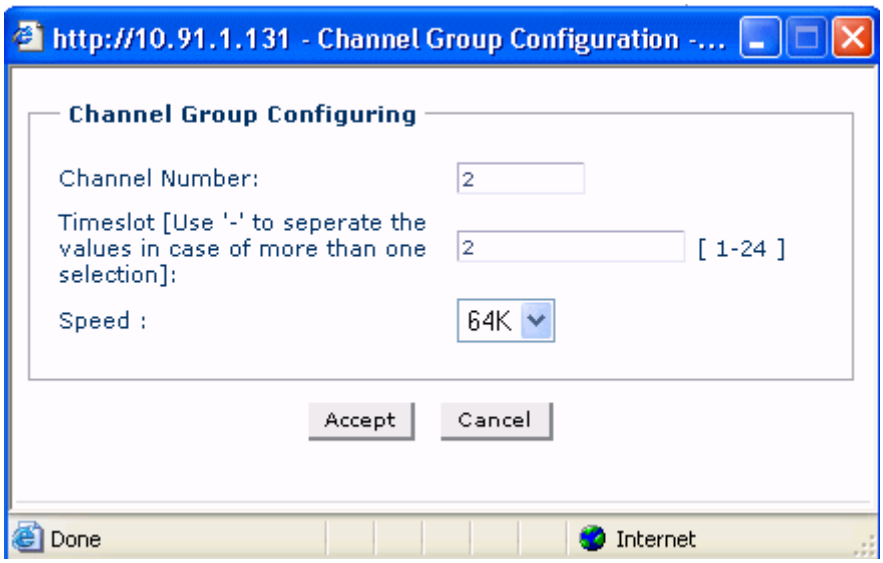


Figure 13: Interfaces - T1 Controller - Channel Group Configuring

- Enter the channel number in the **Channel Number** field.
- Enter the range of the time slots that can be associated with the T1 controller in the **Time Slot** field.
- Select the speed from the **Speed** drop down list. Default speed is 64 kbps.
- Click **Accept**. The channel group thus configured is displayed under the **Channel Group Configuration** table. Repeat this procedure to configure more channel groups.

Step 5: Click **Apply** to save the T1 Controller configuration or click **Close** to cancel the operation.

Step 6: The channel-group thus configured forms the channelized serial interface, and is displayed in the Interfaces page.

Note: You can configure encapsulation on a channelized serial interface. See "Configure Encapsulation on a Channelized Serial Interface" for more details on this.

CONFIGURE E1 CONTROLLER

The interface page allows you to configure the E1 Controller.

The E1 interface provides a transmission rate of 2.048 Mbps. It can support up to 32 user channels, though usually only 30 channels are used as dedicated user channels. An E1 basic frame is made up of 256 bits, 32 time slots, each containing 8 bits. Each time slot 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.

Follow the procedure below to configure the E1 Controller.

Step 1: On the **Interfaces** page, click **Configure** icon against the E1 Controller that is to be configured. The following page is displayed:

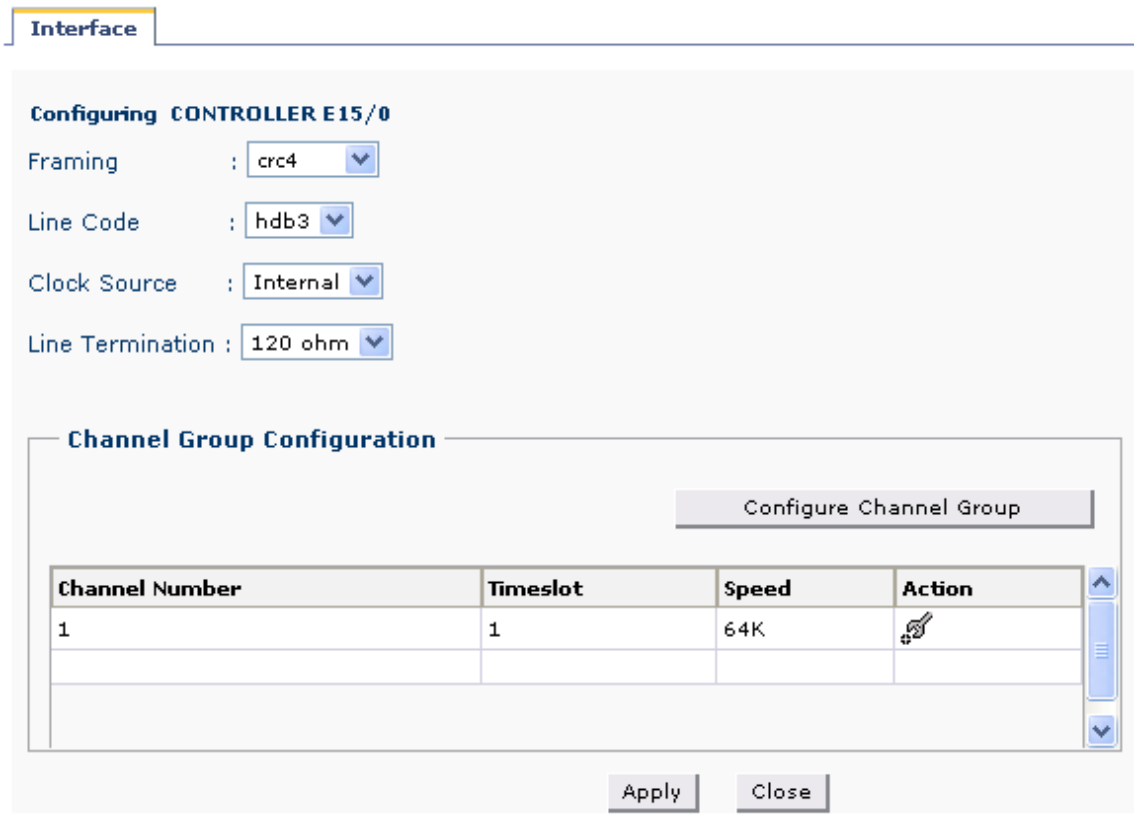


Figure 14: Interfaces - Configuring E1 Controller

Step 2: Select the framing, line code, and clock source, and Line Termination from the **Framing, Line Code, Clock Source**, and **Line Termination** drop down lists.

- **Framing**: Select the framing option to determine which framing type is required for the E1 circuit.

  Framing is configured where the router or access server is intended to communicate with E1 fractional data lines.

  i. **crc4**: 4-bit cyclic redundancy check, i.e., crc4 frame is the E1 frame type.

  ii. **no-crc4**: No cyclic redundancy check, i.e., crc4 frame is not the E1 frame type.

- **Line Code**: Select the line option: **ami/hdb3** to set the line code for E1.

  Line Code is configured where the router or access server is intended to communicate with E1 fractional data lines.

  i. **ami**: Alternate Mark Inversion (AMI) line-code type.

  ii. **hdb3**: High-density bipolar 3 (hdb3) line-code type.

- **Clock Source**: Select the clock source option: **Internal/Line** to set the clock source for E1. Clock source is used to transmit clock signals.

  i. **Internal**: The controller synchronizes itself to the internal (system) clock.

  ii. **Line**: The controller recovers external clock from the line and provides the recovered clock to the internal (system) clock generator.

- **Line Termination**: Select the line termination option: **120 ohm/75 ohm** to configure a line impedance.

Step 3: Configure channel groups on the controller. This creates a channel-group that will form a channelized serial interface. Click **Configure Channel Group** to configure channel group. **Channel Group Configuring** pop up window is displayed.

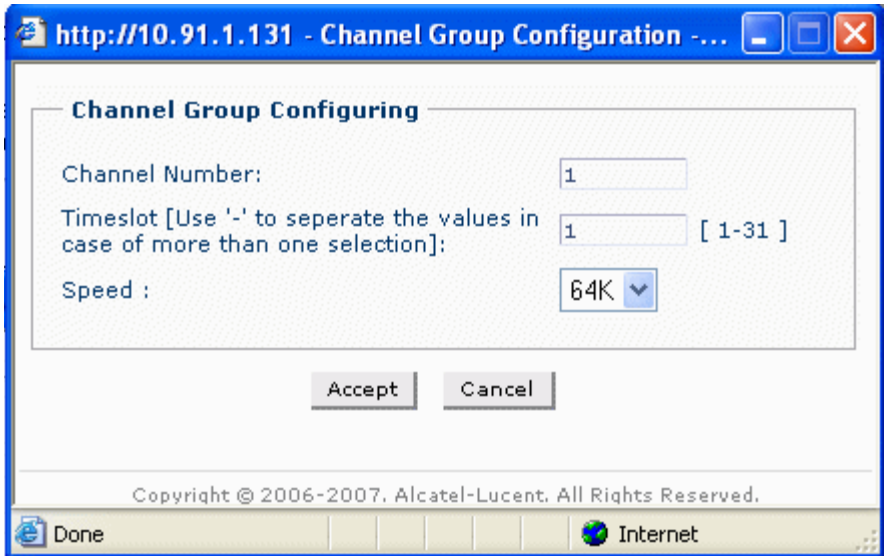


Figure 15: Interfaces - E1 Controller - Channel Group Configuring

- Enter the channel number in the **Channel Number** field.
- Enter the range of the time slots that can be associated with the E1 controller in the **Time Slot** field.
- Select the speed from the **Speed** drop down list. Default speed is 64 kbps.
- Click **Accept**. The channel group thus configured is displayed under the **Channel Group Configuration** table. Repeat this procedure to configure more channel groups.

Step 4: Click **Apply** to save the E1 Controller configuration or click **Close** to cancel the operation.

Step 5: The channel-group thus configured forms the channelized serial interface, and is displayed in the Interfaces page.

Note: You can configure encapsulation on a channelized serial interface. See "Configure Encapsulation on a Channelized Serial Interface" for more details on this.

CONFIGURE ENCAPSULATION ON A CHANNELIZED SERIAL INTERFACE

This page enables you to set encapsulation on a channelized Serial Interface formed by the channel group configuration on a T1E1 controller.

Follow the procedure below to configure Serial interface.

Step 1: In the **Interfaces** page, click **Configure** icon for the Serial interface whose parameters are to be configured. This displays the **Configuration Serial** page in the Center Panel.

Step 2: You need to set the encapsulation type on the interface by selecting the required option under **Encapsulation**: **HDLC/PPP/Frame Relay/MLPPP/MLFR.** By default, **HDLC** radio button is selected.

HDLC ENCAPSULATION

High-level Data Link Control (HDLC) - 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.

1. By default **HDLC** radio button is selected. (HDLC is the default encapsulation on the interface), and the following page displays the HDLC parameters:

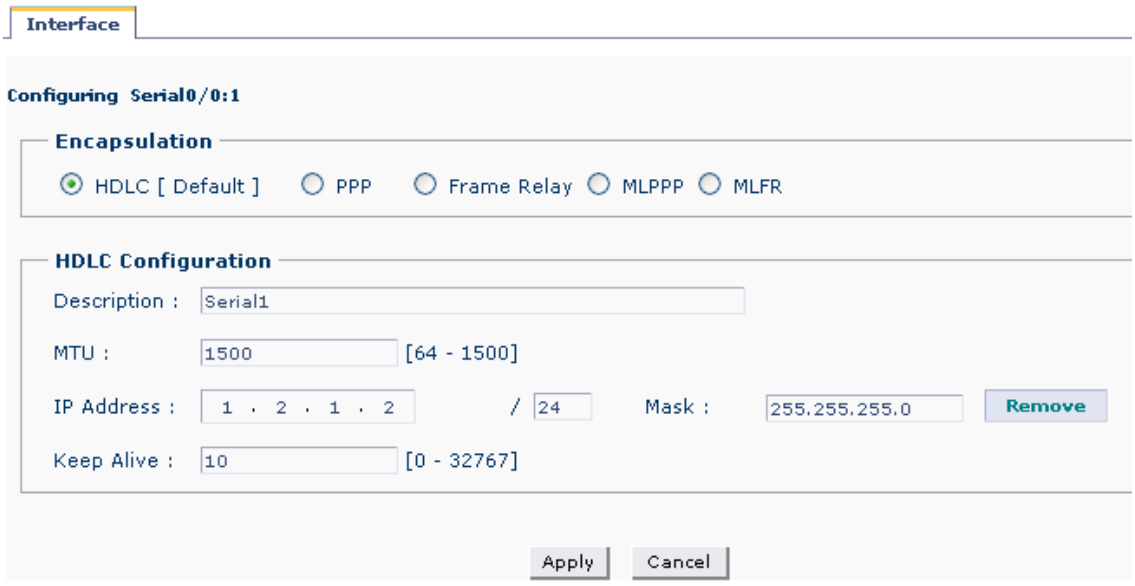


Figure 16: Interfaces - Configure HDLC Encapsulation on a Channelized Serial Interface

2. Enter the description for the serial interface in the **Description** field.
3. Enter the Maximum Packet size or Maximum Transmission Unit (MTU) size in the **MTU** field.
4. Enter the IP address and the Mask in the **IP Address** and **Mask** fields. Click **Remove** to delete the IP address and re-enter the new IP address.
5. Configure the HDLC keep alive interval by entering the value in **Keep Alive** field. It must be less than the corresponding interval at the switch. Range is 0-32767. Value of 0 turns off the keep alive feature.
6. Click **Apply** to save the HDLC configuration or click **Cancel** to cancel the operation.

PPP Encapsulation

The Point-to-Point protocol (PPP) 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, asynchronous and synchronous encapsulation, 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 Link Control Protocol (LCP) and a family of Network Control Protocols (NCP) to negotiate optional configuration parameters and facilities. PPP supports protocols like IP, IPX and DECnet through the Network Control Protocols.

1. Set the PPP encapsulation on the interface by selecting **PPP** radio button under **Encapsulation**. The following page is displays the PPP parameters:

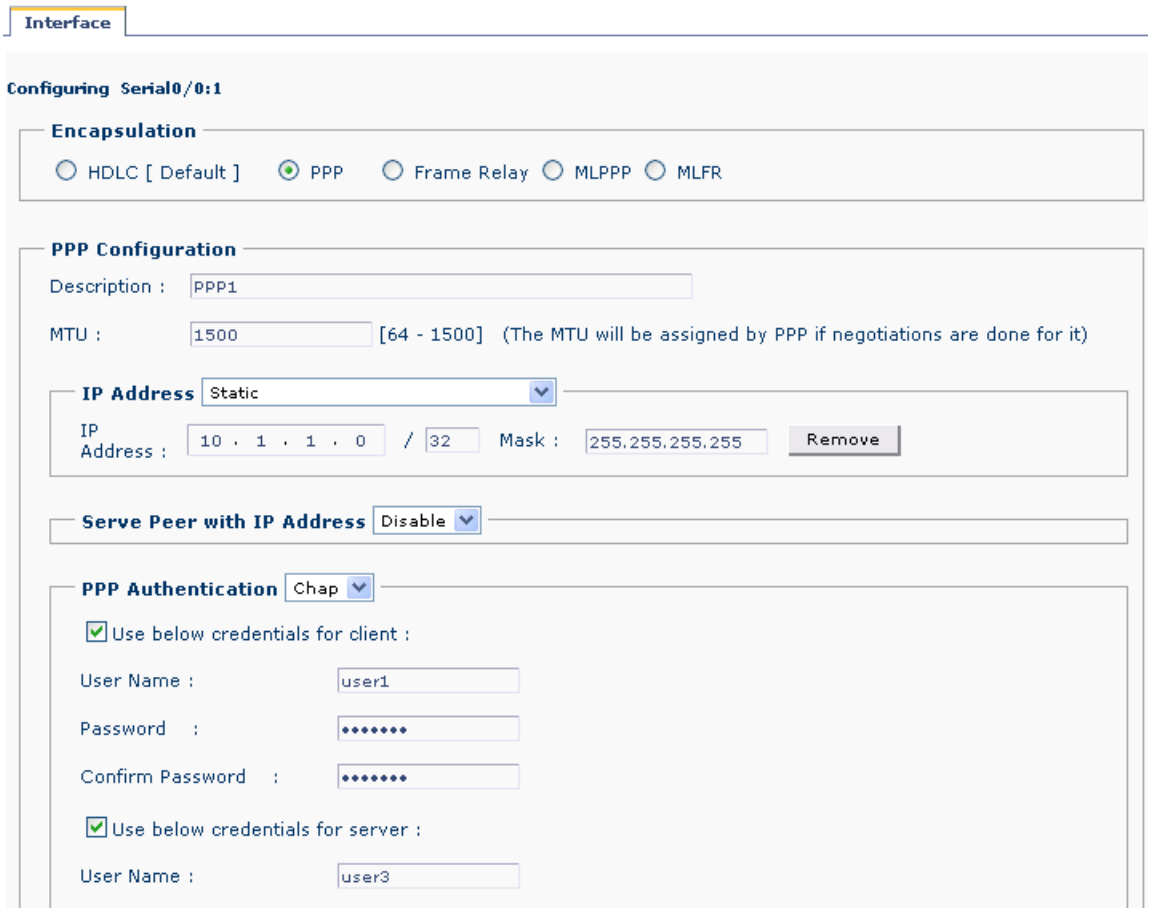


Figure 17: Interfaces - Configure PPP Encapsulation on a Channelized Serial Interface

2. Enter the description for the serial interface in the **Description** field.
3. Enter the Maximum Transmission Unit (MTU) size in the **MTU** field. This should be between 64 and 1500.
4. Select the IP address option from the **IP Address** drop down list: **Static/ Negotiate IP Address with the Peer**
   - If **Static** option is selected, enter the IP address and the Mask in the **IP Address** and **Mask** fields. Click **Remove** to delete the IP address and re-enter the new IP address.
   - If **Negotiate IP Address with the Peer** is selected, the IP Address will be assigned based on the negotiation with the peer. Hence the IP address and the mask fields are not displayed.
5. Select the **Server Peer with IP Address** option: **Enable/Disable**
   - If **Enable** option is selected, enter the IP address in the **IP Address** field. This will allow to assign IP address entered to the peer on negotiation if "Negotiate IP Address with the Peer" is selected on the Peer.
   - **Disable** option disables Server Peer with IP Address.

6. 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 (CHAP - Challenge Authentication Protocol, PAP - Password Authentication Protocol, EAP - Extensible Authentication Protocol). Authentication is not mandatory.
7. Set the authentication protocol for authenticating the peer by selecting the option from **PPP Authentication** drop-down list: **Chap/Pap/Eap/None**
   - You can set a user name for PPP authentication on either the server side or client side. Select the **Use below credentials for client/Use below credentials for server** check box to enter the user name and password on the client side/server side.
     i. Enter the user name and the password in the **User Name** and **Password** fields. Confirm password in the **Confirm Password** field.
   - Selecting **None** option for PPP authentication resets or negates the authentication protocol.
8. Click **Advanced Options** to initiate LCP negotiation on a PPP encapsulation and configure PPP Timers. The following page is displayed:

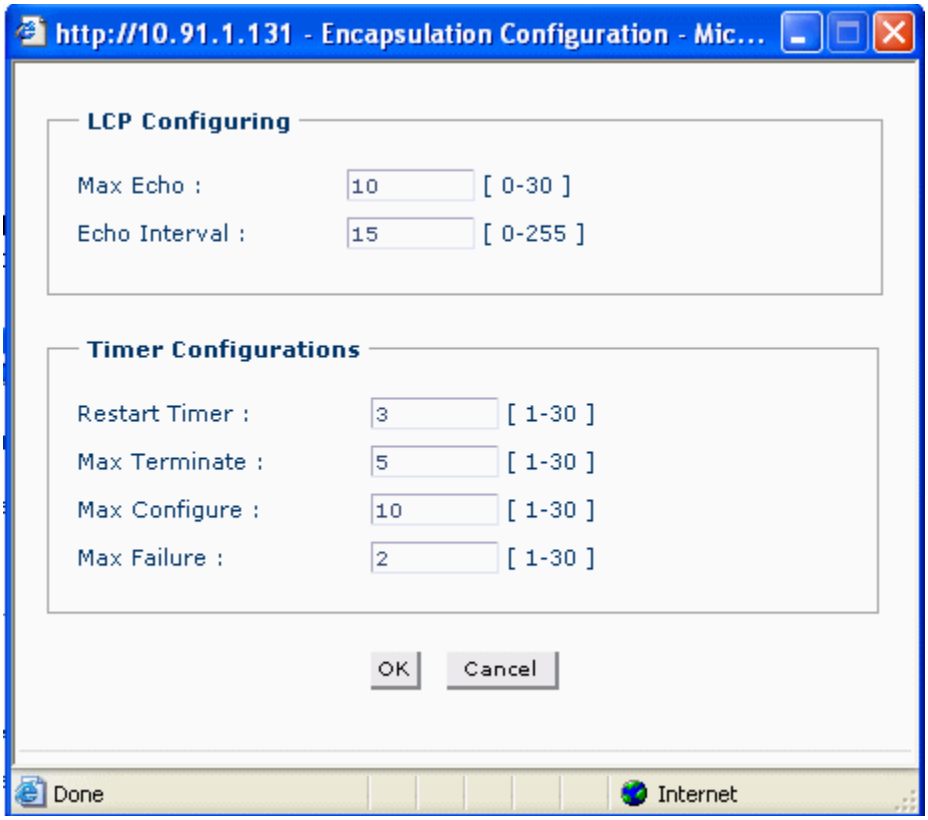


Figure 18: Interfaces - Configure PPP Encapsulation on a Channelized Serial Interface - Advanced Options

- Configure LCP parameters in **LCP Configuring** table. This helps in deciding whether the system initiates the LCP negotiation or just responds.
  i. Enter the maximum echo value in **Max Echo** field.

     This 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. Default echo interval is 5 seconds.

  ii. Enter the echo interval in **Echo Interval** field.

     This denotes the interval between the LCP echo requests sent. “0” implies that no echo requests are sent. The default value is 10 seconds.
- Configure the PPP Timer configuration in **Timer Configuring** table.
  i. Enter the restart timer in **Restart Timer** field to set the time period for retransmission of LCP and NCP packets. The default value is 3 seconds.
  ii. Enter the maximum number of pings before terminating to send packets in the **Max Terminate** field.

     This terminates request packets (Number of LCP or NCP) without receiving a Terminate Ack before assuming that the peer is unable to respond. The default value is 2 seconds.
  iii. Enter the max configure value in **Max Configure** field.

     Configure Request packets (Number of LCP or NCP) without receiving a valid Configure Ack/NaK/Reject before assuming that the peer is unable to respond. The default value is 10 seconds.
  iv. Enter the max failure value in **Max Failure** field.

     Configure NaK packets (Number of LCP or NCP) without receiving a Configure Ack before assuming that configuration is not converging. The default value is 5 seconds.
- Click **OK** to save LCP and PPP Timers configuration or click **Cancel** to cancel the operation.

9. After configuring the parameters, click **Apply** to save the PPP configuration or click **Cancel** to cancel the operation.

FRAME RELAY ENCAPSULATION

Frame Relay (FR) is a high performance 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. Frame-relay is a strictly layer 2 protocol suite which enables it to offer high performance and greater transmission efficiency. This makes Frame Relay suitable for current WAN applications like LAN interconnection.

1. Set the Frame Relay encapsulation on the interface by selecting **Frame Relay** radio button under **Encapsulation**. The following page is displays the Frame Relay parameters:

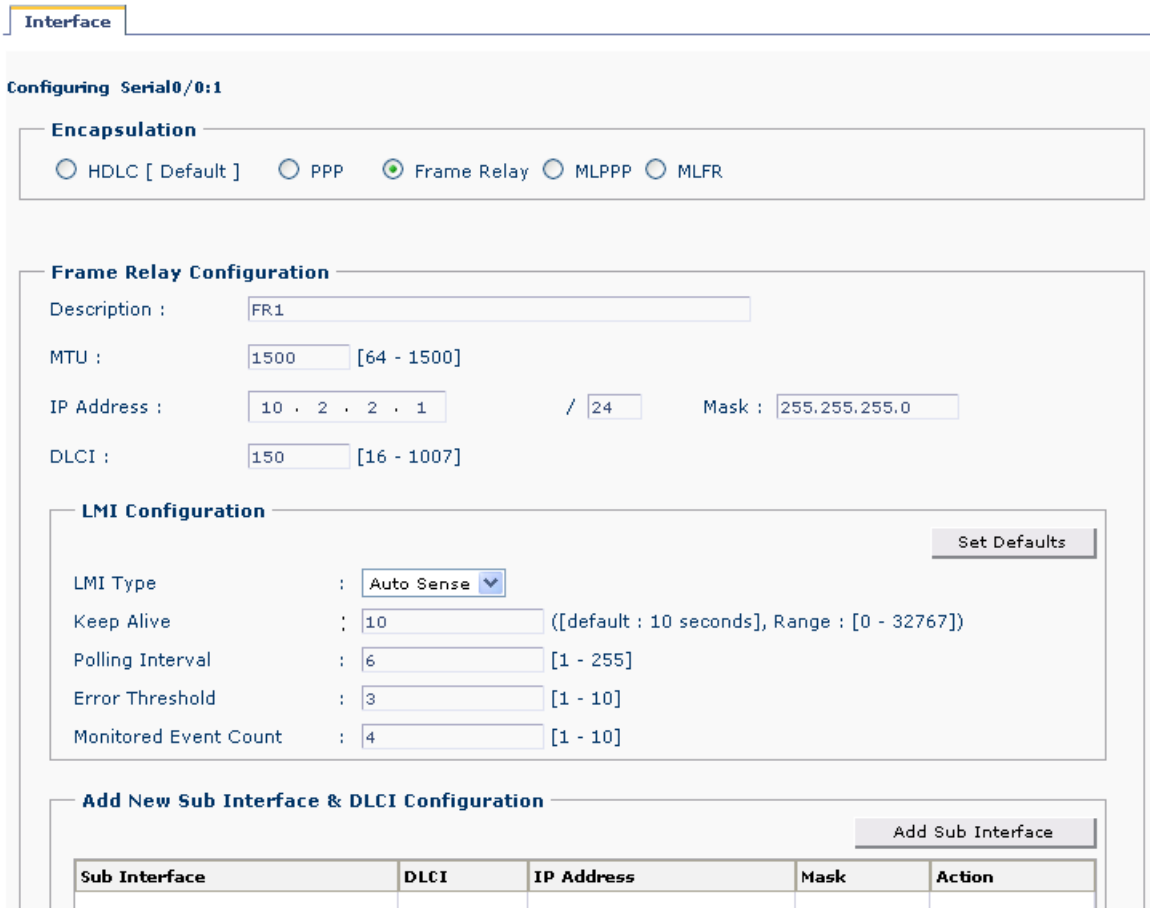


Figure 19: Interfaces - Configure Frame Relay Encapsulation on a Channelized Serial Interface

2. Enter the description for the serial interface in the **Description** field.
3. Enter the Maximum Packet size or Maximum Transmission Unit (MTU) size in the **MTU** field. This should be between 64 and 1500.
4. Enter the IP address and the Mask in the **IP Address** and **Mask** fields.

5. Enter the DLCI value in the **DLCI** field.

   Data-link Connection Identifiers - Frame Relay virtual circuits are identified by DLCIs. These values are typically assigned by the Frame Relay service provider. The DLCIs have a local significance which means that their values are unique to the link. The system provides support for point-to-point FR DLCIs only.

6. Configure the LMI (Local Management Interface) parameters in the **LMI Configuration** table.

   Configure the LMI values manually or click **Set Defaults** to set the default values for LMI parameters.

   - Select the LMI type from the **LMI Type** drop down list: **Auto Sense/ANSI/ Q933A**.

     LMI Auto Sense is activated by default (as the system acts as a DTE). The LMI Auto Sense will be activated when the physical interface is up and LMI type is not configured on that interface.

   - Enter the LMI Keep Alive interval in the **Keep Alive** field.

     The default value is 10 seconds. The LMI keepalive value should typically be equal to the corresponding interval at the switch.

   - Enter the polling interval value in the **Polling Interval** field. The default value is 6. This is used to set the full status polling interval on a DTE interface.
   - Enter the DTE error threshold value in **Error Threshold** field. The default value is 3.
   - Enter the DTE monitored event count in the **Monitored Event Count** field. The default value is 4.

7. 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 on a serial interface, follow the steps given below:

   - Click **Add Sub Interface** to configure a sub interface. **Create Sub Interface** pop up window is displayed.

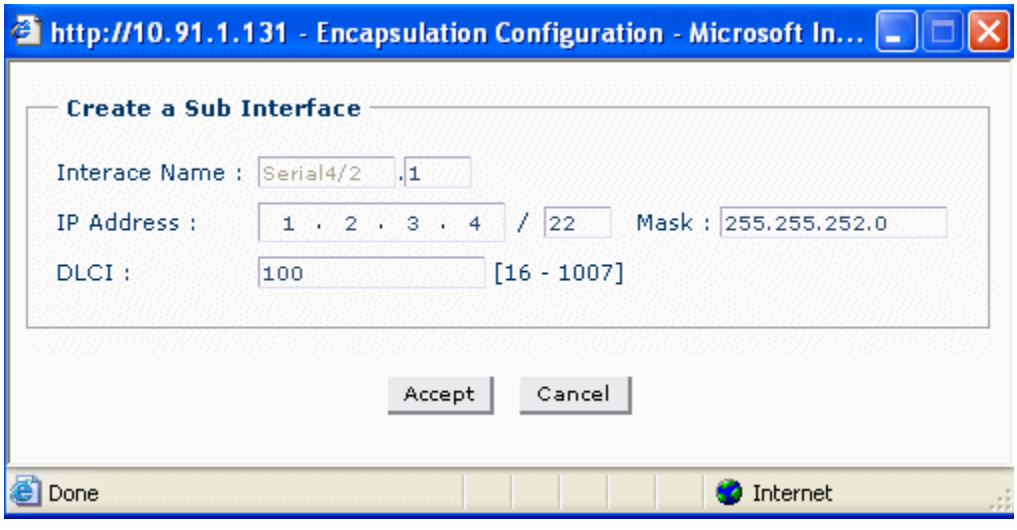


Figure 20: Interfaces - Configure Frame Relay Encapsulation on a Channelized Serial Interface - Create Sub Interface

- Enter the sub interface number in the **Interface Name** field.
- Enter the IP address and the Mask in the **IP Address** and **Mask** fields.
- Enter the DLCI value in the **DLCI** field.
- Click **Accept** to save the configuration or click **Cancel** to cancel the operation.

- Click **Accept**. The sub interface thus configured is displayed under the **Add New Sub Interface & DLCI Configuration** table. Repeat this procedure to configure more sub interfaces.

8. After configuring the parameters, click **Apply** to save the Frame Relay configuration or click **Cancel** to cancel the operation.
9. The sub interfaces thus configured is displayed in the Interfaces page.

MLPPP Encapsulation

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.

Note: **To configure MLPPP encapsulation on an interface, first a bundle interface needs to be configured and then MLPPP encapsulation is set on the member interfaces, to link them to the bundle.**

Currently, you can configure the bundle interface only through CLI. The Interface page lists the MLPPP bundle interfaces created via CLI. Each MLPPP interface is identified by a bundle ID.

1. Set the MLPPP encapsulation on the interface by selecting **MLPPP** radio button under **Encapsulation**. The following page is displays the MLPPP parameters:

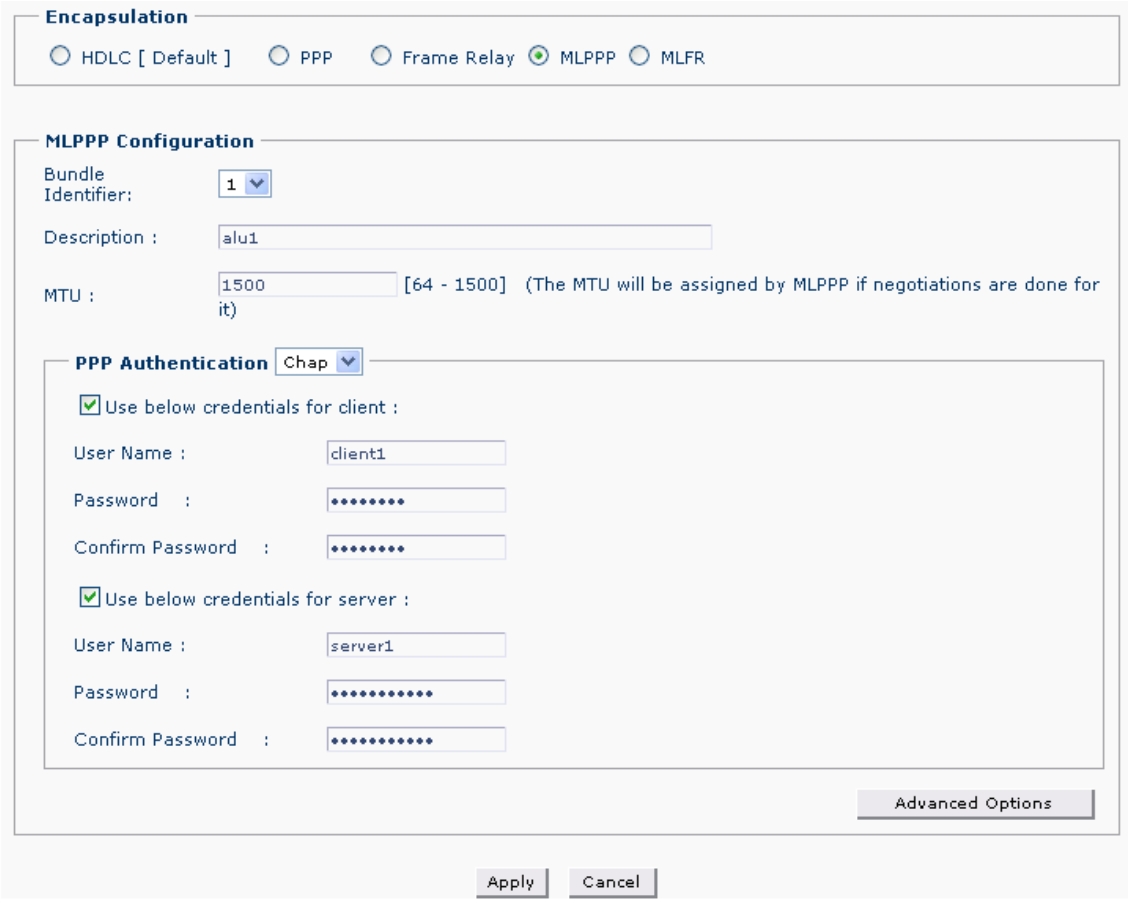


Figure 21: Interfaces - Configure MLPPP Encapsulation on a Channelized Serial Interface

2. Each MLPPP interface is identified by a bundle ID. The interface becomes a member link of the bundle interface identified by the bundle ID. Select the bundle identifier from the **Bundle Identifier** drop-down list.
3. Enter the bundle identification (BID) name to the bundle interface in the **Description** field.
4. Enter the Maximum Packet size or Maximum Transmission Unit (MTU) size in the **MTU** field. The default MTU on an MLPPP bundle interface is 1494.
5. 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 (CHAP - Challenge Authentication Protocol, PAP - Password Authentication Protocol, EAP - Extensible Authentication Protocol). Authentication is not mandatory.
6. Set the authentication protocol for authenticating the peer by selecting the option from **PPP Authentication** drop down list: **Chap/Pap/Eap/None**

- You can set a user name for PPP authentication on either the server side or client side. Select the **Use below credentials for client/Use below credentials for server** check box to enter the user name and password on the client side/server side.
  i. Enter the user name and the password in the **User Name** and **Password** fields. Confirm password in the **Confirm Password** field.
- Selecting **None** resets or negates the authentication protocol.

7. Click **Advanced Options** to initiate LCP negotiation on a PPP encapsulation and configure PPP Timers. The following page is displayed:

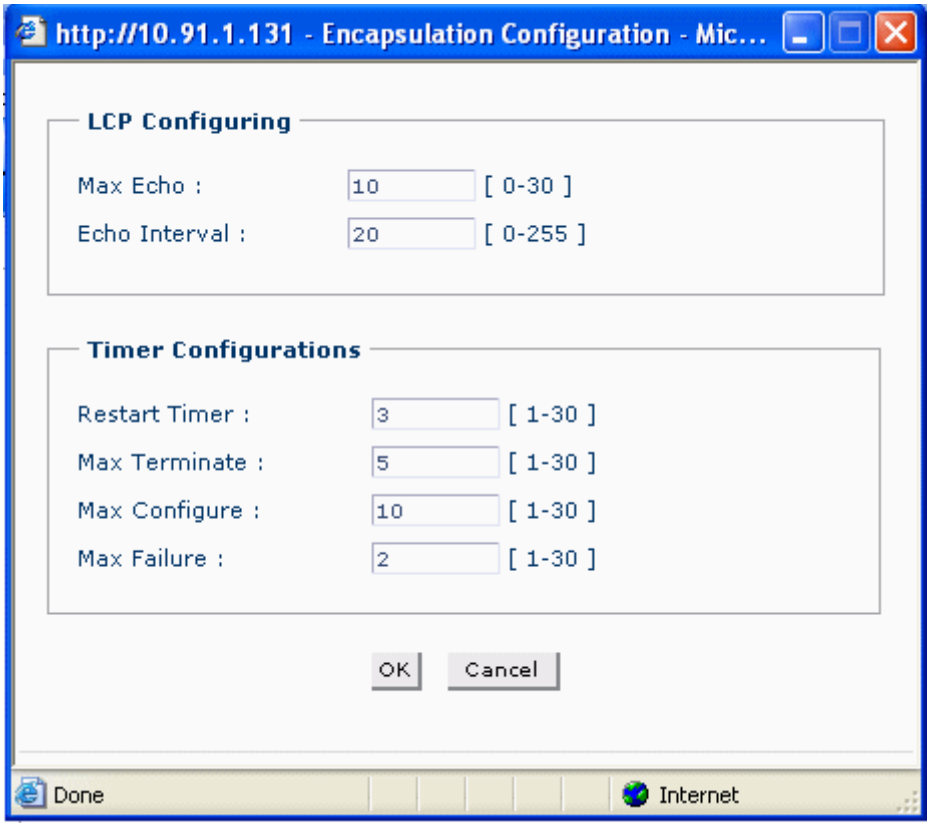


Figure 22: Interfaces - Configure MLPPP Encapsulation on a Channelized Serial Interface - Advanced Options

- Configure LCP parameters in **LCP Configuring** table. This helps in deciding whether the system initiates the LCP negotiation or just responds.
  i. Enter the maximum echo value in **Max Echo** field.

  This 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. Default echo interval is 5 seconds.

  ii. Enter the echo interval in **Echo Interval** field.

  This denotes the interval between the LCP echo requests sent. “0” implies that no echo requests are sent. The default value is 10 seconds.

- Configure the PPP Timer configuration in **Timer Configuring** table.
  i. Enter the restart timer in **Restart Timer** field to set the time period for retransmission of LCP and NCP packets. The default value is 3 seconds.
  ii. Enter the maximum number of pings before terminating to send packets in the **Max Terminate** field.

  This terminates request packets (Number of LCP or NCP) without receiving a Terminate Ack before assuming that the peer is unable to respond. The default value is 2 seconds.
  iii. Enter the max configure value in **Max Configure** field.

  Configure Request packets (Number of LCP or NCP) without receiving a valid Configure Ack/NaK/Reject before assuming that the peer is unable to respond. The default value is 10 seconds.
  iv. Enter the max failure value in **Max Failure** field.

  Configure NaK packets (Number of LCP or NCP) without receiving a Configure Ack before assuming that configuration is not converging. The default value is 5 seconds.
- Click **OK** to save LCP and PPP Timers configuration or click **Cancel** to cancel the operation.

8. After configuring the parameters, click **Apply** to save the MLPPP configuration or click **Cancel** to cancel the operation.

MLFR ENCAPSULATION

MLFR is defined in FRF 16.1. It is an extension to the Frame Relay Protocol.

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.

Note: **To configure MLFR encapsulation on an interface, first a bundle interface needs to be configured and then MLFR encapsulation is set on the member interfaces, to link them to the bundle.**

Currently, you can configure the bundle interface only through CLI. The Interface page lists the MLFR bundle interfaces created via CLI. Each MLFR interface is identified by a bundle ID.

1. Set the MLFR encapsulation on the interface by selecting **MLFR** radio button under **Encapsulation**. The following page is displays the MLFR parameters:

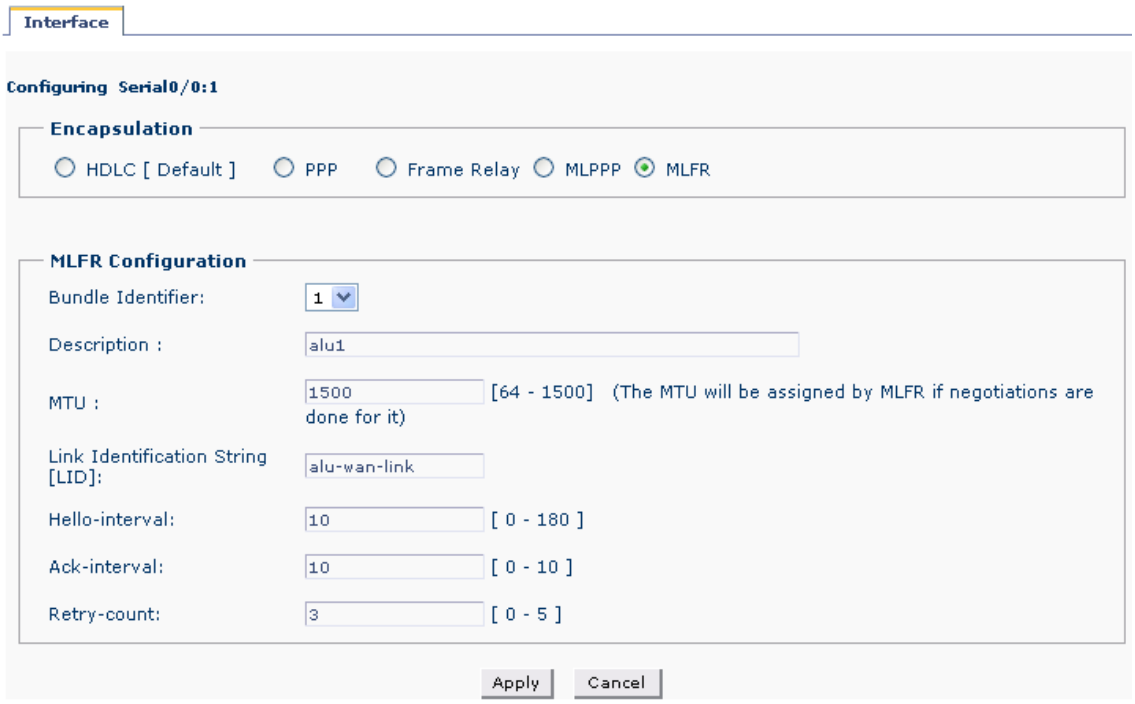


Figure 23: Interfaces - Configure MLFR Encapsulation on a Channelized Serial Interface

2. Each MLFR interface is identified by a bundle ID. The interface becomes a member link of the bundle interface identified by the bundle ID. Select the bundle identifier from the **Bundle Identifier** drop-down list.
3. Enter the bundle identification (BID) name to the bundle interface in the **Description** field.
4. Enter the Maximum Packet size or Maximum Transmission Unit (MTU) size in the **MTU** field. The default MTU on an MLPPP bundle interface is 1494.
5. Enter the Link Identification name to the interface that is part of the bundle in the **LID** field. The LID can be a maximum of 255 characters.
6. Enter the hello-interval in the **Hello-interval** field. Hello interval is the duration in seconds between successive hello messages sent.
7. Enter the ack-interval in the **Ack-interval** field. 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.
8. Enter the retry-count in the **Retry-count** field. Retry count is the number of times the bundle link will send out a hello message before any acknowledgment is received from its peer.
9. After configuring the parameters, click **Apply** to save the MLFR configuration or click **Cancel** to cancel the operation.

CONFIGURE SERIAL INTERFACE (V.35/ X.21)

This page enables you to configure the parameters for a Serial Interface (V.35/ X.21).

Follow the procedure below to configure Serial interface.

Step 1: In the **Interfaces** page, click **Configure** icon for the Serial interface whose parameters are to be configured. This displays the **Configuration Serial** page in the Center Panel.

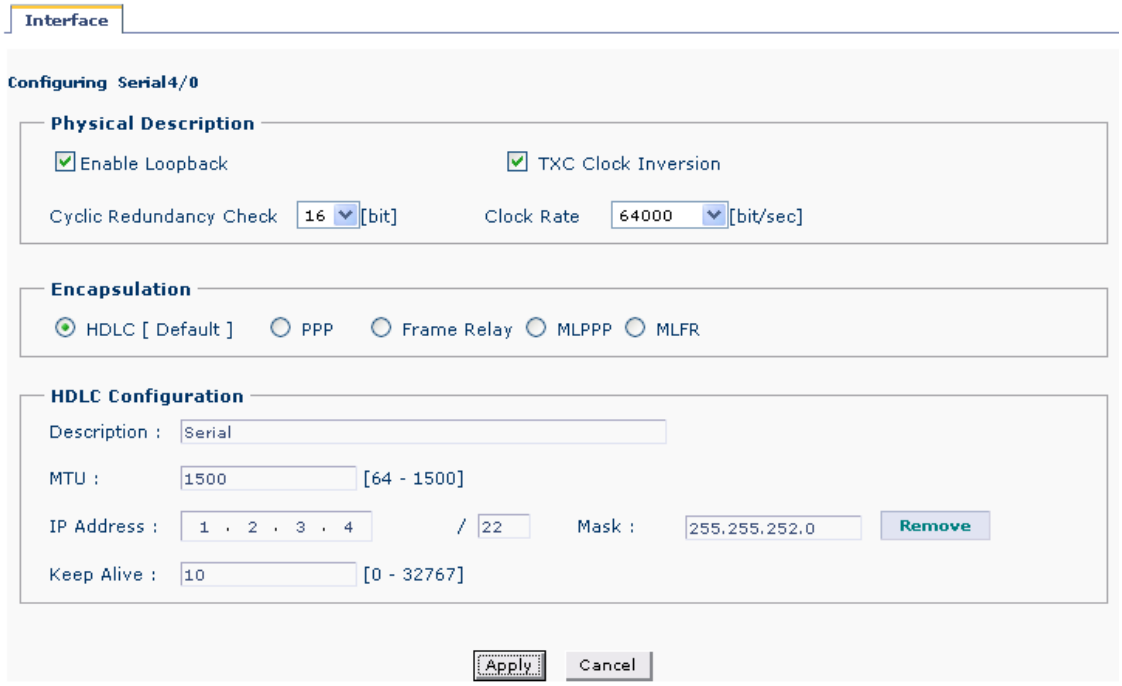


Figure 24: Interfaces - Configuring Serial Interface (V.35/X.21)

Step 2: Configure V.35/X.21 DTE (Data Terminal Equipment) and DCE (Data Circuit-Terminating Equipment) specific parameters under the Physical Description box.

- Select the **Enable Loopback** check box to configure the interface in the loopback mode.

  Loopback is used for troubleshooting and diagnostic purpose. When an 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.

- Select the **TXC Clock Inversion** check box to invert the transmit clock to correct phase shift between the clock and the data.

  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. By default, the transmit clock is not inverted.
- Enter the CRC in the **Cyclic Redundancy Check** field.
- Select the clock rate from the Clock Rate drop-down list. Clock rate configures the speed of the clock.

Step 3: Set the encapsulation for the interface.

Note: **You can set the encapsulation type on a Serial interface (V.35/X.21) by selecting the required option under Encapsulation: HDLC/PPP/Frame Relay/MLPPP/ MLFR. By default, HDLC encapsulation is selected.**

The steps to configure encapsulation on the interface is already covered in the previous section. The same steps hold good for configuring encapsulation on a serial interface. For more details on encapsulation configuration, refer to "Configure Encapsulation on a Channelized Serial Interface" section.

Step 4: After configuring the parameters, click **Apply** to save the Serial interface configuration or click **Cancel** to cancel the operation.

CONFIGURE LOGICAL INTERFACE

Follow the procedure below to configure logical interfaces. You can configure Virtual LAN, GRE Tunnel, and Loopback interfaces.

Step 1: Click **Add Logical Interface** on the **Interfaces** page. A drop-down list lists the logical interfaces that can be configured: **Virtual LAN/GRE Tunnel**/ **Loopback**. Choose the required option.

VIRTUAL LAN (VLAN)

You can configure VLAN on L2GE Switch ports. L2GE card has 8 Switch Ports and VLAN on L2 ports can be configured for three modes of operation.

- **Access** - This is the default mode. Used to connect end stations (LAN devices) to switch ports. Each access port can belong to only 1 VLAN. This port can send and receive untagged packets.
- **Trunk** - A trunk port sends and receives only tagged packets. It interconnects one OA-700 (as a switch) to another OA-700 (as a router). VLAN information is exchanged between them.
- **Hybrid** - Used to connect to both VLAN-aware (tagged) devices as well as VLAN unaware (untagged) devices.

Some points to note:

- By default, all the L2 Switch Ports are in Access mode and they are a part of VLAN 1 (already configured in the device).
- If a VLAN is configured on a particular L2 card, it cannot be configured on another card.
- VLAN can be configured for a L2 card and not across L2 cards (i.e, if your device has more than one L2 card). For routing across VLANs or between traffic on the L2 card, IRB (Integrated Routing and Bridging) is to be used. This enables L2 port capable of taking part in both bridging and routing at the same time.

  IRB allows multiple router interfaces to be in a common VLAN, with routing across such VLAN's.
- A given VLAN interface for IRB can be used only on the 8 ports of the same L2-GE card.
- If IRB is not enabled for a VLAN interface, policies cannot be configured.
- 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.

You can also configure Per VLAN STP for the VLAN.

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.

Follow the following procedure to configure VLAN, enable IRB, and configure Per VLAN STP.

Step 1: Click **Add Logical Interface** on the **Interfaces** page. A drop-down list lists the logical interfaces that can be configured. Select **Virtual LAN** from the list. **Configure VLAN** page is displayed as shown below.

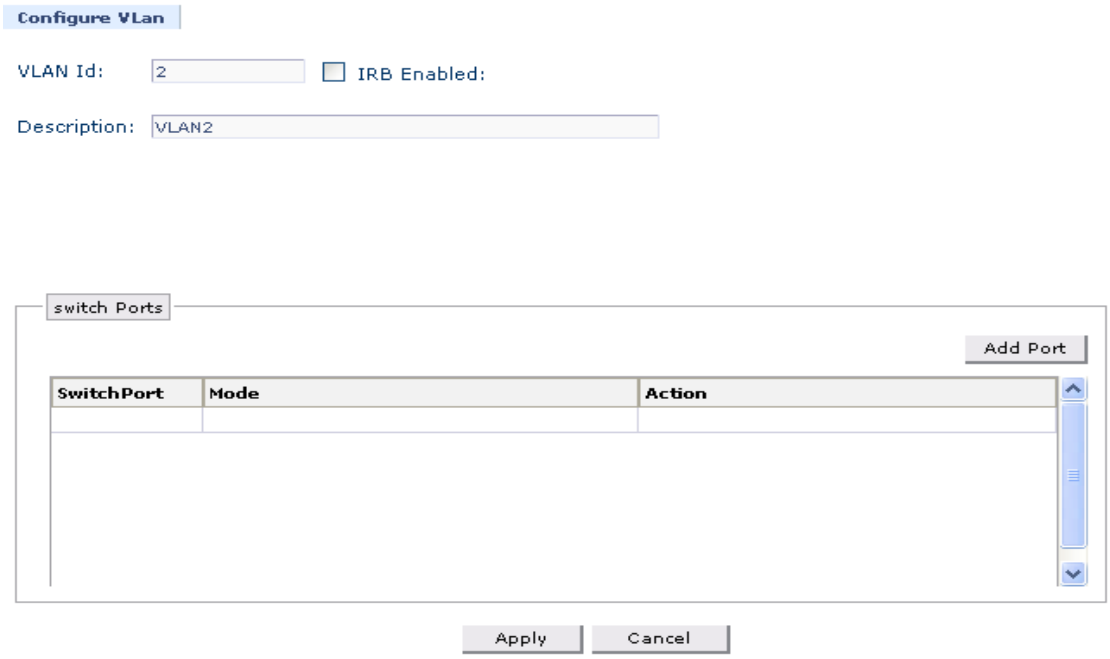


Figure 25: Interfaces - Configure VLAN

Step 2: Enter the VLAN ID in the **VLAN ID** field.

Step 3: Check the **IRB Enabled** check box to configure IRB. The IP Address and Mask field appears when this check box is selected.

IRB (Integrated Routing and Bridging) allows you to route a given protocol between routed interfaces and bridge groups within a single switch router.

- Enter the IP address and the Mask in the **IP Address** and **Mask** fields.

Step 4: Click **Add Port** to add the Switch Port/s to the VLAN. **Switch Port Configuring** pop up window is displayed.

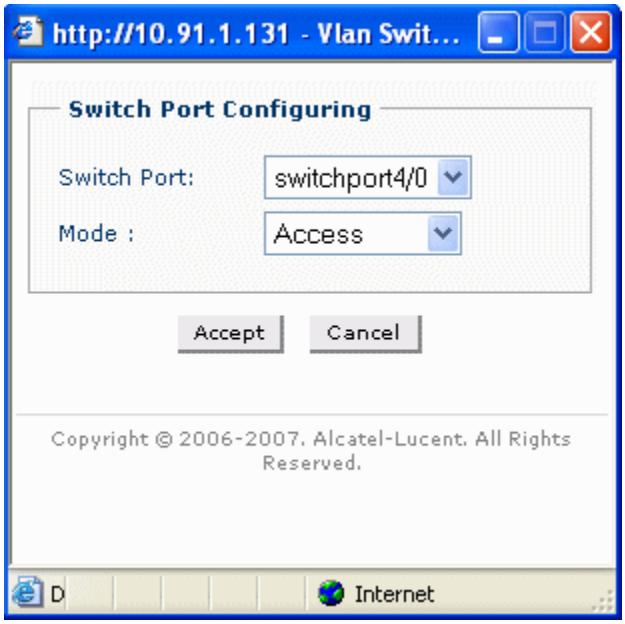


Figure 26: Interfaces - Configure VLAN - Switch Port Configuring

- Select the Switch Port from the **Switch Port** drop down list.
- Select the mode from the **Mode** drop down list: **Access/Trunk/Hybrid**. This command is used configure the L2 interface in the access, trunk or hybrid mode.
- Click **Accept**. The configured switch port is displayed in the Switch Port table. Repeat this procedure to add more ports.

Note: Maximum of 8 switch ports can be added to a VLAN. Switch ports with only trunk mode can be added to multiple VLANs.

Step 5: Click **Apply** to configure the VLAN or click **Cancel** to cancel the operation. VLAN is updated and a prompt to configure STP is displayed.

Step 6: Click **OK** to continue STP configuration. **STP Config** page is displayed with the default values in the respective fields.

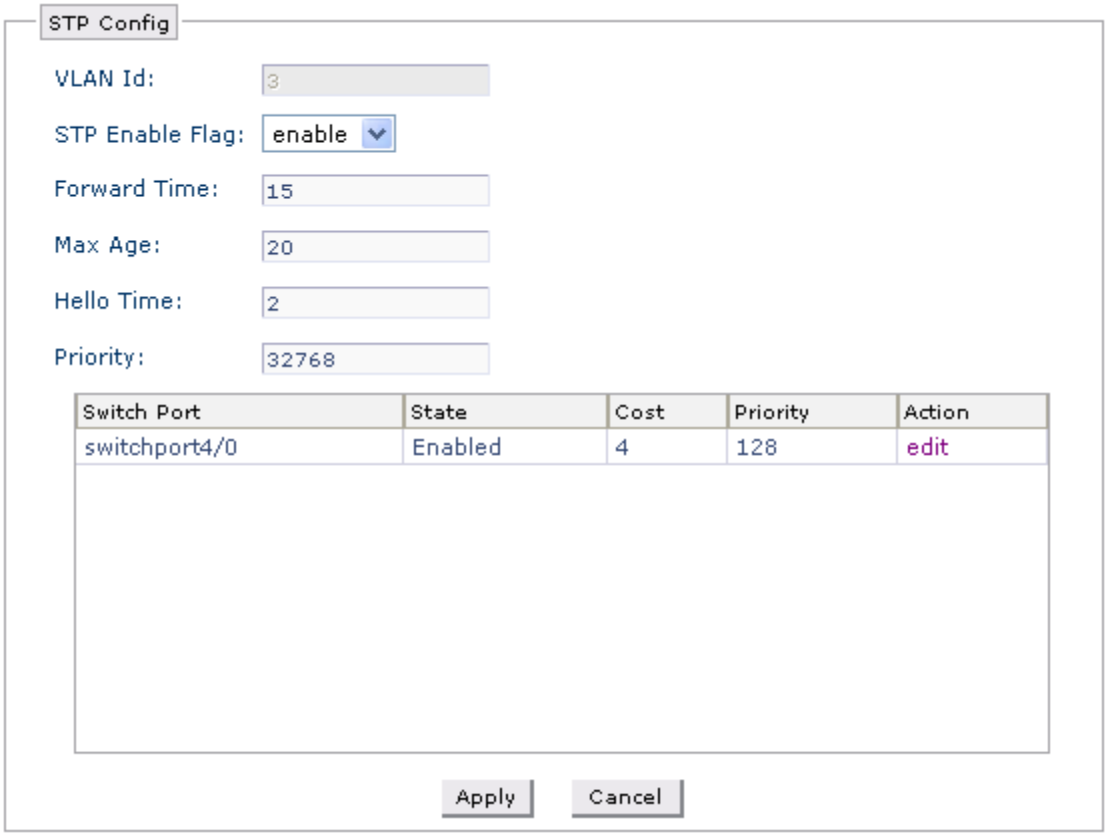


Figure 27: Interfaces - Configure VLAN - STP Config

Step 7: The VLAN ID for the selected VLAN is displayed in the **VLAN ID** field. This is not editable.

Step 8: Enable/Disable the STP Flag by selecting **Enable/Disable** option from the **STP Enable Flag** drop down list.

- Enable enables Spanning Tree parameters - Forward Time, Max Age, Hello Time and Priority fields. Enter the values in the respective fields. An option to edit the STP parameters is also enabled.
  i. **Forward Time** - Enter the forward time in the range 4 - 30 seconds. Default is 15 seconds.
  ii. **Max Age** - Enter the max age value in the range 6 - 40 seconds. Default is 20 seconds.
  iii. **Hello Time** - Enter the value in the range 1- 10 seconds. Default is 2 seconds.
  iv. **Priority** - Enter the bridge priority in the range 0 - 65535. Default is 32768.
- Selecting **Disable** option disables the Forward Time, Max Age, Hello Time and Priority fields. Also, the option to edit the STP parameters is disabled.

Step 9: Configure the Switch Port parameters. These are configured on per port basis.

- Click **Edit** link under **Action** column against the Switch Port whose state, priority, and cost parameters are to be configured.
- Configure the required value in the respective fields.
  i. Select the state from the **State** drop down list: **Enable/Disable**
  ii. Enter the path cost in the **Cost** field (range 1- 65535). The default value is 4.

Note: When two bridges compete for position as the root bridge, configure the PVST cost to prioritize an interface.

  iii. Enter the port priority in the **Priority** field (range 0 - 255). This priority value is used to prioritize an interface when two bridges compete for position as the root bridge. Default value for port-priority is 128.
  iv. Click **OK** to configure the Switch Port parameters or click **Cancel** to cancel the operation.

Step 10: Click **Apply** to save the VLAN STP configuration or click **Cancel** to cancel the operation.

Step 11: The VLAN interface thus configured is displayed in the Interfaces page.

EDIT VLAN CONFIGURATION

Follow the procedure given below to edit the VLAN configuration:

1. In the **Interfaces** page, click **Edit All** icon against the VLAN that needs to be edited. **Configure VLAN** page is displayed.

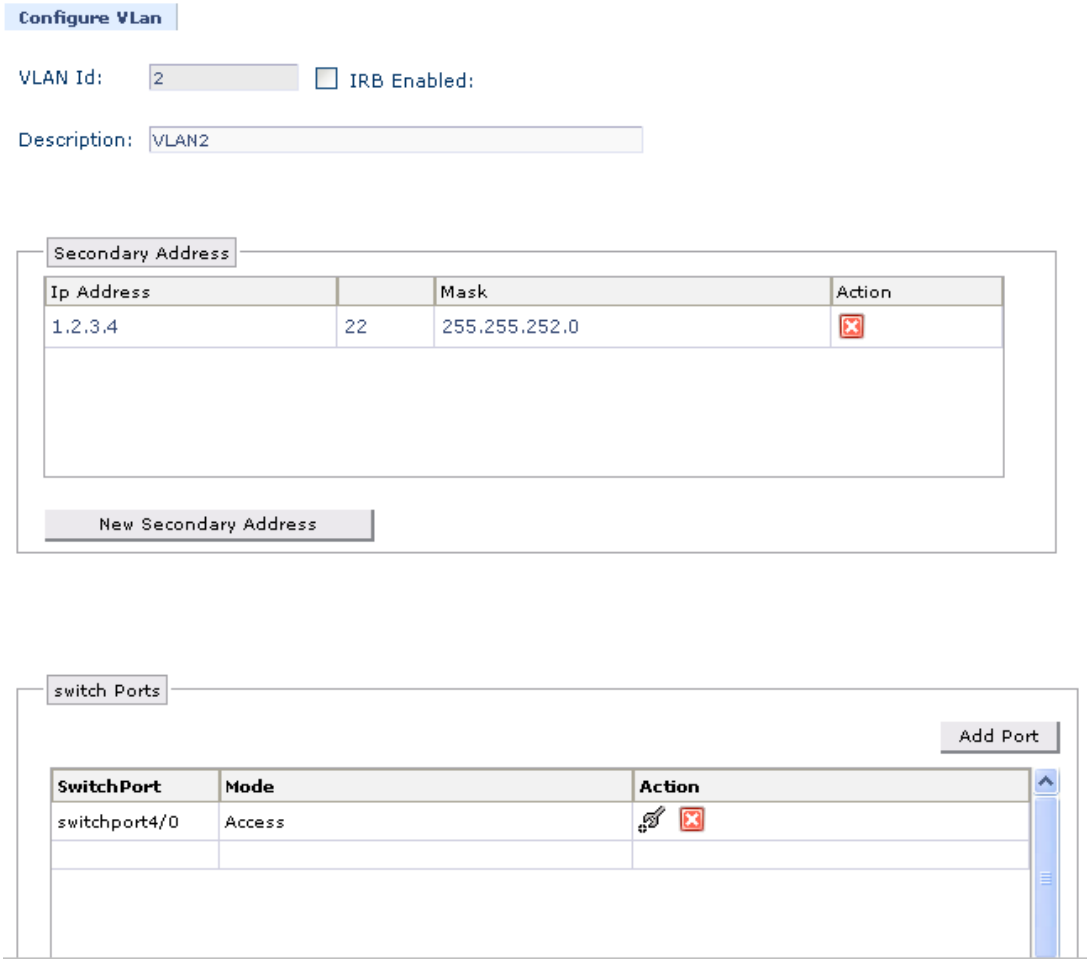


Figure 28: Interfaces - Edit VLAN Configuration

2. VLAN Id is not editable.
3. If the IRB is enabled, the IP Address and Mask field displays the configured IP address and mask. Modify if necessary.
4. You can configure the secondary IP address for the VLAN interface in the **Secondary Address** table.

   Click **New Secondary Address** to add a new secondary address to the selected interface. Fields to enter the IP address is populated.

   - Enter the secondary IP address and subnet mask for the interface in the **IP Address** and **Mask** column.
   - Click **Apply** to add the secondary IP address, or click **Cancel** to cancel adding secondary IP address.
   - Click **Delete** icon in the Action column to delete the secondary address.

5. The Switch Ports table displays the switch ports configured for the VLAN interface. You can edit/delete the switch ports configured.

   Edit Switch Port

   - In **Edit** icon against the switch port that needs to be edited. **Switch Port Configuring** pop up window is displayed.
   - Edit the Mode for the switch port. Click **Accept** or click **Cancel** to cancel the operation.

   Delete Switch Port

   - Click **Delete** icon against the switch port to be deleted.
   - The switch port gets deleted.
6. Click **Add Port** to add new switch ports.
7. After making the necessary changes, click **Apply** to save the changes or click **Cancel** to cancel the operation.

EDIT STP CONFIGURATION

STP for a VLAN can be configured by selecting a particular VLAN in the Interfaces page.

1. In the **Interfaces** page, click **Edit STP** icon for the VLAN interface whose STP parameters is to be configured. **STP Config** page is displayed.
2. The VLAN ID for the selected VLAN is displayed in the **VLAN ID** field. This is not editable.
3. Make the necessary changes and click **Apply** to save the changes or click **Cancel** to cancel the operation.

DELETE VLAN INTERFACE

1. In the **Interfaces** page, click **Delete** icon in the **Action** column against the VLAN to be deleted.
2. Confirm at the prompt to delete the VLAN.

CONFIGURE TUNNEL INTERFACE

You can configure IPsec tunnel interface or GRE tunnel interface from the interfaces page.

- **Generic Routing Encapsulation Tunnel Interface**

  Generic Routing Encapsulation is a simple, stateless protocol that allows for the tunneling of any in GRE. 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.

  With GRE tunnels, a provider does not need to convert any core devices to MPLS or establish MP-BGP sessions. There is also no need to establish BGP route reflectors or modify existing routing configuration or policies. Therefore, a provider may offer an alternative VPN solution to MPLS in a much shorter time frame with greatly simplified provisioning and support. GRE tunnels are used to carry non-IP traffic (like IPX, Appletalk, DECnet from legacy networks) over an IP backbone.

GRE tunnel setup and mapping

A GRE tunnel is configured by specifying two endpoints, one local and the other remote. In order to establish a bidirectional path, a GRE tunnel must be configured from the remote endpoint as well. No intermediary routers need to be configured, and the tunnel rides on top of 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

  Because of the flexible nature of GRE, tunnels can be established in different topologies.

  This 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 OA-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 connection 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.

- ACLs on GRE tunnels

  Access Control Lists (ACLs) 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. ACLs 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 without the need to migrate to an MPLS core network. Contexts and interfaces are used in combination with GRE tunneling to create a VPN service complete with private addressing, routing, user authentication, and 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 tunneled.
- GRE packet is encapsulated using an outer IP header.
- Outer IP header’s IP protocol value = 47

Alcatel-Lucent Specific Overview

- OA-700 does not support overlapping of private addresses.
- The source IP address must be configured either on a loopback interface or on one of the physical interfaces.

- **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, ACL can be applied.
  - Traffic classifier will be route 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 when configuring OA-700 for IPsec Tunnel Interface.

  - Routing setup must be in ordinance.
  - The interface being configured be a configurable interface, i.e., associated with an IP address.
  - 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.
  - Parameters required in tunnel negotiation should be configured. These parameters are IPSec transform set, IKE policy, SA lifetime, PFS, IKE Identity.

  Default Configuration

  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 IKE policy 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**

Follow the below procedure to add IPSec or GRE Tunnel:

Step 1: Click **Add Logical Interface** on the **Interfaces** page. A drop-down list lists the logical interfaces that can be configured. Select **Tunnel** from the list. **Tunnel Configuration** page is displayed as shown below.

Figure 29: Interfaces - Tunnel Configuration

Step 2: Configure a tunnel by entering the mode, tunnel number, IP address, and description for the interface.

- Enter the number for the tunnel interface in the **Tunnel Number** field.
- Select **IPsec/GRE** radio button to configure the mode on the tunnel interface. By default, tunnel is configured in the GRE mode.
- Enter the IP address and the subnet mask of the tunnel interface in the **IP Address** and **Mask** field. Click **Remove** to delete the IP address.
- Enter the description for the tunnel in the **Description** field.

Step 3: Click **Apply** to configure the tunnel interface or click **Cancel** to cancel the operation.

Step 4: The tunnel interface thus configured is displayed in the Interfaces page.

EDIT TUNNEL INTERFACE

Follow the procedure given below to configure GRE/IPsec tunnel interface:

Step 1: In the **Interfaces** page, click **Configure** icon for the GRE/IPsec tunnel interface whose parameters are to be configured. This displays the **Configuration Serial** page in the Center Panel.

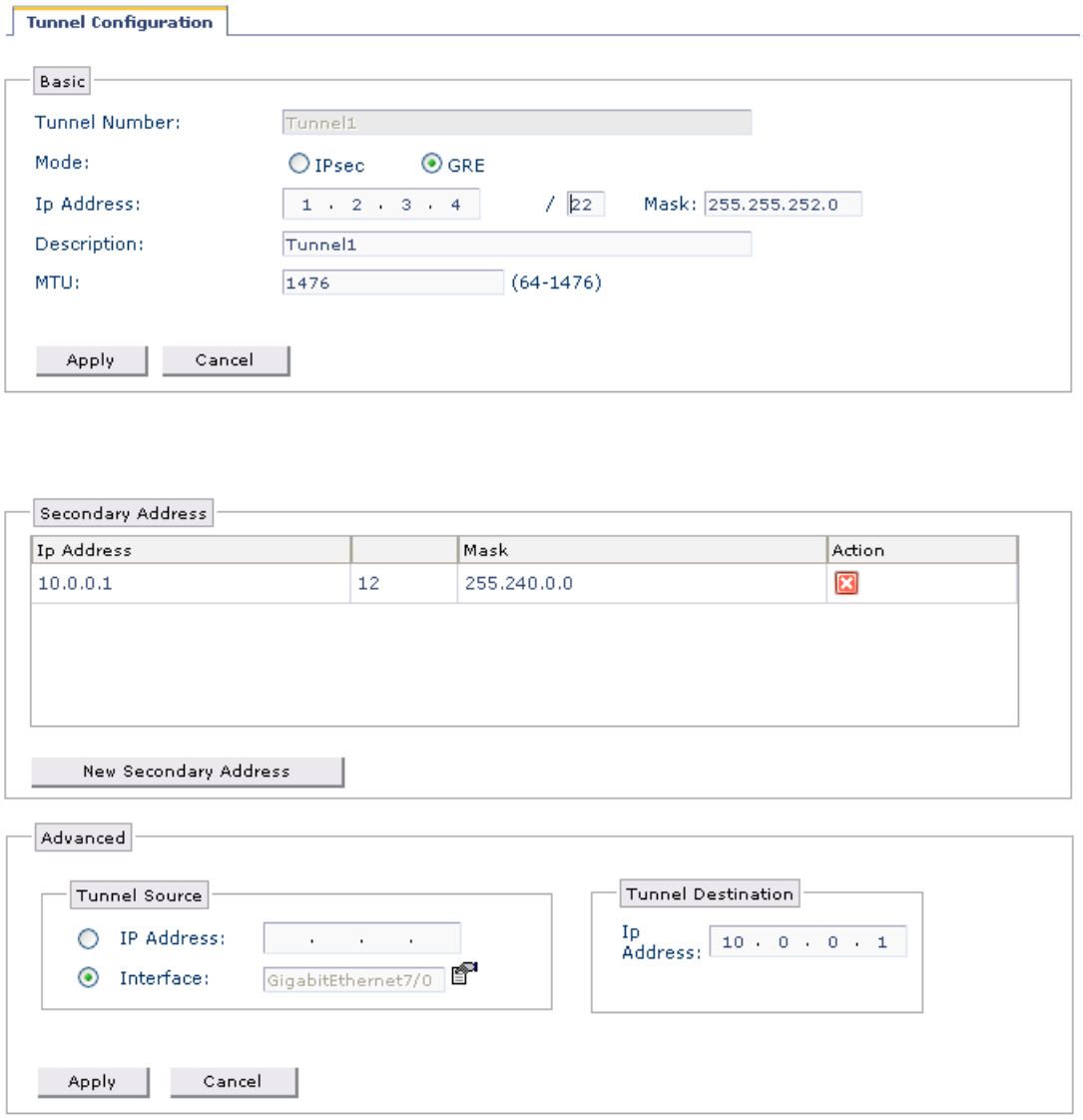


Figure 30: Interfaces - Tunnel Configuration

Step 2: Tunnel number, mode, IP address, and description configured for the interface is displayed in the **Basic** box. Make the necessary changes if necessary. Tunnel Number is not editable.

Step 3: Configure the Secondary IP address for the tunnel interface in the **Secondary** box.

Click **New Secondary Address** to add a new secondary address to the selected interface. Fields to enter the IP address is populated.

1. Enter the secondary IP address and subnet mask for the interface in the **IP Address** and **Mask** column.
2. Click **Apply** to add the secondary IP address, or click **Cancel** to cancel adding secondary IP address.
3. Click **Delete** icon in the Action column to delete the secondary address.

Step 4: Enter the tunnel source and tunnel destination information in the **Advanced** box.

- Enter the tunnel source information in the **Tunnel Source** box.
  i. Enter the source IP address of the tunnel interface in the **IP Address** field or Select the interface that the tunnel will use from the **Interface** list.

Note: The source IP address of the tunnel must be of either a loopback interface or one of the physical interfaces. Ensure that the interface is reachable from the other end of the tunnel.

- Enter the destination IP address of the tunnel at the remote end in the **Tunnel Destination** box. This is the source interface from the point of view of the other end of the tunnel.
  i. Enter the IP address in the **IP Address** field. Make sure that this address is reachable using the ping command; else, the tunnel will not be created properly.

Step 5: Click **Apply** to configure the tunnel interface or click **Cancel** to cancel the operation.

DELETE TUNNEL INTERFACE

1. In the **Interfaces** page, click **Delete** icon in the **Action** column against the tunnel that is to be deleted.
2. Confirm at the prompt to delete the tunnel.

LOOPBACK INTERFACE

Follow the below procedure to add a loopback interface.

Step 1: Click **Add Logical Interface** on the **Interfaces** page. A drop-down list lists the logical interfaces that can be configured. Select **Loopback** from the list. **Loopback Configuration** page is displayed as shown below.

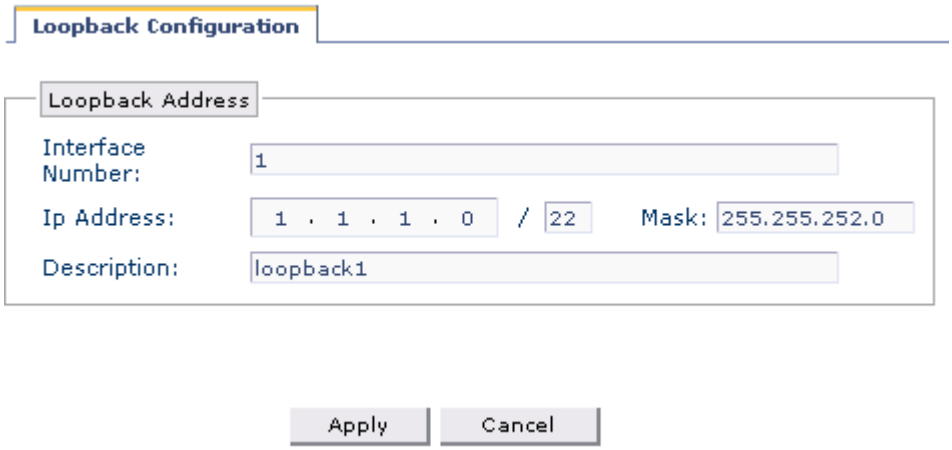


Figure 31: Interfaces - Loopback Configuration

Step 2: Configure the loopback interface by entering the interface number, IP address, and description for the interface.

- Enter the number for the interface number in the **Interface Number** field.
- Enter the IP address and the subnet mask of the interface in the **IP Address** and **Mask** field. Click **Remove** to delete the IP address.
- Enter the description for the loopback interface in the **Description** field.

Step 3: Click **Apply** to configure the loopback interface or click **Cancel** to cancel the operation.

Step 4: The loopback interface thus added is displayed in the Interfaces page.

CONFIGURE LOOPBACK INTERFACE

Follow the procedure below to configure Loopback interface.

Step 1: On the **Interfaces** page, click **Configure** icon for the Loopback interface to be configured. **Configuring Loopback** page is displayed in the Center Panel.

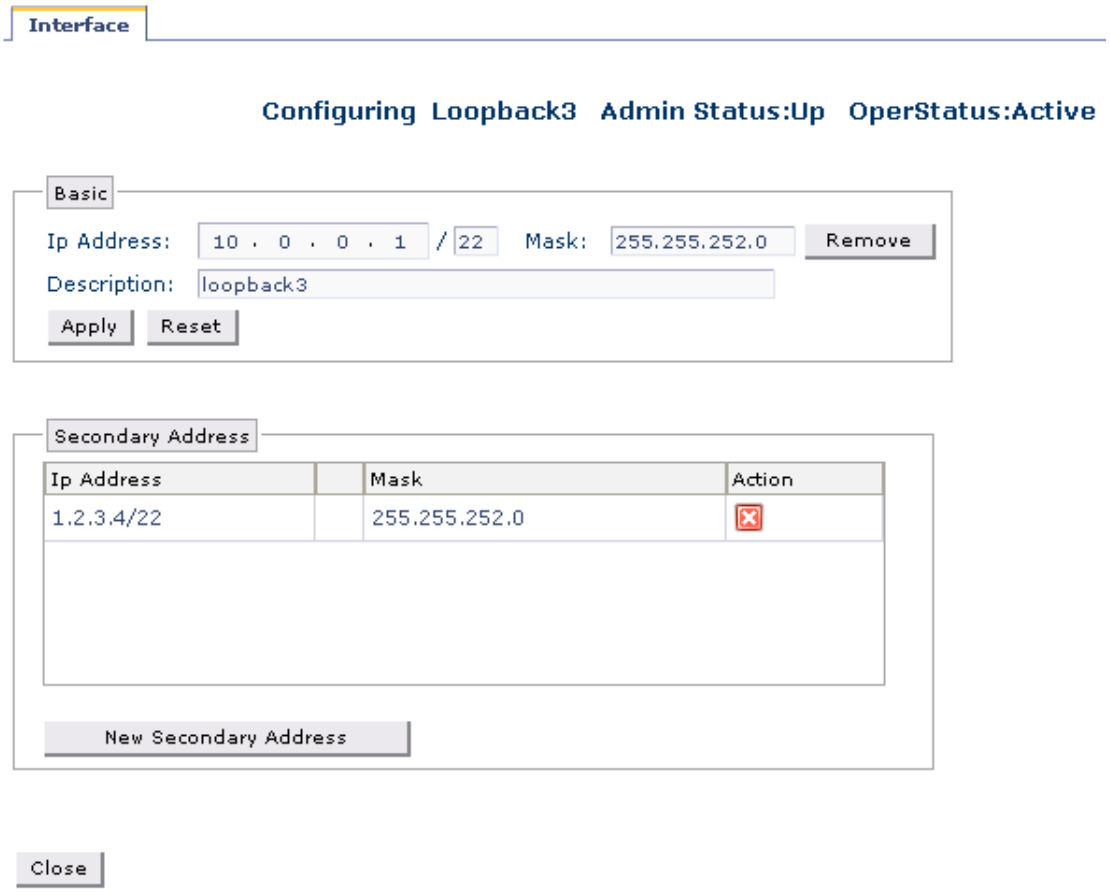


Figure 32: Interfaces - Loopback Configuration

Step 2: The primary address configured for the interface is displayed in the **Basic** box.

1. IP address and the description configured for the interface is displayed in the **Basic** box.
2. Make the changes and click **Apply** or click **Reset** to retain the original details.

Step 3: Configure Secondary IP address for the loopback interface in the **Secondary** box.

Click **New Secondary Address** to add a new secondary address to the selected interface. Fields to enter the IP address is populated.

1. Enter the secondary IP address and subnet mask for the interface in the **IP Address** and **Mask** column.

2. Click **Apply** to add the secondary IP address, or click **Cancel** to cancel adding secondary IP address.
3. Click **Delete** icon in the Action column to delete the secondary address.

Step 4: Click **Close** at the bottom of the page to save the Loopback Interface configuration.

DELETE LOOPBACK INTERFACE

1. In the **Interfaces** page, click **Delete** icon in the **Action** column against the loopback interface that is to be deleted.
2. Confirm at the prompt to delete the loopback interface.

ASSOCIATE POLICY TO AN INTERFACE

You can attach a Filter, NAT, Firewall, QoS, Transparent Firewall, Policy Based Routing, and IPSec policies on the selected interface if these policies are already configured in your OA-700 system.

Steps to configure these individual policies are explained in detail in the later section of this document.

Follow the procedure given below to attach policy to an interface:

Step 1: In the **Interfaces** page, click **Policy** icon against the interface to which policy/ies is to be attached. **Policy Association** page is displayed.

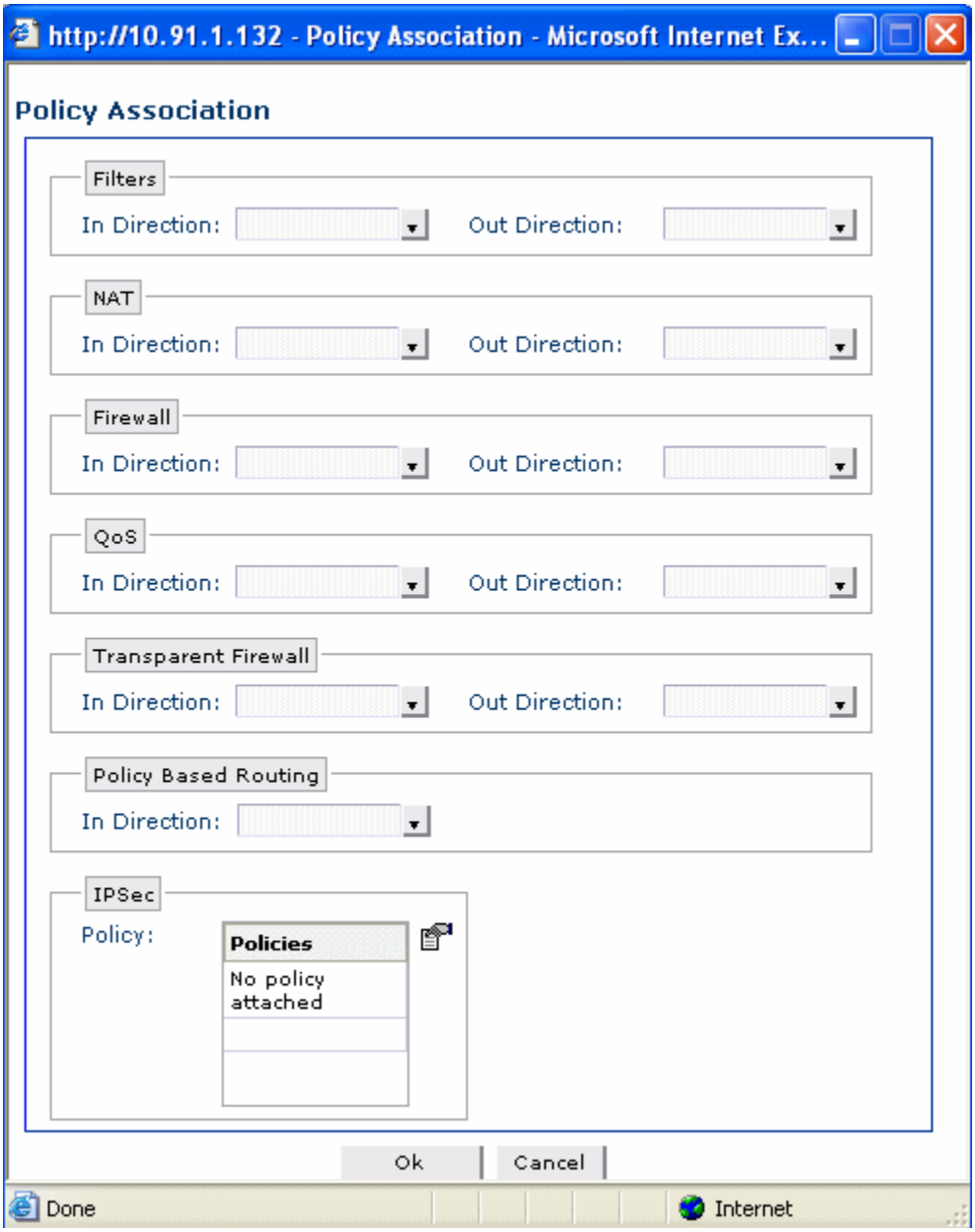


Figure 33: Interfaces - Policy Association

1. To attach a filter:

   Under the **Filters** table, configure the following:

   i. Click **In Direction** drop-down list. Filters created in your system are displayed. Select the filter to be attached to the interface in the ingress direction from the list.

   ii. Click **Out Direction** drop-down list. Filters created in your system are displayed. Select the filter to be attached to the interface in the ingress direction from the list.

   If filters are not configured, see "Creating a Filter" section.

2. Similarly select the required **NAT**, **Firewall**, **QoS, Transparent Firewall**, **Policy Based Routing** policies to be attached to the interface in the Ingress and Egress direction from their respective fields.

   The In Direction and Out Direction drop-down lists displays the NAT, Firewall, QoS, Transparent Firewall, Policy Based Routing policies already configured in your system.

   If NAT policy is not configured, see "Creating NAT Policy and Configure NAT Rule" section.

   If Firewall policies are not configured, see Creating Firewall Policy section.

   If QoS policies are not configured, see "QoS (Quality of Service)" section.

   If Transparent Firewall policies are not configured, see "Creating TF Policy" section.

   If Policy Based Routing policies are not configured, see "Configuring an IP Policy and a Rule for an IP Policy" section.

3. Attach an IPSec policy.

   - Select the IPSec policy/ies to be attached to the interface from the list. The IPsec policies already configured in your system is displayed. Check the check box against the IPSec policy/ies.

   If IPSec policies are not configured, see "IPSec Configuration Wizard" section.

Step 2: Click **OK** to attach the policies to an interface or click **Cancel** to cancel the operation.

VIEW INTERFACE DETAILS

Follow the procedure given below to view the details of a selected interface:

1. In the **Interfaces** page, click **Interface Name** whose configuration details are to be viewed.
2. The interface details for the selected interface are displayed in the **Interface Details** table. The details displayed vary based on the selected interface.

ACTIVATE THE INTERFACE

To bring the interface up, click **Activate** icon for the selected interface. Confirm at the prompt to activate the interface. This changes the administrative status of the interface to ‘Active’.

Note: The **Activate** icon is displayed only when the interface is in ‘inactive’ state.

SHUTDOWN THE INTERFACE

To shutdown an interface, click **Shutdown** icon for the selected interface and confirm at the prompt. This will administratively bring down the interface and the status changes to ‘Inactive’.

Note: The **Shutdown** icon is displayed only when the interface is in ‘active’ state.

DHCP (Dynamic Host Configuration Protocol)

The DHCP page allows you to enable OA-700 to act as DHCP Server or DHCP Relay.

DHCP Server

DHCP is a protocol for dynamically assigning IP addresses to 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 Provider) use dynamic IP addressing for dial-up users.

Alcatel-Lucent Specific Overview

Note: By default, the DHCP service is disabled and you should 'enable' the DHCP server explicitly for the service to become available. Currently, you can enable the DHCP service only through CLI.

- The DHCP server in 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**.
  - **Pool** - A pool is a collection of IP addresses maintained by the DHCP server. A pool can have only a single network or host configured inside it, and is accordingly called a network or a host pool.
  - **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.

    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.

VIEWING DHCP SERVER

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **DHCP** sub-menu.

DHCP page has two tabs: **DHCP Sever** and **DHCP Relay**. By default, **DHCP Sever** page is displayed in the center panel.

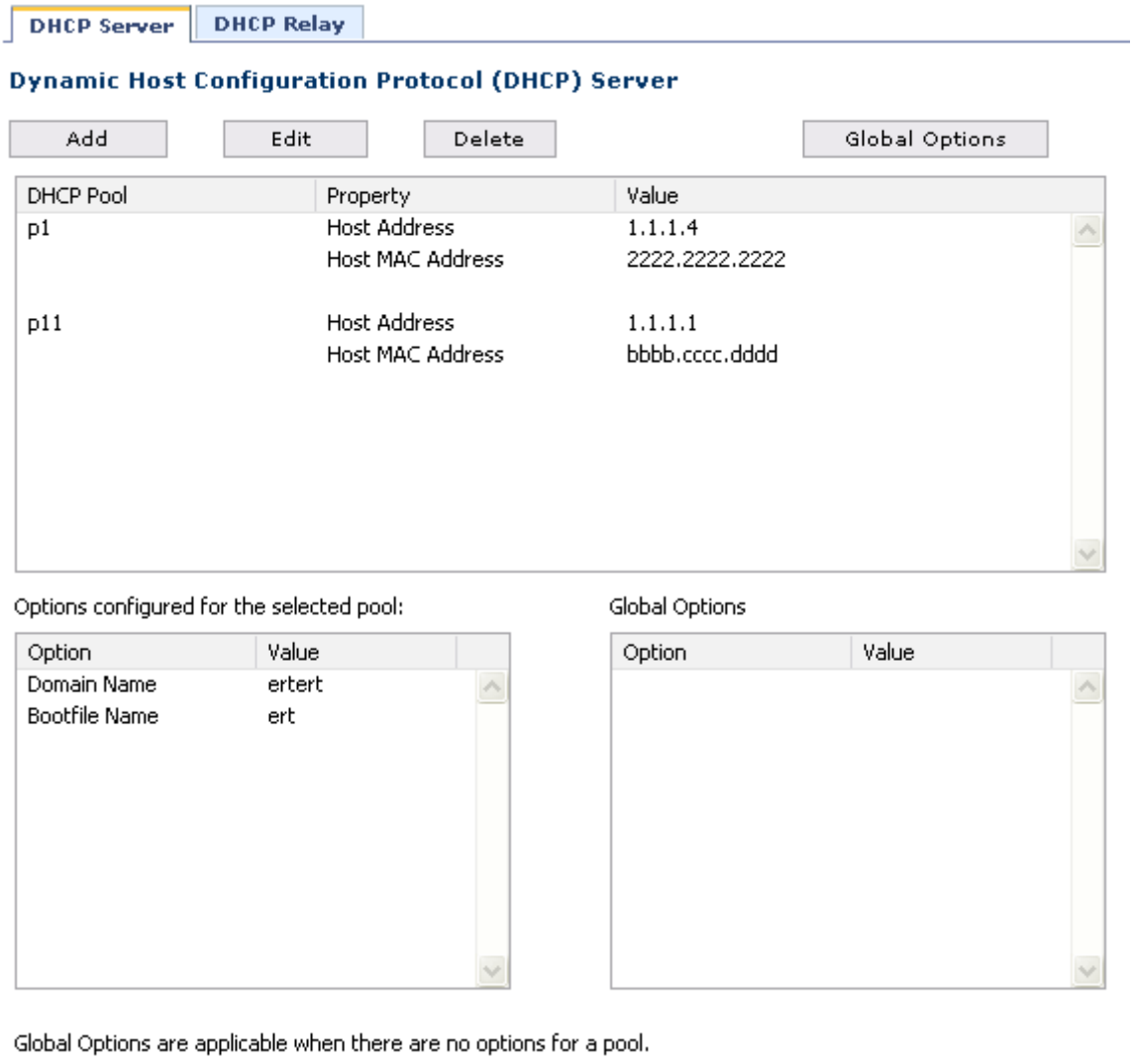


Figure 34: DHCP Server

The table below provides description for DHCP Server page.

Table 5: DHCP Server Field Description

Field	Description
DHCP SERVER	
DHCP Pool	DHCP Pool name.
Property	Pool property
Value	Values of the pool like IP address, MAC address and so on.
Options configured for the selected pool	Displays the options configured for the selected pool
Global Options	Displays the global options configured for the pools.

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.

To configure a DHCP pool, follow the procedure given below:

Step 1: Click **Add** in the **DHCP Server** page.

Step 2: Add DHCP Pool pop up window is displayed. This window has two tabs: **DHCP IP Address** and **Options**. By default, **DHCP IP Addresses** tab is selected, and its details are displayed.

CONFIGURE NETWORK POOL

1. Enter the name for the DHCP pool in the **DHCP Pool Name** field.
2. Under the pool type, select **Network** radio button. By default, **Network** is selected. This allows you to specify the network to which the pool belongs to.

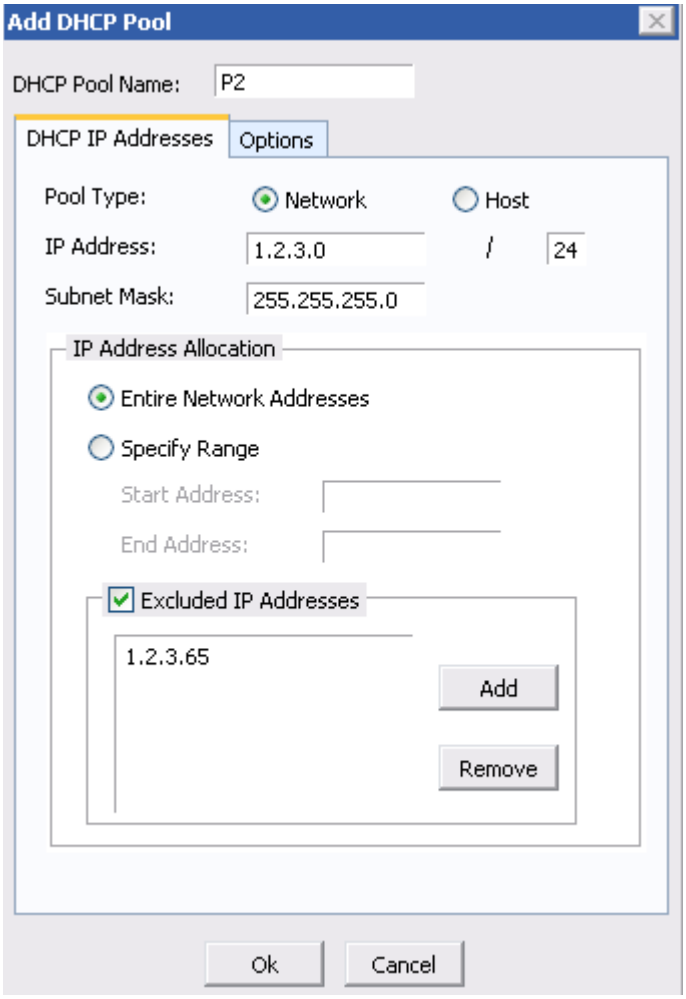


Figure 35: DHCP Server - Add DHCP Pool - Network

3. Enter the IP address and the Mask in the **IP Address** and **Subnet Mask** fields.

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.

4. Configure the following in the IP address allocation box.
   - Select **Entire Network Addresses** radio button to specify the entire network addresses to be available to the client.
   - Select **Specify Range** radio button to configure the range of IP addresses within the network of the pool.
     i. Specify the lower and the upper addresses of the network range in the **Start Address** and **End Address** fields. The range should not include the network address and the broadcast address of the network.

- Select **Excluded IP Addresses** check box to exclude an IP address of the range from the pool. The excluded IP address should exist within the configured range.
  i. Click **Add**. **Add IP** pop up window is displayed.

Figure 36: DHCP Server - Add DHCP Pool - Network - Exclude IP Address

  ii. Enter the IP address to be excluded in the IP Address field. Click **OK**.
  iii. The IP address entered is listed in Exclude IP Addresses box. Add as many IP addresses as required.
  iv. To remove the IP address from the list, click **Remove**.

5. After configuring the parameters, click **OK** to save the network pool or click **Cancel** to cancel the operation.

CONFIGURE HOST POOL

This allows you to statically bind an IP address with a hardware (MAC) address. The IP address should exist within the configured network range.

1. In the **Add DHCP Pool** window, enter the name for the DHCP pool in the **DHCP Pool Name** field.
2. Under the pool type, select **Host** radio button.

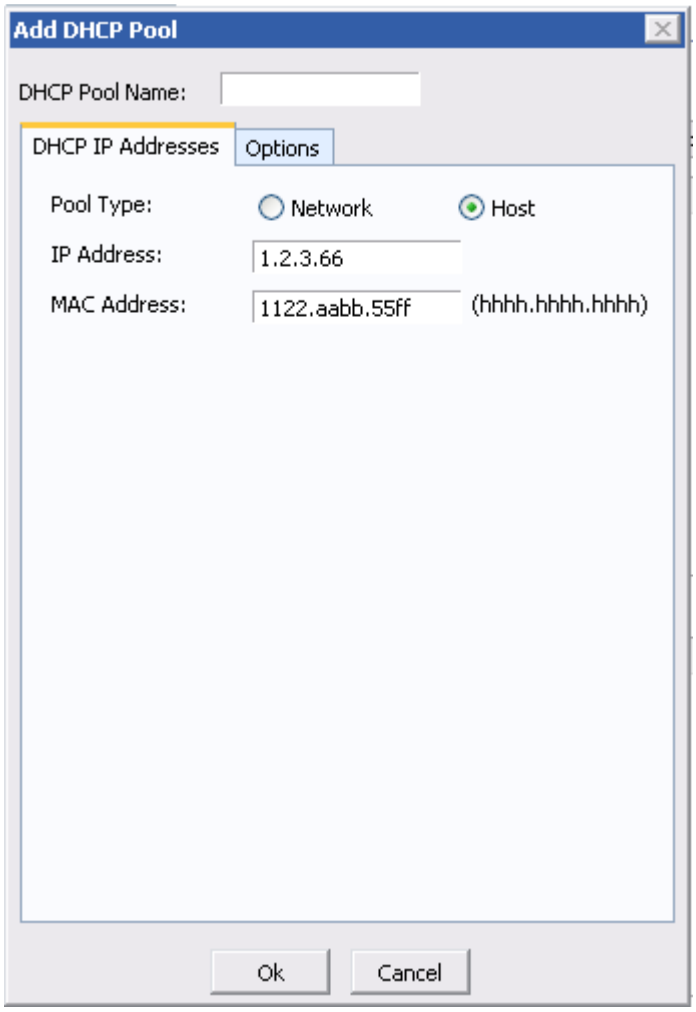


Figure 37: DHCP Server - Add DHCP Pool - Host

3. Enter the host IP address (that exists within a configured network pool) in the **IP Address** field.
4. Enter the hardware address of the host in the **MAC Address** field.
5. Click **OK** to save or click **Cancel** to cancel the operation.

DHCP Pool Options

This window allows you to configure DHCP Options to a specific pool.

1. Enter the name for the DHCP pool in the **DHCP Pool Name** field.
2. Select **Options** tab to configure the pool options.

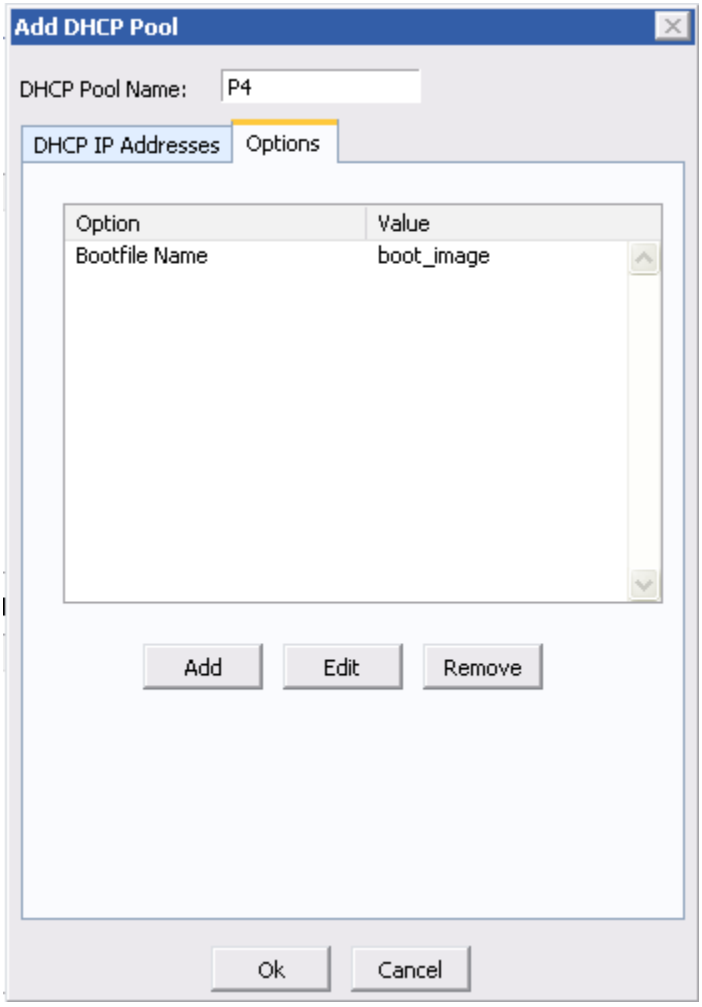


Figure 38: DHCP Server - Add DHCP Pool - Options

3. Click **Add** to add an option to a pool. The following pop up window is displayed.

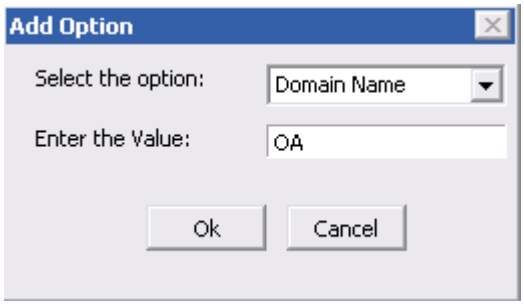


Figure 39: DHCP Server - Add DHCP Pool - Options - Add Option

4. Select the option to be added from the drop-down list, and enter the corresponding value in the **Value** field.
5. Click **OK**. The option added to the pool is listed in the options tab. Add as many options as required.
6. Click **OK** to save the DHCP pool options or click Cancel to cancel the operation.

Edit DHCP Pool Option

1. Select the option to be edited from the options listed in the Options tab. Click **Edit**. Edit Option pop up is displayed.
2. Make the required changes and click **OK** to save the changes.

Delete DHCP Pool Option

1. Similarly, select the option to be deleted from the options listed in the Options tab. Click **Delete**.
2. Confirm at the prompt to delete.

EDIT DHCP POOL

To edit a DHCP pool, follow the procedure given below:

1. DHCP Server page displays the list of the DHCP pools configured. Select the DHCP pool whose details are to be edited and click **Edit**.
2. **Edit DHCP pool** pop up window is displayed.
3. Make the required changes. The DHCP Pool name is not editable. Based on the pool type selected, the network or the host radio button is not editable.
4. Click **OK** to save the changes.

DELETE DHCP POOL

To delete a DHCP pool, follow the procedure given below:

1. DHCP Server page displays the list of the DHCP pools configured. Select the DHCP pool to be deleted, and click **Delete**.
2. Confirm at the prompt to delete.

CONFIGURE DHCP GLOBAL OPTIONS

You can configure Global Options applicable to all the configured 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.

To configure a DHCP global option, follow the procedure given below:

Step 1: Click **Global Options** in the **DHCP Server** page.

Step 2: Configure Global Options pop up window is displayed.

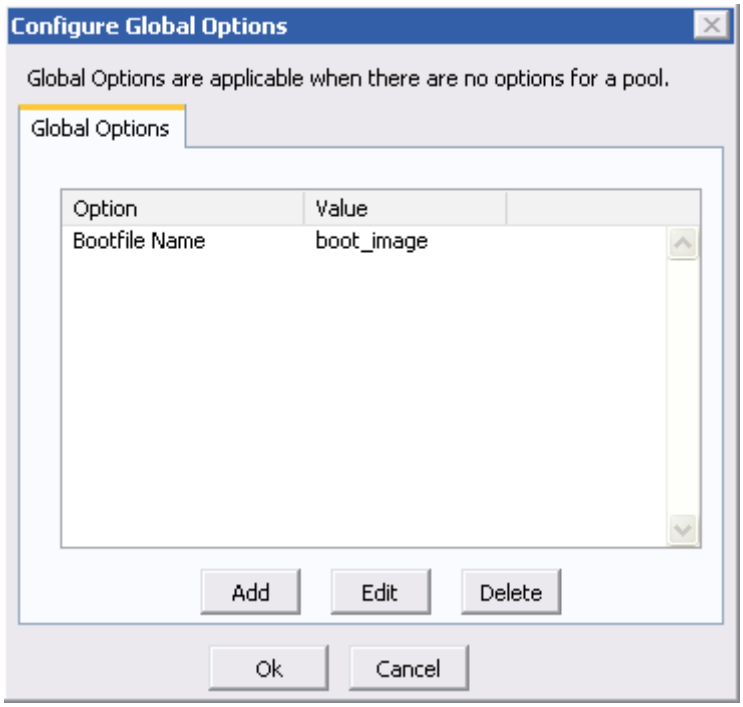


Figure 40: DHCP Server - Configure Global Options

3. Click **Add** to add a global option. The following pop up window is displayed.

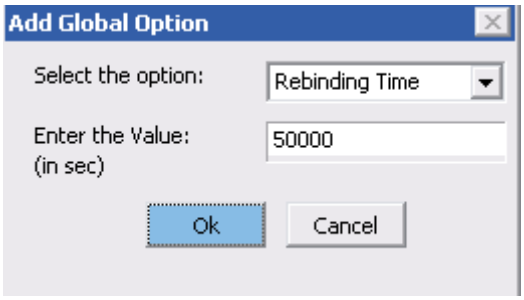


Figure 41: DHCP Server - Configure Global Options - Add Global Option

4. Select the option to be added from the drop-down list, and enter the corresponding value in the **Value** field.
5. Click **OK**. The global option added is listed in the Configure Global Options window. Add as many options as required.
6. Click **OK** to save the global options or click Cancel to cancel the operation.

Edit DHCP Global Option

1. Configure Global Options window lists all the configured global options. Select the global option to be edited from the list and click **Edit**. **Edit Global Option** pop up is displayed.
2. Make the required changes and click **OK** to save the changes.

Delete DHCP Global Option

1. Similarly, select the global option to be deleted from the list, and click **Delete**.
2. Confirm at the prompt to delete.

DHCP Relay

DHCP Relay Agent acts as an intermediary between clients and servers by listening to client DHCP broadcast requests and forwarding them to the DHCP 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

We implement forwarding to the DHCP server directly or via rebroadcast on another interface on the OA-700.

Viewing DHCP Relay

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **DHCP** sub-menu.

DHCP page has two tabs: **DHCP Sever** and **DHCP Relay**. Click **DHCP Relay** tab. The following page is displayed in the center panel.

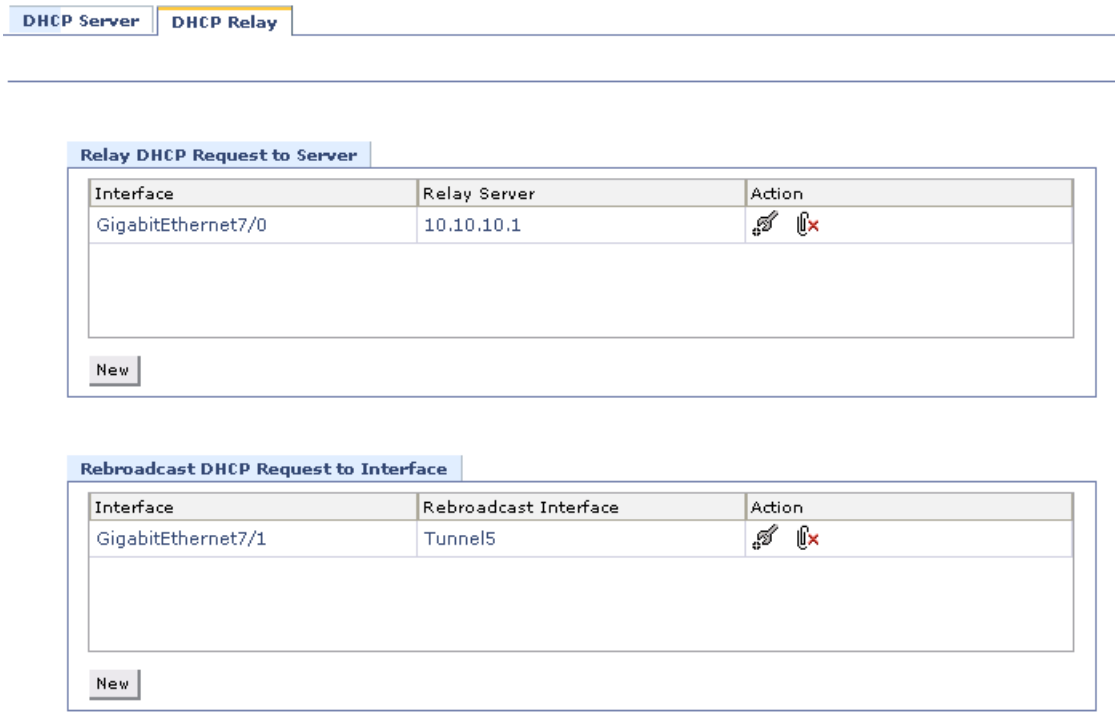


Figure 42: DHCP Relay

The table below provides description for DHCP Relay page.

Table 6: DHCP Relay Field Description

Field	Description
DHCP RELAY	
Relay DHCP Request to Server	
Interface	The interface on which the DHCP relay is configured. A maximum of four DHCP relays can be configured on an interface.
Relay Server	The DHCP server to which the DHCP requests are forwarded.
Action	Provides option to edit/delete relay server parameters.
Rebroadcast DHCP Request to Interface	
Interface	The interface which receives the DHCP requests.
Rebroadcast Interface	The interface through which the DHCP relay requests are rebroadcasted.
Action	Provides option to edit/delete rebroadcast DHCP parameters.

CONFIGURE RELAY DHCP REQUEST TO SERVER

Relay DHCP Request to Server allows you enable the DHCP Relay Agent to forward the DHCP requests received on a particular interface to a DHCP Server.

Follow the procedure below to configure DHCP request to server.

1. Click **New** in the **Relay DHCP Request to Server** table.
2. Select the interface from the **Interface** column.
3. Enter the IP address of the Relay Server in the **Relay Server** column.
4. Click **Apply** to save the configuration or click **Cancel** to cancel the operation.

Edit Relay DHCP Request to Server

1. Click **Edit** icon in the **Action** column to edit the Relay Server IP.
2. Edit the Relay Server IP address.
3. Click **Apply** to save the changes or **Cancel** to retain original parameters.

Delete Relay DHCP Request to Server

1. Click **Delete** icon in the **Action** column to delete the Relay DHCP Server parameters.
2. Confirm at the prompt to delete.

CONFIGURE REBROADCAST DHCP REQUEST TO INTERFACE

Broadcast DHCP Request to Interface allows you to rebroadcast the forwarded DHCP Request packets to another interface.

Follow the procedure below to configure Rebroadcast DHCP Request to Interface.

1. Click **New** in the **Rebroadcast DHCP Request to Interface** table.
2. Select the interface from the **Interface** column.
3. Select the re-broadcast interface from the **Rebroadcast Interface** column.
4. Click **Apply** to save the configuration or click **Cancel** to cancel the operation.

Edit Rebroadcast Interface

1. Click **Edit** icon in the **Action** column to edit the rebroadcast interface.
2. Select the new re-broadcast interface.
3. Click **Apply** to save the changes made or **Cancel** to retain original parameters

Detach Rebroadcast DHCP Request to Interface

1. Click **Delete** icon in the **Action** column to delete the rebroadcast interfaces.
2. Confirm at the prompt to delete.

ROUTING

This **Routing** page allows you to configure the following in your system:

- Static Routes
- Policy Based Routing (PBR)

STATIC ROUTE

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 the 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.

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.

VIEWING STATIC ROUTING

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Routing** sub-menu.

Routing page has two tabs: **Routing** and **Policy Based Routing**. By default, **Static Route Details** table is displayed in the center panel.

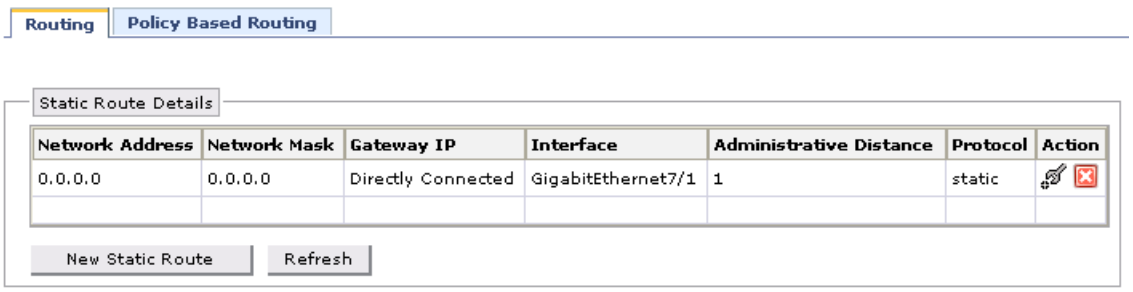


Figure 43: Routing - Static Route Details

The table below provides field description for Static Routing Details page.

Table 7: Static Route Details Field Description

Field	Description
STATIC ROUTE DETAILS	
Network Address	IP address and prefix length of the destination network.
Network Mask	Network mask of the destination network
Gateway IP	IP address of the gateway (next hop) through which the traffic is routed
Interface	IP address of the next hop interface through which the traffic is routed
Administrative Distance	The administrative distance of the routing protocol
Protocol	Protocol type (Static)
Action	Provides an option to edit/delete static routes.
New Static Routes	Add static routes.
Refresh	Update Static Routing table.

ADD NEW STATIC ROUTE

To add a Static route, follow the procedure given below:

Step 1: Click on **New Static Route** in the **Static Route Details** page.

Step 2: Add New Static Route page is displayed.

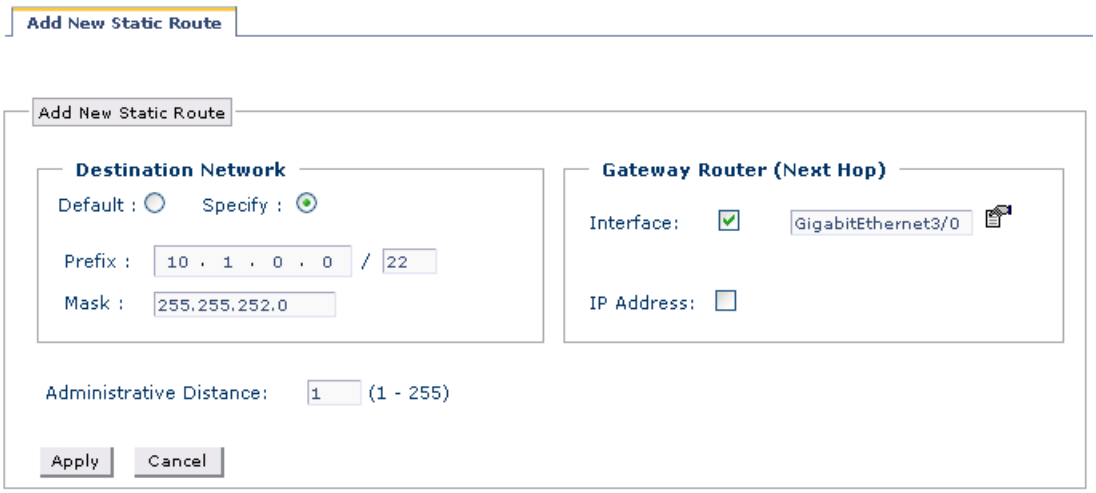


Figure 44: Routing - Add New Static Route

Step 3: Configure the destination network for the static route.

- Select the **Specify** radio button, and enter the IP address and prefix length of the destination network in the **Prefix** and **Mask** fields respectively.
- Select the **Default** radio button if you want the static route to be the default route. By default, 0.0.0.0/0 is configured as the default static route. This is not editable.

Step 4: Configure the Gateway Router (Next Hop) IP address or the interface through which the traffic is routed.

- Select the **Interface** check box and select the interface from the list.
- Select the **IP Address** check box and enter the IP address.

Note: 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.

Step 5: Enter the administrative distance of the routing protocol in the **Administrative Distance** field. By default, this is set to 1.

Step 6: Click **Apply** to add a new static route or click **Cancel** to cancel the operation.

EDIT STATIC ROUTE

1. In the **Static Route Details** page, under **Action** column, click **Edit** icon against the static route that needs to be edited. **Configure VLAN** page is displayed. Only the Administrative Distance can be edited.
2. Enter the new administrative distance in the **Administrative Distance** field.
3. Click **Apply** to save changes, or **Cancel** to retain the original key.

DELETE STATIC ROUTE

1. Under **Action** column, click **Delete** icon against the static route to be deleted in the **Static Route Details** page.
2. Confirm at the prompt to delete the static route and its details.

POLICY BASED ROUTING (PBR)

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.

VIEWING PBR

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Routing** sub-menu.

Routing page has two tabs: **Routing** and **Policy Based Routing**. Click **Policy Based Routing** tab. The following page is displayed:

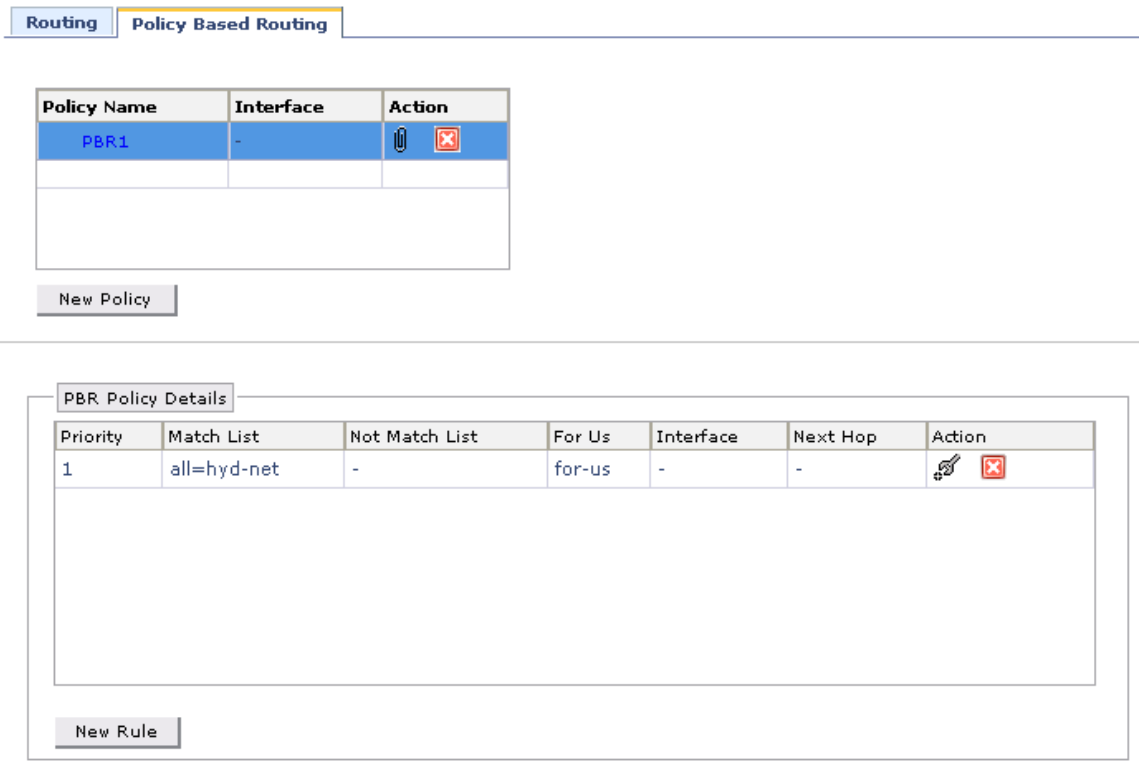


Figure 45: Routing - Policy Based Routing

The table below provides field description for PBR page.

Table 8: PBR Field Description

Field	Description
PBR	
Policy Name	Name of the IP Policy
Interface	Interface to which the IP policy is applied
Action	Provides an option to attach the IP policy to an interface and delete an IP policy.
PBR POLICY DETAILS	
Priority	Priority set for the IP policy
Match List	Match-list included in the IP policy
Not Match List	Match-list not included in the IP policy
For Us	Route: For Us/Next Hop
Interface	Name of the interface. Specifies the egress path of the packet.
Next Hop	The egress path of the packet.
Action	Provides option to edit and/or delete IP policy rule.

CONFIGURING AN IP POLICY AND A RULE FOR AN IP POLICY

Follow the procedure given below to create a new IP Policy and configure a rule for an IP policy:

Step 1: Click **New Policy** in the **Policy Based Routing** page to create a new IP policy.

Step 2: The following page is displayed:

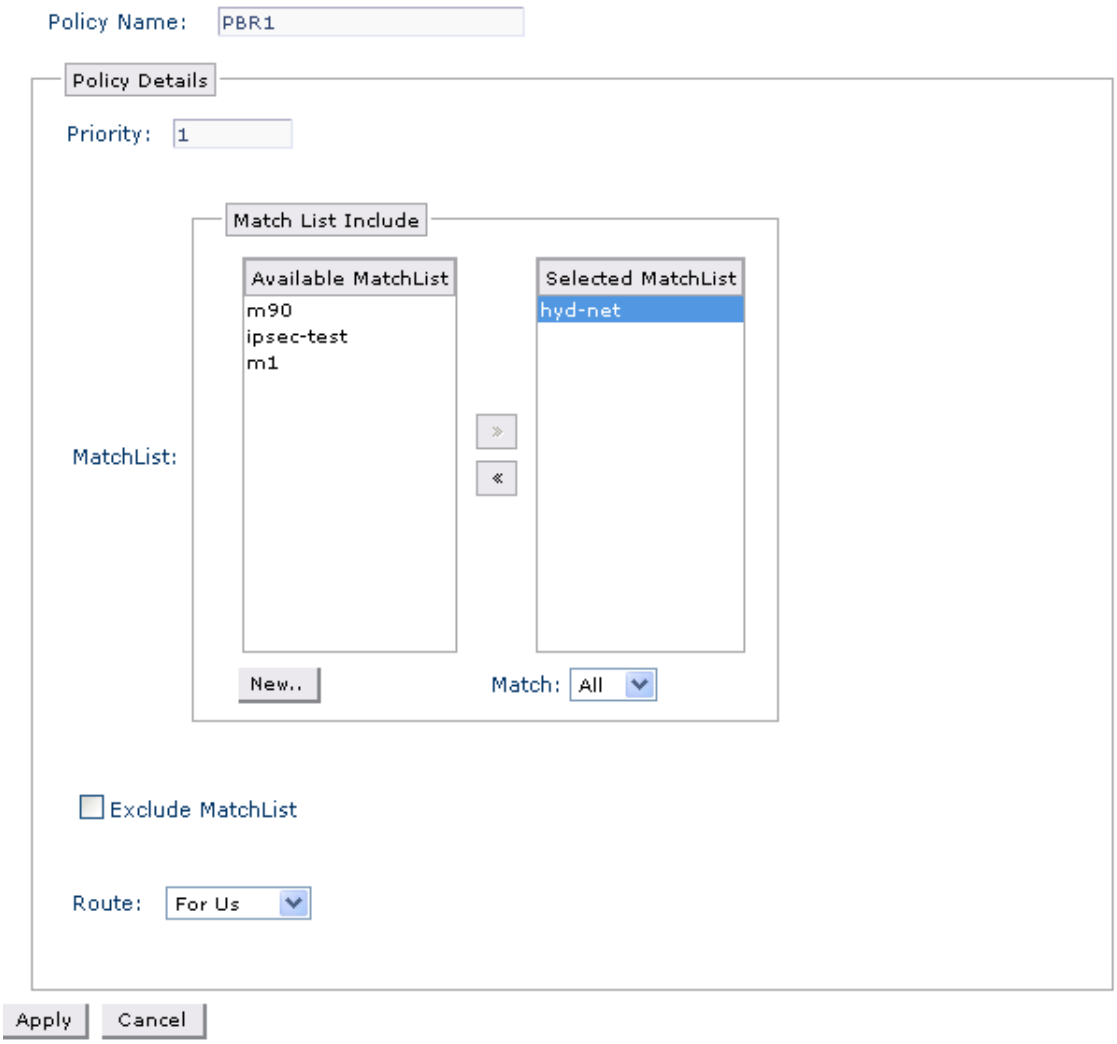


Figure 46: Policy Based Routing - Create New IP Policy

Step 3: Enter the name for IP Policy in the Policy Name field.

Step 4: Configure a rule for the IP policy. Specify the match conditions and forwarding action for the IP policy.

1. Enter the priority of the rule in the **Priority** field.
2. Rule can have multiple match-lists along with the option of any/all. **Match List Include** table displays a list of match-lists already configured in the system.
   - Select the match-list to be included from the **Available MatchList** column and click the '**>**' button to move it to the **Selected MatchList** column. Select as many match-lists from the Available MatchList column and move it to the Selected MatchList column.
   - Select the option Any/All from the **Match** drop-down list.
   - Click **New** to configure new match-lists or if there are no match-lists configured. **Create Traffic Classifier** pop-up window is displayed.

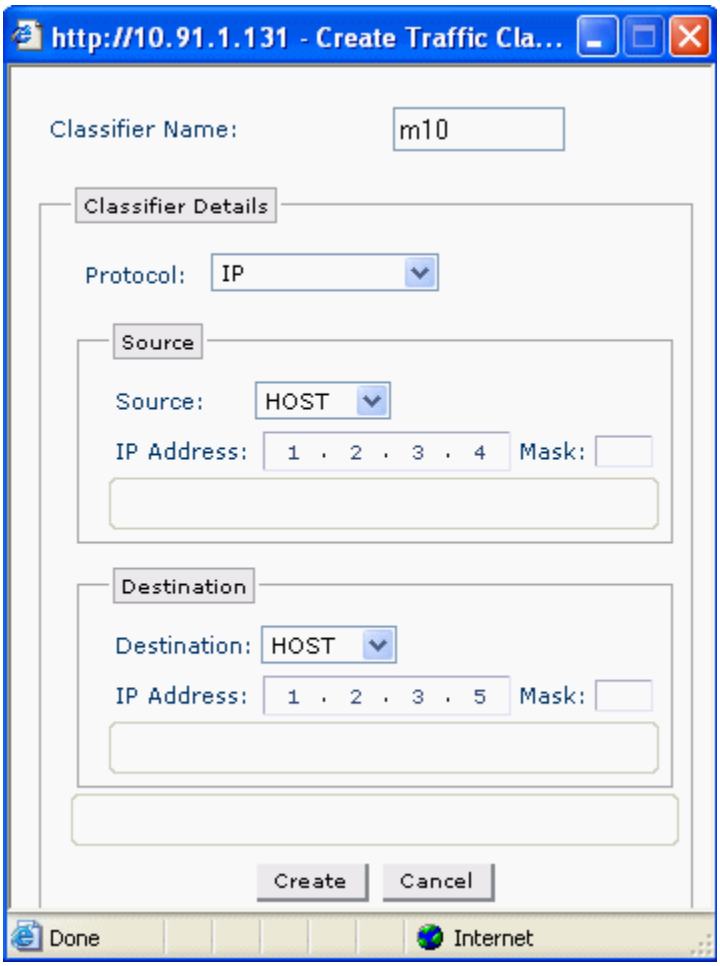


Figure 47: Policy Based Routing - Create New IP Policy - Create New Match-list

Configure the match-list parameters.

i. Enter the match-list name in the **Classifier** filed.

ii. Select any of the protocols from the **Protocol** drop down list.

iii. Select source from the **Source** drop-down list: **HOST/PREFIX.** Enter the source IP address for host, and enter the source address with prefix length for prefix.

iv. Select the destination from the **Destination** drop-down list: **HOST/ PREFIX.** Enter the source IP address for host, and enter the source address with prefix length for prefix.

v. Click **Create**. The match-list thus created is displayed in the **Available MatchList** column.

3. Select **Exclude MatchList** check box to exclude a specific match-list. Select the required match-list from the drop-down list.

   You can create a new match-list by clicking **New**. The newly created match-list will be displayed in the drop-down list. Select the same to exclude it.

4. Select the route option from the Route drop-down list: **For Us/Next Hop**

- Select For Us to redirect the packet to the management plane of the OA-700.
- Select Next Hop option. Interface and IP address options are displayed. Select the required option. Next hop specified the egress path of the packet.

Note: The interface-name and/or next-hop shall specify the egress path of the packet.

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.

When the interface option is chosen as Ethernet/VLAN, it is mandatory to specify the next hop.

Step 5: Click **Apply** to create a new IP policy or **Cancel** to cancel the operation. The IP policy thus configured is displayed in the PBR page. And, the PBR Policy Details table displays the rule elements configured to the IP policy.

ADD NEW RULE TO AN IP POLICY

Follow the procedure below to add more rules to an IP policy configured.

1. In the **Policy Based Routing** page, select the IP policy to which new rule is to be added.
2. Click **New Rule**. Page to add new rule is displayed.
3. Configure the required rule elements.

EDITING IP POLICY RULE

1. In the **Policy Based Routing** page, select the IP policy whose rule details are to be edited. The rules already configured for the selected IP policy is displayed in the **PBR Policy Details** table.
2. Click **Edit** icon in the **Action** column to edit the rule details.
3. Edit rule page is displayed. Make the required changes. Policy Name is not editable.
4. Click **Apply** to save changes, or **Cancel** to retain the original settings.

DELETING RULE FOR A MATCH-LIST

1. In the **Policy Based Routing** page, select the IP policy whose rule/s is to be deleted. The rules already configured for the selected IP policy is displayed in the **PBR Policy Details** table.
2. Click **Delete** icon in the **Action** column against the rule to be deleted.
3. Confirm at the prompt to delete the rule.

ATTACH AN IP POLICY TO AN INTERFACE

This command is used to attach an IP policy to an interface.

Note: An interface can have only one IP policy applied on it at any time.

'Transparent-forwarding' if in effect shall be cleaned up before PBR is configured.

Step 1: Attach an IP Policy to the interface in the **Policy Based Routing** table.

1. Select the IP policy to be attached on an interface from the Policy Name list.
2. Click **Attach Interface** icon. **Attach Interface** page is displayed:

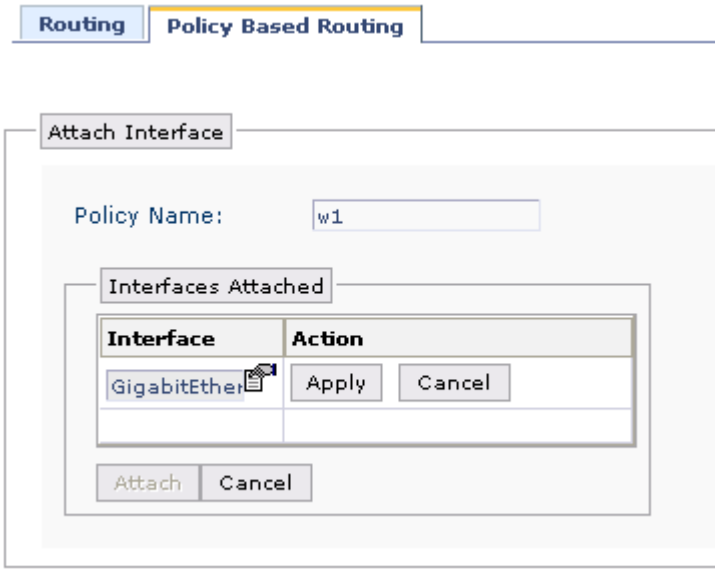


Figure 48: Policy Based Routing - Attach Interface

Step 2: The Policy Name field displays the name of the IP policy. This is not editable.

Step 3: Click **Attach**.

Step 4: Field to attach interface is populated. Select the interface from the **Interface** list

Step 5: Click **Apply** to attach the selected interface to the IP policy or click **Cancel** to cancel the operation.

DETACH IP POLICY FROM AN INTERFACE

1. Select the IP Policy from the Policy list. Click **Attach Interface** icon.

   Interface/s already bound to the selected filter is displayed in **Attach Interface** page.
2. Click **Detach** icon in the **Action** column to detach the IP policy from the selected interface.
3. Confirm at the prompt to detach the IP Policy.

DELETING IP POLICY

1. Click **Delete** icon in the **Action** column against the IP Policy to be deleted.
2. Confirm at the prompt to delete the IP Policy.

SYSTEM ACCESS

This page allows you to configure the following in your system:

- SNMP
- Syslog
- File Transfer and Access

SNMP

SNMP (Simple Network Management Protocol) is a request-and-response protocol that is used in sharing networking information between two or more network entities. SNMP plays a vital role and serves as the nervous system of entire network management system. The network management is about keeping the network up and running, monitoring, and controlling 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 a human intervention where the managed object is situated. This becomes cumbersome when the network devices are more and widespread. Managing such a system becomes tedious and quite impossible. SNMP comes here handy 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.

In SNMP, two types of communicating devices exist: Agents and Managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

This page allows you to configure SNMP parameters.

VIEWING SNMP

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **System Access** sub-menu.

System Access page has three tabs: **SNMP, Syslog,** and **File Transfer & Access**. By default, **SNMP** tab is active, and its details are displayed in the center panel.

Figure 49: System Access: SNMP

The table below provides description for SNMP parameters.

Table 9: SNMP Field Description

Field	Description
SNMP	
SNMP Service	Check this check box to enable/disable SNMP service
Community Settings	
Traps Enable	Enable SNMP trap
Version	SNMP version
Read Community	Read community string
Read-Write Community	Read-Write community string
Trap Host Configuration	
IP Address	IP address of the SNMP trap host
Port	Port number of the SNMP trap host
SNMP Version	SNMP version configured of the trap host
Community String	Community string set on the SNMP trap host
Action	Provides option to edit and/or delete trap host details

CONFIGURING SNMP PARAMETERS

Follow the procedure below to configure SNMP parameters:

Step 1: Enable SNMP Service.

To enable the SNMP service, check **SNMP Service** check box.

Step 2: Configure Community Settings.

1. Select the **Traps Enable** check box to enable SNMP trapping.
2. Select the SNMP version from the **Version** drop down list.
3. Enter the **Read Only/Read-Write Community** string for the SNMP agent.
4. Click **Apply** to configure Community Settings.

Step 3: Configure SNMP trap host. This is to configure the trap destination where the agent will send the snmp traps.

If you have checked the **Traps Enable** check box, configure SNMP trap hosts. To configure new SNMP trap hosts, click **New Trap Host** in the Trap Host Configuration box. This populates fields to add SNMP trap host details.

1. The host IP address to which the trap messages are to be sent in the in the **IP Address** field.
2. Enter the notification host's UDP port number in the **Port** field.
3. Select the SNMP version from the **SNMP Version** drop-down list.
4. Set the SNMP community string in the **Community String** field.

Note: You can configure a maximum of 3 SNMP trap receivers.

5. Click **Apply** to add SNMP trap host.

EDITING A SNMP TRAP HOST

1. Click **Edit** icon in the **Action** column against the trap host that is to be edited.
2. Enter the new host details in the respective columns.

   IP Address, Port, SNMP Version, and Community String details.
3. Click **Apply** to save changes, or **Cancel** to retain the original settings.

DELETING A SNMP TRAP HOST

1. Click **Delete** icon in the **Action** column against the trap host to be deleted.
2. Confirm at the prompt to delete the SNMP trap host.

SYSLOG

This page allows you to configure system logging parameters. The OA-700 system can be configured for logging based on severity and module. The logging information can further be directed to the logging buffer, to the console or terminal or to a remote syslog server. Logging to the console and the logging buffer is “ON” by default.

VIEWING SYSLOG

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **System Access** sub-menu.

System Access page has three tabs: **SNMP, Syslog,** and **File Transfer & Access**. Click **Syslog** tab. The following page is displayed.

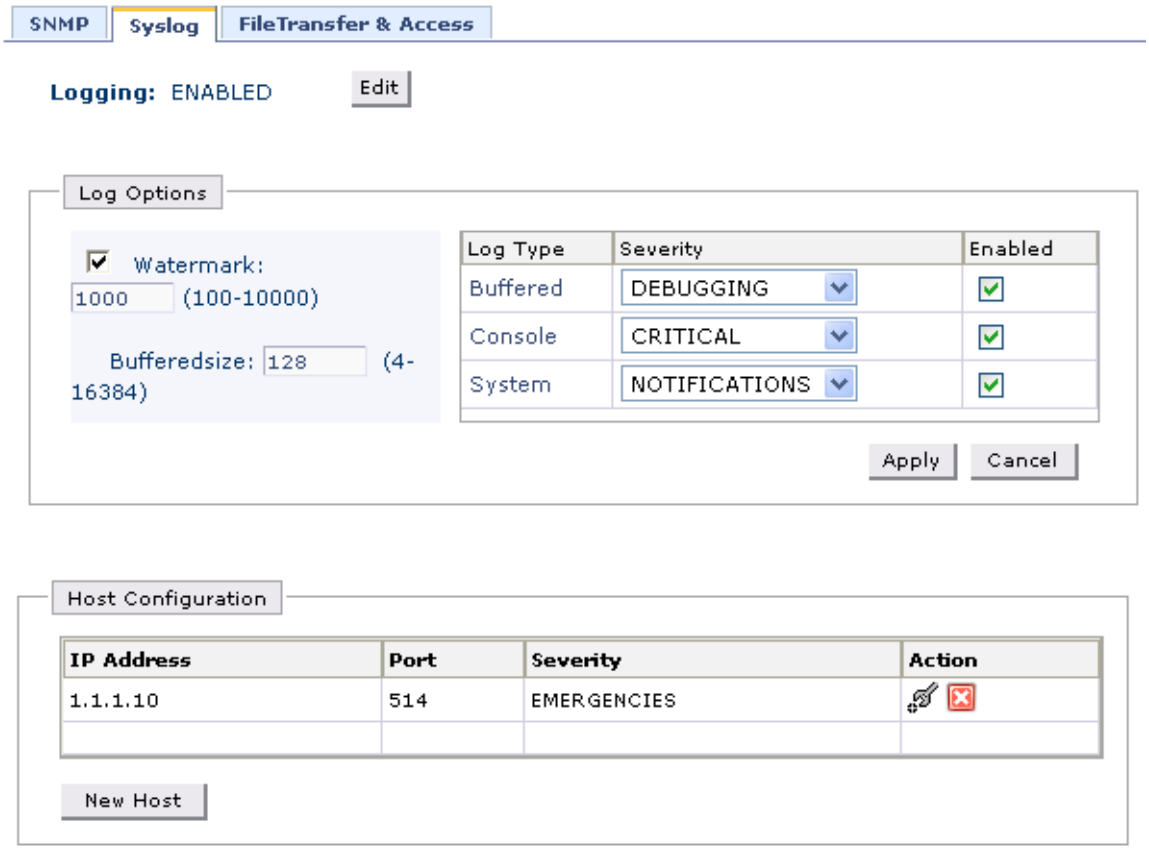


Figure 50: System Access - Syslog

The table below provides description for Syslog page.

Table 10: Syslog Field Description

Field	Description
SYSLOG	
Logging: ENABLED	Logging of messages is enabled
Edit	Enable or disable syslog
Log Options	
Watermark	Maximum number of log messages that can be stored in the buffer Watermark in the range of 100-10000.
Buffered size	Buffer size in the range of 4-16384. The size of the buffer where logs are stored.
Log Type	
Buffered	If Buffered is enabled, it will store the logs in the memory buffer. This will apply for logs having severity equal or smaller than the selected severity when enabled.
Console	If Console is enabled, it will show logs on the console. This will apply for logs having severity equal or smaller than the selected severity when enabled.
System	If System is enabled, it will log the system logs. This will apply for logs having severity equal or smaller than the selected severity when enabled.
Severity	Levels of severity that can be set: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, and Debugging.
Enabled	Select the check box to either enable/ disable log types.
Host Configuration	
IP Address	IP address of the host to which logs should be sent.
Port	Port number of the host.

Field	Description
Severity	The logs of the severity equal or smaller is the sent to the host.
Action	Provides option to delete the host details.

Configuring Syslog Parameters

Follow the procedure below to configure Syslog:

Step 1: Enable **Logging** in the **Syslog** page.

By default, logging is enabled. If not, click **Edit**, check the **Logging** check box, click **Apply**.

Step 2: Set log options in the **Log Options** table.

1. Click **Edit** to set the log options.
2. Set the watermark in the **Watermark** field in the range 100-10000.
3. Enter buffered size in the **Buffered Size** field in the range between 4-16384.

The Log Options table lists log type, severity level, and enable status. There are three log types: Buffered, Console, and System.

1. Select the log type for which you want to enable logging by checking the **Enabled** check box.
2. Set any of the following severity levels for each of the log type: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, and Debugging.
3. Click **Apply** to save the changes made to Log Options table.

Add Host

Configure host details in the Host Configuration table.

1. Click **New Host** to configure new host.
2. Enter IP address in the **IP Address** field, port number in the **Port** field, and select severity from **Severity** drop down list.
3. Click **Apply** to add new host.

Delete Host

1. To delete any host, click **Delete** icon.
2. Confirm at the prompt to delete the host.

File Transfer and Access

This page displays the protocols supported to access the device and for file transfer.

It allows you to enable/disable the access protocols such as HTTP, HTTPS, SSH, Telnet, and SNMP to access the OA-700.(ssh/telnet to access CLI, HTTP/HTTPS for Web based management and SNMP service.)

Viewing File Transfer & Access

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **System Access** sub-menu.

System Access page has three tabs: **SNMP, Syslog,** and **File Transfer & Access**. Click **File Transfer & Access** tab.

File Transfer and Access page is displayed. **File Transfer Protocol Status** table displays the protocols that are supported for file transfer. The **Access Status** table provides an option to enable/disable the access protocols.

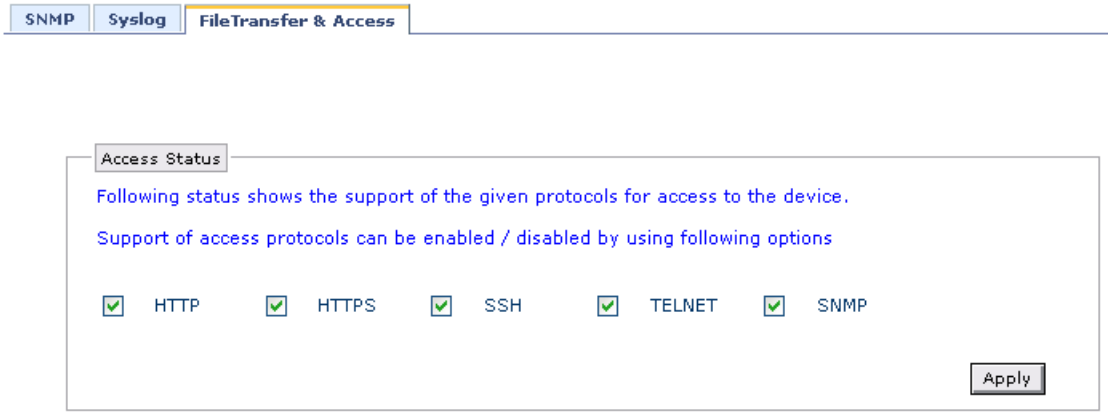


Figure 51: Management Utilities: File Transfer & Access

Enable/Disable the Support of Access Protocols

Follow the procedure below to enable/disable the access protocols.

Step 1: Select the **HTTP/HTTPS/SSH/Telnet/SNMP** check box, and click **Apply** to enable the protocols for file transfer and access. Multiple options can be selected.

Step 2: Uncheck the required check box to disable the support of a specific access protocol.

TIME RANGE

This page allows you to configure the time range object that can be used across the application.

VIEWING TIME RANGE

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Time Range** sub-menu. Time Range table is displayed in the center panel.

Note: If there is no time range configured, “There is no Time Range To Display“ message is displayed in the Time Range table.

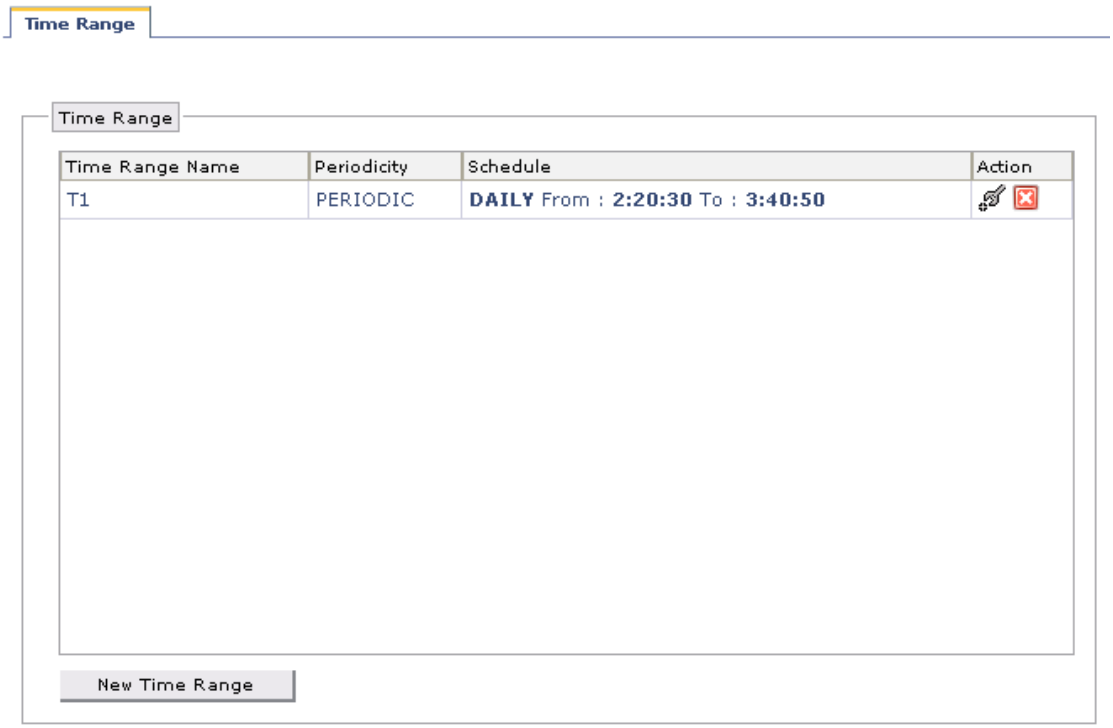


Figure 52: Time Range

The table below provides field description for Time Range page.

Table 11: Time Range Field Description

Field	Description
TIME RANGE	
Time Range Name	Lists the time range configured.
Periodicity	Time range period: Absolute or Periodic.
Schedule	Start and end time for the time range.
Action	Provides option to edit/delete the time range.
New Time Range	Create a new time range.

CONFIGURING TIME RANGE

Follow the procedure below to configure the time range:

Step 1: Click **New Time Range** to configure a new time range. This displays the **Time Range** configuration page in the center panel.

Step 2: Enter the name for time range in **Time Range** field.

Step 3: Select the type of time range: **Absolute** or **Periodic** radio button. By default, **Absolute** is selected.

ABSOLUTE TIME RANGE

To configure time range on a one time basis, set the absolute time range.

1. Select the **Absolute** radio button in the time range configuration page. **Absolute** time range table is displayed.

Figure 53: Time Range: Create New Absolute Time Range

2. Set the start date and time.
   i. Set the start date.

      Click "**+**" button in the **Date** field and select the start date.
   ii. Enter the start time in hh:mm:ss format in the **Time** field.
3. Set the end date and time.

   Check the **End Date/Time** check box if you want to specify end date and time for the time range you are configuring.
   i. Set the end date.

      Click "**+**" button in the date field and select the end date.
   ii. Enter the end time in *hh:mm:ss* format in the **Time** field.
4. Click **Apply** to configure Absolute Time Range.

Note: If the End Date/Time is not specified, the time range is applied continuously from the specified start time.

PERIODIC TIME RANGE

To configure time range on a periodic basis, set the periodic time range.

1. Select the **Periodic** radio button in the time range configuration page. **Periodic** time range table is displayed.

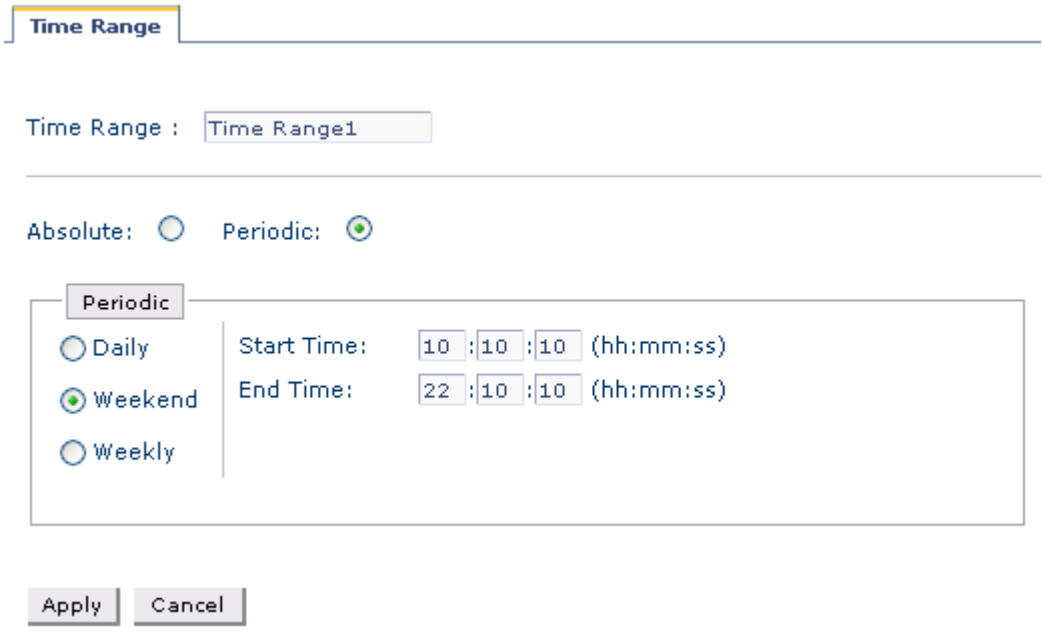


Figure 54: Time Range: Create New Periodic Time Range

2. Set the periodicity.

   Select the periodicity: Daily, Weekend, or Weekly radio button.

   - **Daily** – Select this radio button to apply the time range every day at the specified time.
   - **Weekend** – Select this radio button to apply the time range every weekend at the specified time.
   - **Weekly** – Select this radio button to apply the time range on the specified day every week.

3. Set the start and end time.

   Enter the start and end time in hh:mm:ss format.

   For Weekly periodicity, also select the day of week from the **Day of Week** drop down list.

4. Click **Apply** to configure the Periodic Time Range.

EDIT TIME RANGE

1. Click on the **Edit** icon in the **Action** column for the time range to be edited.
2. Make changes to the time range settings. Click **Apply** to save changes.

DELETE TIME RANGE

1. Click on the **Delete** icon in the **Action** column for the time range to be edited.
2. Confirm at the prompt to delete time range.

TRAFFIC CLASSIFICATION

The Traffic Classification feature is commonly used within the network devices in order to selectively categorize packet traffic and deal with it differently. Classifications 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 Traffic Classification feature contains List and Match List sub-features.

LIST

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.

The List page allows you to create lists.

VIEWING LIST

Follow the procedure given below to view List page.

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Traffic Classification** sub-menu.

Traffic Classification has two tabs: **List** and **Match List**. By default, **List** page is displayed in the center panel.

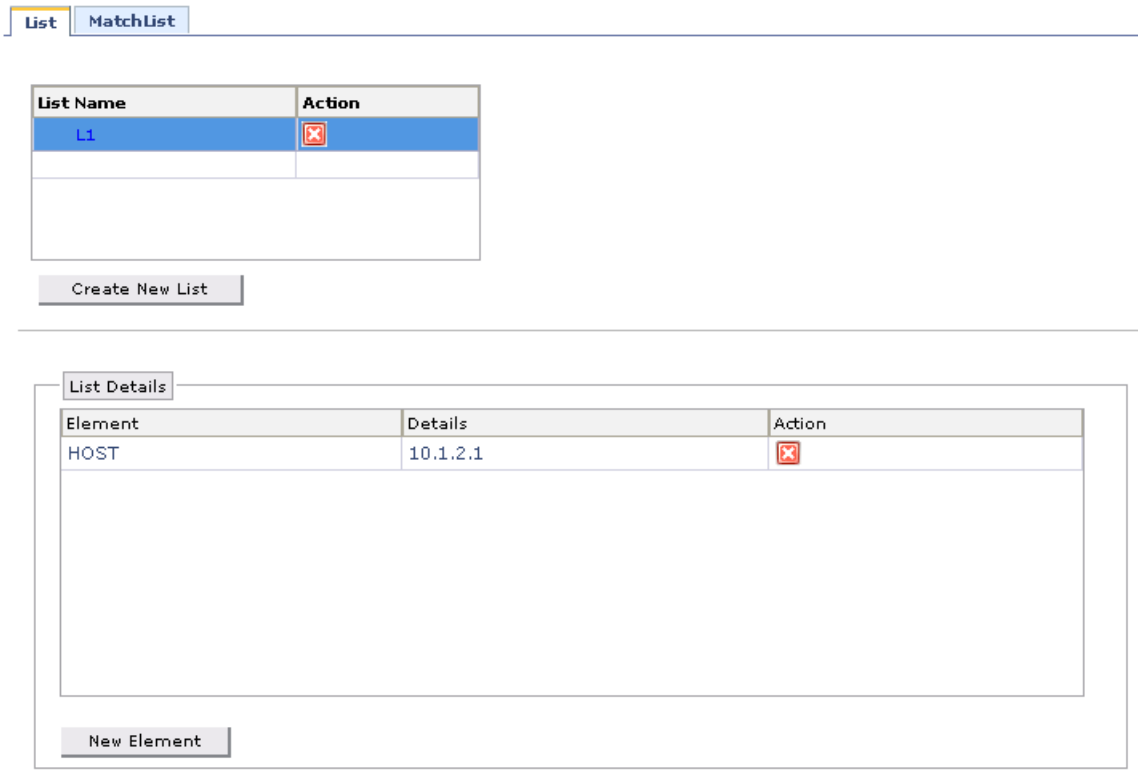


Figure 55: Traffic Classification: List

The table below provides field description for List page.

Table 12: List Field Description

Field	Description
LIST	
List Name	Lists configured on your system.
Action	Provides option to delete the lists.
Create New List	Add a new list.
LIST DETAILS	
Element	Elements configured for the list. Element type: Host, Prefix, Interface, or List. Host - Host IP address; Prefix - IP address/prefix length Interface – Interface name List– Other lists configured on the system.
Action	Provides option to delete the elements.
New Element	Create new element.

CREATING A LIST

Follow the procedure given below to create lists:

Step 1: From the **List** page, click **Create New List** to create a new list.

Create New List page is displayed.

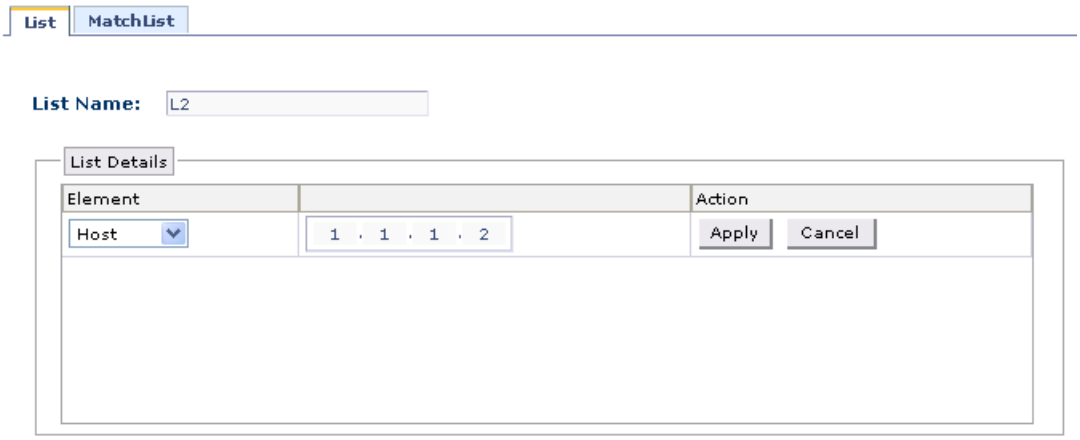


Figure 56: Traffic Classification: Create New List

Step 2: Enter name of the list being configured in the **List Name** field.

Step 3: Add the elements for the list in **List Details** table.

1. Select the type of element from the drop down list in the **Element** column and enter its respective details: **Host/Prefix/Interface/List**
   - For the **Host** element type, enter the IP address.
   - For the **Prefix** element type, enter IP address and prefix length.
   - For the **Interface** element type, select the interface from the interfaces list.
   - For the **List** element type, select the list from the lists configured, if any. This allows you to include a list within a list.
2. Click **Apply** to create a new list or **Cancel** to cancel the operation. The list thus configured is displayed in the List page. And, the List Details table displays the elements configured to the list.

ADD ELEMENTS TO A LIST

Follow the procedure below to add element/elements to a list configured:

1. In the **List** page, select the list to which new element is to be added.
2. Click **New Element**. The fields to add element is populated in the List Details table as shown below:

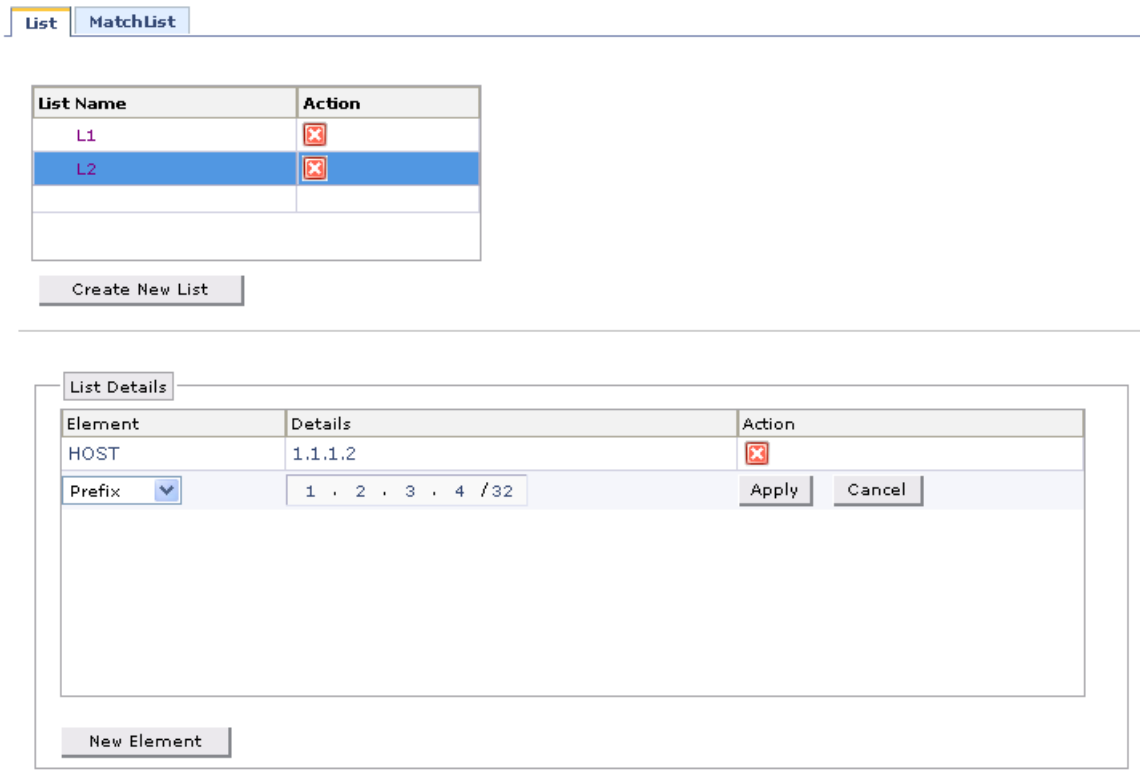


Figure 57: Traffic Classification: List - Create New Element

3. Select the type of element from the drop down list in the **Element** column and enter its respective details: **Host/Prefix/Interface/List**.
4. Click **Apply** to add the element to the list or **Cancel** to cancel the task.

DELETE A LIST

Follow the procedure below to delete a list:

1. Click **Delete** icon in the **Action** column against the list to be deleted.
2. Confirm at the prompt to delete the list.

DELETE ELEMENTS FROM A LIST

Follow the procedure below to delete elements from a list.

1. In the **List** page, select the list whose elements are to be deleted. Elements already configured for the selected list is displayed in the **List Details** table.
1. Click **Delete** icon in the **Action** column against the element to be deleted.
2. Confirm at the prompt to delete the element from the selected list.

MATCH LIST

The Match List page allows you to create and manage match-lists.

VIEWING MATCH LIST

Follow the procedure given below to view Match List page.

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Traffic Classification** sub-menu.

Traffic Classification has two tabs: **List** and **Match List**. Click the **MatchList** tab. The following page is displayed in the center panel.

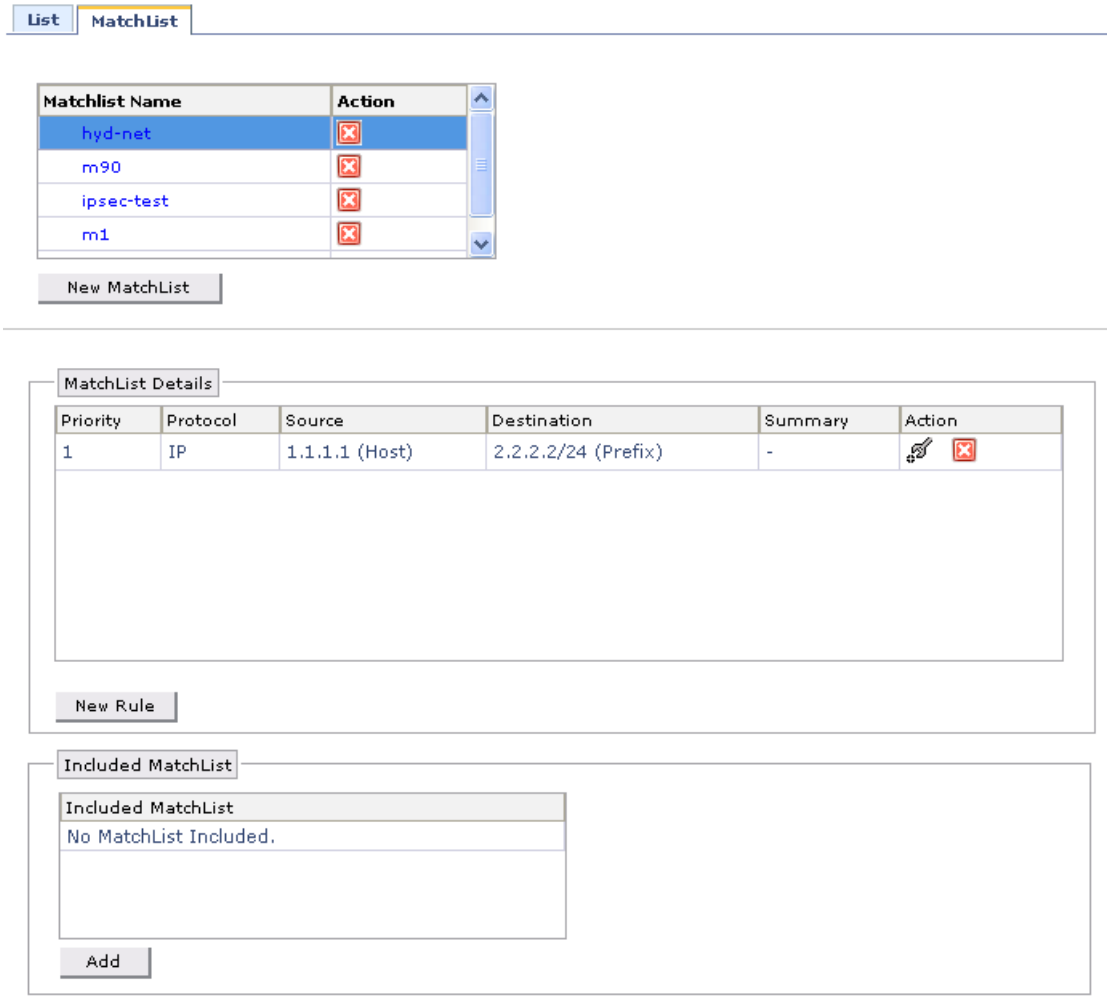


Figure 58: Traffic Classification - Match List

The table below provides field description for Match List page.

Table 13: Match List Field Description

Field	Description
MATCH LIST	
MatchList Name	Match-lists configured on your system.
Action	Provides option to delete the selected match-list.
New MatchList	Add new match-lists.
MatchList Details	
Protocol	Type of the protocol: IP, TCP, UDP, ICMP, AH, ESP, and other protocols
Source	Source type - Any, Host, Prefix, Interface, List.
Destination	Destination type - Any, Host, Prefix, Interface, List.
Summary	Summary of the list rules.
Action	Provides option to edit and/or delete MatchList rules.
New Rule	Create new match-list rule
Include MatchList	
Add	Include available match-lists to a match-list.

CREATING A MATCH-LIST

Follow the procedure given below to create match-lists:

Step 1: Click **New MatchList** in the **Match List** page to create new match-list.

Step 2: New Match List page is displayed.

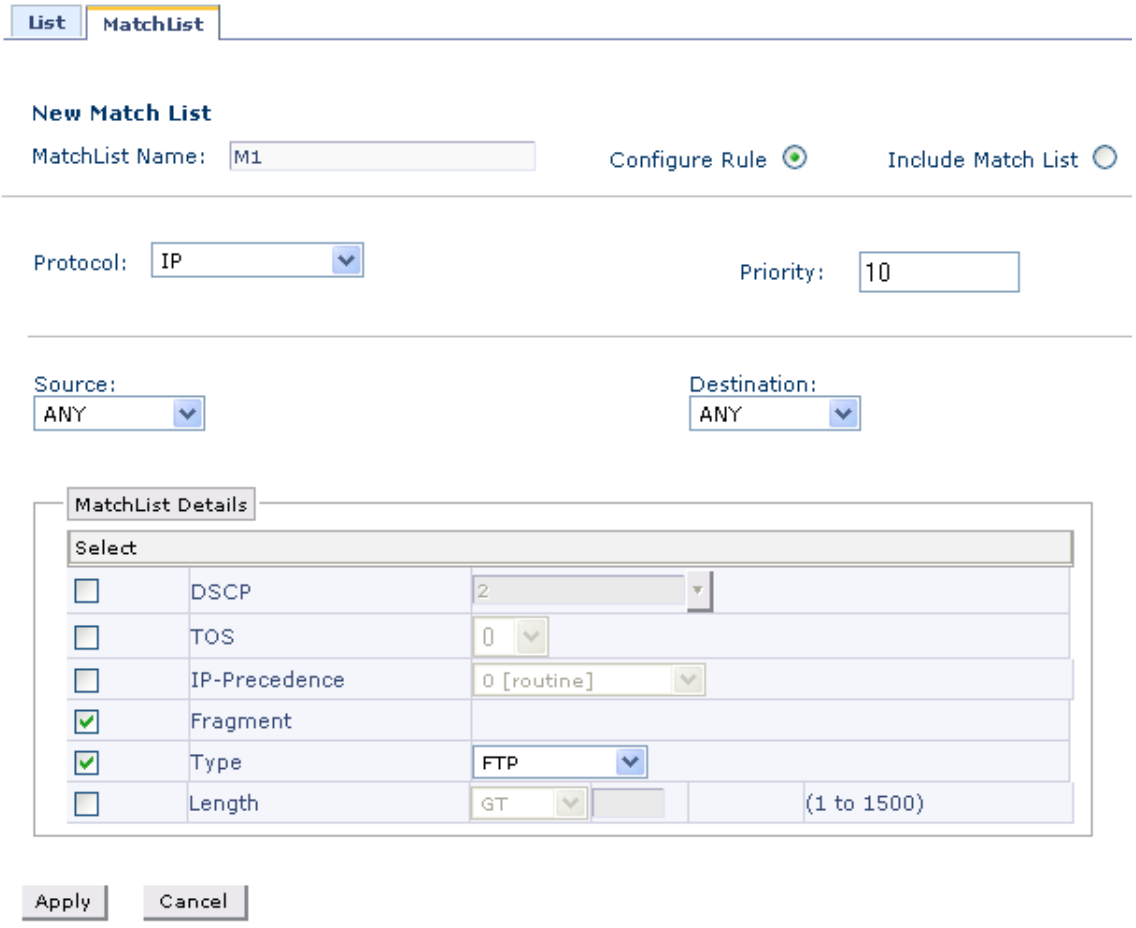


Figure 59: Traffic Classification: - New Match List - Configure Rule / Include Match List

Step 3: Enter the name for match-list in **MatchList Name** field.

Select **Configure Rule** radio button to define the rule for the match-list you are creating, or select the **Include Match List** radio button to include rules from the match-lists already configured in your system.

CONFIGURE RULE

Step 1: Select the **Configure Rule** radio button to define the rules to a match-list.

Select any of the protocols from the **Protocol** drop down list: **IP/TCP/UDP/ICMP/ Protocol/AH/ESP/GRE/OSPF/IGMP.** Rule elements vary for each of the protocols.

Step 2: Enter the rule number to specify the rule priority in the **Priority** field. This is in the range 1-65535.

Step 3: Select source from the **Source** drop-down list: **ANY/HOST/PREFIX/ INTERFACE/LIST**.

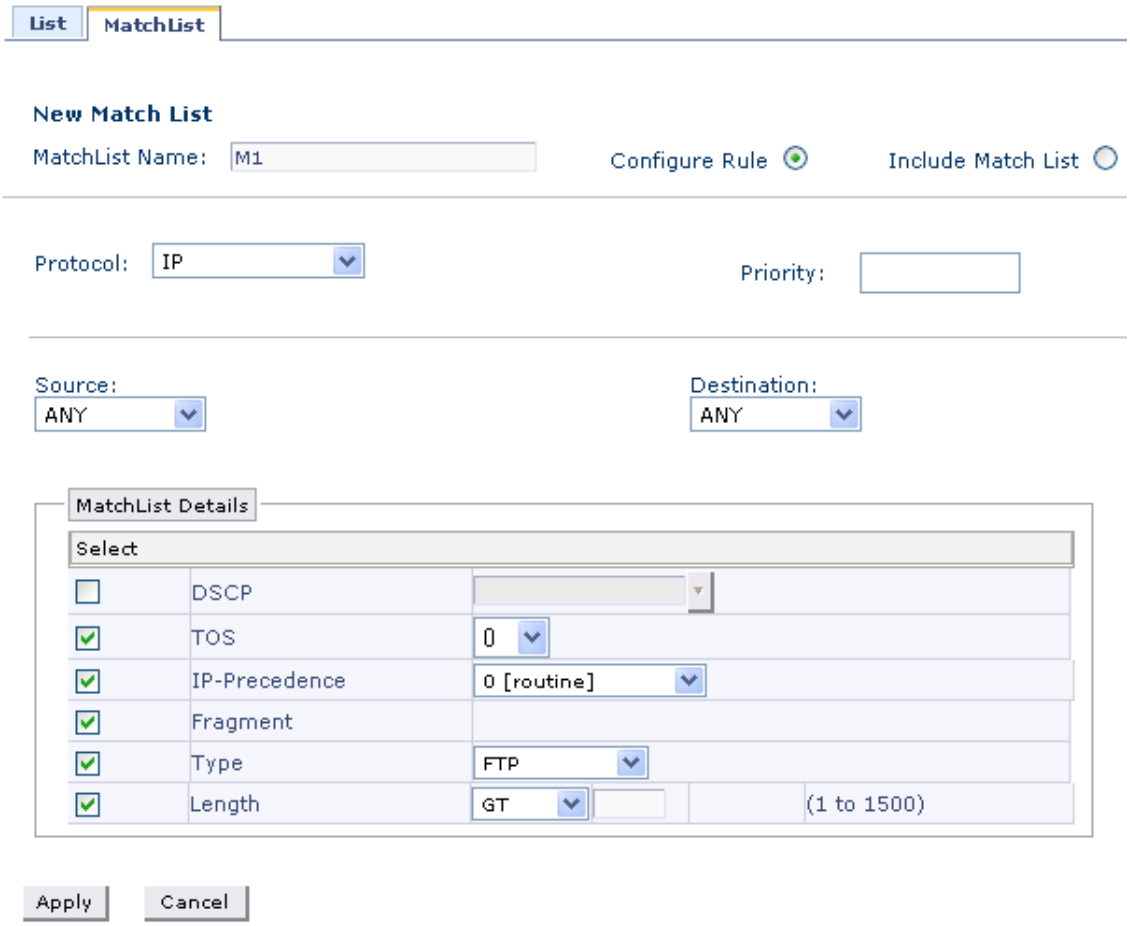
- Enter the source IP address for **Host**.
- Enter the source address with prefix length for **Prefix**.
- Select the interface from the interfaces list for **Interface**.
- Select the list from the lists configured for **List**.

Step 4: Select the destination from the **Destination** drop-down list: **ANY/HOST/ PREFIX/INTERFACE/LIST.**

- Enter the destination IP address for **Host**.
- Enter the destination address with prefix length for **Prefix**.
- Select the interface from the interfaces list for **Interface**.
- Select the list from the lists configured for **List**.

Step 5: Select rule elements for the protocols.

RULE ELEMENTS FOR IP / PROTOCOL / AH / ESP / GRE/ OSPF/ IGMP



Traffic Classification: New Match List Rule - IP / Protocol / AH / ESP/ GRE/ OSPF/ IGMP

1. Add the DSCP.

   Check the **DSCP** check box to add the DSCP. Provide the DSCP value in the range between 0 and 63 or select the value from the drop-down list.

2. Add ToS (Type of Service)

   Check the **TOS** check box; select the ToS value from the drop-down list.

3. Set the IP precedence level.

   Check the **IP-Precedence** check box to set IP precedence level in the range between 0 and 7.

4. Add fragments.

   Check the **Fragment** check box to match the IP Fragment bit.

5. Select the type of traffic.

   Check the **Type** check box to apply rule to the type of traffic. Select the type of traffic from the list: **FTP/NORMAL/RPC/TFTP/SIP**

6. Define rule based of packed length.

   Check the **Length** check box to apply rule based on the packet length. Specify the length or length range between 1 and 1500. You have the option to apply the rule for sizes greater than (GT), greater than or equal to (GE), less than (LT), less than or equal to (LE), between the range (RANGE), or for the fixed length (FIXED).

RULE ELEMENTS FOR TCP

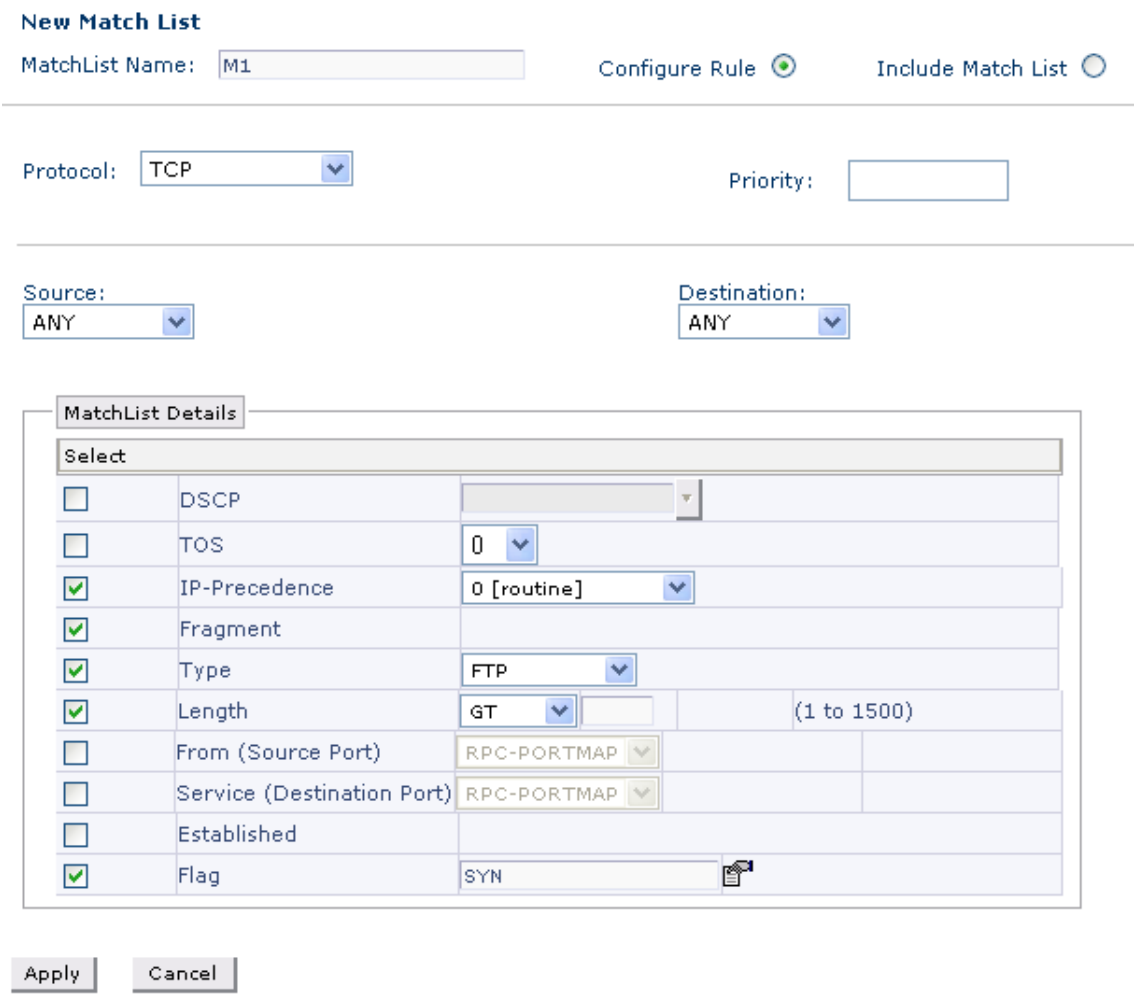


Figure 60: Traffic Classification: New Match List Rule - TCP

1. Add the DSCP.

   Check the **DSCP** check box to add the DSCP. Provide the DSCP value in the range between 0 and 63 or select the value from the drop-down list.
2. Add ToS

   Check the TOS check box; select the ToS value from the drop-down list.
3. Set the IP precedence level.

   Check the **IP-Precedence** check box to set IP precedence level in the range between 1 and 7.
4. Add Fragments.

   Check the **Fragment** check box to match the IP Fragment bit.

5. Select the type of traffic.

   Check the **Type** check box to apply rule to the type of traffic. Select the type of traffic from the list: **FTP/NORMAL/RPC/TFTP/SIP**.

6. Define rule based of packed length.

   Check the **Length** check box to apply rule based on the packet length. Specify the length or length range between 1 and 1500. You have the option to apply the rule for sizes greater than (GT), greater than or equal to (GE), less than (LT), less than or equal to (LE), between the range (RANGE), or for the fixed length (FIXED).

7. Apply rule based on source.

   Check the **From (Source Port)** check box to apply rule based on source. Select from the following options: RPC-PORTMAP, SMTP, SNMP, SNMPTRAP, SSH, TELNET, TFTP, BGP, DNS, FTP, FTP-DATA, HTTP, HTTPS, IMAP, POP2, POP3, GT, GE, LT, LE, RANGE, FIXED, NFS.

8. Apply rule based on destination.

   Check the **Service (Destination Port)** check box apply rule based on destination. Select from the following options: RPC-PORTMAP, SMTP, SNMP, SNMPTRAP, SSH, TELNET, TFTP, BGP, DNS, FTP, FTP-DATA, HTTP, HTTPS, IMAP, POP2, POP3, GT, GE, LT, LE, RANGE, FIXED, NFS.

9. Apply rule based on the session state.

   Check the **Established** check box.

10. Apply rule based on the flagged traffic.

    Check the **Flag** check box to apply the rule based on the TCP Segment Flag.

    - Click **Select** next to the field. **Flag** window is displayed with the list of flags available for selection.
    - Select the flags to be included from the **Available Flags** column and click '**>>**' button to move it to the **Selected Flags** column.
    - Select as many flags from the Available Flags column and move it to the Selected Flags column and click **OK**. The selected flag/s is displayed in the Flag field.

RULE ELEMENTS FOR UDP

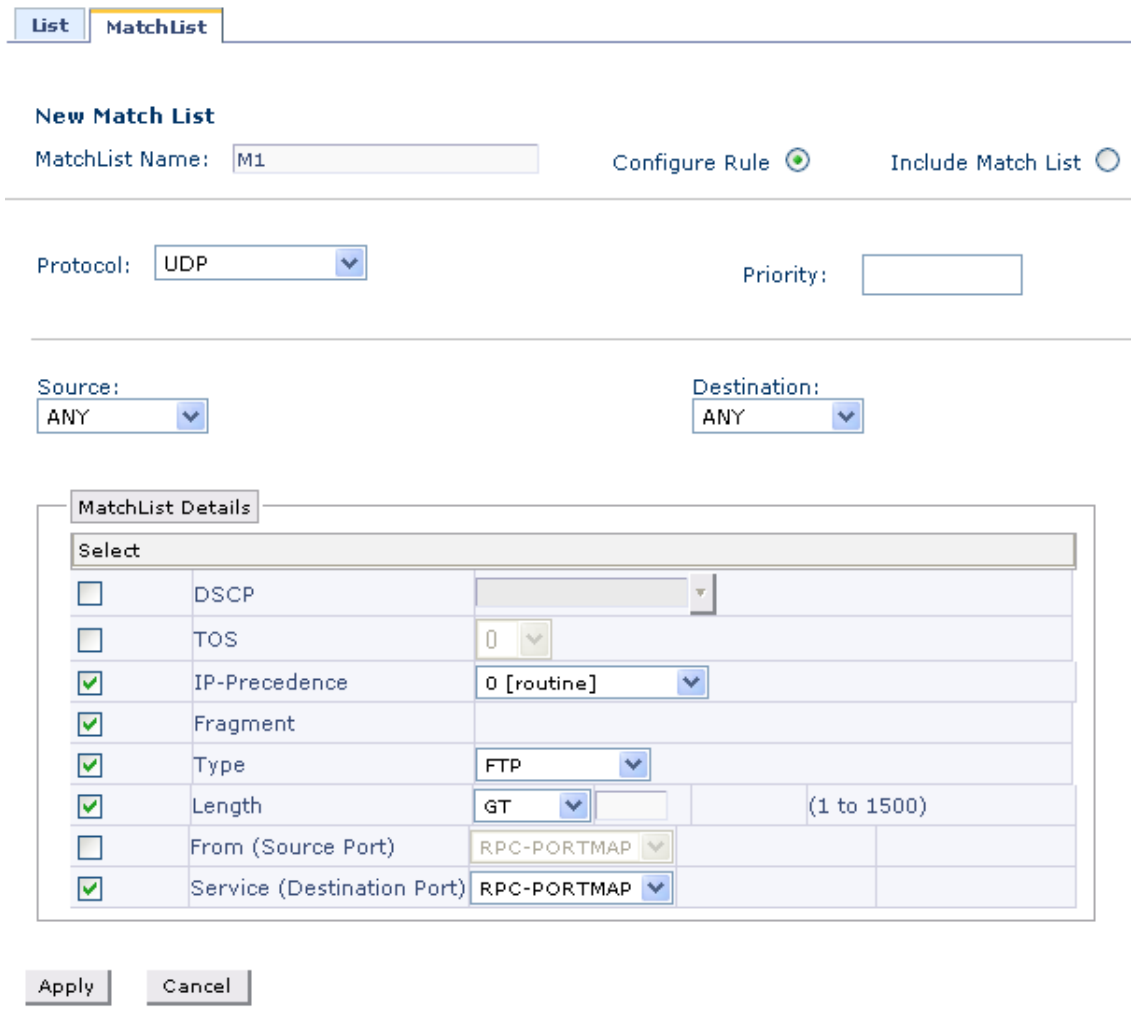


Figure 61: Traffic Classification: New Match List Rule - UDP

1. Add the DSCP.

   Check the **DSCP** check box to add the DSCP. Provide the DSCP value in the range between 0 and 63 or select the value from the drop-down list.
2. Add ToS

   Check the TOS check box; select the ToS value from the drop-down list.
3. Set the IP precedence level.

   Check the **IP-Precedence** check box to set IP precedence level in the range between 0 and 7.
4. Add fragments.

   Check the **Fragment** check box to match the IP Fragment bit.

5. Specify the type of service.

   Check the **Type** *of Service* check box to specify the Type of Service. Select Type of Service from the list.

6. Select the type of traffic.

   Check the **Type** check box to apply rule to the type of traffic. Select the type of traffic from the list: FTP, NORMAL, RPC, TFTP or SIP.

7. Define rule based of packed length.

   Check the **Length** check box to apply rule based on the packet length. Specify the length or length range between 0 and 1500. You have the option to apply the rule for sizes greater than (GT), greater than or equal to (GE), less than (LT), less than or equal to (LE), between the range (RANGE), or for the fixed length (FIXED).

8. Apply rule based on source.

   Check the **From (Source Port)** check box to apply rule based on source. Select from the following options: RPC-PORTMAP, SNMP, SNMPTRAP, TFTP, DNS, GT, GE, LT, LE, RANGE, NFS, SIP.

9. Apply rule based on destination.

   Check the **Service (Destination Port)** check box apply rule based on destination. Select from the following options: RPC-PORTMAP, SNMP, SNMPTRAP, TFTP, DNS, GT, GE, LT, LE, RANGE, NFS, SIP.

RULE ELEMENTS FOR ICMP

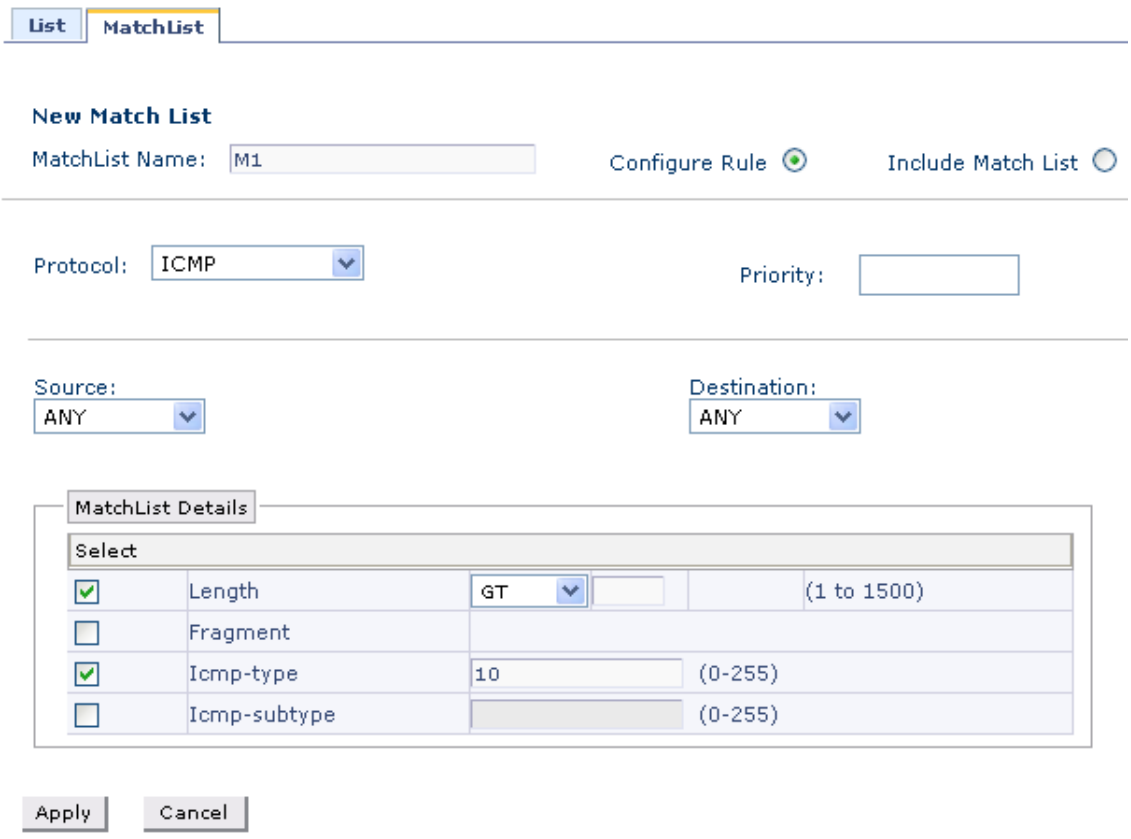


Figure 62: Traffic Classification: New Match List Rule - ICMP

1. Define rule based of packed length.

   Check the **Length** check box to apply rule based on the packet length. Specify the length or length range between 0 and 1500. You have the option to apply the rule for sizes greater than (GT), greater than or equal to (GE), less than (LT), less than or equal to (LE), between the range (RANGE), or for the fixed length (FIXED).

2. Add fragments.

   Check the **Fragment** check box to match the IP Fragment bit.

3. Apply rule based on ICMP type.

   Check the **ICMP-type** check box to apply rule based on ICMP type (0-255). Specify the ICMP type.

4. Apply rule based on ICMP sub-type.

   Check the **ICMP-subtype** check box to apply rule based on ICMP subtype (0-255). Specify the ICMP subtype.

Step 6: Click **Apply** to create match-list and to return to Match List page, or **Cancel** to return to the Match List page.

INCLUDE MATCH-LIST

Step 1: Select the **Include Match List** radio button in the **New Match List** page to include rules from the match-lists already created in your system to another match-list.

Step 2: Match List Include table is displayed. This displays all the configured match-lists.

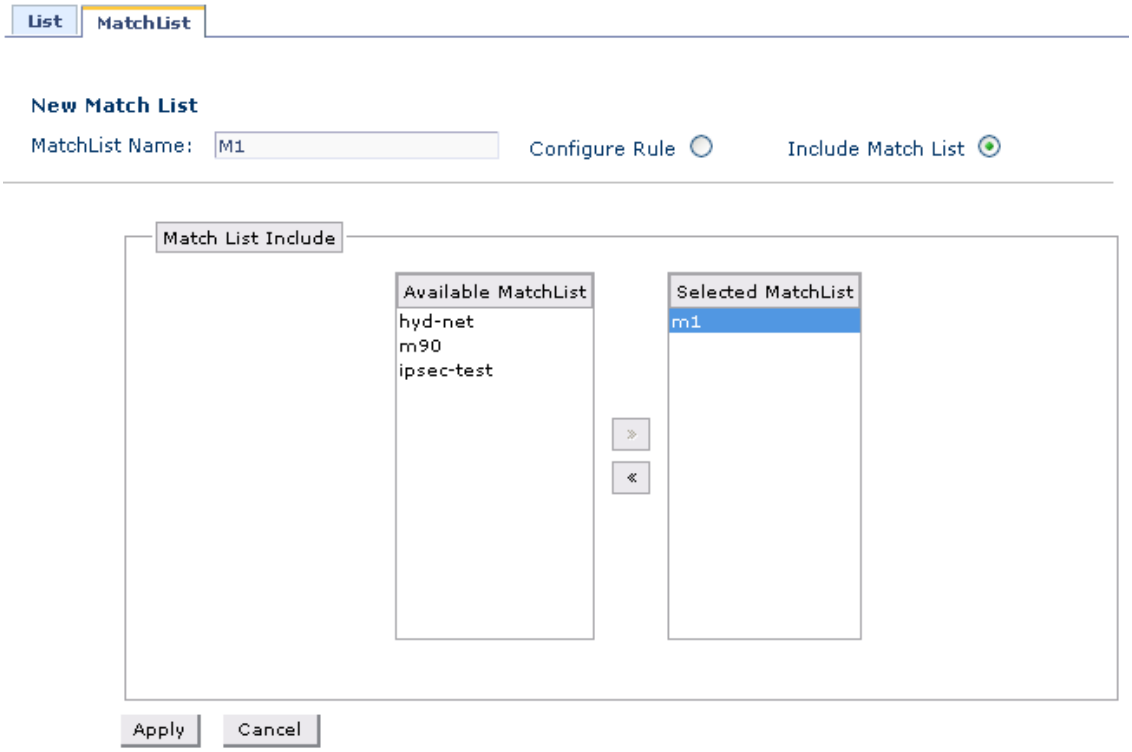


Figure 63: Traffic Classification - New Match List Include

Step 3: Select the match-list to be included from the **Available MatchList** column and click the '**>>**' button to move it to the **Selected MatchList** column. Select as many match-lists from the Available MatchList column and move it to the Selected MatchList column.

Step 4: Click **Apply** to include the selected match-list to the match-list you are creating and to return to Match Lists page, or **Cancel** to return to the Match List page.

EDITING RULE/INCLUDED MATCH-LISTS FOR A MATCH-LIST

Editing Rule

1. Select the match-list whose rule details are to be edited. The rules already configured for the selected match-list is displayed in the **MatchList Details** table.
2. Click **Edit** icon in the **Action** column to edit the rule details.
3. **Edit Rule** page is displayed.

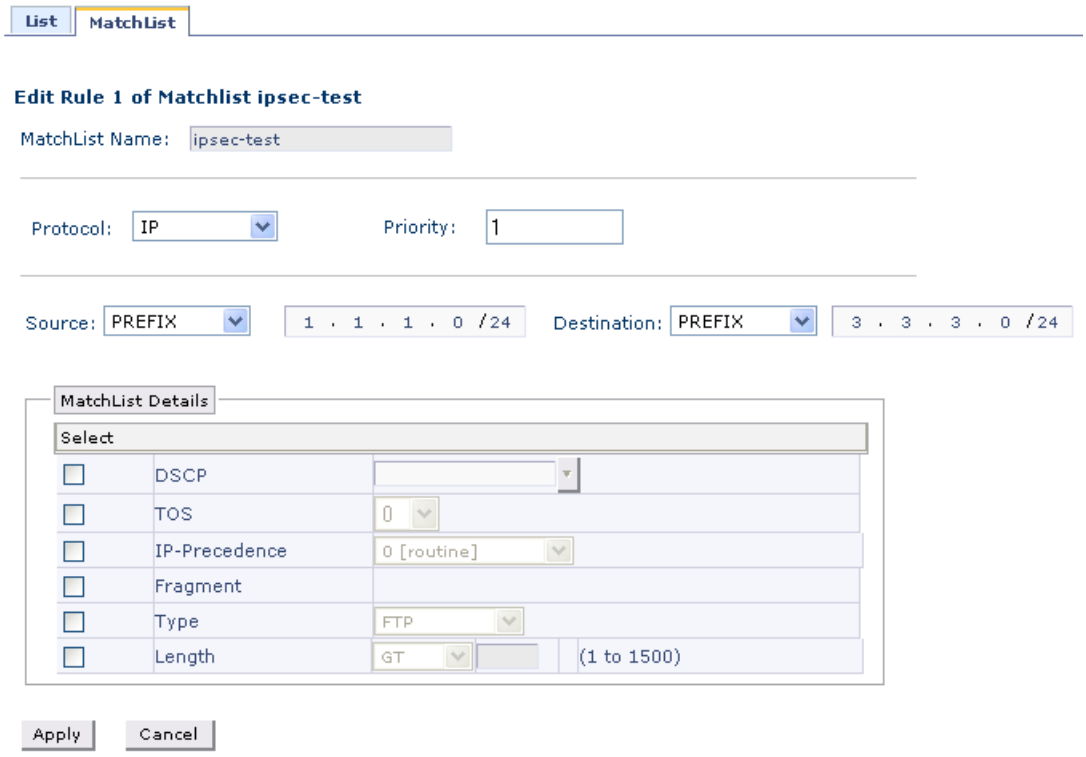


Figure 64: Traffic Classification - Match-list - Edit Rule

4. Make the required changes. Match-list Name is not editable.
5. Click **Apply** to save changes, or **Cancel** to retain the original settings.

Editing Included Match-lists

1. Select the match-list whose included match-list details are to be edited. The match-list/s included for the selected match-list is displayed in the **Included MatchList** table.
2. Select the match-list whose match-list details are to be edited, and click **Edit**.
3. **Edit MatchList Include** page is displayed. The match-list/s included for the selected match-list is displayed.

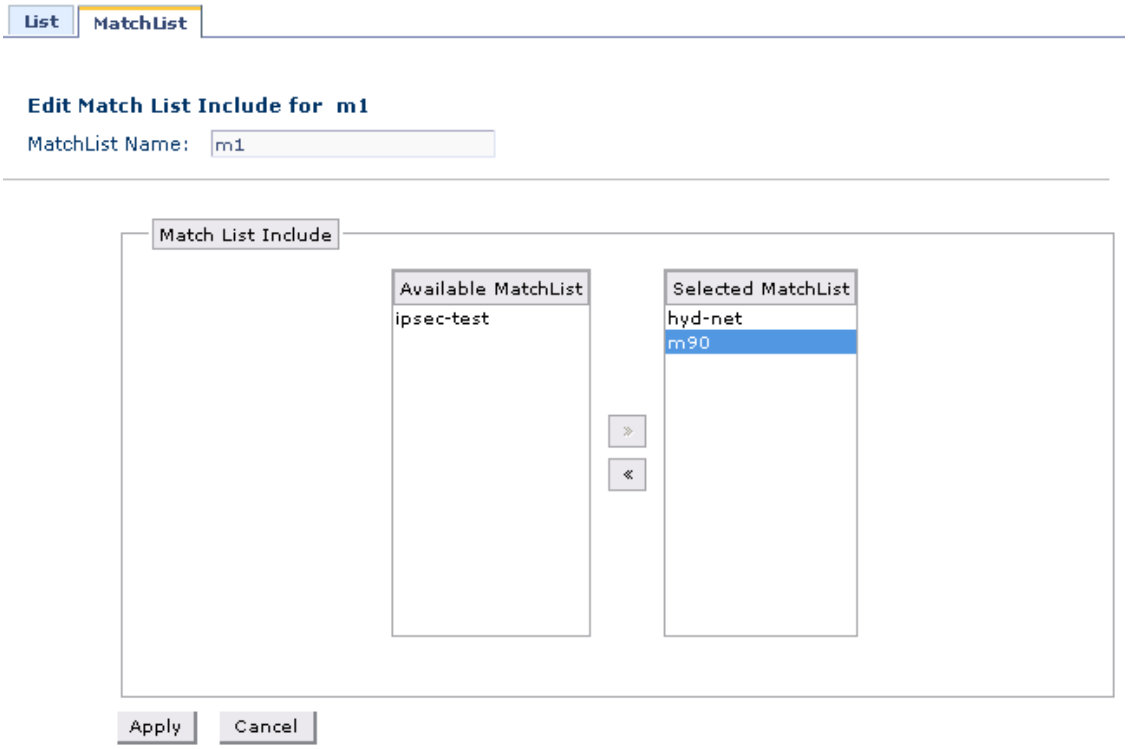


Figure 65: Traffic Classification - Add/Edit Included Match List

4. Make the required changes. Match-list Name is not editable.
5. Click **Apply** to save changes, or **Cancel** to retain the original settings.

Deleting Match-list

1. Click **Delete** icon in the **Action** column against the match-list to be deleted.
2. Confirm at the prompt to delete the match-list. This action deletes the match-list along with the rule and the included match-list details.

Deleting Rule for a Match-list

1. Select the match-list whose rule/s is to be deleted. The rules already configured for the selected match-list is displayed in the **MatchList Details** table.
2. Click **Delete** icon in the **Action** column against the rule to be deleted.
3. Confirm at the prompt to delete the rule.

FIREWALL

This allows you to apply the following settings on your system.

- Filters
- NAT
- DOS Attack
- Transparent Firewall
- Firewall Policy

FIREWALL CONFIGURATION WIZARD

This wizard allows you to create Firewall policy in few easy steps. It is a three Zone configuration:

1. Trusted Zone - It comprises of the local network (like LAN).

2. Untrusted Zone - It comprises of the Internet (like WAN).

3. Demilitarized Zone (DMZ) - It allows to publish the services (like ftp, mail), to the outside world. DMZ Services have a local IP (addresses in the intranet) and a global IP (addresses in the Internet).

Depending on the Management protocols that are selected, a firewall policy is generated that controls the traffic flow from the Untrusted network.

VIEWING FIREWALL WIZARD

Follow the procedure given below to view the Firewall Wizard page.

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Firewall** sub-menu.

The Firewall has the following tabs: **Firewall Wizard**, **Filters**, **NAT**, **DOS Attack, Transparent Firewall** and **Firewall Policy**. By default **Firewall Wizard** tab is selected and the **Firewall Configuration Wizard** page is displayed in the center panel.

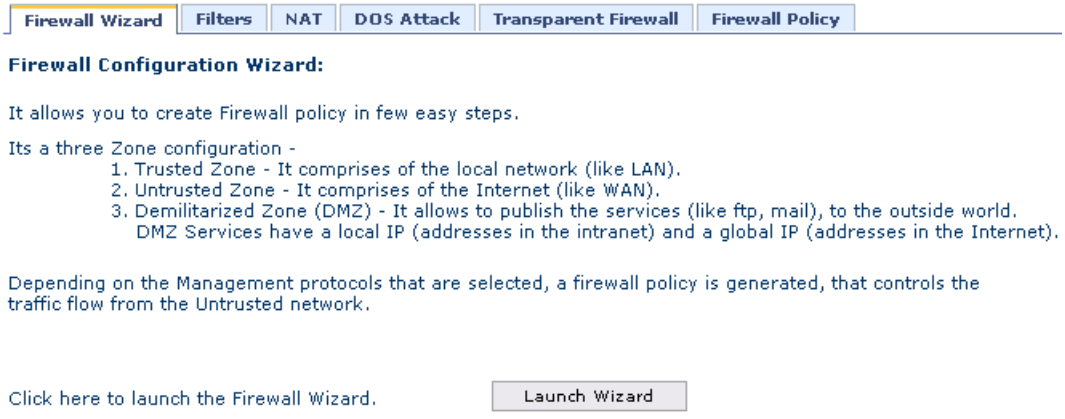


Figure 66: Firewall: Firewall Wizard

CONFIGURE FIREWALL POLICY USING THE WIZARD

Follow the procedure below to configure a Firewall Policy using the wizard.

Step 1: Click **Launch Wizard** in the **Firewall Configuration Wizard Policy** page to create new Firewall Policy. The following window is displayed:

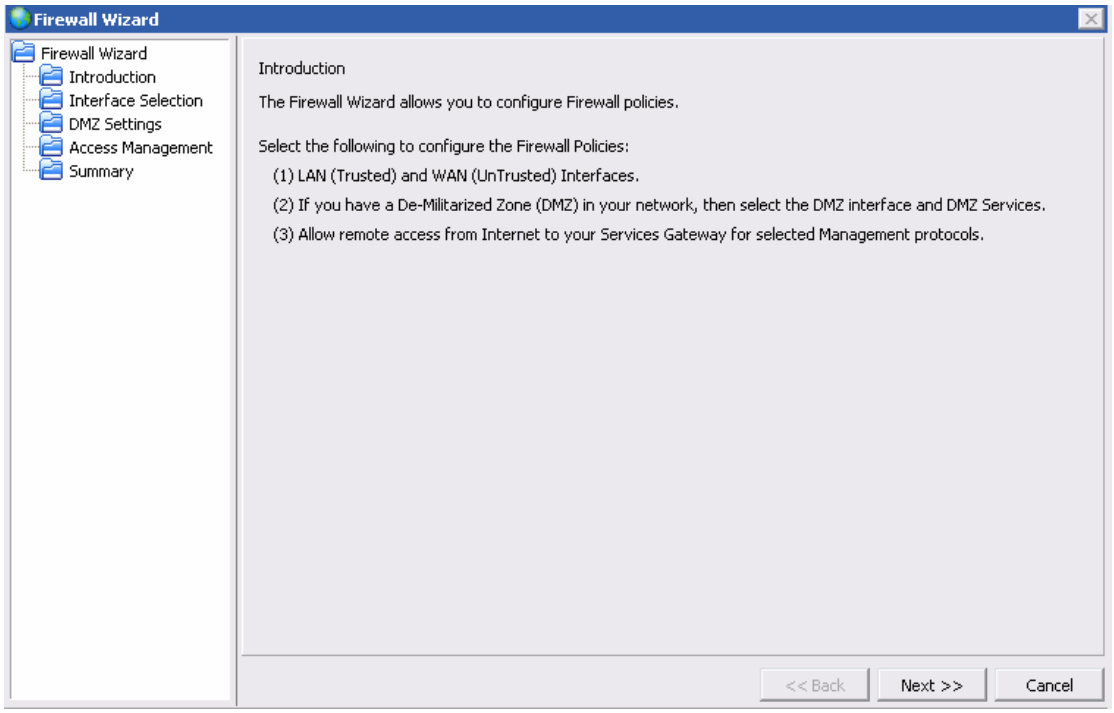


Figure 67: Firewall: Firewall Wizard - Introduction

Step 2: Click **Next**. **Interface Selection** window is displayed. This page allows you to attach a firewall policy to an interface.

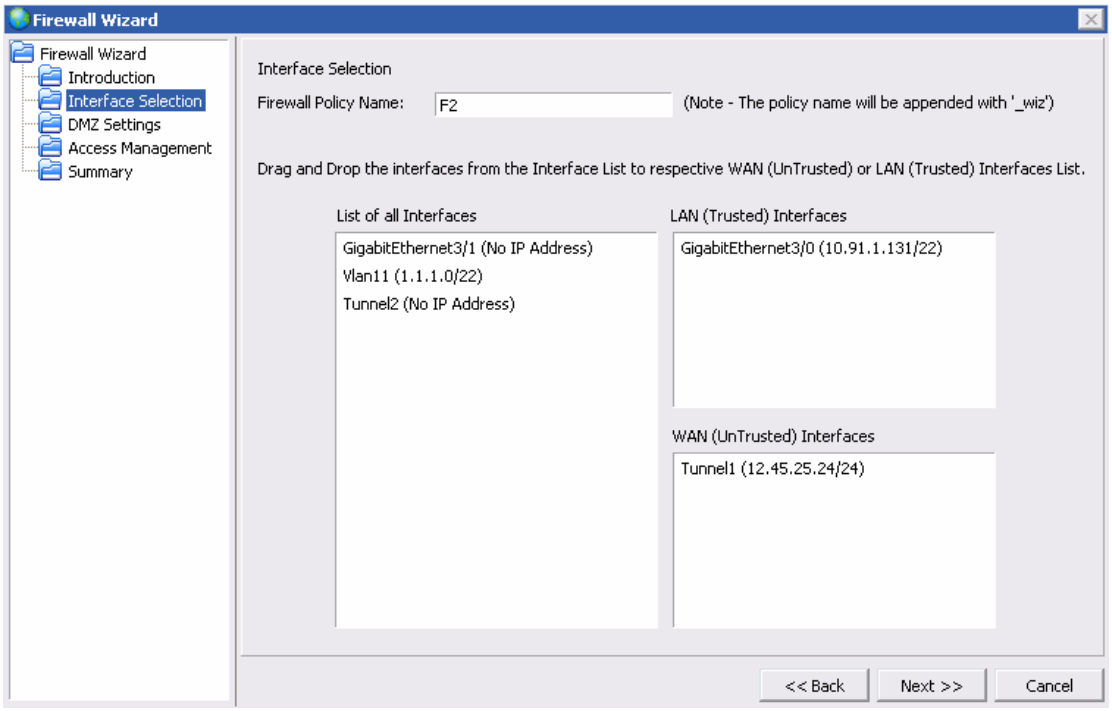


Figure 68: Firewall: Firewall Wizard - Interface Selection

1. Enter the firewall policy name in the **Firewall Policy Name** field.

Note: Once the firewall policy is created successfully, the policy name will be appended with '_wiz".

2. **List of Interfaces** box displays the interfaces that are available that can be attached to the firewall policy. Drag and drop the interfaces from this list to **LAN (Trusted) Interfaces** or **WAN (Untrusted) Interfaces** box.

Step 3: Click **Next**. **DMZ Settings** window is displayed.

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.

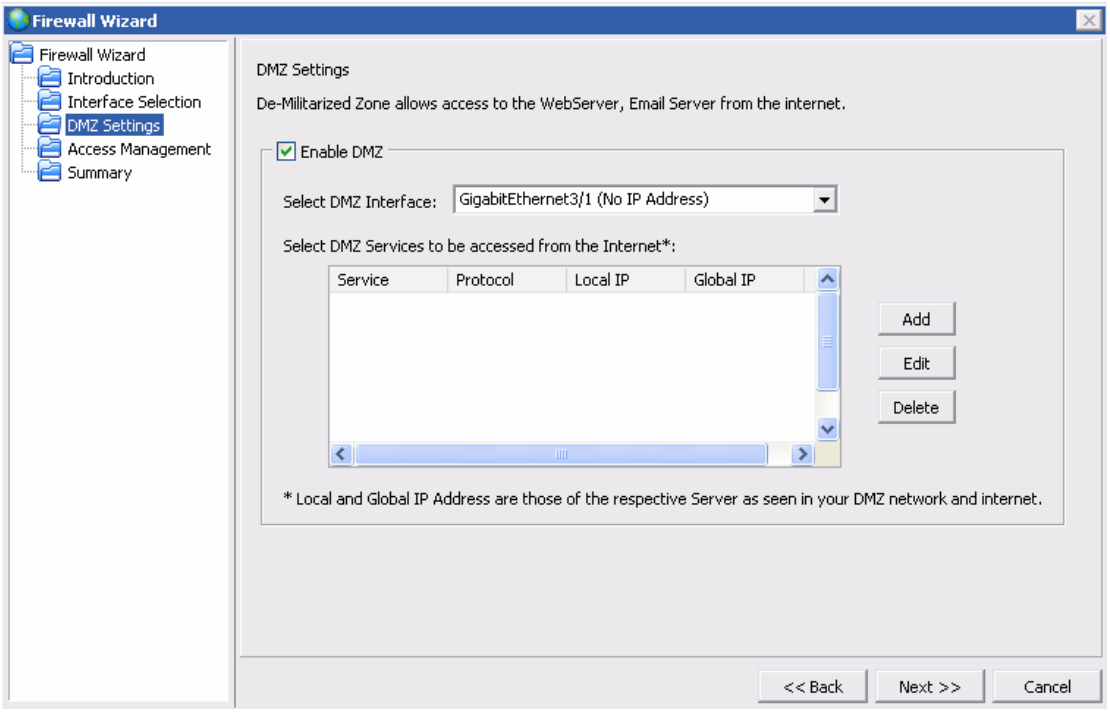


Figure 69: Firewall: Firewall Wizard - DMZ Settings

DMZ Settings for a firewall policy is optional.

In the wizard, by default, DMZ is enabled. Unselect the **Enable DMZ** check box, and click **Next** to continue firewall policy configuration without configuring DMZ settings.

Or

To configure DMZ settings, follow the procedure given below.

1. Select the DMZ interface from the **Select DMZ interface** drop-down list. If a policy is already attached to the selected interface, the system prompts you a message.
2. Add the DMZ services to be accessed through the internet. Click **Add**. **Add DMZ Services** pop up window is displayed:

   You have to add at least one DMZ service.

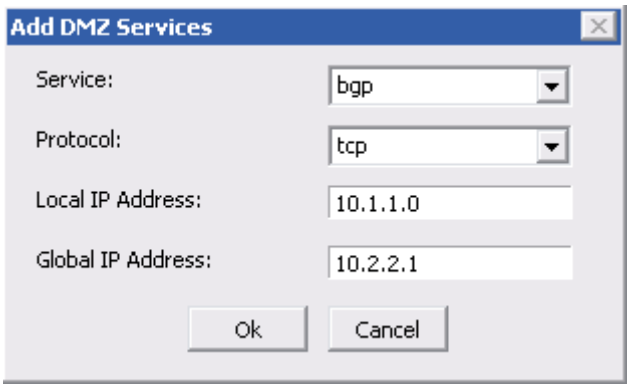


Figure 70: Firewall: Firewall Wizard - DMZ Settings - Add DMZ Service

- Select the service to be added from the **Service** drop-down list.
- Select the protocol type from the **Protocol** drop-down list.
- Enter the local and the global IP address in the **Local IP Address** and the **Global IP Address** fields.
  Local and Global IP Address are those of the respective Server as seen in your DMZ network and internet
- Click **OK**. The added service is displayed in the Select DMZ Services to be accessed from the Internet list. Repeat the procedure to add as many services as required.
- Select the service to be edited, and **Edit** to edit the service parameters, and click **Delete** to delete the selected service.

Step 4: Click **Next** to continue. **Access Management** window is displayed. Access Management allows remote management of the OA-700.(SSH/Telnet to access CLI, HTTP/HTTPS for Web based management and SNMP service.)

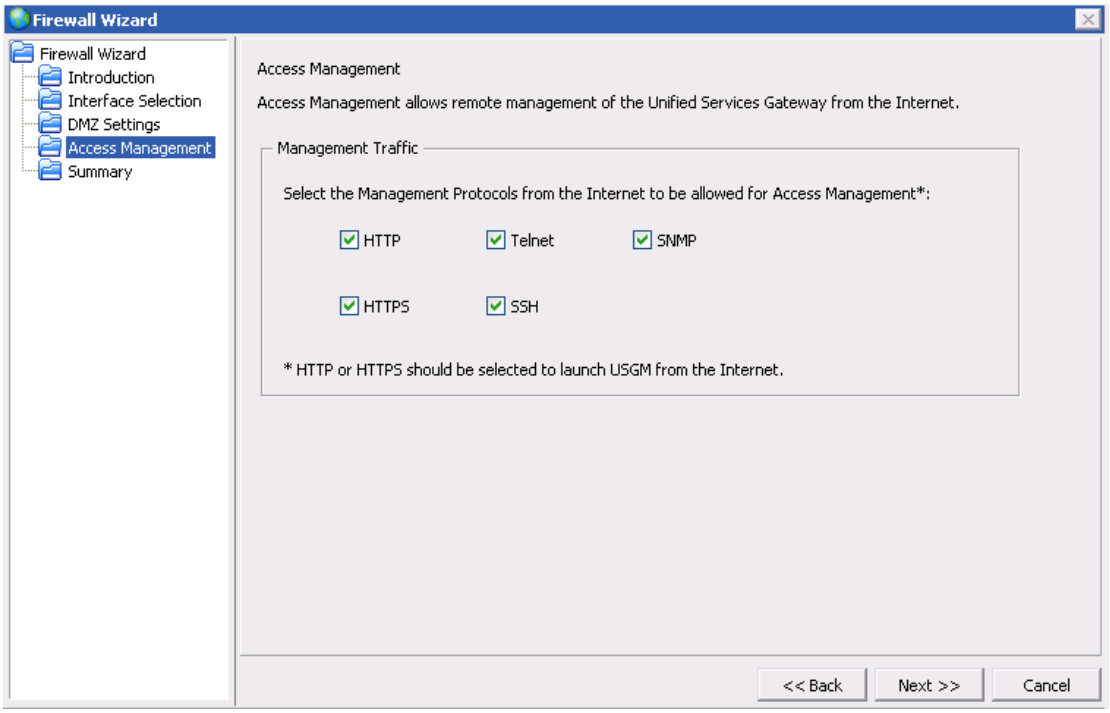


Figure 71: Firewall: Firewall Wizard - Access Management

1. By default all the access protocol are enabled.
2. Unselect the check box to disable the access protocol.

Step 5: Click **Next**. **Summary** window displays the summary of the firewall policy configuration.

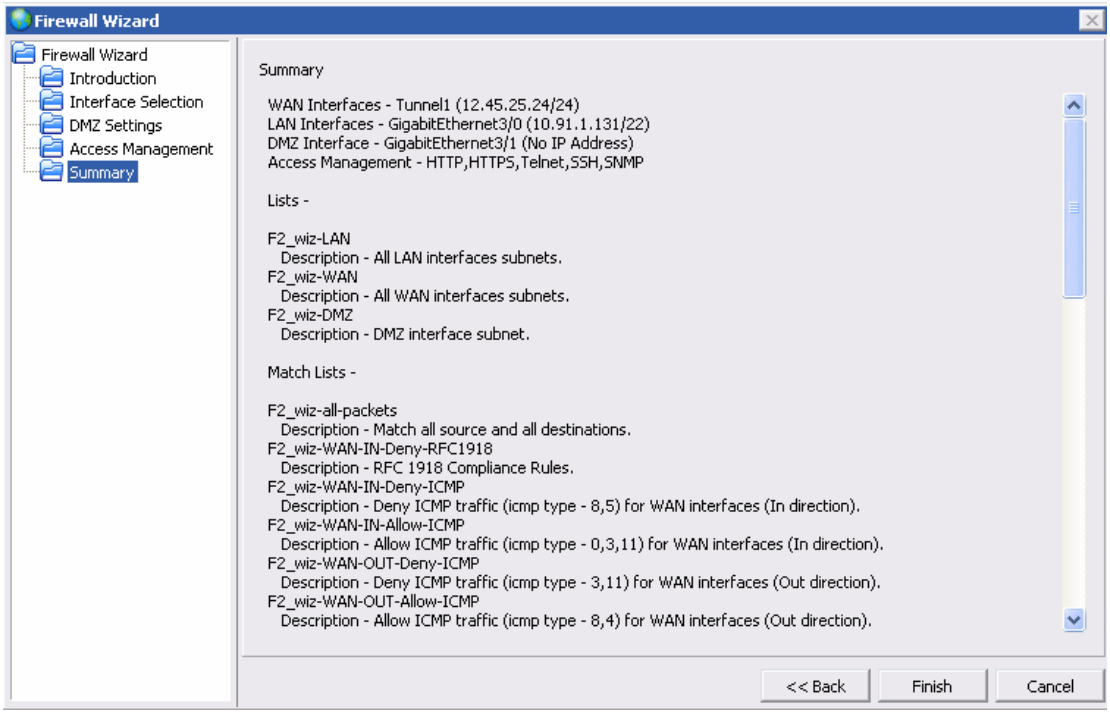


Figure 72: Firewall: Firewall Wizard - Summary

The Summary window displays the details of the firewall Policy being configured: The LAN and the WAN interfaces, DMZ interface (if any), the management protocols being configured for the firewall policy. It also displays the filters and the rules (lists and the match-lists) associated with the filter, and the DoS attack that are auto generated by the wizard.

Step 6: Click **Finish** to save the configuration and generate the firewall policy.

Step 7: A status bar is displayed showing the firewall policy creation. Once the firewall policy is configured successfully, a successful message is displayed.

The filters, DOS attack, and the firewall policy auto configured by the wizard is displayed in the **Filters**, **DoS Attack** and **Firewall Policy** tabs as shown below.

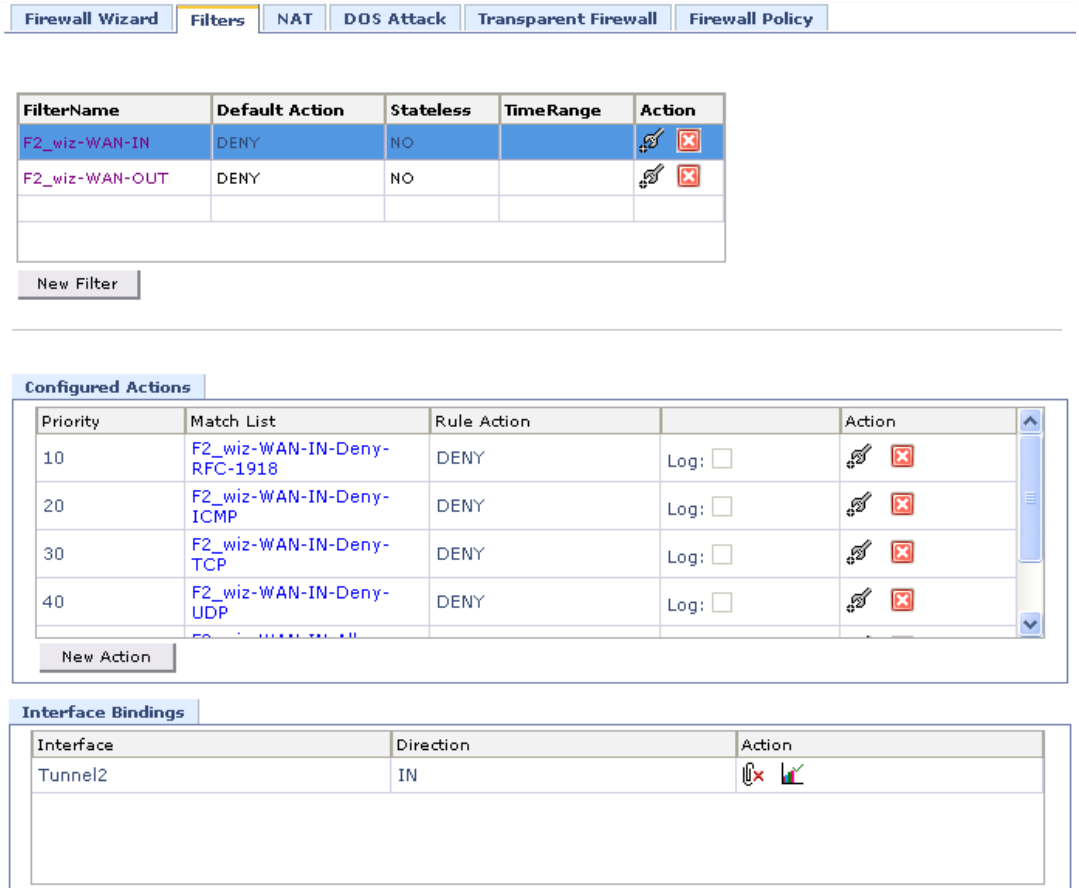


Figure 73: Firewall: Filters Generated by the Wizard

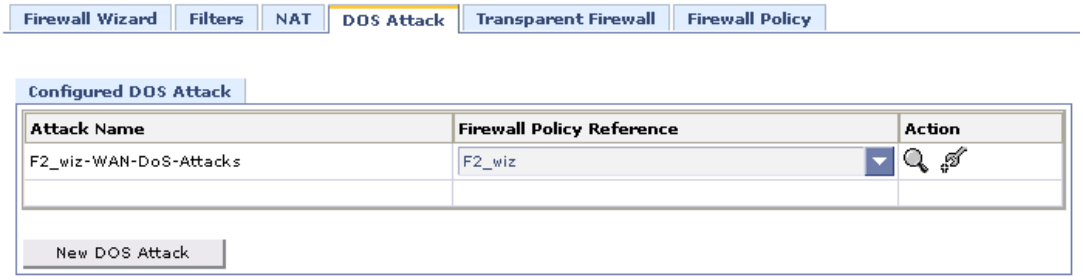


Figure 74: Firewall: DoS Attack Generated by the Wizard

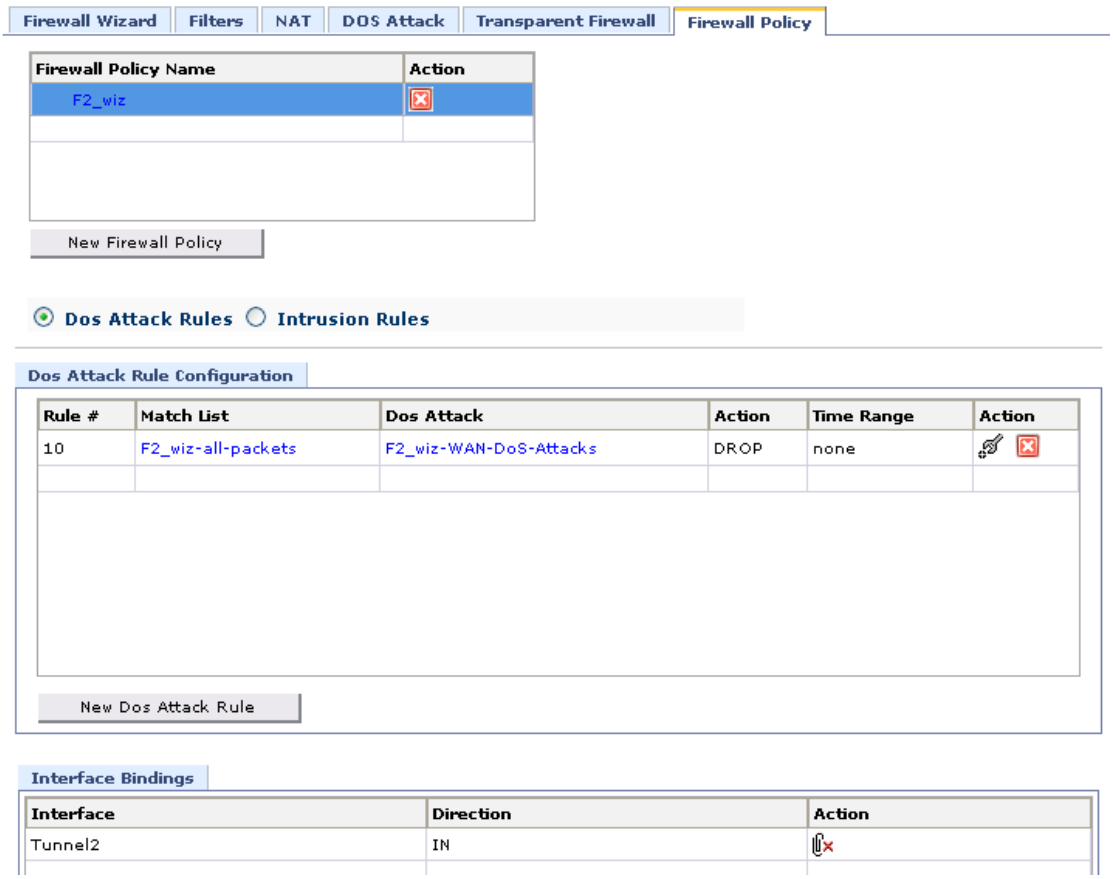


Figure 75: Firewall: Firewall Policy Generated by the Wizard

FILTERS

This page allows you to add/edit the filters.

OA-700 Specific Overview

- The default action for a filter is **“deny”**. However, you can change this to “**permit**”.
- By default OA-700, supports “**stateful inspection**”. However, you can change this to “**stateless**”.
- 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.

VIEWING FILTERS

Follow the procedure given below to view the Filters page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall** sub-menu.

The Firewall has the following tabs: **Firewall Wizard**, **Filters**, **NAT**, **DOS Attack, Transparent Firewall** and **Firewall Policy**. Select **Filters** tab. **Filters** page is displayed in the center panel.

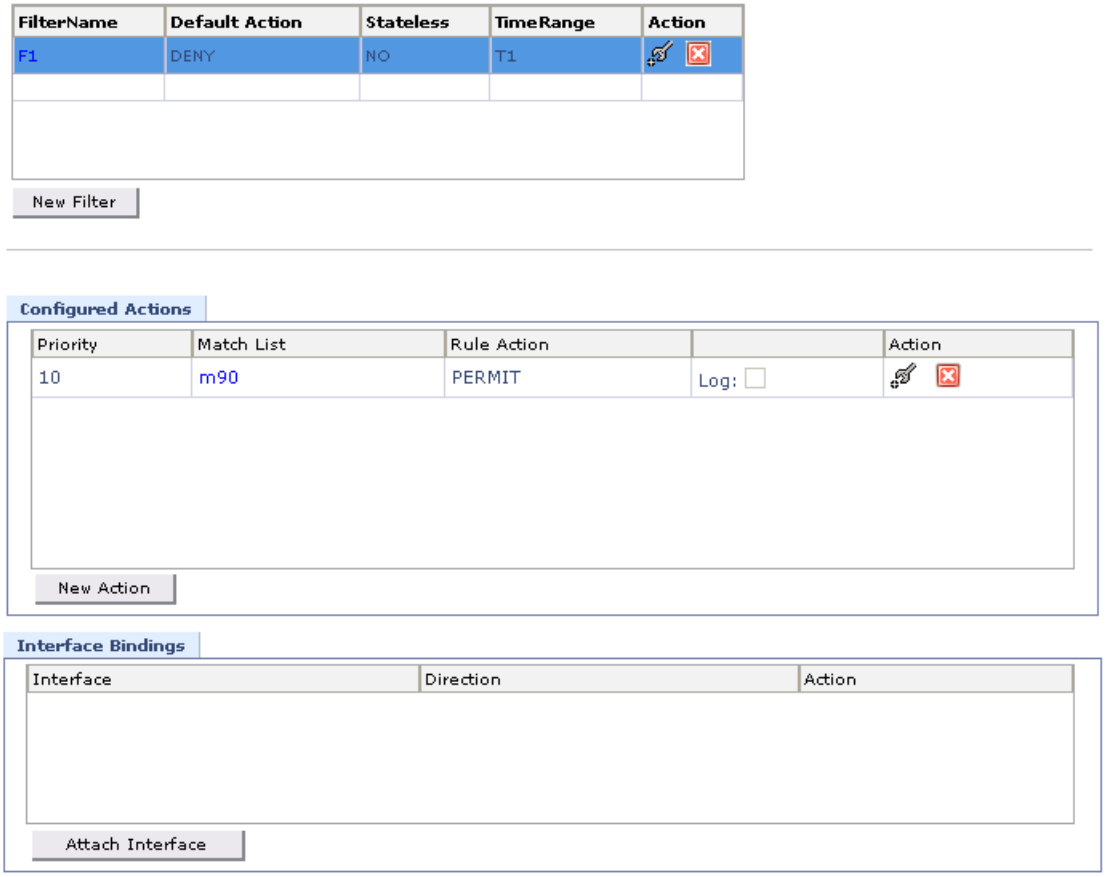


Figure 76: Firewall - Filters

The table below provides field description for the Filters page.

Table 14: Filter Field Description

Field	Description
FILTER	
Filter Name	Name of the filter
Default Action	Default action for the filter: PERMIT or DENY
Stateless	Displays if the filter is stateless or stateful
Time Range	Time range configured for the filter.
Action	Provides option to edit the filter parameters and delete the filter
New Filter	Create a new filter
Configured Actions	
Priority	Priority set for the filter rule
Match-list	Match-lists associated to the filter.
Rule Action	Action for the rule: DENY/PERMIT
Action	Provides option to edit/delete the configured rule
New Action	Add a new rule to the filter
Interface Bindings	
Interface	List of interfaces to which the filters are applied
Direction	Filter Direction: Ingress (IN)/Egress (OUT) direction
Attach Interface	Attach filter to an interface.

CREATING A FILTER

Follow the procedure given below to create filter:

Step 1: Click **New Filter** in the **Filters** page to create new filter.

The **New Filter** page is displayed.

Figure 77: Firewall: Filters - New Filter

Step 2: Set the filter parameters in the **Filter Params** table.

1. Enter the filter name in the **Filter Name** field.
2. Select the default action for the filter from the **Default Action** drop-down list: **DENY/PERMIT**.
3. Select the stateless filtering option from the **Stateless** drop-down list: **YES/ NO**

Note: You can configure time range for a filter. The option to add time range to the filter is enabled in Edit Filter Params table. See "Edit Filter Parameters" section to configure time range for the filter.

Step 3: Click **Apply** to add a new filter, or **Cancel** to cancel adding new filter.

CONFIGURE RULE FOR A FILTER

You can 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.

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.

Step 1: Configure rule for the filter in the **Configured Actions** table.

1. Select the filter from the **Filter** list.
2. Click **New Action** in the **Configured Actions** table.

   This populates fields to define action for the filter as shown below:

Figure 78: Firewall: Filters - Add Rule to a Filter

3. Enter the priority number in the **Priority** field.

   Priority number indicates which rule would be applied first when the filter is bound to an interface. Lower the number, higher the priority. If you do not enter any priority, the system takes default priority number of 10, or increments 10 to the last entered value.
4. Select the match-list for the filter from the **Match List** field.
5. Set the action for the filter in the **Rule Action** field: **Permit, Deny, Deny-Reset**.

   Permit allows traffic to pass through, Deny blocks the traffic. Deny-reset sends TCP RST to the source, for TCP traffic that matches the classification, and drops packets for other non-TCP traffic.
6. Check **Log** check box to enable logging. This logs the first packet of a session.
7. Click **Apply** to set new action for the filter.

ATTACH FILTER TO AN INTERFACE

Step 1: Bind the filter to the interface in the **Interface Bindings** table.

1. Select the filter from the **Filter** list.
2. Click **Attach Interface** to attach filter to the interface. This populates fields to as shown below:

Figure 79: Firewall: Filters - Attach Filter to an Interface

3. Select the interface from the **Interface** list.
4. Set the direction to which the filter is to be applied: IN/OUT
5. Click **Apply** to attach the filter to the selected interface.

DETACH FILTER FROM AN INTERFACE

1. Select the filter from the filter list.

   Interfaces already bound to the selected filter are displayed in **Interface Bindings** table.
2. Click **Detach** icon in the **Action** column to detach filter from the selected interface.
3. Confirm at the prompt to detach the filter.

ENABLE INTERFACE STATISTICS

1. Select the filter from the filter list.

   Interfaces already bound to the selected filter are displayed in **Interface Bindings** table.
2. Click **Enable Interface Statistics** icon to enable interface statistics.
3. Click the same icon to disable interface statistics for a filter.

EDIT FILTER PARAMETERS

1. From the Filter list, click on the **Edit** icon in the **Action** column against the filter whose parameters is to be edited.

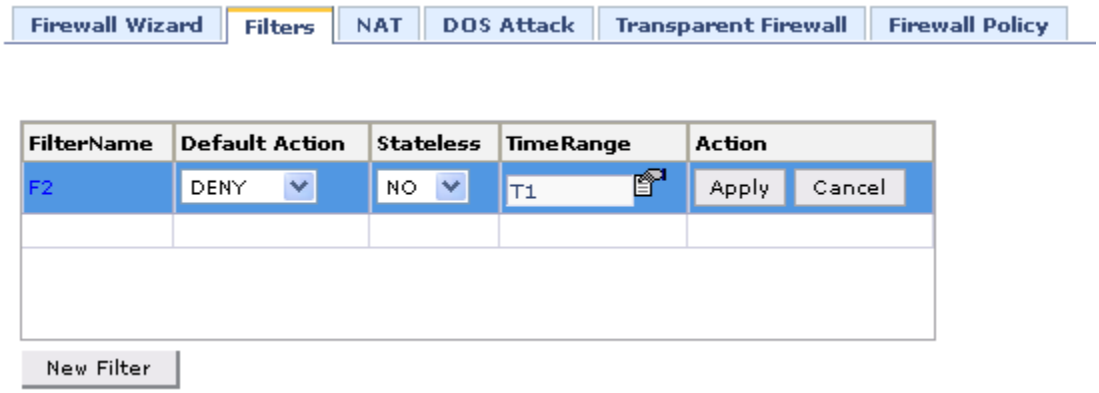


Figure 80: Firewall: Filters - Edit Filter Parameters

2. Enter the new filter parameters in the respective columns.

   Default Action, Stateless, and Time Range.
3. Click **Apply** to save the changes made to filter parameters, or **Cancel** to retain original parameters.

DELETE FILTER

1. Select the filter policy from the Filter list.
2. Click **Delete** icon in the **Action** column against the filter to be deleted.
3. Confirm at the prompt to delete the selected filter.

EDIT FILTER RULE

1. Select the filter from the filter list.

   Rules already configured for the selected filter is displayed in **Configured Actions** table.
2. Click **Edit** icon in the **Action** column against the filter rule to be edited.
3. Edit the rule parameters for the filter.

   Edit Priority, Match-list, Rule Action, and Log settings.
4. Click **Apply** to save changes, or **Cancel** to retain original settings.

DELETE FILTER RULE

1. Select the filter from the filter list.

   Rules already configured for the selected filter is displayed in **Configured Actions** table.
2. Click **Delete** icon in the **Action** column against the filter rule to be deleted.
3. Confirm at the prompt to delete action.

NAT

This page allows you to add/or edit the NAT policies.

OA-700 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.
- 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.

VIEWING NAT

Follow the procedure given below to view NAT page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall** sub-menu.

The Firewall has the following tabs: **Firewall Wizard**, **Filters**, **NAT**, **DOS Attack, Transparent Firewall** and **Firewall Policy**. Select **NAT** tab. **NAT** page is displayed in the center panel.

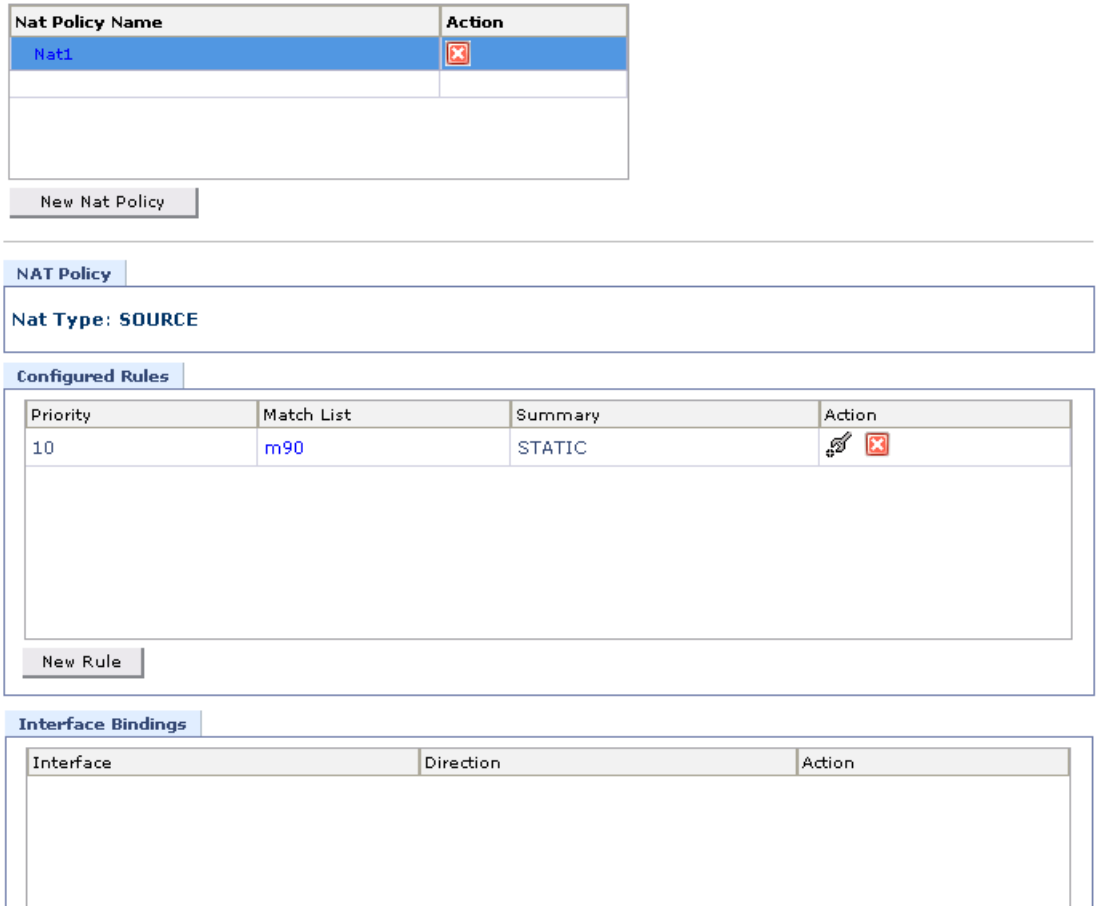


Figure 81: Firewall and Security: NAT

The table below provides field description for NAT page.

Table 15: NAT Field Description

Field	Description
NAT	
Nat Name	Lists the NAT policies configured.
Action	Provides option to delete the selected NAT policy.
New Nat	Create a new NAT Policy.
NAT Policy	
Nat Type	Type of the NAT configured: Source NAT or Destination NAT.
Configured Rules	
Priority	Priority set for the NAT rule.
Match List	Match-list associated to the NAT rule.
Summary	Summary of parameters on the NAT filter
Action	Provides option to edit/delete the configured NAT Rule
New Rule	Configure new NAT rule.
Interface Bindings	
Interface	List of interfaces to which the NAT is applied
Direction	The direction to which the NAT is applied: In coming (IN) or out going (OUT).
Attach Interface	Attach NAT to an interface.

CREATING NAT POLICY AND CONFIGURE NAT RULE

Follow the procedure given below to create NAT policy and configure NAT Rule:

Step 1: Click **New NAT Policy** in the **NAT Policy** page to create a new NAT policy.

The **New NAT Configuration** page is displayed.

Figure 82: Firewall: NAT - New NAT Configuration

Step 2: Enter NAT name in the **NAT Policy Name** field.

Step 3: Select type of NAT: **Source** or **Destination** from **NAT Type** box.

Step 4: Click **Apply** to create new NAT. **NAT Rule Configuration** page for the new NAT you just created is displayed.

Step 5: Configure NAT rule for selected rule type.

Select the NAT Rule Type: **Static Address Translation (1:1)**, **Address & Port Translation** or **Bypass**.

STATIC ADDRESS TRANSLATION (1:1)

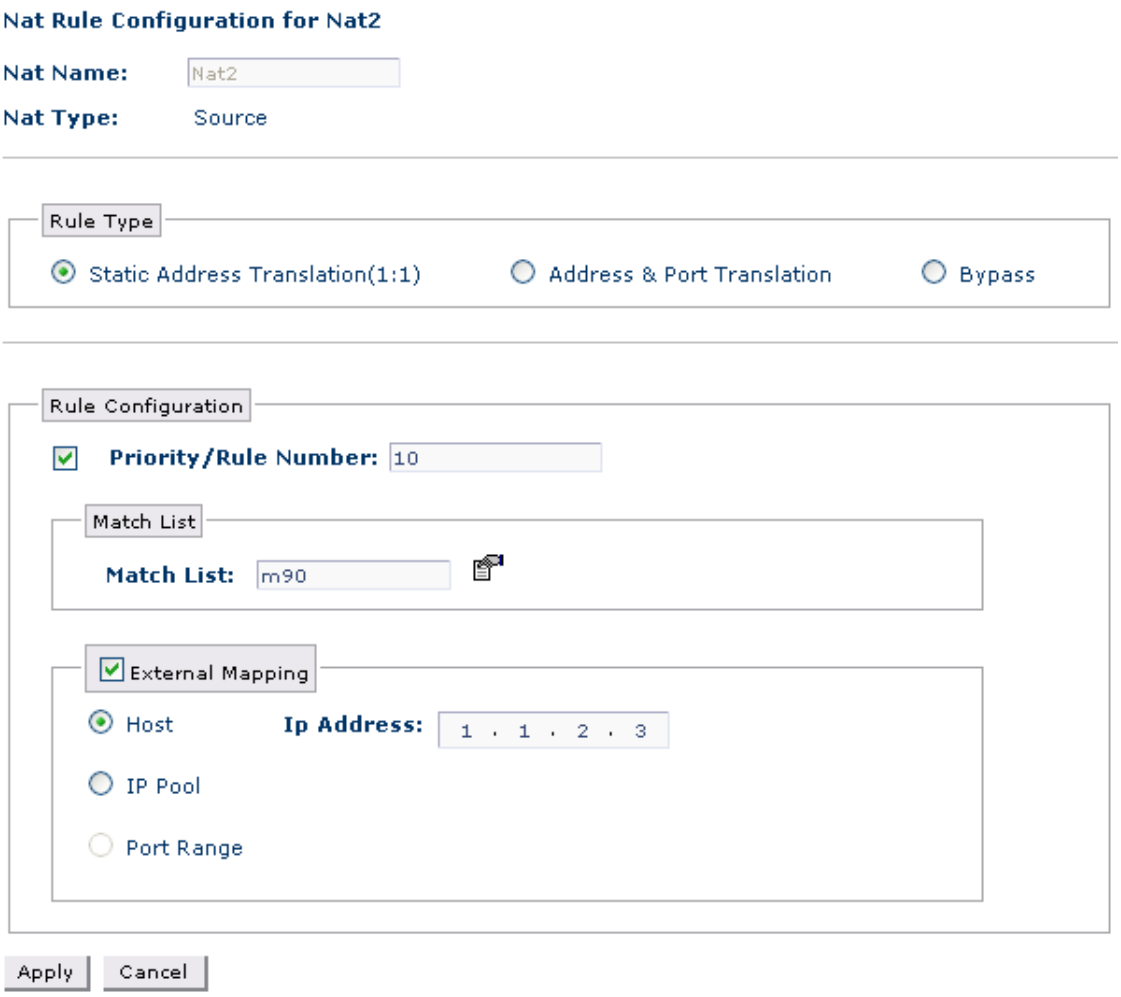


Figure 83: Firewall: NAT Rule - Static Address Translation

1. Select the **Priority/Rule Number** check box to set the priority number for the rule to be applied.
   Priority number indicates which rule would be applied first when the NAT policy is bound to an interface. Lower the number, higher the priority. If you do not enter any priority, the system takes default priority number of 10, or increments 10 to the last entered value.
2. Select the match-list. Select the match-list from the **Match List** field in the Match List box.
3. Set External Mapping. Select the **External Mapping** check box to set the external mapping to the NAT filter you are creating. This populates external mapping fields.
   - Select **Host** radio button, enter the IP address of the host in the **IP Address** field.
   - Select **IP Pool** radio button, select the list name from the **Pool Name** list.
   - The **Port Range** radio button is disabled for Static Address Translation.

ADDRESS AND PORT TRANSLATION

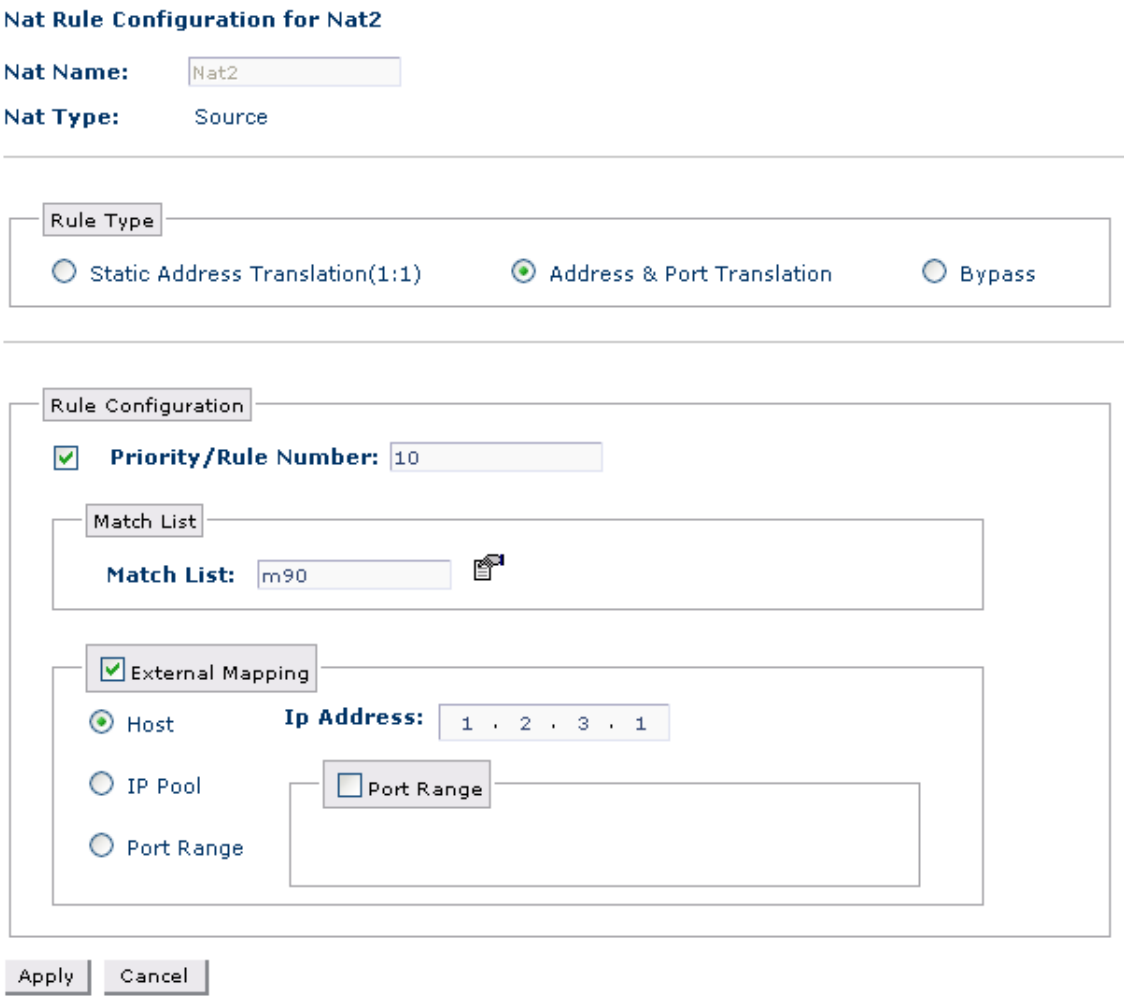


Figure 84: Firewall: NAT Rule - Address & Port Translation

1. Set Priority/Rule Number.

   Check the **Priority/Rule Number** check box to set the priority number for the rule to be applied. Higher the number, higher is the priority.

2. Select match-list.

   Select the match-list from the **Match List** field in the Match List box.

3. Set External Mapping.

   Check the **External Mapping** check box to set external mapping to the NAT filter you are creating. This populates external mapping fields.

   - Select **Host** radio button, enter the IP address of the host in the **IP Address** field.
   - Select **IP Pool** radio button, select the list name from the **Pool Name** list.
   - Check **Port Range** check box or select the **Port Range** radio button, enter lower and upper port range values in the **Lower** and **Upper** fields.

BYPASS

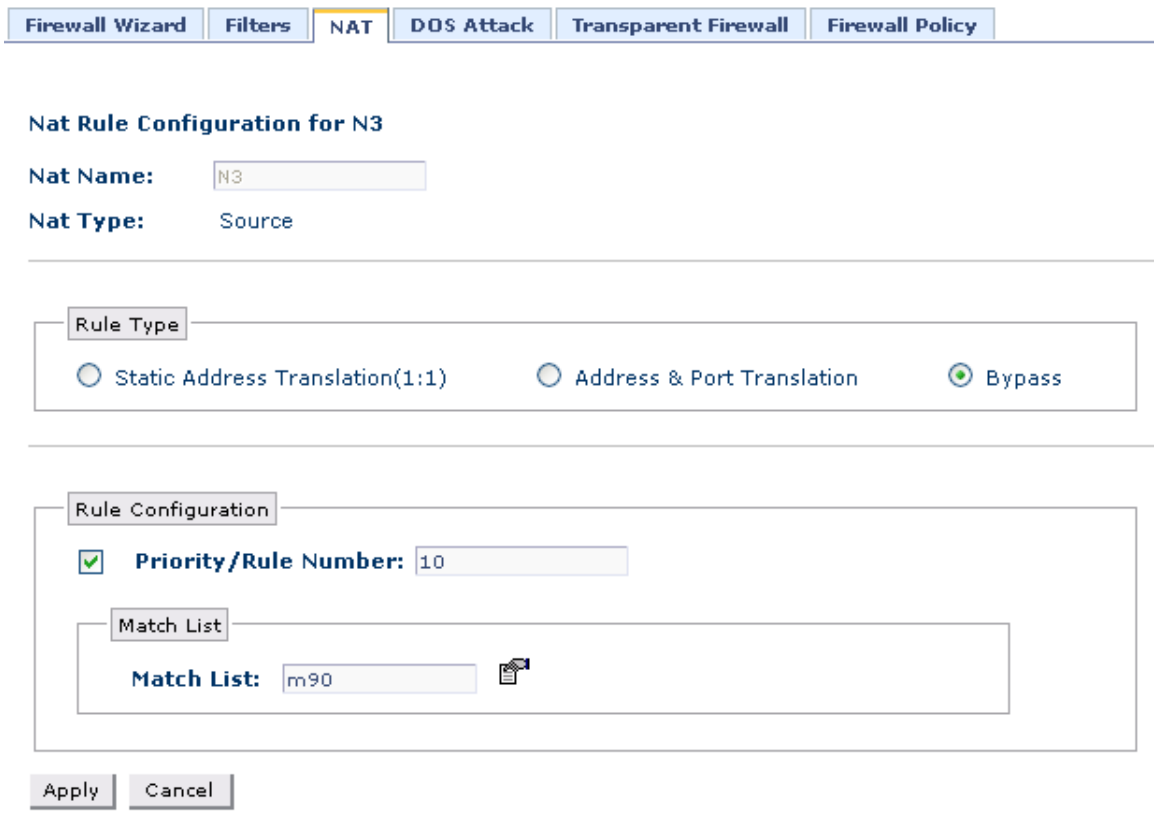


Figure 85: Firewall: NAT Rule - Bypass

1. Set Priority/Rule Number.

   Check the **Priority/Rule Number** check box to set the priority number for the rule to be applied. Higher the number, higher is the priority.
2. Select match-list.

   Select the match-list from the **Match List** field in the Match List box.

Step 6: Click **Apply** to configure NAT rules for the newly created NAT policy, or **Cancel** to return to the NAT Policy page.

ATTACH NAT POLICY TO AN INTERFACE

Follow the procedure to attach a NAT policy on an interface.

1. Select the NAT policy to be attached on an interface from the **NAT Policy Name** list.
2. Click **Attach Interface** in the **Interface Bindings** table. This populates fields to as shown below:

Figure 86: Firewall: NAT - Attach NAT to an Interface

3. Select the interface in the **Interface** column.

   The direction for the interface is set automatically when the interface is selected.
4. Click **Apply** to add the selected NAT to the selected interface or click **Cancel** to cancel the operation.

DETACH NAT FROM AN INTERFACE

1. Select the NAT from the NAT list.

   Interfaces already bound to the selected NAT are displayed in **Interface Bindings** table.
2. Click **Detach** icon in the **Action** column to detach the NAT from the selected interface.
3. Confirm at the prompt to detach the NAT.

ENABLE INTERFACE STATISTICS

1. Select the NAT from the NAT list.

   Interfaces already bound to the selected NAT are displayed in **Interface Bindings** table.
2. Click **Enable Interface Statistics** icon to enable interface statistics.
3. Click the same icon to disable interface statistics for a NAT policy.

ADD NEW RULE TO NAT POLICY

1. Select a NAT policy from the **NAT Policy Name** field.

   Rules already configured for the selected NAT policy is displayed in **Configured Rules** table. You can add more rules for the NAT policy.
2. Click on **New Rule** in the **Configured Rules** table.

   NAT Rule Configuration page for the selected NAT policy is displayed.
3. Select the rule type from the **Rule Type** box.
4. Configure rule settings in the Rule Configuration box.

   Follow Step 5 in the section “Creating NAT Policy and Configure NAT Rule”.
5. Click **Apply** to add new rule to the selected NAT.

EDIT NAT RULE

1. Select the NAT policy from the NAT policy list.

   Rules already configured for the selected NAT policy is displayed in **Configured Rules** table. You can edit the rule settings for the NAT policy.
2. Click **Edit** icon in the **Action** column against the NAT rule to be edited.

   NAT Rule Configuration page for the selected NAT rule is displayed.
3. Configure/edit NAT rule.

   Refer Step 5 in the “Creating NAT Policy and Configure NAT Rule” section to configure NAT rule settings.

DELETE NAT RULE

1. Select the NAT policy from the NAT policy list.

   Rules already configured for the selected NAT policy is displayed in **Configured Rules** table.
2. Click **Delete** icon in the **Action** column against the NAT rule to be deleted.
3. Confirm at the prompt to delete NAT rule.

DELETE NAT POLICY

1. Select the NAT policy from the NAT Policy list.
2. Click **Delete** icon in the **Action** column against the NAT policy to be deleted.
3. Confirm at the prompt to delete the selected NAT policy.

DOS ATTACK

This page allows you to add and/or edit DOS attacks.

VIEWING DOS ATTACK

Follow the procedure below to view DOS Attack page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall** sub-menu.

The Firewall has the following tabs: **Firewall Wizard**, **Filters**, **NAT**, **DOS Attack, Transparent Firewall** and **Firewall Policy**. Select **DOS Attack** tab. **DOS Attack** page is displayed in the center panel.

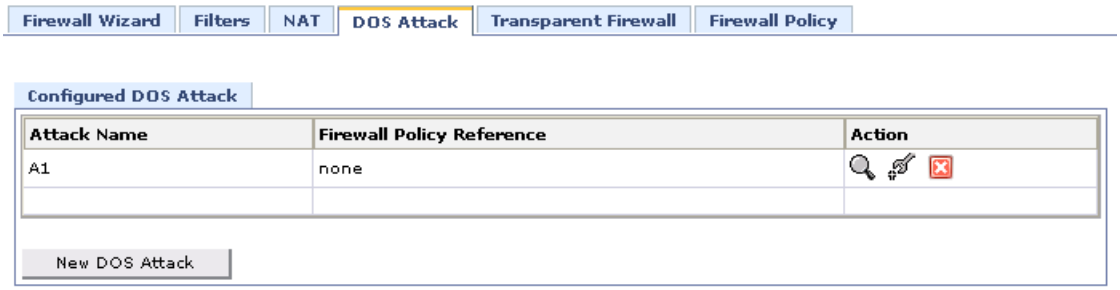


Figure 87: Firewall: DOS Attack

The table below provides field description for DOS Attack page.

Table 16: DOS Attack Field Description

Field	Description
DOS ATTACK	
Configured DOS Attack	
Attack Name	DOS attack configured on your system.
Firewall Policy Reference	Firewall policy to which the DOS attack is attached.
Action	Provides option to view the configured DOS attacks, edit, and delete the configured DOS attacks.
New DOS Attack	Allows to create a new DOS attack.

CREATING DOS ATTACK

Follow the procedure below to create DOS Attacks.

Step 1: Click **New DOS Attack** in **DOS Attack** page to create new DOS Attack.

The **New Attack** page is displayed.

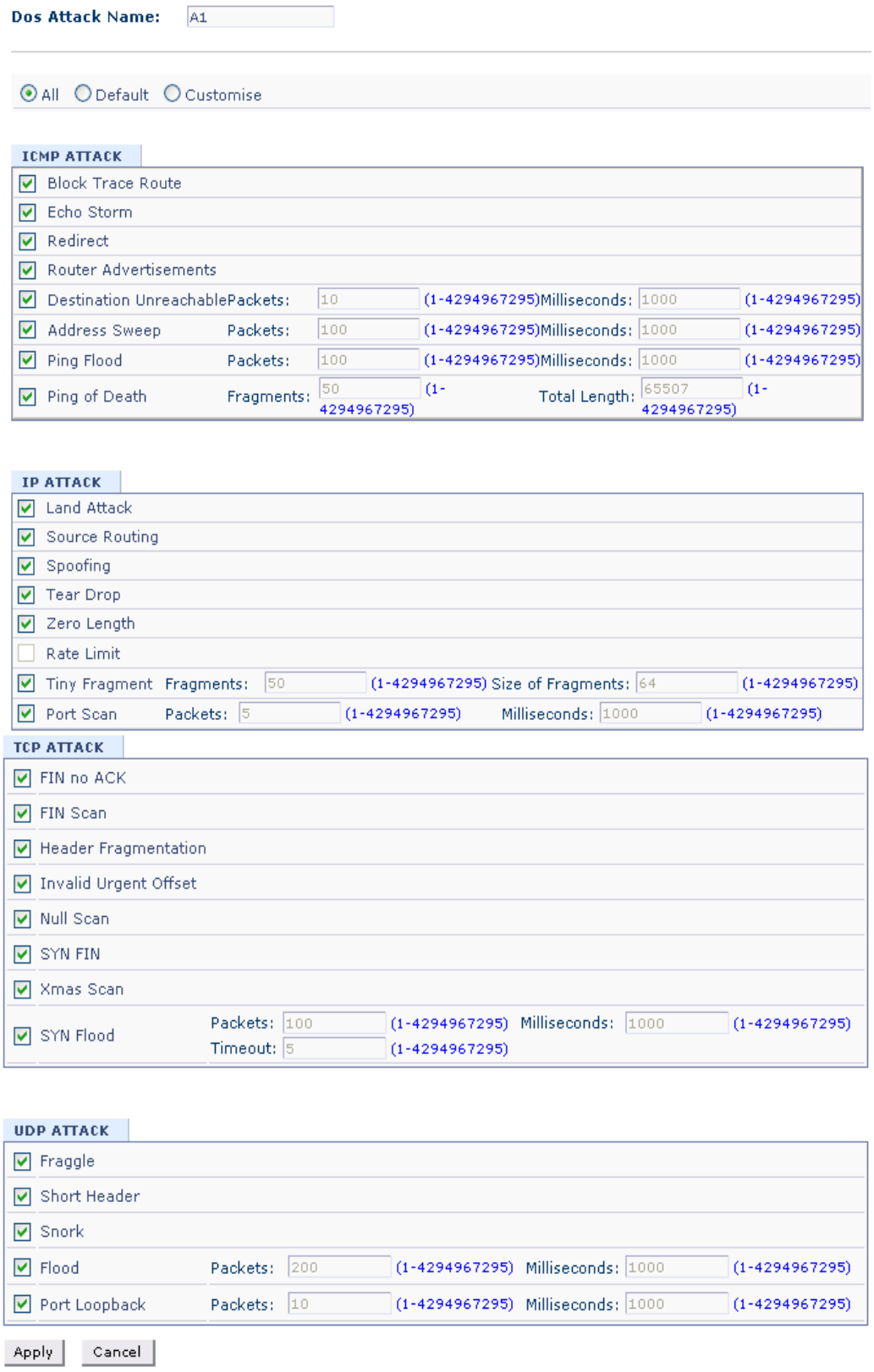


Figure 88: Firewall: DOS Attack - New

Step 2: Enter the name in **DOS Attack Name** filed.

Step 3: Choose the DOS Attack type: **All**/**Default**/**Customize**.

- If you want to choose all the DOS attack types defined in the system, select **All** radio button.
- If you want to choose default set of DOS attack types, select **Default** radio button.
  - Default option has two more radio buttons: **Stateful** and **Stateless**

    If you want to configure stateful attacks, select **Stateful** radio button.

    If you want to configure stateless attacks, select **Stateless** radio button.
- If you want to choose specific DOS attack types, select **Customize** radio button.

Step 4: To save the newly created DOS Attack, click **Apply**, else click **Cancel** to return to DOS Attack page.

VIEW CONFIGURED DOS ATTACKS

This enables you to view all the DOS attacks configured for a particular DOS Attack policy.

1. Click **View** icon in the **Action** column against the DOS attack policy whose DOS attacks is to be viewed.
2. The DOS attacks configured for the DOS attack policy is displayed in a pop up window as shown below:

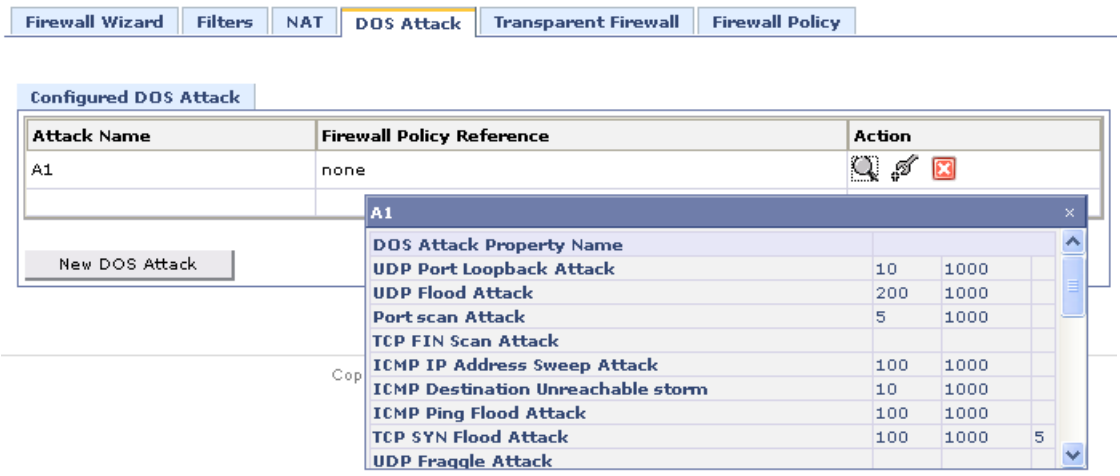


Figure 89: Firewall: DOS Attack - View

EDIT DOS ATTACK POLICY

1. Click the **Edit** icon in the **Action** column against the DOS attack to be edited.
2. Edit DOS attack settings in the **Configuration Attack** page.
3. Click **Apply** to save configuration changes or **Cancel** to return to DOS Attack page.

DELETE A DOS ATTACK POLICY

1. Click **Delete** icon in the **Action** column against the DOS attack to be deleted.
2. Confirm at the prompt to delete DOS attack policy.

Note: You cannot delete a DoS attack if the attack is attached to a firewall policy. To delete the attack object, disassociate the DOS attack from the firewall policy.

For more information on attaching an attack to a firewall policy, see “Adding Rule to Firewall Policy” section.

TRANSPARENT FIREWALL

This page allows you to add and/or edit Transparent Firewall (TF) policy.

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 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.

VIEWING TF

Follow the procedure below to view TF page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall** sub-menu.

The Firewall has the following tabs: **Firewall Wizard**, **Filters**, **NAT**, **DOS Attack, Transparent Firewall** and **Firewall Policy**. Select **Transparent Firewall** tab. **Transparent Firewall** page is displayed in the center panel.

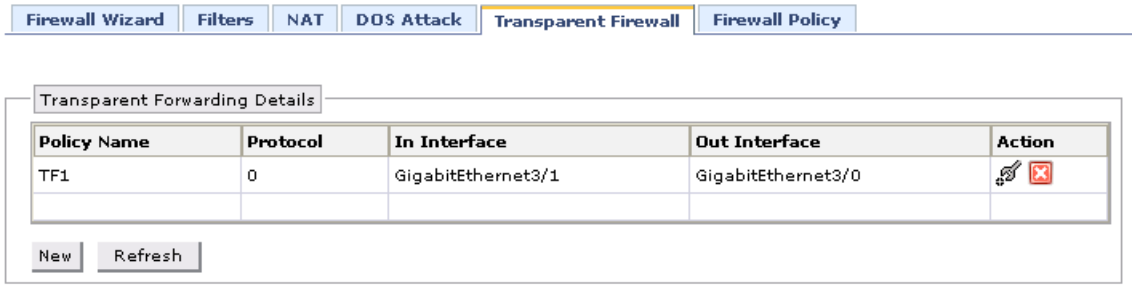


Figure 90: Firewall: Transparent Firewall

The table below provides field description for DOS Attack page.

Table 17: DOS Attack Field Description

Field	Description
TRANSPARENT FORWARDING DETAILS	
Policy Name	Name for the TF policy
Protocol	Protocol type
In Interface	Incoming interface on which the TF is configured
Out Interface	The outgoing interface
Action	Provides option to edit or delete the configured TF policy.
New	Allows to create a new TF policy.

CREATING TF POLICY

Follow the procedure below to create TF policy.

Step 1: Click **New** in **Transparent Forwarding Details** page to create new TF policy.

Add Transparent Forwarding page is displayed.

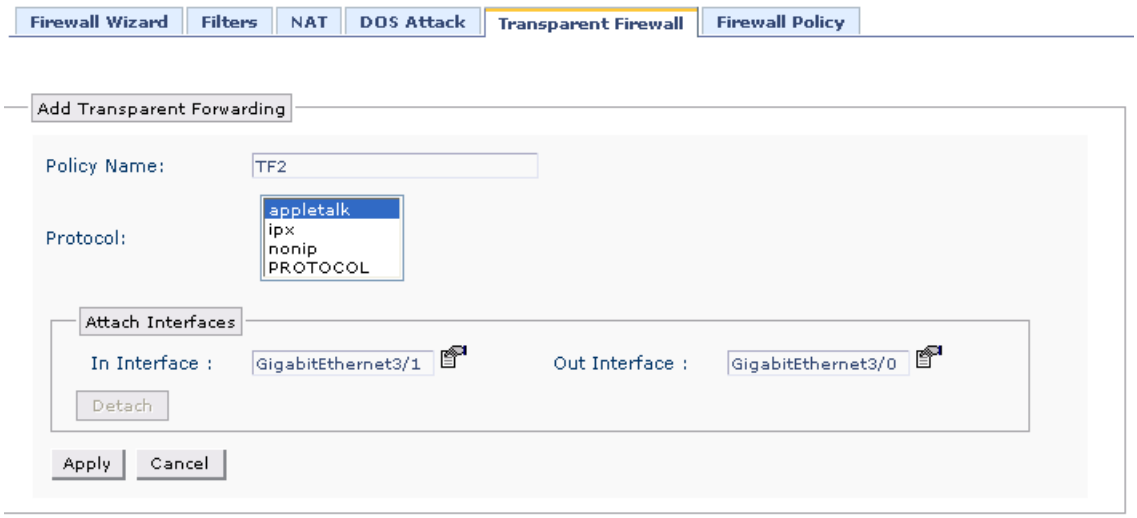


Figure 91: Firewall: Transparent Firewall - New

Step 2: Enter the TF policy name in the **Policy Name** field.

Step 3: Select the protocol type from the **Protocol** list.

By this, you are configuring protocols like IPX, Apple-talk to be bridged across the transparent firewalling interfaces. By default, IP and ARP protocols are configured as pass-through protocols.

Step 4: Select the incoming interface from the **In Interface** list. This configures the TF feature on the interface.

Step 5: Select the outgoing interface from the **Out Interface** list.

Step 6: Click **Apply** to add the new TF policy, or **Cancel** to cancel the operation.

EDIT TF POLICY

1. Click the **Edit** icon in the **Action** column against the TF policy to be edited.
2. Make the required changes. Policy Name cannot be modified.
3. Click **Detach** to detach the interfaces attached to the TF policy, if required.
4. Click **Apply** to save the changes or **Cancel** to cancel the operation.

DELETE TF POLICY

1. Click **Delete** icon in the **Action** column against the TF policy to be deleted.
2. Confirm at the prompt to delete TF policy.

FIREWALL POLICY

This page allows you to add and/or edit Firewall policies.

VIEWING FIREWALL POLICY

Follow the procedure below to view Firewall Policy page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall** sub-menu.

The Firewall has the following tabs: **Firewall Wizard**, **Filters**, **NAT**, **DOS Attack, Transparent Firewall** and **Firewall Policy**. Select **Firewall Policy** tab. **Firewall Policy** page is displayed in the center panel.

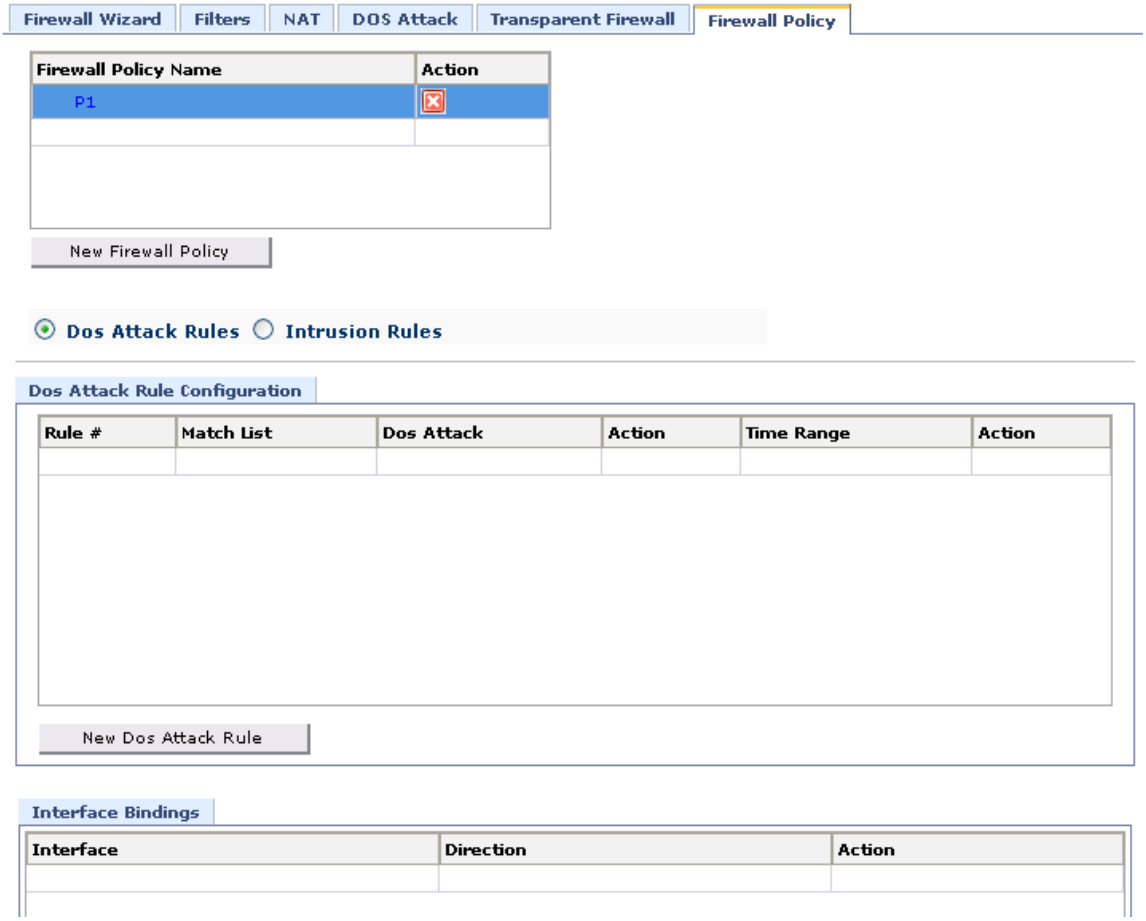


Figure 92: Firewall: Firewall Policy

The table below provides field description for Firewall Policy page.

Table 18: Firewall Policy Field Description

Field	Description
FIREWALL POLICY	
Firewall Policy Name	Name of the firewall policy.
Action	Provides option to delete the selected firewall policy.
New Firewall Policy	Allows to create new firewall policy.
DOS ATTACK RULE CONFIGURATION/INTRUSION RULE CONFIGURATION	
Dos Attack Rules	Select the **DOS Attack Rules** radio button for configuring DOS attack rule to the firewall.
Rule #	The rule number.
Match List	Match-list associated with the firewall policy.
Dos Attack	DOS attack policy associated with the firewall policy.
Action	Action defined for the firewall policy.
Time Range	Time range associated with the firewall policy.
Action	Provides option to edit or delete the DOS attack rules.
New DOS Attack Rule	Allows to create new DOS attack rule to the firewall policy.
Intrusion Rules	Select **Intrusion Rules** radio button for configuring intrusion rule to the firewall.
Rule #	The rule number.
Match List	Match-list associated with the firewall policy.
Sensor Name	The name of the sensor.
Threshold/Pkts	Threshold for the number of packets/ second.
Threshold/Milli Sec	Time in millisecond.
Mode	Detection, Prevention or Prevention-Reset.

Field	Description
Action	Provides option to edit or delete the intrusion rules.
New Intrusion Rule	Allows to create new intrusion rule for firewall policy.
INTERFACE BINDINGS	
Interface	Interface to which the firewall policy is attached.
Direction	Direction IN or OUT.
Action	Provides option to detach the firewall policy from an interface.
Attach Interface	Allows to attach a firewall policy to an interface.

CREATING FIREWALL POLICY

Follow the procedure below to create a Firewall Policy.

Step 1: Click **New Firewall Policy** in the **Firewall Policy** page to create new Firewall Policy.

The **New Firewall Policy** page is displayed.

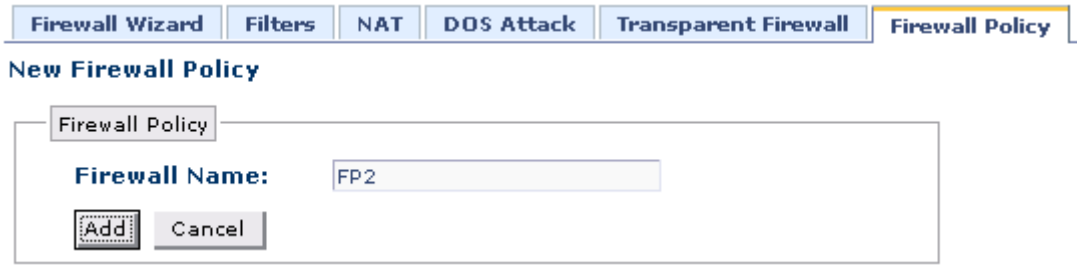


Figure 93: Firewall: Firewall Policy - New Firewall Policy

Step 2: Enter the firewall policy name in the **Firewall Name** field.

Step 3: Click **Add** to new firewall policy or click **Cancel** to cancel the operation.

ADDING RULE TO FIREWALL POLICY

Step 1: Select the firewall policy from the firewall list to which rule is to be configured.

Step 2: Select the firewall policy rule type: **DOS Attack Rules** or **Intrusion Rules**.

Step 3: Configure rule for selected rule type.

Adding DOS Attack Rule to the Firewall Policy

1. Select **DOS Attack Rules** radio button for configuring DOS attack rule to the firewall.
2. Fields to add new DOS Attack Rules is populated in the **DOS Attack Rule Configuration** table.

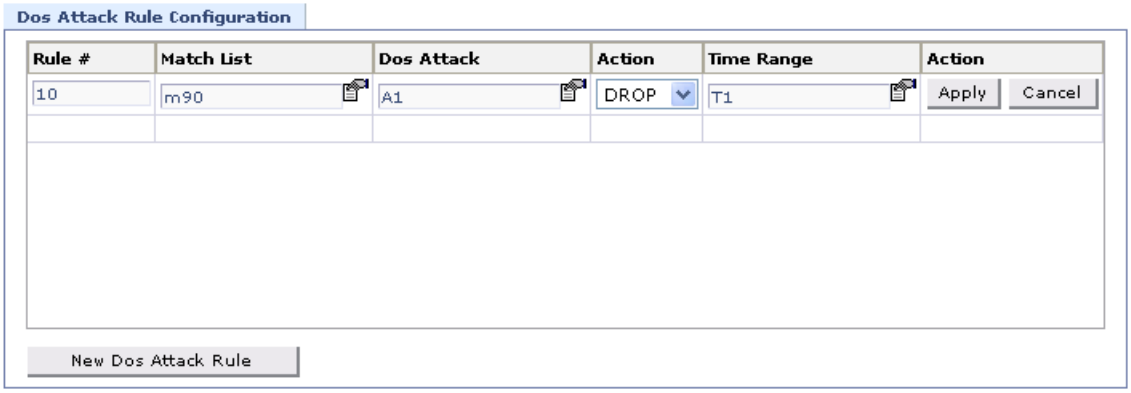


Figure 94: Firewall: Firewall Policy - Add New DOS Attack Rule

3. Enter rule number, select match-list, DOS attack policy, define action, and select the time range.
4. Click **Apply** to add new DOS Attack rule.
5. Add as many rules as required.

ADDING INTRUSION RULE TO THE FIREWALL POLICY

Note: You need to configure the Intrusion Prevention settings prior to adding intrusion rule to the firewall policy.

For more information on the procedure to configure intrusion prevention settings and view intrusion prevention configuration status, see "Intrusion Prevention" section.

1. Click **Intrusion Rules** radio button for configuring Intrusion rule to the firewall.
2. Fields to add new intrusion rule is populated in the **Intrusion Rule Configuration** table.

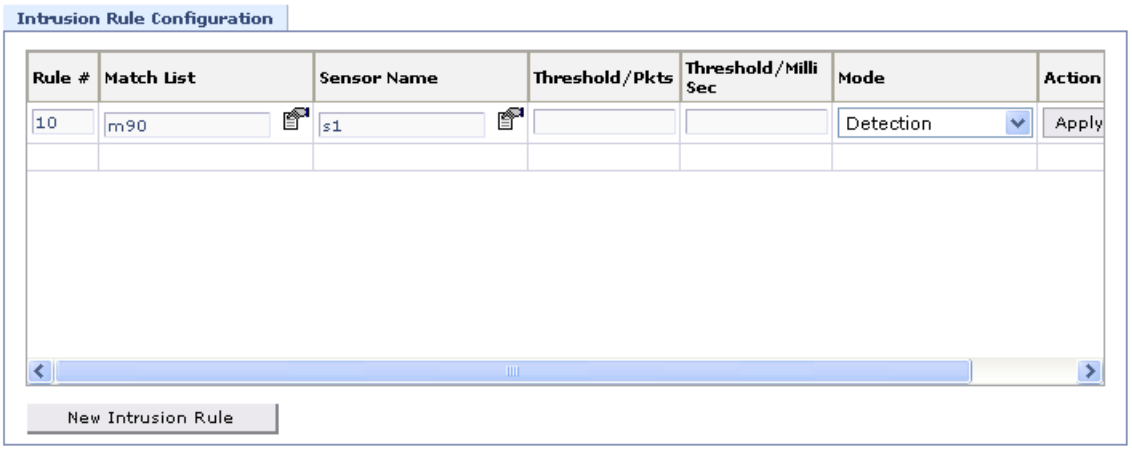


Figure 95: Firewall: Firewall Policy - Add New Intrusion Rule

3. Enter rule number, select match-list, sensor name, enter Threshold/Packets and Threshold/Milli Sec, and select mode.
4. Click **Apply** to add new intrusion rule.
5. Add as many rules as required.

ATTACH FIREWALL TO AN INTERFACE

Step 1: Select the firewall policy from the firewall list

Step 2: Click **Attach Interface** in the **Interface Bindings** table.

Fields to attach an interface is populated as shown below.

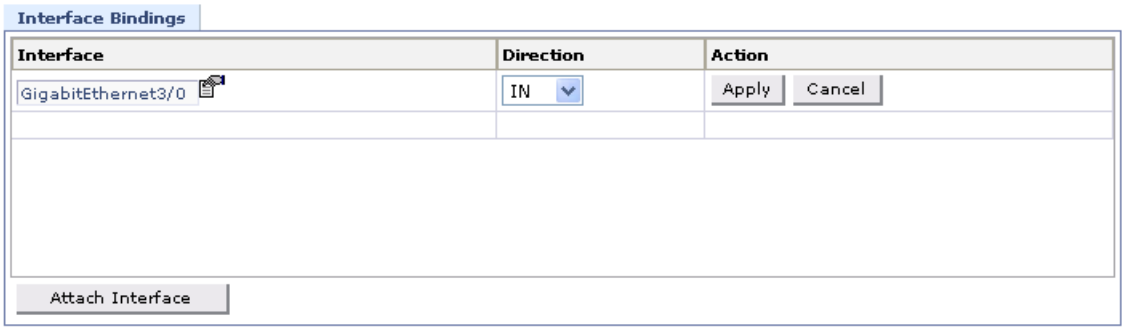


Figure 96: Firewall: Firewall Policy - Attach Interface

Step 3: Select the interface from the **Interface** list

Step 4: Select the direction **IN/OUT.**

Step 5: Click **Attach** to attach the selected interface to the firewall policy.

DELETING FIREWALL POLICY

1. Click **Delete** icon in the **Action** column against the Firewall Policy to be deleted.
2. Confirm at the prompt to delete the selected firewall policy.

Note: To delete the firewall policy, detach the firewall policy from the interface and/or disassociate the DOS attack policy or time range.

EDITING FIREWALL POLICY RULE

1. Select the firewall policy from the Firewall Policy Name list.

   Rules already configured (DOS Attack/Intrusion rules) for the selected firewall policy is displayed in **DOS Attack Rule/Intrusion Rule Configuration** table.
2. Click **Edit** icon in the **Action** column for the firewall policy rule to be edited.
3. Enter the new firewall policy rule parameters in the respective columns.
4. Click **Apply** to save the changes or **Cancel** to retain original parameters.

Deleting Firewall Policy Rule

1. Select the firewall policy from the Firewall Policy Name list.

   Rules already configured (DOS Attack/Intrusion rules) for the selected firewall policy is displayed in **DOS Attack Rule/Intrusion Rule Configuration** table.
2. Click **Delete** icon in the **Action** column for the firewall policy rule to be deleted.
3. Confirm at the prompt to delete the firewall Policy rule.

Detach Firewall Policy from an Interface

1. Select the firewall policy from the Firewall Policy Name list.

   Interfaces already configured for the selected firewall policy is displayed in the **Interface Bindings** table.
2. Click **Detach** icon in the **Action** column to detach firewall policy from the selected interface.
3. Confirm at the prompt to detach the firewall policy.

VPN IPSEC

This page allows you to configure IPsec policy using the IPSec Wizard.

The page also provides provision to also add/edit the IPsec VPN parameters like Preshared Keys, IKE Policy, and Transform Set.

IPSEC CONFIGURATION WIZARD

VPN (IPSec) Wizard allows you to configure VPN (IPSec) policies using VPN (IPSec) Profiles (Tunnel Interface only) or Crypto-map (other interfaces) in a few easy steps.

VPN (IPSec) Wizard configures the following:

- Creates Crypto-map or IPSec profiles with Tunnel Interface.
- For Crypto-map, creates VPN Peers, VPN Traffic to be tunneled using Match-lists and associate Interfaces.
- For IPsec Profiles, creates VPN Peers and associates IPSec Profiles to the created Tunnel Interfaces.
- IKE settings for configuring PFS, Lifetime, security proposals
- VPN (IPSec) settings for configuring PFS, Lifetime & transform set

VIEWING IPSEC WIZARD

Follow the procedure given below to view the **IPSEC** Wizard page.

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **VPN IPSec** sub-menu.

The **VPN IPSec** has four tabs: **IPSec Wizard**, **Preshared Keys**, **IKE Policy**, and **Transform Set**. By default, **IPSec Wizard** tab is selected and IPSec Wizard page is displayed in the center panel.

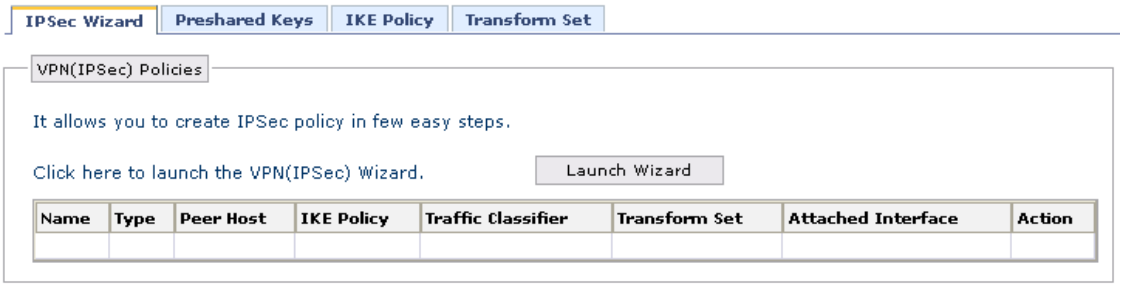


Figure 97: VPN IPSec: IPSec Wizard

CONFIGURE IPSEC POLICY USING THE WIZARD

Follow the procedure below to configure a IPSec Policy using the wizard.

Step 1: Click **Launch Wizard** in the **IPSec Wizard** page to create new IPSec Policy. The following page is displayed:

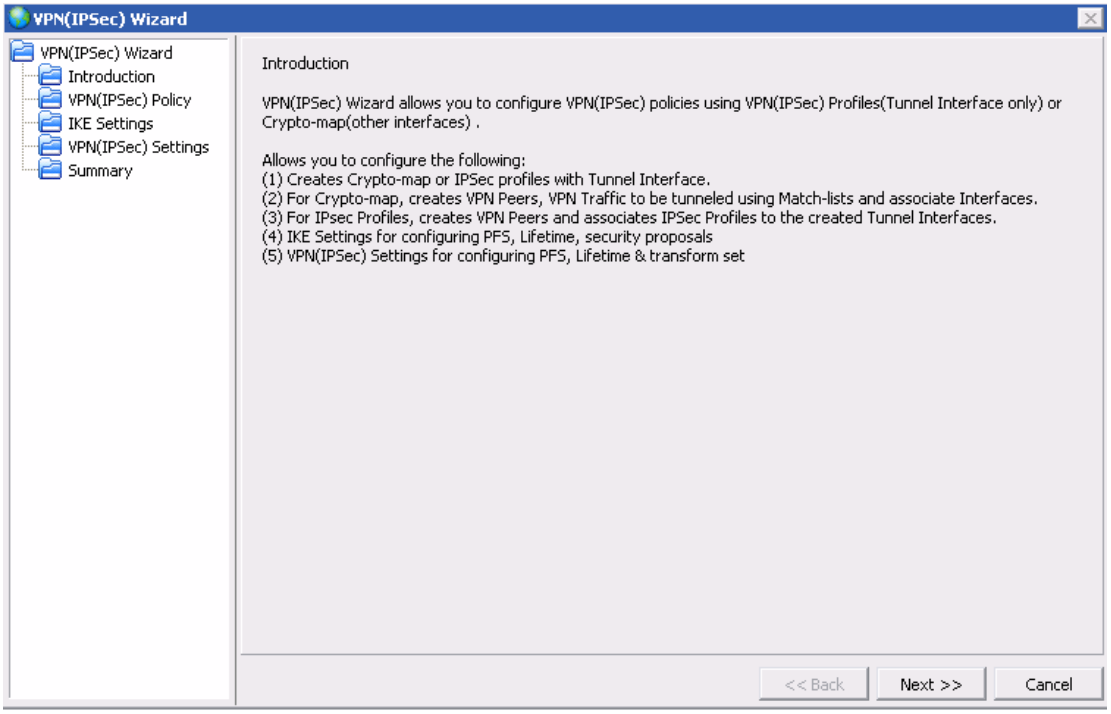


Figure 98: VPN IPSec: IPSec Wizard - Introduction

Step 2: Click **Next**. **VPN IPSec Policy** window is displayed. This window allows you to create Crypto-map or IPSec profiles with Tunnel Interface.

Create IPSec Profile with Tunnel Interface

1. By default, **IPSec-Profile** radio button is selected, and the parameters to configure IPSec Profile is displayed.

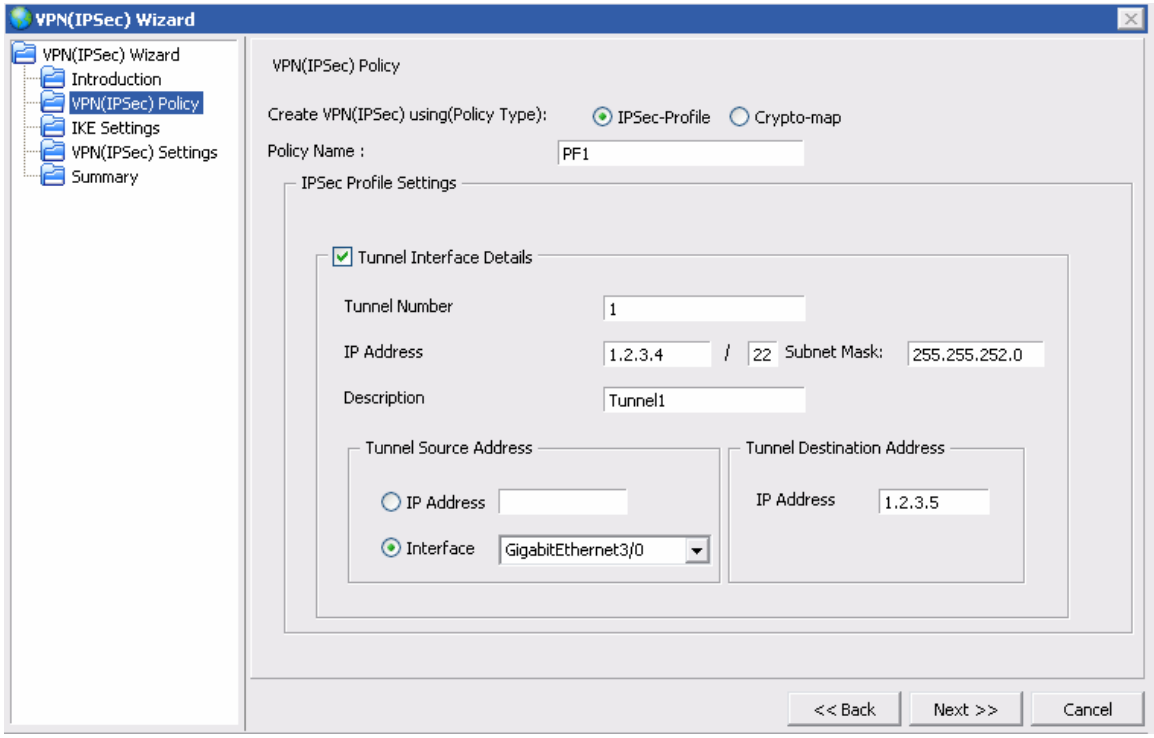


Figure 99: VPN IPSec: IPSec Wizard - Create IPSec Policy with IPSec Profile

2. Enter the IPsec Profile name in the **Policy Name** field.
3. **Tunnel Interface Details is optional.**

   By default, **Tunnel Interface Details** check box is enabled. Unselect the Tunnel Interface Details check box, and click **Next** to continue IPsec profile configuration.

   Or

   Configure a Tunnel interface.

   - Enter the number for the tunnel interface in the **Tunnel Number** field.
   - Enter the IP address and the subnet mask of the tunnel interface in the **IP Address** and **Subnet Mask** fields.
   - Enter the description for the tunnel in the **Description** field.
   - Configure the tunnel source and tunnel destination for the tunnel interface in the **Tunnel Source Address** box and **Tunnel Destination Address** box.
     i. Enter the source IP address of the tunnel interface in the **IP Address** field or select the interface that the tunnel will use from the **Interface** list.

Note: The source IP address of the tunnel must be of either a loopback interface or one of the physical interfaces. Ensure that the interface is reachable from the other end of the tunnel.

ii. Enter the destination IP address of the tunnel at the remote end in the **IP Address** field. This is the source interface from the point of view of the other end of the tunnel. Make sure that this address is reachable using the ping command; else, the tunnel will not be created properly.

Configure Crypto-map

1. Select **Crypto-map** radio button. Crypto-map settings is displayed.

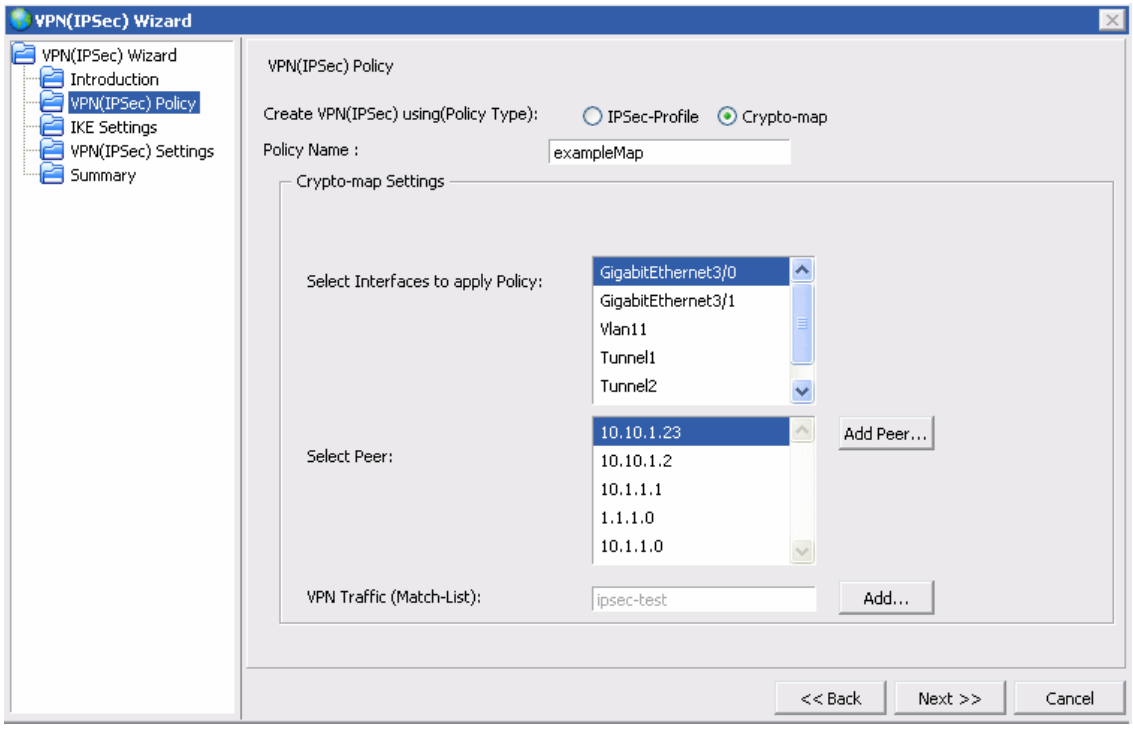


Figure 100: VPN IPSec: IPSec Wizard - Create IPSec Policy with Crypto-map

2. Enter the crypto-map name in the **Policy Name** field.
3. Configure the crypto-map settings.
   - Attach a crypto-map to an interface. **Select Interfaces to apply Policy** list displays the interfaces configured. Select the interface from the list.

     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.

- Attach a peer to a crypto-map. Click **Add Peer**. **Peer** pop-up window is displayed.

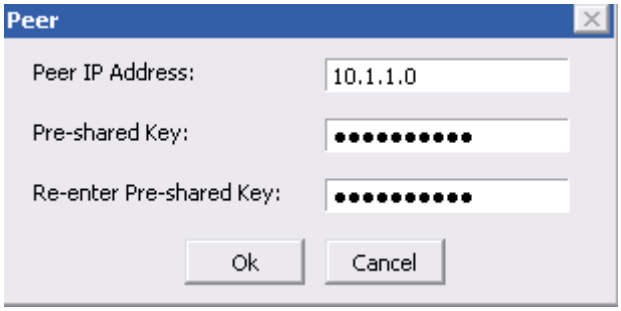


Figure 101: VPN IPSec: IPSec Wizard - Create IPSec Policy with Crypto-map - Add Peer

i. Enter the peer IP address in the **Peer IP Address** field.
ii. Enter the pre-shared key in the **Pre-Shared Key** field.
iii. Confirm the pre-shared key by entering it in the **Re-enter Pre-Shared Key** field.
iv. Click **OK**. The peer thus added is displayed in the **Select Peer** list.
v. Repeat the steps to add more peers.

- Attach a match-list to a crypto-map under **VPN Traffic (Match-list)** filed. You can either attach an exiting match-list or create a new match-list and attach it to the crypto-map. Click **Add**. **Create New** and **Attach Existing** options are displayed.

Create New Match-list

i. Select **Create New** option to configure new match-list. **Create Match-list** pop-up window is displayed.

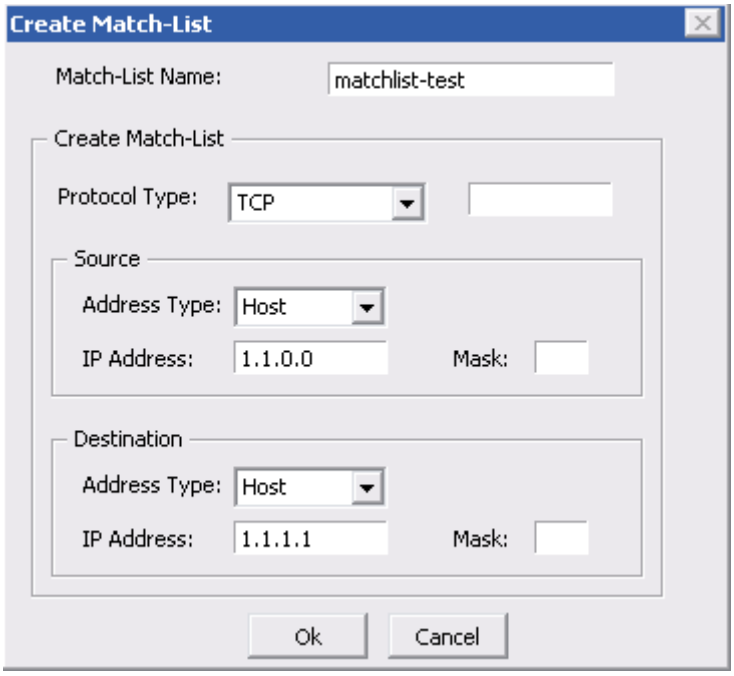


Figure 102: VPN IPSec: IPSec Wizard - Create IPSec Policy with Crypto-map - Create Match-list

ii. Enter the match-list name in the **Match-list Name** filed.

iii. Select any of the protocols from the **Protocol Type** drop down list.

iv. Enter the source information in the **Source** box. Select the address type from the **Address Type** drop-down list: **Host/Prefix.** Enter the source IP address for host, and enter the source address with prefix length for prefix.

v. Enter the source information in the **Destination** box. Select the address type from the **Address Type** drop-down list: **Host/Prefix.** Enter the source IP address for host, and enter the source address with prefix length for prefix.

vi. Click **OK**. The match-list thus created is displayed in the **VPN Traffic (Match-list)** field.

Attach Existing Match-list

i. Select **Attach Existing** option to attach an existing match-list to a crypto-map. **Select Match-list** pop-up window is displayed.

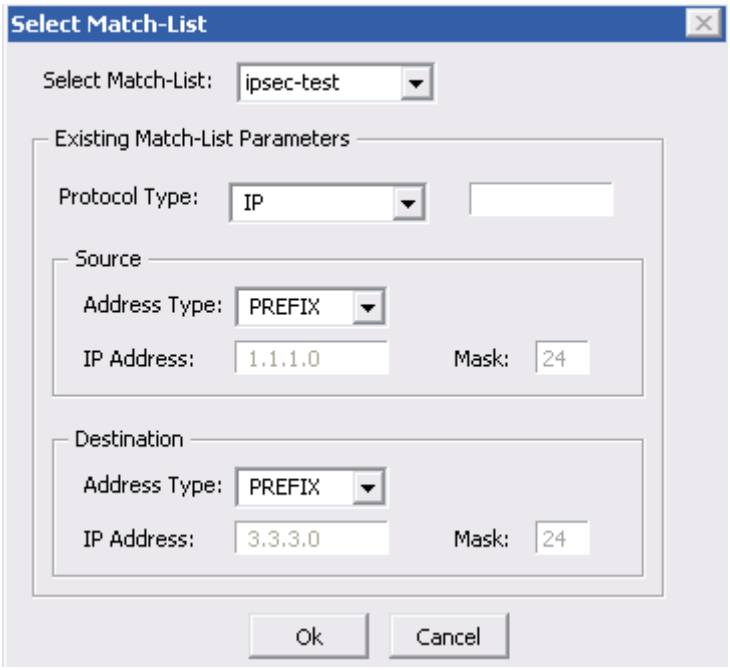


Figure 103: VPN IPSec: IPSec Wizard - Create IPSec Policy with Crypto-map - Select Match-list

i. Select **Match-list** drop-down list displays the match-lists already configured in the system. Select the required one from the drop-down list.

ii. The parameters configured for the selected match-list is displayed in the respective fields under **Existing Match-list Parameters**. None of these parameters are editable.

iii. Click **OK**. The match-list thus selected is displayed in the **VPN Traffic (Match-list)** field.

Step 3: Click **Next**. **IKE Settings** window is displayed. This window allows you to configure IKE policy, and IKE settings like PFS, Lifetime, security proposals.

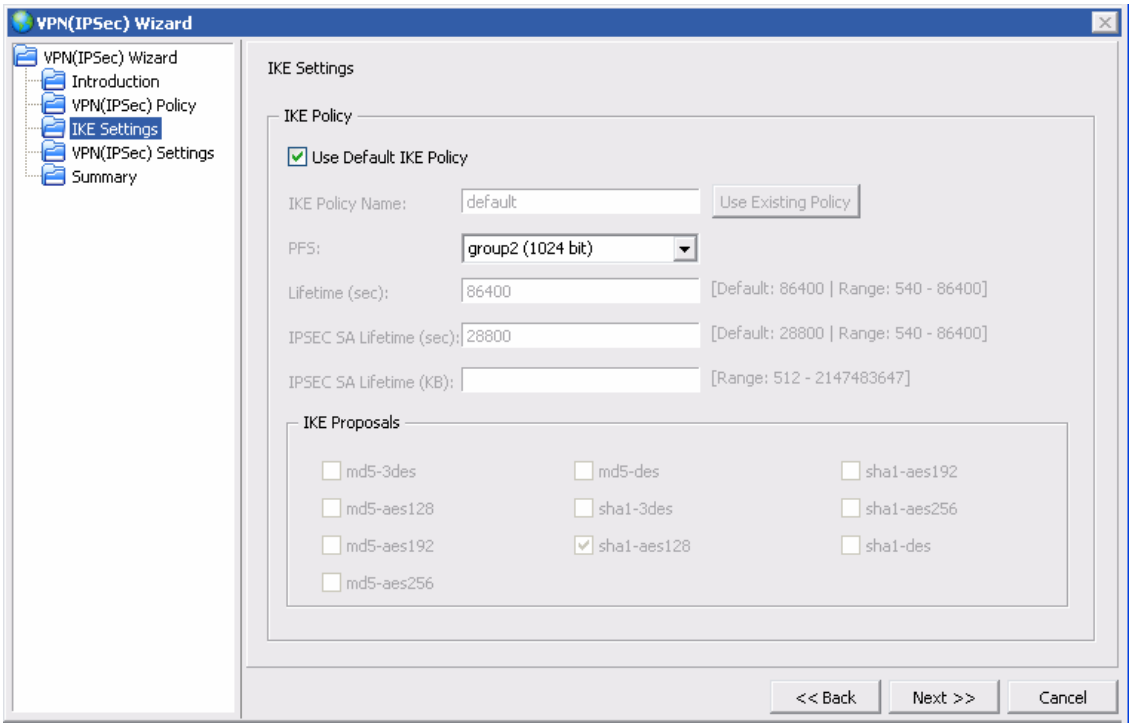


Figure 104: VPN IPSec: IPSec Wizard - IKE Settings

1. By default, **Use Default IKE Policy** check box is enabled.

   An IKE policy '**default**' is created in your system. If an IKE policy is not configured, the 'default' IKE policy is applied to the IPSec profile. Following are the default values for IKE policy '**default**':

   - Default Perfect Forward Secrecy (PFS) group in IKE policy: **pfs group2**
   - Default IKE lifetime in seconds: **86400**
   - Default IPsec security-association lifetime in seconds: **28800**
   - Default proposal in IKE policy: **sha1-aes128**

   Retain the default values or configure as required.

2. Configure IKE setting as required. To do the same, uncheck the **Use Default IKE Policy** check box.
   - Here you have two options: Configure a new IKE policy or use an already created IKE Policy.

     Configure New IKE Policy

     i. Enter the name for IKE policy in the **IKE Policy Name** field.

     ii. Select the predefined PFS group in **PFS** drop-down list.

     iii. Enter the lifetime for the IKE policy in **Lifetime (Sec)** field.

     iv. Enter the IPSec SA lifetime in the **IPSec SA Lifetime (Sec)** and **IPSec SA Lifetime (KB)** field.

v. Select the encryption algorithm in the **IKE Proposal** box. Maximum of four proposals can be associated with an IKE policy. The system prompts if more than four encryption algorithms are selected.

Use an Existing IKE Policy

i. Click **Use Existing Policy** against the IKE Policy name field to use the IKE policy already configured in the system. Following pop-up window is displayed:

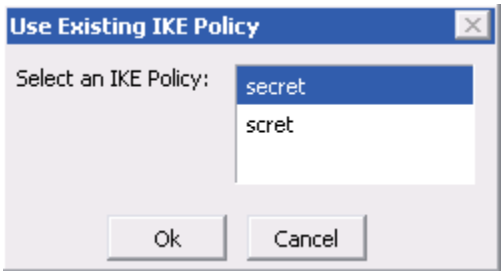


Figure 105: VPN IPSec: IPSec Wizard - IKE Settings - Use Existing IKE Policy

ii. **Select an IKE Policy** list displays the IKE policies already configured in the system. Select the required one from the list, and click **OK**. The selected IKE policy is displayed in the **IKE Policy Name** field.

iii. And the parameters configured for the selected IKE Policy is displayed in their respective fields. **These are not editable. Only IPSec SA Lifetime (KB) can be modified.**

Step 4: Click **Next**. **VPN (IPSec) Settings** window is displayed. This window allows you to configure VPN (IPSec) Settings like configuring PFS, Lifetime & transform set.

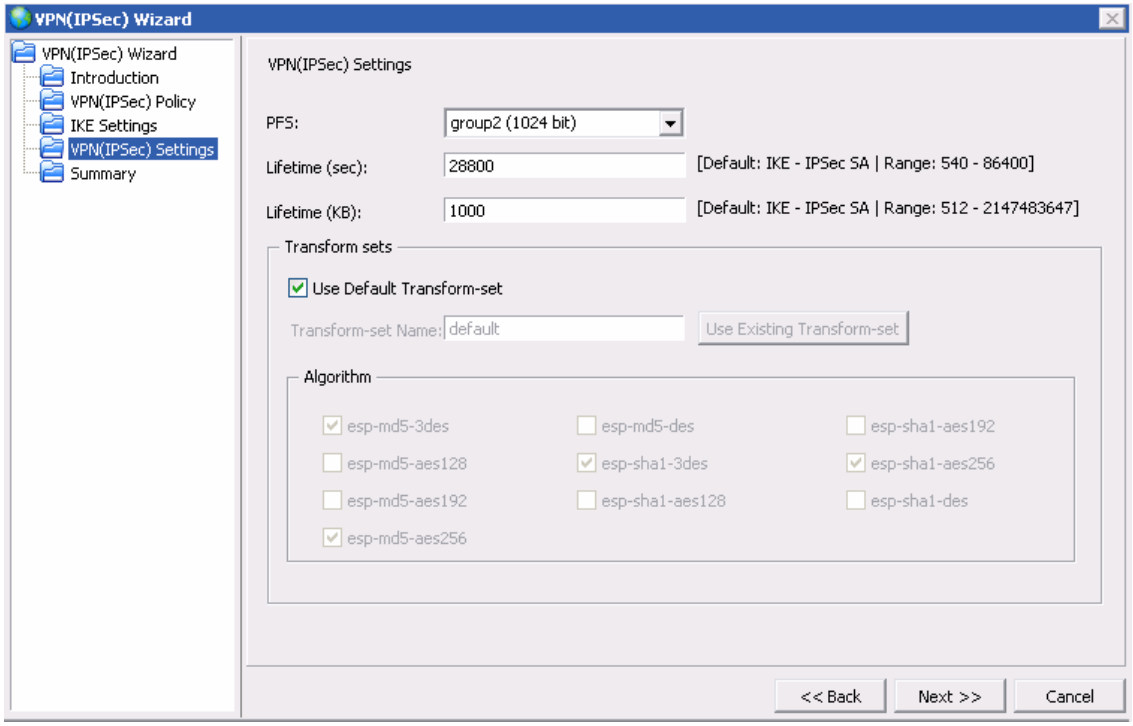


Figure 106: VPN IPSec: IPSec Wizard - VPN (IPSec) Settings

1. Select the predefined PFS group in **PFS** drop-down list. Default PFS group is group2 (1024 bit).
2. Enter the IPSec SA lifetime in the **Lifetime (Sec)** and **Lifetime (KB)** fields.The default lifetime for IPSec SA is 28800 seconds.
3. By default, **Use Default Transform-set** check box is enabled.

   A transform set '**default**' is created in your system. If a Transform-set is not configured, the 'default' Transform-set policy is applied to the IPSec profile. Following are the default values for transform-set '**default**':

   - esp-sha1-aes256
   - esp-sha1-3des
   - esp-md5-aes256
   - esp-md5-3des

   Retain the default values or configure as required.
4. Configure Transform-set as required. To do the same, unselect the **Use Default Transform-set** check box.
   - Here you have two options: Configure a new Transform-set or use an already created Transform-set.

Configure New Transform-set

i. Enter the name for Transform-set in the **Transform-set Name** field.

ii. Select the encapsulation under the **Algorithm** box. Select the required check box. A maximum of four encapsulations can be assigned for a transform set. The system prompts if more than four encapsulations are selected.

Use an Existing Transform-set

i. Click **Use Existing Transform-set** against the Transform-set name field to use the Transform-set already configured in the system. Following pop-up window is displayed:

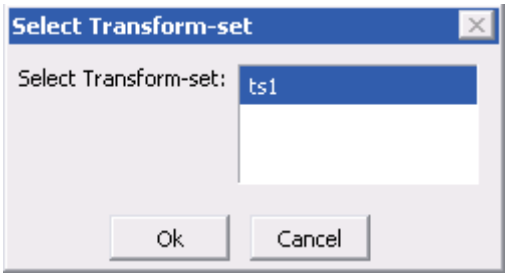


Figure 107: VPN IPSec: IPSec Wizard - IKE Settings - Select Existing Transform-set

ii. **Select Transform-set** list displays the Transform-set already configured in the system. Select the required one from the list, and click **OK**. The selected Transform-set is displayed in the **Transform-set Name** field.

iii. And the encapsulations configured for the selected Transform-set is displayed in the Algorithm box. **These are not editable.**

Step 5: Click **Next**. **Summary** window is displayed. Based on the IPSec policy type configured (Crypto-map or IPSec Profile using Tunnel interface), the Summary window displays the respective IPSec policy configuration.

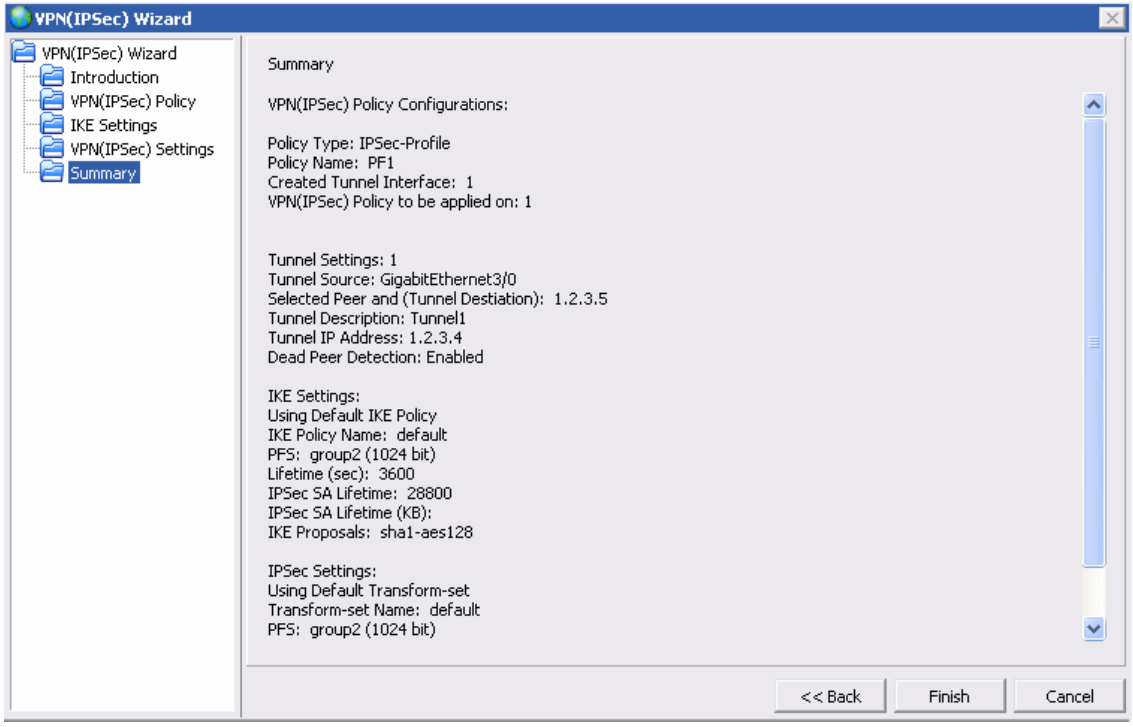


Figure 108: VPN IPSec: IPSec Wizard - Summary (IPSec Profile Policy Type)

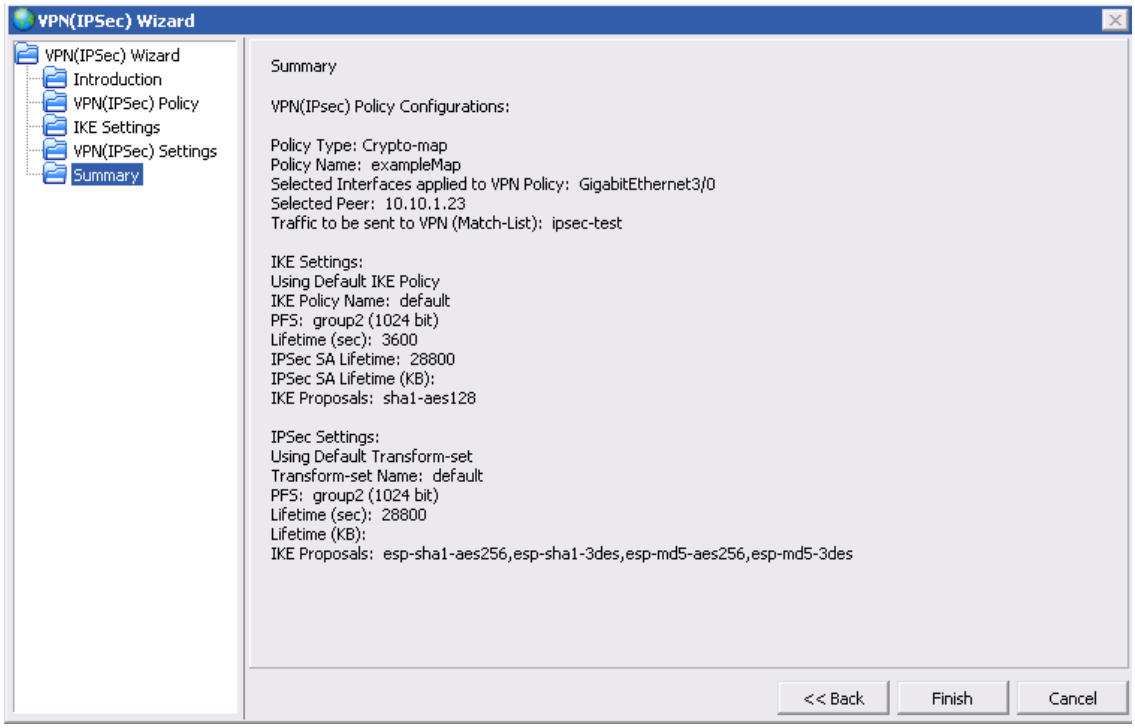


Figure 109: VPN IPSec: IPSec Wizard - Summary (Crypto-map Policy Type)

Step 6: Click **Finish** to save the configuration and generate the IPSec policy.

Step 7: A status bar is displayed showing the IPSec policy creation. Once the IPSec policy is configured successfully, a successful message is displayed.

The IPSec policy thus generated by the wizard is displayed in the **IPSec Wizard** tab as shown below.

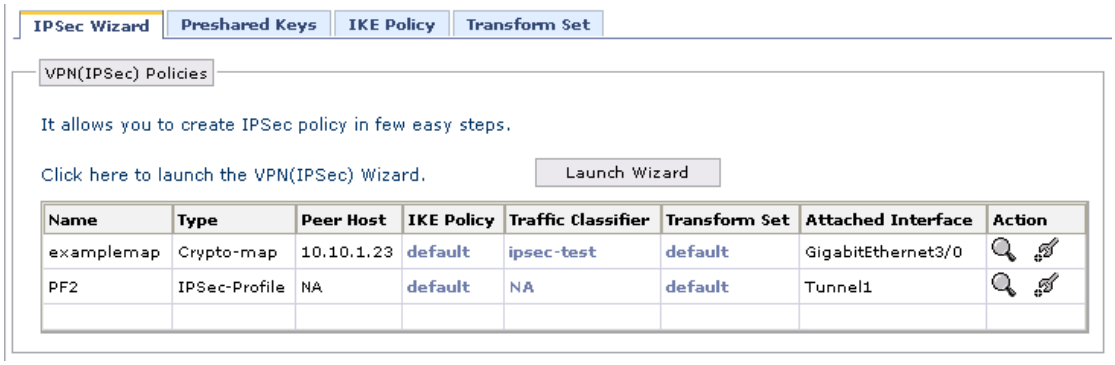


Figure 110: VPN IPSec: IPSec Wizard - IPSec Policy/ies Generated by the Wizard

The following information is displayed:

Table 19: VPN (IPSec) Policies Field Description

Field	Description
VPN (IPSEC) POLICIES	
Name	Name of IPSec policy.
Type	IPSec policy type configured (Crypto-map or IPSec Profile)
Peer Host	IP address of the peer host/remote host.
IKE Policy	IKE policy associated with the IPSec policy. Click on this to view the details of the IKE policy configured for the IPSec policy.
Traffic Classifier	Match-list associated with the IPSec policy. Click on this to view the details of the Match-list configured for the IPSec policy.

Field	Description
Transform Set	Transform set associated with the IPSec policy. Click on this to view the details of the Transform-set configured for the IPSec policy.
Attached Interface	Interface to which the IPSec policy is attached.
Action	Provides option to view, edit, or delete an IPSec policy.

EDIT IPSEC POLICY

The IPSec policy configured using the wizard can be edited/modified. Follow the procedure to edit the IPSec policy.

1. In the **VPN (IPSec) Policies** page, click **Edit** icon in the **Action** column against the IPSec policy to be edited.
2. **Edit IPSec Policy** page is displayed. This page displays the parameters configured for the selected IPSec policy. Modify the required parameters.

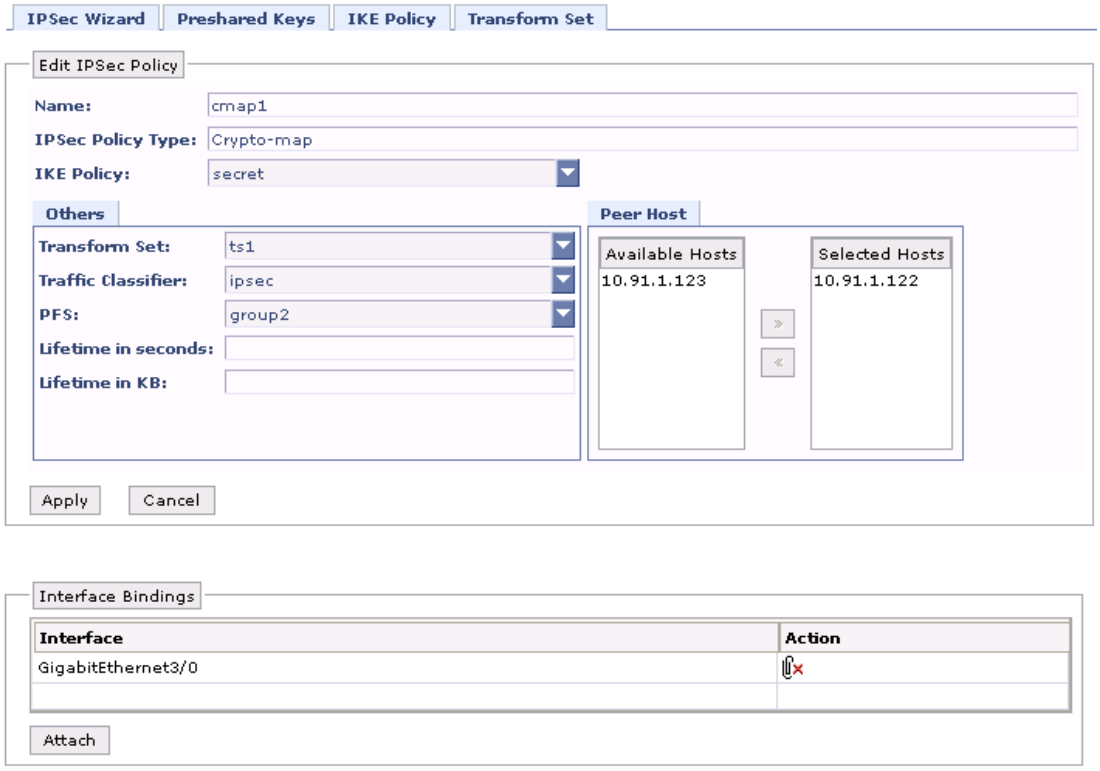


Figure 111: VPN IPSec: IPSec Wizard - Edit IPSec Policy

3. Modify the required parameters. Name and IPSec Policy Type fields cannot be modified.
4. Select IKE policy, transform set, traffic classifier (match-list), PFS group from the respective drop-down list.
5. Enter lifetime for the IPSec policy in seconds and KB in **Lifetime in seconds** and **Lifetime in KB** field.
6. Peer Host displays the Peer added to the IPSec policy. Modify the same if required under **Peer Host**.
   - Select the Peer Host to be added to the IPSec policy from the **Available Hosts** column and click the '**>>**' button to move it to the **Selected Hosts** column.
   - Select as many peer hosts from the Available Hosts column and move it to the Selected Hosts column.

   The Available Hosts column lists only the hosts to which preshared key is configured and the Selected Hosts lists the remote/peer hosts selected.
7. Click **Apply** to save the IPSec policy parameters, or **Cancel** return to VPN (IPSec) Policies page.
8. Interface Bindings table displays the interfaces to which the IPSec policy is attached. Modify if required.
   - Click **Attach** in the **Interface Bindings** table. This populates fields to select the interface.
   - Select the interface from the list of interfaces to which you want to attach the IPSec policy.

     The same IPSec policy can be assigned to multiple interfaces, and the same interface can be attached to multiple IPSec policies.
   - Click **Apply** to attach the interface to the IPSec policy.
9. Click **Detach** icon in the **Action** column to detach the interface from the IPSec policy.
10. Confirm at the prompt to detach the interface from the IPSec policy.

DELETING IPSEC POLICY

1. In the **VPN (IPSec) Policies** page, click **Delete** icon in the **Action** column against the IPSec policy to be deleted.
2. Confirm at the prompt to delete the IPSec policy.

Note: An IPSec policy assigned to an interface cannot be deleted. To delete an IPSec policy associated with an interface, disassociate the IPSec policy from the interface and then delete.

VIEW IPSEC POLICY DETAILS

1. Click on the **View Details** icon in the **Action** column against the IPSec policy whose details are to be viewed.
2. A pop-up window displays the IKE Policy, Peer Host, Traffic Classifier, Transform Set, PFS, Lifetime in Seconds and KB details for the selected IPSec policy as shown below:

Figure 112: VPN IPSec: IPSec Wizard - View IPSec Policy Details

PRESHARED KEYS

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.

This page allows you to add/edit preshared key for IPSec policy.

VIEWING PRESHARED KEYS

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **VPN IPSec** sub-menu.

The **VPN IPSec** has four tabs: **IPSec Wizard**, **Preshared Keys**, **IKE Policy**, and **Transform Set**.

Select **Preshared Key** tab. **Preshared Key** page is displayed in the center panel.

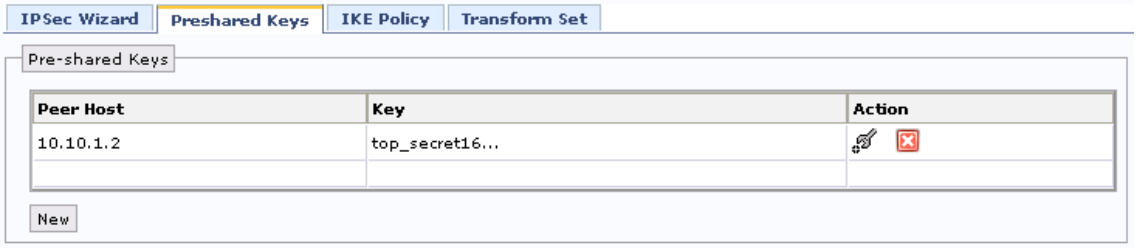


Figure 113: VPN IPSec: Preshared Keys

The table below provides field description for Preshared Keys page.

Table 20: Preshared Keys Field Description

Field	Description
PRE-SHARED KEYS	
Peer Host	IP address of the peer
Key	Preshared key.
Action	Provides option to edit or delete a key.
New	Configure new preshared key.

ASSIGN PRESHARED KEYS

Follow the procedure below to assign preshared key to a host.

Step 1: Click **New** in the **Preshared Keys** page to assign preshared key to a host. The fields to add preshared keys are populated in the **Pre-shared Keys** table as shown below.

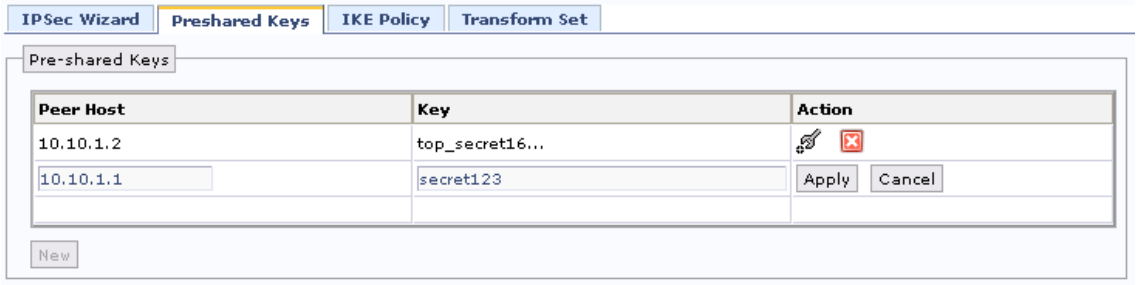


Figure 114: IPSec VPN: Assign Preshared Keys

Step 2: Enter IP address of the peer host in the **Peer Host** field.

Step 3: Enter the preshared key in the **Key** field.

Currently, the preshared-key length is restricted to 128 characters, and the minimum length is 8 characters.

The same preshared key can be assigned to multiple hosts; however, a host cannot have different preshared keys.

Step 4: Click **Apply** to create a new preshared key.

EDIT PRESHARED KEYS

1. Click **Edit** icon in the **Action** column against the key to be edited.
2. Enter the new preshared key in the **Key** column. Peer Host cannot be edited.
3. Click **Apply** to save changes, or **Cancel** to retain the original key.

DELETING PRESHARED KEYS

1. Click **Delete** icon in the **Action** column against the key you want to delete.
2. Confirm at the prompt to delete the key assigned to a host.

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, use of 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.

This page allows you to create IKE policy.

VIEWING IKE POLICY

Follow the procedure below to view IKE Policy page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **IPSec VPN** sub-menu.

The **VPN IPSec** has four tabs: **IPSec Wizard**, **Preshared Keys**, **IKE Policy**, and **Transform Set**.

Select **IKE Policy** tab. **IKE Policy** page is displayed in the center panel.

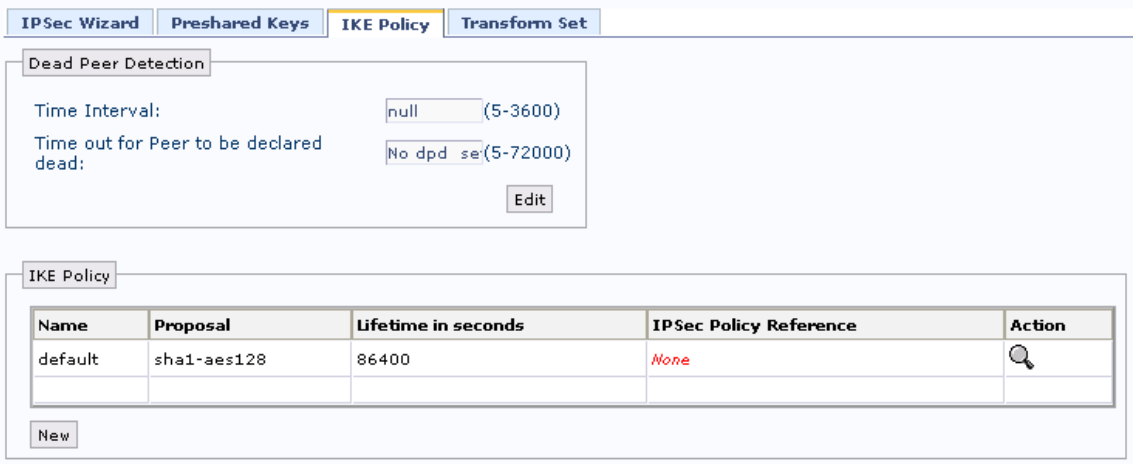


Figure 115: VPN IPSec: IKE Policy

The table below provides field description for IKE Policy page.

Table 21: IKE Policy Field Description

Field	Description
IKE POLICY	
Name	Name of the IKE policy.
Proposal	Encryption algorithm to be used.
Lifetime in seconds	Lifetime of the policy, in seconds.
IPSec Policy Reference	Lists IPSec policy/policies to which the particular IKE policy is attached.
Action	Provides option to edit or delete a IKE policy.
New	Create new/edit IKE policy.

CONFIGURE 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.

Follow the procedure below to configure DPD.

Step 1: Configure the DPD values in the IKE Policy page under Dead Peer Detection box.

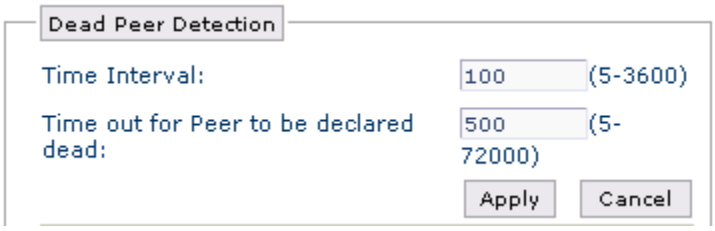


Figure 116: VPN IPSec: Dead Peer Detection

Step 2: Click **Edit** to enter the DPD values.

Step 3: Enter the interval in seconds for which the keep-alive messages will be sent in the Time Interval field.

Step 4: Enter the time out in seconds after which the peer will be declared to be dead in the **Time out for Peer to be declared dead** field.

Step 5: Click **Apply** to save the DPD values or click **Cancel** to cancel the operation.

CREATING NEW IKE POLICY

By default, an IKE policy '**default**' is created in your system, and cannot be edited or deleted.

Follow the procedure below to create a new IKE Policy.

Step 1: Click **New** in the **IKE Policy** page to create a new IKE policy.

New IKE Policy page is displayed.

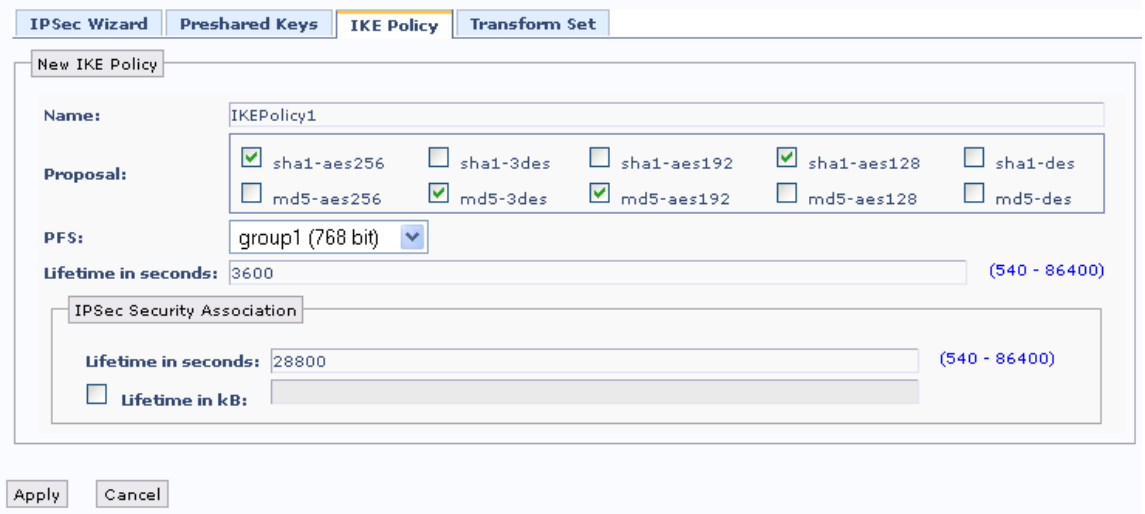


Figure 117: VPN IPSec: New IKE Policy

Step 2: Enter the name for IKE policy in **Name** field.

IKE policy name can be any alphanumeric name not exceeding 128 characters.

Step 3: Select the encryption algorithm in the **Proposal** field.

The default algorithm is sha1-aes128. Maximum of four proposals can be associated with an IKE policy. The system prompts if more than four encryption algorithms are selected.

Step 4: Select the predefined Perfect Forward Secrecy (PFS) group in **PFS** drop-down list.

Default PFS group is group2 (1024 bit).

Step 5: Set lifetime for the IKE policy in **Lifetime in Seconds** field in the range of 540 - 86400 seconds. The default lifetime for IKE is 86400 seconds.

Step 6: Set IPSec SA lifetime in the **IPSec Security Association** box.

- Enter the lifetime for IPSec SA in **Lifetime in seconds** field.

  The default lifetime for IPSec SA is 28800 seconds.
- Select the **Lifetime in KB** check box to enter lifetime of IPSec SA in kilobyte (KB).

When both lifetime in kilobytes and lifetime in seconds are set, renegotiation of new security associations are triggered depending on which lifetime expires first. When rekeying happens, both lifetimes get reset.

Step 7: Click **Apply** to add new IKE policy, or **Cancel** return to IKE Policy page.

EDITING IKE POLICY

1. Click on the **Edit** icon in the **Action** column against the IKE policy you want to edit.
2. **Edit IKE Policy** page is displayed.
3. Edit the IKE policy settings.Name field cannot be edited.
4. Click **Apply** to save changes or **Cancel** to retain the original values.

DELETING IKE POLICY

1. Click **Delete** icon in the **Action** column against the IKE policy you want to delete.
2. Confirm at the prompt to delete the IKE policy.

Note: An IKE policy associated with any IPSec policy cannot be deleted. To delete an IKE policy associated with an IPSec policy, either disassociate that IKE policy from the IPSec policy, or delete the IPSec policy.

VIEW IKE POLICY DETAILS

1. Click on the **View Details** icon in the **Action** column for the IKE policy which you want to view the details.
2. A pop up window displays the Proposal, PFS, Lifetime, IP Security Association details for the selected IKE policy as shown below:

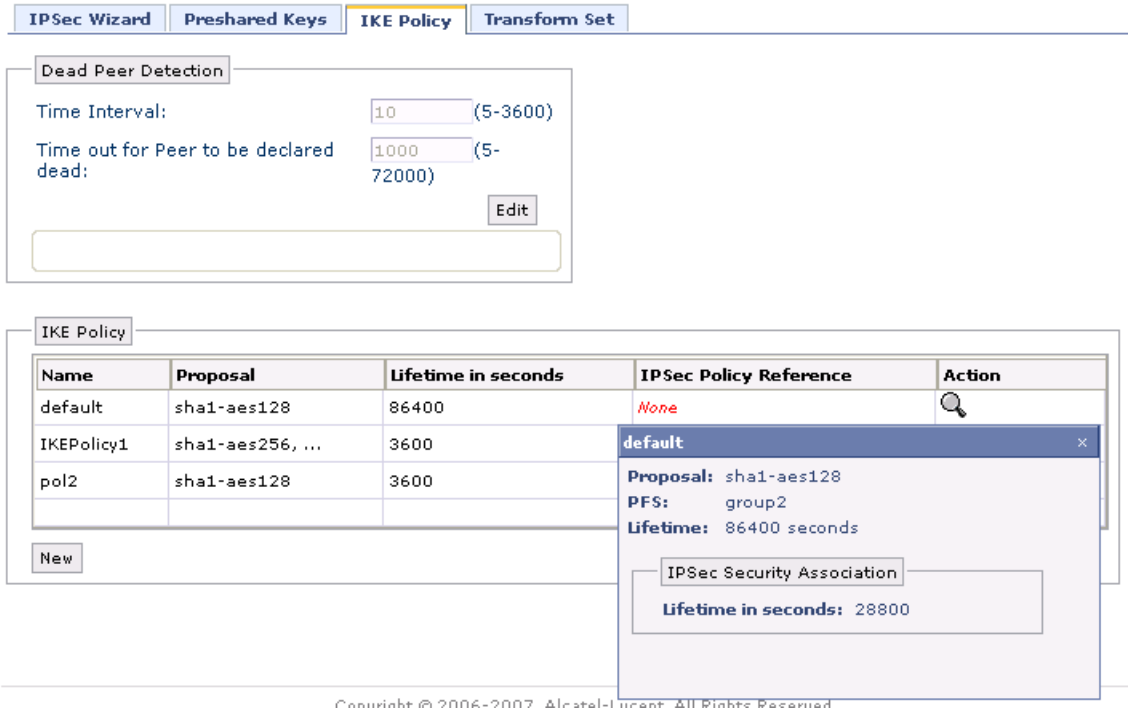


Figure 118: VPN IPSec: View IKE Policy Details

TRANSFORM SET

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.

This page allows you to add/edit transform sets.

VIEWING TRANSFORM SET

Follow the procedure below to view Transform Sets page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **VPN IPSec** sub-menu.

The **VPN IPSec** has four tabs: **IPSec Wizard**, **Preshared Keys**, **IKE Policy**, and **Transform Set**.

Select **Transform Set** tab. **Transform Sets** page is displayed in the center panel.

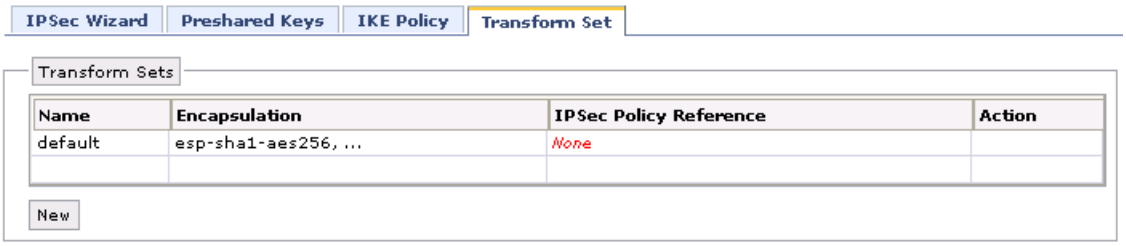


Figure 119: VPN IPSec: Transform Sets

The table below provides description for Transform Sets page.

Table 22: Transform Set Field Description

Field	Description
TRANSFORM SETS	
Name	Name of the transform set.
Encapsulation	Encapsulation set for the transform set.
IPSec Policy Reference	Lists IPSec policy/policies to which the particular IKE policy is attached.
Action	Provides option to edit and/or delete a transform set.
New	Create new transform set.

CREATING TRANSFORM SET

By default, a transform set '**default**' is created in your system, and cannot be edited or deleted.

Follow the procedure below to create a new transform set.

Step 1: Click **New** in the **Transform Sets** page to create a new transform set.

The fields to add name and encapsulation for transform set are populated.

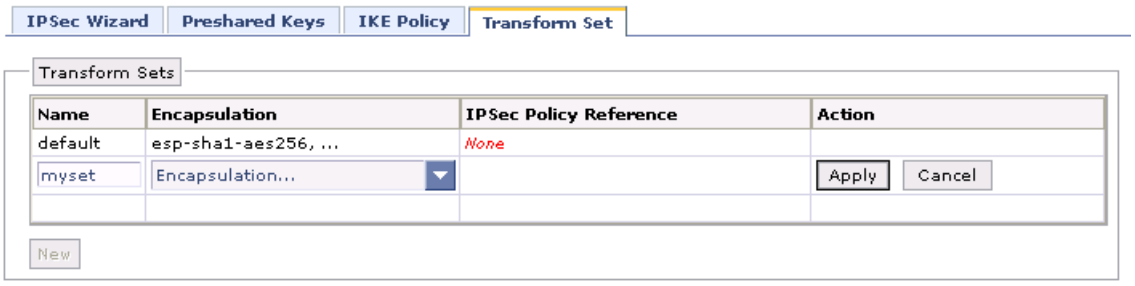


Figure 120: VPN IPSec: New Transform Set

Step 2: Enter the name for the transform set.

The Transform Set name can be any alphanumeric name not exceeding 128 characters.

Step 3: Select the encapsulation.

The default encapsulation is esp-sha1-aes128. A maximum of four encapsulations can be assigned for a transform set. The system prompts if more than four encapsulations are selected.

Step 4: Click **Apply** to add new transform set, or **Cancel** return to transform set page.

EDITING TRANSFORM SET

1. Click on the **Edit** icon in the **Action** column against the transform set you want to edit.
2. Change the encapsulation for transform set. Name field cannot be edited.
3. Click **Apply** to save changes or **Cancel** to retain the original values.

DELETING TRANSFORM SET

1. Click **Delete** icon in the **Action** column against the transform set you want to delete.
2. Confirm at the prompt to delete the transform set.

Note: A transform set associated with any IPSec policy cannot be deleted. To delete a transform set associated with an IPSec policy, either disassociate that transform set from the IPSec policy, or delete the IPSec policy.

VRRP

Virtual Routing Redundancy Protocol (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 gateway routers.

VRRP specifies an election protocol that dynamically assigns responsibility for 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 dynamic fail-over in the forwarding responsibility should the Master become 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.

VRRP is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backup in case of the failure of the virtual router master.

The Virtual Router Redundancy protocol 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 can be configured only on multi-access interfaces like Ethernet. VRRP is supported only on Gigabit-Ethernet interface on the OA-700 system. Maximum of 8 VRRP groups is configurable on an Interface.

Virtual Router Redundancy Protocol 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.

VIEWING VRRP

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **VRRP** sub-menu. **Virtual Routing Redundancy Protocol (VRRP) Groups** page is displayed in the center panel.

This page allows you to view the details for all the VRRP groups configured on the interfaces. It also provides an option to configure new groups, edit/delete the configured VRRP groups.

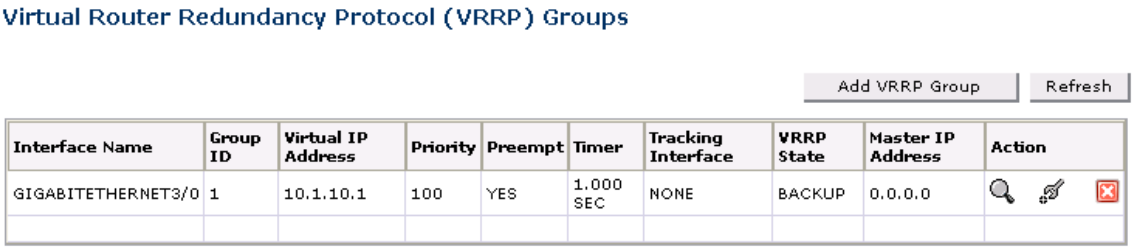


Figure 121: Virtual Routing Redundancy Protocol (VRRP) Groups

The table below provides field description for VRRP page.

Table 23: VRRP Field Description

Field	Description
VRRP	
Interface Name	Interface on which VRRP is configured
Group ID	Group ID configured for the VRRP group.
Virtual IP Address	The virtual IP address configured for the VRRP
Priority	The priority set for the router for a specific VRRP group.
Preempt	Pre-emption mode: enabled or disabled
Timer	The interval value set between sending successive advertisements by the master virtual router in a group. (Seconds/Milliseconds)
Tracking Interface	Interface tracked for the VRRP group OR Displays if the Track on Interface Mode is enabled or disabled

Field	Description
VRRP State	Indicates whether the current router is a Master / Slave in its VRRP group. (Master router acts as a default gateway for receiving or transmitting packets for a network. The backup virtual routers are referred to as slaves.)
Master IP Address	The interface IP address configured for the virtual master router.
Action	Provides an option to view master router details, and edit/delete the VRRP Group.

CONFIGURE VRRP GROUP

Follow the procedure below to configure VRRP group.

Step 1: From the **VRRP Groups** page, click **Add VRRP Group**.

Step 2: VRRP Group Configuration page is displayed.

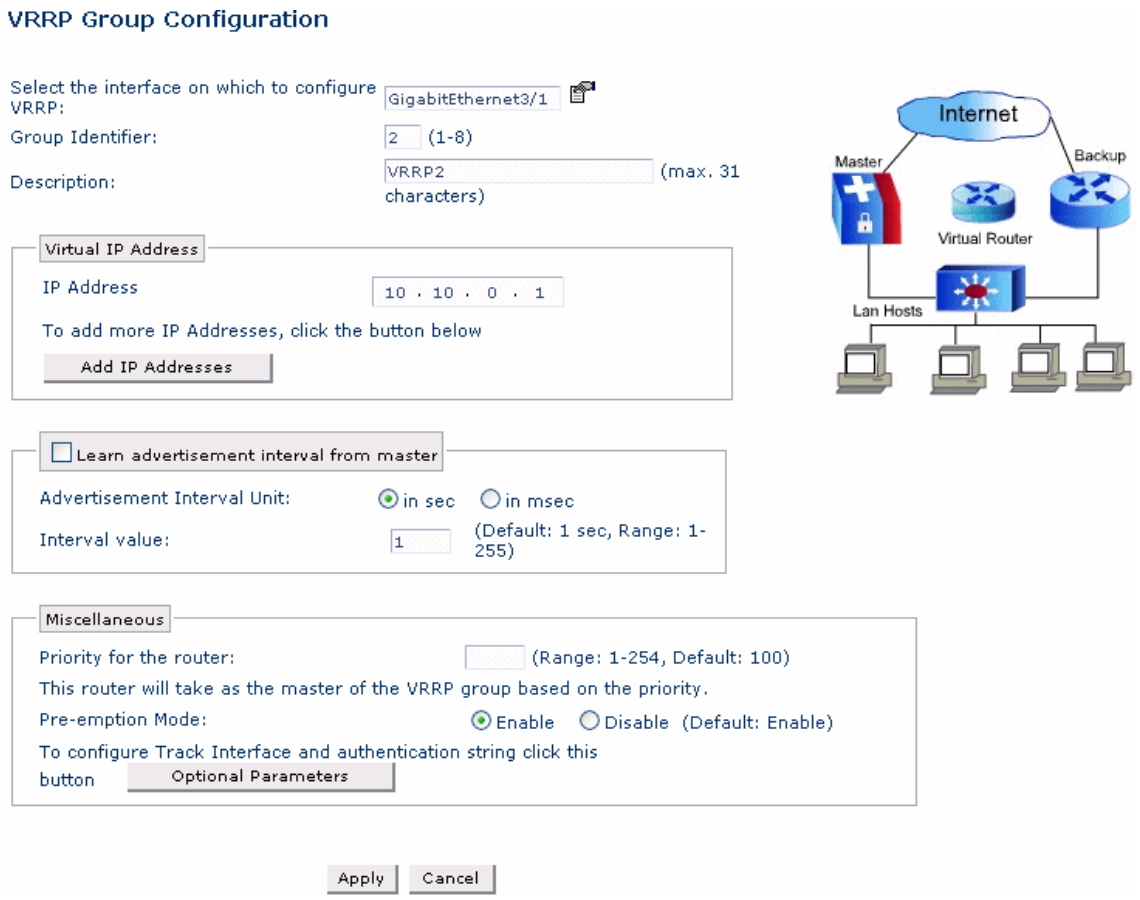


Figure 122: VRRP Group Configuration

Step 3: VRRP is configured on an interface. Hence, first select an interface on which VRRP is to be configured. Note that operational state of the interface must be up.

Select the interface on which VRRP is to be configured from the list.

Step 4: Enter the group ID in the **Group Identifier** field. This is in the range 1-8.

Step 5: Enter the description for the VRRP group in the **Description** field.

Step 6: Enter the Virtual IP address parameters in the **Virtual IP Address** table.

Note: The IP address must be unique across the system. That is, the IP address used for a VRRP group cannot be used as interface address (primary or secondary) on any interface except on the interface on which the group is getting configured and it cannot be used as the group address for any other group on the same interface or on any other interface.

- Enter the primary IP address in the **IP Address** field.
- To add more IP addresses (Secondary IP address), click **Add IP Addresses**. **Secondary Virtual IP Address** pop up window is displayed:

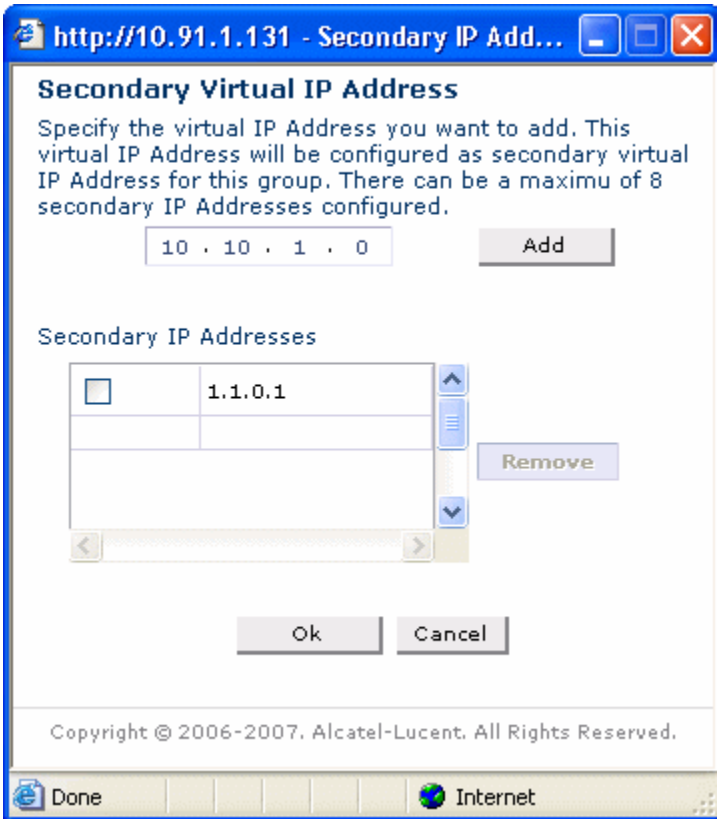


Figure 123: VRRP Group Configuration - Secondary Virtual IP Address

- Specify the virtual IP Address you want to add in the field, and click **Add**. The addresses added are listed in the Secondary IP Addresses box.

  This virtual IP Address will be configured as the secondary virtual IP Address for the group being created. **There can be a maximum of 8 secondary IP Addresses configured on an interface.**
- If you wish to remove the addresses from the list, select the check box against IP address/es to be removed, click **Remove**. The IP address/es is removed from the list.
- Click **OK** to add the secondary IP address/s click **Cancel** to cancel the operation.

Step 7: Set the advertisement interval for the VRRP group.

- Select the **Learn advertisement interval from Master** check box to configure the backup virtual router to learn the advertisement interval used by the master virtual router.

  When the above check box is selected, the **millisec** radio button is disabled as Learning and Advertisement millisecond timers are mutually exclusive. Learning cannot be enabled when millisecond timers are enabled and vice versa.
- Select the **Advertisement Interval Unit** option: **In Sec/In Msec** radio button.
- Enter the interval value in the **Interval Value** field. This sets the interval between sending successive advertisements by the master virtual router in a group.
  i. If you have selected **In Sec** radio button, enter the interval value in seconds. The valid time range for an advertisement packet is between 1 and 255 seconds with the default being 1 (one) second.
  ii. If you have selected In **MSec** radio button, enter the interval value in milliseconds. The valid time range for an advertisement packet is between 50 and 999.

Step 8: Configure the VRRP parameters like Priority, Pre-empt, interface tracking and authentication string in the **Miscellaneous** table.

- Enter the priority for the router in the **Priority for the router** field. The valid range for the priority range is between 1 and 254 with the default being 100. This router will take as the master of the VRRP group based on the priority.
- Enable or disable the **Pre-emption Mode** by selecting **Enable/Disable** radio button. By default, pre-emption is enabled.
  i. Enable option enables the pre-empt mode. By enabling pre-empt, the configured router takes over as the master of a group if it has a higher priority than the existing master virtual router.
  ii. Disabling the pre-empt mode disables the pre-emption of the VRRP group.

- Configure track Interface and set the authentication option for a virtual router.

  To configure track interface and set authentication option, click **Optional Parameters**. **VRRP Optional Parameters** pop up window is displayed.

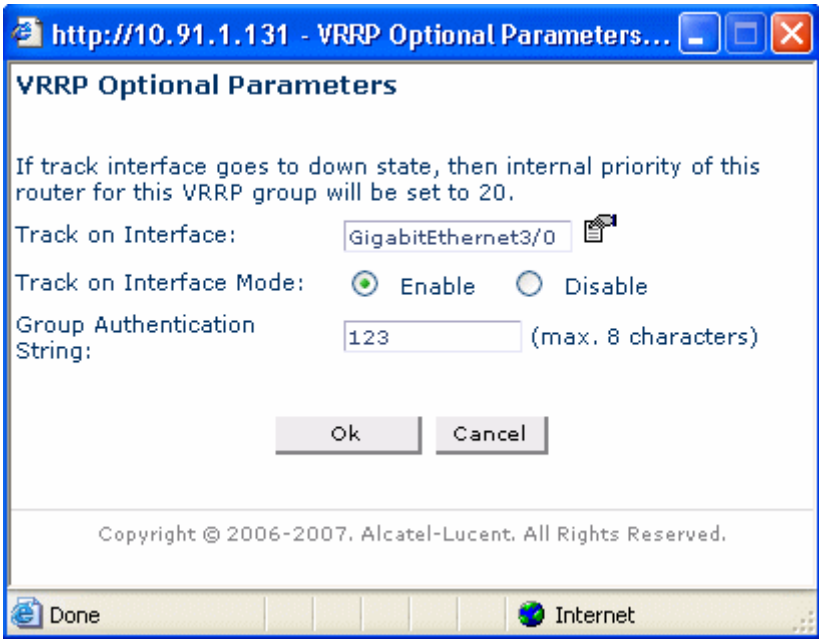


Figure 124: VRRP Group Configuration - VRRP Optional Parameters

i. Select the interface to be tracked for the VRRP group from the **Track on Interface** list.

ii. Enable of disable the **Track on Interface Mode** by selecting **Enable/Disable** radio button.

- Enabling the track on interface mode enables the interface to be tracked for the VRRP group. **The priority of the group is lowered when the tracked interface state changes to down.**
- Disabling the track on interface mode removes tracking of the interface.

iii. Set the authentication sting for the VRRP in the **Group Authentication** field. OA-700 supports null authentication and plain-text authentication. Maximum of 8 characters are allowed in the authentication string.

iv. Click **OK** to configure the track interface and authentication string for the VRRP or click **Cancel** to cancel the operation.

Step 9: Once you have entered the required configuration values, click **Apply** to create a new VRRP Group or click **Cancel** to cancel the operation.

VIEW MASTER ROUTER DETAILS

Master Router Details pop up window displays the details for the master for that VRRP group.

1. Click **View Master Details** icon in the **Action** column whose master router details is to be viewed.
2. Master Router Details pop up window displays the IP Address, Priority, Advertisement Interval, and Down Interval values for the selected interface in a table as shown below:

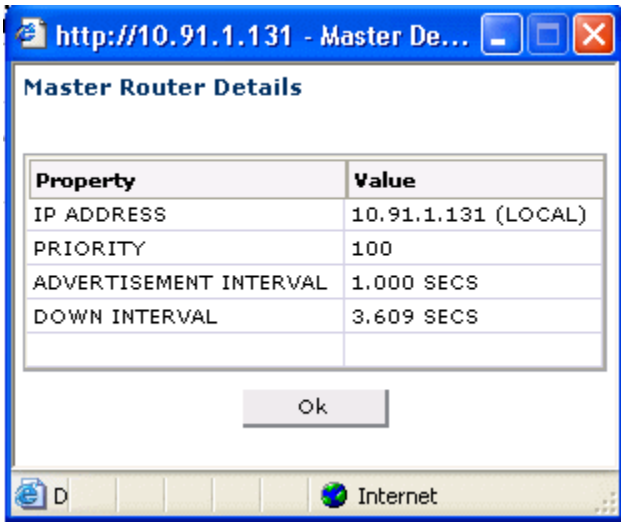


Figure 125: VRRP Group Configuration - View Master Router Details

EDIT VRRP CONFIGURATION

1. Click **Edit** icon in the **Action** column against the interface whose VRRP configuration is to be edited. VRRP Group configuration for the interface is displayed.
2. Make necessary changes in the respective fields. Interface and the Group ID fields cannot be hi edited.
3. Click **Apply** to save changes, or **Cancel** to retain the original configuration.

DELETING VRRP GROUP

1. Click **Delete** icon in the **Action** column for the interface whose VRRP Group is to be deleted.
2. Confirm at the prompt to delete the VRRP group.

INTRUSION PREVENTION

Intrusion Prevention is a network security system designed to identify intrusive or malicious behavior via monitoring of network activity. The IPS identifies suspicious patterns that may indicate an attempt to attack, break in, or otherwise compromise a system. An IPS can be network based or host based, passive or reactive, and can rely on either misuse detection or anomaly detection.

OA-700 supports Snort engine for IPS functionality.

This page provides the procedure to configure intrusion prevention settings and view intrusion prevention configuration status.

This page allows you to:

- View IPS configuration Status
- Set IPS Global Settings
- Configure Signature Policies
- Configure Sensors
- View Alerts and Reports
- View Rule File

STATUS

This page allows viewing and rebuilding the signature database. This also allows to rollback to previous versions of signature database.

VIEWING STATUS

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Intrusion Prevention** sub-menu.

The **Intrusion Prevention** menu has **six** tabs: **Status**, **Global Settings**, **Signature Policies**, **Sensors**, **Alerts and Reports**, and **View Rule File**. By default, Status tab is selected, and the status of the signature database in IPS Status table is displayed in the center panel.

Figure 126: Intrusion Prevention: Status

The table below provides field description for Status page.

Table 24: Status Field Description

Field	Description
STATUS	
Intrusion Sensor	
IPS Status	
Signature Database Version	The version of the signature database, which will have the vendor version information as well as the local version information.
Signature Database TimeStamp	This displays the timestamp of the signature file.
Signature Update Report	This displays the last time the security appliance on device checked for the signature updates on remote signature server.

Field	Description
Signature Schedule	This displays the scheduled time at which the security appliance on the device shall automatically check the remote signature server for any updates.
Edit Signature Schedule	Provides an option to automatically update the signature set on the OA-700. This sets the time at which the signature update is scheduled.
Rebuild	This allows to manually rebuild the latest updated signature database.
Rollback	This allows to rollback to different versions of Snort rule database. **Rollback is not allowed if Rebuild is in progress.**
Report Status	This displays conflicts between the user changes in the current version and the new version. This also displays the additions and deletions in the new version against the current version, and the signature update status.
Refresh	Refresh the Report Status.

EDIT SIGNATURE SCHEDULE

1. Click **Edit Signature Schedule** icon in **IPS Status** table. **Signature Schedule** page is displayed.

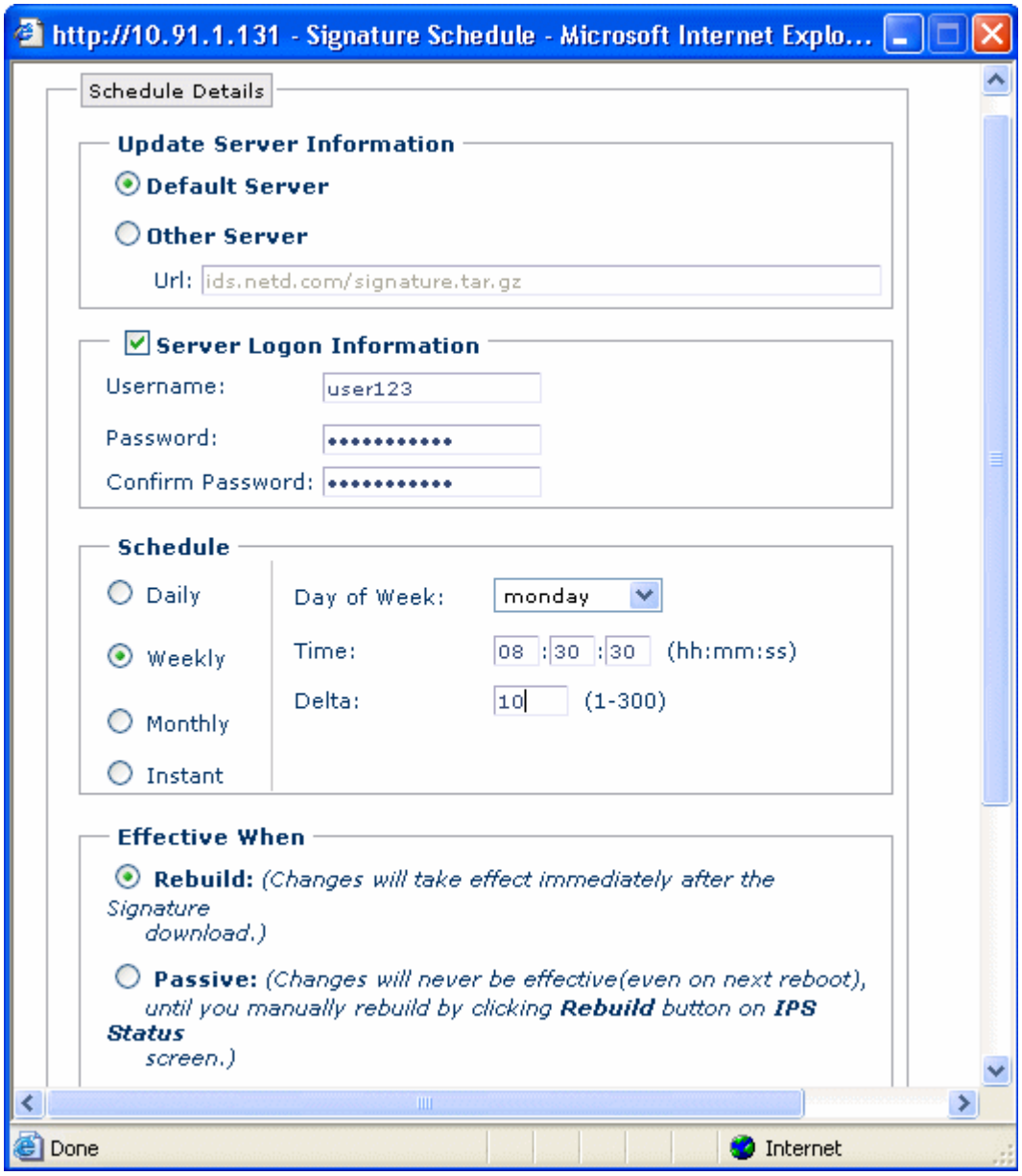


Figure 127: Intrusion Prevention: Status - Signature Update

2. Select the **Signature Server** option: **Default Server/Other Server** from where you want to download the Signature files. If you have selected **Other Server** option, enter the URL of the location from where Signature file has to be downloaded in the **URL** field.

3. Select the **Server Logon Information** check box to enter the Server Logon Information:
   - Enter the user name, password, and confirm password in the **Username**, **Password**, and **Confirm password** fields.
4. Set the schedule:
   - Select **Daily** radio button, enter time in Time field, and Delta to update signature database daily.
   - Select **Weekly** radio button, set the day in Day of Week field, enter time in Time field, and Delta to update signature database once a week.
   - Select **Monthly** radio button, select the date in Day field, enter time in Time field, and Delta to update the signature database once a month.
   - Select **Instant** radio button to update the signature database instantly.
5. Choose the **Effective When** option by selecting **Rebuild/Passive** radio button. Based on the chosen option, the new signature file comes into effect and gets updated in the IDS database.
   - **Rebuild**: Downloads the latest signature database. The signature database will come into effect immediately after download.
   - **Passive**: Downloads the latest signature database. Changes will not come into effect even on next reboot, until you manually rebuild by clicking **Rebuild** button on the IPS Status page.
6. Click **Apply** to schedule the Signature Update or click the **Cancel** to cancel the operation.

MANUALLY REBUILD SIGNATURE SCHEDULE

Click **Rebuild** to manually rebuild the signature database.

ROLLBACK TO PREVIOUS VERSION OF THE SIGNATURE FILE

This page allows you to rollback to different versions of Snort rule database.

1. Click **Rollback**. **IPS Status Rollback** page is displayed.

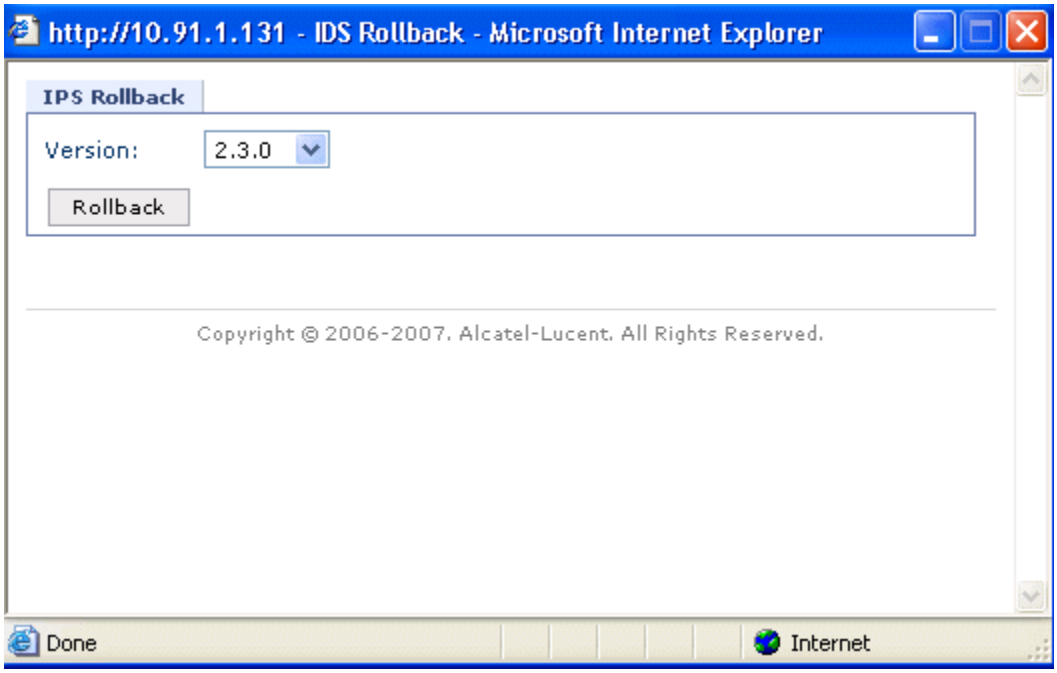


Figure 128: Intrusion Prevention: Status - IPS Rollback

2. Select the desired version of the signature database from the **Version** drop-down list.
3. Click **Rollback** to roll back to the previous version of Signature file in the Signature Database in IDS.

GLOBAL SETTINGS

This page allows you to configure the IPS rules globally.

VIEW GLOBAL SETTINGS

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Intrusion Prevention** sub-menu.

The **Intrusion Prevention** menu has six tabs: **Status**, **Global Settings**, **Signature Policies**, **Sensors**, **Alerts and Reports**, and **View Rule File**.

Select the **Global Settings** tab. Global Settings page is displayed in the center panel.

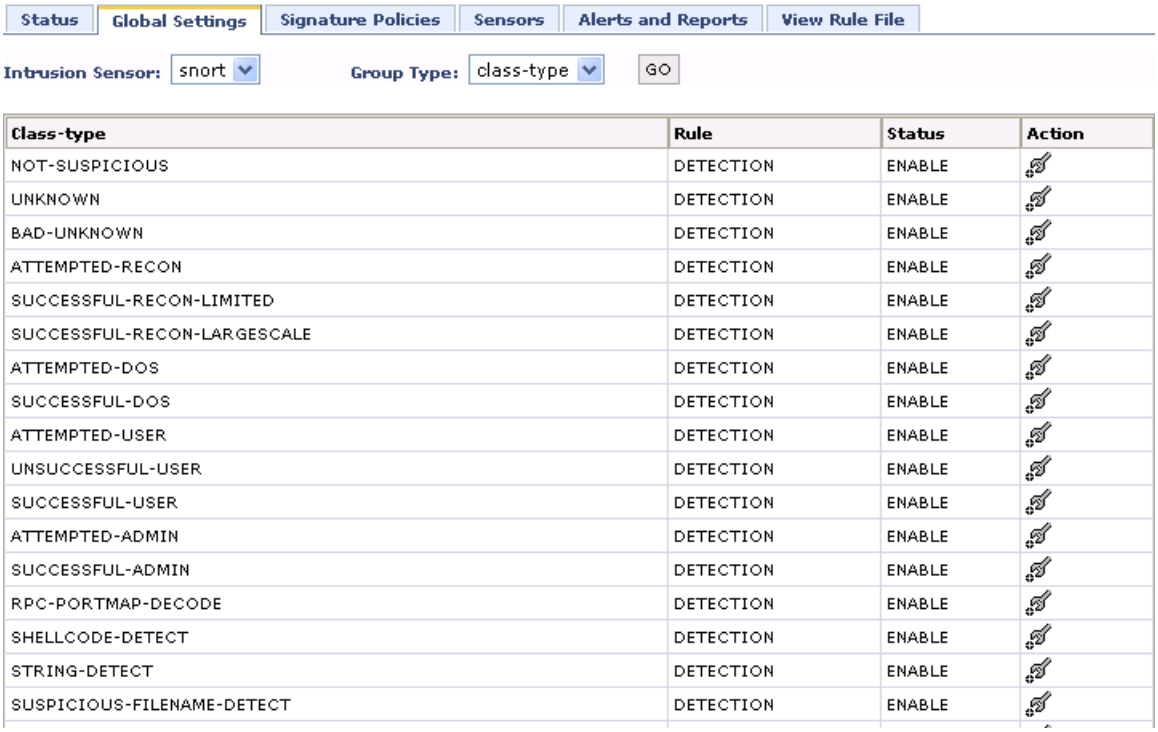


Figure 129: Intrusion Prevention: Global Settings

The table below provides field description for Global Settings page.

Table 25: Global Settings Field Description

Field	Description
GLOBAL SETTINGS	
Intrusion Sensor	Allows to select the intrusion sensor type.
Group Type	Allows to select the group type: Class Type/Category/Priority
Class-type	Table is displayed based on IPS classes.
Rule	Indicates if the rule is used for DETECTION or PREVENTION or PREVENTION-RESET.
Status	Displays if a specific rule is enabled or disabled.
Action	Provides an option to edit the IPS rules.

CONFIGURING GLOBAL SETTINGS

Follow the procedure below to configure global settings for IPS rules.

Step 1: From the **Global Settings** page, select the intrusion sensor type from the **Intrusion Sensor** list.

Step 2: Select group type (Class-type, Category, or Priority) from **Group Type** list and click **GO**. The selected group type is displayed in the table with options to edit rule and status.

Step 3: Click the **Edit Rule** icon against the rule to be edited under the **Action** column. Editable fields for the selected rule is populated in **Rule and Status** column.

Step 4: Set the rule from the **Rule** drop-down list. Select **Prevent-Reset/Prevent/ Detection** to set the action to reset prevent settings/prevent/detect. This specifies if the rule should be used for prevention or detection of the type of IP traffic that is generating an attack.

Step 5: Set status to **ENABLE** or **DISABLE** from the **Status** drop-down list.

Step 6: Click **Apply** to save changes.

SIGNATURE POLICIES

This page allows you to configure IPS signature policies. This page also displays signatures based on class/category/priority. You can also view a signature based on SID.

VIEWING SIGNATURE POLICIES

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Intrusion Prevention** sub-menu.

The **Intrusion Prevention** menu has six tabs: **Status**, **Global Settings**, **Signature Policies**, **Sensors**, **Alerts and Reports**, and **View Rule File**.

Select **Signature Policies** tab. **Signature Policies** page is displayed in the center panel.

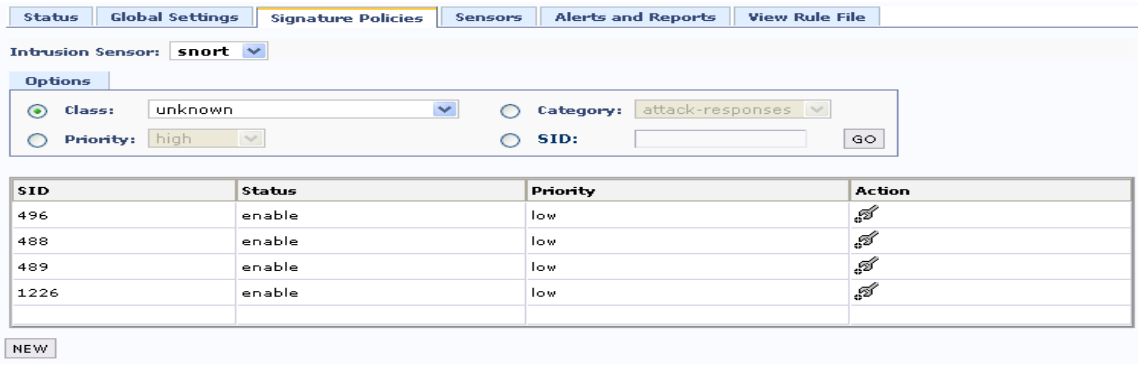


Figure 130: Intrusion Prevention: Signature Policies

The table below provides field description for Signature Policies page.

Table 26: Signature Policies Field Description

Field	Description
VIEWING SIGNATURE POLICIES	
Intrusion Sensor	Allows to select the intrusion sensor type.
Options	
Class	Allows to select class type.
Category	Allows to select category type.
Priority	Allows to set priority.
SID	Lookup Signature ID.
SID	The database ID number of the signature.
Status	The status of the signature policy: Enabled/Disabled
Priority	Defines the attack signature as Low, Medium, or High.
Action	Provides option to edit the IPS signature policy.
New	Allows to create new rule for the signature.

CONFIGURING SIGNATURE POLICY

Follow the procedure below to configure signature policy.

Step 1: From the **Signature Policies** page, click **New**. **Signature Configuration** page is displayed.

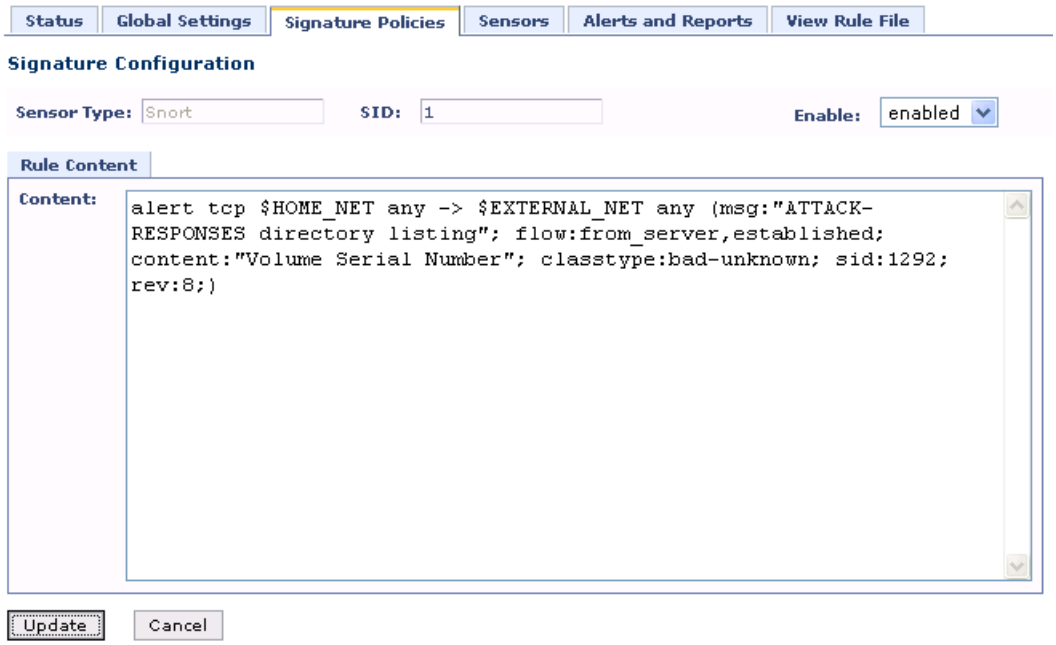


Figure 131: Intrusion Prevention: Signature Policies - New

Step 2: Select intrusion sensor type from the **Intrusion Sensor Type** list.

Step 3: Enter the signature ID in **SID** field.

Step 4: Chose enabled or disabled in the **Enable** field. Based on the selected option, the signature is enabled or disabled.

Step 5: Enter the contents for the signature rule (policy) in the **Contents** field under the Rule Content box.

Step 6: Click **Update** to add the new signature rule or click **Cancel** to cancel adding new rule.

EDITING SIGNATURE POLICY

1. From the **Signature Policies** page, click **Edit** icon in the **Action** column against the Signature Policy you want to edit. **Signature Configuration** page is displayed.
2. Change the Signature Policy parameters. The Sensor Type and the SID cannot be modified.
3. Click **Apply** to save changes or **Cancel** to retain the original values and to return to Signature Policy page.

SENSORS

Sensor is a Intrusion Prevention system which when applied to an interface (using Firewall) will detect and prevent any attacks coming on that interface. You can attach a sensor to a Firewall policy also.

VIEWING SENSORS

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Intrusion Prevention** sub-menu.

The **Intrusion Prevention** menu has six tabs: **Status**, **Global Settings**, **Signature Policies**, **Sensors**, **Alerts and Reports**, and **View Rule File**.

Select **Sensors** tab. **Sensors page** is displayed in the center panel.

Figure 132: Intrusion Prevention: Sensors

The table below provides field description for Sensors page.

Table 27: Sensors Field Description

Field	Description
SENSORS	
Intrusion Sensor	Allows to select the intrusion sensor type.
Name	Name of the sensor.
Rate Threshold / Packets	Denotes number of packets to be sent every second.
Rate Threshold / Per Milli Seconds	Rate threshold in milli seconds.
Associated Firewall Policy	The firewall policy to which the sensor is attached.
Action	Provides option to edit/delete the sensor.
New	Add new sensor.

CONFIGURING SENSORS

Follow the procedure below to configure sensors.

Step 1: Click **New** in Sensors page. **Create a New Intrusion Sensor** page is displayed.

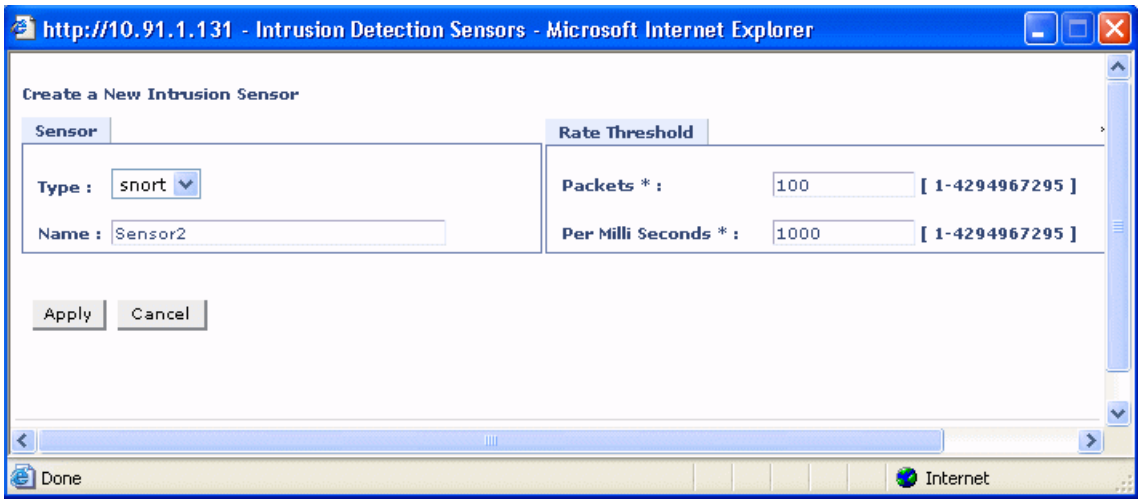


Figure 133: Intrusion Prevention: Sensor - New

Step 1: Select the sensor type in the **Type** drop-down list in the Sensor box.

Step 2: Enter the name for new sensor in **Name** field in Sensor box.

Step 3: Enter the rate threshold packet value for the sensor in **Packets** field in Rate Threshold box. The rate threshold packet value is in the range of 1-4294967295.

Step 4: Enter the rate threshold time in **Per Milli Seconds** field. The rate threshold time value is in the range of 1-4294967295 milli seconds.
This denotes the threshold time in milliseconds inside which if the specified threshold number of packets are received, those packets are treated as attacks.

Step 5: Apply to add new intrusion sensor.

ASSOCIATING SENSOR TO A FIREWALL POLICY/EDITING SENSOR

1. Create a Sensor.

   Follow Step 1 through Step 4 in the "Configuring Sensors" section.

2. Click **Edit** icon in the **Action** column against the Sensor you want to associate a Firewall Policy/edit the sensor parameters.

   Editing an Existing Intrusion Sensor page is displayed.

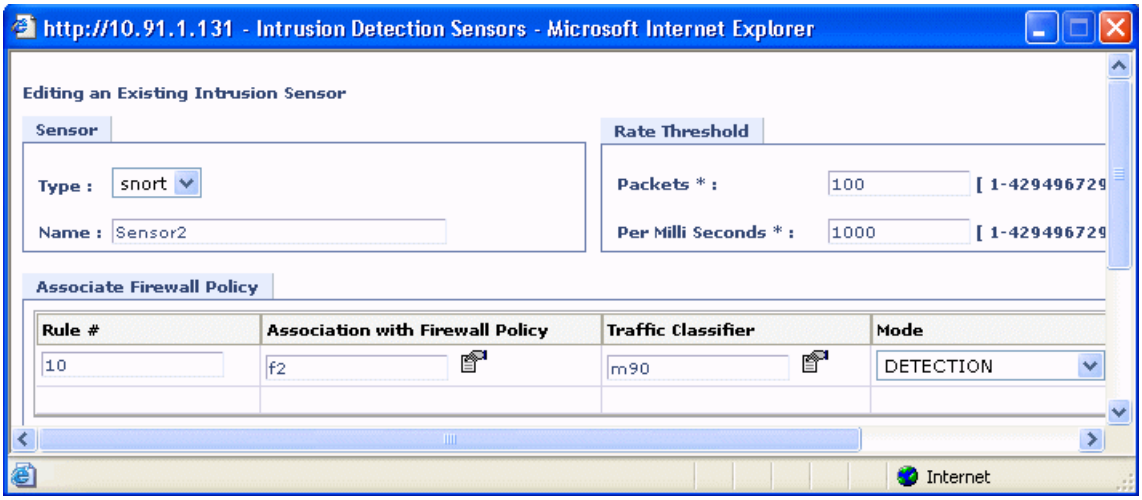


Figure 134: Intrusion Prevention: Sensor - Associating Sensor to a Firewall Policy

3. Change the existing sensor parameters, if required.
4. Click **New** in the **Associate Firewall Policy** table.

   This populates fields to associate the Firewall Policy.

5. Enter the rule number in the **Rule** # field.
6. Select the firewall policy from the **Firewall Policy** list to which you want to associate a sensor.

   The same Sensor can be associated to multiple Firewall Policies, and the same Firewall Policy can be attached to multiple Sensors. And, the same Firewall Policy can be attached multiple times to the same Sensor as well.

7. Select the match-list from the **Traffic Classifier** list.
8. Select the mode from the **Mode** list: **Detection/Prevention/Prevention-Reset**.
9. Click **Apply** to associate a Firewall Policy to a Sensor/edit the sensor parameters or **Cancel** to cancel the operation.

Delete Rule in a Sensor

1. Click **Edit** icon in the **Action** column against the sensor for which you want to delete the rule/firewall policy.

   Editing an Existing Intrusion Sensor page is displayed.
2. Click **Delete** icon in the **Action** column against the firewall policy to be removed in **Associate Firewall** Policy table.
3. Confirm at the prompt to delete the rule/firewall policy from a Sensor.

Deleting a Sensor

1. Click **Delete** icon in the **Action** column against the Sensor you want to delete.
2. Confirm at the prompt to delete the Sensor.

Note: A Sensor assigned to a Firewall Policy cannot be deleted. To delete a Sensor associated with a Firewall Policy, disassociate the Sensor from the Firewall Policy and then delete.

ALERTS AND REPORTS

This page allows to view the intrusion alerts and reports messages.

VIEWING ALERTS AND REPORTS

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Intrusion Prevention** sub-menu.

The **Intrusion Prevention** menu has six tabs: **Status**, **Global Settings**, **Signature Policies**, **Sensors**, **Alerts and Reports**, and **View Rule File**.

Select **Alerts and Reports** tab. **IDS Alerts and Reports** page is displayed in the center panel.

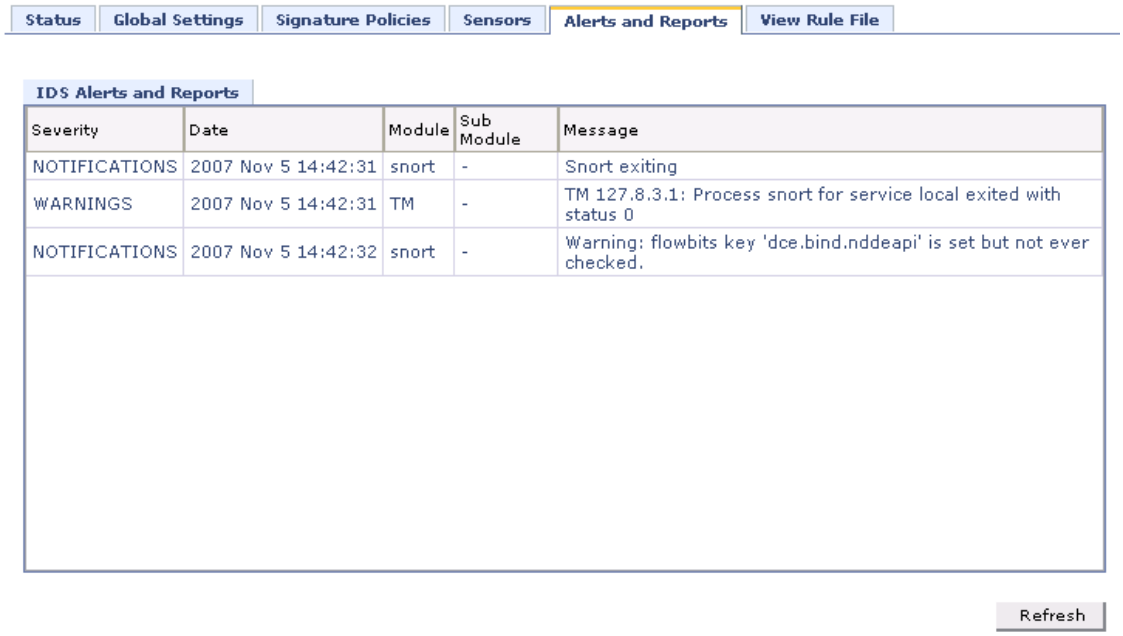


Figure 135: Intrusion Prevention: Alerts and Reports

IDS Alerts and Reports page displays all the alerts and reports based on its severity, date, module, sub module, and the message.

The table below provides field description for Alerts and Reports page.

Table 28: Alerts and Reports Field Description

Field	Description
IDS ALERTS AND REPORTS	
Severity	Severity of the alert message.
Date	Date the alert message is posted.
Module	Module for which the alert message is posted.
Sub Module	Sub-module for which the alert message is posted.
Message	The alert message.
Refresh	Refresh the messages.

VIEW RULE FILE

This page displays the Rule File contents.

Step 1: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 2: Click **Intrusion Prevention** sub-menu.

The **Intrusion Prevention** menu has six tabs: **Status**, **Global Settings**, **Signature Policies**, **Sensors**, **Alerts and Reports**, and **View Rule File**.

Select **View Rule File** tab. **View Rule File** page is displayed in the center panel.

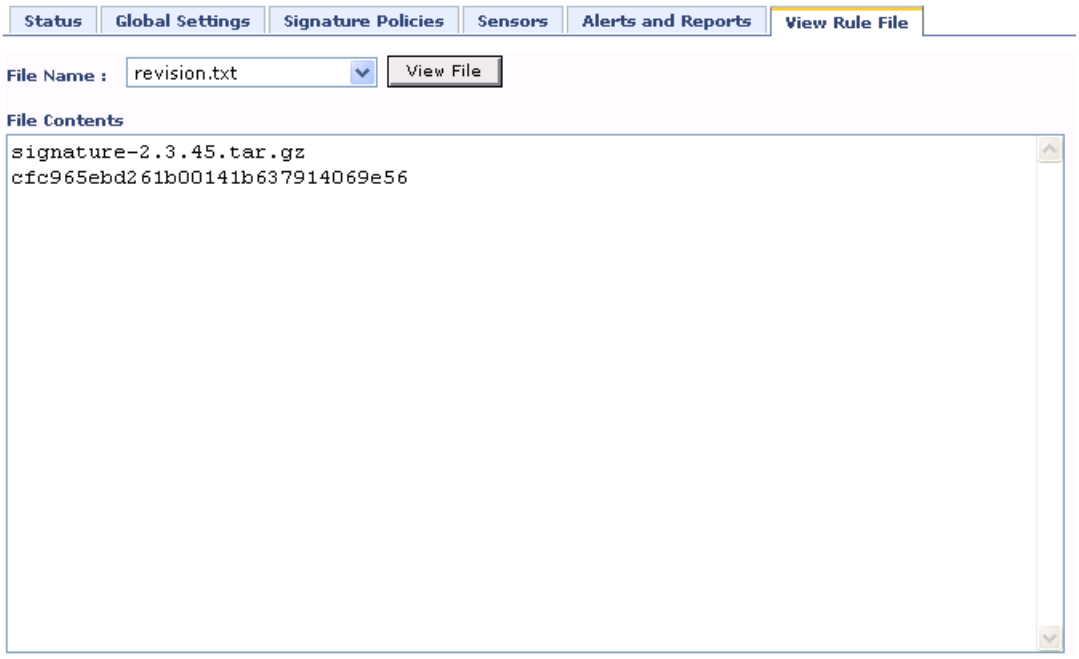


Figure 136: Intrusion Prevention: View Rule File

The table below provides field description for View Rule File page.

Table 29: View Rule File Field Description

Field	Description
VIEW RULE FILE	
File Name	Name of the rule file to be viewed.
View File	View the selected rule file.
File Contents	This box displays the contents of the selected rule file.

Step 3: Select the rule file to be viewed from the **File Name** drop-down list.

Step 4: Click **View File** to view the contents of the selected rule file in **File Contents** box.

QoS (Quality of Service)

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 part of QoS to insure that networks are performing at the desired level.

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 deal 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 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
   - 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/T1/E1)
    - 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

QoS Configuration Wizard

This wizard allows you to configure QoS policies for Branch Office (pre-defined Template) in few easy steps.

QoS wizard allows you to configure QoS policy map and associate it to an interface.

The wizard creates a policy with the following classes:

- Voice Class - To handle Real-time traffic (like RTP).
- Business Critical Class - To handle enterprise traffic (like SNMP, SSH, Telnet).
- Network Control Class - To handle routing traffic (like OSPF, BGP).
- Best Effort - To handle the traffic that does not fall under the above 3 classes.

You can associate link bandwidth for each of these classes. Depending on the bandwidth distribution for each of the classes, a QoS policy map is generated that controls the traffic flow for the selected interface.

Viewing QoS Wizard

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Quality of Service** sub-menu.

Quality of Service has four tabs: **QoS Wizard**, **Class Map**, **Policy Map**, and **Interface Association**. By default, **QoS Wizard** tab is selected and QoS Wizard window is displayed in the center panel.

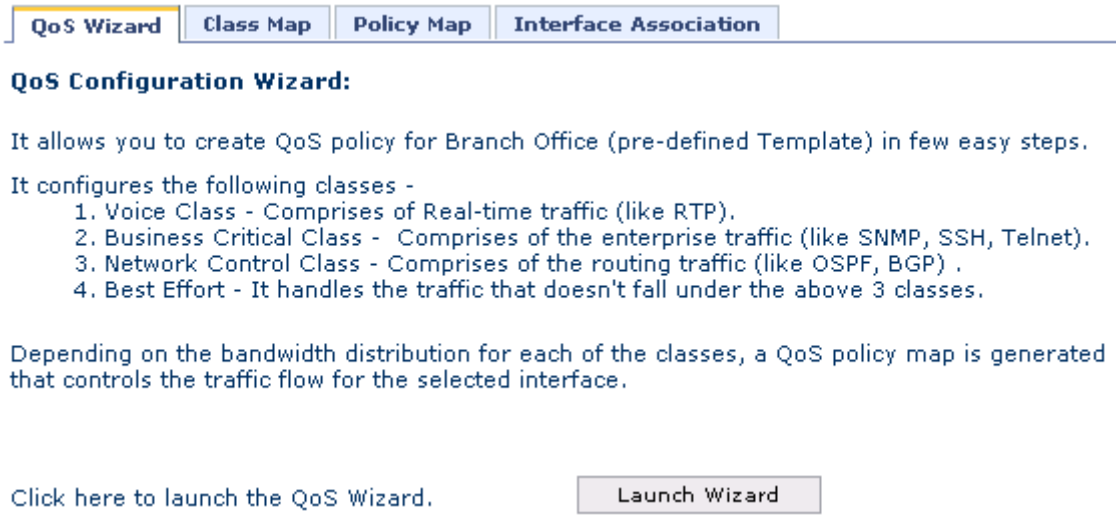


Figure 137: Quality of Service: QoS Wizard

CONFIGURE QOS POLICY USING THE WIZARD

Follow the procedure below to configure a QoS Policy using the wizard.

Step 1: Click **Launch Wizard** in the **QoS Configuration Wizard** page to begin configuring a QoS Policy. The following page is displayed:

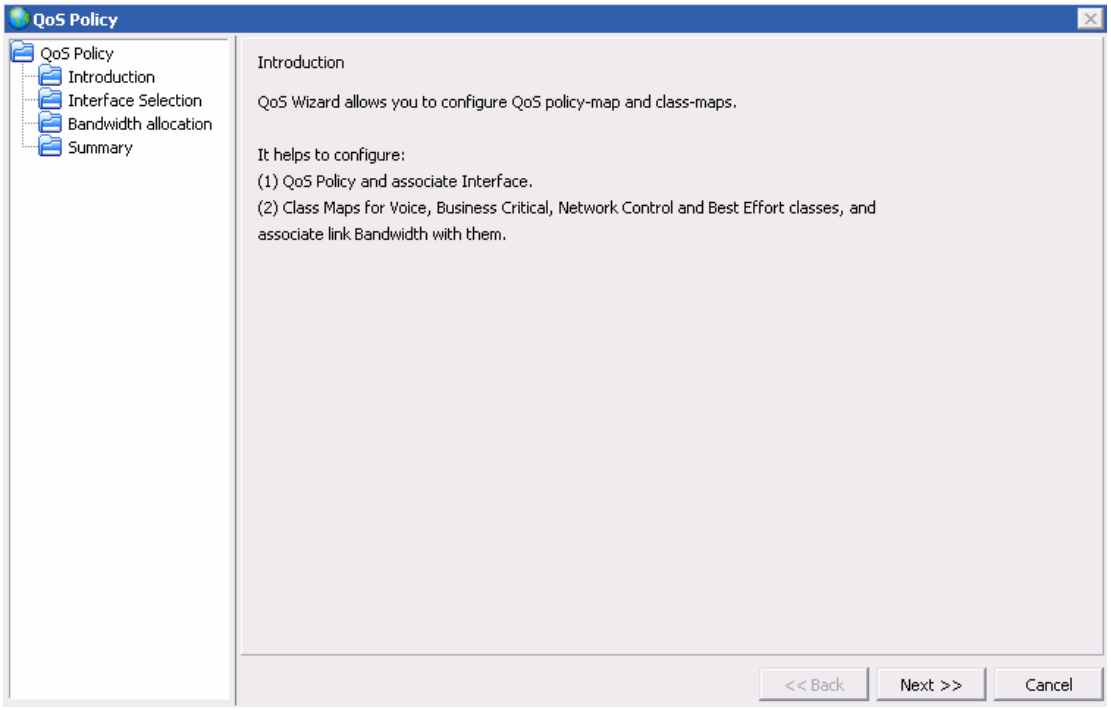


Figure 138: Quality of Service: QoS Wizard - Introduction

Step 2: Click **Next**. **Interface Selection** page is displayed. This window allows you create a policy map and attach it to an interface.

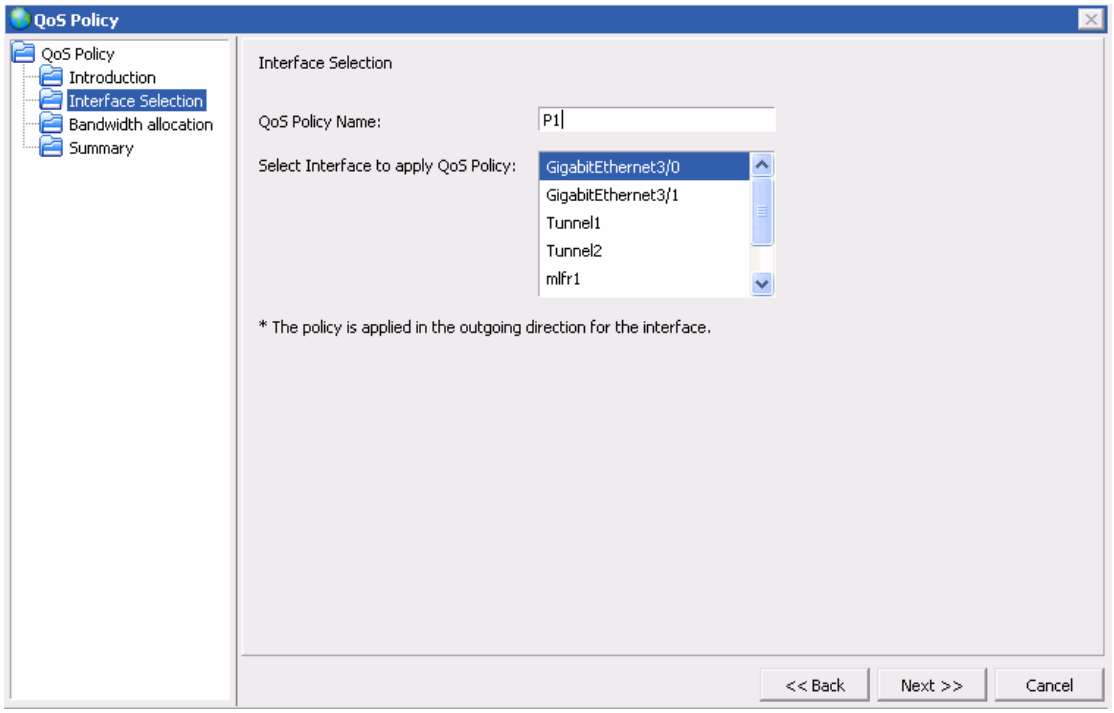


Figure 139: Quality of Service: QoS Wizard - Interface Selection

1. Enter the Qos policy name in the **QoS Policy Name** field.
2. Choose the interface on which you want to configure the QoS policy. Select the interface from the **Select Interface to apply QoS policy** list.

   By default, the policy will be attached to the interface in the egress direction.

Step 3: Click **Next**. **Bandwidth Allocation** window is displayed.

The wizard creates a policy with the following traffic classes: Voice Class, Business Critical Class, Network Control Class, Best Effort. This window allows you to configure the bandwidth for these classes.

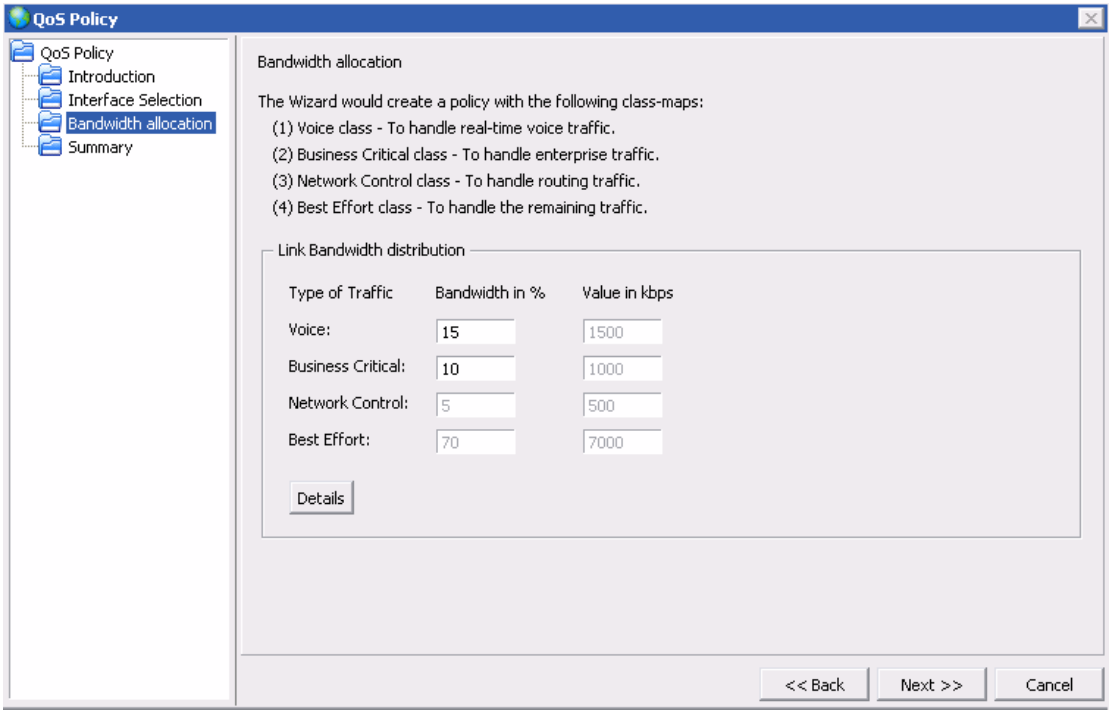


Figure 140: Quality of Service: QoS Wizard - Bandwidth Allocation

1. **Link Bandwidth Distribution** table shows the default bandwidth values for each of the classes both in percentage and as well as value in Kb. **Only Voice and Business Critical bandwidth values are editable.**

   Bandwidth for Network Control and Best Effort class is not editable.
2. Enter the required bandwidth in percentage for Voice and Business Critical in the **Bandwidth in %** field. The value in Kbps for the entered bandwidth is displayed in the **Value in Kbps** field.
3. Click **Details** to view the QoS classes created by the wizard and the details of the bandwidth assigned to the classes. The following pop-up window is displayed:

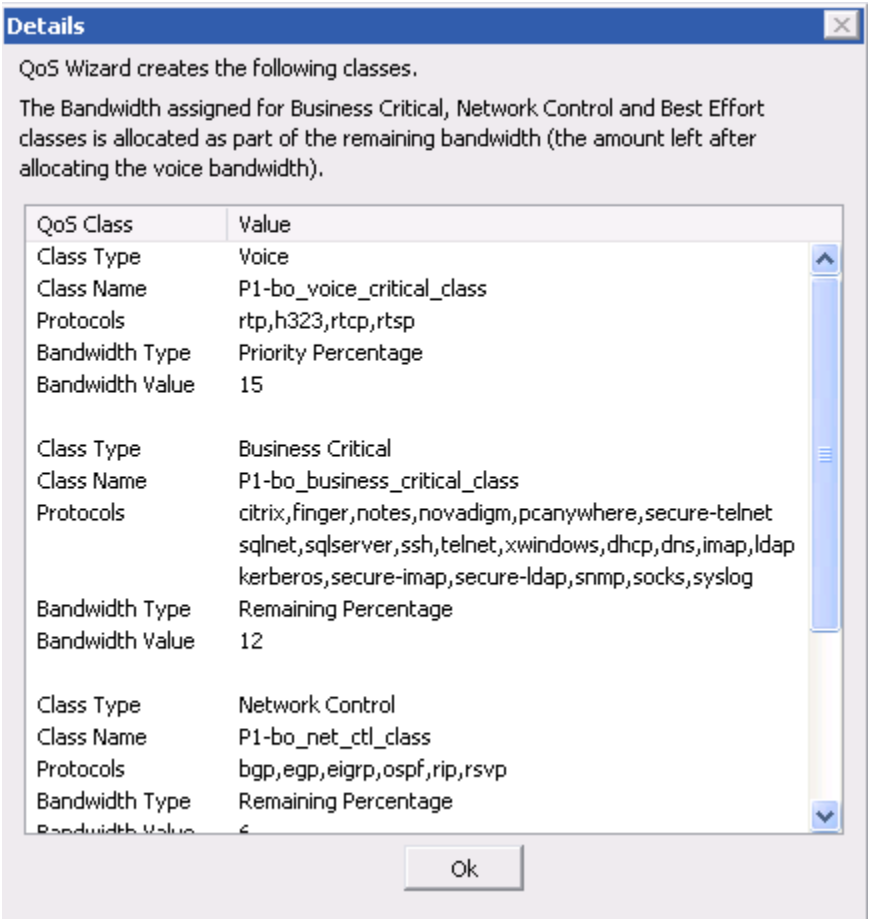


Figure 141: Quality of Service: QoS Wizard - Bandwidth Allocation - Details

Note: Voice bandwidth get precedence over the others. The amount of bandwidth left after the Voice bandwidth is distributed/assigned for Business Critical, Network Control and Best Effort classes.

Step 4: Click **Next**. **Summary** window displays the summary of the QoS policy configuration.

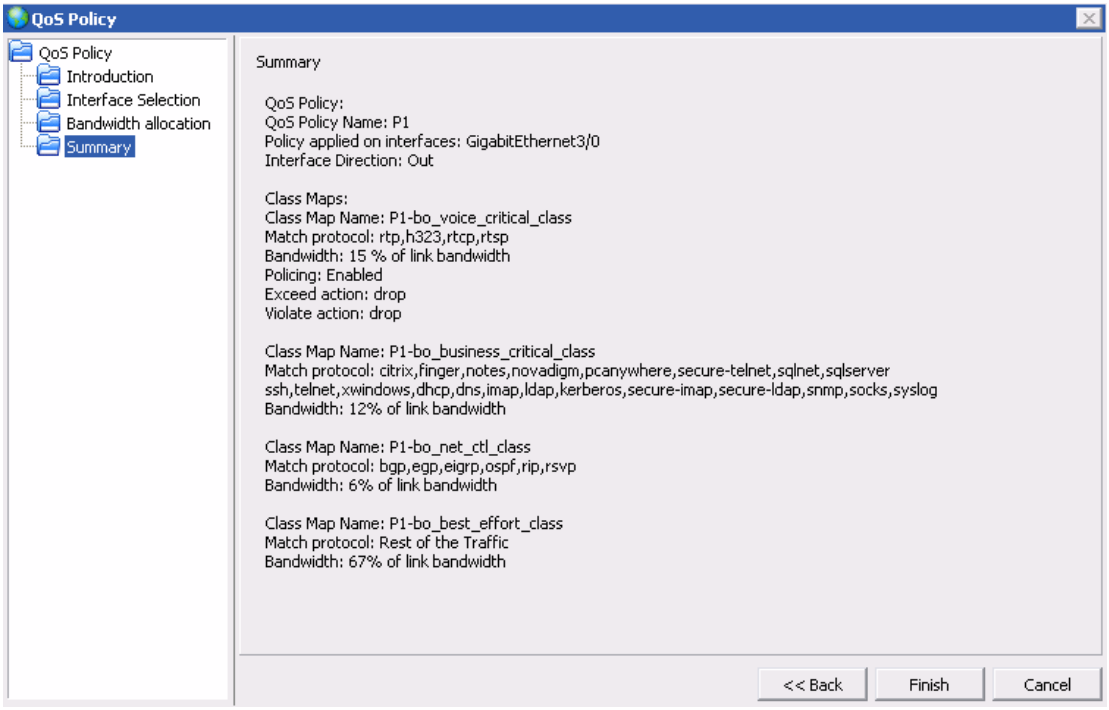


Figure 142: Quality of Service: QoS Wizard - Summary

The Summary window displays the details of the QoS Policy being configured: Policy map being configured and the interface to be associated with it. It also displays the classes auto created by the wizard, configured bandwidth and the policing parameters.

Step 5: Click **Finish** to save the configuration and generate the QoS policy.

Step 6: A status bar is displayed showing the QoS policy creation. Once the QoS policy is configured successfully, a successful message is displayed.

The policy map, the interface associated with the policy map, and the class maps auto configured by the wizard is displayed in the **Policy Map**, **Interface Association** and **Class Map** tabs as shown below.

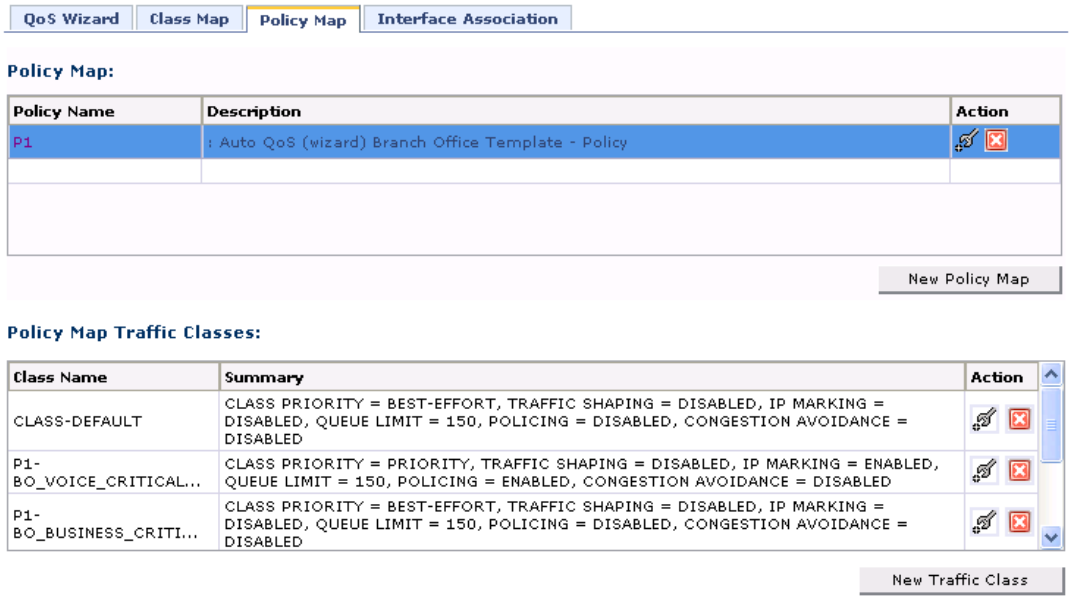


Figure 143: Quality of Service: Policy Map Generated by the Wizard

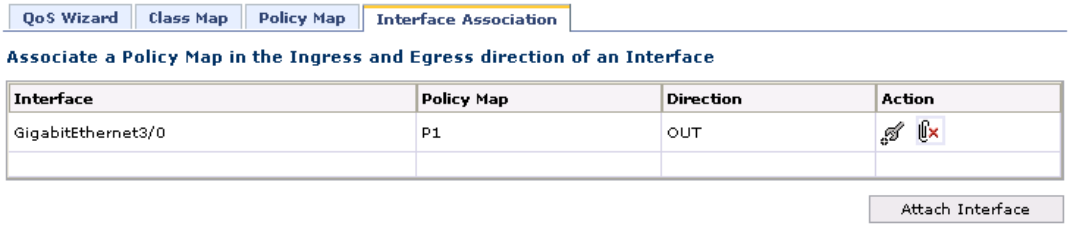


Figure 144: Quality of Service: Interface Association Generated by the Wizard

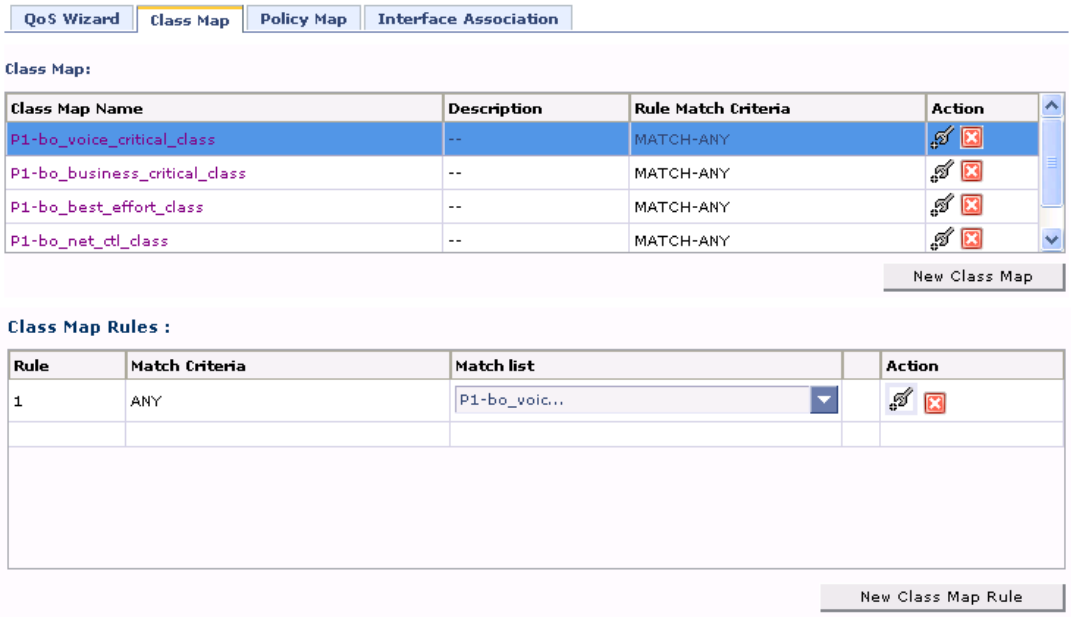


Figure 145: Quality of Service: Class Map Generated by the Wizard

CLASS MAP

This page allows you to add/or edit class map.

VIEWING CLASS MAP

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Quality of Service** sub-menu.

Quality of Service has four tabs: **QoS Wizard**, **Class Map**, **Policy Map**, and **Interface Association**. Select **Class Map** tab. Class Map page is displayed in the center panel.

Figure 146: Quality of Service: Class Map

The table below provides field description for the Class Map page.

Table 30: Class Map Field Description

Field	Description
CLASS MAP	
Class Map Name	Name of the class map
Description	Description for the class map
Rule Match Criteria	Match criteria for rules: MATCH ALL or MATCH ANY.
New Class Map	Create new class map.
CLASS MAP RULES	
Rule	Class map rule ID.
Match Criteria	Match criteria for rules: ALL/ANY
Match list	Match list to be associated with the class map.
Action	Provides option to edit and/or delete class map rules.
New Class Map Rule	Create new class map rule.

CONFIGURE CLASS MAP

Follow the procedure given below to create a class map:

Step 1: From the **Class Map** page, click **New Class Map** to create a new class map.

New Class Map page is displayed in the center panel.

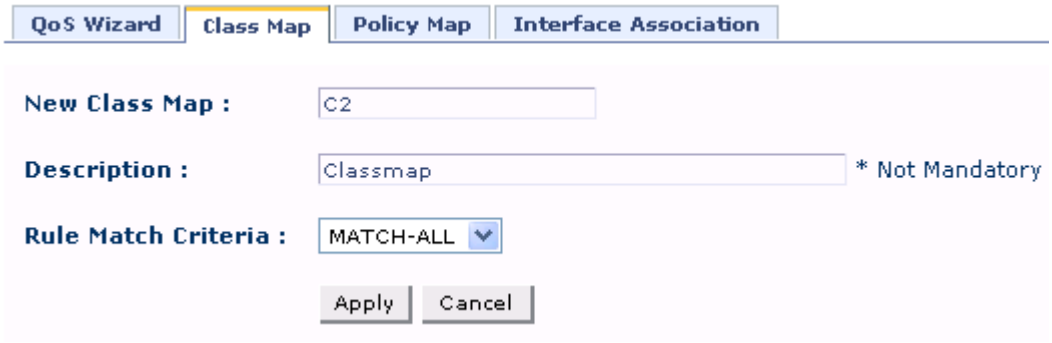


Figure 147: Quality of Service: New Class Map

Step 2: Enter the name for new class map in **New Class Map** field.

Step 3: Enter description for the new class map in the **Description** field. (optional)

Step 4: Set the rule match criteria for the class map from the **Rule Match Criteria** drop-down list: MATCH ALL/MATCH ANY

Step 5: Click **Apply** to create a new class map or click **Cancel** to cancel the operation.

ADD CLASS MAP RULE

Step 1: From the Class Map page, select the class map name for which rule is to be added. Click **New Class Map Rule** in the **Class Map Rules** table to create class map rule. Fields to add new class map rule is populated as shown below.

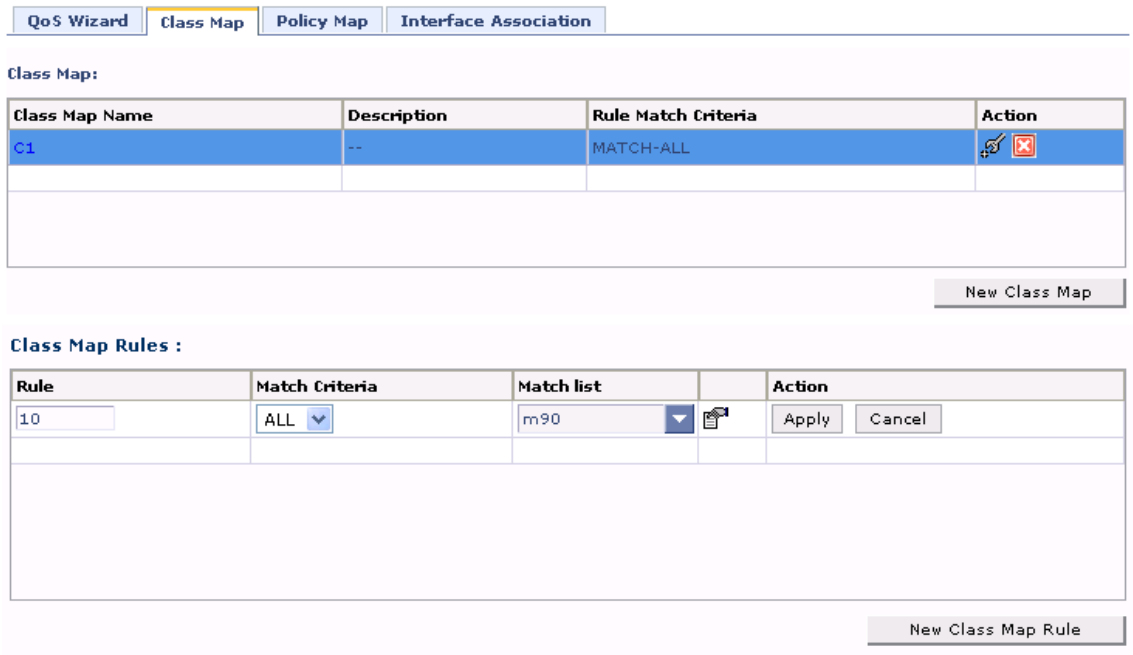


Figure 148: Quality of Service: New Class Map Rule

Step 2: Enter class map rule number in **Rule** field.

Step 3: Set match criteria by selecting it from the **Match Criteria** drop-down list: ALL/ANY

Step 4: Associate the match-list with the class map. You can configure any number of match-lists.

Select the match-list/s from the **Match List** field in the **Match List** box. It lists out all the match-lists available.

- Select the match-list to be included from the **Available MatchList** column and click the '>>' button to move it to the **Selected MatchList** column. Select as many match-lists from the Available MatchList column and move it to the Selected MatchList column.
- Click **OK**. The selected match-lists is displayed in the Match List drop-down list.

Step 5: Click **Apply** to add new class map rule or click **Cancel** to cancel the operation.

EDIT CLASS MAP

Follow the procedure given below to edit a class map:

1. Click **Edit** icon under the **Action** column against the class map to be edited.

   Fields to edit class map are populated.
2. Change the description and class map rule match criteria. Class map name cannot be edited.
3. Click **Apply** to save changes or **Cancel** to cancel the operation.

EDIT CLASS MAP RULES

Follow the procedure given below to edit class map rule:

1. From the **Class Map** table, select the Class Map whose rule details are to be edited. The rules already configured for the selected class map is displayed in the **Class Map Rules** table.
2. Click **Edit** icon under the **Action** column.

   Fields to edit class map rules are populated.
3. Edit the class map rule match criteria and the match list. Class map rule ID cannot be edited.
4. Click **Apply** to save changes or **Cancel** to cancel the operation.

DELETE CLASS MAP

Note: A class map cannot be deleted if it is associated to a policy map.

Follow the procedure below to delete a class map:

1. Click **Delete** icon under the **Action** column against the class map to be deleted.
2. Confirm at the prompt to delete the selected class map.

DELETE CLASS MAP RULE

Follow the procedure below to delete a class map rule:

1. Click **Delete** icon under the **Action** column against the class map rule to be deleted.
2. Confirm at the prompt to delete the selected class map rule.

POLICY MAP

This page allows you to add/or edit policy map.

VIEWING POLICY MAP

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Quality of Service** sub-menu.

Quality of Service has four tabs: **QoS Wizard**, **Class Map**, **Policy Map**, and **Interface Association**. Select **Policy Map** tab, Policy Map page will be displayed in the center panel.

Figure 149: Quality of Service: Policy Map

The table below provides field description for the Policy Map page.

Table 31: Policy Map Field Description

Field	Description
POLICY MAP	
Policy Name	Name of the policy map.
Description	Description for the policy map.
Action	Provides option to edit/delete policy map.
New Policy Map	Create new policy map.
POLICY MAP TRAFFIC CLASSES	
Class Name	Traffic class name.
Summary	Summary of the configured parameters of the traffic class
Action	Provides option to edit/delete traffic class.

CONFIGURE POLICY MAP

This page allows you to configure a policy map.

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. 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.
3. Priority and network-control commands are not applicable for the ‘class-default’.

Follow the procedure given below to configure a policy map:

Step 1: From the **Policy Map** page, click **New Policy Map** to create a new policy map.

Policy Map Configuration page is displayed in the center panel.

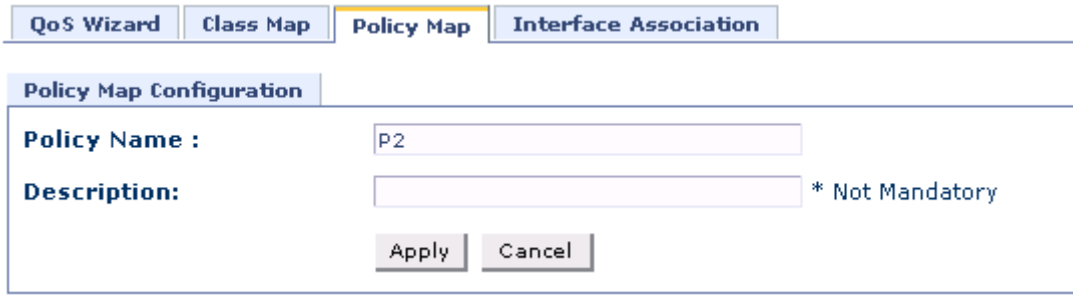


Figure 150: Quality of Service: Policy Map - New

Step 2: Enter the name for new policy map in the **Policy Name** field.

Step 3: Enter description for the new policy map in the **Description** field. (optional)

Step 4: Click **Apply** to create a new policy map.

Step 5: By default, the default-class exists for a policy map, and is displayed in the Policy Map Traffic Classes table.

ADD NEW TRAFFIC CLASS

Step 1: Click **New Traffic Class** in the **Policy Map** page to create traffic class for the just created policy map. The New Traffic Class page is displayed in the center panel.

Step 2: The policy name for which the traffic class is being created is displayed against the **Policy Name** field.

Step 3: Attach the class map to the policy map. This sets the selected class map as the traffic class of the policy-map through which the traffic flows.

Select the class map to be attached from the **Class Name** List.

Step 4: Define basic, policing, and congestion avoidance configuration for the Traffic Class. There are three tabs provided: **Basic Configuration**, **Policing Configuration**, **Congestion Avoidance**. Click on the respective tab to display the parameters.

Basic Configuration

1. Click **Basic Configuration** tab in the New Traffic Class page. Various parameters to define the Basic Configuration for the traffic class is displayed as shown below:

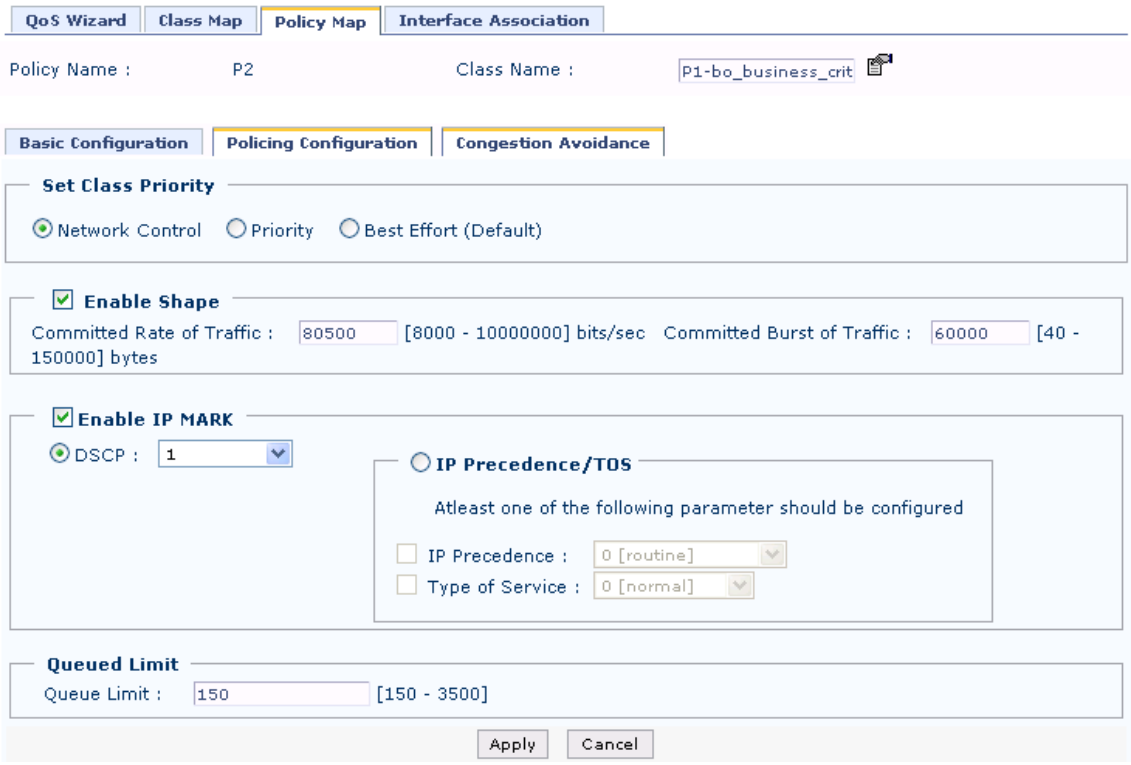


Figure 151: Quality of Service: Policy Map - New Traffic Class Basic Configuration

2. Configure the traffic class as a network control class, priority class or default class.

   Select the **Network Control**, **Priority**, or **Best Effort** radio button in **Set Class Priority** box. By default, **Best Effort** radio button is selected.

   Network-control class will have highest priority among all the traffic classes, Priority class will have the next priority, and Default class has the least priority.

3. Enable traffic shaping on the traffic class, and set committed rate and committed burst of traffic.

   Select the **Enable Shape** check box to enable 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.

   i. Enter the committed rate in the **Committed Rate of Traffic** field. Committed rate is the target rate for a packet flow.

   ii. Enter the committed burst in the **Committed Burst of Traffic** field. Committed burst is the amount of bandwidth allocated to accommodate burst traffic in excess of the rate.

4. Enable IP marking to set the packet marking and the value to mark. Set the DSCP and IP Precedence values.

   Select **Enable IP MARK** check box to enable IP marking.

   i. Select the **DSCP** radio button to set the DSCP value.

      Select the DSCP value from the **DSCP** drop-down list.

      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.

   ii. Select IP Precedence/ToS radio button to set IP precedence value. At least one IP Precedence or ToS value must be configured.

      - Select the **IP Precedence** check box and select **IP Precedence** value from the drop down list.
      - Select **Type of Service** check box and select the type of service from the drop down list.

5. Set the queue limit for the scheduler for the traffic class.

   Set the queue limit between 150 and 3500 in the **Queue Limit** filed in the Queued Limit box. Default queue limit is 150.

6. Click **Apply** to create a new Traffic Class with basic configuration.

Policing Configuration

1. Click **Policing Configuration** tab in the New Traffic Class page. Policing Configuration page is displayed:

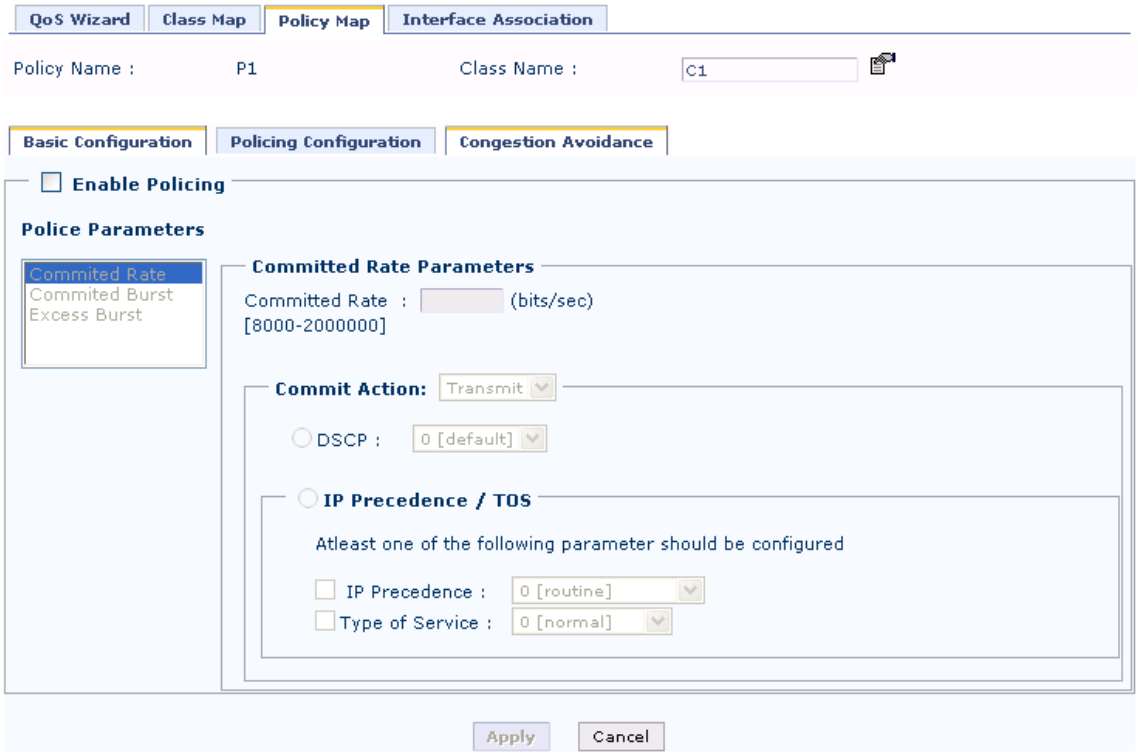


Figure 152: Quality of Service: Policy Map - New Traffic Class Policing Configuration

2. Enable policing.

   Select the **Enable Policing** check box.

3. Select and set the policing parameters. This configures the policer on the particular traffic-class of the policy map.

   There are three **Police Parameters** available: **Committed Rate**, **Committed Burst**, and **Excess Burst**.

   - Select **Committed Rate** option in the **Police Parameters** box. The **Committed Rate Parameters** fields are displayed as shown below.

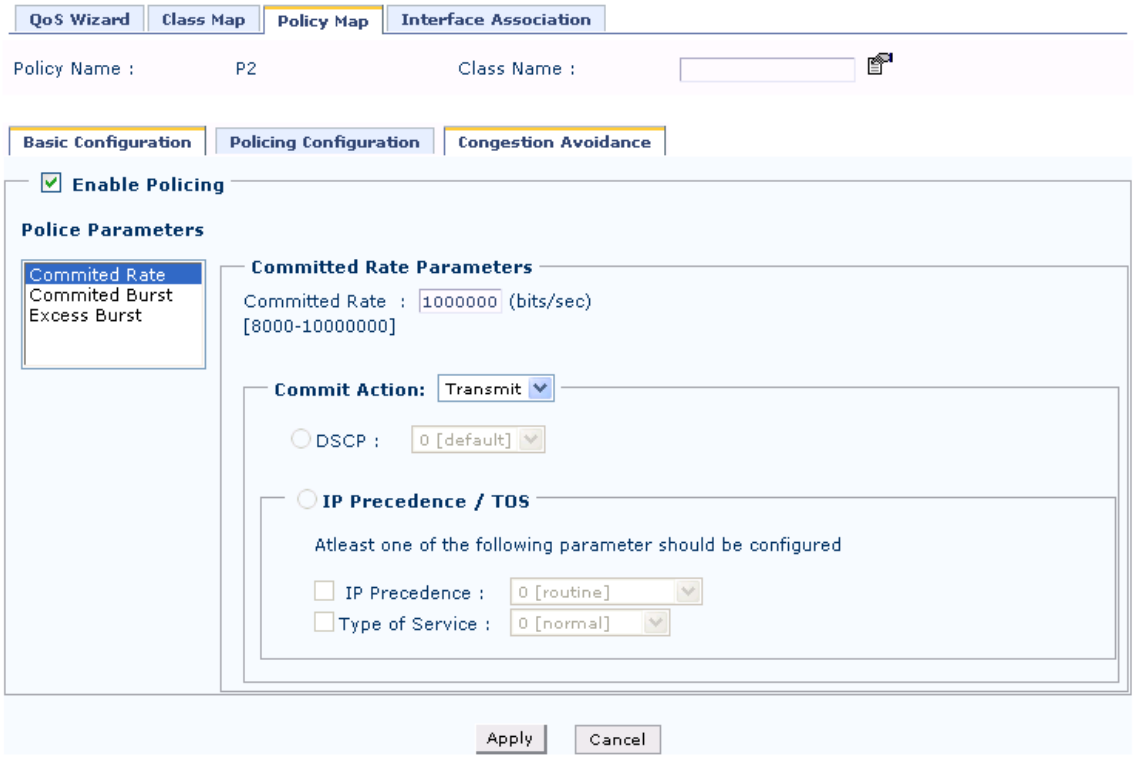


Figure 153: Quality of Service: Policy Map - New Traffic Class Policing Configuration – Committed Rate

i. Set Committed Rate in the **Committed Rate** field.

ii. Set Commit Action as Drop, Transmit, or IP Mark. Select the required option from the **Commit Action** drop-down list.

If you set Commit Action as **IP Mark**, set also the **DSCP** or **IP Precedence/ToS** values.

- Select **DSCP** radio button to set the DSCP values. Select DSCP values from the DSCP drop-down list.
- Select **IP Precedence/TOS** radio button to set IP precedence value. At least, IP Precedence or TOS value parameters must be configured.

Select the **IP Precedence** check box, select IP Precedence value from the drop down list.

Select **Type of Service** check box, select the type of service from the drop down list.

4. Select **Committed Burst** in the **Police Parameters** box. **Committed Burst Parameters** are displayed as shown below.

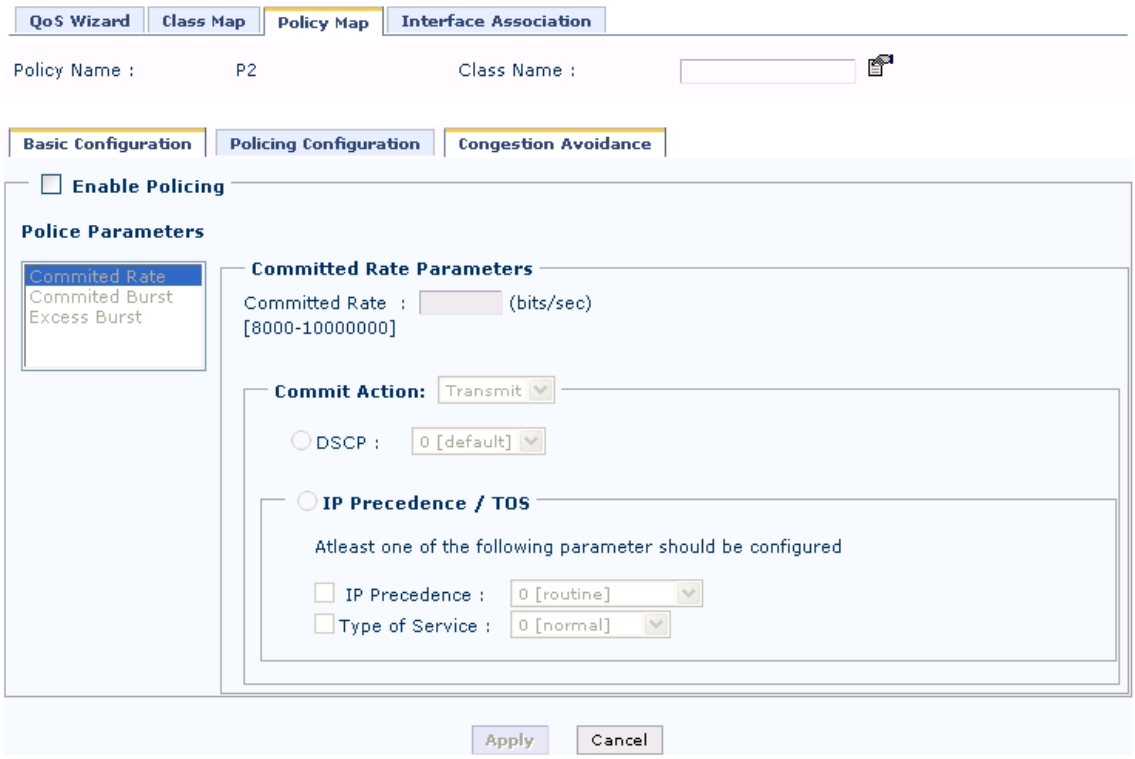


Figure 154: Quality of Service: Policy Map - New Traffic Class Policing Configuration – Committed Burst

i. Set Committed Burst rate in the **Committed Burst** field. The default burst rate is 1500 bytes.

ii. Set Exceed Action as Drop, Transmit, or IP Mark. Select the required option from the **Exceed Action** drop-down list.

If you set Exceed Action as **IP Mark**, set also the **DSCP** or **IP Precedence/TOS** values.

- Select **DSCP** radio button to set DSCP values. Select DSCP values from the DSCP drop down menu.
- Select **IP Precedence/ToS** radio button to set IP precedence value. At least one IP Precedence or TOS values must be configured.

Select the **IP Precedence** check box and select IP Precedence value from the drop down list.

Select **Type of Service** check box and select the type of service from the drop down list.

5. Select **Excess Burst** in the **Police Parameters** box. **Excess Burst Parameters** fields are displayed as shown below.

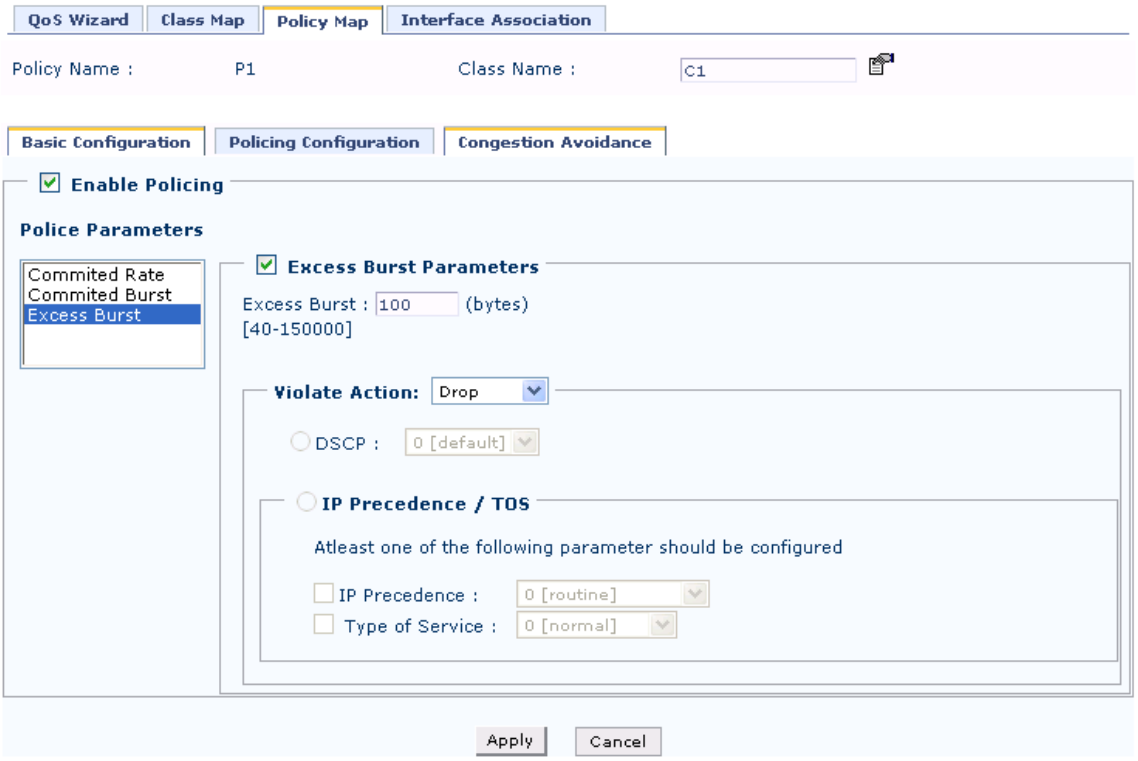


Figure 155: Quality of Service: Policy Map - New Traffic Class Policing Configuration – Excess Burst

i. Check **Excess Burst Parameters** check box to set the excess burst values.

ii. Set Excess Burst rate in the **Committed Burst** field. The default burst rate is 1500 bytes.

iii. Set Violate Action as Drop, Transmit, or IP Mark. Select the required option from the **Violate Action** drop-down list.

If you set Violate Action as **IP Mark**, set also the **DSCP** or **IP Precedence/TOS** values.

- Select **DSCP** radio button to set DSCP values. Select the DSCP values from the DSCP drop down menu.
- Select **IP Precedence/TOS** radio button to set IP precedence value. At least one IP Precedence or TOS values must be configured.

Select the **IP Precedence** check box and select IP Precedence value from the drop down list.

Select **Type of Service** check box and select the type of service from the drop down list.

6. Click **Apply** to create a new Traffic Class with policing configuration.

Traffic Class with Congestion Avoidance

1. Click on **Congestion Avoidance** tab in the New Traffic Class page. The following page is displayed:

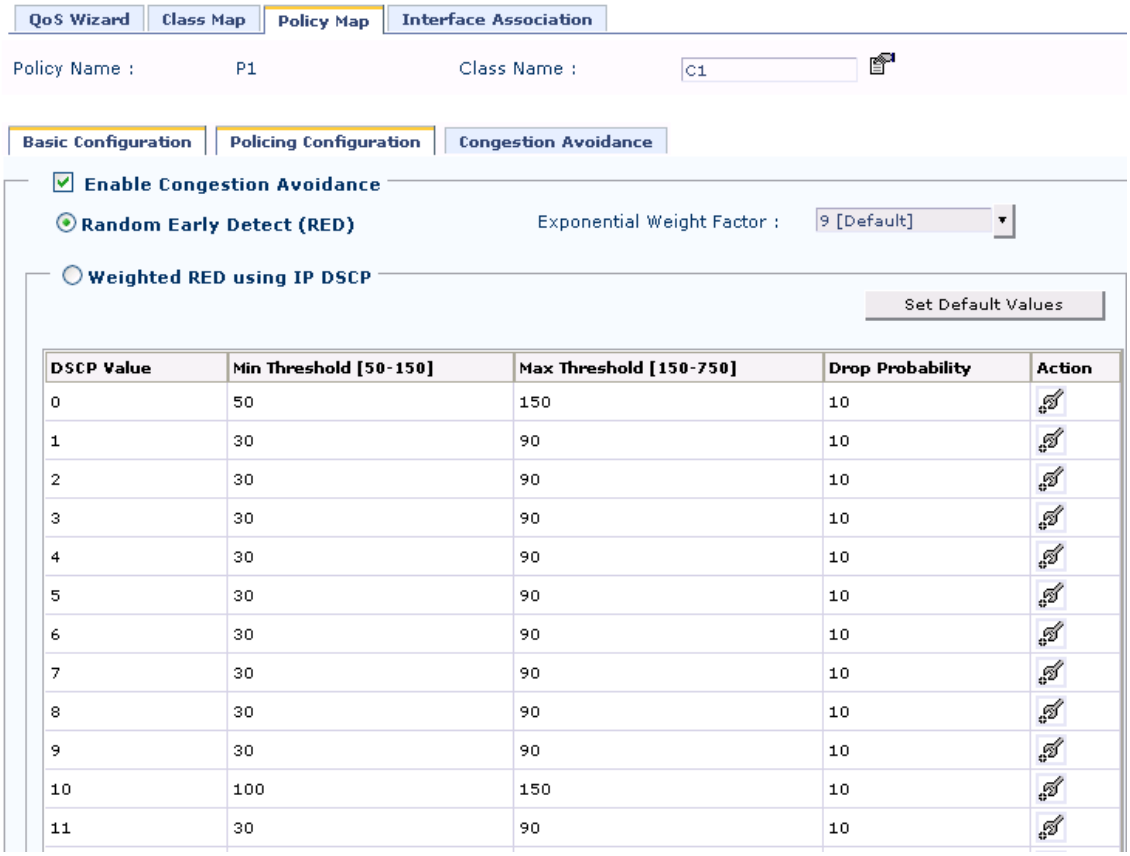


Figure 156: Quality of Service: Policy Map - New Traffic Class Congestion Avoidance

2. Select **Enable Congestion Avoidance** check box to set the Congestion Avoidance values.
3. Select **Random Early Detect (RED)** radio button to use RED as the congestion avoidance technique.
4. Set Exponential Weight Factor by selecting the value from the **Exponential Weight Factor** drop down list. Default values is 9.
5. Select **Weighted RED using IP DSCP** radio button to set the congestion avoidance based on IP DSCP values.

   The DSCP, Min Threshold, Max Threshold, and Drop Probability, and Action fields are displayed in a table.

   DSCP - Displays the DSCP value set earlier in the Policing Configuration page.

   Min Threshold - Minimum threshold of the queue.

   Max Threshold - Maximum threshold of the queue.

Drop Probability - Displays the drop probability. By default, it is 10.

Action - Provides an option to edit the Min Threshold, Max Threshold values.

- Click **Set Default Values** to configure the congestion avoidance using default IP DSCP values.
- If you want to change any IP DSCP value, click **Edit** icon under the **Action** column.

  Only the Minimum and Maximum Threshold values can be edited. Make the required changes in the respective fields, and click **Apply** or click **Cancel** to cancel the operation.

6. Select **Weighted RED using IP Precedence** radio button to set congestion avoidance based on IP precedence values.

   The IP Precedence, Min Threshold, Max Threshold, and Drop Probability, and Action fields are displayed in a table.

   IP Precedence - Displays the IP Precedence value set earlier in the Policing Configuration page.

   Min Threshold - Minimum threshold of the queue.

   Max Threshold - Maximum threshold of the queue.

   Drop Probability - Displays the drop probability. By default, it is 10.

   Action - Provides an option to edit the Min Threshold, Max Threshold values.

   - Click **Set Default Values** button to configure congestion avoidance using default IP Precedence values.
   - If you want to change any IP precedence value, click **Edit** icon under the **Action** column.

     Only the Minimum and Maximum Threshold values can be edited. Make the required changes in the respective fields, and click **Apply** or click **Cancel** to cancel the operation.

7. Click **Apply** to create a new Traffic Class with congestion avoidance or click **Cancel** to cancel the operation.

EDIT POLICY MAP

Follow the procedure given below to edit a policy map:

1. Click **Edit** icon under the **Action** column of **Policy Map** table.
2. Edit the description of the policy map. Policy map name cannot be edited.
3. Click **Apply** to save changes or **Cancel** to cancel the operation.

EDIT POLICY MAP TRAFFIC CLASS

Follow the procedure given below to edit the policy map traffic class parameters:

1. From the **Policy Map** table, select the policy map whose traffic class details are to be edited. The traffic classes already configured for the selected policy map is displayed in the **Policy Map Traffic Classes** table.
2. Click **Edit** icon under the **Action** column.

   Fields to edit the traffic class parameters page is displayed.
3. Edit the traffic class configuration as desired. Policy Name and Class Name cannot be edited.
4. Click **Apply** to save changes or **Cancel** to cancel the operation.

DELETE POLICY MAP

Note: You cannot delete a policy-map if it is attached to an interface either in In/Out direction.

Follow the procedure below to delete a class map:

1. Click **Delete** icon under the **Action** column against the policy map to be deleted.
2. Confirm at the prompt to delete the selected class map.

DELETE POLICY MAP TRAFFIC CLASS

Follow the procedure below to delete a policy map rule:

1. From the **Policy Map** table, select the policy map whose rule/s is to be deleted. Traffic classes configured for the selected policy map is displayed in the **Policy Map Traffic Classes** table.
2. Click **Delete** icon under the **Action** column against the traffic class to be deleted.
3. Confirm at the prompt to delete the selected policy map traffic class.

INTERFACE ASSOCIATION

This page allows you to associate a Policy Map with an interface.

VIEWING INTERFACE ASSOCIATION

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Configure**. All submenu/links under Configure are displayed in the left navigation panel as shown below.

Step 3: Click **Quality of Service** sub-menu.

Quality of Service has four tabs: **QoS Wizard, Class Map**, **Policy Map**, and **Interface Association**. Select **Interface Association** tab, Interface Association page will be displayed in the center panel.

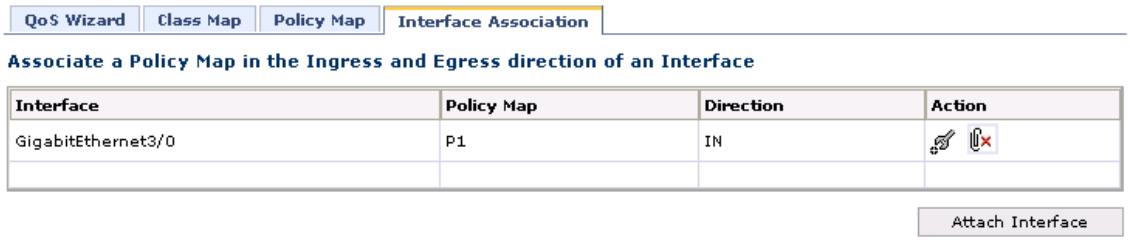


Figure 157: Quality of Service: Interface Association

The table below provides field description for the Interface Association page.

Table 32: Interface Association Field Description

Field	Description
INTERFACE ASSOCIATION	
Interface	Lists interfaces
Policy Map	Policy map associated with the interface.
Direction	Direction Ingress or Egress (IN or OUT).
Action	Provides option to edit/detach the policy map for the interface.
Attach Interface	Allows to attach selected policy map to an interface.

ATTACHING 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 police 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.

Follow the procedure given below to attach a policy map to an interface:

Step 1: From the **Interface Association** page, click **Attach Interface** to attach a policy map to an interface.

Fields to select interface, select policy map, and to set the direction will be populated.

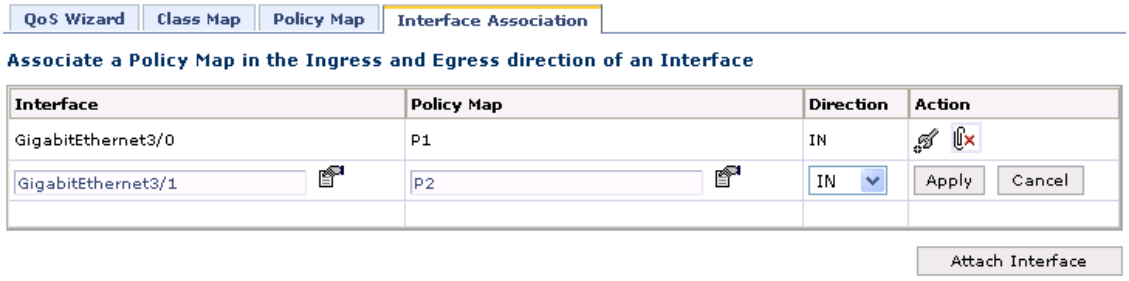


Figure 158: Quality of Service: Interface Association - Attach Interface

Step 2: Select the available interface from the **Interface** list.

Step 3: Select the policy map from the **Policy Map** list.

Step 4: Set the ingress or egress direction (IN or OUT) from the **Direction** drop-down list.

Step 5: Click **Apply** to attach selected policy map to selected interface or click **Cancel** to cancel the operation.

EDIT INTERFACE ASSOCIATION

1. Click **Edit** icon in the **Action** column.

   Make necessary changes in the associated Policy Map, and the direction for the selected interface.
2. Click **Apply** to make the changes or click **Cancel** to cancel the operation.

DETACH POLICY MAP FROM AN INTERFACE

1. Click **Detach Interface** icon in the **Action** column to detach the policy map from the selected interface.
2. Confirm at the prompt to detach the policy-map from the interface it has been bound.

CHAPTER 4

MAINTENANCE

MAINTENANCE

This chapter describes the procedure to maintain the OA-700 system, configure lifeline, upgrade software, flash and its components.

From the USGM menu bar, click **Maintenance**. All submenu/links under Maintenance are displayed in the left navigation panel.

UTILITIES

The utilities page allows saving the running configuration, rebooting the system, and deleting selected files from the USB. Also, this page provides an option to ping, trace route, and establish telnet connection to the OA-700.

VIEWING UTILITIES

Follow the procedure below to view the Interface statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Maintenance**. All submenu/links under Maintenance are displayed in the left navigation panel as shown below.

Step 3: Click **Utilities** sub-menu.

Utilities page is displayed in the center panel.

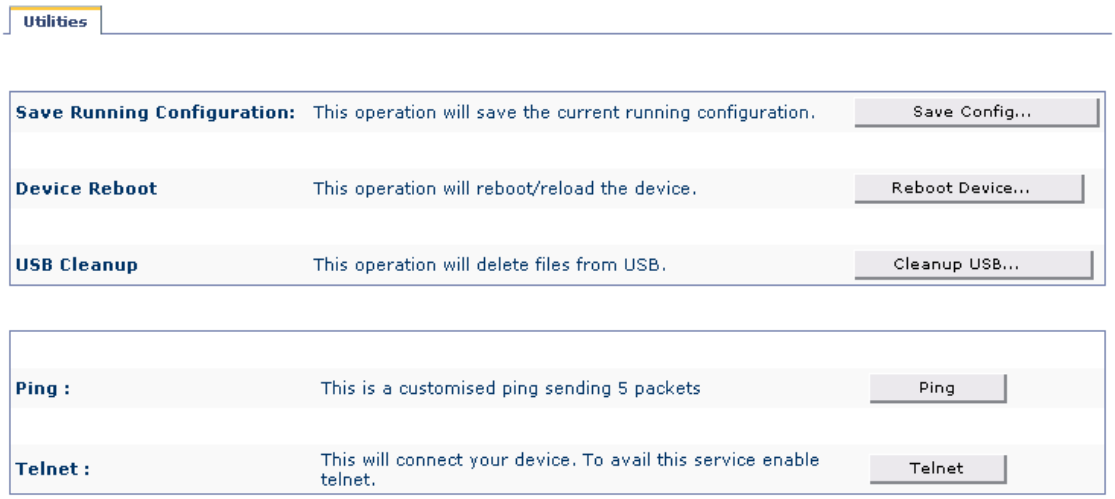


Figure 159: Maintenance: Utilities

The table below provides field description for Maintenance page.

Table 33: Maintenance Field Description

Field	Description
MAINTENANCE	
Save Running Config…	Saves the running configuration of the system
Reboot Device...	Reboots the OA-700 system
Cleanup USB...	Deletes the selected file/s from USB
Ping	Sends ICMP echo requests, and checks the connectivity to a specific host
Telnet	Starts a telnet connection to a remote host  **Note:** This option is available only in Windows Operating System.

SAVE CONFIGURATION

You can save the running configuration to the start-up configuration.

1. Click **Save Config…** to save the current running configuration. The following page is displayed:

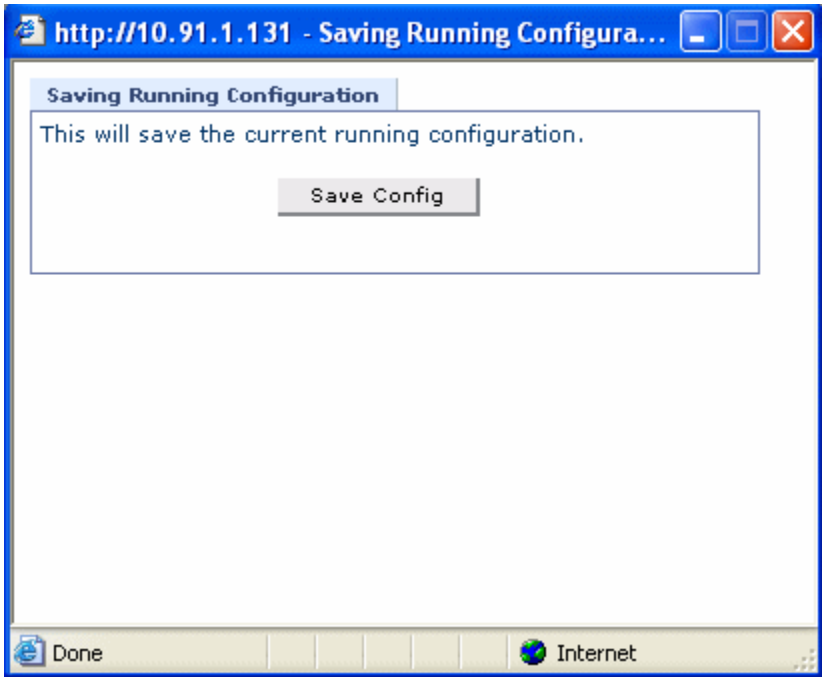
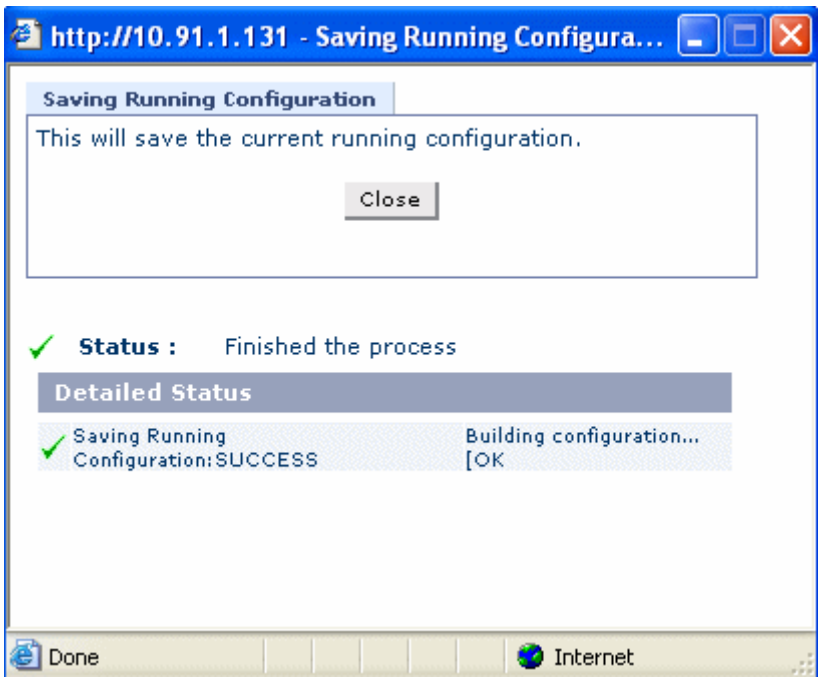


Figure 160: Maintenance: Utilities - Save Running Configuration

- Click **Save Config**. Once the configuration is saved, the following page is displayed:



Note: You can also save the configuration by clicking **Save Running-config** under **Device** menu.

REBOOT DEVICE

You can reboot the OA-700 system. Reboot has the same effect as power cycling the chassis.

1. Click **Reboot Device…** to reboot the system. The following page is displayed asking you to confirm the reboot.

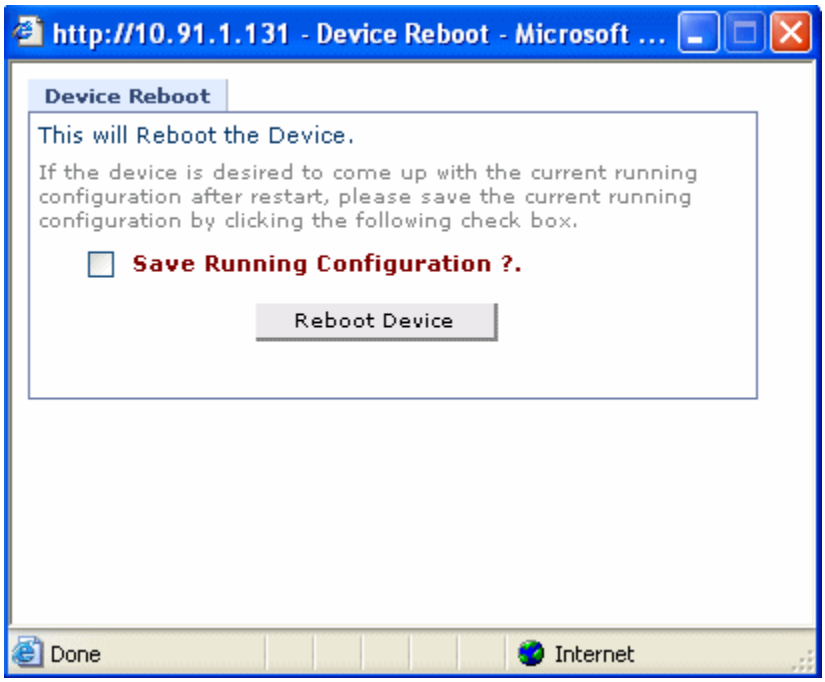


Figure 161: Maintenance: Utilities - Device Reboot

2. You will be asked if you want to save the current configuration before rebooting. If the information is not saved, any changes made since the system was last started will be lost. To save the current configuration, select the **Select Running Configuration** check box.
3. Click **Reboot Device**.
4. Once the reboot is successful, USGM login page is displayed.

Note: You can also reboot the device by clicking **Device Reboot** under **Device** menu.

CLEANUP USB

You can clean up the selected file/s from the USB. This deletes the selected files from the user area of the USB.

1. Click **Cleanup USB...** to cleanup the files from the USB. **USB Cleanup** page is displayed.

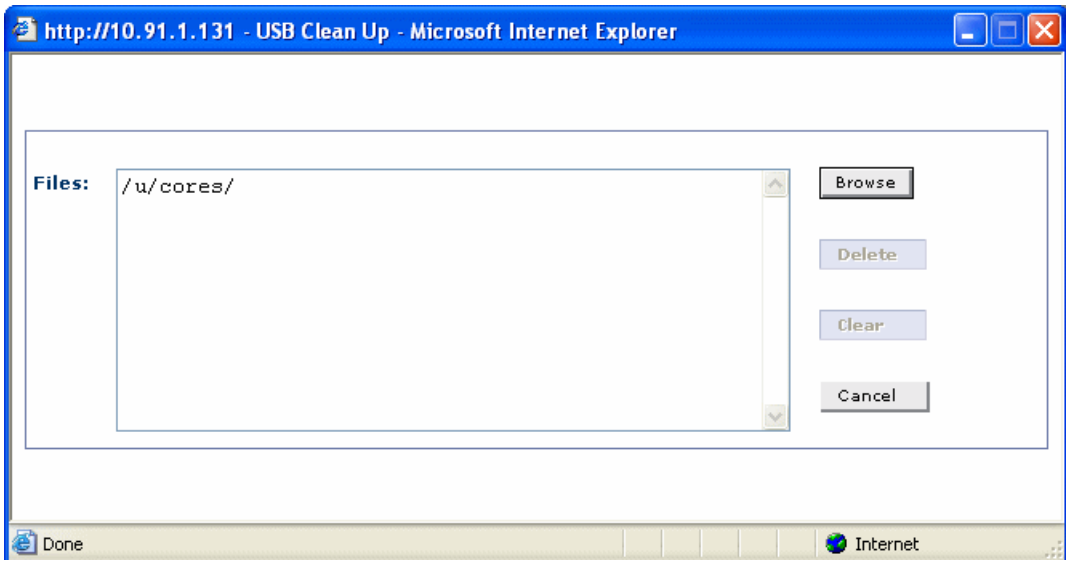


Figure 162: Maintenance: Utilities - USB Cleanup

2. Click **Browse** to select the files to be deleted. The files selected is displayed in the **Files** box.
3. Click **Delete** to delete the selected files.
4. Click **Clear** to clear the file selection and add new files for deletion.
5. Click **Cancel** to cancel the cleanup operation.

PING

Ping is used to check the connectivity to a specific host by using the IP address of the remote host.

Ping is invoked to send ICMP echo requests. Pings send a series of ICMP echo requests, capture responses, and corollary statistics regarding data packet loss.

1. Click **Ping** to display the **Ping** page.

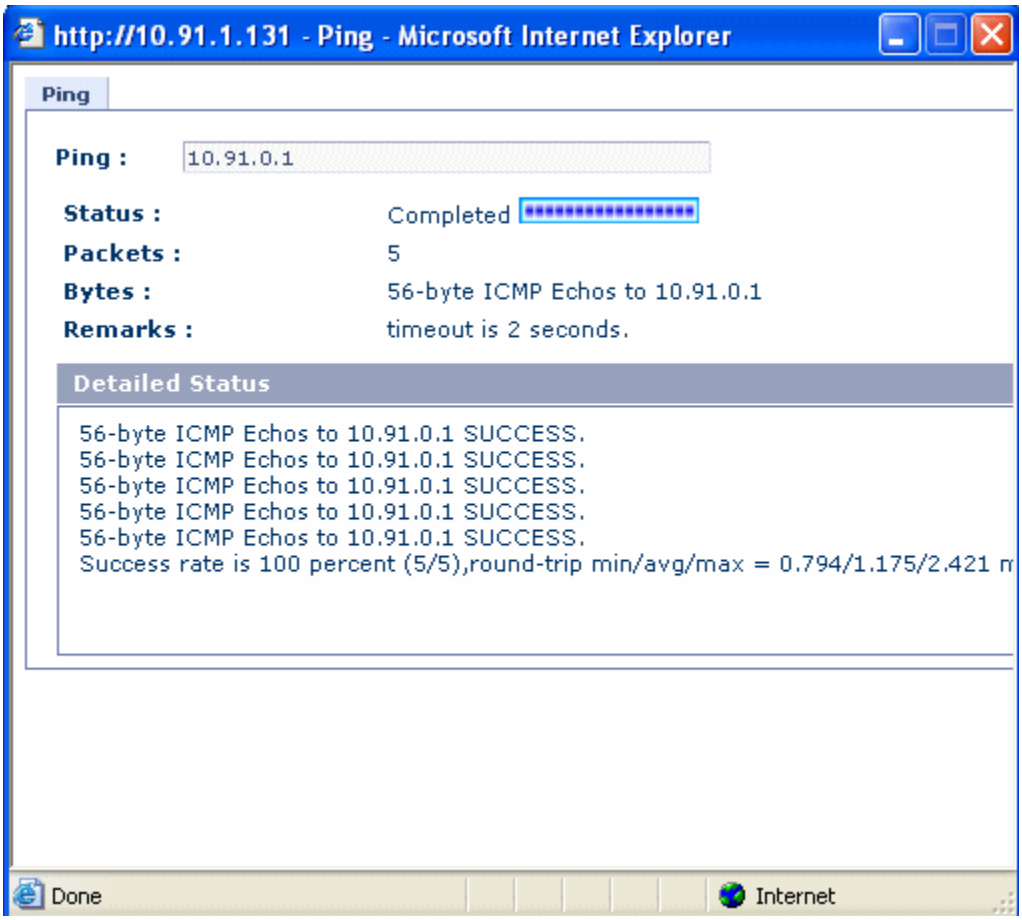


Figure 163: Maintenance: Utilities - Ping

- Enter the IP address of the remote host in the **Ping** field.
- Click **Ping**. A status bar is displayed showing the ping status.
- Once the ping is successful, the following information is displayed
  - Status - The ping status: Complete/In progress
  - Packets - The number of packets sent.
  - Bytes - Number of bytes for each packet.
  - Remarks - Time out for each packet.
  - Detailed Status - Displays the detailed ping status.

Note: You can also ping by clicking **Ping** under **Tools** menu.

TELNET

Telnet is an underlying TCP/IP protocol for accessing remote computers. Telnet is a program that enables connection to foreign or remote host computers over the internet, and provides access information on them.

When you issue a Telnet session, you connect to the Telnet host and login. The connection enables you to work with the remote machine as though you were a terminal connected to it.

Note: In order to establish Telnet connection for accessing remote computers, make sure Access Status of the Telnet protocol is **enabled**.
To do this, click **Configure** -> **System Access** -> **File Transfer & Access** tab -> Select **Telnet** check box.
For more information, see "File Transfer and Access" section in Configure chapter.

1. Click **Telnet.** The following page is displayed:

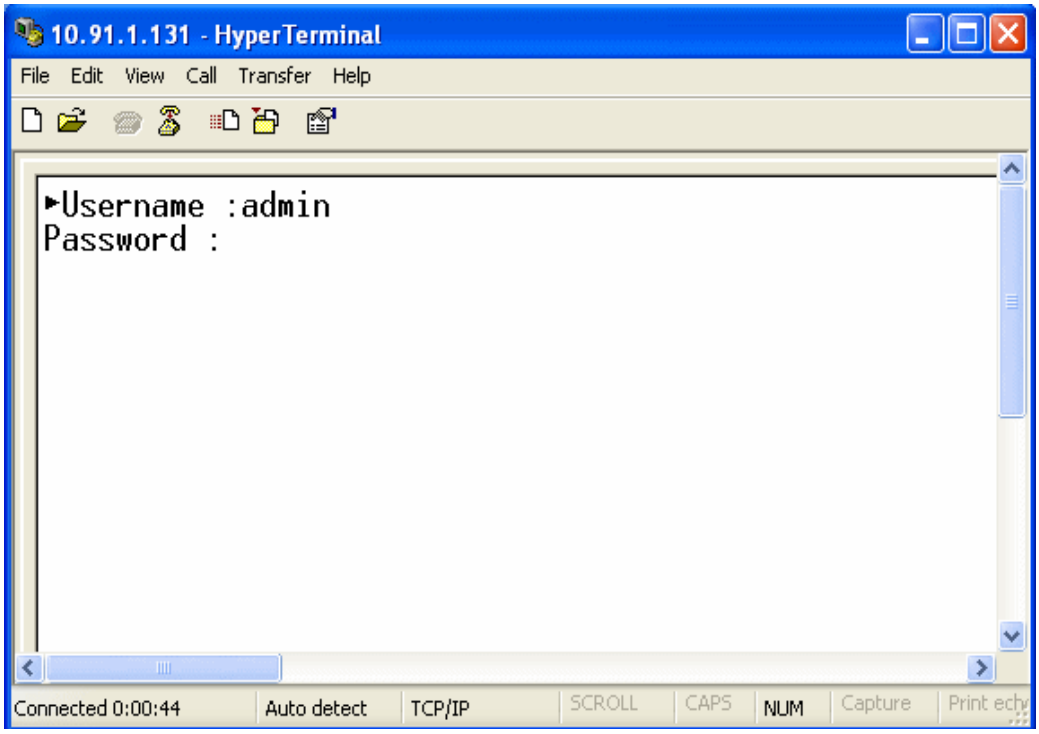


Figure 164: Maintenance: Utilities - Telnet

2. Enter the authenticated user name and the password to get the access to the remote system.

Note: You can also use Telnet by clicking **Telnet** under **Tools** menu.

LIFELINE

Note: This feature is applicable only for OA-780.

The Lifeline feature provides remote accessibility for management of the OA-780 under failure conditions. Through the Lifeline management framework, 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.

The lifeline page allows you to enable/disable lifeline functionality, and configure Lifeline routes that can be used when the system goes to the Lifeline Mode.

VIEWING LIFELINE

Follow the procedure below to view the Lifeline page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Maintenance**. All submenu/links under Maintenance are displayed in the left navigation panel as shown below.

Step 3: Click **Lifeline** sub-menu.

Lifeline page is displayed in the center panel.

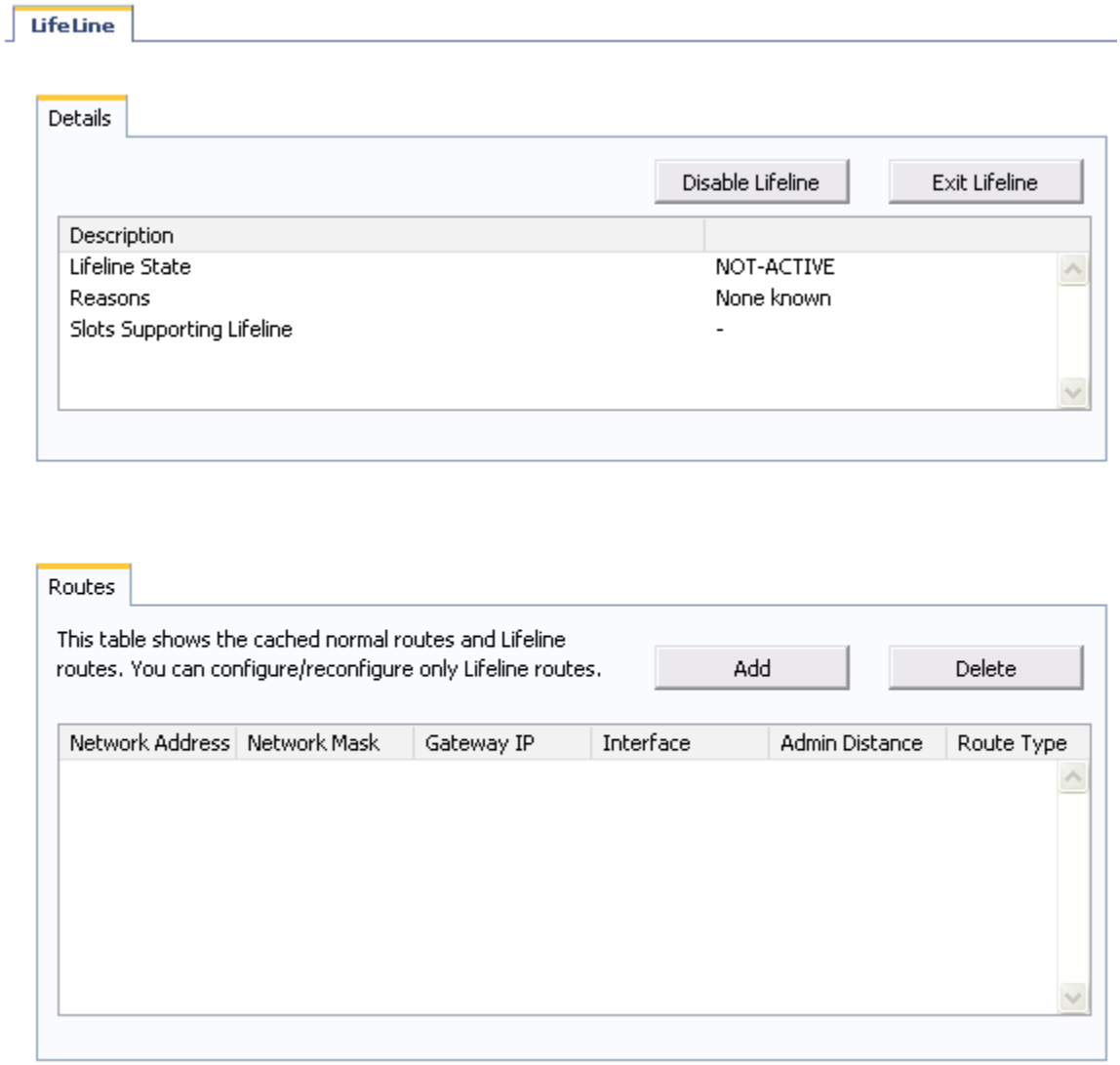


Figure 165: Maintenance: Lifeline

The table below provides field description for Lifeline page.

Table 34: Lifeline Field Description

Field	Description
LIFELINE	
Details	
Description	Displays the information about the Lifeline like the lifeline state, reason for lifeline state, and the slots supporting the lifeline.
Routes This table displays the cached normal routes and lifeline route information.	
Network Address	IP address and prefix length of the destination network.
Network Mask	Network mask of the destination network
Gateway IP	IP address of the gateway (next hop) through which the traffic is routed
Interface	IP address of the next hop interface through which the traffic is routed
Admin Distance	The administrative distance of the routing protocol
Route Type	Route type

DISABLE/ENABLE LIFELINE

You can save the enable or disable the Lifeline functionality. By default Lifeline is enabled.

1. Click **Disable Lifeline** in the **Details** table in the Lifeline page. Confirm at the prompt to disable the Lifeline functionality.
2. Once disabled, the button will change to **Enable Lifeline**. Click this button to enable the Lifeline.

EXIT LIFELINE

You can exit the Lifeline functionality.

1. Click **Exit Lifeline** in the Lifeline page. Confirm at the prompt to disable the Lifeline functionality.

CONFIGURE A STATIC ROUTE FOR LIFELINE MANAGEMENT STATION ACCESSIBILITY

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.

This page allows you to configure a special Lifeline static route, which allows you to configure a route to a management station well-known to you. This route 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.

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.

Interface Cards that are Currently Supported: T1E1 line card - all L2 encapsulation protocols available on the T1E1 ports in Normal Mode are supported in Lifeline Mode viz. HDLC, PPP and Frame Relay, and L2-GE (Layer 2) line cards.

To add a Lifeline static route, follow the procedure given below:

1. Click **Add** in the **Routes** table in Lifeline page.
2. The following age is displayed:

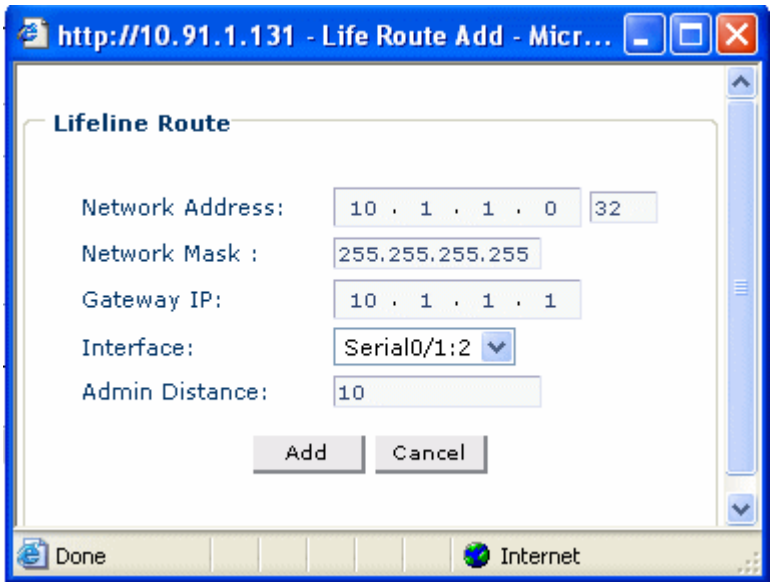


Figure 166: Add Lifeline Route

3. Configure the destination network for the static route.
   - Enter the IP address and prefix length of the destination network in the **Network Address** and **Network Mask** fields respectively.
4. Configure the Gateway Router (Next Hop) IP address or the interface through which the traffic is routed.
   - Enter the Gateway IP address in the **Gateway IP** field.
   - Select the interface from the **Interface** drop-down list.
5. Enter the administrative distance of the routing protocol in the **Admin Distance** field.
6. Click **Add** to add a new lifeline static route or click **Cancel** to cancel the operation.

DELETE LIFELINE ROUTE

1. From the Routes table, select the lifeline route to be deleted, and click **Delete**.
2. Confirm at the prompt to delete.

Note: You can also configure Lifeline by clicking **Lifeline** under **Device** menu.

UPGRADE

Note: 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 the different module versions.

The Upgrade submenu allows you to perform

- Software Upgrade
- Flash Upgrade

SOFTWARE UPGRADE

The Software Upgrade page allows you to add/install a release or a component package from the given location. The package file can be obtained from the user area or the fpkey (Front Panel key) or it can be obtained from a remote site using FTP, TFTP, HTTP or HTTPS.

It also allows to backup the default package, remove packages other than default, and to set another package as a default package.

Packages are the vehicles for software delivery on a Alcatel Lucent system. There are three kinds of packages:

1. **alu-x.<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.

VIEWING SOFTWARE UPGRADE

Follow the procedure below to view Software Upgrade page.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Maintenance**. All submenu/links under Maintenance are displayed in the left navigation panel as shown below.

Step 3: Click **Upgrade** sub-menu.

The **Upgrade** menu has two tabs: **Software Upgrade** and **Flash Upgrade**.

Select **Software Upgrade** tab. Software Upgrade page is displayed in the center panel. This displays the current software configuration.

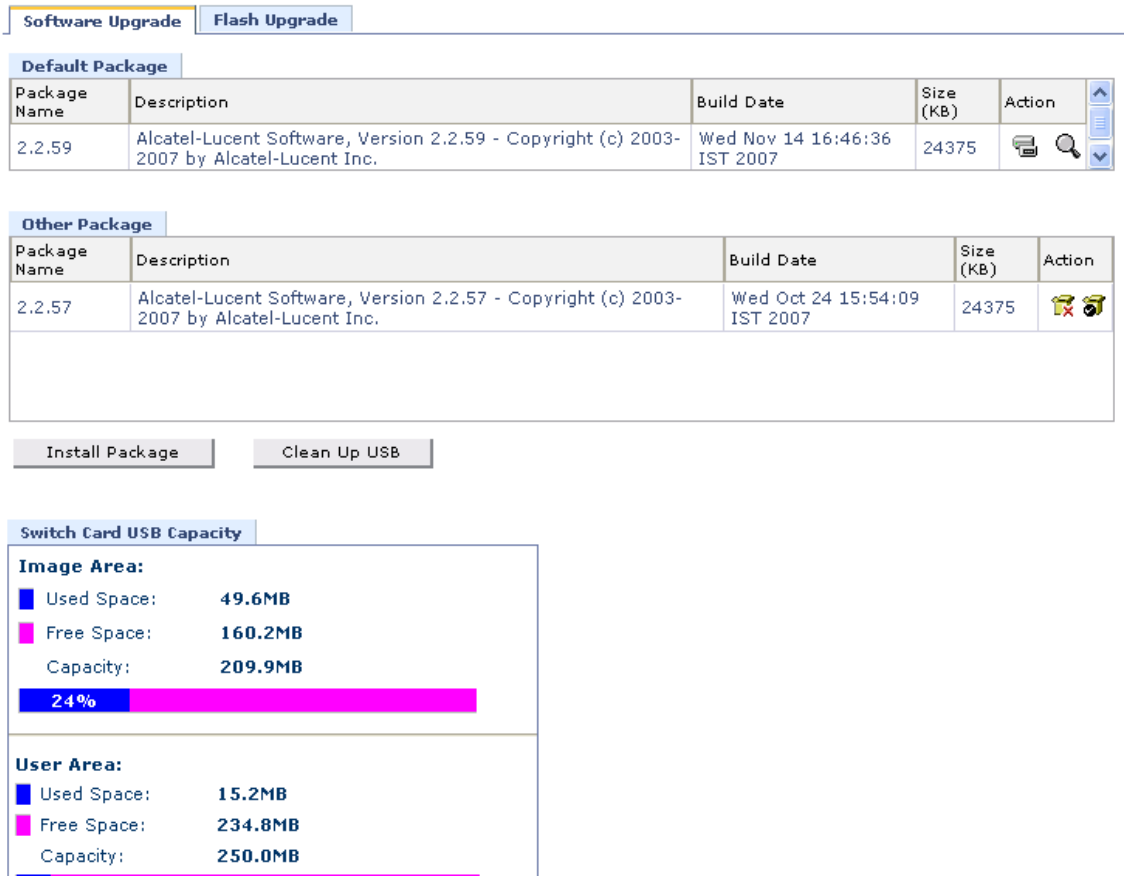


Figure 167: Maintenance: Upgrade - Software Upgrade

The table below provides field description for Software Upgrade page.

Table 35: Software Upgrade Field Description

Field	Description
DEFAULT PACKAGE	
Package Name	Name of the package currently running.
Description	Package description.
Build Date	Date the package was built.
Size (KB)	Size of the package in KB.
Action	Provides options to create a backup of the default package and to view components of the default package.
Install Package	Install a new package.
Cleanup USB	Clean up files from the USB. This deletes the selected files from the user area of the USB.
SWITCH CARD USB CAPACITY	Provides information on the capacity, used space, and free space on the image area and the user area of the Switch Card USB drive.
OTHER PACKAGE	
Package Name	Displays packages other than the Default Package. One is allowed to have multiple packages stored in the system. These package names are displayed in the Other Packages table.
Description	Package description.
Build Date	Date the package was built.
Size (KB)	Size of the package in KB.
Action	Provides option to set the selected package as the default package or remove the package.

INSTALL PACKAGE

This is used to install a release or a component package from the given location. The package file can be obtained from the user area or fpkey: or it can be obtained from a remote site using FTP, TFTP, or HTTP.

Follow the procedure below to install/upgrade a new package and its components.

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.

Step 1: Click **Install Package** in the Software Upgrade page.

Step 2: The **Package Installation Details** page is displayed**.** The package can be installed either from the device (USB) or from the remote location.

Install Package from the Device

1. Select **Package present on Device** radio button in the **Package Installation Details** page.

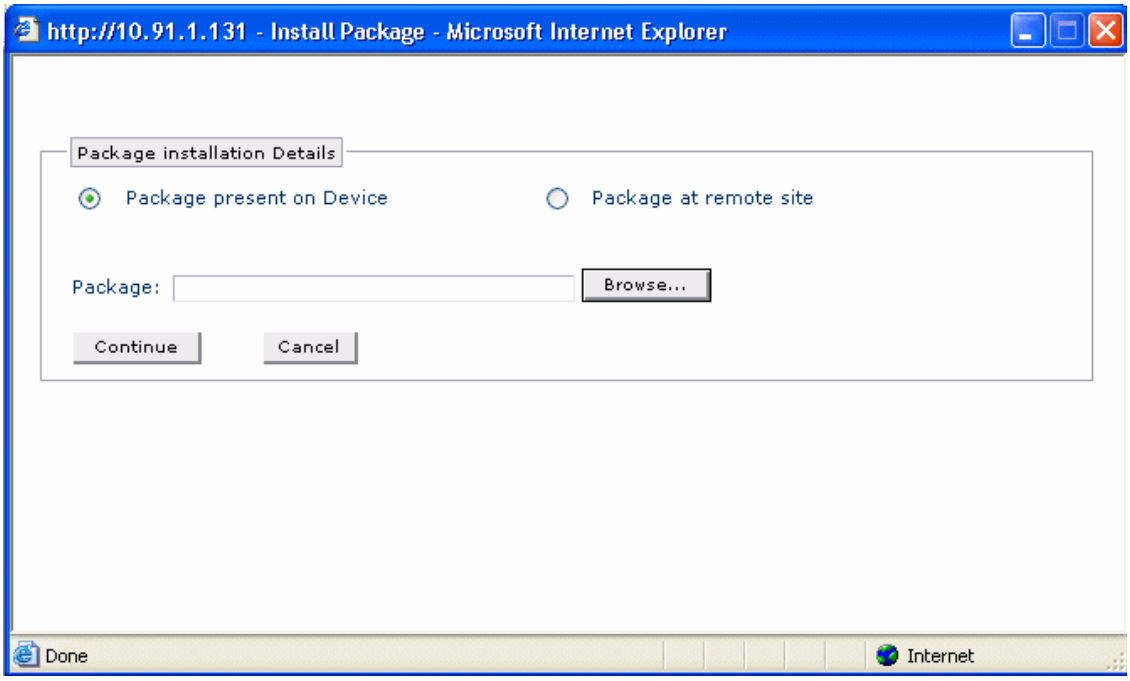


Figure 168: Upgrade: Software Upgrade - Install Package from Device

2. Click **Browse…** to select the path for the package.The browser page opens up.

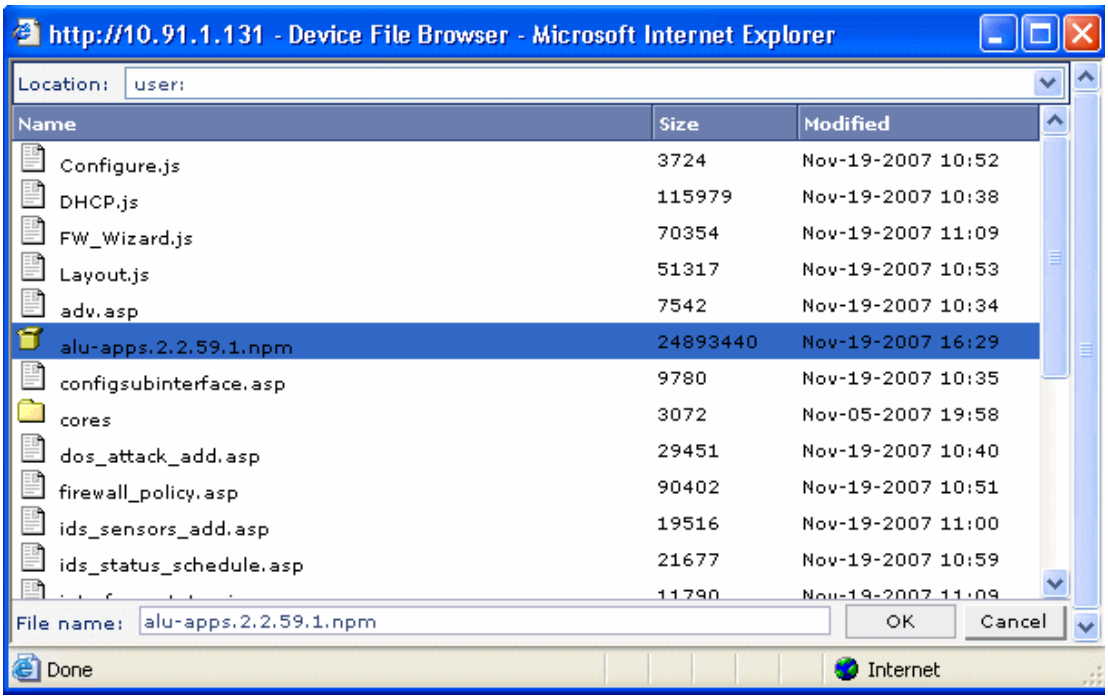


Figure 169: Upgrade: Software Upgrade - Install Package from Device - Browser page

3. Select the required file and click **OK**.
4. Click **Continue** to install the package or click **Cancel** to quit installing the package.
   - Clicking Continue verifies the package and leads to next page based on the **Package Type** being installed, and also if the verification succeeds.

     There can be two kinds of Package Type: **Release** and **Component Upgrade**.

- The following page is displayed for Package Type Release.

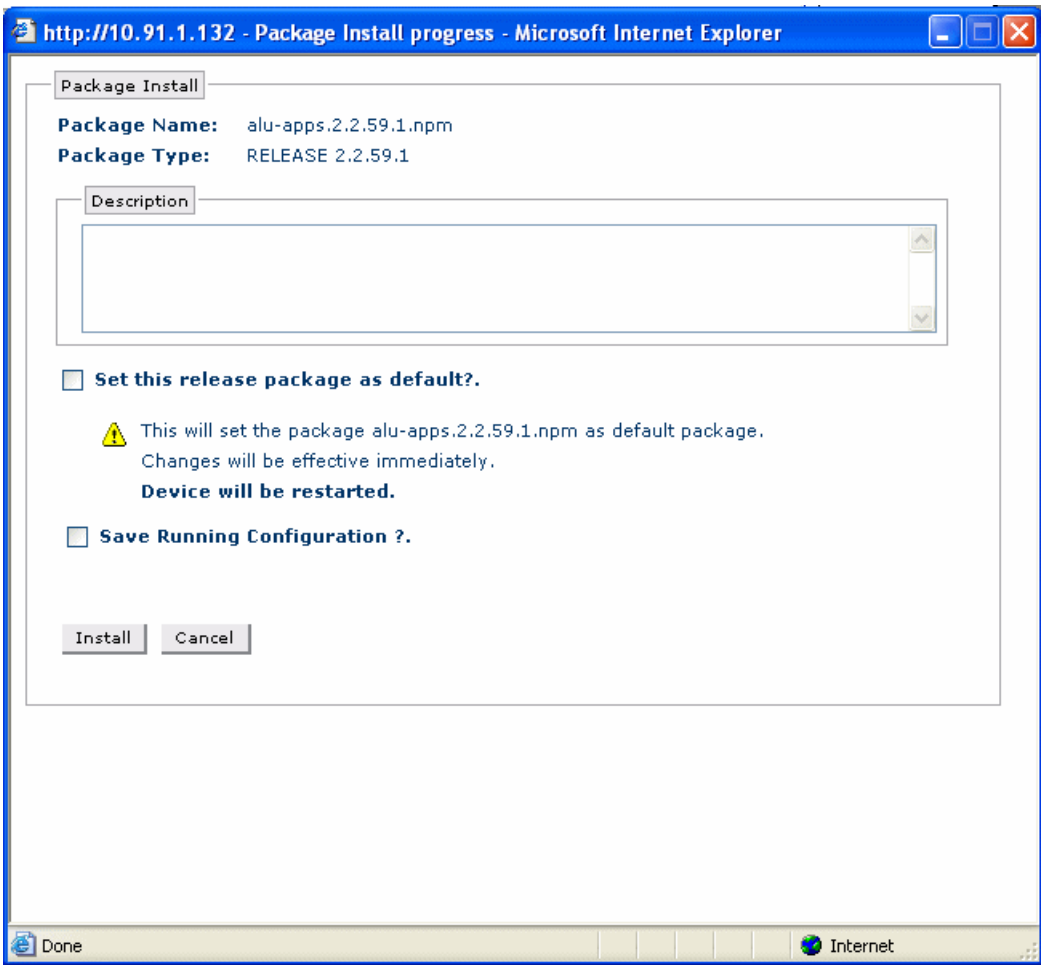


Figure 170: Upgrade: Software Upgrade - Install Package from Device (b)

- Select **Set this release package as default** check box to set the package as default. If this is done, the changes will come into effect immediately and the box will be restarted.

  If the above check box is not selected, then the package installed will be displayed in the Other Package table.
- Select the **Save Running Configuration** check box to save the running configuration. Once the system is rebooted, the system will boot up with the saved running configuration.

5. Click **Install**. This instals the new package.

Install Package from Remote Site

1. Select **Package at remote site** radio button in the **Package Installation Details** page.

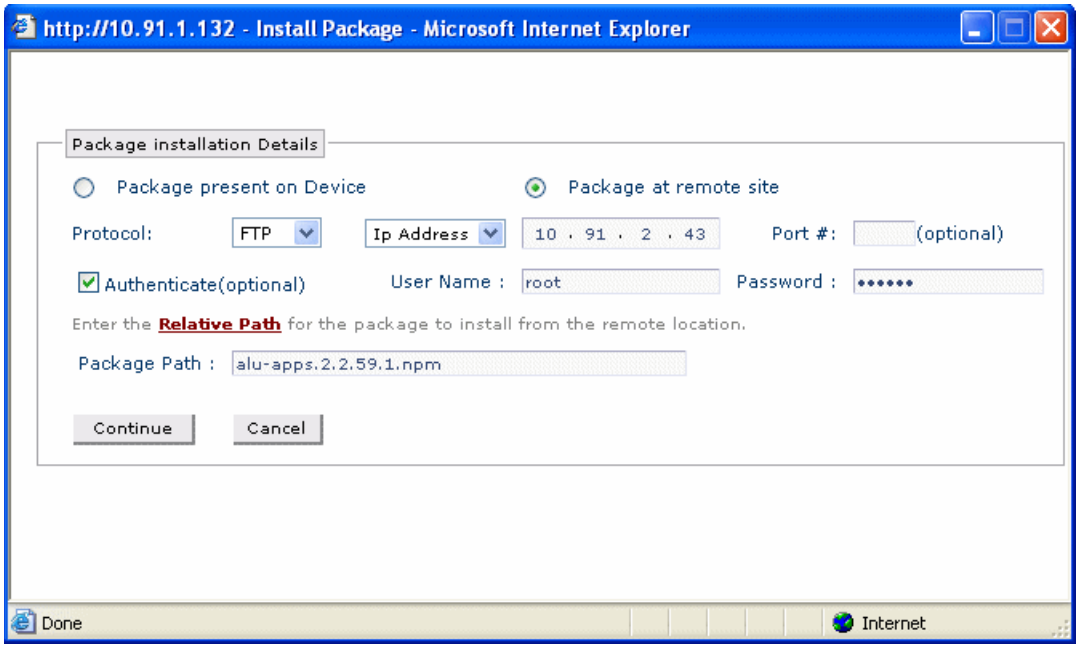


Figure 171: Upgrade: Software Upgrade - Install Package from Remote Site (a)

2. Select protocol from the **Protocol** list: HTTP/FTP/TFTP
3. Enter IP address/Host Name of remote host in **IP Address/Host Name** field. Entering port number of the remote site in the **Port #** field is optional.
4. Authentication at the remote site is optional. If remote site requires you to authenticate, check (select) the **Authenticate** check box. enter the user name *in the* **User Name** field and the password in **Password** field. **Authenticate is applicable only for HTTP/FTP protocol**.
5. Enter the relative path of the package to be installed from the remote site in **Package Path** field.
6. Click **Continue** or click **Cancel** to quit installing the package at any time.
   - Clicking Continue verifies the package and leads to next page based on the **Package Type** being installed, and also if the verification succeeds.

     There can be two kinds of Package Type: **Release** and **Component Upgrade**.

- The following page is displayed for Package Type Release.

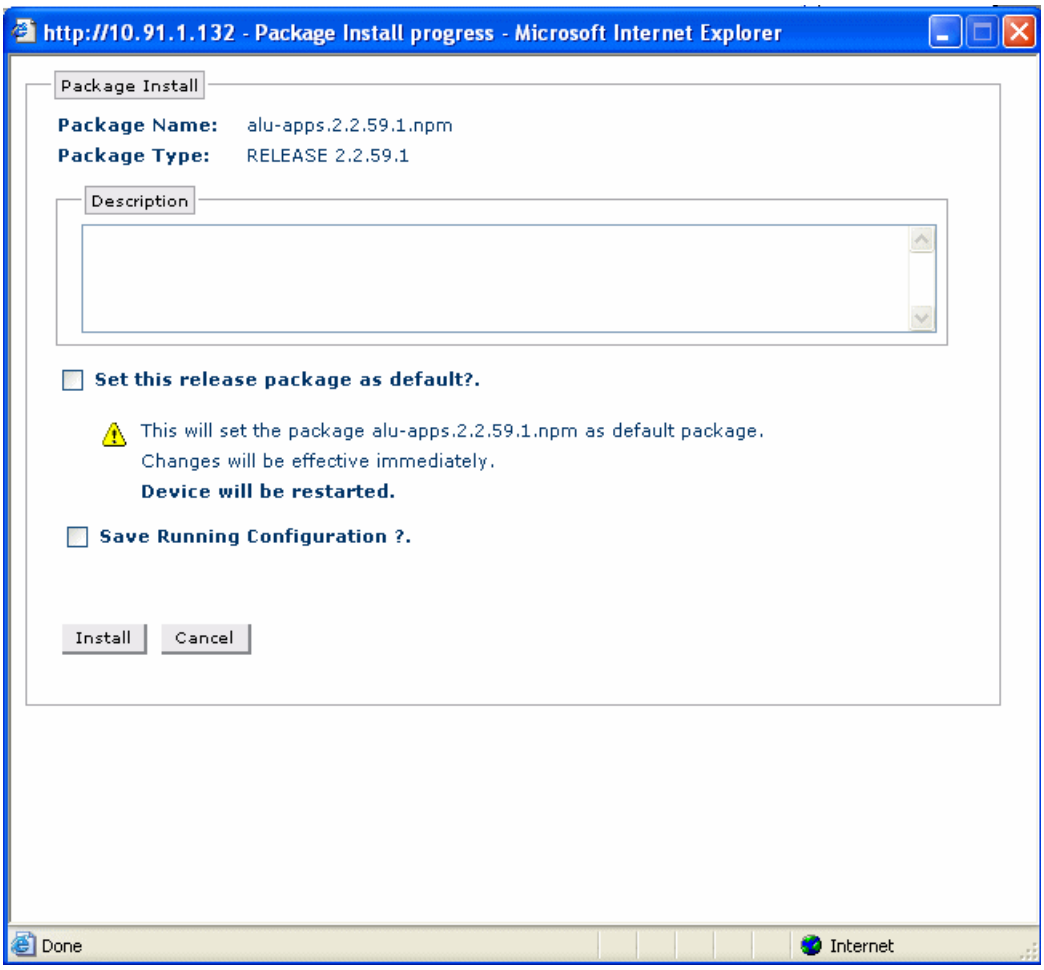


Figure 172: Upgrade: Software Upgrade - Install Package from Remote Site (b)

- Select **Set this release package as default** check box to set the package as default. If this is done, the changes will come into effect immediately and the box will be restarted.

  If the above check box is not selected, then the package installed will be displayed in the Other Package table.
- Select the **Save Running Configuration** check box to save the running configuration. Once the system is rebooted, the system will boot up with the saved running configuration.

7. Click **Install**. This instals the new package.

BACKUP DEFAULT PACKAGE

This is used to back-up the default package at a given destination.

The backup file can be stored in the user area or fpkey. It can also be sent to a remote location using FTP or TFTP.

Note: You can only take a backup of the default package.

Step 1: Click **Backup Default Package** icon in the Software Upgrade page. **Backup Details** page is displayed**.**

Step 2: The package backup can be taken either on the device (USB) or at the remote location.

Backup Package on the Device

1. Select **Backup Package on USB Device** radio button in the **Backup Details page**.

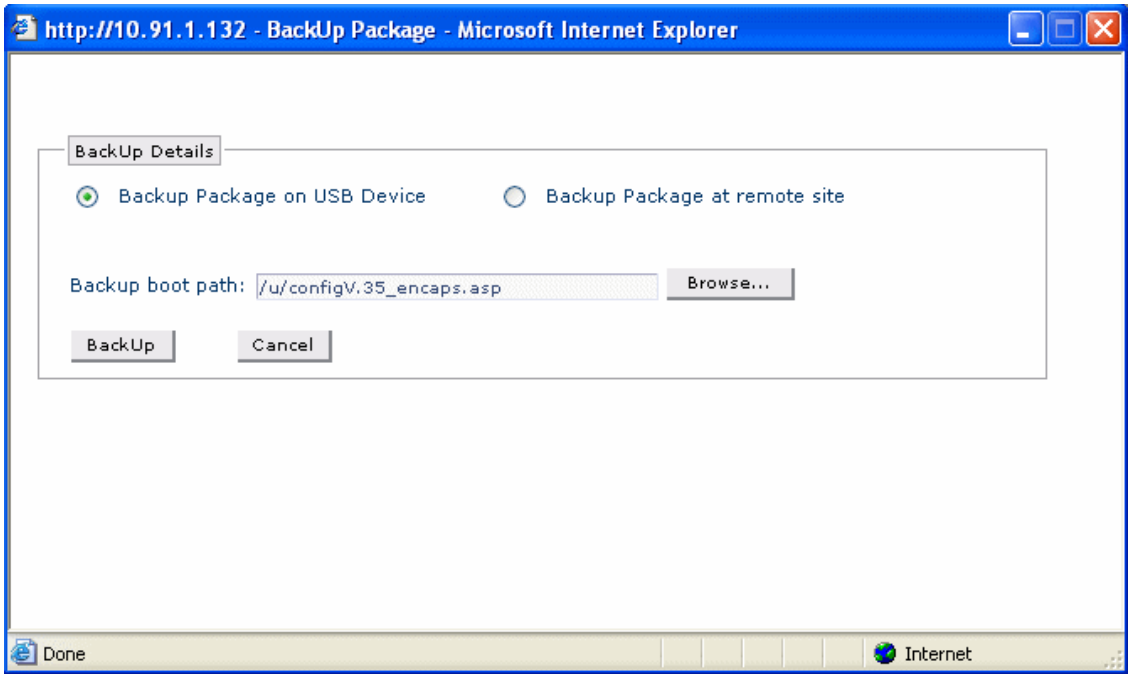


Figure 173: Upgrade: Software Upgrade - Backup Package on USB Device

2. Click **Browse...** to select the path for taking backup of default package.The Browser page opens up. Select the file and click **OK.**
3. Click **Backup** to backup the package.

Backup Package at Remote Site

1. Select **Backup Package at remote site** radio button in the **Backup Details** page.

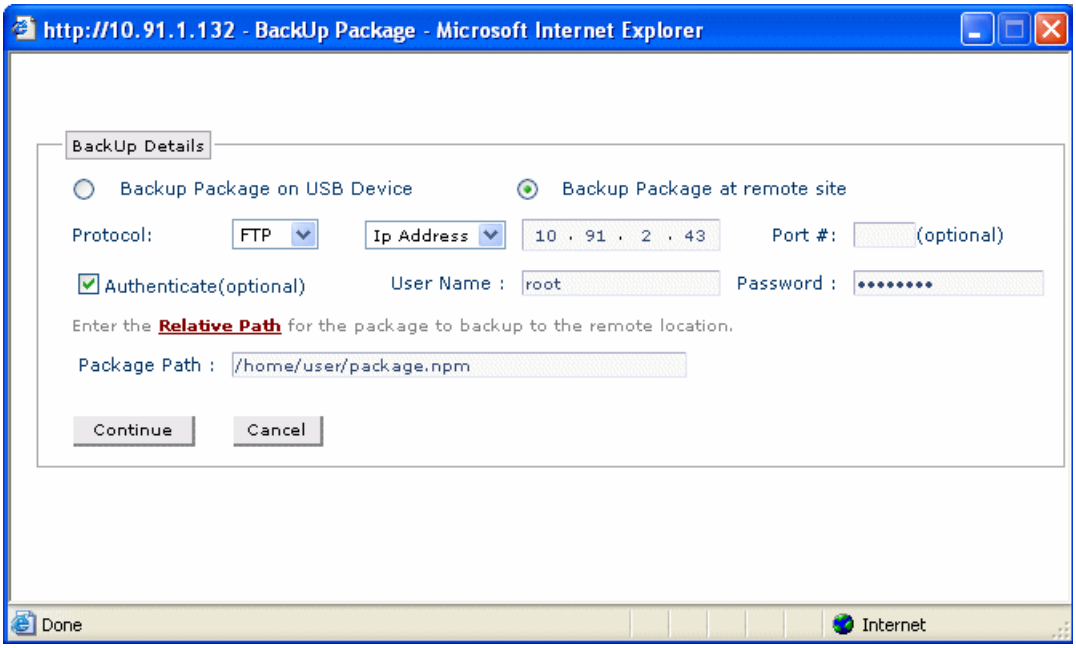


Figure 174: Upgrade: Software Upgrade - Backup Package at Remote Site

2. Select protocol from the **Protocol** list: FTP/TFTP
3. Select IP address/Host Name of remote site in **Ip Address/Host Name** field. Entering port number of the remote site in the **Port #** field is optional.
4. Authentication at the remote site is optional. If remote site requires you to authenticate, check (select) the **Authenticate** check box. Enter the user name in the **User Name** field and the password in the **Password** field. **Authenticate is applicable only for FTP protocol**.
5. Enter the relative path for the package to backup at remote location in the **Package Path** field.
6. Click **Continue** to save the default package backup in the destination path.
7. Click **Cancel** to quit the process.

SET OTHER PACKAGE AS DEFAULT PACKAGE

The package that comes with OA-700 system is always set as default package.

If you install another package and would like to set that newly installed package as default package, use the following procedure.

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.

1. Install a new package. Refer "Install Package" section to install new package. The newly installed package is listed under Other Package table.
2. Click **Set as Default** icon under the **Action** column in **Other Package** table. This opens **Set as Default** page.

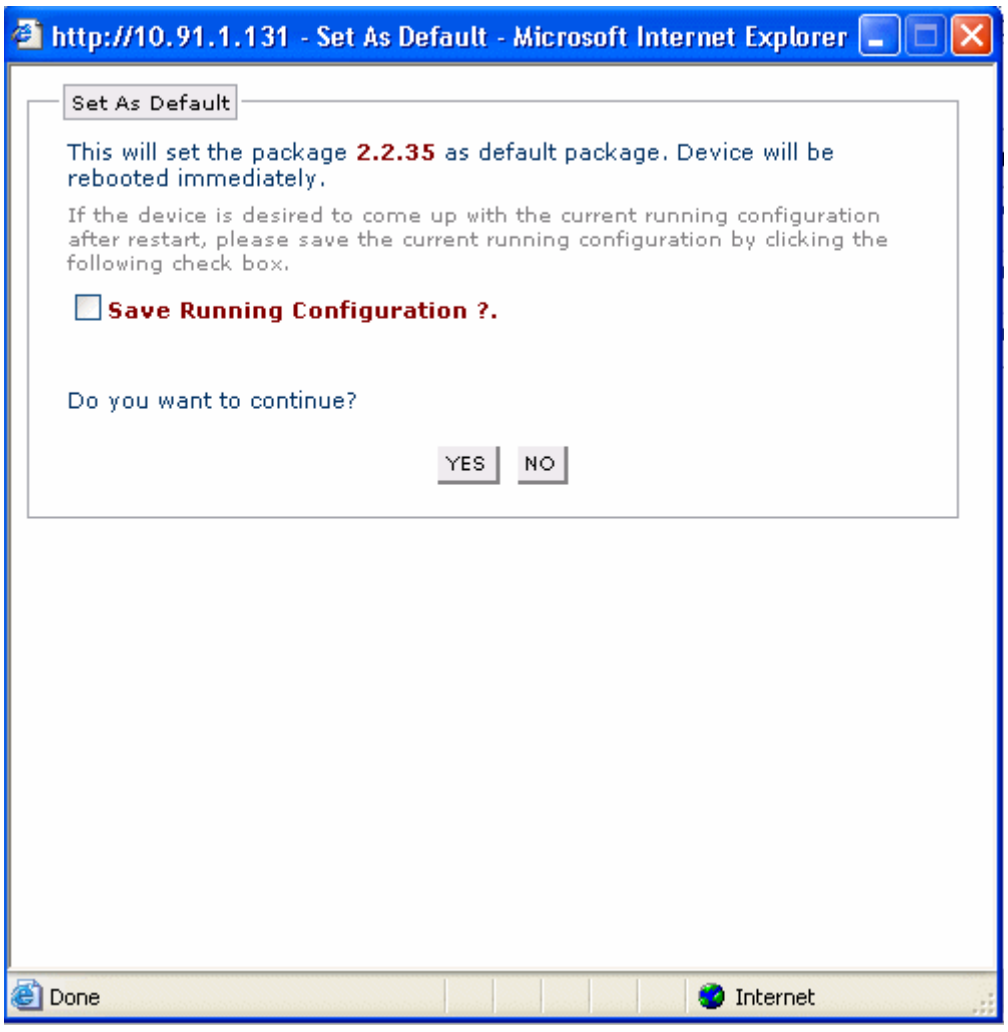


Figure 175: Upgrade: Software Upgrade - Set Default Package

3. Select **Save Running Configuration** check box to save the running configuration.
4. Click **Yes** to continue to confirm setting the selected package as default or click **No** to cancel the operation.

VIEW PACKAGE COMPONENTS

The Component Details pop up window shows the components present in the running package.

1. To view all the components in the package, click **View Components** icon under the **Action** column in **Default Package** table.
2. The details such as component name, component version, and the component size (in kilobytes), and the total number of components in the package is displayed in the **Component Details** pop up window.

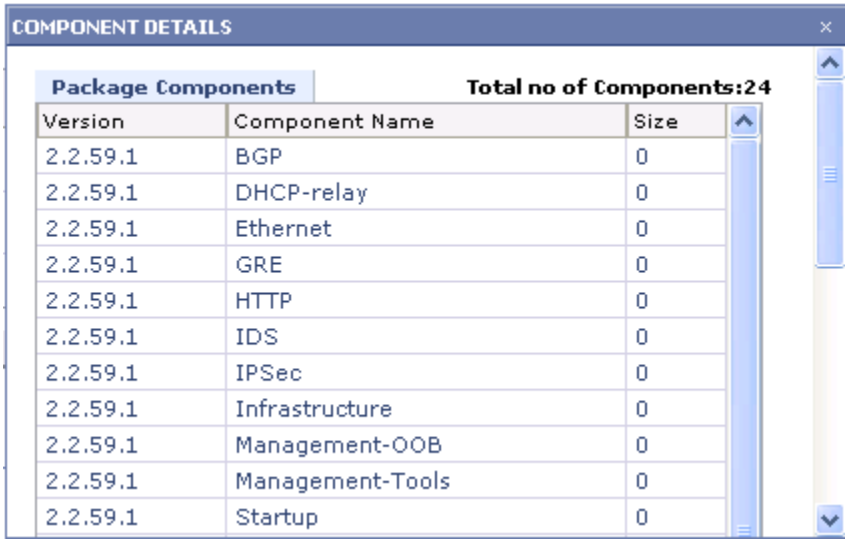


Figure 176: Upgrade: Software Upgrade - Package Component Details

CLEANUP USB

The Software Upgrade page provides an option to clean up the files on the USB.

1. To cleanup files from USB, click on **Cleanup USB**. **USB Cleanup** page is displayed.

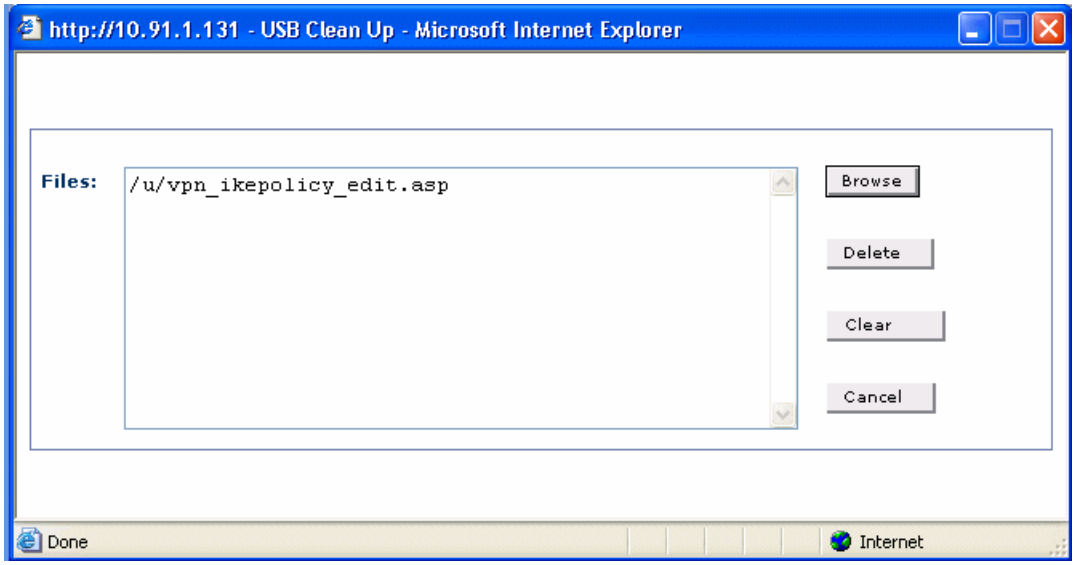


Figure 177: Upgrade: Software Upgrade - Cleanup USB

2. Click **Browse** to select the files to be deleted. The files selected is displayed in the **Files** box.
3. Click **Delete** to delete the selected files.
4. Click **Clear** to clear the file selection and add new files for deletion.
5. Click **Cancel** to cancel the cleanup operation.

REMOVE PACKAGE

1. To remove a package, click **Remove Package** icon under the **Action** column in **Other Package** table.
2. Confirm at the prompt to remove the package.

Note: The default package cannot be removed.

FLASH UPGRADE

The Flash Upgrade page installs a flash image on all the cards. The package file can be installed from the user:area or fpkey, or it can be obtained from a remote location using FTP, TFTP, HTTP or HTTPS.

VIEWING FLASH UPGRADE

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Maintenance**. All submenu/links under Maintenance are displayed in the left navigation panel as shown below.

Step 3: Click **Upgrade** sub-menu.

The **Upgrade** menu has two tabs: **Software Upgrade** and **Flash Upgrade**.Select **Flash Upgrade** tab. Flash Upgrade page is displayed in the center panel.

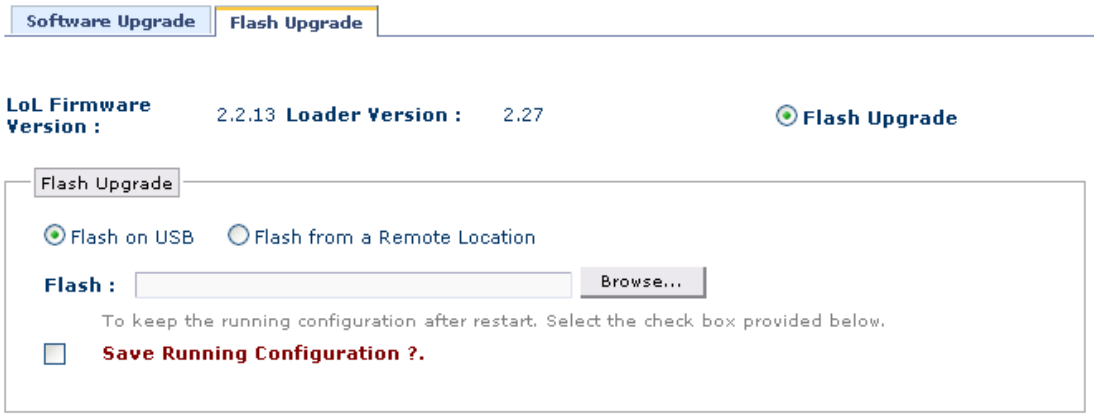


Figure 178: Upgrade: Flash Upgrade

The table below provides field description for Flash Upgrade page.

Table 36: Flash Upgrade Field Description

Field	Description
FLASH UPGRADE	
Flash	Version of the flash.
Red Boot Version	Version of Red Boot.
Flash Upgrade	Upgrade flash either from USB or from a remote site.
Flash Upgrade	Select this radio button to upgrade flash.

UPGRADING FLASH IMAGE

Follow the procedure below to upgrade the flash image

Step 1: Select **Flash Upgrade** radio button in the **Flash Upgrade** page.

Step 2: Flash Upgrade box displays two different options to upgrade the package. The package can be installed either from the device (USB) or from the remote location.

Upgrade Flash on USB Device

1. Select **Flash on USB** radio button in the **Flash Upgrade** box.

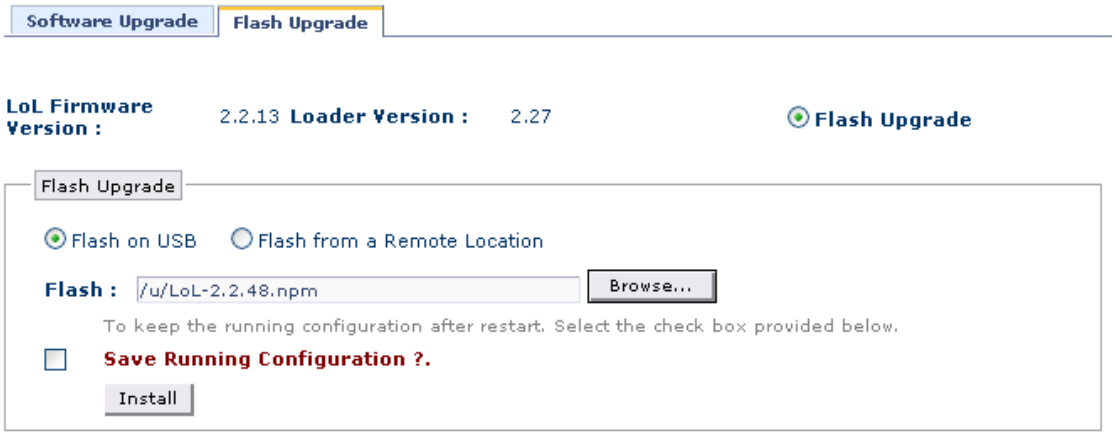


Figure 179: Upgrade: Flash Upgrade - Flash Upgrade on USB

2. Click **Browse…** to select the path for the flash in the USB drive.
3. Select **Save Running Configuration** check box to save the running configuration to the startup configuration.

4. Click **Install** to upgrade the flash. Install button is displayed only when the flash is selected after clicking the **Browse.**
5. System restarts and the new flash image is installed in the system.

Upgrade Flash from a Remote Location

1. Select **Flash from a Remote Location** radio button in the **Flash Upgrade** box.

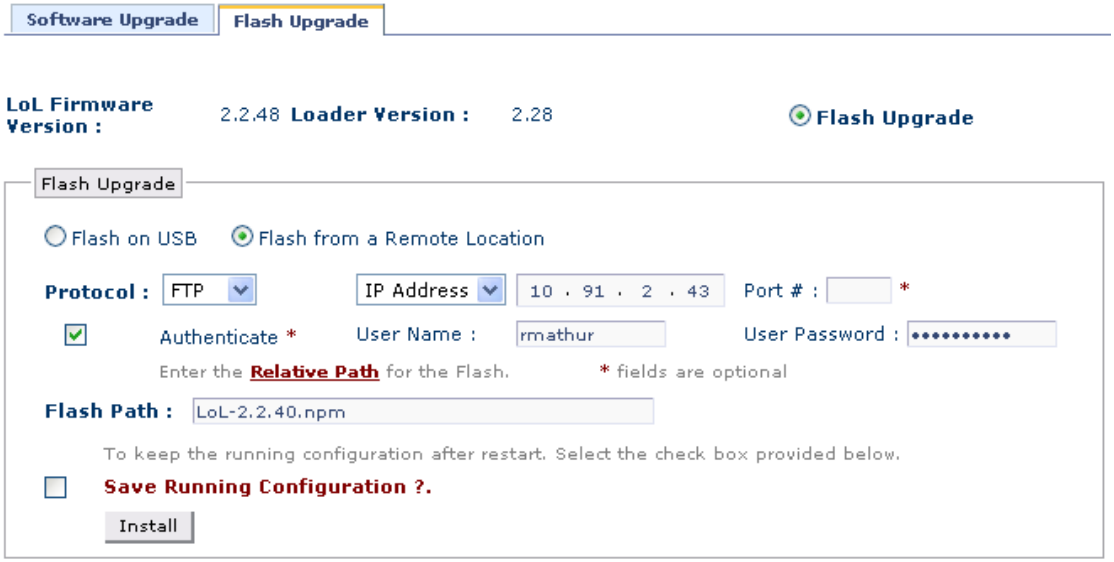


Figure 180: Upgrade: Flash Upgrade - Flash Upgrade from a Remote Location

2. Select the transfer protocol from the **Protocol** list.
3. Select the IP address/Host Name of the remote site in **Ip Address/Host Name** field. Entering port number of the remote site in the **Port #** field is optional.
4. Authentication at the remote site is optional. If remote site requires you to authenticate, check (select) the **Authenticate** check box. Enter the user name **User Name** field and the password in **User Password** field. **Authenticate is applicable only for HTTP/FTP protocol.**
5. Enter the relative path of the Flash to be installed from the remote site in the **Flash Path** field.
6. Select **Save Running Configuration** check box to save the running configuration to the startup configuration.
7. Click **Install** to install the flash image.
8. System restarts and the new flash image is installed in the system.

CHAPTER 5

MONITOR

MONITOR

This menu displays the statistics of the various services configured on the system such as Firewall, Interfaces, IPSec VPN, IPS, QoS, Active Routes.

From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel.

INTERFACE STATISTICS

The Interface page displays the details of all the interfaces configured on the OA-700 system.

VIEWING INTERFACE STATISTICS

Follow the procedure below to view the Interface statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Interface Statistics** sub-menu.

Interfaces page displays the details of all the interfaces configured on the system in the center panel.

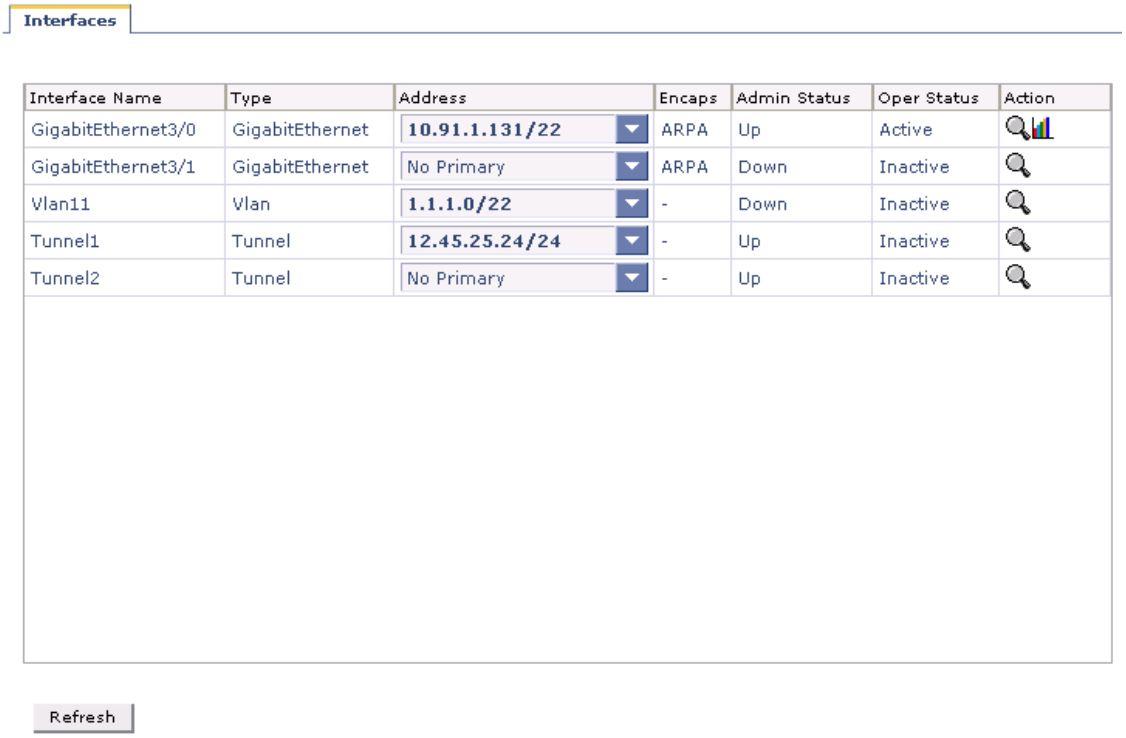


Figure 181: Monitor: Interfaces Statistics

The table below provides description for interfaces page.

Table 37: Interfaces Statistics Field Description

Field	Description
INTERFACES	
Interface Name	Name of the interface configured on the system.
Type	Interface type configured.
Address	IP address assigned to the interface.
Encaps	Encapsulation configured on the interface.
Admin Status	Indicates if the interface is administratively up or down.
Oper Status	Indicates if the interface is active or inactive.
Action	Provides option to view the interface statistics.
Refresh	Refresh the Interface Statistics page

TO VIEW INTERFACES STATISTICS

Follow the procedure given below to view the statistics of a selected interface:

1. In the **Interfaces** page, click **View** icon in the **Action** column against the interface whose statistics are to be viewed.
2. The interface statistics is displayed in a pop up window as shown below:

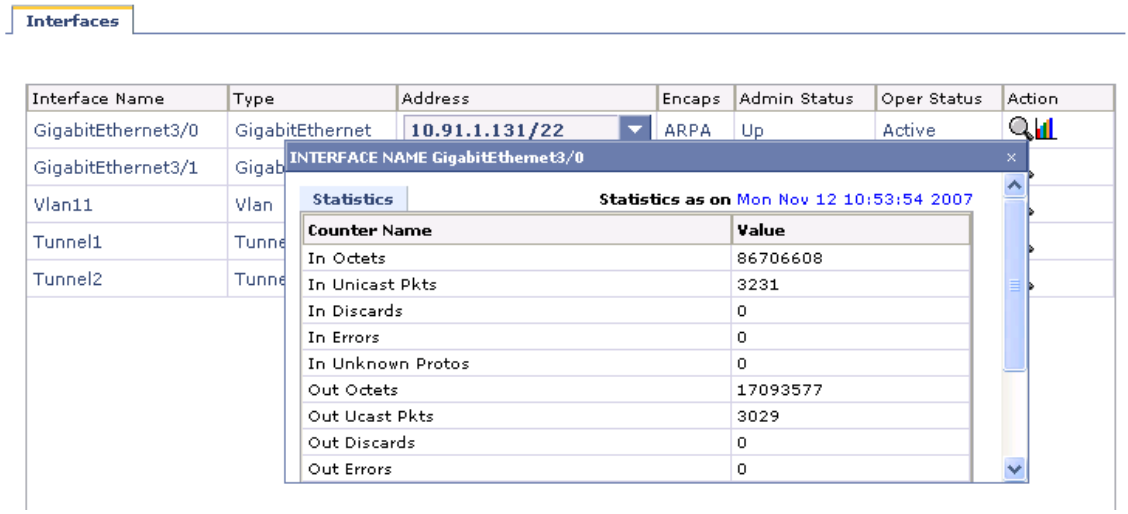


Figure 182: Monitor: Interfaces Statistics - View Interface Statistics

TO VIEW GRAPHICAL REPRESENTATION OF INTERFACE STATISTICS

Follow the procedure given below to view the statistics of a selected interface in a graphical representation:

1. In the **Interfaces** page, click **Real Time Graph** icon in the **Action** column against the interface whose statistics are to be viewed.
2. The graphical representation of the interface statistics is displayed in a pop up window as shown below:

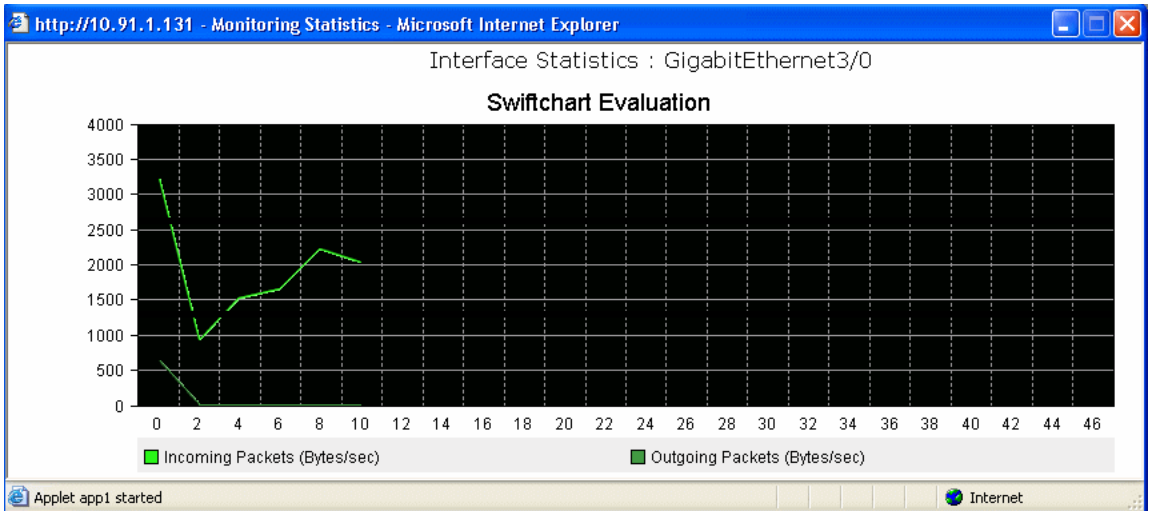


Figure 183: Monitor: Interfaces Statistics - View Interface Statistics

3. The graph shows the real time statistical details -the number of packets sent and received on an interface (Bytes/sec).

DHCP BINDINGS

The DHCP Bindings page displays all the dynamically assigned leases (the IP addresses allocated to the hosts) of all the network pools and manually linked leases of all the host pools.

VIEWING DHCP BINDINGS

Follow the procedure below to view the DHCP Bindings.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **DHCP Bindings** sub-menu.

The following page is displayed in the center panel.

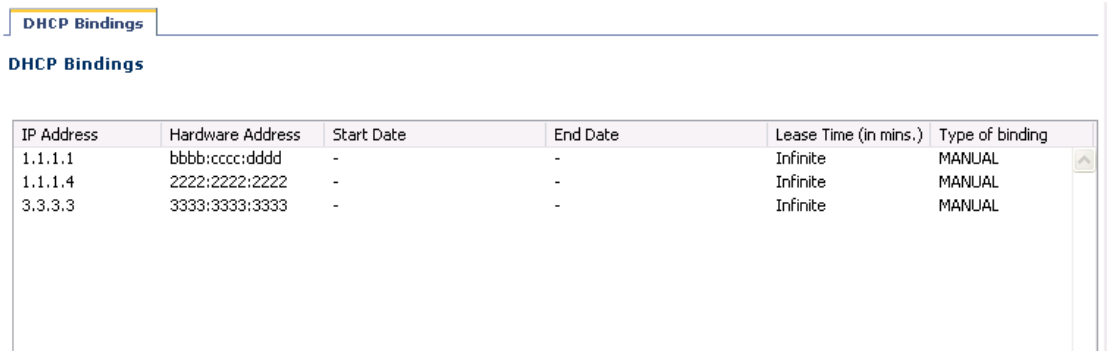


Figure 184: Monitor: DHCP Bindings

The table below provides description for DHCP Bindings page.

Table 38: DHCP Bindings Field Description

Field	Description
DHCP BINDINGS	
IP Address	IP address allocated to the host
Hardware Address	Hardware address of the host.
Start Date End Date	Specifies the start date and end date for which the clients can use the IP address assigned to them.
Lease Time	Specifies the time for which the clients can use the IP address assigned to them. **This will be 'Infinite' for Manual bindings.**
Type of Binding	Displays the type of DHCP binding: Dynamic/Manual

ACTIVE ROUTES

This menu displays the information about the active routes.

VIEWING ACTIVE ROUTES

Follow the procedure below to view the Active Route statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Active Routes** sub-menu.

Active Route Details page displays the details of all the active routes configured on the system in the center panel.

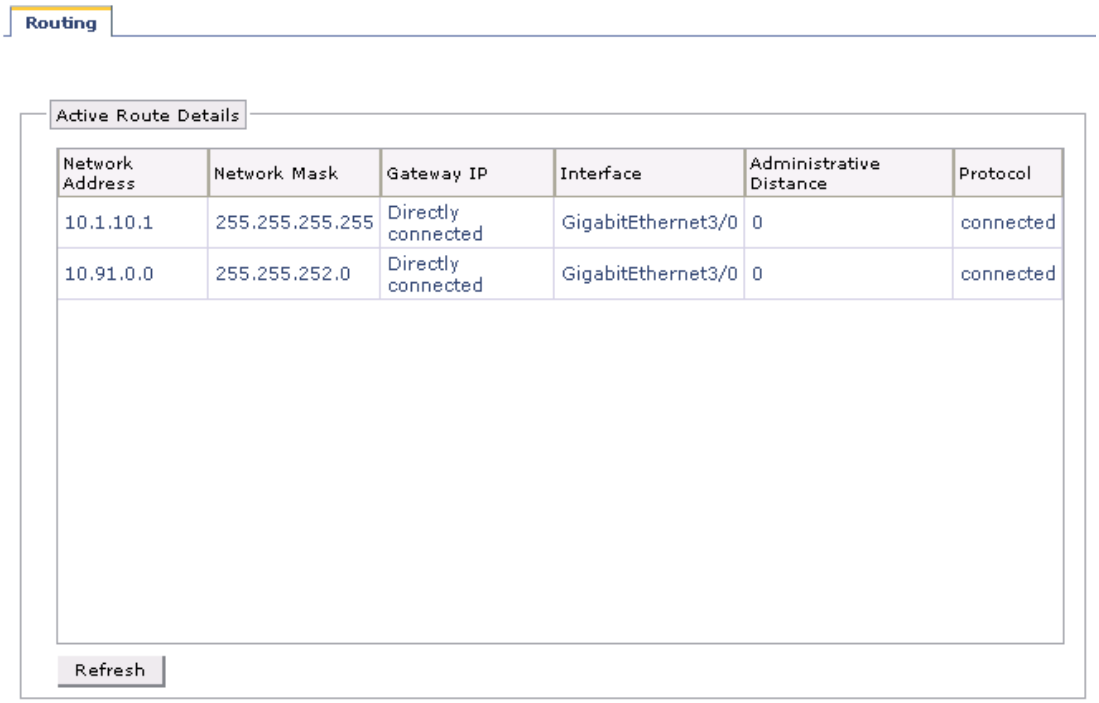


Figure 185: Monitor: Active Route Details

The table below provides field description for Active Routes page.

Table 39: Active Routes Field Description

Field	Description
ACTIVE ROUTE DETAILS	
Network Address	IP address of the destination network
Network Mask	Network mask of the destination network
Gateway IP	IP address of the gateway through which the traffic is routed
Interface	IP address of the interface through which the traffic is routed
Administrative Distance	The administrative distance of the routing protocol
Protocol	Static/Connected/Protocol type (RIP, OSPF, etc.)
Refresh	Update the Active Routes page.

TRAFFIC STATISTICS

This page displays the IP and ICMP statistics.

IP STATISTICS

This page displays the IP Statistics.

VIEWING IP STATISTICS

Follow the procedure below to view the IP statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Traffic Statistics** sub-menu.

The Traffic Statistics has two tabs: **IP Statistics** and **ICMP Statistics**. By default, **IP Statistics** tab is selected and IP Statistics page is displayed in the center panel.

The IP Statistics page allows to view the IP statistical details. It displays received, sent, fragment and other parameter counter values.

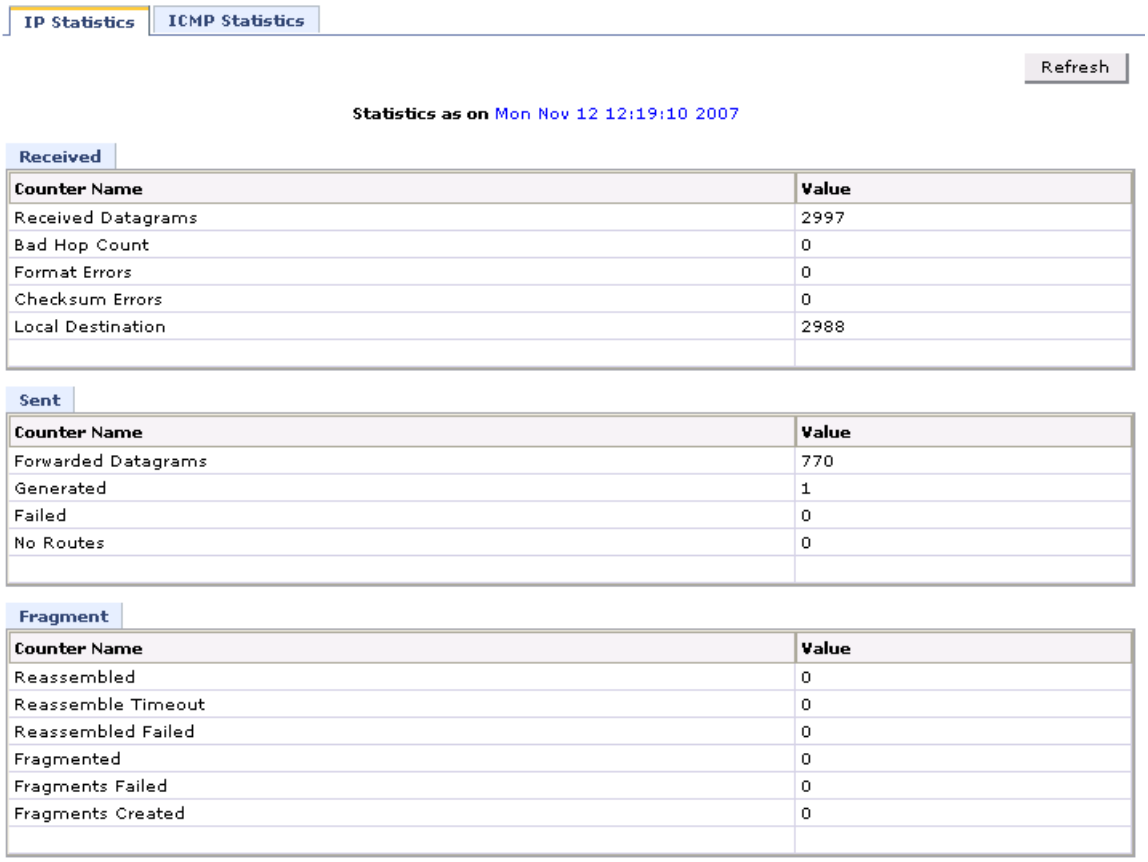


Figure 186: Monitor: Traffic Statistics - IP Statistics

The table below provides description for Traffic Statistics - IP Statistics page.

Table 40: IP Statistics Field Description

Field	Description
IP STATISTICS	
Other Parameters	
Counter Name	Counters supported
Value	The value of each of the counters
Received	
Counter Name	Counters supported for incoming traffic
Value	The value of each of the counters
Sent	
Counter Name	Counters supported for outgoing traffic
Value	The value of each of the counters
Fragment	
Counter Name	Counters supported
Value	The value of each of the counters
Refresh	Refresh the IP Statistics page

ICMP STATISTICS

This page displays the ICMP Statistics.

VIEWING ICMP STATISTICS

Follow the procedure below to view the ICMP statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Traffic Statistics** sub-menu.

The Traffic Statistics has two tabs: **IP Statistics** and **ICMP Statistics**.

Step 4: Click **ICMP Statistics** tab.

The ICMP Statistics page displays the ICMP statistical details like the received and sent counter values.

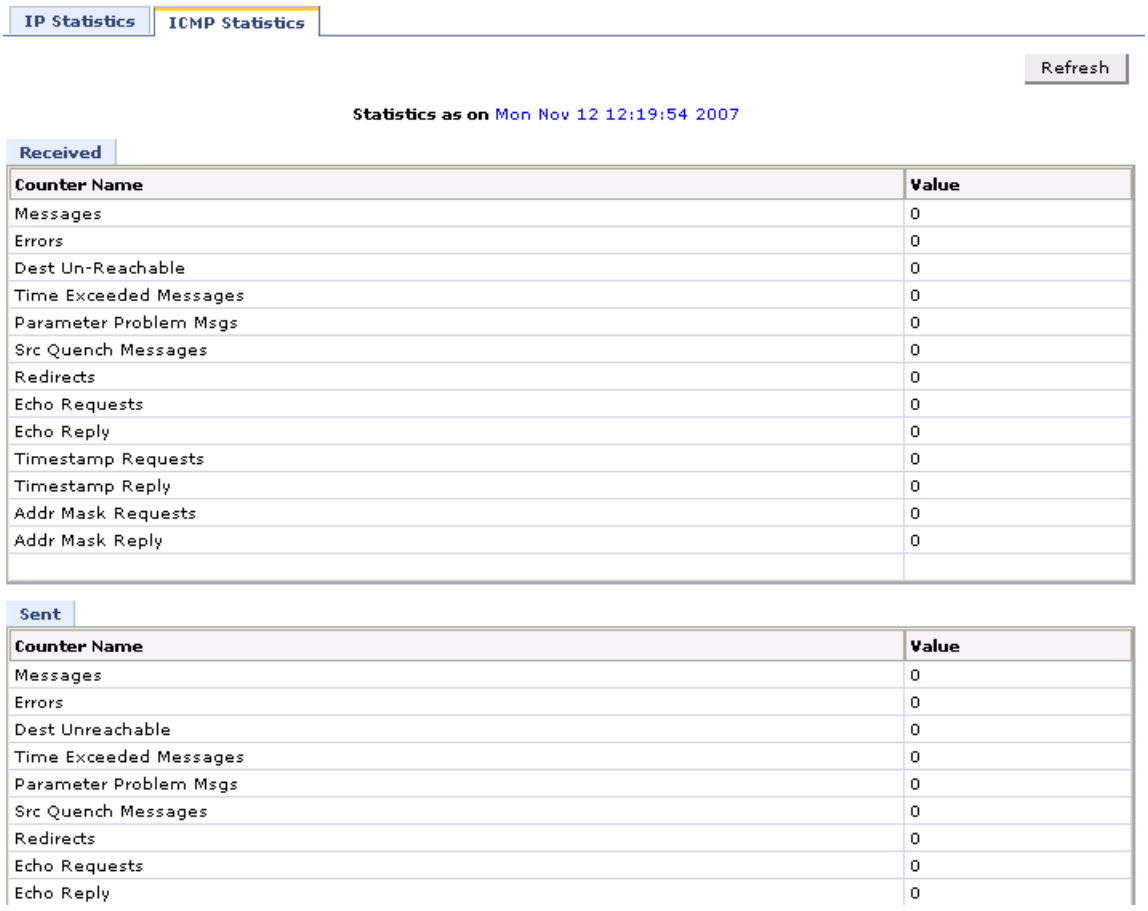


Figure 187: Monitor: Traffic Statistics - ICMP Statistics

The table below provides description for Traffic Statistics - ICMP Statistics page.

Table 41: ICMP Statistics Field Description

Field	Description
ICMP STATISTICS	
Sent	
Counter Name	Counters supported
Value	The value of each of the counters
Received	
Counter Name	Counters supported
Value	The value of each of the counters
Refresh	Refresh the ICMP Statistics page

SNMP STATISTICS

This menu displays the information about the SNMP Statistics.

VIEWING SNMP STATISTICS

Follow the procedure below to view the SNMP Statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **SNMP Statistics** sub-menu.

SNMP Statistics page displays the SNMP statistics in the center panel.

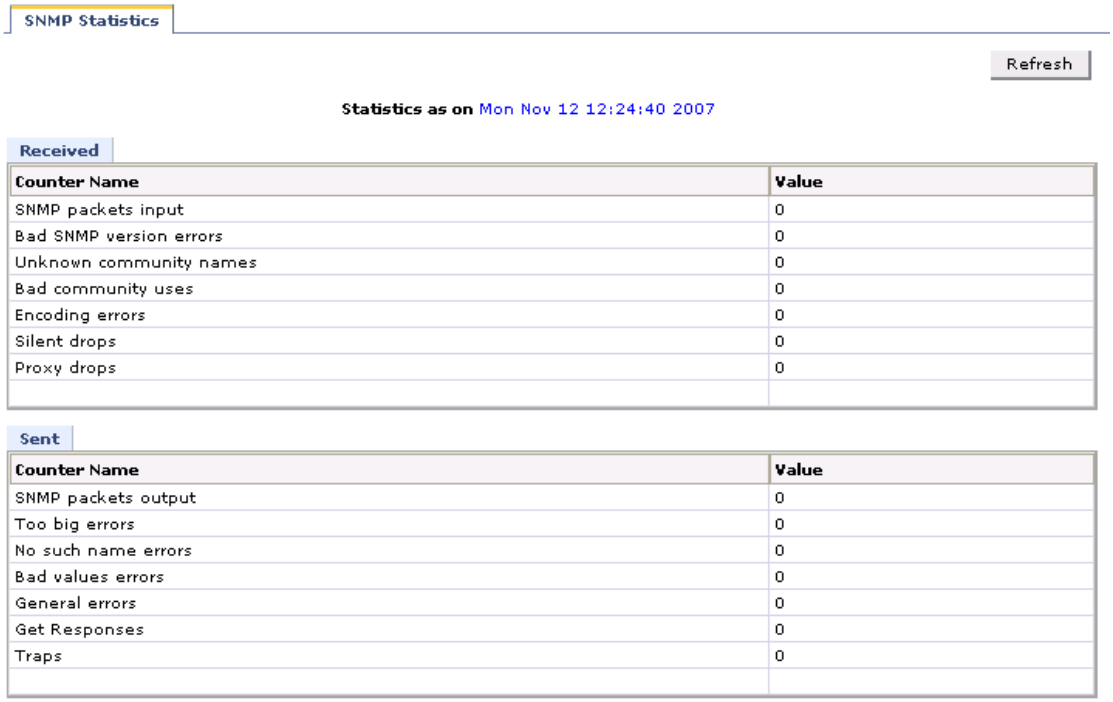


Figure 188: Monitor: SNMP Statistics

The table below provides field description for Active Routes page.

Table 42: SNMP Statistics Field Description

Field	Description
SNMP STATISTICS	
Received	
Counter Name	Number of SNMP requests received.
Value	The value of each of the counters
Sent	
Counter Name	Number of SNMP requests sent.
Value	The value of each of the counters

FIREWALL SESSION STATISTICS

This page displays the Firewall Session Statistics. The Firewall Session Summary section displays information about the different sessions maintained by the Firewall module. The Firewall Session Details section displays detailed information about each of these sessions.

VIEWING FIREWALL SESSION STATISTICS

Follow the procedure below to view the Firewall Session statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall Session Statistics** sub-menu.

Firewall Session Statistics page displays the Firewall Session summary and the details table in the center panel.

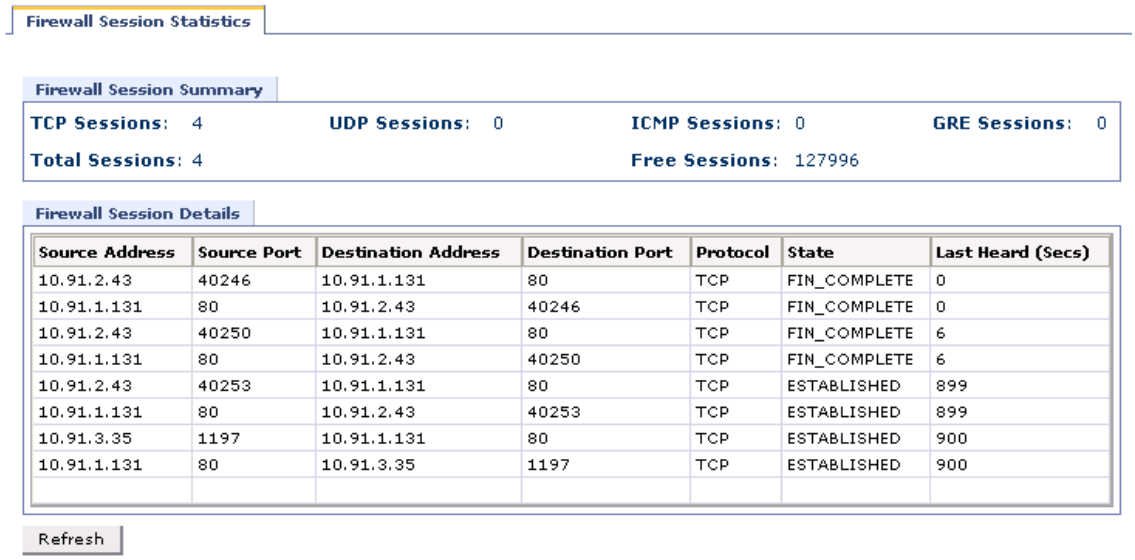


Figure 189: Monitor: Firewall Session Statistics

The table below provides description for Firewall Session Statistics page.

Table 43: Firewall Session Statistics Field Description

Field	Description
FIREWALL SESSION STATISTICS	
Firewall Session Summary	
TCP Sessions	Number of TCP sessions maintained by the firewall module
UDP Sessions	Number of UDP sessions maintained by the firewall module
ICMP Sessions	Number of ICMP sessions maintained by the firewall module
GRE Sessions	Number of GRE sessions maintained by the firewall module
Total Sessions	Total number of sessions maintained by the firewall module
Free Sessions	Number of free sessions available to the firewall module
Firewall Session Details	Displays details of each of the above sessions.
Source Address	IP address of the source
Source Port	Port number at the source
Destination Address	IP address of the destination
Destination Port	Port number at the destination
Protocol	The type of protocol used for the session
State	The state the session is in based on the protocol
Last Heard	Time elapsed since the last data transfer took place. This helps in deleting a session if it has been idle for too long.
Refresh	Refresh the Firewall Session Statistics page

FIREWALL AND SECURITY

This page allows to view the Filters, NAT, DOS Attack, and Firewall Policy settings configured on your system.

FILTERS

This page displays information about an IP Filter. The **Filter Params** section displays the description of the IP Filter selected. The **Configured Actions** section displays the actions that have been configured. The **Interface Bindings** section displays information about the interfaces to which the filter policies have been applied. On clicking the **Show Policy Statistics**, global statistics for that Filter policy is displayed.

VIEWING FILTER STATISTICS

Follow the procedure below to view the Filter statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall and Security** sub-menu.

The Firewall and Security has four tabs: **Filters**, **NAT**, **DOS Attack** and **Firewall Policy**. By default, **Filters** tab is selected and Filter page is displayed in the center panel.

Step 4: Select the filter whose statistical information is to be viewed from the **Filter List** drop down list. The filter page displays the parameters, actions and the interface information for the selected filter.

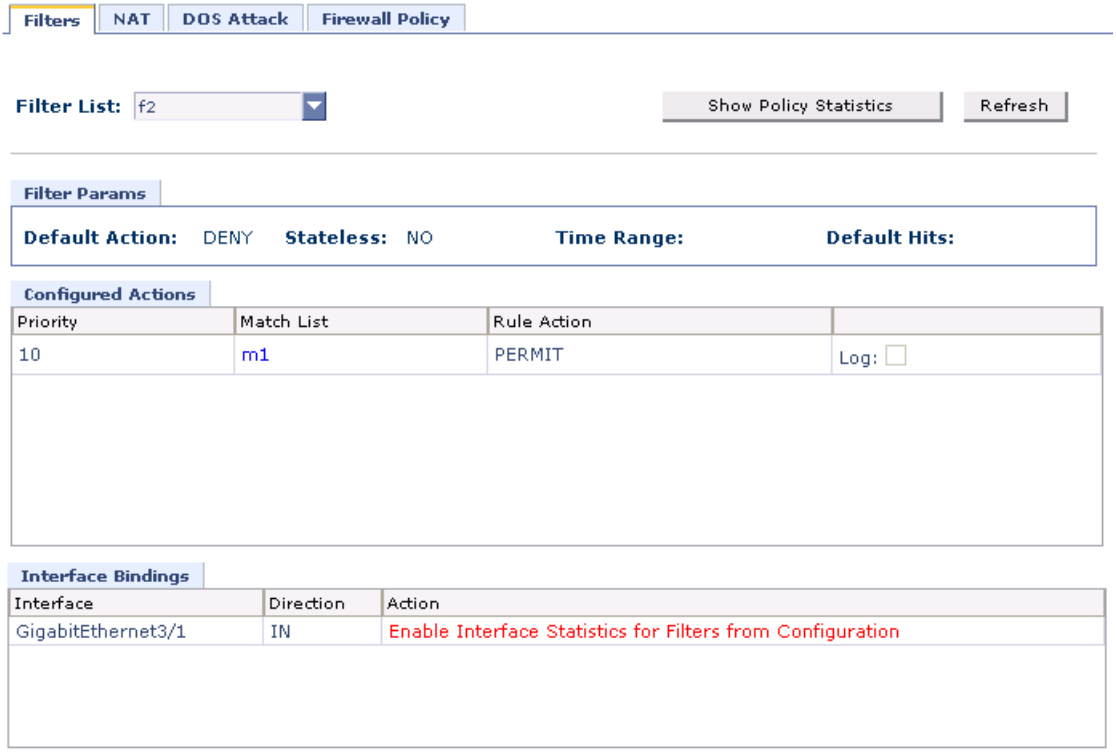


Figure 190: Monitor: Firewall and Security - Filters

The table below provides description for filters page.

Table 44: Filters Field Description

Field	Description
FILTERS	
Filter List	Lists the filters configured in the system
Show Policy Statistics	Displays global statistics for the selected Filter policy
Filter Params	
Default Action	Default action of the filter: PERMIT/ DENY.
Stateless	Indicates if the filter is stateless or not
Time Range	Time range associated with the filter.
Default Hits	Number of default hits associated with the filter.
Configured Actions	
Priority	Priority set for the filter.
Match List	Match list associated with the filter.
Rule Action	Action for the rule: DENY/PERMIT
Packet Hits	Number of packets hit for that particular action.
Interface Bindings	
Interface	The interface to which the filter is applied
Direction	The direction of the traffic to which the filter is applied: In/Out
Action	Enable/Disable statistics for a selected interface from the **Configuration** page.

NAT

This page displays information about NAT policies. The **Configured Rules** table displays the rules that have been configured. The **Interface Bindings** table displays information about the interfaces to which the NAT policies have been applied.

VIEWING NAT STATISTICS

Follow the procedure below to view the NAT statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall and Security** sub-menu.

The Firewall and Security has four tabs: **Filters**, **NAT**, **DOS Attack** and **Firewall Policy**. By default, **Filters** tab is selected. Click the **NAT** tab.

Step 4: Select the NAT policy whose statistical information is to be viewed from the **NAT Policy Name** drop down list. The NAT page displays the policy name, type of policy, rules configured and the interface that the policy is applied to for the selected NAT Policy.

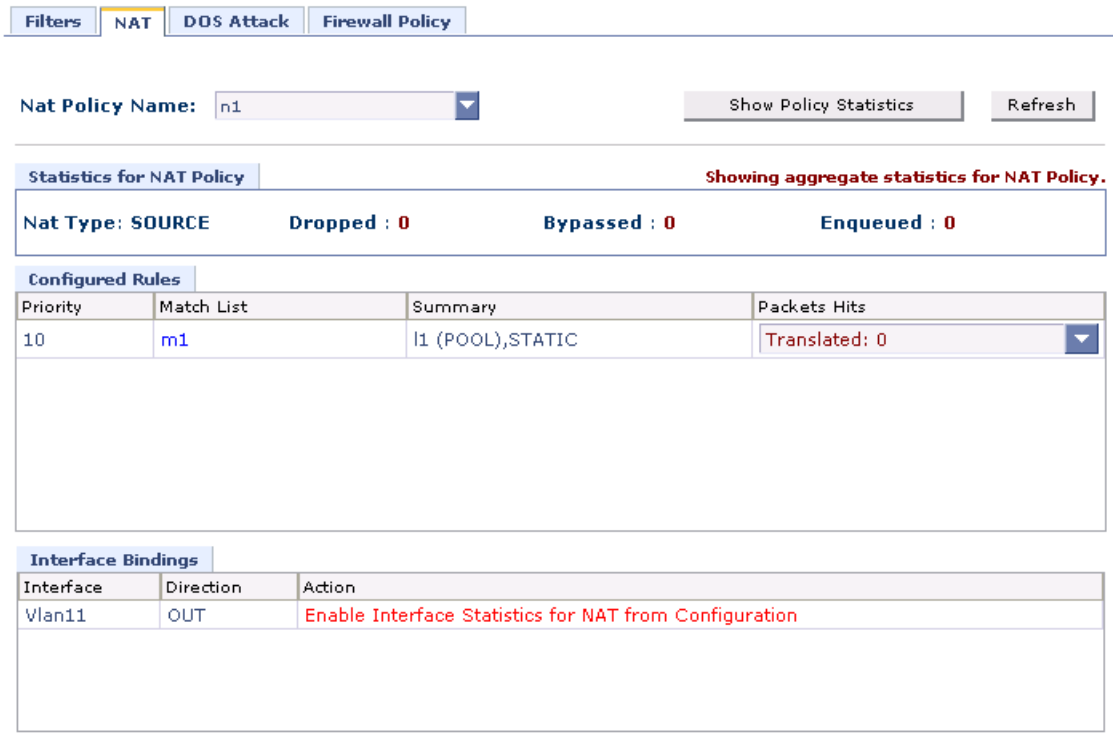


Figure 191: Monitor: Firewall and Security - NAT

The table below provides description for NAT page.

Table 45: NAT Field Description

Field	Description
NAT	
NAT Policy Name	Name of the NAT policy
NAT Type	Destination NAT or Source NAT
Configured Rules	
Priority	Priority of the rule
Match list	Match list associated with the rule
Summary	Displays information about the rule: Dynamic NAT/Static NAT/Bypass.
Packet hits	Number of packets that got hit for that particular rule.
Interface Bindings	
Interface	The interface to which the NAT policy is applied
Direction	The direction of the traffic to which the policy is applied: In/Out
Action	Enable/Disable statistics for an interface from the **Configuration** page

DOS ATTACK

This page displays the DOS attacks configured in the system.

VIEWING DOS ATTACK STATISTICS

Follow the procedure below to view the DOS Attack statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall and Security** sub-menu.

Step 4: The Firewall and Security has four tabs: **Filters**, **NAT**, **DOS Attack** and **Firewall Policy**. Select **DOS Attack** tab.

DOS Attack page is displayed in the center panel with the statistical information of all the DOS Attacks configured in the system.

Click **Show DoS Attack Statistics**. This displays the DoS Attack statistics for the selected DoS Attack in a pop up window.

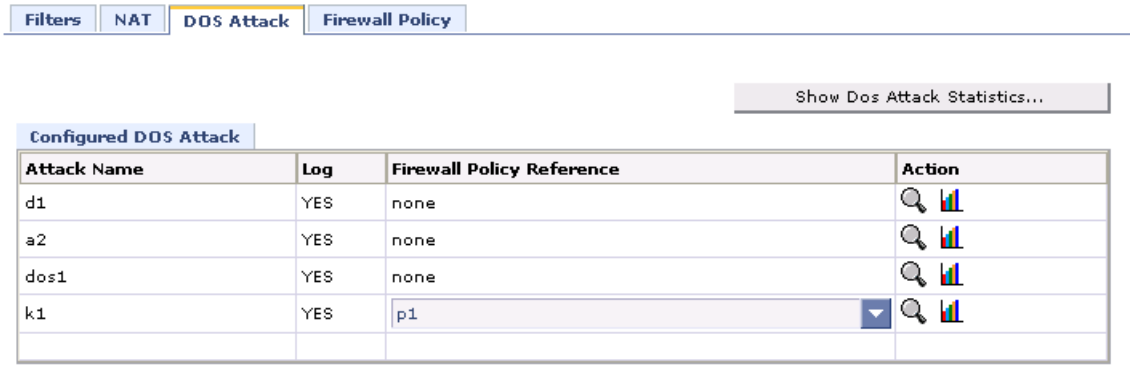


Figure 192: Monitor: Firewall and Security - DOS Attack

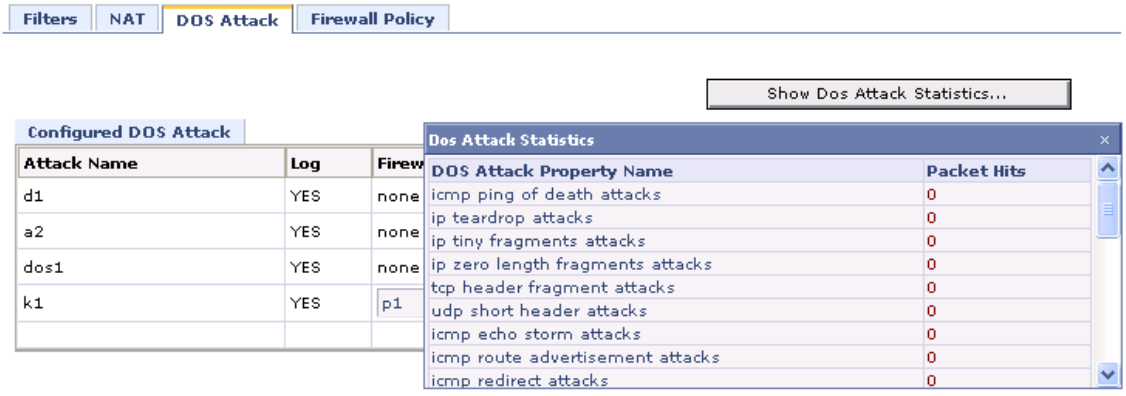


Figure 193: Firewall and Security - DOS Attack - Show DOS Attack Statistics

The table below provides description for DOS Attack page.

Table 46: DOS Attack Field Description

Field	Description
DOS ATTACK	
Show DOS Attack Policy Statistics	Displays the DOS Attack policy statistics.
Configured DOS Attack	
Attack Name	List of DOS Attacks configured in the system.
Log	The logged attacks
Firewall Policy Reference	The firewall policy to which the DOS Attack is attached.
Action	Provides option to view the DOS attack statistics.

FIREWALL POLICY

This page displays the Firewall Policies configured in the system.

VIEWING FIREWALL STATISTICS

Follow the procedure below to view the firewall policies statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Firewall and Security** sub-menu.

The Firewall and Security has four tabs: **Filters**, **NAT**, **DOS Attack** and **Firewall Policy**. Select **Firewall Policy** tab. Firewall Policy page is displayed in the center panel with the statistical information of all the firewall policies configured in the system.

Step 4: Select the Firewall Policy whose statistical information is to be viewed from the **Firewall Policy Name** drop down list. The Firewall Policy page displays the all the Firewall Policy information for the selected filter.

Click **Show Policy Statistics**. This displays the Firewall Policy statistics for the selected firewall policy in a pop up window.

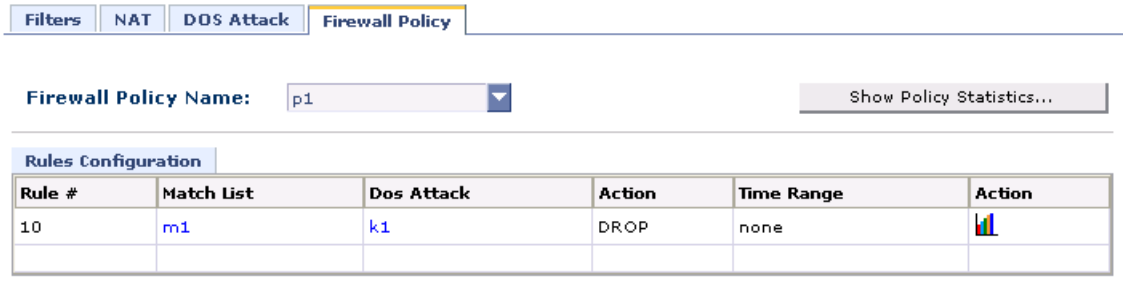


Figure 194: Monitor: Firewall and Security - Firewall Policy

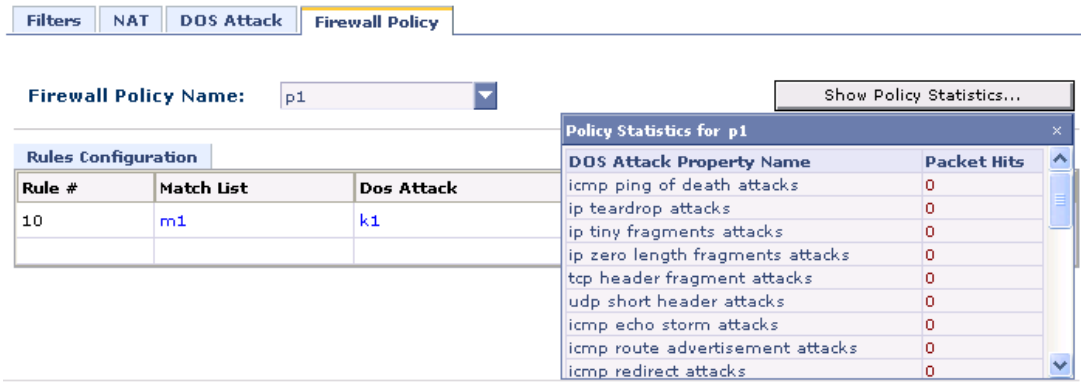


Figure 195: Firewall and Security - Firewall Policy - Show Policy Statistics

The table below provides description for Firewall Policy page.

Table 47: Firewall Policy Field Description

Field	Description
FIREWALL POLICY	
Firewall Policy Name	Lists the firewall policies configured in the system.
Show Policy Statistics	Displays the firewall policy statistics.
Rules Configuration	
Rule #	Rule number.
Match List	Match list associated with the firewall policy.
DOS Attack	DOS attack policy associated with the firewall policy.
Action	Action defined for the firewall policy.
Time Range	Time range associated with the firewall policy.
Action	Provides option to view the firewall statistics for the rule.

IPSEC VPN STATISTICS

This menu displays the IPSec VPN statistics.

VIEWING INTERFACE STATISTICS

Follow the procedure below to view the Interface statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **IPSec VPN Statistics** sub-menu.

Select the Interface and the IPSec Policy from the **Interface** and the **IPSec Policies** drop-down list. IPSec VPN Statistics page displays the details of all the IPSec VPNs configured on the system in the center panel for the selected filter.

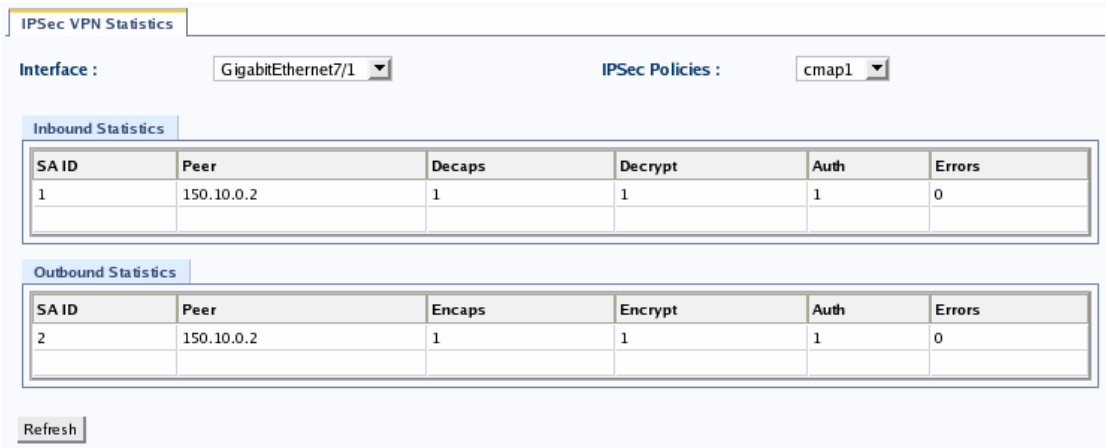


Figure 196: Monitor: IPSec VPN Statistics

The table below provides description for IPSec VPN Statistics page.

Table 48: IPSec VPN Statistics Field Description

Field	Description
IPSEC VPN	
Inbound Statistics	
SA ID	The Security Association ID for the inbound SA
Peer	IP address of the peer
Decaps	Number of packets decapsulated
Decrypt	Number of packets decrypted
Auth	Number of packets authenticated
Errors	Number of packets with errors
Outbound Statistics	
SA ID	The Security Association ID for the outbound SA
Peer	IP address of the peer
Encaps	Number of packets encapsulated
Encrypt	Number of packets encrypted
Auth	Number of packets authenticated
Errors	Number of packets with errors
Refresh	Refresh the IPSec VPN Statistics page

IPS STATISTICS

This menu displays the information about the number of packets that came in for intrusion detection to snort. It displays the statistics of the intrusions checked by the snort.

SUMMARY

This page displays snort statistics.

VIEWING IPS SUMMARY

Follow the procedure below to view the snort statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **IPS Statistics** sub-menu.

The IPS Statistics has three tabs: **Summary**, **Preprocessor**, and **Rules**. By default, **Summary** tab is selected and Summary page is displayed in the center panel.

The Summary page displays the snort statistics.

Click **Clear Counter(s)** to clear the statistics counters.

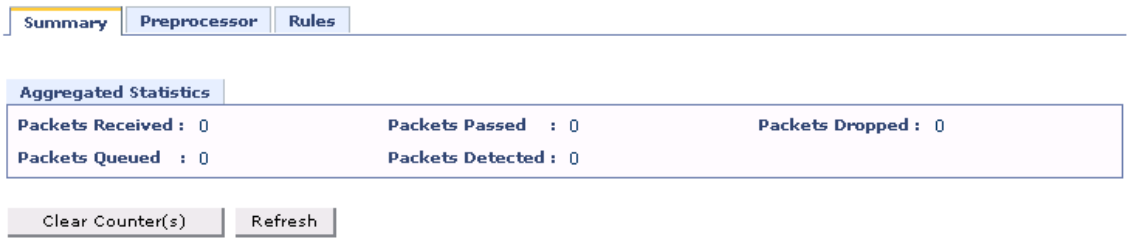


Figure 197: Monitor: IPS Statistics - Summary

The table below provides description for Summary page.

Table 49: Summary Field Description

Field	Description
SUMMARY	
Aggregated Statistics	
Packets Received	The number of packets received by snort
Packets Passed	The number of packets that were passed by snort
Packets Dropped	The number of packets that were dropped because an intrusion was detected
Packets Queued	The number of packets that are queuing up for detection by snort
Packets Detected	The number of packets that were identified as an intrusion
Clear Counter(s)	Clears the statistics counters
Refresh	Refresh the IPS Summary statistics

PREPROCESSOR

This page displays the snort preprocessor statistics. It displays information about the intrusions that were detected by the various preprocessors.

VIEWING PREPROCESSOR STATISTICS

Follow the procedure below to view the snort preprocessor statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **IPS Statistics** sub-menu.

The IPS Statistics has three tabs: **Summary**, **Preprocessor**, and **Rules**. Select **Preprocessor** tab. Preprocessor page is displayed in the center panel with the snort preprocessor statistics.

Click **Clear Counter(s)** to clear the statistics counters.

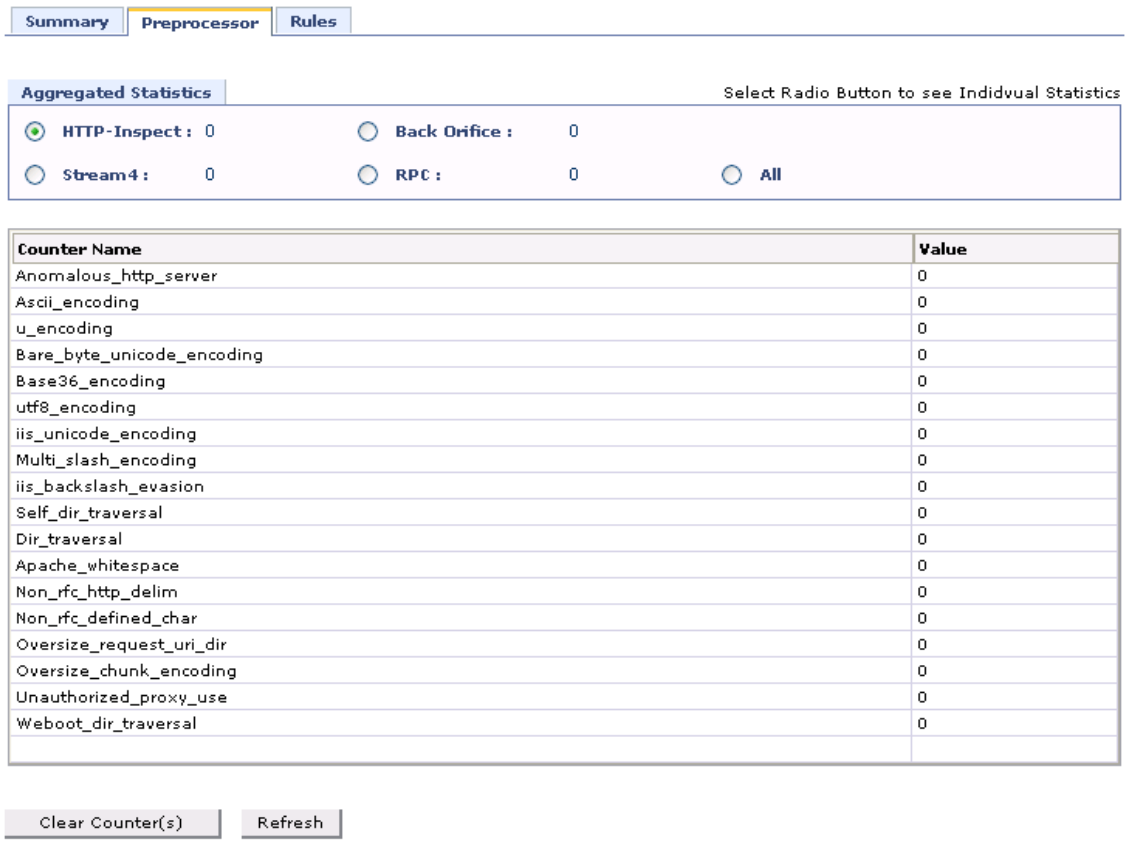


Figure 198: Monitor: IPS Statistics - Preprocessor

The table below provides description for Preprocessor page.

Table 50: Preprocessor Field Description

Field	Description
PREPROCESSOR	
Aggregated Statistics	
HTTP-Inspect	Type of preprocessor
Back Orifice	Type of preprocessor
Stream4	Type of preprocessor
RPC	Type of preprocessor
All	Includes all types of preprocessors
Counter Name	Displays the names of counters under each preprocessor
Value	Displays the number of intrusions detected for each of the corresponding counters
Clear Counter(s)	Clears the statistics counters
Refresh	Refresh the IPS Preprocessor statistics page

RULES

This page displays information about the intrusions detected as per the various rules configured for IPS.

VIEWING PREPROCESSOR STATISTICS

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **IPS Statistics** sub-menu.

The IPS Statistics has three tabs: **Summary**, **Preprocessor**, and **Rules**. Select **Rules** tab. **Rules** page is displayed in the center panel with information about the intrusions that were detected as per the snort rules.

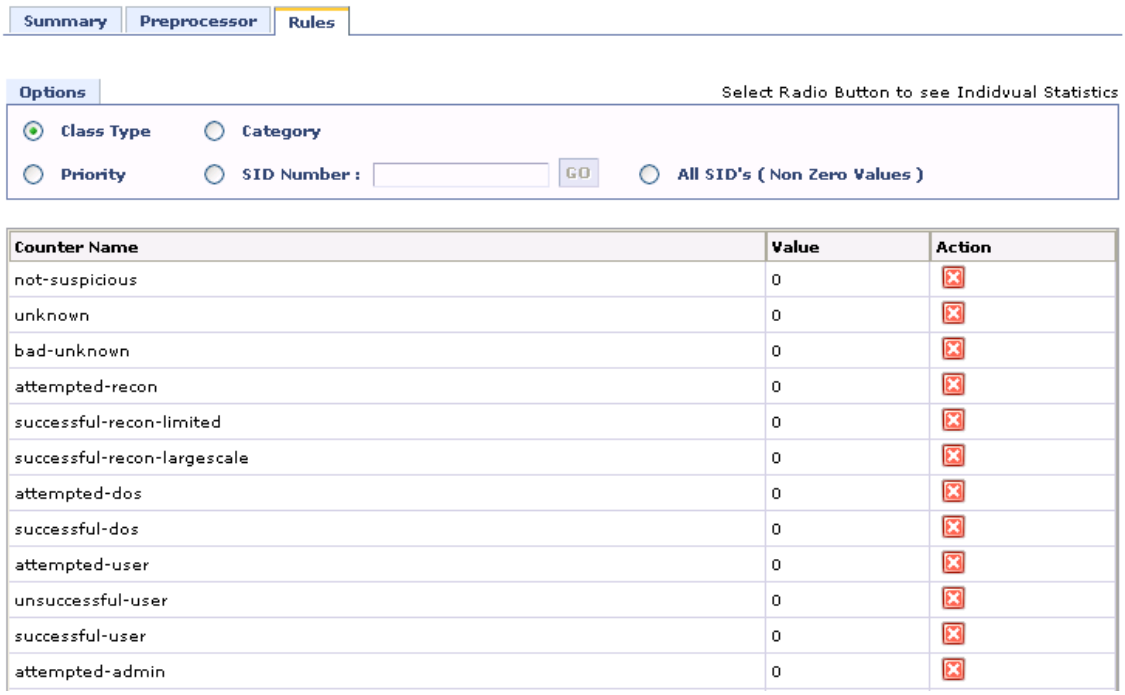


Figure 199: Monitor: IPS Statistics - Rules

The table below provides description for filters page.

Table 51: Rules Field Description

Field	Description
RULES	
Options	
Class Type	Snort rule class type
Category	Snort rule category
Priority	Snort rule priority
SID Number	SID number
All SIDs	All SID numbers
Counter Name	Displays the names of counter under each rule
Value	Number of intrusions detected as per the particular counter for that rule
Action	Clears the individual counter
Clear Counter(s)	Clears the statistics counters
Refresh	Refresh the IPS Rules statistics page

QoS Statistics

This page displays the QoS statistics for those interfaces to which the QoS policy is attached. The **Ingress Statistics** table displays the QoS statistics for the interface in the ingress direction. The **Egress Statistics** table displays the QoS statistics for the interface in the ingress direction.

Note: QoS statistics page displays only those QoS policies that are attached to the active interfaces.

Viewing QoS Statistics

Follow the procedure below to view the QoS statistics.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **QoS Statistics** sub-menu.

QoS Statistics page displays the details of the QoS configured on the system in the center panel.

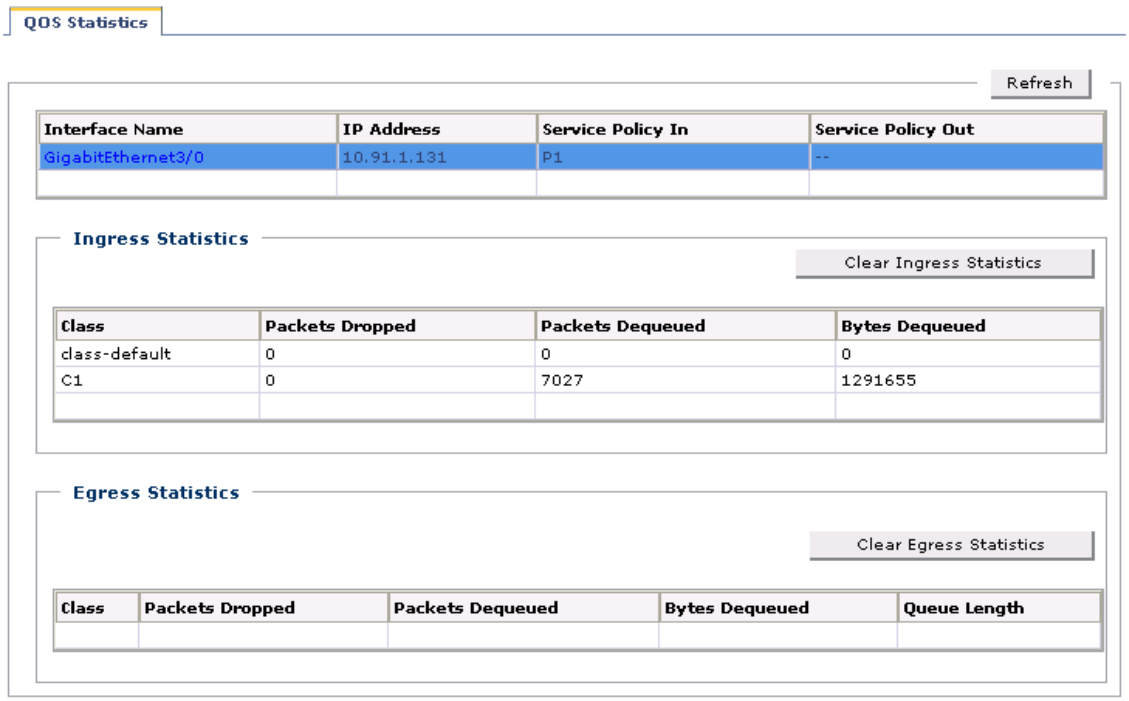


Figure 200: QoS Statistics

The table below provides field description for QoS page.

Table 52: QoS Field Description

Field	Description
QoS Statistics	
Interface Name	Name of the interface to which the QoS is attached.
IP Address	IP address assigned to the interface.
Service Policy In	The QoS policy attached in the ingress direction
Service Policy Out	The QoS policy attached in the egress direction
Ingress Statistics	
Class	The class map attached to the policy map
Packets Dropped	Number of packets dropped from a queue
Packets Dequeued	Number of packets transmitted by the traffic class
Bytes Dequeued	Total amount of bytes dequeued by the traffic class
Clear Ingress Statistics	Clears the ingress statistics
Egress Statistics	
Class	The class map attached to the policy map
Packets Dropped	Number of packets dropped from a queue.
Packets Dequeued	Number of packets transmitted by the traffic class
Bytes Dequeued	Total amount of bytes dequeued by the traffic class
Queue Length	Number of packets currently in the queue.
Clear Ingress Statistics	Clears the egress statistics
Refresh	Refresh the QoS page.

LOGS

This page displays the logs (like emergency logs, alerts, critical logs, errors, etc.) based on the severity of the message. These logs enable you to take appropriate action for smooth functioning of the system.

VIEWING LOGS

Follow the procedure below to view the Logs.

Step 1: Launch the Web GUI tool.

Step 2: From the USGM menu bar, click **Monitor**. All submenu/links under Monitor are displayed in the left navigation panel as shown below.

Step 3: Click **Logs** sub-menu. Logs page is displayed in the center panel.

Step 4: Select the log severity from the **Select the Log severity** drop-down list. The following is displayed based on the log selected:

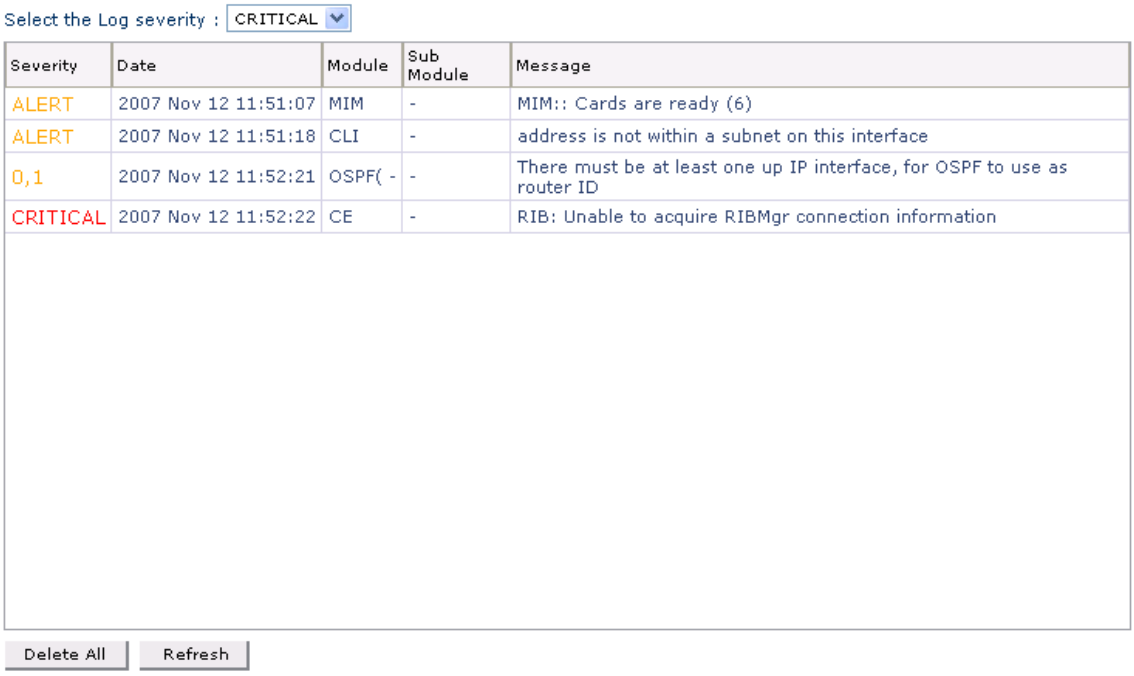


Figure 201: Monitor: Logs

The table below provides description of all the fields in the Logs page.

Table 53: Logs Field Description

Field	Description
LOGS	
Severity	The severity of the log message like warning, alert, etc.
Date	The date the log was generated.
Module	The module for which the log was generated.
Sub Module	The sub module for which the log was generated.
Message	The detailed log message.
Delete Log(s)	Deletes all the logs from the Logs page.
Refresh	Refreshes the logs in the Logs page.