FDN40

Configuration User Manual

ulteriustech

FDN40ConfigUM/20160505

Version No: 2.0

Contents

Figures

Web Screens List

Tables

Chapter 1

Introduction

1.1 Purpose and Scope

FDN40 is a Multi Service Business Gateway solution for providing scalable, converged voice and data connectivity to SMB customers.

FDN40 is an integrated data infrastructure solution providing:

- Converged Data, Switching, Security & Robust Routing Platform
- Integrated advanced routing, security applications & WLAN access point with application-aware QoS into an single box solution
- Simplicity via integration and expandability

This document is applicable for the below FDN40 Variants

1. **FDN40-4**
2. **FDN40-6**
3. **FDN40-6P**

1.2 Acronyms

Table 1-1- Acronyms used in the Document

Acronym	Explanation
ACL	Access Control List
AH	Authentication Header
ALG	Application Layer Gateway
BOOTP	Bootstrap Protocol

Acronym	Explanation
BPDU	Bridge Protocol Data Unit
CBS	Committed Burst Size
CIR	Committed Information Rate
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DOS	Denial of Service
DSCP	Differentiated Services Code Point
DES	Data Encryption Standard
DH	Diffie-Hellman
DPI	Deep Packet Inspection
DUT	Device Under Test
EIR	Excess Information Rate
EBS	Excess Burst Size
ESP	Encapsulating Security Protocol
EXEC	EXECutable mode
FID	Filtering Identifier
IP	Internet Protocol
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPSec	Internet Protocol for Security
IETF	Internet Engineering Task Force
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IVL	Independent VLAN Learning
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MTU	Maximum Transfer Unit
NAT	Network Address Translation
NAPT	Network Address Port Translation
NTP	Network Time Protocol
NVRAM	Non-Volatile Random Access Memory
PNAC	Port Based Network Authentication Protocol
PVID	Port VLAN ID
QoS	Quality-of-Service
RADIUS	Remote Authentication Dial-In User Service
RA-VPN	Remote Access Virtual Private Network

Acronym	Explanation
RSA	Rivest Shamir Adleman Algorithm
RIP	Routing Information Protocol
RRD	Route Redistribution
RTM	Routing Table Manager
RFC	Request For Comments
RMON	Remote Monitoring
SA	Security Association
SAD	Security Association Database
SG	Security Gateway
SHA1	Secure Hash Algorithm 1
SPD	Security Policy Database
SPI	Security Parameter Index
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VAP	Virtual Access Point
VACM	View based Access Control Model
VID	VLAN Identifier
VLAN	Virtual Local Area Network
WAN	Wide Area Network

1.3 References

FDN40 CLI Configuration Guide

1.4 Document Conventions

Table 1-2: Document Conventions

Convention	Usage
Bold	CLI commands
Italics	User inputs for CLI commands
`Courier New 10 Regular`	CLI command outputs
	Notes / Guidelines / Pre-requisites are keyed using this style.
	Output areas specific to the configuration

1.5 General Configurations

1.5.1 CLI Modes

The following table provides the access and exit methods to various general configuration modes.

Table 1-3: General Configurations

Command Mode	Access Method	Prompt	Exit method
User EXEC	This is the initial mode to start a session.	**UltOs>**	The logout method is used.
Privileged EXEC	The User EXEC mode command **enable,** is used to enter the Privileged EXEC mode.	**UltOs#**	To return from the Privileged EXEC mode to User EXEC mode the **disable** command is used.
Global Configuration	The Privileged EXEC mode command **configure terminal**, is used to enter the Global Configuration mode	**UltOs(config)#**	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
Interface Configuration	The Global Configuration mode command **interface <interface-type><interface-id>** is used to enter the Interface Configuration mode.	**UltOs(config-if)#**	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.
VLAN Configuration	The Global Configuration Mode command **VLAN <VLANid>**, is used to enter the VLAN configuration mode	**UltOs(config-vlan)#**	To exit to the Global Configuration Mode, the **exit** command is used and to exit to the Privileged EXEC mode, the **end** command is used
NTP Configuration	The Global Configuration mode command **ntp** is used to enter the NTP configuration mode.	**UltOs(config-ntp)#**	To exit to the Global Configuration mode the **exit** command is used and to exit to the Privileged EXEC mode the **end** command is used.

1.5.2 SNMP Configurations

SNMP configurations can be done in two ways:

1. Using NETSNMP commands
2. Using Scotty manager

We have done the configurations using Scotty manager version 2.1.10. To start the configurations, follow the steps given below.

3. Execute Scotty.

   root@localhost mibs# scotty2.1.10

   %

4. Load the mib files. This is to register the mib files with the SNMP manager.

   % **mib load** *fsrmon.mib*

   % **mib load** *stdrmon.mib*

5. Create a session.

   % **snmp** session -address 12.0.0.1 -community "NETMAN" -retries 0 -version SNMPv2C -timeout 30

   snmp0

To configure a particular object, use the set command as given below.

% snmp0 set {{ rmonEnableStatus.*0 enable***}}**

Where rmonEnableStatus is the object name, 0 is the index and enable is the object value to be set.

To obtain a configured value, use the get command. For example,

% snmp0 get rmonEnableStatus.*0*

Where rmonEnableStatus is the object name, 0 is the index.

If the object is the tabular object, use the interface ID to which the object is configured as the index.

Chapter 2

System Features

2.1 Topologies

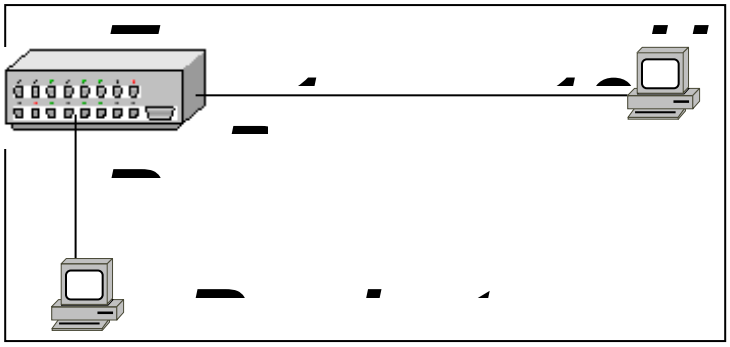


Figure 2-1: Configuration for Basic System Features

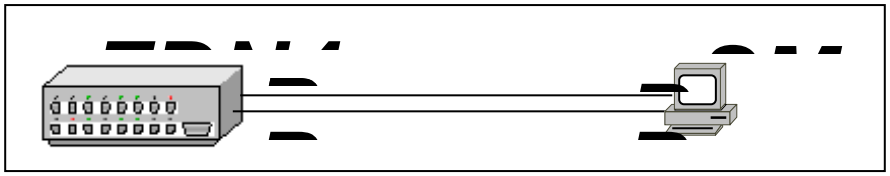


Figure 2-2: Configuration for Advanced System Features

2.2 System Features / Configurations

2.2.1 Configuring the Default IP Address

Configuring the Default IP Address will result in the IP address to be written to the NVRAM and this will be used as the IP address of the default interface when the switch is restarted. This will update the IP address of the Inband Management VLAN.

2.2.1.1 CLI Configuration

1. Execute the following commands to configure the Default IP Address.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the default IP address and subnet mask as 10.10.10.1 and 255.255.0.0, respectively.

     UltOs(config)# default ip *10.10.10.1* **subnet-mask** *255.255.0.0*
   - Exit from the Global Configuration mode.

     UltOs(config)#end
2. View the default IP address and subnet mask by executing the following command.

   UltOs# show nvram

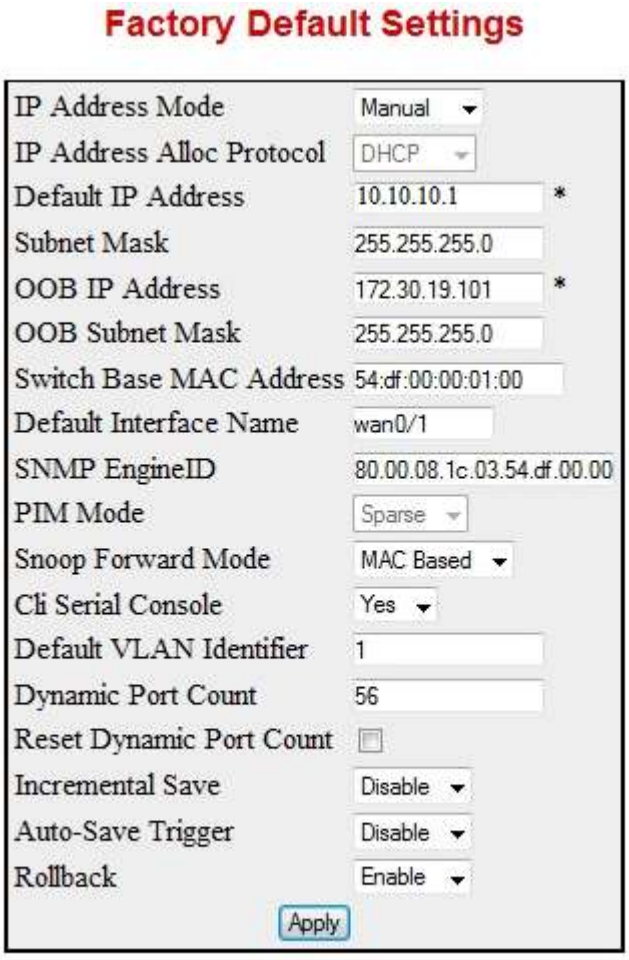
```
Default IP Address                          : 10.10.10.1
Default Subnet Mask                         : 255.255.255.0
OOB IP Address                              : 172.30.19.108
OOB Subnet Mask                             : 255.255.255.0
Default IP Address Config Mode              : Manual
Default IP Address Allocation Protocol      : DHCP
Switch Base MAC Address                  : 54:df:00:00:08:01
Default Interface Name                      : wan0/1
Default RM Interface Name                   : NONE
Config Restore Option                       : Restore
Config Save Option                          : Startup save
Auto Save                                   : Disable
Incremental Save                            : Disable
Roll Back                                   : Enable
Config Save IP Address                      : 0.0.0.0
Config Save Filename                        : zeus.conf
Config Restore Filename                     : zeus.conf
PIM Mode                                    : Sparse Mode
IGS Forwarding Mode                         : MAC based
```

```
Cli Serial Console                    : Yes
SNMP EngineID                       : 80.00.08.1c.03.54
SNMP Engine Boots                     : 351
Default VLAN Identifier               : 1
Stack PortCount                       : 0
ColdStandby                           : Disable
Store Default Value                   : Disable
Vrf Unique Mac                        : Disable
Hitless Restart  Flag                 : Disable
Hardware Version                      : 2.0
Firmware Version                      : v1.2.29
Hardware Part Number                  : 1511MMC001
Software Serial Number                : 1-0-0
Software Version                      : R1.1.3
Switch Name                           : FDN40-4
RM Heart Beat Mode                    : Internal
RM Redundancy Type                    : Hot
RM Data Plane Type                    : Shared
RM Type                               : OOB
NPAPI mode                            : Synchronous
TimeStamp Method                      : TransHardware
Restore Flag                          : Disabled
Dynamic Port Count                    : 56
FIPS operation mode                   : Disabled
Restore Option                        : Enabled
BRIDGE_MODE_WAN1                     :Customer Bridge
BRIDGE_MODE_WAN2                     :Customer Bridge
Debugging Log File Location           :/media/iss-db/
Management Port                       : Enabled
Automatic Port Create Flag            : Enabled
IMG_DUMP_PATH                         :
Manufacturing Date                    : 04202016
```

VLAN 1 (default VLAN) will have this IP address and subnet mask after the switch restart only if the allocation method is manual.

2.2.1.2 WEB Configuration

Default IP Address can be configured through WEB interface using the **Factory Default Settings** screen (Navigation - **System > NVRAM Settings**)



Screen 2-1: Factory Default Settings

2.2.2 Configuring IP address for an Interface

Configuring IP address for an Interface configures the IP address which will be used for sending and receiving the packets.

2.2.2.1 CLI Configuration

1. Execute the following commands to configure an IP address for a VLAN interface.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter the VLAN Configuration Mode (for VLAN 1).

     UltOs(config)# VLAN *1*
   - Add member ports for VLAN.

     UltOs(config-vlan)# ports *lan 0/1-4* **untagged** *lan 0/1-4*

– Enter the Interface Configuration mode.

UltOs(config)# interface vlan *1*

– Shut down the VLAN interface.

UltOs(config-if)# shutdown

– Configure the IP address and subnet mask.

UltOs(config-if)# ip address *10.0.0.100 255.0.0.0*

– Bring up the VLAN interface.

UltOs(config-if)#no shutdown

– Exit from the Interface Configuration mode.

UltOs(config)#end

Configuring the IP address for an Interface requires the interface to be shutdown prior to the configuration.

2. View the configured interface IP address by executing the following show command.

UltOs# show ip interface

```
Vlan1 is up, line protocol is up
Internet Address is 10.0.0.100/8
Broadcast Address 10.255.255.255
```

2.2.2.2 WEB Configuration

IP Address for an interface can be configured through WEB interface using the **IPv4 Interface Settings** screen (Navigation - **Layer3 Management** > **IP** > **IPv4 Addr Conf**)

Screen 2-2: IPv4 Interface Setings

2.2.3 Configuring the Base MAC Address

Configuring the Base MAC Address will result in the Switch Base MAC address to be written to the NVRAM. This will be used as the Base MAC address of the when the switch is restarted.

2.2.3.1 CLI Configuration

1. Execute the following commands to change the base MAC address of the switch.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the base MAC address for the switch.

     UltOs(config)# base-mac *00:01:02:03:0A:0B*
   - Exit from the Global Configuration mode.

     UltOs(config)#end
2. View the base MAC address by executing the following show command.

   UltOs# show nvram

```
Default IP Address                          : 12.0.0.1
Default Subnet Mask                         : 255.0.0.0
Default IP Address Config Mode              : Manual
Default IP Address Allocation Protocol      : DHCP
Switch Base MAC Address                                 :
00:01:02:03:0a:0b
Default Interface Name                      : wan0/1
Config Restore Option                       : No restore
Config Save Option                          : No save
Auto Save                                   : Enable
Incremental Save                            : Disable
Roll Back                                   : Enable
Config Save IP Address                      : 0.0.0.0
Config Save Filename                        : FDN40.conf
Config Restore Filename                     : FDN40.conf
PIM Mode                                    : Sparse Mode
IGS Forwarding Mode                         : MAC based
Cli Serial Console                          : Yes
SNMP EngineID                                           :
80.00.08.1c.04.46.53
```

The configuration takes effect only on switch restart.

2.2.3.2 WEB Configuration

Base MAC can be configured through WEB interface using the **Factory Default Settings** screen. For screenshot, refer section 2.2.1.2

2.2.4 Configuring the Login Authentication Method

Configuring the Login Authentication Method sets the authentication method for user logins.

2.2.4.1 CLI Configuration

1. Execute the following commands to change the authentication method for switch login.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the login authentication method as RADIUS.

     UltOs(config)# login authentication radius
   - Exit from configuration mode.

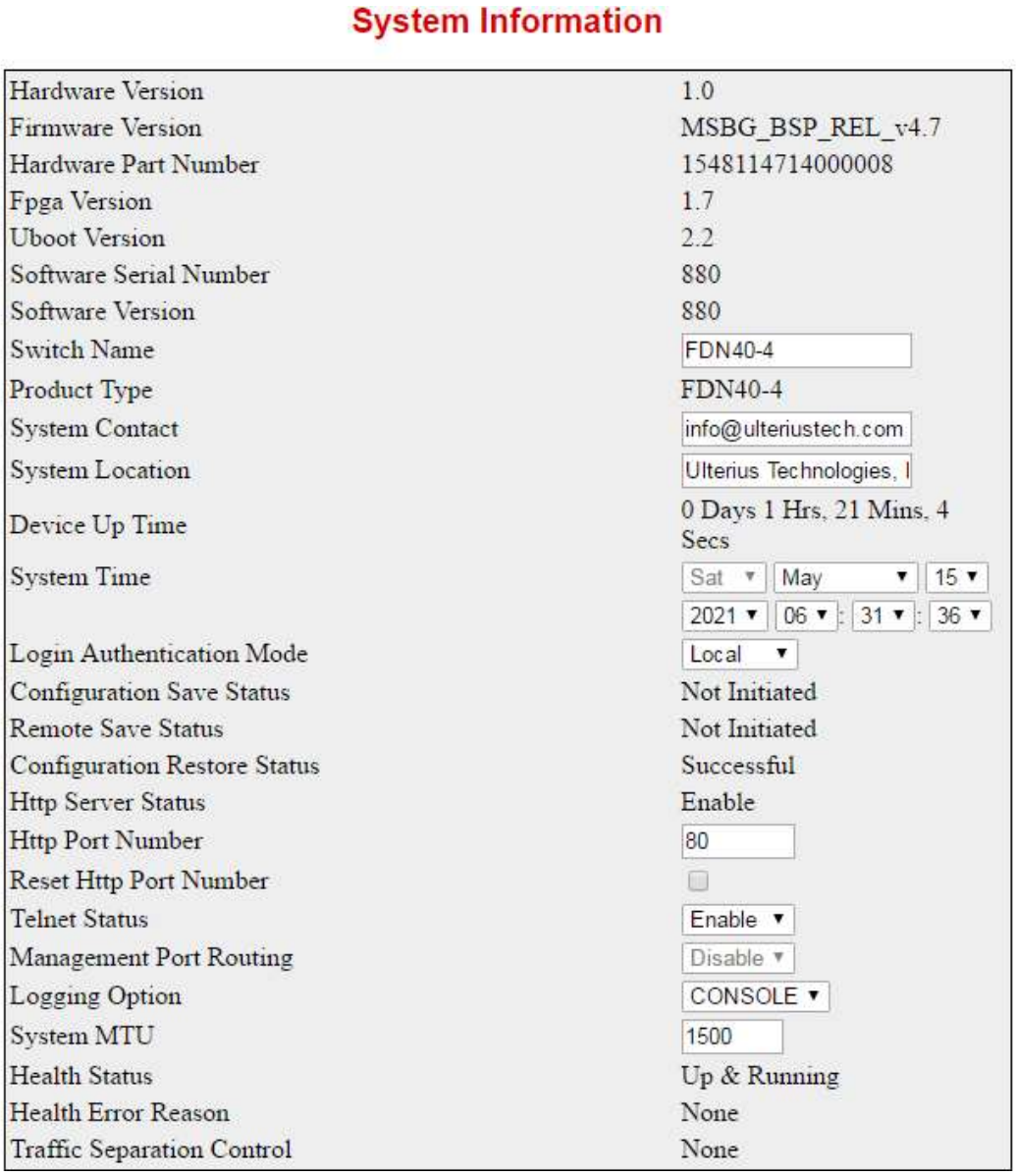
     UltOs(config)#end
2. View the current authentication method by executing the following show command.

   UltOs# show system information

```
Hardware Version                    : 5.2.3
Firmware Version                    : 4.0.0.0
Switch Name                         : FDN40-4
System  Contact                                    :
info@ulteriustech.com
System Location                     : Ulterius
Logging Option                      : Console Logging
Login Authentication Mode           : Remote
Config Save Status                  : Not Initiated
Remote Save Status                  : Not Initiated
Config Restore Status               : Not Initiated
```

2.2.4.2 Web Configuration

Login Authentication can be set through WEB interface using the **System Information** screen (Navigation - **System > System Information)**



Screen 2-3: System Information- Login Authentication

2.2.5 Configuring the Restoration File Name

Configuring the restoration file name will result in the restoration file name to be written to the NVRAM. This will be used as the configuration restoration file.

2.2.5.1 CLI Configuration

1. Execute the following commands to configure the restoration file name.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the configuration restoration file name for the Switch.

UltOs(config)# default restore-file *switch.conf*

– Exit from the Global Configuration mode.

UltOs(config)#end

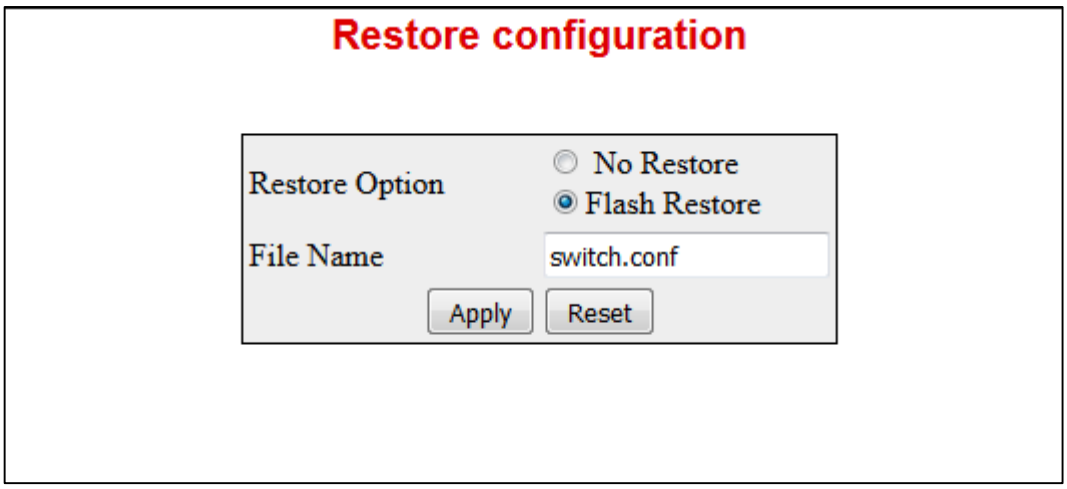
2. View the default restoration file name by executing the following show command.

UltOs# show nvram

```
Default IP Address                          : 12.0.0.1
Default Subnet Mask                         : 255.0.0.0
Default IP Address Config Mode              : Manual
Default IP Address Allocation Protocol      : DHCP
Switch Base MAC Address                                 :
00:01:02:03:0a:0b
Default Interface Name                      : wan0/1
Config Restore Option                       : No restore
Config Save Option                          : No save
Config Save IP Address                      : 0.0.0.0
Auto Save                                   : Enable
Incremental Save                            : Disable
Roll Back                                   : Enable
Config Save Filename                        : zeus.conf
Config Restore Filename                     : switch.conf
PIM Mode                                    : Sparse Mode
IGS Forwarding Mode                         : MAC based
Cli Serial Console                          : Yes
SNMP EngineID                                           :
80.00.08.1c.04.46.53
```

2.2.5.2 Web Configuration

Restore file name can be set through WEB interface using the **Restore Configuration** screen (Navigation - **System > Save and Restore > Restore)**



Screen 2-4: Restore Configuration

2.2.6 Saving the Current Configurations for Restoration

Saving the current configurations for restoration writes the running-config to a flash file, a startup-configuration file or to a remote site.

1. Execute the following command to save the current running configuration into a file.

   UltOs# write startup-config

2. View the restoration status by executing the following show command.

   UltOs# show nvram

```
Default IP Address                          : 12.0.0.1
Default Subnet Mask                         : 255.0.0.0
Default IP Address Config Mode              : Manual
Default IP Address Allocation Protocol      : DHCP
Switch Base MAC Address                                 :
00:01:02:03:04:01
Default Interface Name                      : wan0/1
Config Restore Option                       : Restore
Config Save Option                          : Startup save
Auto Save                                   : Enable
Incremental Save                            : Disable
Roll Back                                   : Enable
Config Save IP Address                      : 0.0.0.0
Config Save Filename                        : switch.conf
Config Restore Filename                     : switch.conf
PIM Mode                                    : Sparse Mode
IGS Forwarding Mode                         : MAC based
Cli Serial Console                          : Yes
```

```
SNMP EngineID                    : 80.00.08.1c.04.46.53
```

3. View the restoration status by executing the following show command.

UltOs# show system information

```
Hardware Version                 : 5.2.3
Firmware Version                 : 4.0.0.0
Switch Name                      : FDN40-4
System Contact                   : info@.com
System Location                  : Ulterius
Logging Option                   : Console Logging
Login Authentication Mode        : Local
Config Save Status               : Successful
Remote Save Status               : Not Initiated
Config Restore Status            : Not Initiated
```

4. View the restoration status after rebooting the switch by executing the following show command.

UltOs# show system information

```
Hardware Version                 : 5.2.3
Firmware Version                 : 4.0.0.0
Switch Name                      : FDN40-4
System  Contact                                  :
info@ulteriustech.com
System Location                  : Ulterius
Logging Option                   : Console Logging
Login Authentication Mode        : Local
Config Save Status               : Not Initiated
Remote Save Status               : Not Initiated
Config Restore Status            : Successful
```

Notes:

- The current configurations will be saved into a file specified by default restore-file command.
- Default name for the restoration file is zeus.conf.
- The switch will start with the saved configuration on reboot.

2.2.7 Erasing a Saved Configuration File

Erasing a saved configuration file clears the contents of the startup configuration or sets the parameters in NVRAM to their default values.

1. Execute the following command to erase the saved configuration file.

UltOs# erase startup-config

2. View the erase status by executing the following show command.

UltOs# show nvram

```
Default IP Address                          : 12.0.0.1
Default Subnet Mask                         : 255.0.0.0
Default IP Address Config Mode              : Manual
Default IP Address Allocation Protocol      : DHCP
Switch Base MAC Address                                 :
00:01:02:03:04:01
Default Interface Name                      : wan0/1
Config Restore Option                       : No restore
Config Save Option                          : No save
Auto Save                                   : Enable
Incremental Save                            : Disable
Roll Back                                   : Enable
Config Save IP Address                      : 0.0.0.0
Config Save Filename                        : switch.conf
Config Restore Filename                     : switch.conf
PIM Mode                                    : Sparse Mode
IGS Forwarding Mode                         : MAC based
Cli Serial Console                          : Yes
SNMP EngineID                                           :
80.00.08.1c.04.46.53
```

The switch will start with the default configurations on reboot.

2.2.8 Copying System Logs into Remote Location

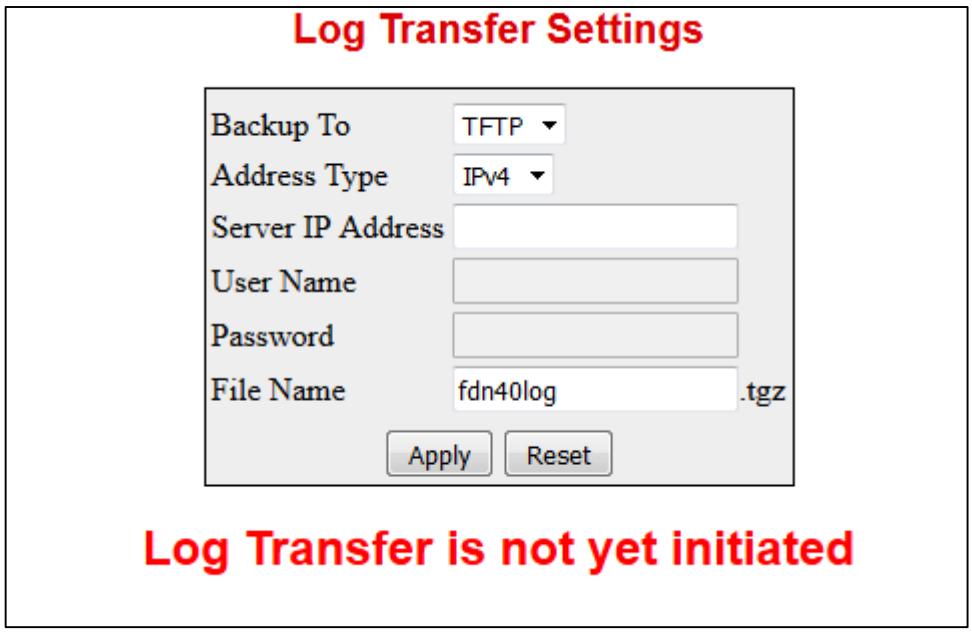
Copying System Logs into Remote Location upload the log file to a remote location.

Execute the following command to upload the log file to remote location 12.0.0.100.

UltOs# copy logs *tftp://12.0.0.100/logfile*

2.2.8.1 Web Configuration

Log transfer can be set through WEB interface using the **Log Transfer Settings** screen (Navigation - **System > Log Transfer)**



Screen 2-5: Log Transfer

2.2.9 Copying a File from Remote Site/Flash to Remote Site/Flash

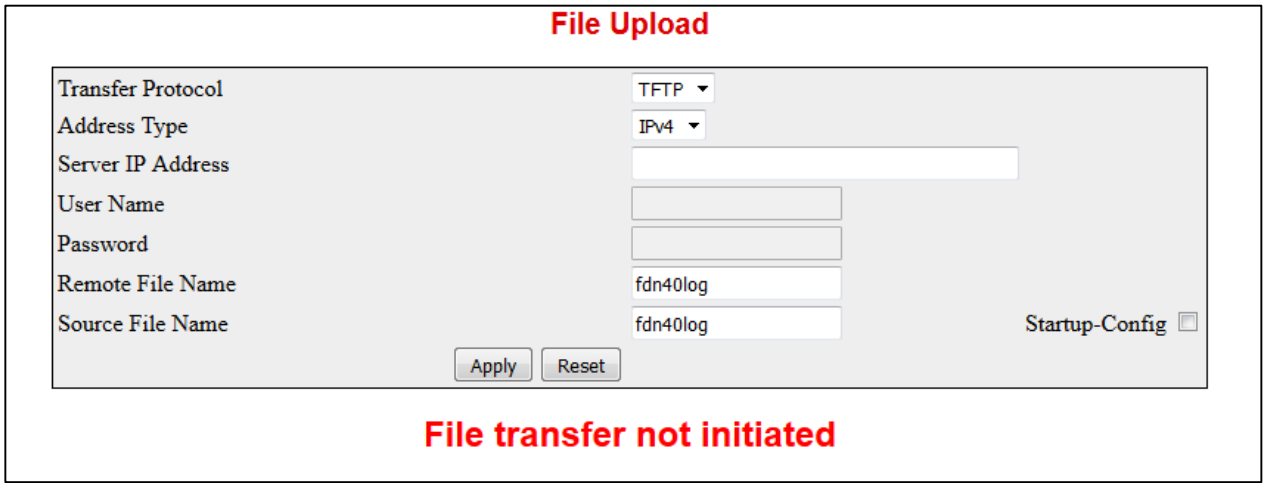
Copying a configuration file from remote location to flash copies a file from a source remote site /flash to a destination remote site/flash.

Execute the following command to copy the file sctipt.txt from remote location 12.0.0.100 to flash.

UltOs# copy *tftp://12.0.0.100/script.txt* **flash:***script.txt*

2.2.9.1 Web Configuration

File Transfer can be set through WEB interface using the **File Upload** screen (Navigation - **System > File Transfer > File Upload)**



Screen 2-6: Log Transfer

2.2.10 Configuring the Default VLAN Identifier

Configuring the default VLAN identifier results in the VLAN ID to be written to the NVRAM and this will be used as the default VLAN ID when the switch is restarted.

2.2.10.1 CLI Configuration

1. Execute the following commands to configure the default VLAN identifier.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the default VLAN ID as 10.

     UltOs(config)# default vlan id *10*
   - Exit from the Global Configuration mode.

     UltOs(config)# end
2. View the default VLAN ID by executing the following command.

   UltOs# show nvram

```
Default IP Address                          : 10.0.0.100
Default Subnet Mask                         : 255.255.0.0
Default IP Address Config Mode              : Manual
Default IP Address Allocation Protocol      : DHCP
Switch Base MAC Address                                 :
00:01:02:03:04:01
Default Interface Name                      : wan0/1
Default RM Interface Name                   : eth0
Config Restore Option                       : No restore
Config Save Option                          : No save
Auto Save                                   : Enable
Incremental Save                            : Disable
Roll Back                                   : Enable
Config Save IP Address                      : 0.0.0.0
Config Save Filename                        : FDN40.conf
Config Restore Filename                     : FDN40.conf
PIM Mode                                    : Sparse Mode
IGS Forwarding Mode                         : MAC based
Cli Serial Console                          : Yes
SNMP EngineID                                           :
80.00.08.1c.04.46.53
SNMP Engine Boots                           : 0
Default VLAN Identifier                     : 10
```

Notes:

- It is not advisable to change the default VLAN ID when some configurations are already saved.
- Once the default VLAN ID is configured, switch has to be restarted before saving any configuration.

2.2.10.2 WEB Configuration

Default VLAN Identifier can be configured through WEB interface using the **Factory Default Settings** screen. For screenshot, refer section 2.2.1.2

2.2.11 Configuring Switch Clock

2.2.11.1 CLI Configuration

Configuring the Clock sets the Switch clock time.

1. Execute the following commands to adjust the switch clock.

   UltOs# clock set *16:00:00 1 jan 2007*

2. View the configured clock by executing the following show command.

   UltOs# show clock

```
Mon Jan 01 16:00:01 2007
```

2.2.11.2 Web Configuration

Switch Clock can be set through WEB interface using the **System Information** screen. For screenshot, refer 2.2.4.2.

2.2.12 Enabling/Disabling Console CLI through Serial Port

2.2.12.1 CLI Configuration

1. Execute the following command to enable console CLI through serial port.

   UltOs# cli console

2. View the console CLI status using the following show command.

   UltOs# show nvram

```
Default IP Address                          : 12.0.0.1
Default Subnet Mask                         : 255.0.0.0
Default IP Address Config Mode              : Manual
Default IP Address Allocation Protocol      : DHCP
Switch Base MAC Address                                 :
00:01:02:03:04:01
Default Interface Name                      : wan0/1
Config Restore Option                       : No restore
Config Save Option                          : No save
Auto Save                                   : Enable
Incremental Save                            : Disable
```

```
Roll Back                                   : Enable
Config Save IP Address                      : 0.0.0.0
Config Save Filename                        : FDN40.conf
Config Restore Filename                     : FDN40.conf
PIM Mode                                    : Sparse Mode
IGS Forwarding Mode                         : MAC based
Cli Serial Console                          : Yes
SNMP EngineID                                          :
80.00.08.1c.04.46.53
```

2.2.12.2 WEB Configuration

CLI Console can be configured through WEB interface using the **Factory Default Settings** screen. For screenshot, refer section 2.2.1.2

2.2.13 Enabling/Disabling HTTP

Enabling/Disabling HTTP enables/disables HTTP server in the switch.

1. Execute the following commands to enable HTTP server on the switch.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable HTTP server in the switch.

     UltOs(config)# set ip http enable
   - Exit from the Global Configuration mode.

     UltOs(config)# end
2. View the http server status using the following show command.

   UltOs# show http server status

```
HTTP server status              : Enabled
HTTP port is                    : 80
```

2.2.14 Configuring HTTP Port Number

2.2.14.1 CLI Configuration

Configuring the HTTP port number sets the HTTP port number to be used for HTTP packets.

1. Execute the following commands to configure the HTTP Port Number in the switch.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the port number for the HTTP server as 6080.

     UltOs(config)# ip http port *6080*
   - Exit from the Global Configuration mode.

UltOs(config)# end

2. View the HTTP port number by executing the following show command.

UltOs# show http server status

```
HTTP server status                : Enabled
HTTP port is                      : 6080
```

2.2.14.2 Web Configuration

HTTP Port can be configured through WEB interface using the **System Information** screen. For screenshot, refer 2.2.4.2.

2.2.15 Configuring HTTP Authentication scheme

HTTP Authentication scheme is designed using two parameters namely, Operational Authentication scheme and the Configurable Authentication scheme.

The Configurable HTTP Authentication scheme can be modified at run time. For the modified Authentication scheme to be effective the value has to be saved in configuration file and the system has to be restarted. The Configurable HTTP Authentication scheme can be set to default or basic or digest.

The Operational HTTP Authentication scheme is initialized on start up and cannot be modified at run-time. The Operational Authentication scheme is used to authenticate all the HTTP sessions. During startup, the Operational Authentication scheme is set to the Configurable Authentication scheme.

2.2.15.1 CLI Configuration

1. Execute the following commands to configure the HTTP Authentication scheme as DEFAULT in the switch.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the authentication scheme for the HTTP server as default.

     UltOs(config)# set http authentication-scheme default
   - Exit from the Global Configuration mode.

     UltOs(config)# end
   - View the HTTP authentication scheme by executing the following show command.

     UltOs# show http authentication-scheme

```
The Operational HTTP authentication scheme is Digest
The Configured HTTP authentication scheme is Default
```

   - Save the configuration.

     UltOs# write startup-config
   - Restart the exe.
   - Ensure the MSR restoration is complete.

- View the HTTP authentication scheme by executing the following show command.

  UltOs# show http authentication-scheme

```
The Operational HTTP authentication scheme is Default
The Configured HTTP authentication scheme is Default
```

- Restart the web browser and clear the saved session information and cache from the browser.

2. Execute the following commands to configure the HTTP Authentication scheme as BASIC in the switch.
   - Enter the Global Configuration mode.

     UltOs# configure terminal

   - Configure the authentication scheme for the HTTP server as basic.

     UltOs(config)# set http authentication-scheme basic

   - Exit from the Global Configuration mode.

     UltOs(config)# end

   - View the HTTP authentication scheme by executing the following show command.

     UltOs# show http authentication-scheme

```
The Operational HTTP authentication scheme is Digest
The Configured HTTP authentication scheme is Basic
```

   - Save the configuration.

     UltOs# write startup-config

   - Restart the exe.
   - Ensure the MSR restoration is complete.
   - View the HTTP authentication scheme by executing the following show command.

     UltOs# show http authentication-scheme

```
The Operational HTTP authentication scheme is Basic
The Configured HTTP authentication scheme is Basic
```

   - Restart the web browser and clear the saved session information and cache from the browser.

3. Execute the following commands to configure the HTTP Authentication scheme as DIGEST in the switch.
   - Enter the Global Configuration mode.

     UltOs# configure terminal

   - Configure the authentication scheme for the HTTP server as digest.

     UltOs(config)# set http authentication-scheme digest

   - Exit from the Global Configuration mode.

     UltOs(config)# end

– View the HTTP authentication scheme by executing the following show command.

UltOs# show http authentication-scheme

```
The Operational HTTP authentication scheme is Basic
The Configured HTTP authentication scheme is Digest
```

– Save the configuration.

UltOs# write startup-config

– Restart the exe.

– Ensure the MSR restoration is complete.

– View the HTTP authentication scheme by executing the following show command.

UltOs# show http authentication-scheme

```
The Operational HTTP authentication scheme is Digest
The Configured HTTP authentication scheme is Digest
```

– Restart the web browser and clear the saved session information and cache from the browser.

2.2.15.2 WEB Configuration

HTTP Authentication Scheme can be configured through WEB interface using the **HTTP Configuration** screen (Navigation - **System > HTTP>HTTP Scalars**)

Screen 2-7: HTTP Configuration

2.2.16 Enabling/Disabling Trap Generation on an Interface

Enabling/Disabling trap generation on an interface enables/disables trap generation either on the physical interface or on the port-channel interface.

2.2.16.1 CLI Configuration

1. Execute the following commands to disable SNMP trap on the interface lan 0/1.

– Enter the Global Configuration mode.

UltOs# configure terminal

– Enter the Interface Configuration mode for lan 0/1.

UltOs(config)# interface *lan 0/1*

– Disable trap on the interface.

UltOs(config-if)# no snmp trap link-status

– Exit from configuration mode.

UltOs(config-if)# end

2. View the trap state for the interface lan 0/1 by executing the following show command.

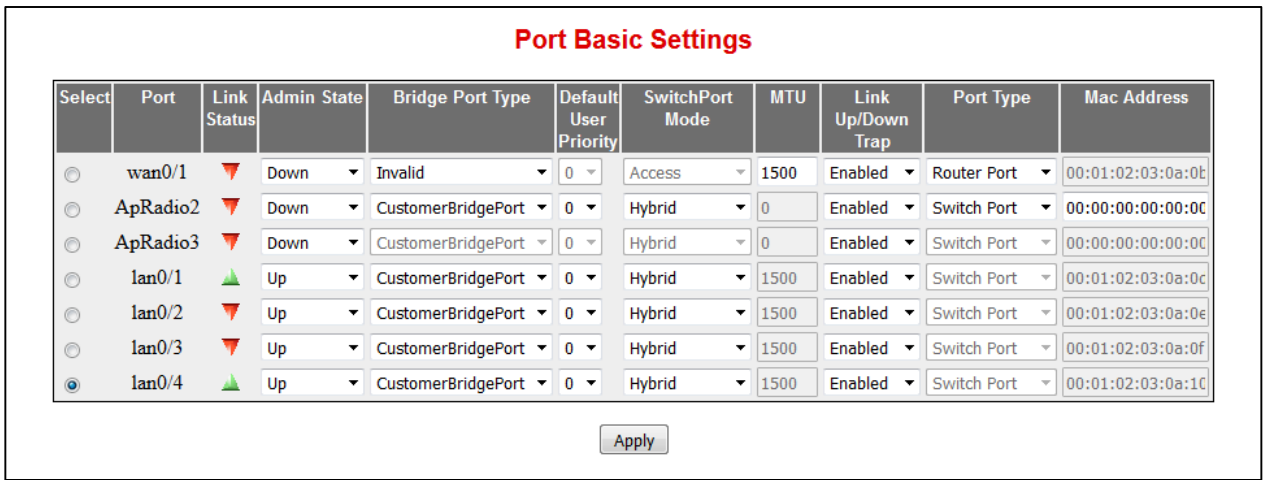
UltOs# show interface *lan 0/1*

```
Lan0/1 up, line protocol is up (connected)
Hardware Address is 00:08:02:03:04:01
MTU 1500 bytes, Full duplex, 100 Mbps, Auto-Negotiation
HOL Block Prevention enabled.

Input flow-control is on, output flow-control is on

Link Up/Down Trap is disabled

Reception Counters
   Octets                          : 0
   Unicast Packets                 : 0
   Discarded Packets               : 0
   Error Packets                   : 0
   Unknown Protocol                : 0

Transmission Counters
   Octets                          : 0
   Unicast Packets                 : 0
   Discarded Packets               : 0
   Error Packets                   : 0
```

If trap is enabled, then the Switch sends trap messages to the SNMP Manager on specific events such as link up, link down, etc.

2.2.16.2 WEB Configuration

Traps can be enabled or disabled on an interface through WEB interface using the **Port Basic Settings** screen (Navigation - **Layer2 Management > Port Manager > Basic Settings**)



Screen 2-8: Port Basic Settings

2.2.17 Configuring an Interface as Switch Port/ Router Port

Configuring an interface as Router Port configures the port as a Layer 3 interface.

2.2.17.1 CLI Configuration

1. Execute the following commands to configure a port as a switch port.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter the Interface Configuration mode for lan 0/1.

     UltOs(config)# interface *lan 0/1*
   - Shutdown the interface.

     UltOs(config-if)# shutdown
   - Configure the interface as switch port.

     UltOs(config-if)# switchport
   - Bring up the interface.

     UltOs(config-if)# no shutdown
   - Exit from configuration mode.

     UltOs(config-if)# end

The specified interface must be shutdown prior to the configuration. "no switchport" configuration is applicable only in WAN ports.

2.2.17.2 Web Configuration

Switch Port/ Router Port can be configured through WEB interface using the **Port Basic Settings** screen. For screenshot, refer 2.2.16.2.

2.2.18 Configuring Debug Logging

Configuring Debug Logging configures where the debug logs are to be displayed, that is, either on the console or on a file or on the flash memory.

2.2.18.1 CLI Configuration

1. Execute the following commands to modify the logging option of debug traces.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure to log the debug traces in to a file.

     UltOs(config)# debug-logging file
   - Exit from the Global Configuration mode.

     UltOs(config)# end
2. View the logging option by executing the following show command.

   UltOs# show system information

```
Hardware Version                    : 5.2.3
Firmware Version                    : 4.0.0.0
Switch Name                         : FDN40-4
System  Contact                                 :
info@ulteriustech.com
System Location                     : Ulterius
Logging Option                      : File Logging
Login Authentication Mode           : Local
Config Save Status                  : Not Initiated
Remote Save Status                  : Not Initiated
Config Restore Status               : Not Initiated
```

3. Execute the following commands to view the debug traces logged in the file.
   - Enable debug trace for any of the module, for example PNAC module.

     UltOs# debug dot1x all
   - View debug logs in the file using the following command.

     UltOs# show debug-logging

     ```
     PNAC: SNMPPROP: Trace Option is set with value: 347
     ```

2.2.18.2 Web Configuration

Debug logging can be configured through WEB interface using the **System Information** screen. For screenshot, refer 2.2.4.2.

2.2.19 Configuring ACL Filters

ACL filters are used to filter packets at the hardware, based on certain filtering criteria configured/programmed in the switch. The switch examines each packet to determine whether it is to be blocked or to be forwarded based on the access lists configured.

2.2.19.1 CLI Configuration

The following example shows how to block the ICMP traffic from a host with IP address 12.0.0.100. Refer

Figure 2-1 for set up. Port 1 of the switch is connected to the host. Execute the following commands in FDN40-1. IP address of Host 1 is assumed as 12.0.0.100.

1. Configure the IP address of the switch as 12.0.0.1.

   UltOs# configure terminal

   UltOs(config)# interface vlan *1*

   UltOs(config-if)# shutdown

   UltOs(config-if)# ip address *12.0.0.1 255.0.0.0*

   UltOs(config-if)# no shutdown

   UltOs(config-if)# end

2. View the ping between Host 1 and FDN40-1 by executing the following command in FDN40-1.

   UltOs# ping *12.0.0.100*

   ```
   Reply Received From: 12.0.0.100, TimeTaken: 30 msecs
   Reply Received From: 12.0.0.100, TimeTaken: 30 msecs
   Reply Received From: 12.0.0.100, TimeTaken: 30 msecs


   --- 12.0.0.100 Ping Statistics ---
   3 Packets Transmitted, 3 Packets Received, 0% Packets
   Loss
   ```

3. Enter the Global Configuration mode.

   UltOs# configure terminal

4. Create a filter with ID 1001.

   UltOs(config)# ip access-list standard 1000

Filter type can be standard. Standard filters are used to filter the traffic based on the source IP address and destination IP address.. IP Access List is supported only on WAN side and not on LAN side. In this example, ICMP packets from 12.0.0.100 need to be filtered.

5. Deny the ICMP traffic from host 12.0.0.100 to any network/host.

   UltOs(config-ext-nacl)# deny host *12.0.0.100* **any priority 2**

6. Exit from Global Configuration mode.

UltOs(config-ext-nacl)# exit

7. Apply the filter 1000 to port1.

   UltOs(config)# interface *wan 0/1*

   UltOs(config-if)# ip access-group *1000* **in**

8. Exit from the Interface Configuration mode.

   UltOs(config-if)# end

9. View the configuration details by executing the following command.

   UltOs# sh access-lists

IP ACCESS LISTS

Standard IP Access List 1000

Filter Priority : 2
IP address Type : IPV4
Source IP address : 12.0.0.100
Source IP address mask : 255.255.255.255
Source IP Prefix Length : 32
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
Destination IP Prefix Length : 0
Flow Identifier : 0
In Port List : wan0/1
Out Port List : NIL
Filter Action : Deny
Filter Creation Mode : External
Redirect Port List : NIL
TrafficDistField : Unknown
Sub Action : NONE
Sub Action Id : 0
Status : Active

MAC ACCESS LISTS

No MAC Access Lists have been configured

USER DEFINED LISTS

No User Defined Lists have been configured

10. View that the ICMP packet from Host 1 is blocked.

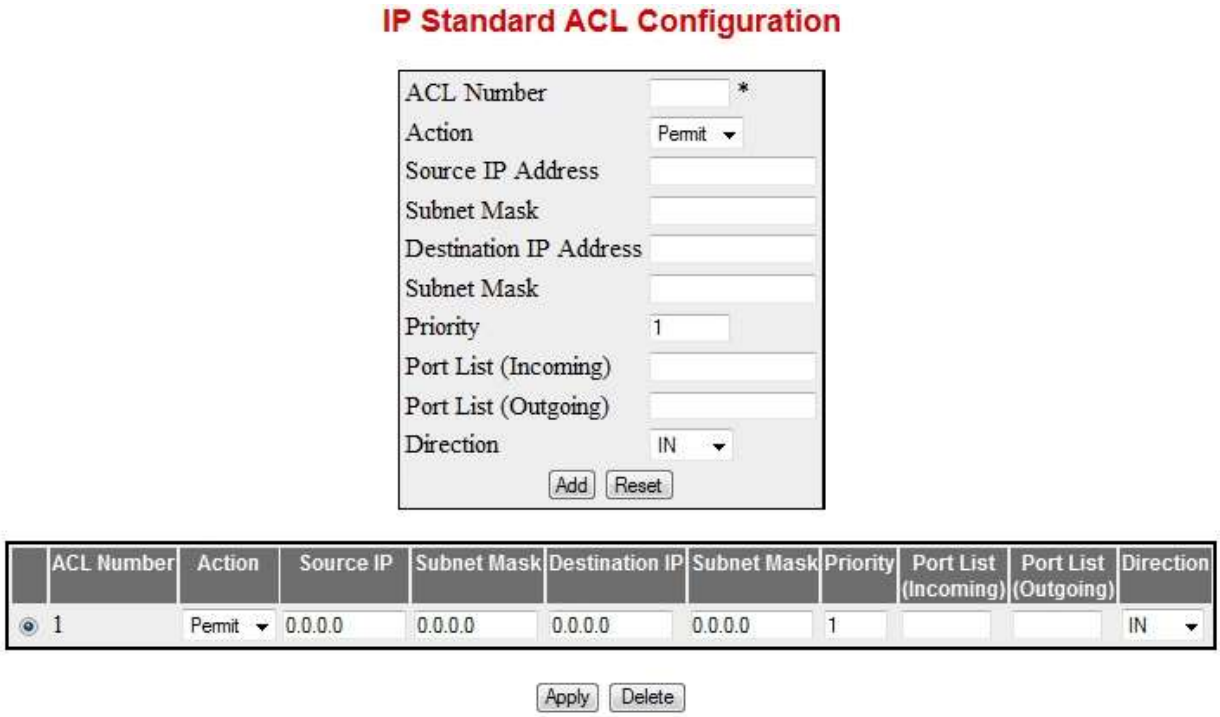
    UltOs# ping *12.0.0.100*

```
Reply Not Received From : 12.0.0.100, Timeout : 5 secs
Reply Not Received From : 12.0.0.100, Timeout : 5 secs
Reply Not Received From : 12.0.0.100, Timeout : 5 secs

--- 12.0.0.100 Ping Statistics ---
3 Packets Transmitted, 0 Packets Received, 100%
Packets Loss
```

2.2.19.2 WEB Configuration

2.2.19.2.1 IP Standard Access List

IP Standard ACLs can be configured through WEB interface using the **IP Standard ACL Configuration** screen (Navigation - **System > ACL > IP Standard ACL**)



Screen 2-9: IP Standard ACL Configuration

2.2.19.2.2 MAC Access List

MAC ACLs can be configured through WEB interface using the **MAC ACL Configuration** screen (Navigation - **System > ACL > MAC ACL**)

Screen 2-10: MAC ACL Configuration

2.2.20 Software image upgradation

2.2.20.1 Software image upgrade through CLI

2.2.20.1.1 Upgrade from R1_1_2 image to R1_1_3

The R1_1_3 is the first fully integrated software image that takes care of automatic upgrade of uboot, IPMC, FPGA, SW application images by the trigger of a single integrated image upgrade procedure.

1. Start **fdn404_r1_1_2.img** as usual and arrive at FDN40 prompt.
2. Upgrade Image through CLI

   UltOs# firmware upgrade tftp tftp://<server IP>/fdn404_r1_1_3.img flash:normal

   UltOs# firmware upgrade tftp tftp://<server IP>/fdn404_r1_1_3.img flash:fallback

   UltOs# reload
3. Image is now upgraded to r1_1_3.img. Since this is first time that an integrated image is applied on filesystem, this process needs to be **repeated again once** more to ensure permanent marking on the file system. Please note that this is only needed for first time upgrade that we execute below step again.

   UltOs# firmware upgrade tftp tftp://<server IP>/fdn404_r1_1_3.img flash:normal

   UltOs# firmware upgrade tftp tftp://<server IP>/fdn404_r1_1_3.img flash:fallback

   UltOs# reload
4. Now system is ready and upgraded fully to new integrated image and all internal parts like FPGA, IPMC,Uboot and SW application. Please verify if below output is seen to confirm upgrade is successful.
5. fdn404/fdn406 is the suffix used to differentiate between FDN40-4 and FDN40-6 board. Error will be thrown when wrong image is uploaded.

Sample:

UltOs# show system information

```
Hardware Version                    : 2.0
Firmware Version                    : v1.2.29
Hardware Part Number                : 1444FDN00007

FPGA Version                        : 2.1
IPMC Version                        : 2.2
UBOOT Version                       : 1.5
Software Serial Number              : 1-0-0
Software Version                    : R1.1.3
Switch Name                         : FDN40-4
```

```
System UpTime                          : 0 Days 0 Hrs, 50
Mins, 11 Secs
System Contact                    : info@ulteriustech.com
System Location     : Ulterius Technologies,Kansas, USA
Logging Option                       : Console Logging
Login Authentication Mode            : Local
Config Save Status                   : Not Initiated
Remote Save Status                   : Not Initiated
Config Restore Status                : Not Initiated
Traffic Separation Control           : none
LCD Brightness                       : 30
```

“show hardware” command is applicable only for FDN40-6 as there is no POE compatible FDN404 device.

UltOs# show hardware

```
Line Card Config table
----------------------
SlotId Status    Card Name   Serial number   MFG id MFG
date         Product   Name   RevisionNo   Mac   Address
Required power MMCVersion
------ ------   ---------  -------------   ------ ----
----  ------------ ---------- ----------------    ----
------     -------------
2         UP           POE           1446FDN00074    BEI
11/25/2014  IOM-POE       2.0          54:DF:00:00:04:58
8              1.4
3         UP           POE           1446FDN00041    BEI
11/24/2014  IOM-POE       2.0          54:DF:00:00:04:40
8              1.4
4         UP           NONPOE        1446FDN00078    BEI
11/24/2014  IOM-ETH       2.0          54:DF:00:00:00:F0
8              1.4
5         UP           NONPOE        1446FDN00077    BEI
11/24/2014  IOM-ETH       2.0          54:DF:00:00:00:E0
8              1.4
6         UP           NONPOE        1446FDN00130    BEI
11/24/2014  IOM-ETH       2.0          54:DF:00:00:00:E8
8              1.4
```

2.2.20.1.2 Upgrade from R1_1_3 image to > R1_1_3

The R1_1_3 is the first fully integrated software image that takes care of automatic upgrade of uboot, IPMC,FPGA, SW application images by the trigger of a single integrated image upgrade procedure.

1. Start **fdn404_r1_1_3.img** as usual and arrive at UltOs prompt.
2. Insert all needed IOM cards in all slots in order to ensure IPMC of IOM cards are also upgraded as part of integrated image upgrade.
3. Upgrade Image through CLI

   UltOs# firmware upgrade tftp tftp://<server IP>/fdn404_r1_1_4.img flash:normal

   UltOs# firmware upgrade tftp tftp://<server IP>/fdn404_r1_1_4.img flash:fallback

   UltOs# reload

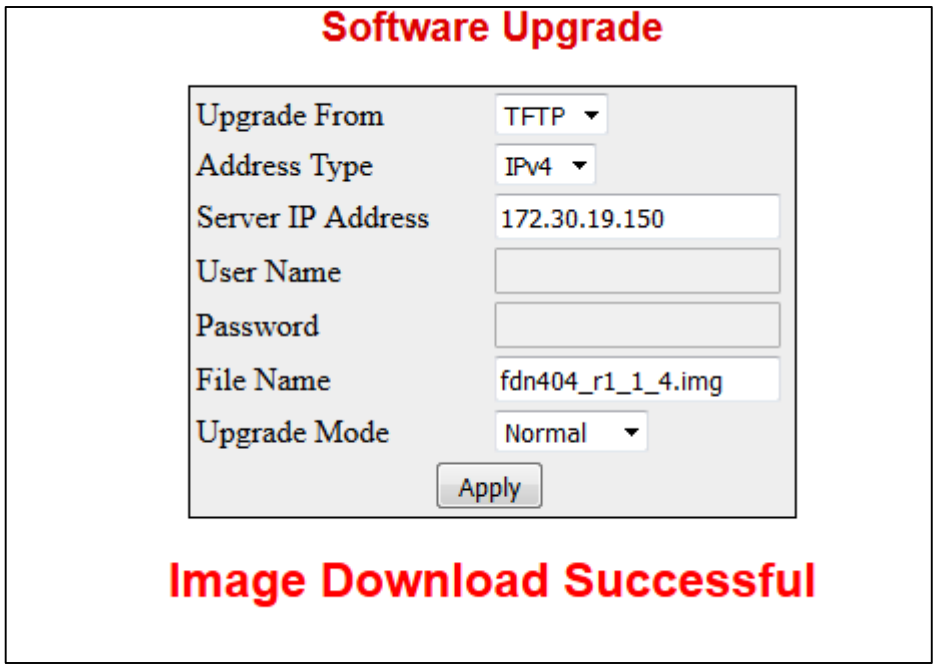
4. Now system is ready and upgraded fully to new integrated image and all internal parts like FPGA, IPMC, Uboot and SW application.

2.2.20.2 Software image upgrade through WEB

1. Start existing **fdn404_rxxxx.img** on board as usual and arrive at FDN40 prompt.
2. Upgrade active image through GUI on active partition
   - Choose option Home->System->Image Download option.
   - Choose upgrade type as TFTP, address type as IPv4 and configure tftp Server IP Address, image File Name and upgrade mode as Normal for flashing image to normal partition and click apply. Once image is downloaded, we should see the notification as “Image Download Successful”
   - Connect to the CLI prompt to restart system for new image to boot up

     UltOs#reload

   - New image should now be loaded from active partition.



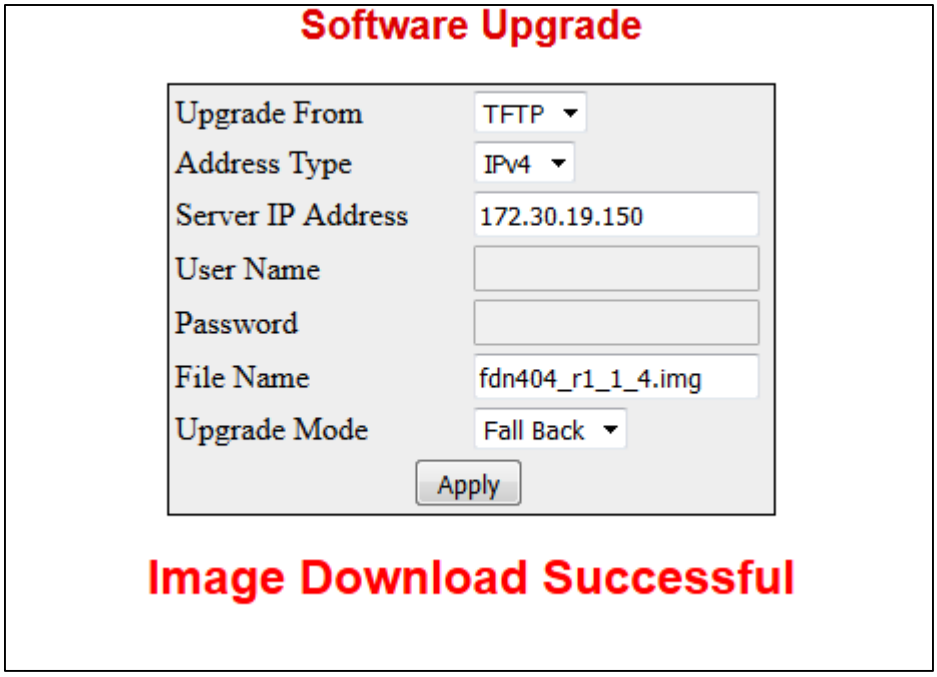
Screen 2-11: Image Upgradation using normal

3 Now software is ready for use.

4 Upgrade standby image through GUI on standby partition

- Choose option Home->System->Image Download option.
- Choose upgrade type as TFTP, address type as IPv4 and configure tftp Server IP Address, image File Name and upgrade mode as Fall Back for flashing image to standby partition and click apply. Once image is downloaded, we should see the notification as “Image Download Successful”
- Connect to the CLI prompt and type below command to restart system for new image to get flashed to standby partition. This image would normally boot up only when active image fails to get loaded successfully.

  UltOs# reload



Screen 2-12: Image Upgradation using FallBack

5 Now software is ready for use.

2.2.21 Setting default OOB IP for system (first time in a new board)

2.2.21.1 CLI Configuration

The R1_1_3 is the first fully integrated software image that boots with default OOB IP as ***10.10.10.1***. This can be changed later to user defined OOB IP using below steps.

1. Assign IP to OOB Interface

UltOs# conf t

UltOs(config)# int oob

UltOs(config)# ip address <new IP> <Netmask>

UltOs(config)# no shut

UltOs(config)# exit

UltOs# write startup-config

Above step saves new IP in NVRAM and for further reboots, configured IP is reflected from NVRAM.

2. Reset OOB IP to factory default

UltOs# erase startup-config

UltOs# erase nvram:

UltOs# reload

Above step restores OOB IP to factory default 10.10.10.1 after reload is successful. If user wants to change OOB IP, step 1 has to be executed.

2.2.21.2 WEB Configuration

Default OOB IP for the system can be configured through WEB interface using the **Factory Default Settings** screen.(Navigation – **System > NVRAM Settings**)

For screenshot, refer section 2.2.1.2.

Erase startup-config and Erase nvram can be done using the **Erase Configuration** Screen.(Navigation – **System > QoS > Save and Restore**)

Screen 2-13: IP Erase configuration

Chapter 3

DHCP Server

3.1 Protocol Description

DHCP server maintains a configured set of IP address pools from which IP addresses are allocated to the DHCP clients, whenever they request the Server dynamically. Once the IP address is allocated, the Server will keep this IP as reserved until the lease time for that IP expires. If the client does not renew the IP before the lease time expiry, this will be returned into the free pool and will be offered to new clients.

3.2 Topology

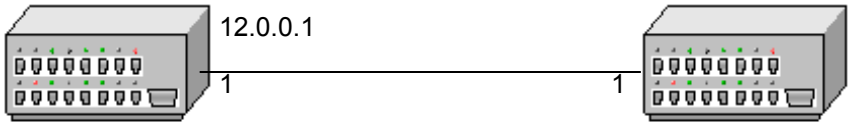


Figure 3-1: DHCP - Topology 1

3.3 Configuration Guidelines

Refer to the CLI Configuration Guide for the complete set of commands and the various options available for configuring DHCP.

The following are the configuration guidelines:

DHCP Client

- If the router interface was not assigned an IP address by the DHCP server, the **renew** DHCP command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

DHCP Server

- DHCP Relay must be disabled before enabling the DHCP server.
- The DHCP server assumes that all pool addresses may be assigned to clients.

3.4 Default Configurations

Table 3-1: Default Configurations

Feature	Default Setting
DHCP server status	Disabled
ICMP echo	Disabled
Offer reuse time out	5 seconds
DHCP next server address	0.0.0.0 (none)
Boot file name	None
DHCP server pool lease time	3600 seconds
DHCP server pool utilization threshold	75%
DHCP server debug level	None
DHCP relay status	Disabled
DHCP relay server address	0.0.0.0 (none)
RAI option	Disabled
DHCP relay debug level	None
DHCP client debug level	None

3.5 DHCP Configurations

3.5.1 Enabling DHCP server

Refer Figure 3-1 for Topology Setup. DHCP server is disabled by default.

3.5.1.1 CLI Configuration

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable DHCP server.

     UltOs(config)# service dhcp-server
   - Exit from the Global configuration mode.

     UltOs(config)# end

2. View the DHCP server status using the following command.

   UltOs# show ip dhcp server information

   The output in FDN40-1 is

```
DHCP server status                          : Enable
Send Ping Packets                           : Disable
Debug level                                 : None
Server Address Reuse Timeout                : 5 secs
Next Server Address                         : 0.0.0.0
Boot file name                              : None
```

3.5.1.2 WEB Configuration

DHCP Server can be enabled / disabled through WEB interface using the **DHCP Basic Settings** screen (Navigation - **Layer3Management > DHCP Server > Basic Settings**)

Screen 3-1: DHCP Basic Settings

3.5.2 Configuring Offer Reuse Time Out

Refer Figure 3-1 for setup. Offer Reuse Timeout is the maximum time frame after which an offered IP can be returned to the free address pool. This can be configured in the range of 1-120 seconds.

3.5.2.1 CLI Configuration

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure offer reuse time out as 10 seconds

     UltOs(config)# ip dhcp server offer-reuse *10*
   - Exit from the Global configuration mode

     UltOs(config)# end
2. View the offer reuse time out configured in FDN40-1.

UltOs# show ip dhcp server information

```
DHCP server status                          : Enable
Send Ping Packets                           : Enable
Debug level                                 : None
Server Address Reuse Timeout                : 10 secs
Next Server Address                          : 0.0.0.0
Boot file name                               : None
```

3.5.2.2 WEB Configuration

Offer Re-use Timeout can be configured through WEB interface using the **DHCP Basic Settings** screen. Refer section 3.5.1.2

3.5.3 Configuring DHCP Address Pools

Refer Figure 3-1 for Topology Setup. Address pools are used by the servers to allocate the IP addresses to the client. This command specifies the IP addresses that are available in the server to configure the clients.

3.5.3.1 Creating a DHCP Address Pool

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter the DHCP pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the network as 12.0.0.0 and mask as 255.0.0.0.

     UltOs(dhcp-config)# network *12.0.0.0 255.0.0.0*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the DHCP server pools available using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                          : 1
-----------------------------------------
Subnet                          : 12.0.0.0
Subnet Mask                     : 255.0.0.0
Lease time                      : 3600 secs
Utilization threshold           : 75%
Start Ip                        : 12.0.0.1
End Ip                          : 12.255.255.255
```

3.5.3.2 Configuring End IP for the Pool

Refer Figure 3-1 for Topology Setup. End IP is used to specify the upper limit for IP addresses in an address pool.

1. Execute the following command in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter into DHCP Pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the network as 12.0.0.0, mask 255.0.0.0 and end IP 12.0.0.100.

     UltOs(dhcp-config)# network *12.0.0.0 255.0.0.0 12.0.0.100*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the end IP for the pools using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                    : 1
-------------------------------------
Subnet                     : 12.0.0.0
Subnet Mask                : 255.0.0.0
Lease time                 : 3600 secs
Utilization threshold      : 75%
Start Ip                   : 12.0.0.1
End Ip                     : 12.0.0.100
```

3.5.3.3 Configuring Lease Time

Refer Figure 3-1 for Topology Setup. Lease time specifies the amount of time that the client can use the IP address assigned by the server. This parameter is specific to each IP address pool. Hence, every IP address allocated from a pool will be returned to the pool, if the client does not renew it.

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter into DHCP Pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the lease time as 1 day 2 hours and 30 minutes.

     UltOs(dhcp-config)# lease *1 2 30*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the lease time of pools using the following command.

UltOs# show ip dhcp server pools

The output in FDN40-1 is

```
Pool Id                          : 1
-----------------------------------------
Subnet                           : 12.0.0.0
Subnet Mask                      : 255.0.0.0
Lease time                       : 95400 secs
Utilization threshold            : 75%
Start Ip                         : 12.0.0.1
End Ip                           : 12.0.0.100
```

DHCP server will return the allocated IP address to the free address pool, if the client does not renew the IP before the lease time expiry interval.

3.5.3.4 Configuring Utilization Threshold

Refer Figure 3-1 for Topology setup. This specifies the upper limit (in percentage) for the address pool utilization, after which a notification will be sent to SNMP manager and an event will be logged into SYSLOG to indicate the possible exhaust of the pool. Range of possible values is 0-100 percentage.

1. Execute the following commands in FDN40-1 to configure Utilization threshold.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter into DHCP pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the utilization threshold as 50%.

     UltOs(dhcp-config)# utilization threshold *50*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the utilization threshold of the pools using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

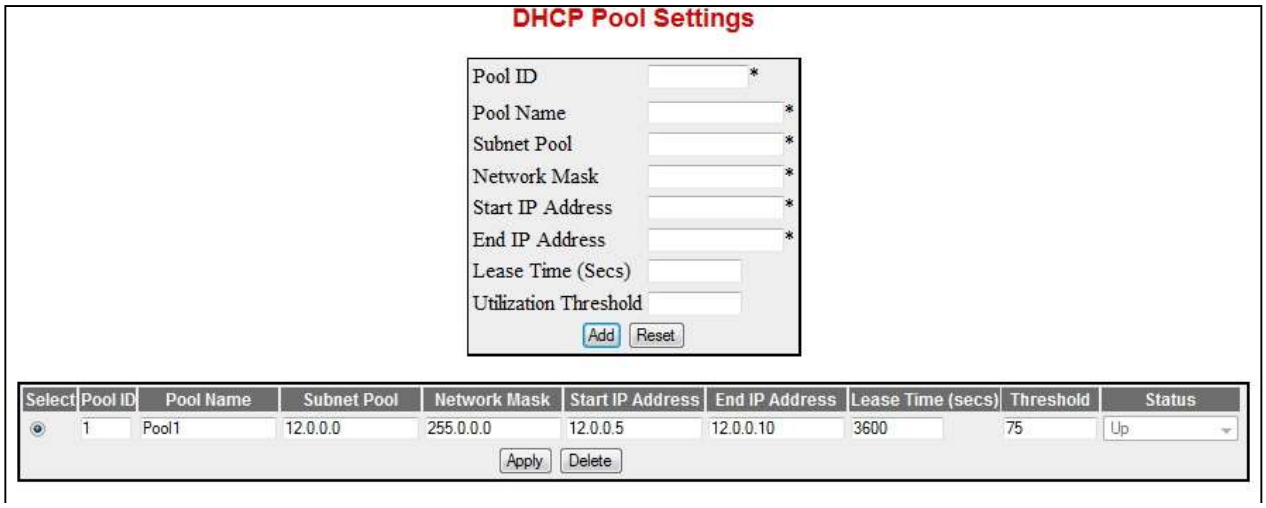
```
Pool Id                          : 1
-----------------------------------------
Subnet                           : 12.0.0.0
Subnet Mask                      : 255.0.0.0
Lease time                       : 95400 secs
Utilization threshold            : 50%
Start Ip                         : 12.0.0.1
End Ip                           : 12.0.0.100
```

If the number of IP addresses allocated from the pool is above the utilization threshold percentage, the server will log an event in SYSLOG and will send a SNMP trap message to the SNMP manager.

Refer SNMPv3 configuration user manual to configure SNMP manager for the Switch, so that the trap message will be sent appropriately.

3.5.3.5 WEB Configuration for DHCP Address Pool

DHCP Address Pool can be configured through WEB interface using the **DHCP Pool Settings** screen (Navigation - **Layer3Management > DHCP Server > Pool Settings**)



Screen 3-2: DHCP Pool Settings

3.5.4 Creating an Excluded Address in the Pool

Refer Figure 3-1 for Topology Setup. Excluded address pool specifies a range of IP addresses that cannot be allocated for the client.

3.5.4.1 CLI Configuration

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter into DHCP pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the excluded address pool from 12.0.0.6 to 12.0.0.8

     UltOs(dhcp-config)# excluded-address *12.0.0.6 12.0.0.8*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the excluded address pools using the following command.

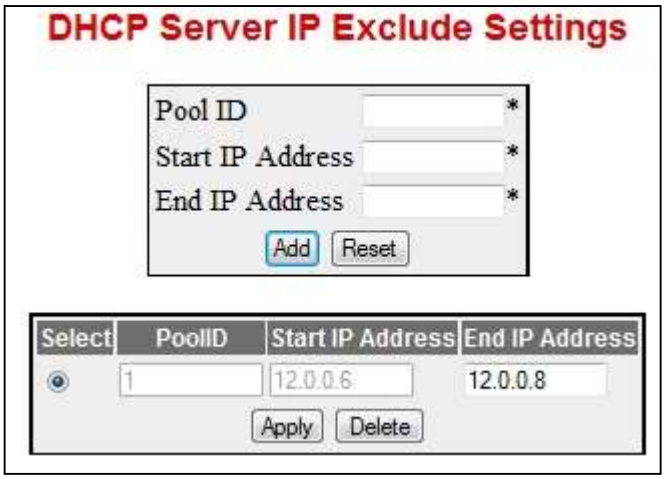
   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                              : 1
-----------------------------------------
Subnet                               : 12.0.0.0
Subnet Mask                          : 255.0.0.0
Lease time                           : 95400 secs
Utilization threshold                : 50%
Start Ip                             : 12.0.0.1
End Ip                               : 12.0.0.100
Exclude Address Start IP             : 12.0.0.6
Exclude Address End IP               : 12.0.0.8
```

3.5.4.2 WEB Configuration

Excluded Address can be configured through WEB interface using the **DHCP Server IP Exclude Settings** screen (Navigation - **Layer3 Management > DHCP Server > Exclude List**)



Screen 3-3: DHCP Server IP Exclude Setings

3.5.5 Configuring DHCP Pool Options

3.5.5.1 Configuring a Domain Name Option

Refer Figure 3-1 for Topology Setup. This is a pool specific option and will be offered to the clients in the pool as a configuration parameter.

1. Execute the following commands in FDN40-1 to configure a domain name option.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter into the DHCP Pool Configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the domain name for this network as “future”.

UltOs(dhcp-config)# domain-name *future*

- Exit from the DHCP Pool configuration mode.

  UltOs(dhcp-config)# end

2. View the domain name option configured using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                                  : 1
-------------------------------------------------
Subnet                                   : 12.0.0.0
Subnet Mask                              : 255.0.0.0
Lease time                               : 95400 secs
Utilization threshold                    : 50%
Start Ip                                 : 12.0.0.1
End Ip                                   : 12.0.0.100
Exclude Address Start IP                 : 12.0.0.1
Exclude Address End IP                   : 12.0.0.10
Subnet Options
--------------
Code        :    15, Value       : future
```

This option will be offered to the DHCP clients only when there is no Host specific option for the client.
If this option is not configured and there is no Host option too, then the global option will be preferred.

3.5.5.2 Configuring DNS Option with Single IP Address

Refer Figure 3-1 for Topology Setup. This is a pool specific option and will be offered to the DHCP client as a configuration parameter.

1. Execute the following commands in FDN40-1 to configure DNS option.
   - Enter the Global Configuration mode.

     UltOs# configure terminal

   - Create pool 1 and enter to DHCP pool configuration mode.

     UltOs(config)# ip dhcp pool *1*

   - Configure the DNS IP address as *12.0.0.6*.

     UltOs(dhcp-config)# dns-server *12.0.0.6*

   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end

2. View the domain name option configured using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                          : 1
```

```
-----------------------------------
Subnet                              : 12.0.0.0
Subnet Mask                         : 255.0.0.0
Lease time                          : 95400 secs
Utilization threshold               : 50%
Start Ip                          : 12.0.0.1
End Ip                            : 12.0.0.100
Exclude Address Start IP          : 12.0.0.1
Exclude Address End IP            : 12.0.0.10
Subnet Options
--------------
Code        :      6, Value       : 12.0.0.6
Code        :     15, Value       : future
```

Notes:

- This option will be offered to the DHCP client only when there is no Host specific option for the client.
- If this option is not configured and there is no Host option too, then the global option will be preferred.

3.5.5.3 Configuring NTP Option with Two IP Addresses

Refer Figure 3-1 for Topology Setup. This is a pool specific option and will be offered to the DHCP client as a configuration parameter.

1. Execute the following commands in FDN40-1 to configure NTP option.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter DHCP pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the two NTP IP addresses as 12.0.0.6 and 15.0.0.5.

     UltOs(dhcp-config)# ntp-server *12.0.0.6 15.0.0.5.*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the configured ntp server option using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                             : 1
-----------------------------------
Subnet                              : 12.0.0.0
Subnet Mask                         : 255.0.0.0
Lease time                          : 95400 secs
```

```
Utilization threshold          : 50%
Start Ip                     : 12.0.0.1
End Ip                       : 12.0.0.100
Exclude Address Start IP     : 12.0.0.1
Exclude Address End IP       : 12.0.0.10
Subnet Options
-------------
Code       :    42, Value      : 12.0.0.6 15.0.0.5
```

Notes:

- This option will be offered to the DHCP client only when there is no Host specific option for the client.
- If this option is not configured and there is no Host option too, then the global option will be preferred.

3.5.5.4 Configuring Default Router

Refer Figure 3-1 for Topology Setup. This is a pool specific option and will be offered to the clients as a configuration parameter.

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter into DHCP pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the default router for this pool as 12.0.0.3.

     UltOs(dhcp-config)# default-router *12.0.0.3*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the default router configured using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                    : 1
-------------------------------------
Subnet                     : 12.0.0.0
Subnet Mask                : 255.0.0.0
Lease time                 : 95400 secs
Utilization threshold      : 50%
Start Ip                   : 12.0.0.1
End Ip                     : 12.0.0.100
Exclude Address Start IP   : 12.0.0.1
Exclude Address End IP     : 12.0.0.10
```

```
Subnet Options
--------------
Code        :     3, Value       : 12.0.0.3
Code        :     6, Value       : 12.0.0.6
Code        :    15, Value       : future
Code        :    46, Value       : 1
```

This option will be offered to the DHCP clients only when there is no Host specific option for the client.
If this option is not configured and there is no Host option too, then the global option will be preferred.

3.5.5.5 Configuring Options Specific to Address Pools

Refer Figure 3-1 for Topology Setup. Apart from the options in the previous sections, options can be specified using the option codes specified in RFC 2132. These options will be offered to the clients as a configuration parameter.

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Create pool 1 and enter into DHCP pool configuration mode.

     UltOs(config)# ip dhcp pool *1*
   - Configure the option 1 (Subnet mask option) as 255.255.0.0.

     UltOs(dhcp-config)# option *1* **ip** *255.255.0.0*
   - Exit from the DHCP Pool configuration mode.

     UltOs(dhcp-config)# end
2. View the options configured in the Switch using the following commands.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                         : 1
---------------------------------
Subnet                          : 12.0.0.0
Subnet Mask                     : 255.0.0.0
Lease time                      : 95400 secs
Utilization threshold           : 50%
Start Ip                        : 12.0.0.1
End Ip                          : 12.0.0.100
Exclude Address Start IP        : 12.0.0.1
Exclude Address End IP          : 12.0.0.10
Subnet Options
--------------
```

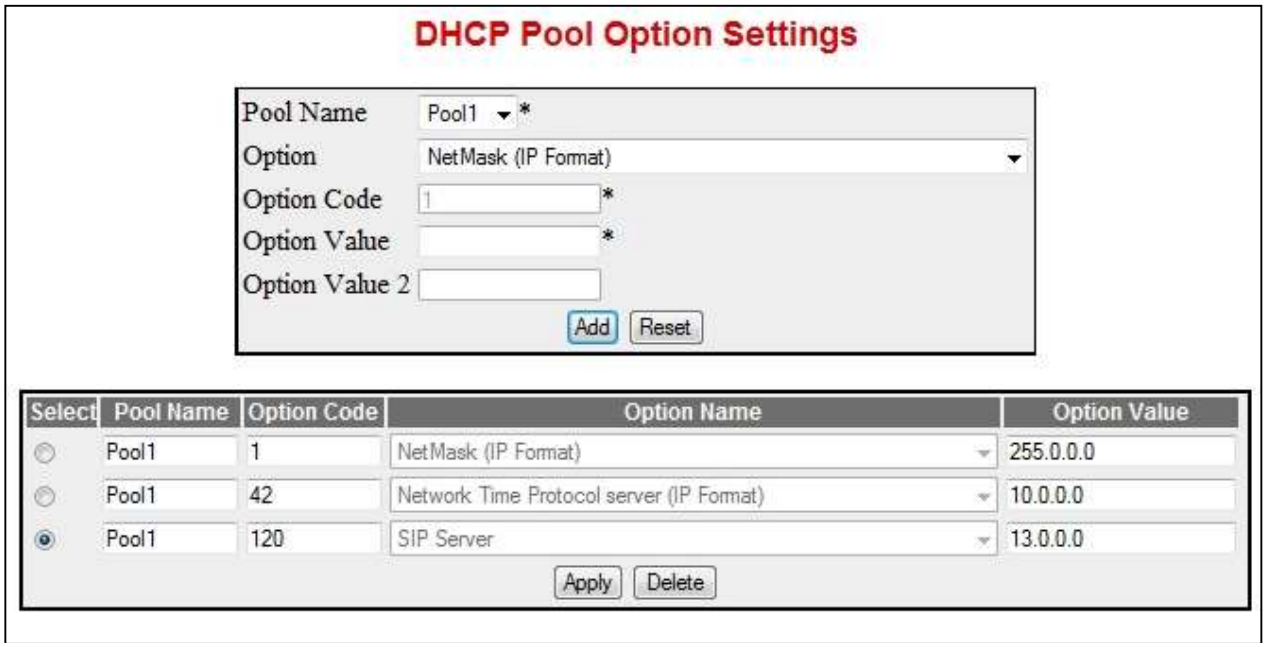
```
Code        :    1, Value      : 255.255.0.0
Code        :    3, Value      : 12.0.0.3
Code        :    6, Value      : 12.0.0.6
Code        :   15, Value      : future
Code        :   46, Value      : 1
```

This option will be offered to the DHCP clients only when there is no Host specific option for the client. If this option is not configured and there is no Host option too, then the global option will be preferred.

Refer RFC 2132 to get the complete list of DHCP options and their corresponding codes.

3.5.5.6 WEB Configuration for DHCP Pool Options

DHCP Pool options can be configured through WEB interface using the **DHCP Pool Options Settings** screen (Navigation - **Layer3 Management >DHCP Server > Pool Options**)



Screen 3-4: DHCP Pool Options Settings

3.5.6 Configuring Host Specific Options

Refer Figure 3-1 for Topology Setup. Apart from the global options and subnet options, options can be specified for Hosts. This configuration will be used for the specific hosts as a configuration parameter.

3.5.6.1 CLI Configuration

1. Execute the following commands in FDN40-1.
   - Enter the Global Configuration mode.

UltOs# configure terminal

- Create pool 1 and enter into the DHCP pool configuration mode.

  UltOs(config)# ip dhcp pool *1*

- Configure the option 1 (subnet mask) as 255.255.255.0 for the client with MAC address 00:11:22:33:44:55.

  UltOs(dhcp-config)# host hardware-type *1* **client-identifier** *00:11:22:33:44:55* **option** *1* **ip** *255.255.255.0*

- Exit from the DHCP Pool configuration mode.

  UltOs(dhcp-config)# end

2. View the options configured in the switch using the following command.

   UltOs# show ip dhcp server pools

   The output in FDN40-1 is

```
Pool Id                              : 1
-------------------------------------------
Subnet                               : 12.0.0.0
Subnet Mask                          : 255.0.0.0
Lease time                           : 3600 secs
Utilization threshold                : 75%
Start Ip                             : 12.0.0.1
End Ip                               : 12.255.255.255
Host Options
------------
Hardware type                        : 1
Client Identifier                    : 00:11:22:33:44:55
Code        :     1, Value           : 255.255.255.0
```

This option will be offered to the DHCP clients with hardware address 00:11:22:33:44:55 even if there is pool specific option or global option with this option code.

Refer RFC 2132 to get the complete list of DHCP options and their corresponding codes.

Chapter 4

RIP

4.1 Protocol Description

RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. RIP is classified by the Internet Engineering Task Force (IETF) as one of several internal gateway protocols (Interior Gateway Protocol).

RIP sends routing-update messages at regular intervals and when the network topology changes. When a Router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count as a way to determine network distance.

The **RIP** basic and advanced configuration tasks are described in the following section(s)

4.2 Topology

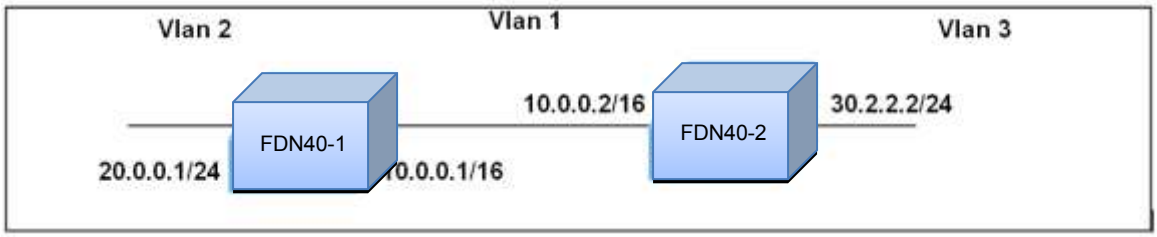


Figure 4-1: RIP Topology 1

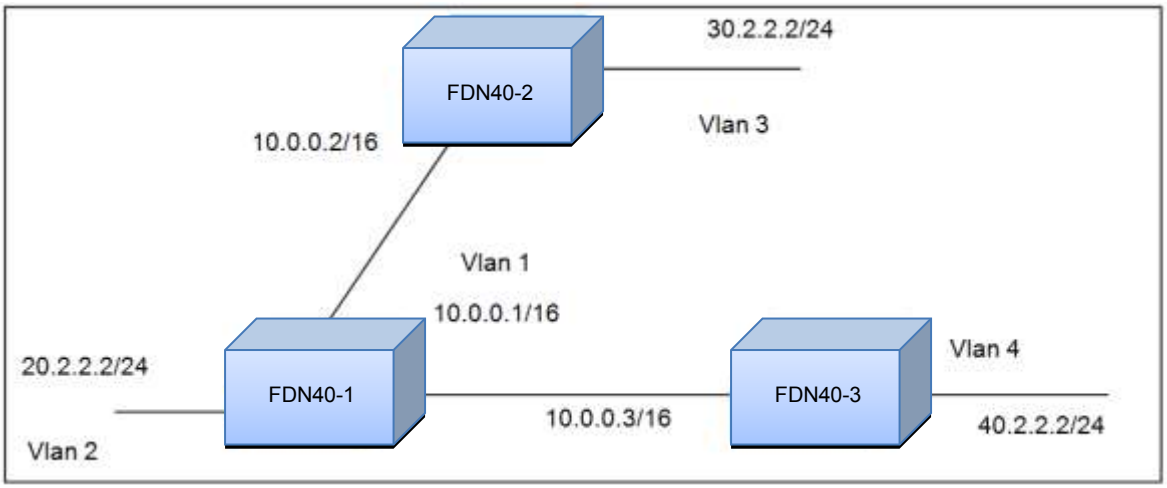


Figure 4-2: RIP Topology 2

4.3 Configuration Guidelines

The following configuration needs to be done in all the switches, FDN40-1 and FDN40-2.

This is a prerequisite for configuring the RIP.

4.3.1 Configuration in FDN40-1

Refer Figure 4-1 for Setup.

Prerequisite: Configuration of VLAN Interfaces (vlan1 and vlan2)

UltOs# configure terminal

UltOs(config)# interface vlan *1*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.0.0.1 255.255.0.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan *1*

UltOs(config-vlan)# ports lan 0/1 untagged lan 0/1

UltOs(config-vlan)# exit
UltOs(config)# interface vlan *2*
UltOs(config-if)# shutdown
UltOs(config-if)# ip address *20.0.0.1 255.255.255.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# vlan *2*
UltOs(config-vlan)# ports lan 0/2 untagged lan 0/2
UltOs(config-vlan)# exit
UltOs(config)# interface lan 0/2
UltOs(config-if)# switchport pvid *2*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit

4.3.2 Configuration in FDN40-2

Refer Figure 4-1 for Setup.

Prerequisite: Configuration of VLAN Interfaces (vlan1 and vlan3)

UltOs# configure terminal
UltOs(config)# interface vlan *1*
UltOs(config-if)# shutdown
UltOs(config-if)# ip address *10.0.0.2 255.255.0.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# vlan 1
UltOs(config-vlan)# ports lan 0/1 untagged lan 0/1
UltOs(config-vlan)# exit
UltOs(config)# interface vlan *3*
UltOs(config-if)# shutdown
UltOs(config-if)# ip address *30.2.2.2 255.255.255.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# vlan *3*
UltOs(config-vlan)# ports lan 0/3 untagged lan 0/3
UltOs(config-vlan)# exit
UltOs(config)# interface lan 0/3
UltOs(config-if)# switchport pvid *3*
UltOs(config-if)# no shutdown

UltOs(config-if)# exit

4.3.3 Configuration in FDN40-3

Refer Figure 4-2 for Setup.

Prerequisite: Configuration of VLAN Interfaces (vlan1 and vlan4)

UltOs# configure terminal

UltOs(config)# interface vlan *1*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.0.0.3 255.255.0.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan *1*

UltOs(config-vlan)# ports lan 0/1 untagged lan 0/1

UltOs(config-vlan)# exit

UltOs(config)# interface vlan *4*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *40.2.2.2 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan *4*

UltOs(config-vlan)# ports lan 0/4 untagged lan 0/4

UltOs(config-vlan)# exit

UltOs(config)# interface lan 0/4

UltOs(config-if)# switchport pvid *4*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

4.4 Default Configurations

None

4.5 RIP Configurations

4.5.1 Enabling and Disabling RIP

4.5.1.1 Enabling RIP

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40- 2) before configuring RIP. RIP is disabled by default.

1. Execute the following commands in the Switch FDN40-1 to enable RIP.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Exit from the router configuration mode.

     UltOs(config-router)# exit

4.5.1.2 Disabling RIP

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in the switch FDN40-1 to disable RIP.
   - Enter the Global Configuration mode.

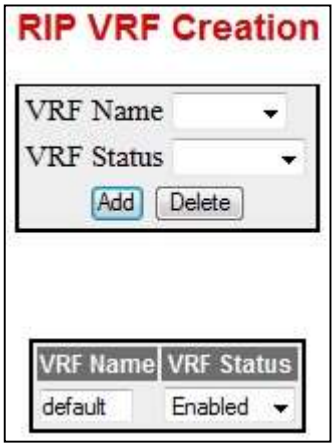
     UltOs# configure terminal
   - Disable RIP globally in the switch FDN40-1.

     UltOs(config)# no router rip
   - Exit from the Global configuration mode.

     UltOs(config)# exit

4.5.1.3 WEB Configuration

RIP can be enabled/ disabled through WEB interface using the **RIP VRF Creation** screen (Navigation - **Layer3 Management > RIP>RIP VRF Creation**)



Screen 4-1: RIP VRF Creation

4.5.2 Enabling RIP on an IP Network

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.2.1 CLI Configuration

1. Execute the following commands in the switch FDN40-1.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Exit from the router configuration mode.

     UltOs(config-router)# exit
2. View the RIP interface using the following command.

   UltOs# show ip rip statistics

```
RIP Global Statistics:
----------------------
 Total number of route changes is 0
 Total number of queries responded is 0
 Total number of periodic updates sent is 11
 Total number of dropped packets is 0
RIP Interface Statistics:
-------------------------
Interface   Periodic      BadRoutes   Triggered
BadPackets   Admin
IP Address  Updates Sent  Received    Updates Sent
Received     Status
----------- ------------  ---------   ------------   -
---------   ------
10.0.0.1      11             0            0
0       Enabled
```

3. View the RIP route

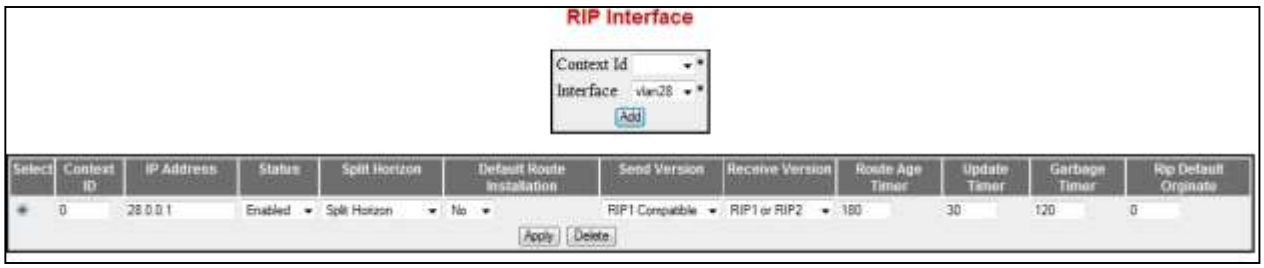
   UltOs# show ip rip database

```
10.0.0.0/8[1]     summary route
10.0.0.0/16        directly connected, vlan1
```

RIP can be enabled on Pseudo wire interface similar to RIP on router port.

4.5.2.2 WEB Configuration

RIP can be enabled/ disabled on an IP network through WEB interface using the **RIP Interface** screen (Navigation - **Layer3 Management > RIP > Interface Configuration**)



Screen 4-2: RIP Interface

4.5.3 Configuring RIP Security

Refer the section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

For enabling authentication, refer section 4.5.13.2.

4.5.3.1 CLI Configuration

Execute the following commands in the switch FDN40-1 to enable RIP security.

1. Enter the Global Configuration mode.

   UltOs# configure terminal

   – Enable RIP globally in the switch FDN40-1.

   UltOs(config)# router rip

   – Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

   UltOs(config-router)# network *10.0.0.1*

   – Enable RIP security.

   UltOs(config-router)# ip rip security *minimum*

   – Exit from the router configuration mode.

   UltOs(config-router)# exit

2. Execute the following commands in the switch FDN40-1 to disable RIP security.

   – Enter the Global Configuration mode.

   UltOs# configure terminal

   – Enable RIP globally in the switch FDN40-1.

   UltOs(config)# router rip

   – Disable RIP security.

   UltOs(config-router)# no ip rip security

   – Exit from the router configuration mode.

   UltOs(config-router)# exit

4.5.3.2 WEB Configuration

RIP security can be set to maximum or minimum through WEB interface using the **RIP Basic Settings** screen (Navigation - **Layer3 Management > RIP > Basic Settings**)

Screen 4-3: RIP Basic Settings

4.5.4 Configuring RIP Packets Retransmission Interval and Retries Count

Refer the section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.4.1 CLI Configuration

1. Execute the following commands in the switch FDN40-1 to configure the RIP packets retransmission interval and retries count.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Configure the retransmission interval.

     UltOs(config-router)# ip rip retransmission interval *10*
   - Configure the retransmission retry count.

     UltOs(config-router)# ip rip retransmission retries *20*
2. View the configured retransmission interval and the number of retries count using the following command.

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 10 seconds
 Number of retransmission retries is 20
```

```
Default metric is 3
Auto-Summarisation of routes is enabled
Routing for Networks :
  10.0.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 30 seconds
 Invalid after 180 seconds
 Flushed after 120 seconds
 Send version is 1 2, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

- Configure the default retransmission interval.

  UltOs(config-router)# no ip rip retransmission interval

- Configure the default retransmission retry count.

  UltOs(config-router)# no ip rip retransmission retries

- Exit from the router configuration mode.

  UltOs(config-router)# exit

3. View the default retransmission interval and number of retries count using the following command.

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specifi Address Summarisation :
 Interface vlan1
  Sending updates every 30 seconds
```

```
Invalid after 180 seconds
Flushed after 120 seconds
Send version is 1 2, receive version is 1 2
Authentication type is none
Split Horizon with poissoned reverse is enabled
Restrcts default route installation
Restricts  default route origination
```

4.5.4.2 WEB Configuration

RIP retransmission interval and maximum retries count can be configured through WEB interface using the **RIP Basic Settings** screen. For screenshot, refer section 4.5.3.2.

4.5.5 Configuring RIP Neighbor

Refer the Section 4.3 for configuration guidelines and Figure 4-2 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1, FDN40-2 and FDN40-3) before configuring RIP.

4.5.5.1 CLI Configuration

Execute the following commands in the switch FDN40-1 to configure the RIP neighbor.

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable RIP globally in the switch FDN40-1.

  UltOs(config)# router rip

- Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16)

  UltOs(config-router)# network *10.0.0.1*

- Configure the RIP trusted neighbor.

  UltOs(config-router)# neighbor *10.0.0.2*

  In FDN40-1, you can view only the routes that are sent as RIP updates from the neighbor router FDN40-2 (10.0.0.2) .

- Delete the configured RIP neighbor.

  UltOs(config-router)# no neighbor *10.0.0.2*

  In FDN40-1, you can view the routes that are sent as RIP updates from both the neighbor routers FDN40-2 (10.0.0.2) and FDN40-3.(10.0.0.3).

- Exit from the router configuration mode.

  UltOs(config-router)# exit

4.5.5.2 WEB Configuration

RIP Neighbor can be set to configured through WEB interface using the **RIP Neighbour List** screen (Navigation - **Layer3 Management > RIP > Neighbors List**)

Screen 4-4: RIP Neighbour List

4.5.6 Configuring RIP Passive Interface

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.6.1 CLI Configuration

1. Execute the following commands in the switch FDN40-1 to configure RIP passive interface.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16)

     UltOs(config-router)# network *10.0.0.1*
   - Configure the passive interface.

     UltOs(config-router)# passive-interface vlan *1*
   - Exit from the router configuration mode.

     UltOs(config-router)# exit
2. View the passive interface configuration information using the following command.

   UltOs# show ip rip statistics

   ```
   RIP Global Statistics:
   ----------------------
   ```

```
 Total number of route changes is 0
 Total number of queries responded is 0
 Total number of periodic updates sent is 0
 Total number of dropped packets is 0
RIP Interface Statistics:
-------------------------
Interface   Periodic      BadRoutes   Triggered
BadPackets   Admin
IP Address  Updates Sent  Received    Updates Sent
Received     Status
----------- ------------  ---------   ------------   -
---------   ------
10.0.0.1        0             0            0
0       Passive
```

- View that no routing updates are sent over the passive interface vlan1

3. Execute the following commands in the switch FDN40-1 to disable RIP passive interface status.
   - Enter Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Disable the passive interface status.

     UltOs(config-router)# no passive-interface vlan *1*
   - Exit from the router configuration mode.

     UltOs(config-router)# exit
4. View the RIP interface for the periodic updates sent over it using the following command.

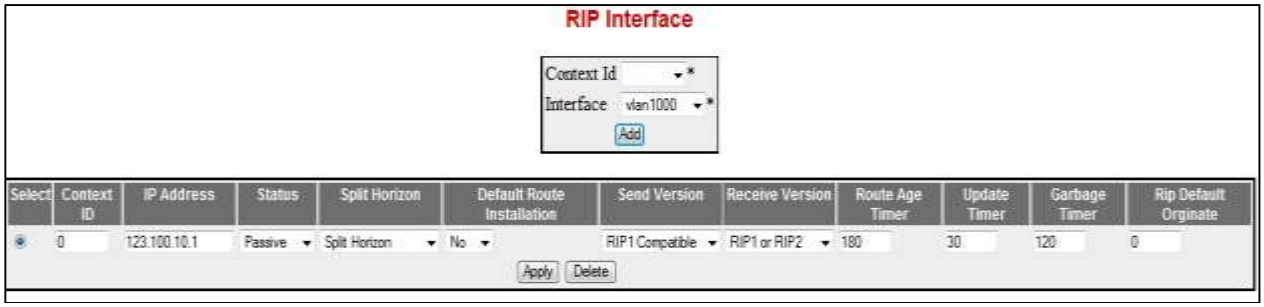
   UltOs# show ip rip statistics

```
RIP Global Statistics:
----------------------
 Total number of route changes is 0
 Total number of queries responded is 0
 Total number of periodic updates sent is 1
 Total number of dropped packets is 0
RIP Interface Statistics:
-------------------------
Interface   Periodic      BadRoutes   Triggered
BadPackets   Admin
```

```
IP Address  Updates Sent  Received    Updates Sent
Received     Status

----------- ------------  ---------   ------------   -
---------   ------

10.0.0.1         1            0            0
0        Enabled
```

4.5.6.2 WEB Configuration

RIP Interface can be configured as passive using the Status field in the **RIP Interface** screen (Navigation - **Layer3 Management > RIP > Interface Configuration**)



Screen 4-5: RIP Interface - Passive

4.5.7 Configuring Output-delay

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.7.1 CLI Configuration

1. Execute the following commands in the switch FDN40-1 to enable the interpacket delay.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Enable the interpacket delay for RIP updates

     UltOs(config-router)# output-delay
   - Exit from the router configuration mode.

     UltOs(config-router)# end
2. View the enabled Output-delay using the following command.

   UltOs# show ip protocols

   ```
   Routing Protocol is rip
   ```

```
RIP2 security level is Maximum
Redistributing : rip
Output Delay is Enabled
Retransmission timeout interval is 5 seconds
Number of retransmission retries is 36
Default metric is 3
Auto-Summarisation of routes is enabled
Routing for Networks :
  10.0.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 30 seconds
 Invalid after 180 seconds
 Flushed after 120 seconds
 Send version is 1 2, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

3. Execute the following commands in the switch FDN40-1 to disable the interpacket delay.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Disable interpacket delay for RIP updates.

     UltOs(config-router)# no output-delay
   - Exit from the router configuration mode.

     UltOs(config-router)# end
4. View the disabled Output-delay using the following command.

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
```

```
Number of retransmission retries is 36
Default metric is 3
Auto-Summarisation of routes is enabled
Routing for Networks :
  10.0.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 30 seconds
 Invalid after 180 seconds
 Flushed after 120 seconds
 Send version is 1 2, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

4.5.7.2 WEB Configuration

Output Delay can be configured through WEB interface using the **RIP Basic Settings** screen. For screenshot, refer section 4.5.3.2

4.5.8 Configuring Redistribution

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.8.1 CLI Configuration

Execute the following commands in the switch FDN40-1 to configure redistribution.

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable RIP globally in the switch FDN40-1.

  UltOs(config)# router rip

- Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

  UltOs(config-router)# network *10.0.0.1*

- Configure the redistribution of static routes into RIP domain.

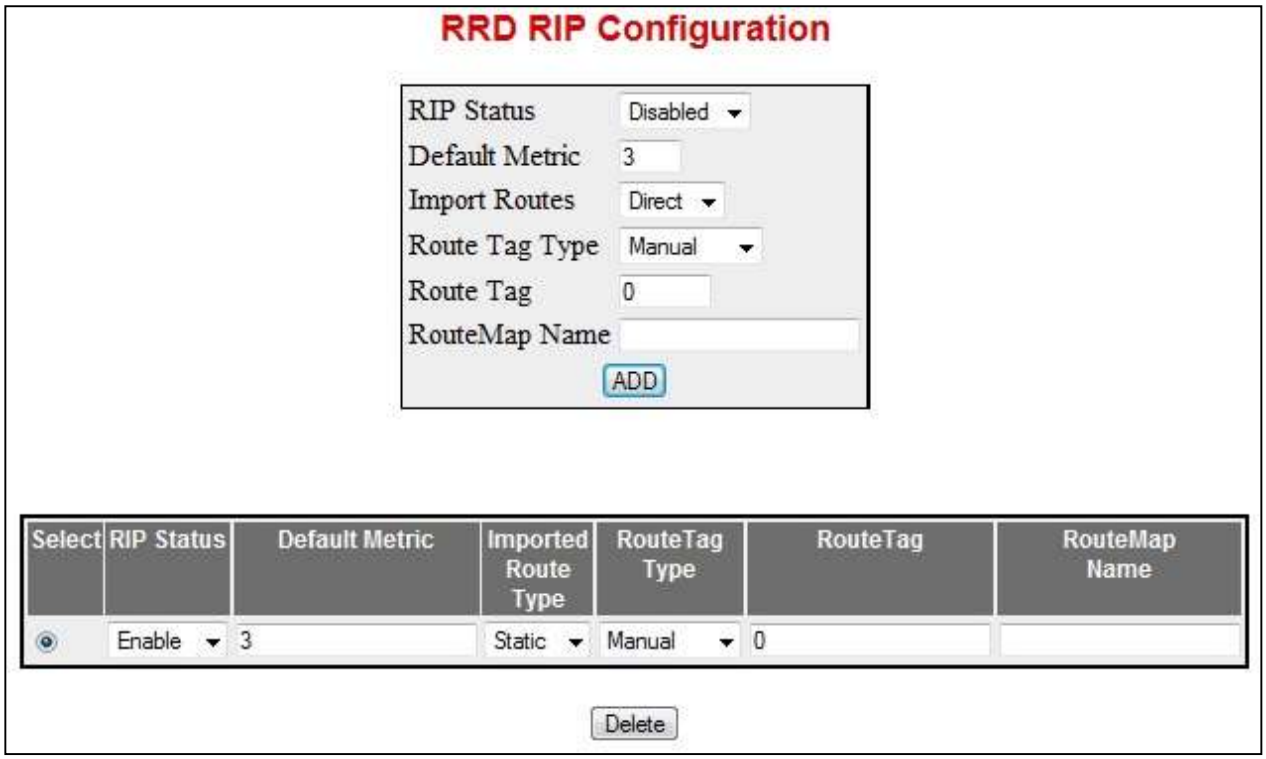
  UltOs(config-router)# redistribute static

- Exit from the router configuration mode.

  UltOs(config-router)# end

4.5.8.2 WEB Configuration

RIP Redistribution can be configured through WEB interface using the **RRD RIP Configuration** screen (Navigation - **Layer3 Management > RRD > RIP**)



Screen 4-6: RRD RIP Configuration

4.5.8.3 Sample Configuration to Test Redistribution

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in the switch FDN40-1 to test redistribution.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16)

     UltOs(config-router)# network *10.0.0.1*
   - Configure redistribution of static routes in the RIP domain

     UltOs(config-router)# redistribute static

     UltOs(config-router)# exit
   - Add static routes

     UltOs(config)# ip route *50.0.0.0 255.0.0.0* **vlan** 2

UltOs(config)# ip route *60.0.0.0 255.0.0.0* **vlan** 2

UltOs(config)# ip route *70.0.0.0 255.0.0.0* **vlan** 2

UltOs(config)# ip route *80.0.0.0 255.0.0.0* **vlan** 2

UltOs(config)# end

2. Execute the following commands in the switch FDN40-2 to test redistribution.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-2.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.2/16)

     UltOs(config-router)# network *10.0.0.2*

     UltOs# config terminal

     UltOs(config)# router rip

     UltOs(config-router)# network *10.0.0.2*

     UltOs(config-router)# end
3. View the redistribution of static routes enabled using the following command.

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip, static
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specific Address Summarisation :
 Interface vlan1
  Sending updates every 30 seconds
  Invalid after 180 seconds
  Flushed after 120 seconds
  Send version is 1 2, receive version is 1 2
  Authentication type is none
  Split Horizon with poissoned reverse is enabled
```

```
Restricts default route installation
Restricts  default route origination
```

4. View the RIP route entries for the static routes added in FDN40-1. (Static routes added in FDN40-1 with metric as 3 are redistributed into the RIP domain. In FDN40-2, view the redistributed static routes with metric as 4.) using the following command.

   UltOs# show ip rip database

```
10.0.0.0/8   [1]        auto-summary
10.0.0.0/16  [1]        directly connected, vlan1
50.0.0.0/8   [4]        auto-summary
50.0.0.0/8   [4]        via 10.0.0.1, vlan1
60.0.0.0/8   [4]        auto-summary
60.0.0.0/8   [4]        via 10.0.0.1, vlan1
70.0.0.0/8   [4]        auto-summary
70.0.0.0/8   [4]        via 10.0.0.1, vlan1
80.0.0.0/8   [4]        auto-summary
80.0.0.0/8   [4]        via 10.0.0.1, vlan1
```

   UltOs# show ip route

```
C 10.0.0.0/16 is directly connected, vlan1
C 30.2.2.0/24 is directly connected, vlan3
R 50.0.0.0/8   [4] via 10.0.0.1
R 60.0.0.0/8   [4] via 10.0.0.1
R 70.0.0.0/8   [4] via 10.0.0.1
R 80.0.0.0/8   [4] via 10.0.0.1
```

5. Execute the following commands in the switch FDN40-1 to disable redistribution.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Disable the redistribution of static routes into RIP domain

     UltOs(config-router)# no redistribute static

     UltOs(config-router)# end.
6. View in FDN40-2, the RIP route entries for the static routes added in FDN40-1, which are made as unreachable with metric as infinity (16) (Static routes added in FDN40-1 are redistributed into the RIP domain.) using the following command.

   UltOs# show ip rip database

```
10.0.0.0/8   [1]         auto-summary
10.0.0.0/16  [1]         directly connected, vlan1
50.0.0.0/8   [16]         via 10.0.0.1, vlan1
60.0.0.0/8   [16]         via 10.0.0.1, vlan1
70.0.0.0/8   [16]         via 10.0.0.1, vlan1
80.0.0.0/8   [16]         via 10.0.0.1, vlan1
```

7. View the RIP route entries for the redistributed static routes are deleted from the IP routing table.

   UltOs# show ip route

   ```
   C 10.0.0.0/16 is directly connected, vlan1
   C 30.2.2.0/24 is directly connected, vlan3
   ```

4.5.9 Configuring Default-metric

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.9.1 CLI Configuration

1. Execute the following commands in the switch FDN40-1 to configure the default-metric.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Configure default-metric for redistributed routes in the RIP domain.

     UltOs(config-router)# default-metric 10
   - Configure redistribution of static routes into RIP domain.

     UltOs(config-router)# redistribute static
   - Exit from the router configuration mode.

     UltOs(config-router)# end

4.5.9.2 WEB Configuration

RIP default metric can be configured through WEB interface using the **RRD RIP Configuration** screen. For screenshot, refer section 4.5.8.2.

4.5.9.3 Sample Configuration to Test Default-metric

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

2. Execute the following commands in the switch FDN40-1 to test default-metric.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network 10.0.0.1
   - Configure default-metric as 10 for redistributing routes into RIP domain.

     UltOs(config-router)# default-metric 10
   - Configure redistribution of static routes into RIP domain.

     UltOs(config-router)# redistribute static

     UltOs(config-router)# exit
   - Add static routes.

     UltOs(config)# ip route *50.0.0.0 255.0.0.0* **vlan** 2

     UltOs(config)# ip route *60.0.0.0 255.0.0.0* **vlan** 2

     UltOs(config)# ip route *70.0.0.0 255.0.0.0* **vlan** 2

     UltOs(config)# ip route *80.0.0.0 255.0.0.0* **vlan** 2

     UltOs(config)# end
3. Execute the following commands in the switch FDN40-2 to test default-metric.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.2/16).

     UltOs(config-router)# network *10.0.0.2*
4. View the metric for redistributed RIP route entries as 10 in FDN40-1 using the following command.

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 10
 Auto-Summarisation of routes is enabled
```

```
Routing for Networks :
  10.0.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 30 seconds
 Invalid after 180 seconds
 Flushed after 120 seconds
 Send version is 1 2, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

UltOs# show ip rip database

```
10.0.0.0/8   [1]        auto-summary
10.0.0.0/16  [1]        directly connected, vlan1
50.0.0.0/8   [10]        auto-summary
50.0.0.0/8   [10]        redistributed via 0.0.0.0
60.0.0.0/8   [10]        auto-summary
60.0.0.0/8   [10]        redistributed via 0.0.0.0
70.0.0.0/8   [10]        auto-summary
70.0.0.0/8   [10]        redistributed via 0.0.0.0
80.0.0.0/8   [10]        auto-summary
80.0.0.0/8   [10]        redistributed via 0.0.0.0
```

5. Execute the following commands in the switch FDN40-1 to disable redistribution.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Disable route redistribution.

     UltOs(config-router)# no redistribute static

     UltOs(config-router)# end.
   - Configure default metric for redistributed routes.

     UltOs(config-router)# no default-metric
   - Enable static route redistribution.

     UltOs(config-router)# redistribute static

UltOs(config-router)# end.

6. View in FDN40-1, the metric for redistributed RIP route entries as 3 using the following command.

   UltOs# show ip rip database

```
10.0.0.0/8[1]      summary route
10.0.0.0/16         directly connected, vlan1
50.0.0.0/8[3]      summary route
50.0.0.0/8 [3]         redistributed via vlan2
60.0.0.0/8[3]      summary route
60.0.0.0/8 [3]         redistributed via vlan2
70.0.0.0/8[3]      summary route
70.0.0.0/8 [3]         redistributed via vlan2
80.0.0.0/8[3]      summary route
80.0.0.0/8 [3]         redistributed via vlan2
```

4.5.10 Configuring Auto-summary

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.10.1 CLI Configuration

1. Execute the following commands in the switch FDN40-1 to configure auto-summary.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Disable auto-summary of RIP routes.

     UltOs(config-router)# auto-summary disable
2. View the disabled auto summarization using the following command.

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
```

```
Default metric is 3
Auto-Summarisation of routes is disabled
Routing for Networks :
  10.0.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 30 seconds
 Invalid after 180 seconds
 Flushed after 120 seconds
 Send version is 1 2, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

3. Execute the following commands in the switch FDN40-1 to enable auto-summary.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable auto-summary of RIP routes.

     UltOs(config-router)# auto-summary Enable
   - Exit from the router configuration mode.

     UltOs(config-router)# end
4. View the enabled auto summarization using the following command.

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
   10.0.0.0
```

```
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 30 seconds
 Invalid after 180 seconds
 Flushed after 120 seconds
 Send version is 1 2, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

4.5.10.2 WEB Configuration

Auto Summary status can be configured through WEB interface using the **RIP Basic Settings** screen. For screenshot, refer section 4.5.3.2

4.5.11 Configuring Interface Specific RIP Parameters

The following configurations are done in the interface mode.

1. Execute the following commands in the switch to configure interface specific RIP parameters.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter the interface configuration mode.

     UltOs(config)# interface vlan *1*

     UltOs(config-if)#
   - Exit from the interface configuration mode

     UltOs(config-if)#exit

4.5.11.1 Configuring RIP Default Route Propagation

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in the switch FDN40-1 to configure RIP default route propagation.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

UltOs(config-router)# network *10.0.0.1*

- Exit router configuration mode.

  UltOs(config-router)# exit

- Enter interface configuration mode.

  UltOs(config)# interface vlan *1*

- Configure RIP default route origination.

  UltOs(config-if)# ip rip default route originate *10*

- Disable rip default route origination.

  UltOs(config-if)# no ip rip default route originate

Refer Section 4.5.11.2.1 for sample configuration to test Default Route Origination and Default Route Installation..

4.5.11.2 Configuring to Install Default Route

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

Execute the following commands in the switch FDN40-1 to install the default route.

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable RIP globally in the switch FDN40-1.

  UltOs(config)# router rip

- Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

  UltOs(config-router)# network *10.0.0.1*

- Exit router configuration mode.

  UltOs(config-router)# exit

- Enter interface configuration mode.

  UltOs(config)# interface vlan *1*

- Enable installation of default route.

  UltOs(config-if)# ip rip default route install

- Disable installation of default route.

  UltOs(config-if)# no ip rip default route install

4.5.11.2.1 Sample Configuration to test Default Route Origination and Installation

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in both the switches.

   - Configure the following in FDN40-1 to test Default Route Origination and Default Route Installation:

     UltOs# configure terminal

UltOs(config)# router rip

UltOs(config-router)# network *10.0.0.1*

UltOs(config-router)# exit

UltOs(config)# interface vlan *1*

- Enable installation of default route.

  UltOs(config-if)# ip rip default route install

  UltOs(config-if)# end

  UltOs#

- Configure the following in FDN40-2 to test Default Route Origination and Default Route Installation.

  UltOs# configure terminal

  UltOs(config)# router rip

  UltOs(config-router)# network *10.0.0.2*

  UltOs(config-router)# exit

  UltOs(config)# interface vlan *1*

- Enable default route origination.

  UltOs(config-if)# ip rip default route originate *11*

  UltOs(config-if)# end

2. View in FDN40-2, the RIP response packet sent out through the interface vlan 1 in the switch FDN40-2. The RIP response packets will have a default route. .

   UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specific Address Summarisation :
 Interface vlan1
  Sending updates every 30 seconds
  Invalid after 180 seconds
  Flushed after 120 seconds
```

```
  Send version is 1 2, receive version is 1 2
  Authentication type is none
  Split Horizon with poissoned reverse is enabled
  Restricts default route installation
  Originate default route
```

3. View in FDN40-1, the default route with next hop as 10.0.0.2 (FDN40-2 interface vlan 1 IP address) and metric as 12 (11+1) using the following command.

UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specific Address Summarisation :
 Interface vlan1
  Sending updates every 30 seconds
  Invalid after 180 seconds
  Flushed after 120 seconds
  Send version is 1 2, receive version is 1 2
  Authentication type is none
  Split Horizon with poissoned reverse is enabled
  Installs default route received
  Restricts  default route origination
```

UltOs# show ip rip database

```
0.0.0.0/0   [12]          via 10.0.0.2, vlan1
10.0.0.0/8   [1]          auto-summary
10.0.0.0/16 [1]           directly connected, vlan1
```

UltOs# show ip route

```
R 0.0.0.0/0   [12] via 10.0.0.2
```

```
C 10.0.0.0/16 is directly connected, vlan1
C 20.0.0.0/24 is directly connected, vlan2
```

4.5.11.3 Configuring Version for Receiving RIP Advertisement

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in the switch FDN40-1 for configuring version for receiving RIP advertisements.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Exit router configuration mode.

     UltOs(config-router)# exit
   - Enter interface configuration mode.

     UltOs(config)# interface vlan *1*
   - Configure version of RIP packets to be received over the interface vlan 1.

     UltOs(config-if)# ip rip receive version 1
2. View how FDN40-1 will receive only RIP version 1 packets over the interface vlan1 using the following command.
   - View the RIP receive version in interface vlan 1 is 1.

     UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specific Address Summarisation :
 Interface vlan1
  Sending updates every 30 seconds
```

```
Invalid after 180 seconds
Flushed after 120 seconds
Send version is 1 2, receive version is 1
Authentication type is none
Split Horizon with poissoned reverse is enabled
Restricts default route installation
Restricts  default route origination
```

4.5.11.4 Configuring Version for Transmitting RIP Advertisement

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands to configure version for transmitting RIP advertisement.
   - Enter Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Exit router configuration mode.

     UltOs(config-router)# exit
   - Enter interface configuration mode.

     UltOs(config)# interface vlan *1*
   - Configure version of RIP packets to be sent over the interface vlan 1.

     UltOs(config-if)# ip rip send version *1*
2. View how FDN40-1 will send (transmit) only RIP version 1 packets over the interface vlan1 using the following command.
   - View the RIP send version in interface vlan 1 is 1.

     UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
```

```
  10.0.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 30 seconds
 Invalid after 180 seconds
 Flushed after 120 seconds
 Send version is 1, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

- Configure the default RIP packets send version

  UltOs(config-if)# no ip rip send version

4.5.11.5 Configuring Timer Basic

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in the switch FDN40-1 to configure Timer Basic.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Exit router configuration mode.

     UltOs(config-router)# exit
   - Enter interface configuration mode.

     UltOs(config)# interface vlan *1*
   - Configure basic timers.

     UltOs(config-if)# timers basic *60 120 120*

     UltOs(config-if)# end
2. View the RIP update packets that are sent after 60 seconds and the configured timer values using the following command.

   UltOs# show ip protocols

   ```
   Routing Protocol is rip
    RIP2 security level is Maximum
   ```

```
Redistributing : rip
Output Delay is disabled
Retransmission timeout interval is 5 seconds
Number of retransmission retries is 36
Default metric is 3
Auto-Summarisation of routes is Enabled
Routing for Networks :
  10.0.0.0
Routing Information Sources :
Interface Specific Address Summarisation :
Interface vlan1
 Sending updates every 60 seconds
 Invalid after 120 seconds
 Flushed after 120 seconds
 Send version is 1 2, receive version is 1 2
 Authentication type is none
 Split Horizon with poissoned reverse is enabled
 Restricts default route installation
 Restricts  default route origination
```

4.5.11.6 Configuring RIP Split Horizon

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

By default, split horizon with poisson reverse will be enabled on all the RIP interfaces.

1. Execute the following commands in the switch FDN40-1 to configure RIP Split Horizon.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Exit router configuration mode.

     UltOs(config-router)# exit
   - Enter interface configuration mode.

     UltOs(config)# interface vlan *1*

– Enable split horizon.

UltOs(config-if)# ip split-horizon

2. View the split horizon enabled in FDN40-1 using the following command.

UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specific Address Summarisation :
 Interface vlan1
  Sending updates every 30 seconds
  Invalid after 180 seconds
  Flushed after 120 seconds
  Send version is 1 2, receive version is 1 2
  Authentication type is none
  Split Horizon is enabled
  Restricts default route installation
  Restricts  default route origination
```

- Disable split horizon.

UltOs(config-if)# no ip split-horizon

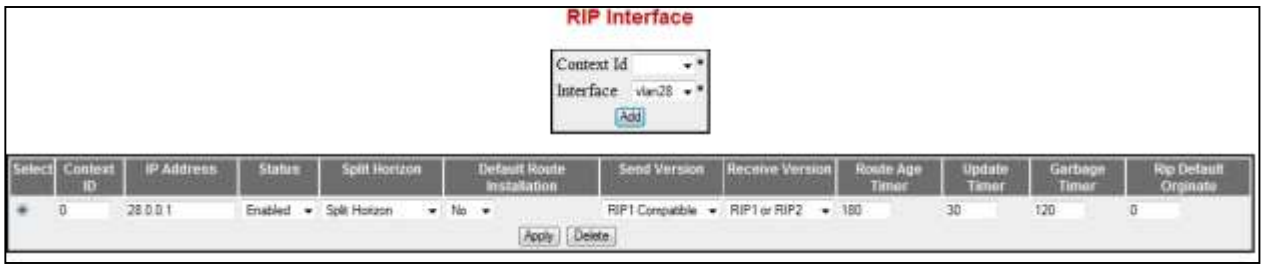
- Enable split horizon with poison reverse.

UltOs(config-if)# ip split-horizon poisson

UltOs(config-if)# end

4.5.11.7 WEB Configuration for RIP Interface Paramters

RIP interface parameters can be configured through WEB interface using the **RIP Interface** screen (Navigation - **Layer3 Management > RIP > Interface Configuration**)



Screen 4-7: RIP Interface - Parameters

4.5.12 Configuring RIP Summary-address

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.12.1 CLI Configuration

Execute the following commands in the switch FDN40-1 to configure RIP summary-address.

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable RIP globally in the switch FDN40-1.

  UltOs(config)# router rip

- Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

  UltOs(config-router)# network *10.0.0.1*

- Disable auto-summary feature.

  UltOs(config-router)# auto-summary disable

- Exit router configuration mode.

  UltOs(config-router)# exit

- Enter the interface configuration mode.

  UltOs(config)# interface vlan *1*

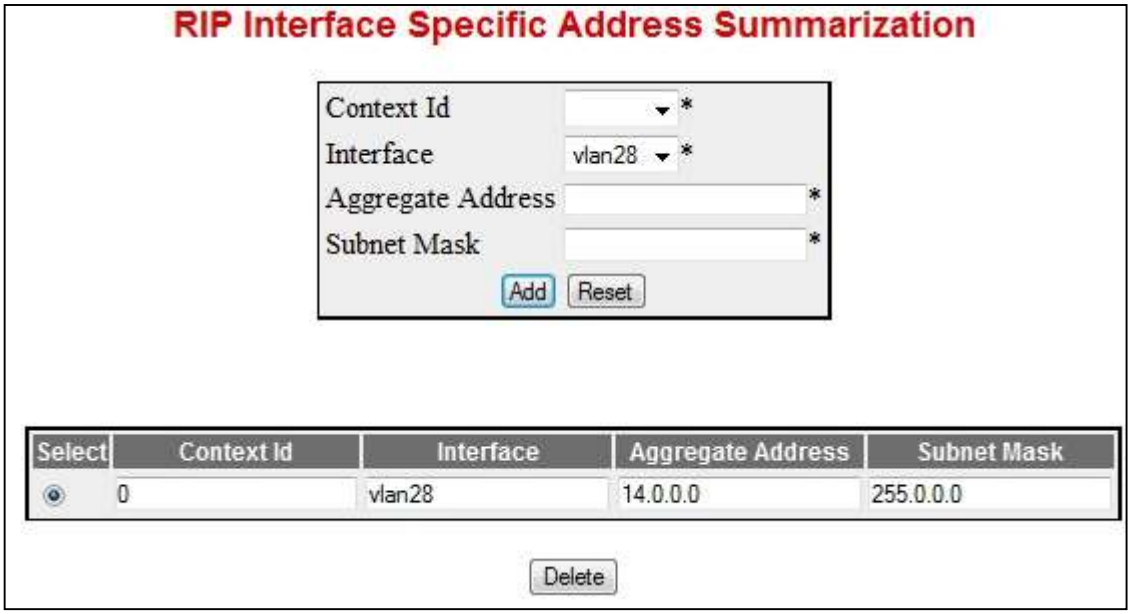
- Configure the version of RIP packets to be sent over the interface vlan 1.

  UltOs(config-if)# ip rip summary-address *40.0.0.0 255.0.0.0*

  UltOs(config-if)# end

4.5.12.2 WEB Configuration

RIP Summary Address can be configured through WEB interface using the **RIP Interface Specific Address Summarization** screen (Navigation - **Layer3 Management > RIP > Interface Configuration**)



Screen 4-8: RIP Interface Specific Address Summarization

4.5.12.3 Sample Configuration to configure RIP summary-address

Refer the Section 4.3 and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following configuration commands in FDN40-1 to configure RIP summary-address.

   UltOs# configure terminal

   UltOs(config)# router rip

   UltOs(config-router)# network *10.0.0.1*

   UltOs(config-router)# redistribute all

   – Disable auto-summary feature.

   UltOs(config-router)# auto-summary disable

   UltOs(config-router)# exit

   – Configure Static routes:

   UltOs(config-router)# ip route *40.1.0.0 255.255.0.0* **vlan** 2

   UltOs(config-router)# ip route *40.2.0.0 255.255.0.0* **vlan** 2

   UltOs(config-router)# ip route *40.3.0.0 255.255.0.0* **vlan** 2

   UltOs(config-router)# ip route *40.4.0.0 255.255.0.0* **vlan** 2

   – Configure Summary address for 20.0.0.0/8:

   UltOs(config)# interface vlan *1*

   UltOs(config-if)# ip rip summary-address *40.0.0.0 255.0.0.0*

   UltOs(config-if)#end

   UltOs#

2. Execute the following configuration commands in FDN40-2.

   UltOs# config terminal

   UltOs(config)# router rip

   UltOs(config-router)# network *10.0.0.2*

   UltOs(config-router)# end

4.5.13 Configuring Interface Specific Authentication

Refer the section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

4.5.13.1 CLI Configuration

1. Execute the following commands in the switch FDN40-1 to enable interface specific authentication.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable RIP globally in the switch FDN40-1.

     UltOs(config)# router rip
   - Enable RIP over the interface vlan 1 (IP address 10.0.0.1/16).

     UltOs(config-router)# network *10.0.0.1*
   - Exit router configuration mode.

     UltOs(config-router)# exit
   - Enter interface configuration mode.

     UltOs(config)# interface vlan *1*
   - Enable md5 authentication.

     UltOs(config-if)# ip rip authentication mode md5 key-chain *12345*
   - Enable sha-1 Crypto authentication

     UltOs(config-if)# ip rip auth-type sha-1
   - Enable sha-1 Crypto authentication

     UltOs(config-if)# ip rip auth-type sha-256
   - Enable sha-1 Crypto authentication

     UltOs(config-if)# ip rip auth-type sha-384
   - Enable sha-1 Crypto authentication
   - **UltOs(config-if)# ip rip auth-type sha-512**Create crypto authentication key-id

     UltOs(config-if)# ip rip authentication key-id 1 key FSS
   - Configure the start-generate time for crypto authentication key-id

     UltOs(config-if)# ip rip key-id 1 start-generate 2013-05-12,21:40:20

- Configure the stop-generate time for crypto authentication key-id

  UltOs(config-if)# ip rip key-id 1 stop-generate 2013-05-12,22:40:20

- Configure the start-accept time for crypto authentication key-id

  UltOs(config-if)# ip rip key-id 1 start-accept 2013-05-12,21:40:20

- Configure the stop-accept time for crypto authentication key-id

  UltOs(config-if)# ip rip key-id 1 stop-accept 2013-05-12,22:40:20

- Delete the configured crypto authentication key-id

  UltOs(config-if)# no ip rip authentication key-id 1

- Disable authentication.

  UltOs(config-if)# no ip rip authentication

2. Execute the following commands in FDN40-1 to enable authentication last-key lifetime status.
   - Enter the Global Configuration mode.

     UltOs# configure terminal

   - Configure the lifetime status for authentication key-id.
   - **UltOs(config)# rip authentication last-key infinite lifetime true**

4.5.13.2 WEB Configuration

RIP Authentication can be configured through WEB interface using the **RIP Security Settings** screen (Navigation - **Layer3 Management > RIP > Security Settings**)

Screen 4-9: RIP Security Settings

4.5.13.3 Sample Configuration for Enabling Authentication

Refer the section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in both the switches for enabling authentication.
   - Configure the following in FDN40-1:

UltOs# config terminal

UltOs(config)# router rip

UltOs(config-router)# network *10.0.0.1*

UltOs(config-router)# redistribute all

UltOs(config-router)# exit

- Enable md5 authentication

  UltOs(config)# interface vlan *1*

  UltOs(config-if)# ip rip authentication mode md5 key-chain *12345*

  UltOs(config-if)#end

  UltOs#

- Configurations in FDN40-2:

  UltOs# config terminal

  UltOs(config)# router rip

  UltOs(config-router)# network *10.0.0.2*

  UltOs(config-router)# exit

- Enable md5 authentication

  UltOs(config)# interface vlan *1*

  UltOs(config-if)# ip rip authentication mode md5 key-chain *12345*

  UltOs(config-if)#end

  UltOs#

2. View in FDN40-1, the authentication type using the following command.
   - View in FDN40-1 all the RIP packets have authentication information.

     UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specific Address Summarisation :
 Interface vlan1
```

```
Sending updates every 30 seconds
Invalid after 180 seconds
Flushed after 120 seconds
Send version is 1 2, receive version is 1 2
Authentication type is md5
Split Horizon with poissoned reverse is enabled
Restricts default route installation
Restricts  default route origination
```

- View in FDN40-2, all the RIP packets have authentication information.

4.5.13.4 Sample Configuration for Enabling Crypto Authentication

Refer the section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

1. Execute the following commands in both the switches for enabling authentication.
   - Configure the following in FDN40-1:

     UltOs# config terminal

     UltOs(config)# router rip

     UltOs(config-router)# network *10.0.0.1*

     UltOs(config-router)# redistribute all

     UltOs(config-router)# exit

     Enable any one of the crypto authentication **UltOs(config)# interface vlan** *1*

     UltOs(config-if)# ip rip auth-type sha-1

     UltOs(config-if)# ip rip authentication key-id *1* **key** *FSS*

     UltOs(config-if)# ip rip key-id 1 start-generate *2013-05-12,21:40:20*

     UltOs(config-if)# ip rip key-id 1 stop-generate *2013-05-12,22:40:20*

     UltOs(config-if)# ip rip key-id 1 start-accept *2013-05-12,21:40:20*

     UltOs(config-if)# ip rip key-id 1 stop-accept *2013-05-12,22:40:20*

     UltOs(config-if)#end

     UltOs#

   - Multiple keys can be configured over an interface, If the start time for generate, accept & stop time for generate, accept are not configured default values will be taken.

     UltOs# config terminal

     UltOs(config)# interface vlan *1*

UltOs(config-if)# ip rip auth-type sha-1

UltOs(config-if)# ip rip authentication key-id *2* **key** *FSS2*

UltOs(config-if)#end

UltOs#

- Configure the following in FDN40-2:

  UltOs# config terminal

  UltOs(config)# router rip

  UltOs(config-router)# network *10.0.0.2*

  UltOs(config-router)# redistribute all

  UltOs(config-router)# exit

- Enable any one of the crypto authentication

  UltOs(config)# interface vlan *1*

  UltOs(config-if)# ip rip auth-type sha-1

  UltOs(config-if)# ip rip authentication key-id 1 key FSS

  UltOs(config-if)# ip rip key-id 1 start-generate *2013-05-12,21:40:20*

  UltOs(config-if)# ip rip key-id 1 stop-generate *2013-05-12,22:40:20*

  UltOs(config-if)# ip rip key-id 1 start-accept *2013-05-12,21:40:20*

  UltOs(config-if)# ip rip key-id 1 stop-accept *2013-05-12,22:40:20*

  UltOs(config-if)#end

  UltOs#

- Multiple keys can be configured over an interface, If the start time for generate, accept & stop time for generate, accept are not configured default values will be taken.

  UltOs# config terminal

  UltOs(config)# interface vlan *1*

  UltOs(config-if)# ip rip auth-type sha-1

  UltOs(config-if)# ip rip authentication key-id *2* **key** *FSS2*

  UltOs(config-if)#end

  UltOs#

2. View the configured authentication information and the active key-id in use during packet transmission in FDN40-1 & FDN40-2 using the following show commands,

   UltOs# show ip rip authentication

```
RIP Interface Authentication Statistics:
Vrf default
Interface Name                  vlan1
Authentication Type             sha-1
```

```
Authentication KeyId in use:     1
Authentication Last key status:  true

RIP Authentication Key Info:
Authentication KeyId        1
Start Accept Time           2013-05-12,21:40:20
Start Generate Time         2013-05-12,21:40:20
Stop Generate Time          2013-05-12,22:40:20
Stop Accept Time            2013-05-12,22:40:20

Authentication KeyId        2
Start Accept Time           2013-05-11,13:13:37
Start Generate Time         2013-05-11,13:13:37
Stop Generate Time          2136-02-06,06:28:15
Stop Accept Time            2136-02-06,06:28:15
```

UltOs# show ip protocols

```
Routing Protocol is rip
 RIP2 security level is Maximum
 Redistributing : rip
 Output Delay is disabled
 Retransmission timeout interval is 5 seconds
 Number of retransmission retries is 36
 Default metric is 3
 Auto-Summarisation of routes is Enabled
 Routing for Networks :
   10.0.0.0
 Routing Information Sources :
 Interface Specific Address Summarisation :
 Interface vlan1
  Sending updates every 30 seconds
  Invalid after 180 seconds
  Flushed after 120 seconds
  Send version is 1 2, receive version is 1 2
  Authentication type is sha-1
  Split Horizon with poissoned reverse is enabled
  Restricts default route installation
  Restricts  default route origination
```

4.5.14 Configuring Debug Level for RIP

Refer the Section 4.3 for configuration guidelines and Figure 4-1 for the Setup. The prerequisite configuration needs to be done in the switches (FDN40-1 and FDN40-2) before configuring RIP.

Execute the following commands in the switch FDN40-1 to configure the debug level for RIP.

UltOs# config terminal

UltOs(config)# router rip

UltOs(config-router)# network *10.0.0.1*

UltOs(config-router)# end

– Configure the debug level for RIP module.

UltOs# debug ip rip all

```
 RIP: Sending regular Update over this interface 0

RIP: Authentication not needed for this interface,
So 25 routes can be composed

RIP: If Agg Rt added to update with metric : 3

RIP: Sending RIP update through Port 0

RIP: Sending regular Update over this interface 0

RIP: Authentication not needed for this interface,
So 25 routes can be composed

RIP: If Agg Rt added to update with metric : 3

RIP: Sending RIP update through Port 0

RIP: Sending regular Update over this interface 0

RIP: Authentication not needed for this interface,
So 25 routes can be composed

RIP: If Agg Rt added to update with metric : 3
```

– Disable the debug level for RIP module.

UltOs# no debug ip rip all

4.5.15 Configuring Route Map – RIP

URM (Unified Route Map) is a portable implementation of the route map capability for IPv4 and IPv6 unicast routing software. The URM provides a single interface for the administrator to set up and manage route maps. It also provides a common unified method for routing protocols and static route management software to use route maps for different purposes. The independent nature of the implementation helps to avoid the duplication of the route maps in the different routing modules in a router.

4.5.15.1 Configuring Route Map

4.5.15.1.1 CLI Configuration

This section lists the CLI configuration steps to define a route map with a specified name and the related parameters such as permission and sequence number.

1. Enter the Global configuration mode.

   UltOs# configure terminal

2. Configure the route map name, permission and sequence number.

   UltOs(config)# route-map aa permit *1*

3. View the configured route map

   UltOs# show route-map

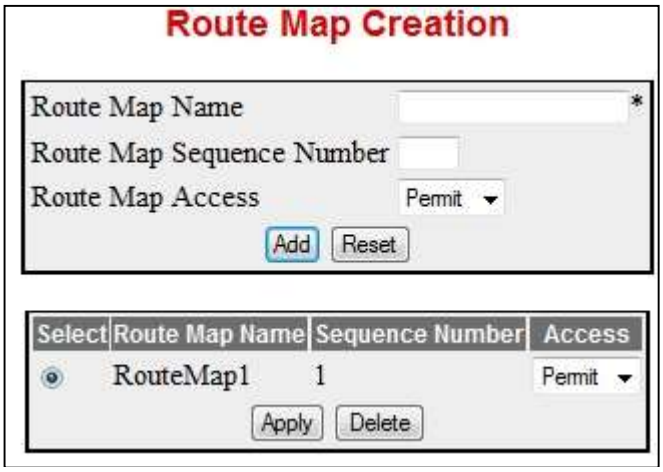
```
Route-map aa, Permit, Sequence 1
Match Clauses:
--------------
Set Clauses:
--------------
```

4. Execute the no form of the command to delete the route map.

   UltOs(config)# no route-map aa 1

4.5.15.1.2 WEB Configuration

Route Map can be created through WEB interface using the **RouteMap Creation** screen (Navigation - **Layer3 Management** > **Route Map** > **Route Map Creation**)



Screen 4-10: RouteMap Creation

4.5.15.2 Configuring Route Map Match Criteria

4.5.15.2.1 CLI Configuration

This section lists the CLI configuration steps to define the filtering criteria for the route map and its related parameters.

1. Enter the Global configuration mode.

   UltOs# configure terminal
2. Configure the route map name, permission and sequence number.

   UltOs(config)# route-map aa permit *1*
3. Configure the route map match source IP address and the subnet mask.

   UltOs(config-rmap-aa)# match source ip *34.0.0.3 255.0.0.0*
4. Configure the route map match source IPv6 address and the prefix length.

   UltOs(config-rmap-aa)# match source ipv6 *2120::3 64*
5. Configure the route map match destination IP address and the subnet mask.

   UltOs(config-rmap-aa)# match destination ip *91.0.0.1 255.0.0.0*
6. Configure the route map match destination IPv6 address and the prefix length.

   UltOs(config-rmap-aa)# match destination ipv6 *2150::2 64*
7. Configure the route map match route-type as remote. (Route-type can be configured either as local or remote.)

   UltOs(config-rmap-aa)# match route-type remote
8. Configure the route map match metric-type as inter-area. (Metric type can be inter-area / intra-area / type-1-external / type-2-external.)

   UltOs(config-rmap-aa)# match metric-type inter-area
9. Configure the route map match metric value.

   UltOs(config-rmap-aa)# match metric *44*
10. Configure the route map match next-hop IP address.

    UltOs(config-rmap-aa)# match next-hop ip *91.0.0.1*
11. Configure the route map match next-hop IPv6 address.

    UltOs(config-rmap-aa)# match next-hop ipv6 *3000::3*
12. Configure the route map match tag.

    UltOs(config-rmap-aa)# match tag *10*
13. View the configured parameters.

    UltOs# show running-config route-map

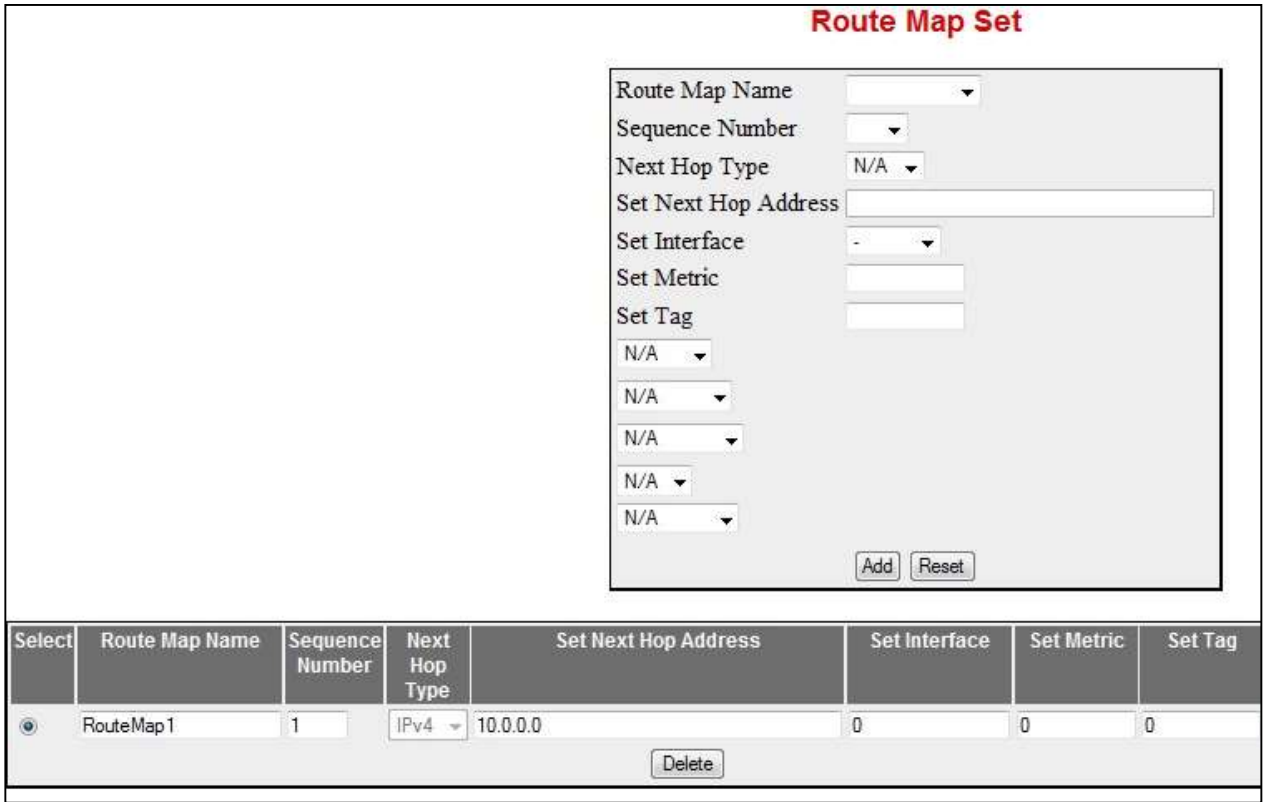
```
Building configuration...
route-map aa permit 1
 match destination ip 91.0.0.1  255.0.0.0
 match destination ipv6 2150::2  64
 match source ip 34.0.0.3  255.0.0.0
 match source ipv6 2120::3  64
 match next-hop ip 91.0.0.1
 match next-hop ipv6 3000::3
 match metric 44
 match tag 10
```

```
match metric-type inter-area
match route-type remote
end
```

14. Execute the no form of the commands to delete the corresponding configurations.

4.5.15.2.2 WEB Configuration

Route Map Match criteria can be configured through WEB interface using the **RouteMap Creation** screen (Navigation - **Layer3Management > Route Map > Route Map Match**)



Screen 4-11: RouteMap Match

4.5.15.3 Configuring RIP Distance

4.5.15.3.1 CLI Configuration

This section lists the CLI configuration steps to set the administrative distance for the RIP router.

1. Enter the Global configuration mode.

   UltOs# configure terminal

2. Enter the RIP router configuration mode.

   UltOs(config)# router rip

3. Configure the distance for the RIP routes.

   UltOs(config-router)# distance *100*

4. View the configured distance.

   UltOs# show running-config rip

```
Building configuration...
router rip
distance  100
!
end
```

   UltOs#

5. Execute the no form of the command to re-configure the distance to its default value.

   UltOs(config-router)# no distance

6. View the configured distance.

   UltOs# sh running-config rip

```
Building configuration...
router rip
!
end
UltOs#
```

4.5.15.3.2 WEB Configuration

RIP Diatance can be configured through WEB interface using the **RIP Basic Settings** screen. For screenshot, refer section 4.5.3.2

4.5.15.4 Configuring Redistribution with Route Map

4.5.15.4.1 CLI Configuration

This section lists the CLI configuration steps to configure the protocol from which the routes have to be redistributed into RIP, by applying the route-map.

1. Enter the Global configuration mode.

   UltOs# configure terminal

2. Enable the RIP router configuration mode.

   UltOs(config)# router rip

3. Configure the network.

   UltOs(config-router)# network *12.0.0.1*

4. Configure the redistribution of all routes with route-map aa.

   UltOs(config-router)# redistribute all route-map *aa*

5. View the configured parameters.

```
UltOs# show running-config rip
Building configuration...
router rip
 redistribute all route-map aa
```

```
 network 12.0.0.1
!
interface vlan 1
!
end
UltOs#
```

6. Execute the no form of the command to disable the redistribution of all routes with route-map.

   UltOs(config-router)# no redistribute all route-map *aa*

7. View the configured parameters after disabling the redistribution of all the routes with route map.

```
UltOs# sh running-config rip
Building configuration...
router rip
 network 12.0.0.1
!
interface vlan 1
!
end
UltOs#
```

4.5.15.5 WEB Configuration

RIP redistribution can be configured through WEB interface using the **RRD RIP Configuration** screen. For screenshot, refer section 4.5.8.2.

Chapter 5

VLAN

5.1 Protocol Description

Virtual LAN (VLAN) technology, defined under the IEEE 802.1q specifications, allows enterprises to extend the reach of their corporate networks across WAN. VLANs enable partitioning of a LAN based on functional requirements, while maintaining connectivity across all devices on the network. VLAN groups network devices and enable them to behave as if, they are in one single network. Data security is ensured by keeping the data exchanged between the devices of a particular VLAN within the same network.

VLAN offers a number of advantages over traditional LAN. They are:

- **Performance**

  In networks with traffic consisting of a high percentage of broadcasts and multicasts, VLAN minimizes the possibility of sending the broadcast and multicast traffic to unnecessary destinations.

- **Formation of Virtual Workgroups**

  VLAN helps in forming virtual workgroups. During this period, communication between the members of the workgroup will be high. Broadcasts and multicasts can be restricted within the workgroup.

- **Simplified Administration**

  Most of the network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, recabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLANs.

- **Reduced Cost**

  VLANs can be used to create broadcast domains, which eliminate the need for expensive routers.

- **Security**

  Sensitive data may be periodically broadcast on a network. Placing only those users, who are allowed to access to such sensitive data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion.

VLAN logically segments the shared media LAN, forming virtual workgroups. It redefines and optimizes the basic Transparent Bridging functionalities such as learning, forwarding, filtering and flooding.

5.2 Topology

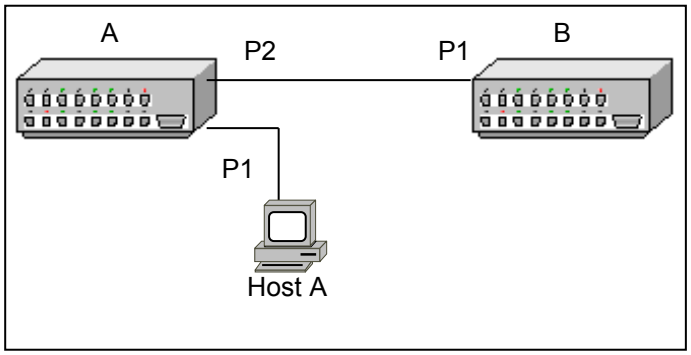


Figure 5-1: Topology for VLAN Configuration

5.3 Configuration Guidelines

- VLAN is enabled in the switch by default. GVRP and GMRP must be disabled prior to disabling VLAN.
- The default interface - VLAN 1- cannot be deleted in the switch.
- If port GVRP state is disabled, but global GVRP status is enabled, then GVRP is disabled on current port. GVRP packets received on that port will be discarded and GVRP registrations from other ports will not be propagated on this port.
- GARP cannot be started, if VLAN is shutdown, and GARP cannot be shutdown, if GVRP and/or GMRP are enabled.
- Mapping of forwarding database identifier (FID) to VLANs is successful only when, VLAN learning mode is hybrid.
- To configure a static unicast/multicast MAC address in the forwarding database, VLAN must have been configured and member ports must have been configured for the specified VLAN.
- Bridge-mode status cannot be set to provider mode, if the protocol/MAC based VLAN is enabled.
- It is not possible to configure a port as trunk, if the port is an untagged member of a VLAN.
- To enable Dot1q-tunneling status, Bridge Mode must be set to 'provider'..
- It is not possible to set the Dot1q-tunnel status on the port, if the port mode is not 'access' type.
- To enable Dot1q tunneling on a port 802.1X (PNAC), port control must be force-authorized.

- BPDU tunneling on the port cannot be set; if Dot1q tunnel status is disabled.
- Leave Timer must be two times greater than Join Timer, and Leaveall Timer must be greater than Leave Timer.

5.4 Default Configurations

Table 5-1: Default Configurations

Feature	Default Setting
VLAN Module status	Enable
Default VLAN Id configured in the switch	1
Mac based VLAN Classification	Disabled
Protocol-VLAN based classification	Enabled
System and port level GVRP and GMRP Module status	Enabled
Mac address table aging time	300 seconds
Acceptable frame types	All (Accepts untagged frames or priority-tagged frames or tagged frames received on the port)
Ingress filtering	Disabled
Switch port priority	0
Switch port mode	Hybrid
GARP Timers	Join: 20 seconds Leave: 60 seconds Leave all: 1000 seconds
Max traffic classes	Maximum number of traffic classes supported on a port is 8
Tunneling	Disabled

In case of Provider Bridges, the default configurations and configuration guidelines are provided in the relevant subsection itself.

5.5 VLAN Configurations

5.5.1 Configuring Static VLAN

Static VLAN entries can be configured with the required number of member ports, untagged ports and forbidden ports. The following configuration deals with the creation of member ports.

5.5.1.1 CLI Configuration

1. Execute the following commands to configure Static VLAN entry in the switch.
   - Enter the Global Configuration Mode.

     UltOs# configure terminal
   - Enter the VLAN Configuration Mode (for VLAN 2).

UltOs(config)# VLAN *2*

- Add member ports for VLAN.

  UltOs(config-vlan)# ports *lan 0/2-5* **untagged** *lan 0/3*

  Member ports represent the set of ports permanently assigned to the VLAN egress list. Frames belonging to the specified VLAN are forwarded to the ports in the egress list.

  If the port type is not explicitly specified as untagged, then all the ports are configured to be of tagged port type allowing transmission of frames with the specified VLAN tag. The **untagged** setting allows the port to transmit the frames without a VLAN tag. This setting is used to configure a port connected to an end user device.

  In the above example, the packets for the interface lan 0/3 are transmitted without the tag. On all the other ports, the packets are transmitted with the tag.

- Configure port 1 as forbidden port.

  UltOs(config-vlan)# ports *lan 0/2-5* **forbidden** *lan 0/1*

  Alternatively, the **forbidden** setting prevents the port from participating in the specified VLAN activity and ensures that, any dynamic requests for the port to join the VLAN will be ignored.

- Exit from the configuration mode.

  UltOs(config)# end

2. View the VLAN information by executing the following command.

   UltOs# show VLAN summary

   ```
   Number of VLANs: 2
   ```

   The output displays the number of VLANs in a switch.

3. View the configuration details of all the VLANs by executing the following show command.

   UltOs# show VLAN

   ```
   VLAN database
   -------------
   VLAN ID              : 1
   Member Ports         : Lan0/1, Lan0/2, Lan0/3, Lan0/4,
   Gi0/5, Gi0/6
                          Gi0/7,  Gi0/8,  Gi0/9,  Lan0/10,
   Lan0/11, Lan0/12
                          Lan0/13,    Lan0/14,    Lan0/15,
   Lan0/16, Lan0/17, Lan0/18
                          Lan0/19,    Lan0/20,    Lan0/21,
   Lan0/22, Lan0/23, Lan0/24
   Untagged Ports       : Lan0/1, Lan0/2, Lan0/3, Lan0/4,
   Gi0/5, Gi0/6
                          Gi0/7,  Gi0/8,  Gi0/9,  Lan0/10,
   Lan0/11, Lan0/12
   ```

```
                        Lan0/13,    Lan0/14,    Lan0/15,
Lan0/16, Lan0/17, Lan0/18
                        Lan0/19,    Lan0/20,    Lan0/21,
Lan0/22, Lan0/23, Lan0/24
Forbidden Ports     : None
Name                :
Status              : Permanent
-------------------------------------------------
VLAN ID             : 2
Member Ports        : Lan0/2, Lan0/3, Lan0/4, Gi0/5
Untagged Ports      : None
Forbidden Ports     : Lan0/1
Name                :
Status              : Permanent
-------------------------------------------------
```

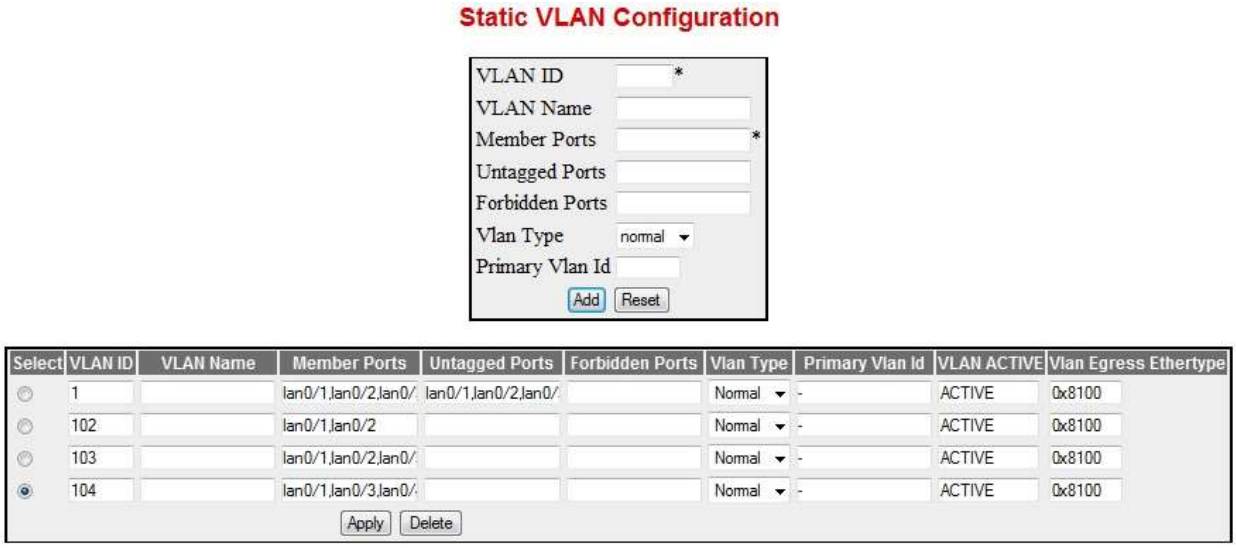
4. View the configuration details of a particular VLAN by executing the following command.

   UltOs# show VLAN id *2*

```
VLAN database
-------------
VLAN ID             : 2
Member Ports        : Lan0/2, Lan0/3, Lan0/4, Gi0/5
Untagged Ports      : None
Forbidden Ports     : Lan0/1
Name                :
Status              : Permanent
-----------------------------------------------
```

5.5.1.2 WEB Configuration

Static VLAN can be configured through WEB interface using the **Static VLAN Configuration** screen (Navigation - **Layer2 Management > VLAN > StaticVLANs)**



Screen 5-1: Static VLAN Configuration

5.5.2 Deleting a VLAN

5.5.2.1 CLI Configuration

It is possible to delete a VLAN from the VLAN list using the **no vlan <vlan-id(1-4094)>** Global Configuration Mode command.

UltOs(config)# no vlan *4*

The default VLAN - VLAN 1 - cannot be deleted.

5.5.2.2 Web Configuration

VLAN can be deleted through WEB interface using the **Static VLAN Configuration** screen. For screenshot, refer section 5.5.1.2

5.5.3 Enabling VLANs

A VLAN can be made active by adding a member port to a VLAN (refer section Configuring Static)

5.5.4 Classifying Frames to a VLAN

As per the IEEE standards, rules are defined for classifying the frames in a VLAN. VLAN classification is accomplished by associating a VLAN ID with each port on the switch. Optionally, frames can be classified according to the protocol identifier contained within the frame. Frame classification priority begins with VLAN Tag; followed by MAC based, protocol match, and finally the PVID.

5.5.4.1 Port Based Classification

In port-based classification, the VLAN ID associated with an untagged or priority-tagged frame is determined, based on the port on which the frame

arrives. Port-based classification requires the association of a specific VLAN ID, the port VLAN identifier (PVID) with each port.

A port can be a member of only one port-based VLAN.

If PVID value has not been explicitly configured for a port, then PVID assumes a default value of 1.

1. Execute the following commands to configure the PVID that is assigned to untagged/priority-tagged frames.
   - Enter the Global Configuration Mode.

     UltOs# configure terminal
   - Enter the Interface Configuration Mode for port gigabitethernet 0/1.

     UltOs(config)# interface lan *0/1*
   - Configure the PVID that is to be assigned to untagged/priority-tagged frames.

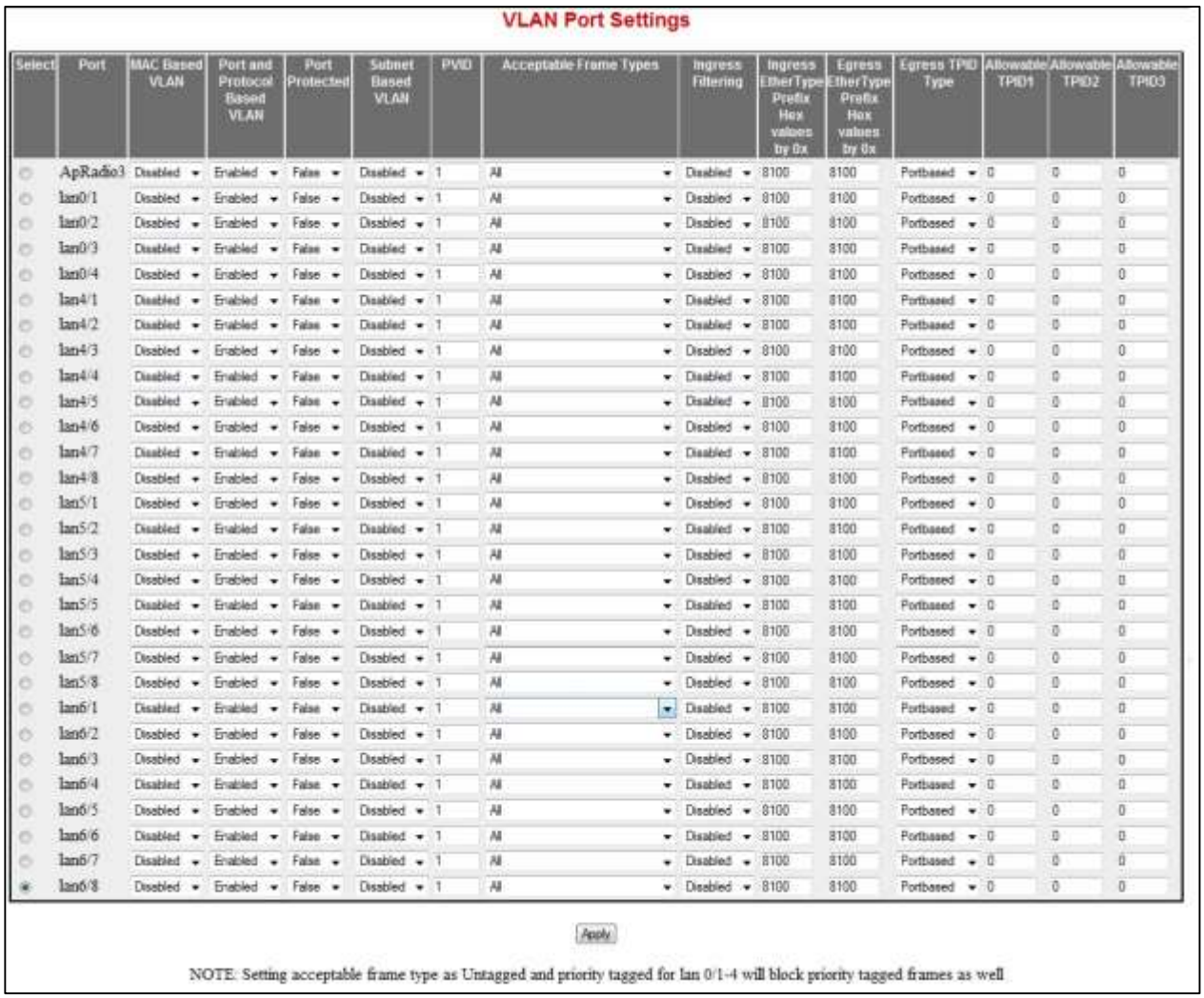
     UltOs(config-if)# switchport pvid
2. View the configuration details by executing the following show command.

   UltOs# show VLAN port config port lan *0/1*

```
VLAN Port configuration table
------------------------------
Port lan0/1

 Port VLAN ID                        : 4
 Port Acceptable Frame Type          : Admit All
 Port Ingress Filtering              : Disabled
 Port Mode                           : Hybrid
 Port Gvrp Status                    : Enabled
 Port Gmrp Status                    : Enabled
 Port Gvrp Failed Registrations      : 0
 Gvrp  last  pdu  origin                          :
00:00:00:00:00:00
 Port Restricted VLAN Registration   : Disabled
 Port Restricted Group Registration  : Disabled
 Mac Based Support                   : Disabled
 Port-and-Protocol Based Support     : Enabled
 Default Priority                    : 0
 ------------------------------------------------
```

5.5.4.2 WEB Configuration

VLAN Frame Classification can be configured through WEB interface using **VLAN Port Settings** screen (Navigation - **Layer2 Management > VLAN > PortSettings)**



Screen 5-2: VLAN Port Settings

5.5.5 Configuring Port Filtering

5.5.5.1 Configuring Acceptable Frametype

It is possible to configure the acceptable frame type for the port as one of the following:

- All frames
- Tagged frames
- Untagged and priority tagged frames.

1. Execute the following commands to configure the acceptable frame type for the port.
   - Enter the Global Configuration Mode.

     UltOs# configure terminal

   - Enter the Interface Configuration Mode and configure the frame type of the port as “tagged” for that interface.

     UltOs(config)# interface lan 0/2

UltOs(config-if)# switchport acceptable-frame-type *tagged*

2. View the configuration information by executing the following show command.

UltOs# show VLAN port config port lan 0/2

```
VLAN Port configuration table
------------------------------
 Port Lan0/2
 Port VLAN ID                          : 1
 Port Acceptable Frame Type            : Admit Only VLAN
Tagged
 Port Ingress Filtering                : Disabled
 Port Mode                             : Hybrid
 Port Gvrp Status                      : Enabled
 Port Gmrp Status                      : Enabled
 Port Gvrp Failed Registrations        : 0
 Gvrp  last  pdu  origin                              :
00:00:00:00:00:00
 Port Restricted VLAN Registration     : Disabled
 Port Restricted Group Registration    : Disabled
 Mac Based Support                     : Disabled
 Port-and-Protocol Based Support       : Enabled
 Default Priority                      : 0
--------------------------------------------------
```

When set to “tagged”, the device will discard untagged and priority tagged frames received on the port and will process only the VLAN tagged frames.

Chapter 6

NAT

6.1 Topology

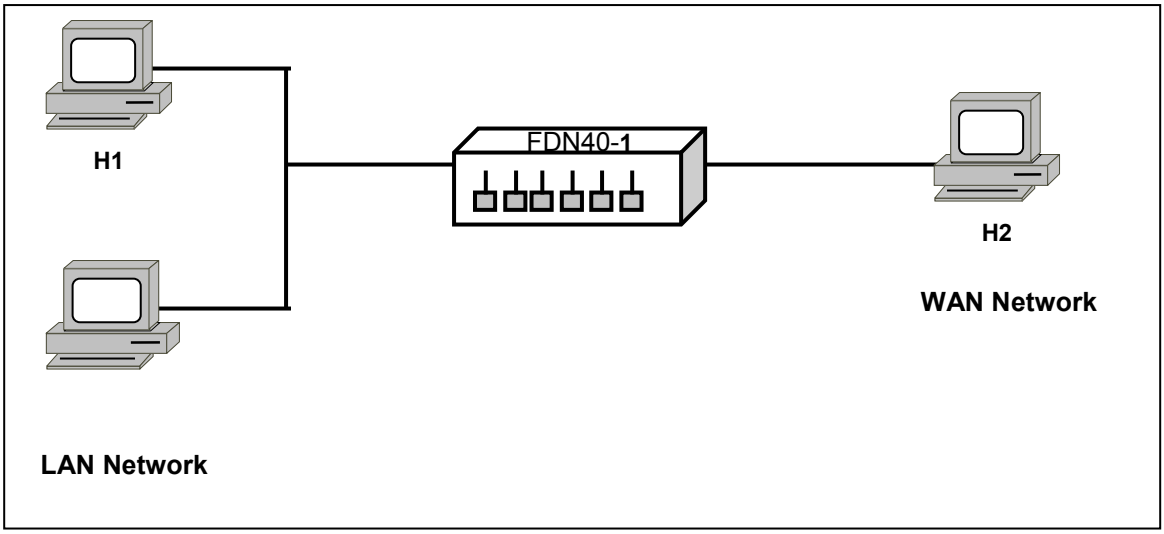


Figure 6-1 - NAT Topology

Interface Index/Name	Interface IPv4 Address
lan0/1	10.0.0.1
wan0/1	80.0.0.1
H1	10.0.0.10
H2	80.0.0.10

6.2 Configuration Guidelines

- NAT and NAPT is enabled or disabled on an interface.

6.3 Default Configurations

Parameter	Default Configuration
NAT	Enabled
NAPT	Enabled

6.4 NAT Configurations

6.4.1 Enabling and Disabling NAT on an Interface

This section describes the steps involved in enabling and disabling the NAT module on an interface. By default, nat module is enabled.

6.4.1.1 CLI Configuration

1. To enable nat on an interface:
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter the Interface Configuration mode.

     UltOs(config)# interface *wan 0/1*
   - Enable nat

     UltOs(config-if)# interface nat *enable*
   - Exit from the Interface Configuration mode.

     UltOs(config-if)# end
2. To view nat status:
   - View the nat interface status

     UltOs# show ip nat interface

```
NAT Configuration on the WAN Interface
-------------------------------------
Interface       NAT         NAPT
---------       ------      -------
 wan0/1          Enabled     Enabled
```

   - View the nat settings

     UltOs# show nat config

```
NAT Configuration
-----------------
```

```
NAT Status                      : Enabled
Maximum Translation Entries : 9000
Start Free Port                 : 6001
Idle Timeout                    : 10 seconds
TCP  Timeout                    : 3600 seconds
UDP  Timeout                    : 100 seconds
ICMP  Timeout                   : 30 seconds
Max Threshold for Dropped Packets : 100
```

To modify NAT setting, nat has to be disabled on all interfaces.

3. To disable nat on an interface:
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter the Interface Configuration mode.

     UltOs(config)# interface *wan 0/1*
   - Disable nat

     UltOs(config-if)# interface nat *disable*
   - Exit from the Interface Configuration Mode.

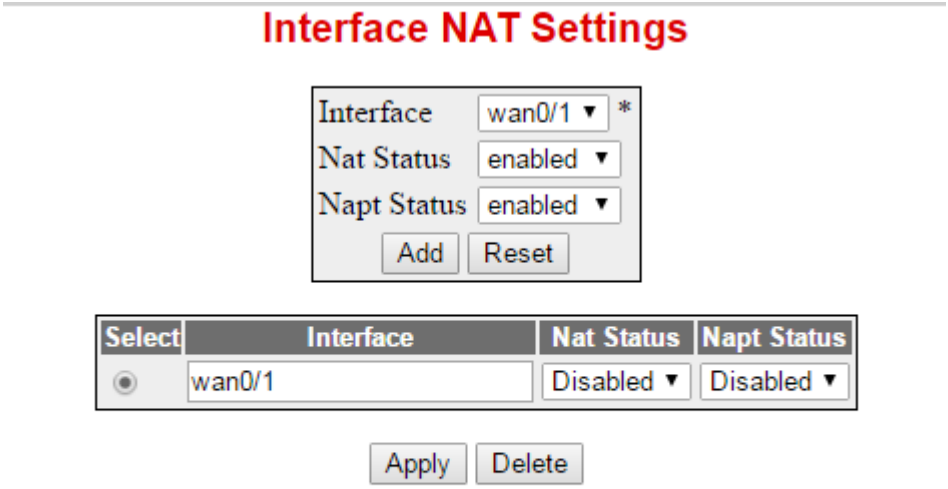
     UltOs(config-if)# end
4. To view the nat status

   UltOs# show ip nat interface

```
NAT Configuration on the WAN Interface
--------------------------------------
Interface       NAT         NAPT
---------       ------      -------
 wan0/1          Disabled     Disabled
```

6.4.1.2 WEB Configuration

NAT can be enabled / disabled on an interface through WEB interface using the **Interface NAT Settings** screen (Navigation - **Layer3 Management > NAT > Interface Settings)**



Screen 6-1: Interface NAT Settings screen - NAT Status

6.4.2 Enabling and Disabling NAPT

The Network Address Port Translation (NAPT) feature helps in conserving the IP address further. Different local addresses can be mapped to the same global address and the source port number present in the UDP and TCP connections will be translated to provide the necessary uniqueness. A new port number is picked out from the free port list maintained by the module.

This section describes the steps involved in enabling and disabling the NAPT in the particular interface. NAPT translates the port number present in the packet to configured value.

6.4.2.1 CLI Configuration

1. To enable napt:
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable Interface Configuration Mode.

     UltOs(config)# interface wan 0/1
   - Enable napt in the interface.

     UltOs(config-if)# ip nat napt enable
   - Exit from the Interface Configuration mode.

     UltOs(config-if)# end
2. To view napt status:
   - View the napt status.

     UltOs# show ip nat interface

     ```
     NAT Configuration on the WAN Interface
     ```

```
-------------------------------------
Interface       NAT         NAPT
---------       ------      -------
wan0/1           Enabled     Enabled
```

3. To disable napt:
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable Interface Configuration Mode.

     UltOs(config)# interface wan 0/1
   - Disable napt in the interface.

     UltOs(config-if)# ip nat napt disable
   - Exit from the Interface Configuration mode.

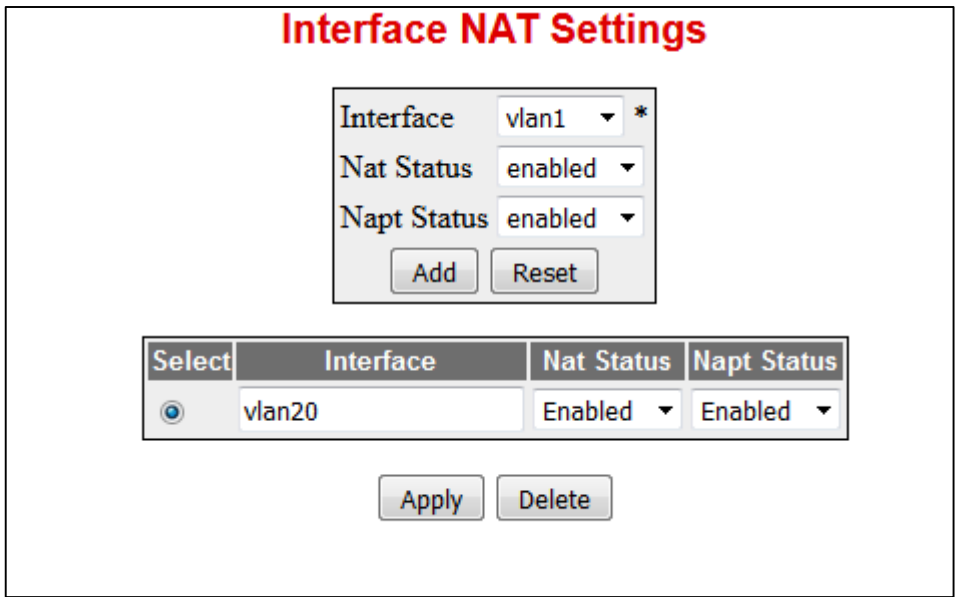
     UltOs(config-if)# end
4. To view napt status:
   - View the napt status.

     UltOs# show ip nat interface

```
NAT Configuration on the WAN Interface
-------------------------------------
Interface       NAT         NAPT
---------       ------      -------
wan0/1           Enabled     Disabled
```

6.4.2.2 WEB Configuration

NAPT can be enabled / disabled through WEB interface using the **Interface NAT Settings** screen (Navigation - **Layer3 Management > NAT > Interface Settings)**



Screen 6-2: Interface NAT Settings screen - NAPT Status

6.4.3 Configuring Static NAT and NAPT

Valid addresses are needed to allow internal users access the Internet NAT allows certain devices on the inside to originate communication with devices on the outside by translating their invalid address to a valid address or pool of addresses.

This section details the static NAT configuration in FDN40 when host H1 tries to communicate with host H2. The steps involved in translating the IP address of host H1 (10.0.0.10) to global IP address 80.0.0.1 for Statis NAT and with port numbers 30 to 40 for Static NAPT is given below. NAT must be enabled in interface wan0/1 to perform network address translation.

6.4.3.1 CLI Configuration

1. To configure static nat:
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter the Interface Configuration mode.

     UltOs(config)# interface wan 0/1
   - Enable nat on the wan interface

     UltOs(config-if)# interface nat enable
   - Configure static nat for H1.

     UltOs(config-if)# static nat *10.0.0.10 80.0.0.1*
   - Configure static napt for H1.

     UltOs(config-if)# static nat *10.0.0.10 30 80.0.0.1 40*

– Exit from the Interface Configuration mode.

UltOs(config)# end

2. To view nat interface status:

– View the nat settings in interfaces.

UltOs# show ip nat interface

```
NAT Configuration on the WAN Interface
--------------------------------------
Interface       NAT         NAPT
---------       ------      -------
Wan 0/1           Enabled     Enabled
```

3. To view static nat configuration:

– View the nat settings in interfaces.

UltOs# show ip nat static

```
Static Address Mapping
----------------------
Interface   Local IP        Translated Local IP
---------   ---------       -------------------
wan 0/1       10.0.0.10       80.0.0.1
```

4. To view static nat configuration:

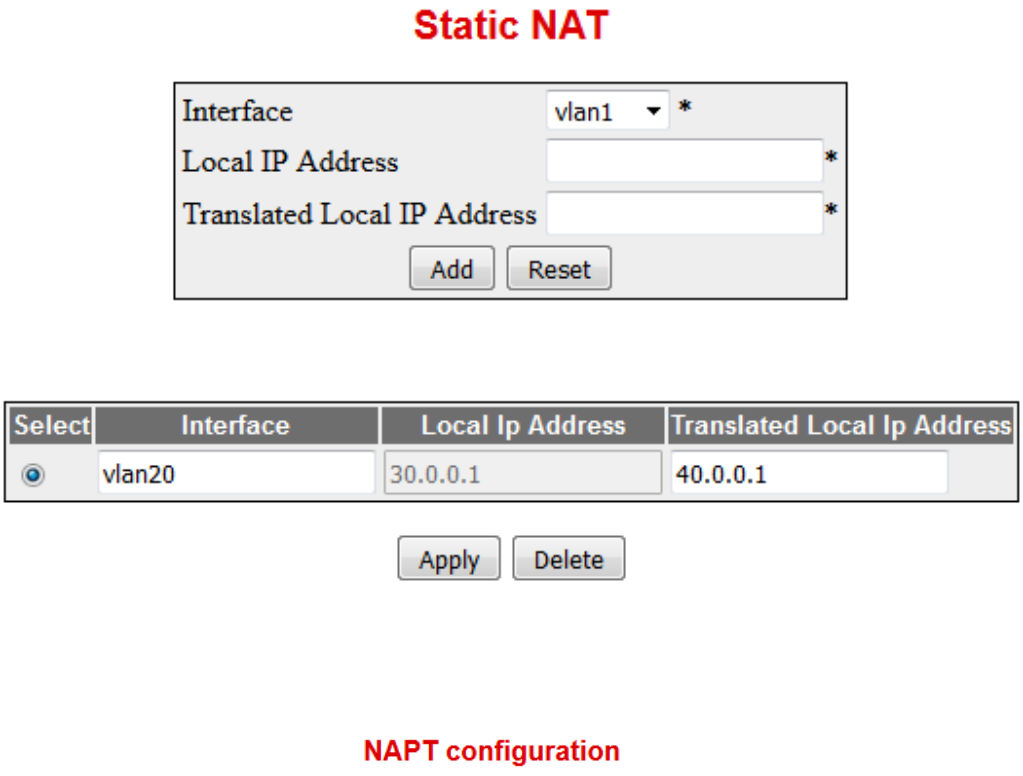
– View the nat settings in interfaces.

UltOs# show ip nat static napt

```
Static NAPT entries
-------------------------------
Interface    :  wan0/1
Local IP     :  10.0.0.10          Local Port  :  30
Protocol     :  ANY
Global IP    :  80.0.0.1           Global Port :  40
App Type     :  OTHER
Description :
Status       :  Enabled
-------------------------------------------------
---
```

6.4.3.2 WEB Configuration

Static NAT can be configured through WEB interface using the **Static NAT** screen (Navigation - **Layer3 Management > NAT > Static NAT)**



Screen 6-3: Static NAT and NAPT

6.4.4 Configuring Dynamic NAT

This section details the dynamic NAT configuration when host H1 communicates with host H2. Global address pool is configured in the interface which allows packets from H1 to retrieve IP address from the configured ip pool while translation.

6.4.4.1 CLI Configuration

1. To configure dynamic nat:
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter the Interface Configuration mode.

     UltOs(config)# interface wan 0/1
   - Enable nat on the wan interface

     UltOs(config-if)# interface nat enable
   - Add global address pool.

     UltOs(config-if)# ip nat pool *80.0.0.5 255.255.255.0*
   - Exit from the Interface Configuration mode.

     UltOs(config)# end
2. To view nat interface status:
   - View the nat settings in interfaces.

     UltOs# show ip nat interface

```
NAT Configuration on the WAN Interface
-------------------------------------
Interface       NAT         NAPT
---------       ------      -------
Wan 0/1           Enabled     Enabled
```

3. To view dynamic NAT configuration:
   - View the NAT settings for interfaces.

     UltOs# show ip nat translations

```
Translated Addresses
--------------------
Interface Local    Translated LocalTranslated
Destination     Dest
          IP       LocalIP    Port   Port     IP
Port
--------  -------- ---------  ------ --------- ----
--------  -
Wan 0/1     10.0.0.10 80.0.0.5   9806   3000
203.199.255.1  2048
```

   - View the dynamic NAT pool settings

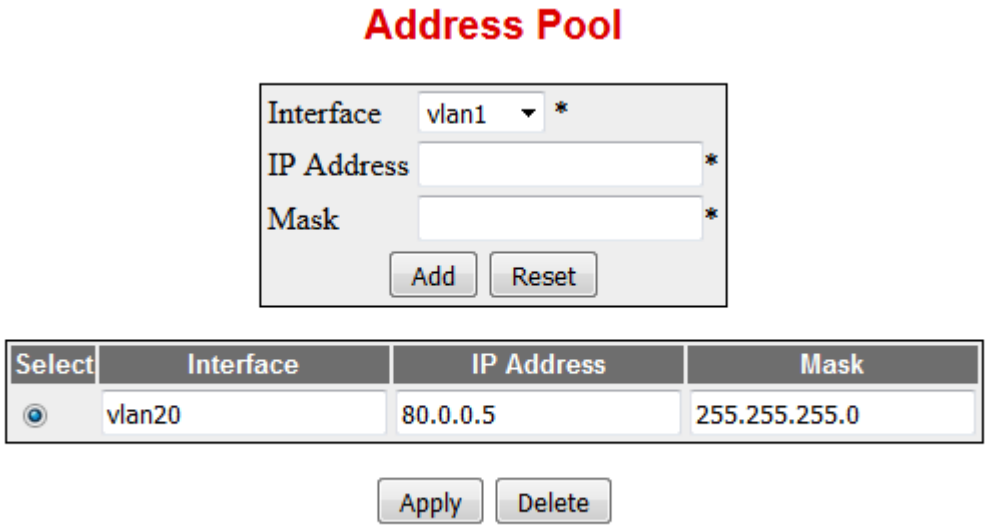
     UltOs# show ip nat global

```
Global Addresses Configured
---------------------------
Interface  Translated Local IP  Translated IP
Address Range
```

```
---------    ------------------- -------------------
----
Wan 0/1        80.0.0.5          255.255.255.0
```

6.4.4.2 WEB Configuration

Dynamic NAT can be configured through WEB interface using the **Address Pool** screen (Navigation - **Layer3 Management > NAT > Dynamic NAT)**



Screen 6-4: Address Pool screen

6.4.5 Configuring Virtual Server

Virtual Server is required to allow external world to avail services in corporate world. This section describes the steps to configure telnet virtual server VS in the LAN network so that the telnet request for H1 given by H2 is received and handled by VS so that the IP address of host H1 remains hidden to outside world.

6.4.5.1 CLI Configuration

1. To create a telnet virtual server:
   - Enter the global configuration mode.

     UltOs# configure terminal
   - Enter Interface Configuration mode

     UltOs(config)# interface wan 0/1
   - Create a virtual server for telnet.

     UltOs(config-if)# virtual server *10.0.0.2 TELNET-server*
   - Exit from the Interface Configuration mode.

     UltOs(config-if)# end
2. To view the configured virtual servers

UltOs# show virtual servers

```
Virtual Servers Configuration
-----------------------------
Interface    :  Wan0/1
Local IP     :  10.0.0.2          Local Port  :  23
Global IP    :  20.10.10.10       Global Port :  23
App Type     :  TELNET
Description  :  Server
Status       :  Enabled
-----------------------------------------------------
```

3. To delete the configured virtual server:
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enter Interface Configuration mode

     UltOs(config)# interface wan 0/1
   - Create a virtual server for telnet.

     UltOs(config-if)# no virtual server *10.0.0.2 23*
   - Exit from the Interface Configuration mode.

     UltOs(config-if)# end

6.4.5.2 WEB Configuration

NAT Virtual Server can be configured through WEB interface using the **Virtual Server Configuration** screen (Navigation - **Layer3 Management > NAT > NAT Virtual Server)**

Screen 6-5: Virtual Server Configuration

Chapter 7

IPSec

7.1 Protocol Description

IPSec provides security services at the IP layer. The security services include access control, connectionless integrity, data origin authentication, rejection of replayed packets, confidentiality and limited traffic flow confidentiality. Since these services are provided at the IP layer, any higher layer protocol above IP (for example, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and the like) can make use of the offered security services.

The protection offered is based on the requirements defined by a SPD (Security Policy Database). The packets are selected on the IP layer header information that is matched against entries in the selectors database. Each incoming and outgoing packet is secured, discarded or bypassed based on the policy identified by the selectors. IPSec performs a SAD (Security Association Database) lookup for both inbound and outbound datagram.

A SAD contains parameters that identify the SA to be used for a particular destination. SA identifies the statement of agreement between two peers. SA defines the mode of operation (Tunnel), security protocol and its associated transforms for a particular peer. The type of the traffic to be protected or filtered is identified by the selectors, which have protocol and interface specific information. The decision to apply or bypass security is based on the configured policy for a particular set of traffic.

IPSec provides the above mentioned security services with the help of the following infrastructure protocol.

The ESP: Provides confidentiality, integrity, data origin authentication and anti-replay service.

Security services are applied to traffic through ESP. Traffic is secured between two hosts or between a host and a security gateway or between two security gateways using two modes namely Tunnel mode or Transport mode.

The Tunnel mode is used to protect traffic between a SG and a host or between two security gateways. The Transport mode is used to protect traffic between a pair of hosts or security gateways.

7.2 Topology

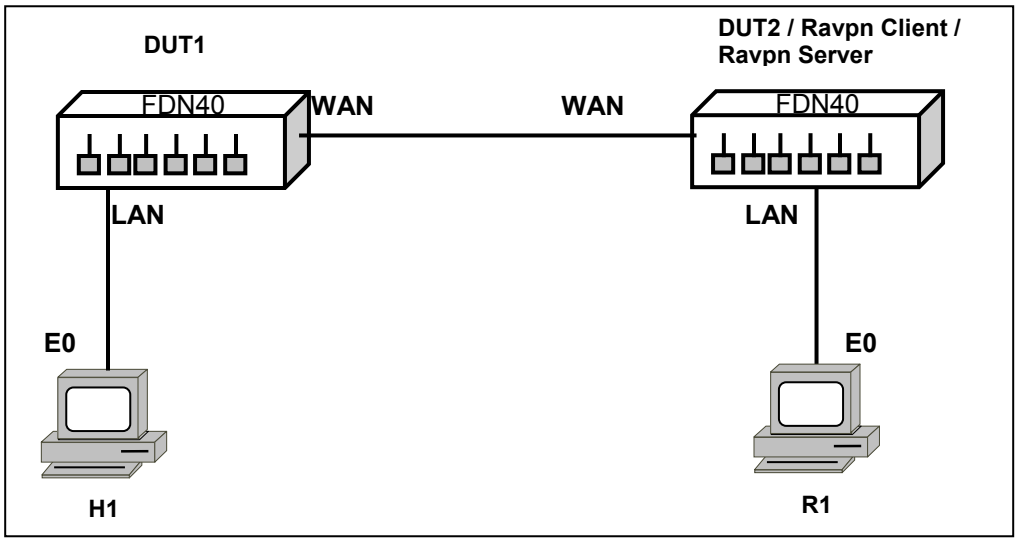


Figure 7-1: IPSec Topology

Node	Interface Index/Name	Interface IP Address
DUT1	WAN	35.0.0.1
DUT2	WAN	35.0.0.2
DUT1	LAN	192.168.1.1
DUT2	LAN	192.168.2.1
H1	E0	192.168.1.10
R1	E0	192.168.2.10

7.3 IPSec Configurations

7.3.1 Enabling VPN Module

The VPN (Virtual Private Network) module is enabled for encryption and decryption of the traffic flows. This section describes the steps involved in enabling the VPN module globally and configuring a VPN policy. This section also describes the verifying of the configuration using corresponding show command.

7.3.1.1 CLI Configuration

To enable VPN globally

1. Enter the Global Configuration mode.

   UltOs# configure terminal

2. Enable the VPN module.

UltOs(config)# set vpn enable

3. Exit from the Global Configuration mode.

UltOs(config)# end

To view the VPN global status

4. View the global VPN settings.

UltOs# show vpn config

```
VPN Global Configuration
------------------------
IPSecurity Status            : Enabled
Maximum Number of Tunnels    : 100
Number of Tunnels configured : 1
Number of Tunnels Established: 1
```

7.3.1.2 WEB Configuration

VPN can be enabled / disabled using the **VPN Policy** screen (Navigation - **Security Management > VPN > VPN Settings > VPN Policy)**

Screen 7-1: VPN Policy - VPN Module Status

7.3.2 Configuring VPN IPSec Policy

7.3.2.1 Creating VPN Policy

Crypto map is created to define a VPN policy that is negotiated for SA creation. Crypto map interacts with and applies various configuration components, security protocols and algorithms to support IPSec security services. This section describes the steps involved in creating a VPN policy.

To create a crypto policy

1. Enter the Global Configuration mode.

UltOs# configure terminal

2. Create a new VPN policy with default configuration

UltOs(config)# crypto map crypto_map_name

3. Exit from the Crypto Map Configuration mode.

UltOs(config-crypto-map)# end

To view the VPN policy parameters

4. View the parameters of the VPN policy.

UltOs# show crypto map

```
                                VPN Policy Parameters
                               -----------------------
    Policy Name                       : crypto_map_name
    Policy Status                     : Inactive
    Policy Type                       : IKE Pre-shared
    Ike Version                       : v1
    Local & Remote Protected N/W's    : None <-- --> None
    Security Mode                     : Tunnel
    Local & Remote Tunnel Term Addr   : None <== ==> None
    Interface Name                    : Not Configured
    Policy Protocol                   : any
    Policy Action                     : Apply
    Anti Replay                       : Disable
    IKE suite Info [PHASE I] :
             Encryption  Algo         : 3DES
             Hash Algorithm           : HMAC SHA1
             Diffie-Hellman Group     : DH Group 2
             IKE Exchange Mode        : Main
             Life Time                : 2400 Secs
    Identity Information :
             Local Identity Type      : Default
             Local Identity value     :
             Peer Identity Type       : Default
             Peer Identity value      :
    IPSEC suite Info [Phase II] :
             Protocol                 : ESP
             Encryption  Algo         : Not Confgiured
             Perfect Forward Secrecy  : Not Confgiured
             Life Time                : 800 Secs
   Crypto Session Status             : Inactive
    Crypto Session Encr Pkts          : 0
    Crypto Session Decr Pkts          : 0
   No.of ACTIVE VPN policies      = 0
   No.of VPN policies configured  = 1
```

7.3.2.2 Configuring VPN Policy Type

The VPN policy type defines the policy to be imposed for the authentication of the users. The different policy types available are IPSec manual,

preshared key, extended authentication, certificate and RA VPN preshared key. This section describes the steps involved in configuring VPN policy type.

To configure VPN policy type

1. Enter the Global Configuration mode.

   UltOs# configure terminal

2. Enter the Crypto Map Configuration mode for an existing policy.

   UltOs(config)# crypto map crypto_map_name

3. Set the key mode as manual mode.

   UltOs(config-crypto-map)# crypto key mode ipsec-manual

4. Exit from the Crypto Map Configuration mode.

   UltOs(config-crypto-map)# end

To view the VPN policy parameters

5. View the parameters of the VPN policy.

   UltOs# show crypto map

```
                              VPN Policy Parameters
                             -------------------------

 Policy Name                          : crypto_map_name
 Policy Status                        : Inactive
 Policy Type                          : IPSec Manual
 Ike Version                          : v1
 Local & Remote Protected N/W's       : None <-- --> None
 Security Mode                        : Tunnel
 Local & Remote Tunnel Term Addr      : None <== ==> None
 Interface Name                       : Not Configured
 Policy Protocol                      : any
 Policy Action                        : Apply
 In/Out bound SPI                     : 0 / 0
 Security Protocol                    : ESP
 Encryption  Algo                     : Not Configured
 Anti Replay                          : Disable
Crypto Session Status                : Inactive
 Crypto Session Encr Pkts             : 0
 Crypto Session Decr Pkts             : 0
No.of ACTIVE VPN policies      = 0
No.of VPN policies configured  = 1
```

7.3.2.3 Configuring IPSec mode

The mode of the IPSec is configured based on the set up for securing the traffic. The mode can be either Tunnel or Transport.

The Tunnel mode is used to protect traffic between a SG and a host or between two security gateways. The Transport mode is used to protect traffic between a pair of hosts or security gateways.

Only the payload of the IP packet is encrypted and/or authenticated, when in transport mode. The entire IP packet is encrypted and/or authenticated, when in tunnel mode.

This section describes the steps involved in configuring the IPSec mode.

To configure the VPN policy mode

1. Enter the Global Configuration mode.

   UltOs# configure terminal
2. Enter the Crypto Map Configuration mode for an existing policy.

   UltOs(config)# crypto map crypto_map_name
3. Set the IPSec mode.

   UltOs(config-crypto-map)# crypto ipsec mode tunnel
4. Exit from the Crypto Map Configuration mode.

   UltOs(config-crypto-map)# end

To view the VPN policy parameters

5. View the parameters of the VPN policy.

   UltOs# sh crypto map

```
                          VPN Policy Parameters
                         -------------------------

 Policy Name                        : crypto_map_name
 Policy Status                      : Inactive
 Policy Type                        : IPSec Manual
 Ike Version                        : v1
 Local & Remote Protected N/W's     : None <-- --> None
 Security Mode                      : Tunnel
 Local & Remote Tunnel Term Addr    : None <== ==> None
 Interface Name                     : Not Configured
 Policy Protocol                    : any
 Policy Action                      : Apply
 In/Out bound SPI                   : 0 / 0
 Security Protocol                  : ESP
 Encryption  Algo                   : Not Configured
 Anti Replay                        : Disable
Crypto Session Status              : Inactive
 Crypto Session Encr Pkts           : 0
 Crypto Session Decr Pkts           : 0
No.of ACTIVE VPN policies      = 0
```

```
No.of VPN policies configured  = 1
```

7.3.2.4 Configuring Peer Identity

Peer identity refers to the destination address set in the packet during authentication and encryption of outbound datagram. This peer identity is used for IPSec SA negotiations. This section describes the steps involved in configuring the peer identity.

To configure the peer identity

1. Enter the Global Configuration mode.

   UltOs# configure terminal
2. Enter the Crypto Map Configuration mode for an existing policy.

   UltOs(config)# crypto map crypto_map_name
3. Set the peer identity.

   UltOs(config-crypto-map)# set peer *35.0.0.1*
4. Exit from the Crypto Map Configuration mode.

   UltOs(config-crypto-map)# end

To view the VPN policy parameters

5. View the parameters of the VPN policy.

   UltOs# show crypto map

```
                              VPN Policy Parameters
                             -------------------------

 Policy Name                          : crypto_map_name
 Policy Status                        : Inactive
 Policy Type                          : IPSec Manual
 Ike Version                          : v1
 Local & Remote Protected N/W's       : None <-- --> None
 Security Mode                        : Tunnel
 Local & Remote Tunnel Term Addr      : 0.0.0.0 <== ==>
35.0.0.1
 Interface Name                       : Not Configured
 Policy Protocol                      : any
 Policy Action                        : Apply
 In/Out bound SPI                     : 0 / 0
 Security Protocol                    : ESP
 Encryption  Algo                     : Not Configured
 Anti Replay                          : Disable
Crypto Session Status                : Inactive
 Crypto Session Encr Pkts             : 0
 Crypto Session Decr Pkts             : 0
No.of ACTIVE VPN policies      = 0
```

```
No.of VPN policies configured  = 1
```

7.3.2.5 Configuring IPSec Session Keys

The IPSec session keys are configured for a VPN policy to set the security protocol, the authentication and encryption algorithms to be applied, and the inbound and outbound security parameter index that is used to uniquely identify a SA. This section describes the steps involved in configuring the IPSec session keys.

To configure the IPSec session keys

1. Enter the Global Configuration mode.

   UltOs# configure terminal

2. Enter the Crypto Map Configuration mode for an existing policy.

   UltOs(config)# crypto map crypto_map_name

3. Configure the IPSec session key.

   UltOs(config-crypto-map)# set session-key authenticator esp hmac-sha1 *abcdef78123456781234567812345678* **esp des cipher** *abcdef7812345678* **outbound** *257* **inbound** *256*

4. Exit from the Crypto Map Configuration mode.

   UltOs(config-crypto-map)# end

To view the VPN policy parameters

5. View the parameters of the VPN policy.

   UltOs# sh crypto map

```
                          VPN Policy Parameters
                         -------------------------

 Policy Name                        : crypto_map_name
 Policy Status                      : Inactive
 Policy Type                        : IPSec Manual
 Ike Version                        : v1
 Local & Remote Protected N/W's     : None <-- --> None
 Security Mode                      : Tunnel
 Local & Remote Tunnel Term Addr    : 0.0.0.0 <== ==>
35.0.0.1
 Interface Name                     : Not Configured
 Policy Protocol                    : any
 Policy Action                      : Apply
 In/Out bound SPI                   : 256 / 257
 Security Protocol                  : ESP
 Authentication Algorithm           : HMAC-SHA1
 Encryption  Algo                   : DES
 Anti Replay                        : Disable
Crypto Session Status             : Inactive
```

```
 Crypto Session Encr Pkts          : 0
 Crypto Session Decr Pkts          : 0


No.of ACTIVE VPN policies      = 0
No.of VPN policies configured  = 1
```

7.3.2.6 Configuring Access List

The access list is configured to specify the traffic type, action to be taken, and source and destination IP address to which the policy is applied. This section describes the steps involved in configuring the access list. Multiple access list can be configured with different indexes.

To configure the access list

1. Enter the Global Configuration mode.

   UltOs# configure terminal

2. Enter the Crypto Map Configuration mode for an existing policy.

   UltOs(config)# crypto map crypto_map_name

3. Configure the access list.

   UltOs(config-crypto-map)# access-list 1 apply any source *192.168.1.0 255.255.255.0* **destination** *192.168.2.0 255.255.255.0*

4. Exit from the Crypto Map Configuration mode

   UltOs(config-crypto-map)# end

To view the VPN policy parameters

5. View the parameters of the VPN policy.

   UltOs# sh crypto map

```
                              VPN Policy Parameters
                             -------------------------

 Policy Name                          : crypto_map_name
 Policy Status                        : Inactive
 Policy Type                          : IPSec Manual
 Ike Version                          : v1
 AclIndex                             : 1
 Local & Remote Protected N/W's       : 192.168.1.0/24 <--
--> 192.168.2.0/24
 Security Mode                        : Tunnel
 Local & Remote Tunnel Term Addr      : 0.0.0.0 <== ==>
35.0.0.1
 Interface Name                       : Not Configured
 Policy Protocol                      : any
 Policy Action                        : Apply
 In/Out bound SPI                     : 256 / 257
```

```
 Security Protocol                : ESP
 Authentication Algorithm         : HMAC-SHA1
 Encryption  Algo                 : DES
 Anti Replay                      : Disable
Crypto Session Status            : Inactive
 Crypto Session Encr Pkts         : 0
 Crypto Session Decr Pkts         : 0

No.of ACTIVE VPN policies      = 0
No.of VPN policies configured  = 1
```

7.3.2.7 Binding of Policy

The configured VPN policy is bound to particular WAN (Wide Area Network) interface for configuring the interface details and local tunnel termination address in the policy and for activating the VPN policy. This section describes the steps involved in binding the policy to the WAN interface

To bind a policy to a particular WAN Interface

1. Enter the Global Configuration mode.

   UltOs# configure terminal
2. Enter the Interface Configuration mode.

   UltOs(config)# interface wan *0/1*
3. Apply the existing policy to the interface.

   UltOs(config-if)# crypto map crypto_map_name
4. Exit from the Interface Configuration mode.

   UltOs(config-if)# end

To view the VPN policy parameters

5. View the parameters of the VPN policy.

   UltOs# show crypto map

```
                              VPN Policy Parameters
                             -------------------------

 Policy Name                      : crypto_map_name
 Policy Status                    : Active
 Policy Type                      : IPSec Manual
 Ike Version                      : v1
 AclIndex                         : 1
 Local & Remote Protected N/W's   : 192.168.1.0/24 <--
--> 192.168.2.0/24
 Security Mode                    : Tunnel
 Local & Remote Tunnel Term Addr  : 35.0.0.2 <== ==>
35.0.0.1
```

```
 Interface Name                    : wan0/1
 Policy Protocol                   : any
 Policy Action                     : Apply
 In/Out bound SPI                  : 256 / 257
 Security Protocol                 : ESP
 Authentication Algorithm          : HMAC-SHA1
 Encryption  Algo                  : DES
 Anti Replay                       : Disable
Crypto Session Status             : Active
 Crypto Session Encr Pkts          : 0
 Crypto Session Decr Pkts          : 0

No.of ACTIVE VPN policies      = 1
No.of VPN policies configured  = 1
```

7.3.2.8 Removing Policy from Interface

The policy assigned to the WAN interface is removed for inactivating the policy. The policy should be inactivated before deleting. Policies assigned to the WAN interface and activated cannot be deleted.

To make the policy inactive

1. Enter the Global Configuration mode.

   UltOs# configure terminal
2. Enter the Interface Configuration mode.

   UltOs(config)#interface wan *0/1*
3. Make the policy inactive.

   UltOs(config-if)# no crypto map crypto_map_name
4. Exit from the Interface Configuration mode.

   UltOs(config-if)# end

To view the VPN policy parameters

5. View the parameters of the VPN policy.

   UltOs# show crypto map crypto_map_name

```
VPN Policy Parameters
                              -------------------------

 Policy Name                       : crypto_map_name
 Policy Status                     : InActive
 Policy Type                       : IKE Pre-shared
 Ike Version                       : v1
 AclIndex                          : 1
 Local & Remote Protected N/W's    : 192.168.1.0/24 <--
--> 192.168.2.0/24
```

```
 Local & Remote Port Range        : 0-65535 <-- --> 0-
65535
 Security Mode                    : Tunnel
 Local & Remote Tunnel Term Addr  : 35.0.0.1 <== ==>
35.0.0.2
```

7.3.2.9 Deleting Policy

This section describes the steps involved in deleting the policy. The policy should be made as inactive (Refer section 7.3.2.8 for the steps) before deleting.

To delete the configured policy

1. Enter the Global Configuration mode.

   UltOs# configure terminal

2. Delete the configured policy.

   UltOs(config)# no crypto map crypto_map_name

3. Exit from the Global Configuration mode.

   UltOs(config)# end

To check the deletion of the policy

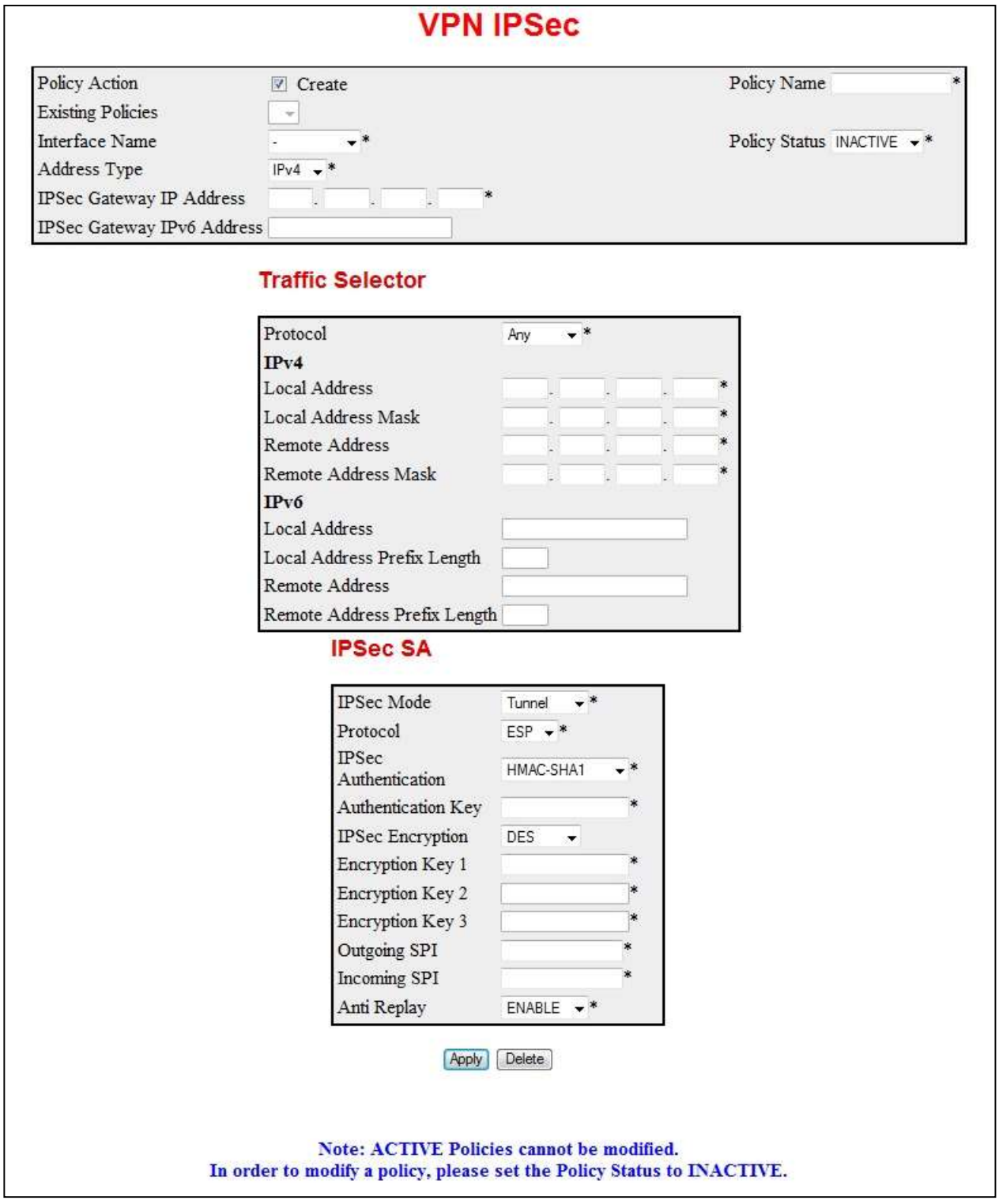
4. View the parameters of the VPN policy.

   UltOs# show crypto map crypto_map_name

No output is displayed for the specified crypto name, as the VPN policy is deleted. This confirms the deletion of the VPN policy.

7.3.2.10 WEB Configuration for IPSec VPN Policy Parameters

VPN IPsec Policy can be configured through the WEB interface using the **VPN IPSec** screen (Navigation - **Security Management > VPN > VPN Settings > IPSec)**



Screen 7-2: VPN IPSec

7.3.3 Sample Configuration

This section describes the sample configuration steps to be performed for configuring the IPSec module in a switch.

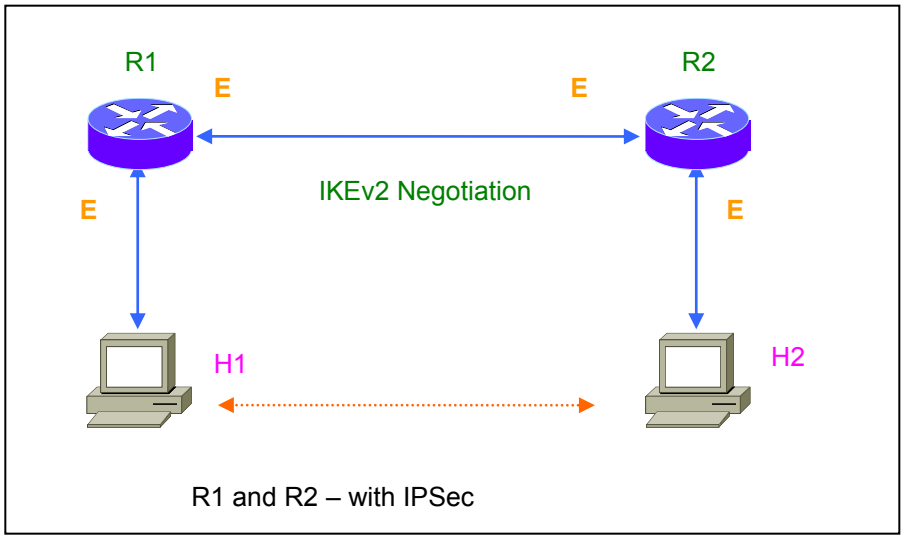


Figure 7-2: Topology Diagram for Sample IPSec Configuration

Node Name	E0 V4 ADDR	E1 V4 ADDR
Host 1(H1)	50.0.0.2	NA
Host 2(H2)	40.0.0.2	NA
FDN40-1(R1)	80.0.0.2	50.0.0.1
FDN40-2(R2)	80.0.0.1	40.0.0.1

IPSec is installed in the Router 1 and the below mentioned commands are executed to configure the IPSec policy.

1. Assigning an IP to wan 0/1.

   UltOs# configure terminal

   UltOs(config)# interface wan *0/1*

   UltOs(config-if)# shutdown

   UltOs(config-if)# ip address *80.0.0.2 255.0.0.0*

   UltOs(config-if)# no shutdown

   UltOs(config-if)# end

   UltOs#

2. Enabling the VPN module.

   UltOs# configure terminal

   UltOs(config)# set vpn enable

   UltOs(config)#exit

   UltOs#

3. Creating an IPSec crypto map policy with name as sa.

   UltOs# configure terminal

UltOs(config)# crypto map sa

UltOs(config-crypto-map)#

4. Configuring IPSec crypto key mode for the policy *sa*.

   UltOs(config-crypto-map)# crypto key mode ipsec-manual

5. Configuring IPSec crypto ipsec mode for the policy *sa.*

   UltOs(config-crypto-map)# crypto ipsec mode tunnel

6. Configuring IPSec crypto peer address for the policy *sa.*

   UltOs(config-crypto-map)# set peer *80.0.0.1*

7. Configuring IPSec crypto session key for the policy sa.

   UltOs(config-crypto-map)# set session-key authenticator esp hmac-md5 *12345678123456781234567812345678* **esp des cipher** *1234567812345678* **outbound** *256* **inbound** *257* **anti-replay**

8. Configuring IPSec crypto access list for the policy sa

   UltOs(config-crypto-map)# access-list 1 apply any source *50.0.0.0 255.255.255.0* **destination** *40.0.0.0 255.255.255.0*

9. Mapping IPSec crypto map policy sa to E1 in the switch

   UltOs(config-crypto-map)# end; configure terminal

   UltOs(config)# interface wan *0/1*

   UltOs(config-if)# crypto map sa

IPSec is installed in the Router 2 and the below mentioned commands are executed to configure the IPSec policy.

10. Assigning an IP to wan 0/1.

    UltOs# configure terminal

    UltOs(config)# interface wan *0/1*

    UltOs(config-if)# shutdown

    UltOs(config-if)# ip address *80.0.0.1 255.0.0.0*

    UltOs(config-if)# no shutdown

    UltOs(config-if)# end

    UltOs#

11. Enabling the VPN module.

    UltOs# configure terminal

    UltOs(config)# set vpn enable

    UltOs(config)#exit

    UltOs#

12. Creating an IPSec crypto map policy with name as sa.

    UltOs# configure terminal

    UltOs(config)# crypto map sa

    UltOs(config-crypto-map)#

13. Configuring IPSec crypto key mode for the policy *sa*.

    UltOs(config-crypto-map)# crypto key mode ipsec-manual

14. Configuring IPSec crypto ipsec mode for the policy *sa.*

    UltOs(config-crypto-map)# crypto ipsec mode tunnel

15. Configuring IPSec crypto peer address for the policy *sa.*

    UltOs(config-crypto-map)# set peer *80.0.0.2*

16. Configuring IPSec crypto session key for the policy sa.

    UltOs(config-crypto-map)# set session-key authenticator esp hmac-md5 *12345678123456781234567812345678* **esp des cipher** *1234567812345678* **outbound** *258* **inbound** *259* **anti-replay**

17. Configuring IPSec crypto access list for the policy sa

    UltOs(config-crypto-map)# access-list 1 apply any source *40.0.0.0 255.255.255.0* **destination** *50.0.0.0 255.255.255.0*

18. Mapping IPSec crypto map policy sa to E1 in the switch

    UltOs(config-crypto-map)# end; configure terminal

    UltOs(config)# interface wan *0/1*

    UltOs(config-if)# crypto map sa

Chapter 8

IKE

8.1 Protocol Description

IKE is used to set up a security association in the IPSec protocol suite. IKE protocol uses UDP (User Datagram Protocol) on port number 500 for negotiating the SAs (Security Associations) with the peers. Therefore, port 500 must be permitted on any IP interface involved in exchanging IKE packets. The negotiated key materials will be given to IPSec stack.

IKE exists in two versions, **IKEv1** and **IKEv2**.

8.1.1 IKEv1

For IKEv1, the peers establish an IKE SA (phase 1 negotiation) using either an MM (Main Mode) exchange or an AM (Aggressive Mode) exchange.

After the IKE SA is established, the IKE peers use the IKE SA for phase 2 negotiation with a QM (Quick Mode) exchange that establishes an IPsec SA pair.

8.1.1.1 Phase 1 – Main/Aggressive

8.1.1.1.1 Main Mode

In an MM exchange, the IKE entities use the following six messages to establish the IKE SA:

- Message 1: Initiator sends IKE SA proposals.
- Message 2: Responder sends accepted IKE SA proposal.
- Message 3: Initiator sends its Diffie-Hellman public value.
- Message 4: Responder sends its Diffie-Hellman public value.
- Message 5: Initiator sends IKE ID and authentication data.

- Message 6: Responder sends IKE ID and authentication data.

8.1.1.1.2 Aggressive Mode

In an AM exchange, the IKE entities use the following three messages to establish the IKE SA:

- Message 1: Initiator sends IKE SA proposals, Diffie-Hellman public value, IKE ID and authentication data.
- Message 2: Responder sends accepted IKE SA proposal, Diffie-Hellman public value, IKE ID, and authentication data.
- Message 3: Initiator sends Diffie-Hellman secured message.

8.1.1.2 Phase 2 - Quick Mode

After an IKEv1 SA is established, the two systems have a secure channel for negotiating IPsec SAs. The IPsec SAs determine IPSec transformation(s) used (ESP (Encapsulation Security Payload) and/or AH (Authentication Header)), the encryption keys for ESP/ESP and other parameters. IPsec SAs are negotiated in pairs: an outbound SA for packets from the local network to the remote network and an inbound SA for packets from the remote network to the local network.

In a QM exchange, the following three messages are required to establish an IPsec SA pair:

- Message 1: Initiator sends IPsec SA proposals, SPI (Security Parameter Index) and traffic IDs.
- Message 2: Responder sends accepted IPsec SA proposal, SPI, and traffic IDs.
- Message 3: Initiator sends hash message to prove liveness.

8.1.2 IKEv2

IKEv2 uses the following four messages to establish an IKE SA and an initial IPsec SA pair.

- Initial request/response of an IKE session (IKE_SA_INIT) negotiates security parameters for the IKE_SA, sends nonces, and sends Diffie-Hellman values.
- Next request/response (IKE_AUTH) transmits identities, proves knowledge of the secrets corresponding to the two identities, and sets up an SA for the first (and often only) AH and/or ESP CHILD_SA.
- Child Exchange (IKE_CHILD) request/response messages are used to refresh the already existing IKE/IPSec SAs or create new IPSec SAs.
- Informational Exchange (IKE_INFO) request/response messages are used to send control messages to the peer.

8.2 IKE Configurations

8.2.1 Importing and Deleting RSA Key

8.2.1.1 Importing a RSA Key

This feature is supported only in CLI mode. The section lists the CLI configuration steps to import a RSA key pair from the specified file, into the database. This configuration is used to import an RSA key pair, if the user already has a RSA key pair and corresponding certificate.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Import the RSA key pair.

  UltOs(config)# vpn import rsa key *rsakey1* **file** *rsakeyfilename*
- Exit the Global configuration mode.

  UltOs(config)#exit
- View the RSA key information.

  UltOs# show vpn rsa keys

```
KeyID rsakey1                RsaKey : ********
```

8.2.1.2 Deleting a RSA Key Pair

This feature is supported only in CLI mode. The section lists the CLI configuration steps to delete an imported or generated RSA key pair.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Delete the imported RSA key pair.

  UltOs(config)# no vpn rsa key index *rsakey1*
- Exit the Global configuration mode.

  UltOs(config)#exit
- View the RSA key information.

  UltOs# show vpn rsa keys

No information is displayed, as the RSA key pair is deleted.

8.2.2 Configuring Certificates

8.2.2.1 Importing a Certificate

This feature is supported only in CLI mode. The section lists the CLI configuration steps to import a certificate from the specified file into the database.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Import the certificate.

UltOs(config)# vpn import cert certid file *RightGty*.**crt encode-type** *PEM* **key** *rsakey1*

- Exit the Global Configuration mode.

  UltOs(config)#exit

- View the certificate information.

  UltOs# show vpn certs index *certid*

```
Cert ID: raskey1
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 2 (0x2)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=IN, ST=AP, L=Hyd, O=AA, OU=Products, CN=SSCA/Email=
Validity
Not Before: Aug 16 23:27:18 2009 GMT
Not After : Aug 16 23:27:18 2010 GMT
Subject: C=CH, O=Linux strongSwan, CN=IssGty
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:d4:aa:32:e8:ab:70:94:5c:8e:cf:38:f8:e9:b1:
b7:1a:b9:4d:72:28:71:b1:33:bb:0b:8a:6b:1e:d9:
30:a9:81:71:e5:aa:47:78:32:47:d7:89:7f:7b:2e:
81:0d:4e:e8:75:65:28:c4:49:b9:9b:96:56:91:f3:
30:c6:ba:d0:f4:bf:db:b2:ba:c7:ab:84:7e:c4:02:
20:c8:69:e3:50:82:3b:d9:c8:fd:a5:75:92:58:a2:
40:1b:af:3f:56:51:d8:d0:9a:95:8f:e0:ba:a7:cd:
2a:fb:9f:69:ce:00:45:34:08:14:c1:1f:ea:44:0d:
8d:c2:a3:2b:3d:30:af:1d:d9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Key Usage:
Digital Signature, Key Encipherment, Key Agreement
X509v3 Subject Key Identifier:
```

```
91:FA:E1:FF:C5:3D:6D:E1:A5:93:B0:F3:1D:E7:08:B1:EA:E8:
D0:30
X509v3 Subject Alternative Name:
IP Address:35.0.0.2
Signature Algorithm: md5WithRSAEncryption
6e:8b:d7:03:3a:8d:fb:e2:fa:21:bd:6e:16:45:16:56:15:3a:
b3:9e:48:96:0f:79:2a:c1:81:a1:22:02:f1:a0:f2:74:d6:2f:
85:52:b3:9c:25:b7:74:db:a6:82:7c:62:19:8c:b7:0d:3e:d7:
80:5e:24:d3:aa:82:26:d8:c9:66:9a:fa:72:10:4f:cc:d2:3d:
83:26:d8:e0:ec:78:87:66:05:dd:60:4e:62:92:f1:c5:1b:85:
ea:65:44:df:52:6b:50:1c:ba:f7:94:95:b0:af:02:8d:fb:56:
91:ea:56:17:18:29:3e:ec:f7:9d:cd:f7:3a:9b:a8:74:44:77:
b3:e9:fa:cb:9a:11:84:04:23:cd:2a:c2:7e:c8:6a:0a:1d:2d:
6a:0d:96:10:6d:ad:cd:3f:36:95:80:6e:65:f2:18:0a:80:43:
52:f9:a0:fa:b2:53:18:00:5e:e8:fd:f2:c0:8c:60:d8:e1:2d:
07:45:b3:0b:c1:5e:12:bd:01:ed:62:e5:af:51:2f:96:bb:29:
39:ae:41:21:d0:16:e5:5b:36:ce:db:c7:5e:6c:86:72:20:63:
bc:2b:b3:d5:b1:a3:f7:86:94:43:9e:21:ca:39:6a:92:8d:4a:
55:cd:44:6a:b2:68:40:f7:99:13:36:9d:5b:52:40:af:48:0f:
86:b8:68:34
```

8.2.2.2 Deleting a Certificate

This feature is supported only in CLI mode. The section lists the CLI configuration steps to delete a certificate from the database.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Delete the imported certificate.

  UltOs(config)# no vpn cert index *certid*
- Exit the Global configuration mode.

  UltOs(config)#exit
- View the certificate information.

  UltOs# show vpn certs index *certid*

No information is displayed, as the imported cerificate is deleted.

8.2.2.3 Importing a CA Certificate

This feature is supported only in CLI mode. The section lists the CLI configuration steps to import a CA (Certificate Authority) certificate from the specified file into the database.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Import the CA certificate.

  UltOs(config)# vpn import ca-cert *cacert* **file** *cacertfilename* **encode-type** *PEM*

- View the CA peer certificate information.

  UltOs# show vpn ca-certs index *cacertid*

```
Cert ID:  cacert
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
91:13:7b:31:9f:20:9c:94
Signature Algorithm: sha1WithRSAEncryption
Issuer:  C=IN,  ST=AP,  L=Hyd,  O=,  OU=Products,
CN=SSCA/Email=help@.com
Validity
Not Before: Mar  5 12:45:08 2009 GMT
Not After : Mar  5 12:45:08 2010 GMT
Subject:  C=IN,  ST=AP,  L=Hyd,  O=,  OU=Products,
CN=SSCA/Email=help@.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:de:cd:6c:38:90:dd:14:6a:ac:9d:20:78:17:85:
37:02:67:cf:47:25:b8:47:4b:28:01:ea:4e:81:ba:
54:5b:c3:0f:c0:5f:2b:bb:b5:bd:a1:60:01:f0:2f:
03:e6:16:5c:a4:c3:7b:ef:bb:b3:70:6b:9f:6e:94:
0a:1a:7c:bc:3b:f0:e1:b3:10:68:15:19:b4:c1:98:
21:36:ba:15:d5:ce:97:d0:19:db:92:dc:03:a6:f4:
8a:03:7e:47:74:d9:59:92:eb:bb:a5:c4:2e:5c:47:
7a:35:18:ed:de:08:25:3f:c7:81:0c:ac:4f:37:72:
23:1f:a3:6a:57:b7:5b:b2:05:42:a6:cb:ec:92:3e:
88:9c:97:76:9d:2a:fb:7d:53:59:6e:4b:ff:f5:ee:
43:2a:76:4d:95:e7:14:61:d7:7e:8e:e2:45:8e:5a:
1e:2a:b8:90:0d:81:8f:e7:0e:05:7d:e2:88:93:e2:
2a:ad:2c:34:6c:a6:1d:b4:32:04:ab:35:e1:ac:89:
df:a1:f0:7a:2f:41:c9:b7:57:df:ac:3f:f6:22:e1:
94:29:c8:44:7e:f2:40:6c:f0:81:59:29:03:c5:e4:
```

```
2d:86:2d:47:2c:14:13:4e:a2:fa:67:a9:b0:5a:7d:
a9:f2:3a:42:d8:0a:30:ba:15:76:99:c2:93:09:af:
eb:f1
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
7F:B4:2F:66:3B:47:67:C4:3E:EE:DC:4A:76:62:B7:D3:7B:EF:
1C:A3
X509v3 Authority Key Identifier:
keyid:7F:B4:2F:66:3B:47:67:C4:3E:EE:DC:4A:76:62:B7:D3:
7B:EF:1C:A3
DirName:/C=IN/ST=AP/L=Hyd/O=
/OU=Products/CN=SSCA/Email=help@.com
serial:91:13:7B:31:9F:20:9C:94
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
d1:16:98:cd:4a:01:99:f1:70:4f:7c:db:99:76:93:e4:42:40:
08:9e:e7:ee:16:41:3e:f5:22:04:b7:97:60:35:cb:09:af:6b:
a0:32:7d:88:9e:5f:86:3b:d9:13:54:f1:c6:4a:2d:78:a2:ab:
03:03:c1:6a:0a:99:6a:be:c5:b8:3b:47:69:07:f4:e6:89:8c:
3f:04:99:d0:8b:80:94:a4:cc:5d:25:c9:53:38:e9:64:14:dd:
7d:8e:01:52:3d:77:44:ac:b6:af:a8:f5:02:b2:f2:3b:bc:18:
6c:8c:67:b3:e1:b0:e9:f9:9c:b1:f1:f5:70:d6:18:4c:0d:8d:
69:6e:fd:ed:89:5d:a0:35:dc:19:13:61:b2:8c:e2:93:ae:c8:
66:40:72:67:c7:c9:2e:70:49:15:09:4e:74:f7:59:7e:52:a2:
1e:bc:c9:41:96:a2:94:9f:70:70:95:4f:e9:80:a0:8f:a6:46:
0f:31:d3:9d:fa:e0:f2:ea:d8:3b:32:79:50:2b:19:1b:8c:e0:
97:76:c7:99:e4:f5:49:ec:16:52:2b:0c:a6:ba:f1:45:d4:80:
c2:63:c3:90:9f:e1:7f:be:1d:73:75:e4:12:d1:6c:c7:59:1b:
92:25:d3:cd:10:95:b7:c0:09:e2:48:f2:14:22:91:5d:1e:08:
3e:b6:6c:fd
```

8.2.2.4 Deleting a CA Certificate

This feature is supported only in CLI mode. The section lists the CLI configuration steps to delete a CA certificate from the database.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Delete the CA certificate.

UltOs(config)# no vpn ca-cert index *cacert*

- View the certificate information.

UltOs# show vpn ca-certs index *cacertid*

No information is displayed, as the CA cerificate is deleted.

8.2.2.5 Importing a Peer Certificate

This feature is supported only in CLI mode. The section lists the CLI configuration steps to import a peer's certificate from the specified file into the database.

- Enter the Global configuration mode.

UltOs# configure terminal

- Import the peer certificate.

UltOs(config)# vpn import peer-cert *peercertid1* **file** *peercertfilename* **encode-type** *PEM trusted*

- View the certificate information.

UltOs# show vpn peer-certs index *peercertid1*

```
Trusted peer certificates
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 2 (0x2)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=IN, ST=AP, L=Hyd, O=, OU=Products,
CN=SSCA/Email=help@.com
Validity
Not Before: Aug 16 23:27:18 2009 GMT
Not After : Aug 16 23:27:18 2010 GMT
Subject: C=CH, O=Linux strongSwan, CN=IssGty
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:d4:aa:32:e8:ab:70:94:5c:8e:cf:38:f8:e9:b1:
b7:1a:b9:4d:72:28:71:b1:33:bb:0b:8a:6b:1e:d9:
30:a9:81:71:e5:aa:47:78:32:47:d7:89:7f:7b:2e:
81:0d:4e:e8:75:65:28:c4:49:b9:9b:96:56:91:f3:
30:c6:ba:d0:f4:bf:db:b2:ba:c7:ab:84:7e:c4:02:
20:c8:69:e3:50:82:3b:d9:c8:fd:a5:75:92:58:a2:
40:1b:af:3f:56:51:d8:d0:9a:95:8f:e0:ba:a7:cd:
2a:fb:9f:69:ce:00:45:34:08:14:c1:1f:ea:44:0d:
```

```
8d:c2:a3:2b:3d:30:af:1d:d9
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Key Usage:
Digital Signature, Key Encipherment, Key Agreement
X509v3 Subject Key Identifier:
91:FA:E1:FF:C5:3D:6D:E1:A5:93:B0:F3:1D:E7:08:B1:EA:E8:
D0:30
X509v3 Subject Alternative Name:
IP Address:35.0.0.2
Signature Algorithm: md5WithRSAEncryption
6e:8b:d7:03:3a:8d:fb:e2:fa:21:bd:6e:16:45:16:56:15:3a:
b3:9e:48:96:0f:79:2a:c1:81:a1:22:02:f1:a0:f2:74:d6:2f:
85:52:b3:9c:25:b7:74:db:a6:82:7c:62:19:8c:b7:0d:3e:d7:
80:5e:24:d3:aa:82:26:d8:c9:66:9a:fa:72:10:4f:cc:d2:3d:
83:26:d8:e0:ec:78:87:66:05:dd:60:4e:62:92:f1:c5:1b:85:
ea:65:44:df:52:6b:50:1c:ba:f7:94:95:b0:af:02:8d:fb:56:
91:ea:56:17:18:29:3e:ec:f7:9d:cd:f7:3a:9b:a8:74:44:77:
b3:e9:fa:cb:9a:11:84:04:23:cd:2a:c2:7e:c8:6a:0a:1d:2d:
6a:0d:96:10:6d:ad:cd:3f:36:95:80:6e:65:f2:18:0a:80:43:
52:f9:a0:fa:b2:53:18:00:5e:e8:fd:f2:c0:8c:60:d8:e1:2d:
07:45:b3:0b:c1:5e:12:bd:01:ed:62:e5:af:51:2f:96:bb:29:
39:ae:41:21:d0:16:e5:5b:36:ce:db:c7:5e:6c:86:72:20:63:
bc:2b:b3:d5:b1:a3:f7:86:94:43:9e:21:ca:39:6a:92:8d:4a:
55:cd:44:6a:b2:68:40:f7:99:13:36:9d:5b:52:40:af:48:0f:
86:b8:68:34
```

8.2.2.6 Deleting Peer Certificate

This feature is supported only in CLI mode. The section lists the CLI configuration steps to import a peer's certificate from database.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Delete the peer certificate.

  UltOs(config)# no vpn import peer-cert index *peercertid1*

- View the peer certificate information.

  UltOs# show vpn peer-certs index *peercertid1*

No information is displayed, as the peer certificate is deleted.

8.2.3 Configuring Remote Identity and Authentication Method

This section lists the CLI configuration steps to configure the the peer or remote identity and authentication method.

8.2.3.1 Authentication Method Preshered-Key

This section lists the CLI configuration steps to configure a remote identity with authentication method as preshared-key.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Configure the pre-shared key for the peer.

  UltOs(config)# vpn remote identity *ipv4 35.0.0.2 psk mypresharedkey*
- Exit the Global configuration mode.

  UltOs(config)#exit
- View the configured remote identity.

  UltOs# show vpn remote-ids

```
Remote identity information table:
Identity type    Identity Value
-------------    --------------
IPv4               35.0.0.2
No.of remote-id's displayed: 1
```

8.2.3.2 Authentication Method RSA Certificate

This section lists the CLI configuration steps to configure authentication method as RSA certificate.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Map the certificate to the peer.

  UltOs(config)# vpn remote identity *ipv4 35.0.0.2 cert rsakey1*
- Exit the Global configuration mode.

  UltOs(config)#exit
- View the configured remote identity.

  UltOs# show vpn remote-ids

```
Remote identity information table:
Identity type    Identity Value
-------------    --------------
IPv4               35.0.0.2
No.of remote-id's displayed: 1
```

- View the certificate mapped to the peer.

  UltOs# show vpn map-cert

```
KeyID rsakey1     PeerID type:  (ipv4)        PeerID:
35.0.0.2
```

8.2.3.3 Deleting a Configured Remote Identity

This section lists the CLI configuration steps to delete a configured remote identity.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Delete the configured remote identity.

  UltOs(config)# no vpn remote identity *ipv4 35.0.0.2*

- Exit the Global configuration mode.

  UltOs(config)#exit

- View the configured remote identities.

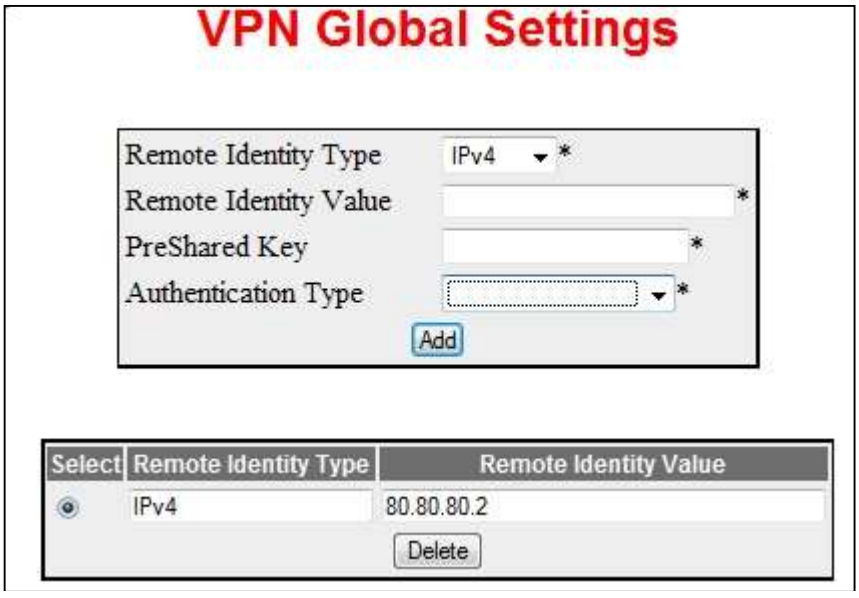
  UltOs# show vpn remote-ids

```
Remote identity information table:
Identity type    Identity Value
-------------    --------------
No.of remote-id's displayed: 0
```

No information is displayed, as the remote identity is deleted.

8.2.3.4 WEB Configuration

VPN remote identity and authentication can be configured through WEB interface using the **VPN Global Settings** screen (Navigation - **Security Management > VPN > VPN Settings)**



Screen 8-1: VPN Global Setings

8.2.4 Creating VPN Policy

This section lists the CLI configuration steps to create a VPN policy which will define the VPN policy to be negotiated for SA creation.

8.2.4.1 CLI Configuration

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Exit the policy configuration mode.

  UltOs(config)#end
- View the policy created. A policy will be created with the default values.

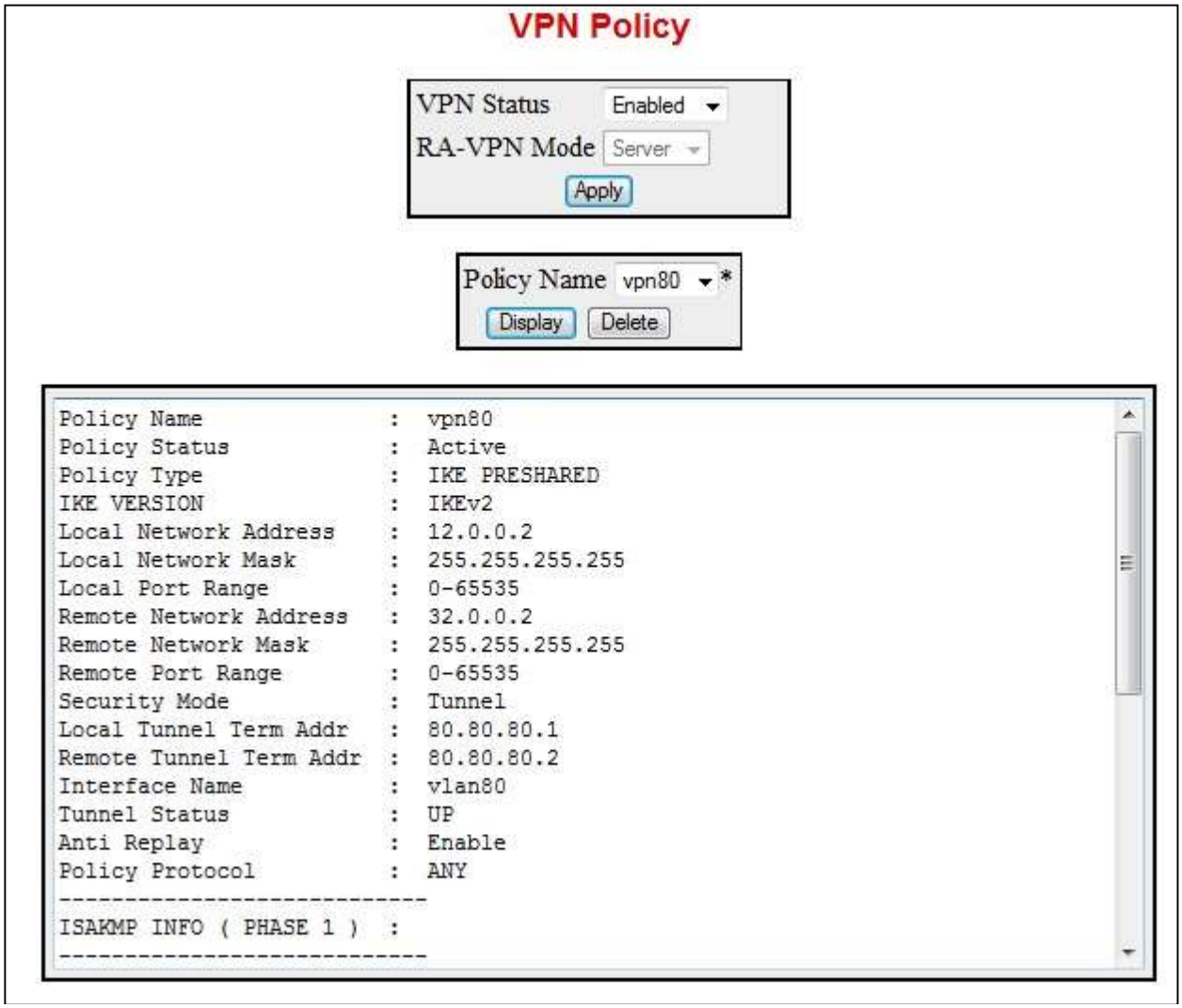
  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                       : sa
Policy Status                     : Inactive
Policy Type                       : IKE Pre-shared
Ike Version                       : v1
Local & Remote Protected N/W's    : None <-- --> None
Security Mode                     : Tunnel
Local & Remote Tunnel Term Addr   : None <== ==> None
Interface Name                    : Not Configured
Policy Protocol                   : any
Policy Action                     : Apply
Anti Replay                       : Disable
IKE suite Info [PHASE I] :
Encryption  Algo         : 3DES
Hash Algorithm           : HMAC SHA1
Diffie-Hellman Group     : DH Group 2
IKE Exchange Mode        : Main
Life Time                : 2400 Secs
Identity Information :
Local Identity Type      : Default
Local Identity value     :
Peer Identity Type       : Default
Peer Identity value      :
IPSEC suite Info [Phase II] :
```

```
Protocol                  : ESP
Encryption  Algo          : Not Confgiured
Perfect Forward Secrecy   : Not Confgiured
Life Time                 : 800 Secs
No.of ACTIVE VPN policies      = 0
No.of VPN policies configured  = 1
```

8.2.4.2 WEB Configuration

- VPN Policies can be created through WEB interface using the **VPN IPSec** screen (Navigation - **Security Management > Firewall > Access List)** or **VPN IKE** screen (Navigation - **Security Management > VPN > VPN Settings > IKE Pre-shared Secret)**
- The Policy details can be viewed through WEB interface using the **VPN Policy** screen (Navigation - **Security Management > VPN > VPN Settings > VPN Policy)**



Screen 8-2: VPN Policy

8.2.5 Configuring VPN IKE Policy Parameters

8.2.5.1 Configuring IKE Version

This section lists the CLI configuration steps to configure the IKE version.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the IKE version (v1 or v2).

  UltOs(config-crypto-map)# set ike version *v1*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured IKE version.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                    : sa
Policy Status                  : Inactive
Policy Type                    : IKE x509 Certificate
Ike Version                    : v1
```

8.2.5.2 Configuring Key Mode

This section lists the CLI configuration steps to configure the certificate mode and the preshared key mode.

8.2.5.2.1 Certificate Mode

This section lists the CLI configuration steps to configure key mode as certificate.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the authentication method.

  UltOs(config-crypto-map)# crypto key mode *cert*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured certificate key mode.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
```

```
Policy Name                    : sa
Policy Status                  : Inactive
Policy Type                    : IKE x509 Certificate
Ike Version                    : v1
```

8.2.5.2.2 Preshared Key Mode

This section lists the CLI configuration steps to configure key mode as preshared key.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the authentication method.

  UltOs(config-crypto-map)# crypto key mode *preshared*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured preshared key mode.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                    : sa
Policy Status                  : Inactive
Policy Type                    : IKE Pre-shared
Ike Version                    : v1
```

8.2.5.3 Configuring Peer IP

This section lists the CLI configuration steps to configure the remote or peer IP.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the peer IP.

  UltOs(config-crypto-map)# set peer *35.0.0.2*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured peer IP.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
```

```
Policy Name                          : sa
Policy Status                        : Inactive
Policy Type                          : IKE Pre-shared
Ike Version                          : v1
Local & Remote Protected N/W's       : None <-- --> None
Security Mode                        : Tunnel
Local & Remote Tunnel Term Addr      : 0.0.0.0 <== ==>
35.0.0.2
```

8.2.5.4 Configuring IPSec Mode

This section lists the CLI configuration steps to configure the IPSec mode.

8.2.5.4.1 Tunnel Mode

This section lists the CLI configuration steps to configure the IPSec mode as tunnel.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the IPSec mode as tunnel.

  UltOs(config-crypto-map)# crypto ipsec mode *tunnel*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured IPSec mode.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                          : sa
Policy Status                        : Inactive
Policy Type                          : IKE Pre-shared
Ike Version                          : v1
Local & Remote Protected N/W's       : None <-- --> None
Security Mode                        : Tunnel
Local & Remote Tunnel Term Addr      : 0.0.0.0 <== ==>
35.0.0.2
```

8.2.5.5 Configuring Remote Identity

This section lists the CLI configuration steps to configure the remote identity of type IPv4.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Configure the remote identity.

  UltOs(config-crypto-map)#)# isakmp peer identity *ipv4 35.0.0.2*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured remote identity.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                        : sa
Policy Status                      : Inactive
Policy Type                        : IKE Pre-shared
Ike Version                        : v1
Local & Remote Protected N/W's     : None <-- --> None
Security Mode                      : Tunnel
Local & Remote Tunnel Term Addr    : 0.0.0.0 <== ==>
35.0.0.2
Interface Name                     : Not Configured
Policy Protocol                    : any
Policy Action                      : Apply
Anti Replay                        : Disable
IKE suite Info [PHASE I] :
Encryption  Algo          : 3DES
Hash Algorithm            : HMAC SHA1
Diffie-Hellman Group      : DH Group 2
IKE Exchange Mode         : Main
Life Time                 : 2400 Secs
Identity Information :
Local Identity Type       : Default
Local Identity value      :
Peer Identity Type        : IPv4
Peer Identity value       : 35.0.0.2
```

8.2.5.6 Configuring Local Identity

This section lists the CLI configuration steps to configure the local identity of type IPv4.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Configure the local identity.

  UltOs(config-crypto-map)#)# isakmp local identity *ipv4 35.0.0.1*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured local identity.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                        : sa
Policy Status                      : Inactive
Policy Type                        : IKE Pre-shared
Ike Version                        : v1
Local & Remote Protected N/W's     : None <-- --> None
Security Mode                      : Tunnel
Local & Remote Tunnel Term Addr    : 0.0.0.0 <== ==>
35.0.0.2
Interface Name                     : Not Configured
Policy Protocol                    : any
Policy Action                      : Apply
Anti Replay                        : Disable
IKE suite Info [PHASE I] :
Encryption  Algo          : 3DES
Hash Algorithm            : HMAC SHA1
Diffie-Hellman Group      : DH Group 2
IKE Exchange Mode         : Main
Life Time                 : 2400 Secs
Identity Information :
Local Identity Type       : IPv4
Local Identity value      : 35.0.0.1
Peer Identity Type        : IPv4
Peer Identity value       : 35.0.0.2
```

8.2.5.7 Configuring Phase 1 Parameters

This section provides the configuration details of phase 1 parameters for IKEv1 and IKEv2.

8.2.5.7.1 For IKEv1

This section lists the CLI configuration steps to configure phase 1 parameters for the main mode.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*

- Set the phase 1 parameters.

  UltOs(config-crypto-map)#)# isakmp policy encryption *des* **hash** *md5* **dh** *group2* **exch main lifetime** *secs 1500*

- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end

- View the configured phase 1 parameters.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters

-------------------------

Policy Name                       : sa

Policy Status                     : Inactive

Policy Type                       : IKE Pre-shared

Ike Version                       : v1

Local & Remote Protected N/W's    : None <-- --> None

Local & Remote Port Range          : 0-65535 <-- --> 0-
65535

Security Mode                     : Tunnel

Local & Remote Tunnel Term Addr   : 0.0.0.0 <== ==>
35.0.0.2

Interface Name                    : Not Configured

Policy Protocol                   : any

Policy Action                     : Apply

Anti Replay                       : Enable

IKE suite Info [PHASE I] :

Encryption  Algo          : DES

Hash Algorithm            : HMAC MD5

Diffie-Hellman Group      : DH Group 2

IKE Exchange Mode         : Main

Life Time                 : 1500 Secs

Identity Information :

Local Identity Type       : IPv4
```

8.2.5.7.2 For IKEv2

This section lists the CLI configuration steps to configure phase 1 parameters for IKEv2.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*

- Set the phase 1 parameters.

  UltOs(config-crypto-map)#)# isakmp policy encryption *des* **hash** *md5* **dh** *group2* **lifetime** *secs 1500*

- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end

- View the configured phase 1 parameters.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters

-------------------------

Policy Name                       : sa

Policy Status                     : Inactive

Policy Type                       : IKE Pre-shared

Ike Version                       : v2

Local & Remote Protected N/W's    : None <-- --> None

Local & Remote Port Range          : 0-65535 <-- --> 0-
65535

Security Mode                     : Tunnel

Local & Remote Tunnel Term Addr   : 0.0.0.0 <== ==>
35.0.0.2

Interface Name                    : Not Configured

Policy Protocol                   : any

Policy Action                     : Apply

Anti Replay                       : Enable

IKE suite Info [PHASE I] :

Encryption  Algo         : DES

Hash Algorithm           : HMAC MD5

Diffie-Hellman Group     : DH Group 2

Life Time                : 1500 Secs

Identity Information :

Local Identity Type      : IPv4
```

8.2.5.8 Configuring Phase 2 Parameters

This section provides the configuration details of phase 2 parameters for ESP protocol.

8.2.5.8.1 ESP Protocol with Integrity

This section lists the CLI configuration steps to configure phase-2 parameters for ESP protocol.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the phase 2 parameters for ESP.

  UltOs(config-crypto-map)#)# crypto map ipsec encryption esp *des* **authentication** *esp sha1* **pfs** *group2* **lifetime** *secs 300*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured phase 2 parameters.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters

-------------------------

Policy Name                       : sa

Policy Status                     : Inactive

Policy Type                       : IKE Pre-shared

Ike Version                       : v2

Local & Remote Protected N/W's    : None <-- --> None

Local & Remote Port Range          : 0-65535 <-- --> 0-
65535

Security Mode                     : Tunnel

Local & Remote Tunnel Term Addr   : 0.0.0.0 <== ==>
35.0.0.2

Interface Name                    : Not Configured

Policy Protocol                   : any

Policy Action                     : Apply

Anti Replay                       : Enable

IKE suite Info [PHASE I] :

Encryption  Algo         : DES

Hash Algorithm           : HMAC MD5

Diffie-Hellman Group     : DH Group 2

Life Time                : 1500 Secs

Identity Information :
```

```
Local Identity Type      : IPv4
Local Identity value     : 35.0.0.1
Peer Identity Type       : IPv4
Peer Identity value      : 35.0.0.2
IPSEC suite Info [Phase II] :
Protocol                 : ESP
Encryption  Algo         : DES
Authenticator            : HMAC-SHA1
Perfect Forward Secrecy  : DH Group 2
Life Time                : 300 Secs
```

8.2.5.9 Configuring Access-list

This section provides the configuration details of access-list for tunnel policy and transport policy.

8.2.5.9.1 Access-list for Tunnel Policy

This section lists the CLI configuration steps to configure access-list for tunnel policy.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the access-list for the tunnel mode.

  UltOs(config-crypto-map)#access-list *apply any* **source** *192.168.1.0 255.255.255.0* **destination** *192.168.2.0 255.255.255.0*
- Exit the policy configuration mode.

  UltOs(config-crypto-map)#end
- View the configured access-list.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                      : sa
Policy Status                    : Inactive
Policy Type                      : IKE Pre-shared
Ike Version                      : v1
Local & Remote Protected N/W's   : 192.168.1.0/24 <--
--> 192.168.2.0/24
Local & Remote Port Range         : 0-65535 <-- --> 0-
65535
```

```
Security Mode                        : Tunnel
```

8.2.5.10 Attaching the Policy to the Interface

This section lists the CLI configuration steps to make the policy active.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Make the policy active and bind to the WAN port.

  UltOs(config)#interface *wan 0/1*

  UltOs(config-if)# crypto map *sa*

- Exit from the interface configuration mode.

  UltOs(config-if)# end

- View the policy active status.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                          : sa
Policy Status                        : Active
Policy Type                          : IKE Pre-shared
Ike Version                          : v1
Local & Remote Protected N/W's    : 192.168.1.0/24 <--
--> 192.168.2.0/24
Local & Remote Port Range         : 0-65535 <-- --> 0-
65535
Security Mode                        : Tunnel
Local & Remote Tunnel Term Addr   : 35.0.0.1 <== ==>
35.0.0.2
Interface Name                       : lan 0/1
```

8.2.5.11 Removing the Policy from the Interface

This section lists the CLI configuration steps to make the policy inactive.

- Enter the Global configuration mode.

  UltOs# configure terminal

- Make the policy inactive.

  UltOs(config)#interface *wan 0/1*

  UltOs(config-if)# no crypto map *sa*

- Exit from the interface configuration mode.

  UltOs(config-if)# end

- View the policy inactive status.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
```

```
-------------------------
Policy Name                          : sa
Policy Status                        : InActive
Policy Type                          : IKE Pre-shared
Ike Version                          : v1
Local & Remote Protected N/W's    : 192.168.1.0/24 <--
--> 192.168.2.0/24
Local & Remote Port Range         : 0-65535 <-- --> 0-
65535
Security Mode                        : Tunnel
Local & Remote Tunnel Term Addr   : 35.0.0.1 <== ==>
35.0.0.2
```

8.2.5.12 Deleting the Policy

This section lists the CLI configuration steps to delete the configured policy.

- Enter the Global configuration mode.

  UltOs# configure terminal
- Delete the configured policy.

  UltOs(config)# no crypto map *sa*
- Exit from the global configuration mode.

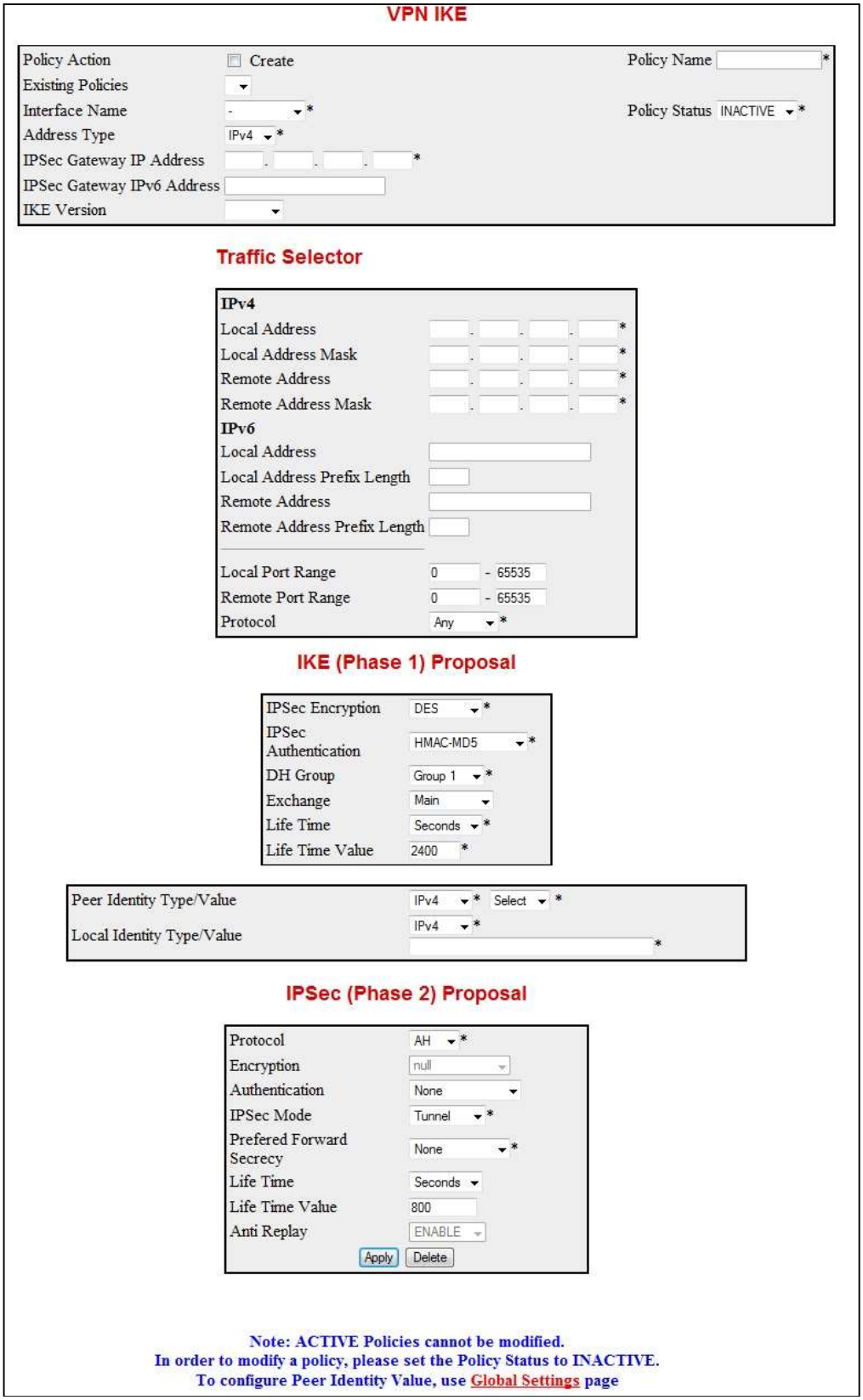
  UltOs(config)# end
- View the configuration to check the policy being deleted.

  UltOs# show crypto map *sa*

No information is displayed, as the configured crypto map is deleted.

8.2.5.13 Web Configuration for VPN IKE Policy

VPN IKE Policy can be configured using the **VPN IKE** screen (Navigation - **Security Management > VPN > VPN Settings > IKE Pre-shared Secret)**



Screen 8-3: VPN IKE

8.2.6 Displaying the VPN Statistics

8.2.6.1 CLI Configuration

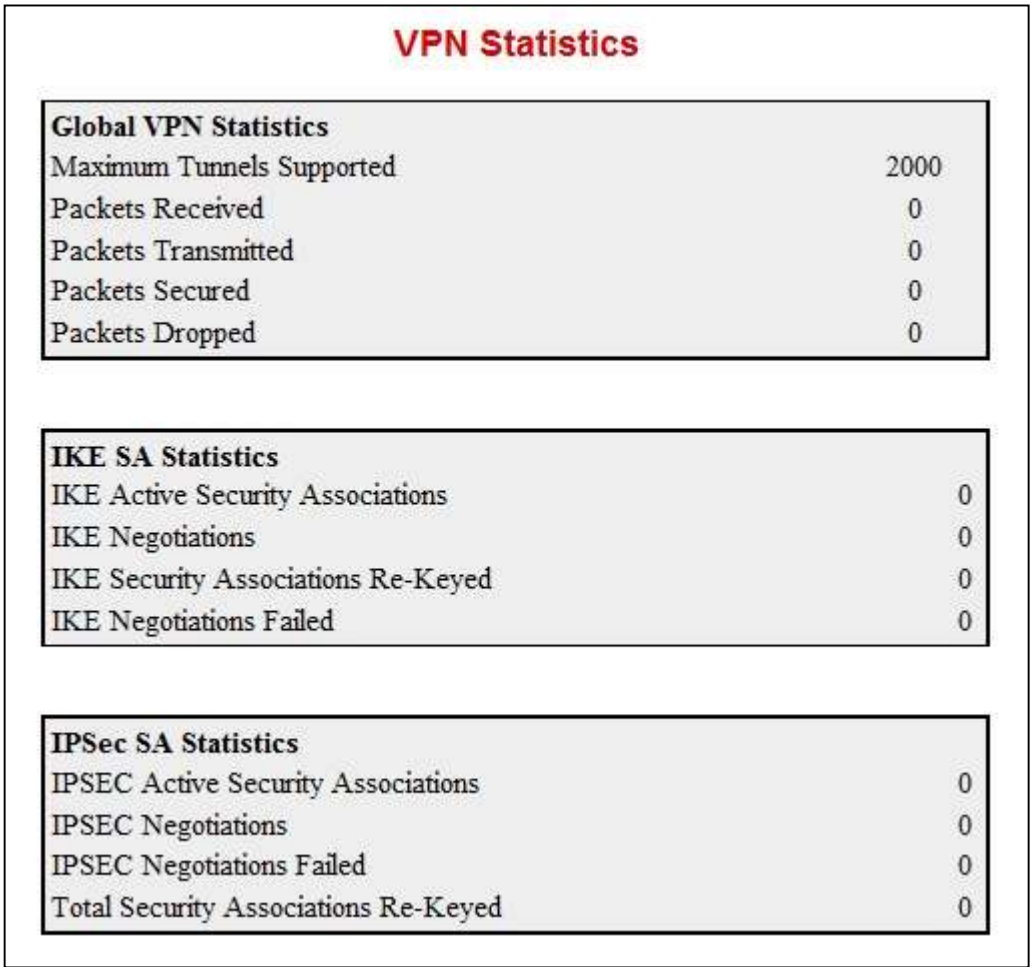
This section lists the CLI command to view the VPN global statistics.

UltOs# show vpn global statistics

```
VPN Global Statistics:
 --------------------------------
Packets In                    : 41
Packets Out                   : 18
Packets Secured               : 0
Packets Dropped               : 7
```

8.2.6.2 WEB Configuration

VPN statistics can be viewed through WEB interface using the **VPN Statistics** screen (Navigation - **Statistics > VPN)**



Screen 8-4: VPN Statistics

8.3 IKE Examples

This chapter provides the sample topology setup and various sample configurations of **IKE**through CLI.

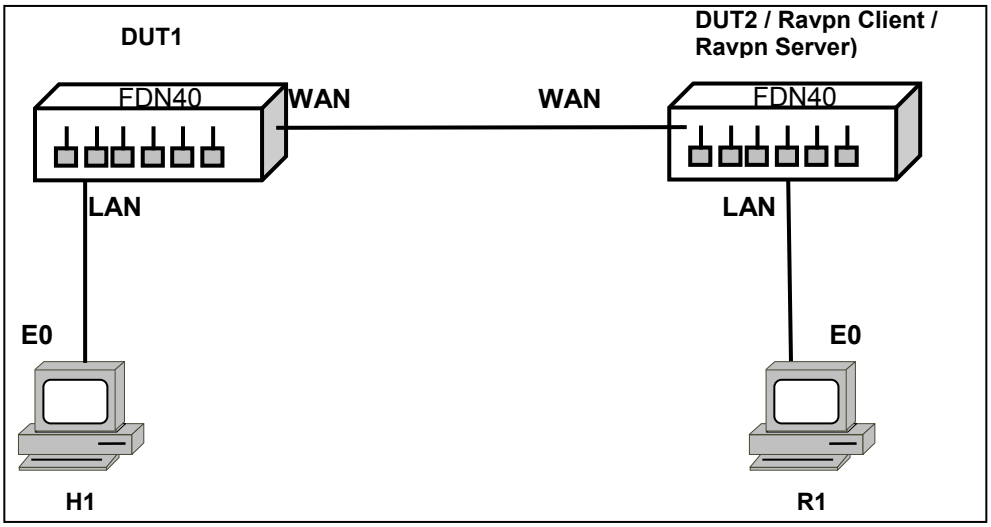


Figure 8-1: IKE Topology

Node	Interface Index/Name	Interface IP Address
DUT1	WAN	35.0.0.1
DUT2	WAN	35.0.0.2
DUT1	LAN	192.168.1.1
DUT2	LAN	192.168.2.1
H1	E0	192.168.1.10
R1	E0	192.168.2.10

8.3.1 General Configuration

To configure a WAN port, execute the following CLI commands:

UltOs#configure terminal

UltOs(config)# interface *wan 0/1*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *35.0.0.1 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# end

8.3.2 Configuring IKEv1 - Tunnel Mode - Preshared key

Tunnel mode is most commonly used between gateways, or at an end-station to a gateway. The gateway acts as a proxy for the hosts behind it.

In IKE Topology , tunnel mode is used to setup an IPSec tunnel between H1 and R1.

This section describes the procedure to configure the IKEv1 site-to-site tunnel mode policy with the authentication method as preshared key.

8.3.2.1 DUT1 Configuration

Execute the following steps in DUT1:

- Enter the Global configuration mode.

  UltOs# configure terminal
- Configure the pre-shared key for the peer.

  UltOs(config)# vpn remote identity *ipv4 35.0.0.2 psk mypresharedkey*
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the IKE version.

  UltOs(config-crypto-map)# set ike version *v1*
- Set the authentication method.

  UltOs(config-crypto-map)# crypto key mode *preshared*
- Set the IPSec mode as tunnel.

  UltOs(config-crypto-map)# crypto ipsec mode *tunnel*
- Set the peer IP (DUT2 WAN IP).

  UltOs(config-crypto-map)# set pee*r 35.0.0.2*
- Set the peer identity.

  UltOs(config-crypto-map)# isakmp peer identity *ipv4 35.0.0.2*
- Set the local identity.

  UltOs(config-crypto-map)# isakmp local identity *ipv4 35.0.0.1*
- Set the phase 1 parameters.

  UltOs(config-crypto-map)# isakmp policy encryption *des* **hash** *md5* **dh** *group2* **exch** *main* **lifetime** *secs 1500*
- Set the phase 2 parameters.

  UltOs(config-crypto-map)# crypto map ipsec encryption esp *des* **authentication** *esp sha1* **pfs** *group2* **lifetime** *secs 300*
- Set the access-list parameters.

  UltOs(config-crypto-map)#access-list *apply any* **source** *192.168.1.0 255.255.255.0* **destination** *192.168.2.0 255.255.255.0*
- Exit from the policy configuration mode.

  UltOs(config-crypto-map)#exit
- Make the policy active and bind to the WAN port.

  UltOs(config)#interface *wan 0/1*

  UltOs(config-if)# crypto map *sa*
- Exit from the interface configuration mode.

  UltOs(config-if)# end
- View the configured VPN policy.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
Policy Name                       : sa
Policy Status                     : Active
Policy Type                       : IKE Pre-shared
Ike Version                       : v1
Local & Remote Protected N/W's    : 192.168.1.0/24 <--
--> 192.168.2.0/24
Local & Remote Port Range         : 0-65535 <-- --> 0-
65535
Security Mode                     : Tunnel
Local & Remote Tunnel Term Addr   : 35.0.0.1 <== ==>
35.0.0.2
Interface Name                    : wan 0/1
Policy Protocol                   : any
Policy Action                     : Apply
Anti Replay                       : Enable
IKE suite Info [PHASE I] :
Encryption  Algo         : DES
Hash Algorithm           : HMAC MD5
Diffie-Hellman Group     : DH Group 2
IKE Exchange Mode        : Main
Life Time                : 1500 Secs
Identity Information :
Local Identity Type      : IPv4
Local Identity value     : 35.0.0.1
Peer Identity Type       : IPv4
Peer Identity value      : 35.0.0.2
IPSEC suite Info [Phase II] :
Protocol                 : ESP
Encryption  Algo         : DES
Authenticator            : HMAC-SHA1
Perfect Forward Secrecy  : DH Group 2
Life Time                : 300 Secs
Crypto Session Status            : Inactive
 Crypto Session Encr Pkts         : 0
 Crypto Session Decr Pkts         : 0
```

8.3.2.2 DUT2 Configuration

Execute the following steps in DUT2:

- Enter the Global configuration mode.

  UltOs# configure terminal
- Configure the pre-shared key for the peer.

  UltOs(config)# vpn remote identity *ipv4 35.0.0.1 psk mypresharedkey*
- Enter the policy configuration mode.

  UltOs(config)# crypto map *sa*
- Set the IKE version.

  UltOs(config-crypto-map)# set ike version *v1*
- Set the authentication method.

  UltOs(config-crypto-map)# crypto key mode *preshared*
- Set the IPSec mode as tunnel.

  UltOs(config-crypto-map)# crypto ipsec mode *tunnel*
- Set the peer IP (DUT1 WAN IP).

  UltOs(config-crypto-map)# set peer *35.0.0.1*
- Set the peer identity.

  UltOs(config-crypto-map)# isakmp peer identity *ipv4 35.0.0.1*
- Set the local identity.

  UltOs(config-crypto-map)# isakmp local identity *ipv4 35.0.0.2*
- Set the phase 1 parameters.

  UltOs(config-crypto-map)# isakmp policy encryption *des* **hash** *md5* **dh** *group2* **exch** *main* **lifetime** *secs 1500*
- Set the phase 2 parameters.

  UltOs(config-crypto-map)# crypto map ipsec encryption esp *des* **authentication** *esp sha1* **pfs** *group2* **lifetime** *secs 300*
- Set the access-list parameters.

  UltOs(config-crypto-map)#access-list *apply any* **source** *192.168.2.0 255.255.255.0* **destination** *192.168.1.0 255.255.255.0*
- Exit from the policy configuration mode.

  UltOs(config-crypto-map)#exit
- Make the policy active and bind to the WAN port.

  UltOs(config)#interface *wan 0/1*

  UltOs(config-if)# crypto map sa
- Exit from the interface configuration mode.

  UltOs(config-if)# end
- View the configured VPN policy.

  UltOs# show crypto map *sa*

```
VPN Policy Parameters
-------------------------
```

```
Policy Name                        : sa
Policy Status                      : Active
Policy Type                        : IKE Pre-shared
Ike Version                        : v1
Local & Remote Protected N/W's     : 192.168.2.0/24 <--
--> 192.168.1.0/24
Local & Remote Port Range          : 0-65535 <-- --> 0-
65535
Security Mode                      : Tunnel
Local & Remote Tunnel Term Addr    : 35.0.0.2 <== ==>
35.0.0.1
Interface Name                     : wan 0/1
Policy Protocol                    : any
Policy Action                      : Apply
Anti Replay                        : Enable
IKE suite Info [PHASE I] :
Encryption  Algo         : DES
Hash Algorithm           : HMAC MD5
Diffie-Hellman Group     : DH Group 2
IKE Exchange Mode        : Main
Life Time                : 1500 Secs
Identity Information :
Local Identity Type      : IPv4
Local Identity value     : 35.0.0.2
Peer Identity Type       : IPv4
Peer Identity value      : 35.0.0.1
IPSEC suite Info [Phase II] :
Protocol                 : ESP
Encryption  Algo         : DES
Authenticator            : HMAC-SHA1
Perfect Forward Secrecy  : DH Group 2
Life Time                : 300 Secs
Crypto Session Status             : Inactive
 Crypto Session Encr Pkts         : 0
 Crypto Session Decr Pkts         : 0
```

Chapter 9

Firewall

9.1 Topology

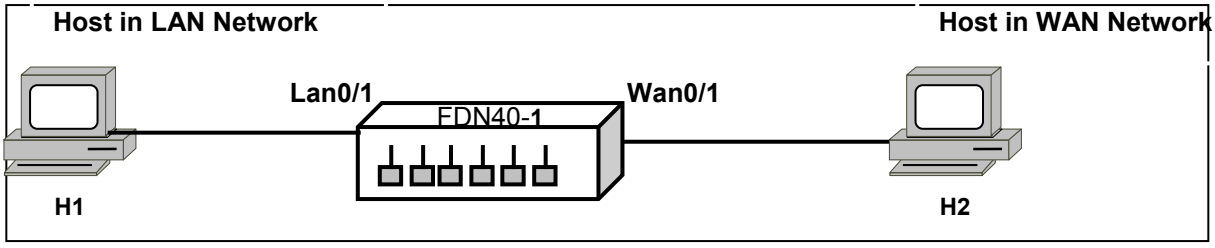


Figure 9-1: Firewall Topology

Table 9-1: IPv4 Addresses of Interfaces and Hosts

Interface Index/Name	Interface IPv4 Address
LAN0/1	10.0.0.1
WAN0/1	80.0.0.1
H1	10.0.0.10
H2	80.0.0.10

9.2 Default Configurations

When **system** comes up, **FIREWALL** is operationally disabled.

Firewall Configurations

9.2.1 Enabling and Disabling Firewall Module

This section describes the steps involved in enabling and disabling the Firewall module globally. By default, firewall module is enabled.

9.2.1.1 CLI Configuration

To enable firewall:

1. Enter the Global Configuration mode.

   UltOs# configure terminal

2. Enable the Firewall module.

   UltOs(config)# firewall

   UltOs(config-firewall)# enable

3. Exit from the Global Configuration mode.

   UltOs(config-firewall)# end

To disable firewall:

4. Enter the Global Configuration mode.

   UltOs# configure terminal

5. Disable the Firewall module.

   UltOs(config)# firewall

   UltOs(config-firewall)# disable

6. Exit from the Global Configuration mode.

   UltOs(config-firewall)# end

To view the firewall status

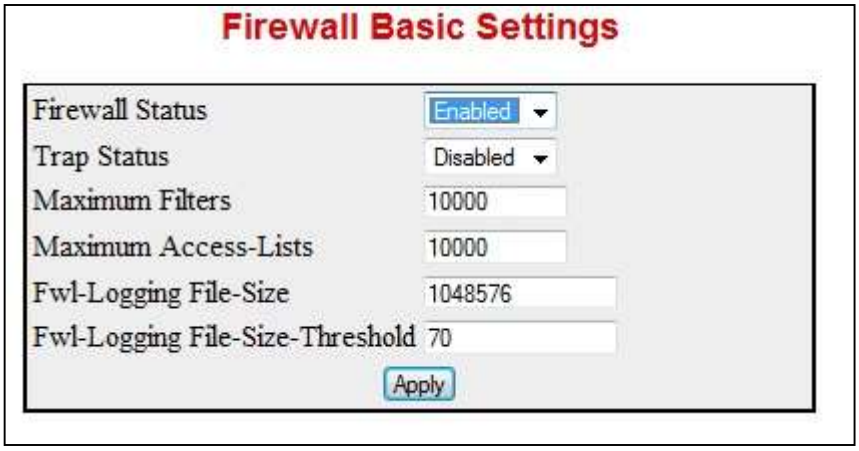
7. View the firewall settings.

   UltOs# show firewall config

```
Firewall Configuration
----------------------


Firewall Status                    : Enabled
Trap Status                        : Disabled
Max Filters                        : 10000
Max Access-Lists                   : 10000
Trap Threshold Configured          : 50
IP Inspect Option                  : src-route
```

9.2.1.2 WEB Configuration

To enable /disable firewall, Configure *Firewall Status* field from the **Firewall Basic Settings** screen (Navigation - **Security Management > Firewall > Basic Settings)**



Screen 9-1: Firewall Basic Settings

9.2.2 Configuring Firewall Filters for IPv4

Traffic from the private network to the Internet is regulated using **Outbound Rules**. These rules determine the services to which the users in the private network have access. Traffic from the Internet is regulated using **Inbound Rules**. These rules determine the access for the outsiders to use the private resources.

Firewall rules are used to permit or deny specific traffic. The type of traffic is defined by a firewall filter, and the decision to permit or deny is defined by a firewall access list. A rule is an access list policy which uses a firewall filter to process any packet.

Firewall, by default, allows outbound traffic from the computers in the private network to the Internet only for the following services:

- FTP (Port 21)
- HTTP (80) and HTTPS (Port 443)
- SSH(22)
- SNMP(161)
- SNMPTRAP(162)
- ISAKMP(500)
- IPSEC NAT TRAVERSAL(4500)

All other outbound traffic is blocked by **Firewall**.

This section describes the steps involved in creation and deletion of firewall filters.

9.2.2.1 CLI Configuration

To create a firewall filter:

1. Go to Global configuration mode.

   UltOs# configure terminal

2. Enter the firewall mode.

   UltOs(config)# firewall

3. Create a new firewall filter to to match the source IP address matches with LAN hostH1, destination IP address matches with H2, any protocol, any source port and destination port.

   UltOs(config-firewall)# filter add *filter1 10.0.0.10/32 80.0.0.10/32* **any**

To view firewall filters

UltOs# show firewall filters

```
                                    Firewall Filters
                                    ----------------

Filter                      Proto  Source
Destination        Src port/  Dest port/ TCP
                                 Address
Address            Icmp type  Icmp code  Flags
------                      -----  -------              -----
--            --------   --------   -----

filter1                     any    10.0.0.10/32
80.0.0.10/32       >1         >1         NA

Def_AH_Filter               51     0.0.0.0/0
192.168.1.1/24     >1         >1         NA

Def_ESP_Filter              50     0.0.0.0/0
192.168.1.1/24     >1         >1         NA

Def_FTP_Filter              tcp    0.0.0.0/0
192.168.1.1/24     >1         =21        any

Def_SSH_Filter              tcp    0.0.0.0/0
192.168.1.1/24     >1         =22        any

Def_HTTP_Filter             tcp    0.0.0.0/0
192.168.1.1/24     >1         =80        any

Def_ICMP_Filter             icmp   0.0.0.0/0
0.0.0.0/0          any        any        NA

Def_SNMP_Filter             udp    0.0.0.0/0
192.168.1.1/24     >1         =161       NA

Def_HTTPS_Filter            tcp    0.0.0.0/0
192.168.1.1/24     >1         =443       any

Def_TELNET_Filter           tcp    0.0.0.0/0
192.168.1.1/24     >1         =6023      any

Def_IKE_UDP_Filter          udp    0.0.0.0/0
192.168.1.1/24     >1         =500       NA

Def_SNTP_UDP_Filter         udp    0.0.0.0/0
0.0.0.0/0          >1         =123       NA

Def_SNMP_Trap_Filter        udp    0.0.0.0/0
192.168.1.1/24     >1         =162       NA

Def_IKE_NAT_UDP_Filter      udp    0.0.0.0/0
192.168.1.1/24     >1         =4500      NA

Def_IKE_UDP_Loc_Filter      udp    0.0.0.0/0
0.0.0.0/0          >1         =500       NA
```

This below section describes the steps involved in deleting the ipv4 firewall filter.

To delete the configured ipv4 firewall filter

4. Enter the Global Configuration mode.

   UltOs# configure terminal

5. Enter into firewall mode

   UltOs(config)# firewall

6. Delete the ipv4 firewall filter

   UltOs(config-firewall)# no filter *filter1*

The below section describes the steps needed to create filters to filter packets from WAN Host to LAN host.

To create a firewall filter:

7. Go to Global configuration mode.

   UltOs# configure terminal

8. Enter the firewall mode.

   UltOs(config)# firewall

9. Create a new firewall filter to to match the source IP address as WAN host IP, destination IP address as LAN host IP, tcp protocol, any source port and destination port.

   UltOs(config-firewall)# filter add *filter2 80.0.0.10/32 10.0.0.10/32* **tcp**

To view firewall filters

UltOs# show firewall filters

```
                                  Firewall Filters
                                  ----------------

Filter                      Proto  Source
Destination        Src port/  Dest port/ TCP

                                 Address
Address            Icmp type  Icmp code  Flags

------                      -----  -------              -----
--            --------   --------   -----

filter1                     any    10.0.0.10/32
80.0.0.10/32       >1         >1         NA

filter2                     tcp    80.0.0.10/32
10.0.0.10/32       >1         >1         any

Def_AH_Filter               51     0.0.0.0/0
192.168.1.1/24     >1         >1         NA

Def_ESP_Filter              50     0.0.0.0/0
192.168.1.1/24     >1         >1         NA

Def_FTP_Filter              tcp    0.0.0.0/0
192.168.1.1/24     >1         =21        any

Def_SSH_Filter              tcp    0.0.0.0/0
192.168.1.1/24     >1         =22        any
```

```
Def_HTTP_Filter          tcp    0.0.0.0/0
192.168.1.1/24     >1          =80         any

Def_ICMP_Filter          icmp   0.0.0.0/0
0.0.0.0/0          any         any         NA

Def_SNMP_Filter          udp    0.0.0.0/0
192.168.1.1/24     >1          =161        NA

Def_HTTPS_Filter         tcp    0.0.0.0/0
192.168.1.1/24     >1          =443        any

Def_TELNET_Filter        tcp    0.0.0.0/0
192.168.1.1/24     >1          =6023       any

Def_IKE_UDP_Filter       udp    0.0.0.0/0
192.168.1.1/24     >1          =500        NA

Def_SNTP_UDP_Filter      udp    0.0.0.0/0
0.0.0.0/0          >1          =123        NA

Def_SNMP_Trap_Filter     udp    0.0.0.0/0
192.168.1.1/24     >1          =162        NA

Def_IKE_NAT_UDP_Filter   udp    0.0.0.0/0
192.168.1.1/24     >1          =4500       NA

Def_IKE_UDP_Loc_Filter   udp    0.0.0.0/0
0.0.0.0/0          >1          =500        NA
```

This below section describes the steps involved in deleting the ipv4 firewall filter.

To delete the configured ipv4 firewall filter

10. Enter the Global Configuration mode.

    UltOs# configure terminal

11. Enter into firewall mode

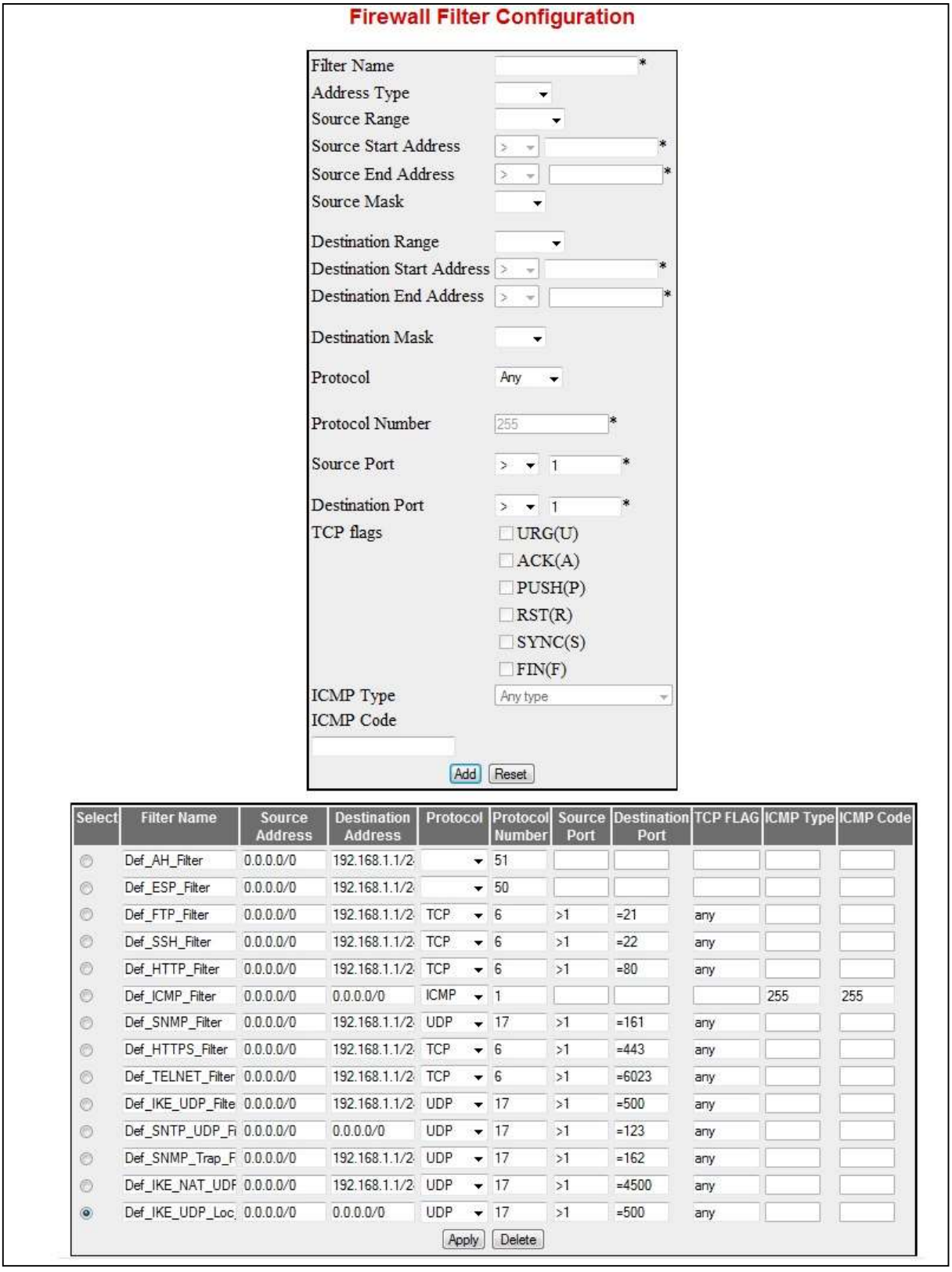
    UltOs(config)# firewall

12. Delete the ipv4 firewall filter

    UltOs(config-firewall)# no filter *filter2*

9.2.2.2 WEB Configuration

Firewall filters can be configured through WEB interface using the **Firewall Filter Configuration** screen (Navigation - **Security Management > Firewall > Filters)**



Screen 9-2: Firewall Filter Configuration

9.2.3 Configuring Firewall Access List

Firewall Access List is a policy which is based on the direction of the traffic, the firewall filter and the order of precedence to allow or deny the traffic. This section describes the steps involved in configuring firewall access-list.

9.2.3.1 CLI Configuration

To create an access-list:

1. Enter the global configuration mode.

   UltOs# configure terminal

2. Enter firewall mode

   UltOs(config)# firewall

3. Create an access list policy to allow traffic from H1 to H2.

   UltOs(config-firewall)# access-list acl1 lan wan filter1 permit 8

To view the configured firewall access list

UltOs# show firewall access-lists

```
Firewall Access Lists


     ACL Name             From     To       Filter
Combination        Action  Prio-  Fragmented
                           Zone     Zone
rity   Packet
--------------------     ------   ------   --------------
-------     ------  -----  ----------
acl1                       LAN      WAN      filter1
permit  8      permit
Def_HTTPS_ACL_LAN_Local  LAN      Local
Def_HTTPS_Filter          permit  9987   permit
Def_HTTP_ACL_LAN_Local   LAN      Local
Def_HTTP_Filter           permit  9984   permit
Def_SNMP_ACL_LAN_Local   LAN      Local
Def_SNMP_Filter           permit  9980   permit
Def_SNMP_Trap_ACL_LAN_LocalLAN      Local
Def_SNMP_Trap_Filter      permit  9976   permit
Def_SSH_ACL_LAN_Local    LAN      Local    Def_SSH_Filter
permit  9991   permit
Def_TELNET_ACL_LAN_Local LAN      Local
Def_TELNET_Filter         permit  9995   permit
Def_AH_ACL_WAN_Local     WAN      Local    Def_AH_Filter
permit  9967   permit
Def_ESP_ACL_WAN_Local    WAN      Local    Def_ESP_Filter
permit  9969   permit
Def_HTTPS_ACL_WAN_Local  WAN      Local
Def_HTTPS_Filter          permit  9989   permit
```

```
Def_IKE_ACL_WAN_Local    WAN      Local
Def_IKE_UDP_Filter        permit  9965   permit

Def_IKE_NAT_ACL_WAN_LocalWAN      Local
Def_IKE_NAT_UDP_Filter    permit  9963   permit

Def_SNMP_ACL_WAN_Local   WAN      Local
Def_SNMP_Filter           permit  9982   permit

Def_SNMP_Trap_ACL_WAN_LocalWAN      Local
Def_SNMP_Trap_Filter      permit  9978   permit

Def_SSH_ACL_WAN_Local    WAN      Local    Def_SSH_Filter
permit  9993   permit

Def_HTTPS_ACL_DMZ_Local  DMZ      Local
Def_HTTPS_Filter          permit  9986   permit

Def_HTTP_ACL_DMZ_Local   DMZ      Local
Def_HTTP_Filter           permit  9983   permit

Def_SNMP_ACL_DMZ_Local   DMZ      Local
Def_SNMP_Filter           permit  9979   permit

Def_SNMP_Trap_ACL_DMZ_LocalDMZ      Local
Def_SNMP_Trap_Filter      permit  9975   permit

Def_SSH_ACL_DMZ_Local    DMZ      Local    Def_SSH_Filter
permit  9990   permit

Def_TELNET_ACL_DMZ_Local DMZ      Local
Def_TELNET_Filter         permit  9994   permit

Def_HTTPS_ACL_VPN_Local  VPN      Local
Def_HTTPS_Filter          permit  9988   permit

Def_HTTP_ACL_VPN_Local   VPN      Local
Def_HTTP_Filter           permit  9985   permit

Def_SNMP_ACL_VPN_Local   VPN      Local
Def_SNMP_Filter           permit  9981   permit

Def_SNMP_Trap_ACL_VPN_LocalVPN      Local
Def_SNMP_Trap_Filter      permit  9977   permit

Def_SSH_ACL_VPN_Local    VPN      Local    Def_SSH_Filter
permit  9992   permit

Def_TELNET_ACL_VPN_Local VPN      Local
Def_TELNET_Filter         permit  9996   permit

Def_ACL_ICMP_Local_LAN   Local    LAN
Def_ICMP_Filter           permit  9961   permit

Def_FTP_ACL_Local_LAN    Local    LAN      Def_FTP_Filter
permit  9999   permit

Def_SNTP_ACL_Local_LAN   Local    LAN
Def_SNTP_UDP_Filter       permit  9972   permit

Def_ACL_ICMP_Local_WAN   Local    WAN
Def_ICMP_Filter           permit  9962   permit

Def_AH_ACL_Local_WAN     Local    WAN      Def_AH_Filter
permit  9968   permit
```

```
Def_ESP_ACL_Local_WAN    Local    WAN      Def_ESP_Filter
permit  9970   permit

Def_FTP_ACL_Local_WAN    Local    WAN      Def_FTP_Filter
permit  10000  permit

Def_IKENAT_ACL_Local_WAN Local    WAN
Def_IKE_NAT_UDP_Filter    permit  9964   permit

Def_IKE_ACL_Local_WAN    Local    WAN
Def_IKE_UDP_Loc_Filter    permit  9966   permit

Def_SNTP_ACL_Local_WAN   Local    WAN
Def_SNTP_UDP_Filter       permit  9974   permit

Def_ACL_ICMP_Local_DMZ   Local    DMZ
Def_ICMP_Filter           permit  9960   permit

Def_FTP_ACL_Local_DMZ    Local    DMZ      Def_FTP_Filter
permit  9998   permit

Def_SNTP_ACL_Local_DMZ   Local    DMZ
Def_SNTP_UDP_Filter       permit  9971   permit

Def_ACL_ICMP_Local_VPN   Local    VPN
Def_ICMP_Filter           permit  9959   permit

Def_FTP_ACL_Local_VPN    Local    VPN      Def_FTP_Filter
permit  9997   permit

Def_SNTP_ACL_Local_VPN   Local    VPN
Def_SNTP_UDP_Filter       permit  9973   permit
```

To delete the configured firewall access list:

4. Enter the Global Configuration mode.

   UltOs# configure terminal

5. Enter into firewall mode

   UltOs(config)# firewall

6. Delete the configured access-list

   UltOs(config-firewall)# no access-list acl1 lan wan

The below section describes the steps needed to allow traffic from WAN host H2 to LAN host H1 when nat configuration is disabled. The filter *filter2* created in section 3.2 is used to create an inbound access-list which permits traffic from H2 to H1.

To create an access-list:

7. Enter the global configuration mode.

   UltOs# configure terminal

8. Enter firewall mode

   UltOs(config)# firewall

9. Create an access list policy to allow traffic from H2 to H1.

   UltOs(config-firewall)# access-list acl2 wan lan filter2 permit 8

To view the configured firewall access list

UltOs# show firewall access-lists

```
Firewall Access Lists


     ACL Name             From     To       Filter
Combination        Action  Prio-  Fragmented
                           Zone     Zone
rity   Packet
--------------------     ------   ------   --------------
-------     ------  -----  ----------
Def_HTTPS_ACL_LAN_Local  LAN      Local
Def_HTTPS_Filter          permit  9987   permit
Def_HTTP_ACL_LAN_Local   LAN      Local
Def_HTTP_Filter           permit  9984   permit
Def_SNMP_ACL_LAN_Local   LAN      Local
Def_SNMP_Filter           permit  9980   permit
Def_SNMP_Trap_ACL_LAN_LocalLAN      Local
Def_SNMP_Trap_Filter      permit  9976   permit
Def_SSH_ACL_LAN_Local    LAN      Local    Def_SSH_Filter
permit  9991   permit
Def_TELNET_ACL_LAN_Local LAN      Local
Def_TELNET_Filter         permit  9995   permit
acl2                     WAN      LAN      filter2
permit  8      permit
Def_AH_ACL_WAN_Local     WAN      Local    Def_AH_Filter
permit  9967   permit
Def_ESP_ACL_WAN_Local    WAN      Local    Def_ESP_Filter
permit  9969   permit
Def_HTTPS_ACL_WAN_Local  WAN      Local
Def_HTTPS_Filter          permit  9989   permit
Def_IKE_ACL_WAN_Local    WAN      Local
Def_IKE_UDP_Filter        permit  9965   permit
Def_IKE_NAT_ACL_WAN_LocalWAN      Local
Def_IKE_NAT_UDP_Filter    permit  9963   permit
Def_SNMP_ACL_WAN_Local   WAN      Local
Def_SNMP_Filter           permit  9982   permit
Def_SNMP_Trap_ACL_WAN_LocalWAN      Local
Def_SNMP_Trap_Filter      permit  9978   permit
Def_SSH_ACL_WAN_Local    WAN      Local    Def_SSH_Filter
permit  9993   permit
Def_HTTPS_ACL_DMZ_Local  DMZ      Local
Def_HTTPS_Filter          permit  9986   permit
Def_HTTP_ACL_DMZ_Local   DMZ      Local
Def_HTTP_Filter           permit  9983   permit
Def_SNMP_ACL_DMZ_Local   DMZ      Local
Def_SNMP_Filter           permit  9979   permit
```

```
Def_SNMP_Trap_ACL_DMZ_LocalDMZ      Local
Def_SNMP_Trap_Filter      permit  9975   permit

Def_SSH_ACL_DMZ_Local    DMZ      Local    Def_SSH_Filter
permit  9990   permit

Def_TELNET_ACL_DMZ_Local DMZ      Local
Def_TELNET_Filter         permit  9994   permit

Def_HTTPS_ACL_VPN_Local  VPN      Local
Def_HTTPS_Filter          permit  9988   permit

Def_HTTP_ACL_VPN_Local   VPN      Local
Def_HTTP_Filter           permit  9985   permit

Def_SNMP_ACL_VPN_Local   VPN      Local
Def_SNMP_Filter           permit  9981   permit

Def_SNMP_Trap_ACL_VPN_LocalVPN      Local
Def_SNMP_Trap_Filter      permit  9977   permit

Def_SSH_ACL_VPN_Local    VPN      Local    Def_SSH_Filter
permit  9992   permit

Def_TELNET_ACL_VPN_Local VPN      Local
Def_TELNET_Filter         permit  9996   permit

Def_ACL_ICMP_Local_LAN   Local    LAN
Def_ICMP_Filter           permit  9961   permit

Def_FTP_ACL_Local_LAN    Local    LAN      Def_FTP_Filter
permit  9999   permit

Def_SNTP_ACL_Local_LAN   Local    LAN
Def_SNTP_UDP_Filter       permit  9972   permit

Def_ACL_ICMP_Local_WAN   Local    WAN
Def_ICMP_Filter           permit  9962   permit

Def_AH_ACL_Local_WAN     Local    WAN      Def_AH_Filter
permit  9968   permit

Def_ESP_ACL_Local_WAN    Local    WAN      Def_ESP_Filter
permit  9970   permit

Def_FTP_ACL_Local_WAN    Local    WAN      Def_FTP_Filter
permit  10000  permit

Def_IKENAT_ACL_Local_WAN Local    WAN
Def_IKE_NAT_UDP_Filter    permit  9964   permit

Def_IKE_ACL_Local_WAN    Local    WAN
Def_IKE_UDP_Loc_Filter    permit  9966   permit

Def_SNTP_ACL_Local_WAN   Local    WAN
Def_SNTP_UDP_Filter       permit  9974   permit

Def_ACL_ICMP_Local_DMZ   Local    DMZ
Def_ICMP_Filter           permit  9960   permit

Def_FTP_ACL_Local_DMZ    Local    DMZ      Def_FTP_Filter
permit  9998   permit

Def_SNTP_ACL_Local_DMZ   Local    DMZ
Def_SNTP_UDP_Filter       permit  9971   permit
```

```
Def_ACL_ICMP_Local_VPN   Local    VPN
Def_ICMP_Filter           permit  9959   permit

Def_FTP_ACL_Local_VPN    Local    VPN      Def_FTP_Filter
permit  9997   permit

Def_SNTP_ACL_Local_VPN   Local    VPN
Def_SNTP_UDP_Filter       permit  9973   permit
```

To delete the configured firewall access list:

10. Enter the Global Configuration mode.

    UltOs# configure terminal

11. Enter into firewall mode

    UltOs(config)# firewall

12. Delete the configured access-list

    UltOs(config-firewall)# no access-list acl2 wan lan

The below section describes the steps needed to create an inbound access-list as above, when nat configuration is enabled. To create an access-list, a virtual server needs to be created in the wan interface of FDN40-4 to allow the traffic from WAN network to LAN network. The filter *filter2* created in section 3.2 is used to create the access-list.

To create a virtual server:

13. Enter the global configuration mode.

    UltOs# configure terminal

14. Enter interface configuration mode

    UltOs(config)# interface wan 0/1

15. Create a virtual server in the wan interface of FDN40-4 (eth1). The following virtual server allows ftp traffic from H2 to H1.

    UltOs(config-if)# virtual server *10.0.0.10 ftp FTP-server*

To create an access-list:

16. Enter the global configuration mode.

    UltOs# configure terminal

17. Enter firewall mode

    UltOs(config)# firewall

18. Create an access list policy to allow traffic from WAN host H2 to LAN host H1.

    UltOs(config-firewall)# access-list natacl wan lan filter2 permit 10

To view the configured firewall access list

UltOs# show firewall access-lists

```
Firewall Access Lists


     ACL Name              From     To       Filter
Combination        Action  Prio-  Fragmented
```

```
                          Zone     Zone
rity   Packet
--------------------     ------   ------   --------------
-------     ------  -----  ----------

Def_HTTPS_ACL_LAN_Local  LAN      Local
Def_HTTPS_Filter          permit  9987   permit

Def_HTTP_ACL_LAN_Local   LAN      Local
Def_HTTP_Filter           permit  9984   permit

Def_SNMP_ACL_LAN_Local   LAN      Local
Def_SNMP_Filter           permit  9980   permit

Def_SNMP_Trap_ACL_LAN_LocalLAN      Local
Def_SNMP_Trap_Filter      permit  9976   permit

Def_SSH_ACL_LAN_Local    LAN      Local    Def_SSH_Filter
permit  9991   permit

Def_TELNET_ACL_LAN_Local LAN      Local
Def_TELNET_Filter         permit  9995   permit

natacl                   WAN      LAN      filter2
permit  10     permit

Def_AH_ACL_WAN_Local     WAN      Local    Def_AH_Filter
permit  9967   permit

Def_ESP_ACL_WAN_Local    WAN      Local    Def_ESP_Filter
permit  9969   permit

Def_HTTPS_ACL_WAN_Local  WAN      Local
Def_HTTPS_Filter          permit  9989   permit

Def_IKE_ACL_WAN_Local    WAN      Local
Def_IKE_UDP_Filter        permit  9965   permit

Def_IKE_NAT_ACL_WAN_LocalWAN      Local
Def_IKE_NAT_UDP_Filter    permit  9963   permit

Def_SNMP_ACL_WAN_Local   WAN      Local
Def_SNMP_Filter           permit  9982   permit

Def_SNMP_Trap_ACL_WAN_LocalWAN      Local
Def_SNMP_Trap_Filter      permit  9978   permit

Def_SSH_ACL_WAN_Local    WAN      Local    Def_SSH_Filter
permit  9993   permit

Def_HTTPS_ACL_DMZ_Local  DMZ      Local
Def_HTTPS_Filter          permit  9986   permit

Def_HTTP_ACL_DMZ_Local   DMZ      Local
Def_HTTP_Filter           permit  9983   permit

Def_SNMP_ACL_DMZ_Local   DMZ      Local
Def_SNMP_Filter           permit  9979   permit

Def_SNMP_Trap_ACL_DMZ_LocalDMZ      Local
Def_SNMP_Trap_Filter      permit  9975   permit

Def_SSH_ACL_DMZ_Local    DMZ      Local    Def_SSH_Filter
permit  9990   permit
```

```
Def_TELNET_ACL_DMZ_Local DMZ      Local
Def_TELNET_Filter         permit  9994   permit

Def_HTTPS_ACL_VPN_Local  VPN      Local
Def_HTTPS_Filter          permit  9988   permit

Def_HTTP_ACL_VPN_Local   VPN      Local
Def_HTTP_Filter           permit  9985   permit

Def_SNMP_ACL_VPN_Local   VPN      Local
Def_SNMP_Filter           permit  9981   permit

Def_SNMP_Trap_ACL_VPN_LocalVPN      Local
Def_SNMP_Trap_Filter      permit  9977   permit

Def_SSH_ACL_VPN_Local    VPN      Local    Def_SSH_Filter
permit  9992   permit

Def_TELNET_ACL_VPN_Local VPN      Local
Def_TELNET_Filter         permit  9996   permit

Def_ACL_ICMP_Local_LAN   Local    LAN
Def_ICMP_Filter           permit  9961   permit

Def_FTP_ACL_Local_LAN    Local    LAN      Def_FTP_Filter
permit  9999   permit

Def_SNTP_ACL_Local_LAN   Local    LAN
Def_SNTP_UDP_Filter       permit  9972   permit

Def_ACL_ICMP_Local_WAN   Local    WAN
Def_ICMP_Filter           permit  9962   permit

Def_AH_ACL_Local_WAN     Local    WAN      Def_AH_Filter
permit  9968   permit

Def_ESP_ACL_Local_WAN    Local    WAN      Def_ESP_Filter
permit  9970   permit

Def_FTP_ACL_Local_WAN    Local    WAN      Def_FTP_Filter
permit  10000  permit

Def_IKENAT_ACL_Local_WAN Local    WAN
Def_IKE_NAT_UDP_Filter    permit  9964   permit

Def_IKE_ACL_Local_WAN    Local    WAN
Def_IKE_UDP_Loc_Filter    permit  9966   permit

Def_SNTP_ACL_Local_WAN   Local    WAN
Def_SNTP_UDP_Filter       permit  9974   permit

Def_ACL_ICMP_Local_DMZ   Local    DMZ
Def_ICMP_Filter           permit  9960   permit

Def_FTP_ACL_Local_DMZ    Local    DMZ      Def_FTP_Filter
permit  9998   permit

Def_SNTP_ACL_Local_DMZ   Local    DMZ
Def_SNTP_UDP_Filter       permit  9971   permit

Def_ACL_ICMP_Local_VPN   Local    VPN
Def_ICMP_Filter           permit  9959   permit

Def_FTP_ACL_Local_VPN    Local    VPN      Def_FTP_Filter
permit  9997   permit
```

```
Def_SNTP_ACL_Local_VPN   Local    VPN
Def_SNTP_UDP_Filter       permit  9973   permit
```

To view the configured virtual server:

UltOs# show virtual servers

```
Virtual Servers Configuration
-----------------------------
Interface   :  wan0/1
Local IP    :  10.0.0.10          Local Port  :  21
Protocol    :  ANY
Global IP   :  100.0.0.1          Global Port :  21
App Type    :  FTP
Description :  FTP-server
Status      :  Disabled
```

----------To delete the configured firewall access list:

19. Enter the Global Configuration mode.

    UltOs# configure terminal

20. Enter into firewall mode

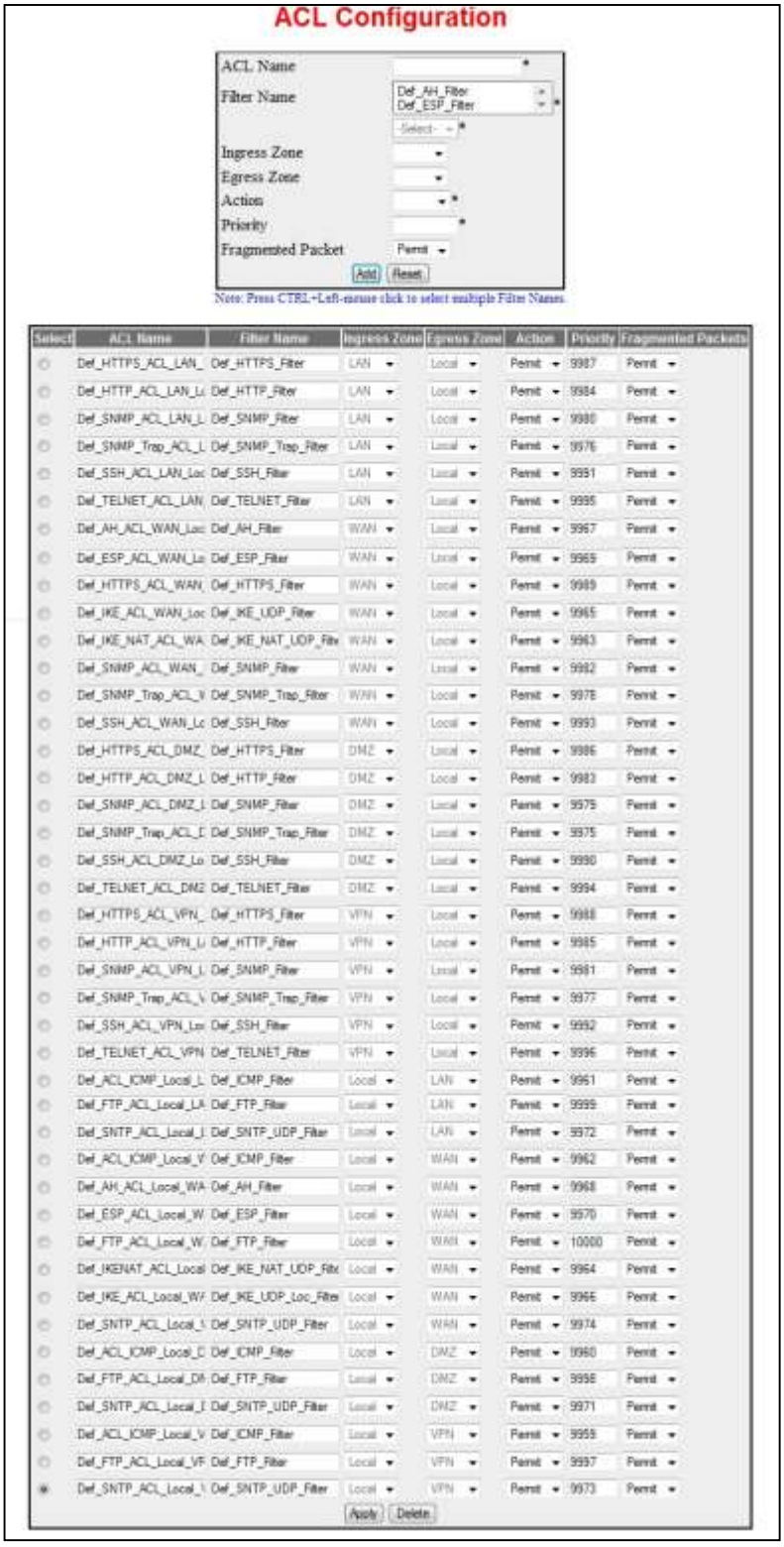
    UltOs(config)# firewall

21. Delete the configured access-list

    UltOs(config-firewall)# no access-list natacl wan lan

9.2.3.2 WEB Configuration

Firewall Access Lists can be configured through WEB interface using the **ACL Configuration** screen (Navigation - **Security Management > Firewall > Access List)**



Screen 9-3: Firewall - ACL Configuration

9.2.4 Configuring Zones

Firewall configuration works on zone basis. User needs to specify ingress and egress zones while configuring Firewall Access List. Zones are classified as follows,

1. Local
2. LAN
3. WAN
4. DMZ
5. VPN

Local zone will be taken by default when IP interface is created.

LAN, WAN and DMZ zones can be configured by the user.

DMZ or De Militarized Zone is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The host/hosts in this zone, called DMZ host, will have unrestricted access from the public/external network (Internet). This section describes the steps involved in setting and resetting a host in the Local Area Network as DMZ host.

VPN zone comes into effect when IPSec tunnel is established.

9.2.4.1 CLI Configuration

To configure a IPv4 DMZ host

UltOs# c t

UltOs(config)# interface wan 0/1

UltOs(config-if)# switchport

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan 10

UltOs(config-vlan)# ports add wan 0/1

UltOs(config-vlan)# exit

UltOs(config)# interface vlan 10

UltOs(config-if)# ip address 10.10.10.2 255.255.255.0

UltOs(config-if)# no shutdown

UltOs(config-if)# zone wan

UltOs(config-if)# exit

UltOs(config)# interface lan 0/1

UltOs(config-if)# no shutdown

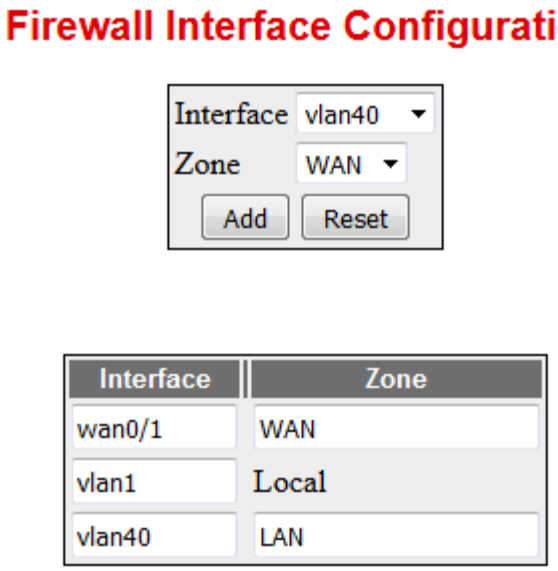
UltOs(config-if)# exit

UltOs(config)# vlan 11

```
UltOs(config-vlan)# ports add lan 0/1
UltOs(config-vlan)# exit
UltOs(config)# interface vlan 11
UltOs(config-if)# no shutdown
UltOs(config-if)# ip address 11.11.11.2 255.255.255.0
UltOs(config-if)# zone lan
UltOs(config-if)# exit
UltOs(config)# vlan 13
UltOs(config-vlan)# ports add lan 0/1
UltOs(config-vlan)# exit
UltOs(config)# interface vlan 13
UltOs(config-if)# ip address 13.0.0.1 255.255.255.0
UltOs(config-if)# zone dmz
UltOs(config-if)# no shutdown
UltOs(config-if)# end
UltOs# show firewall interface config

     Firewall Zones
    ----------------
   Interface         Zone
---------------   -----------
wan0/2          WAN
vlan1           Local
vlan10           WAN
vlan11           LAN
vlan13           DMZ
```

9.2.4.2 WEB Configuration

IPv4 DMZ zone can be configured through WEB interface using the **Firewall Interface Configuration** screen (Navigation - **Layer3 Management > IP > Zone)**



Screen 9-4: Firewall Interface Configuration

Chapter 10

IPS-IDS

10.1 Topology

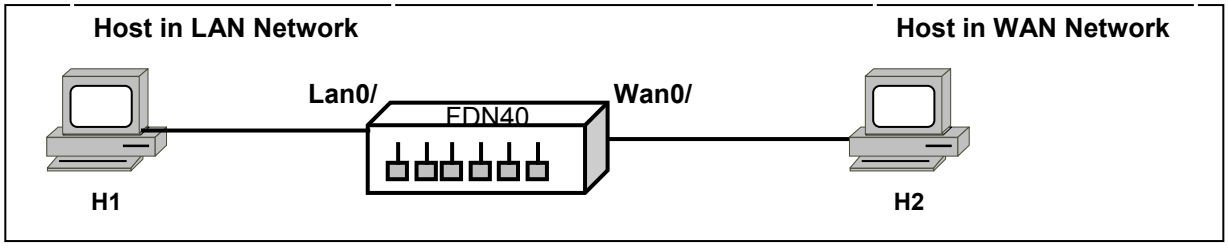


Figure 10-5: IPS Topology

Table 10-1: IPv4 Addresses of Interfaces and Hosts

Interface Index/Name	Interface IPv4 Address
LAN0/1	10.0.0.1
WAN0/1	80.0.0.1
H1	10.0.0.10
H2	80.0.0.10

10.2 Default Configurations

When **system** comes up, **IPS-IDS** is operationally disabled.

10.3 IPS-IDS Configurations

10.3.1 Enabling and Disabling IPS-IDS Module

This section describes the steps involved in enabling and disabling the IPS-IDS status globally. By default, IPS-IDS status is disabled.

10.3.1.1 CLI Configuration

To enable IPS-IDS:

1. Enter the Global Configuration mode.

   UltOs# configure terminal
2. Enable the Firewall module.

   UltOs(config)# firewall

   UltOs(config-firewall)# enable
3. Enable IPS-IDS status

   UltOs(config-firewall)# ips-ids enable
4. Exit from the Global Configuration mode.

   UltOs(config-firewall)# end

To disable IPS-IDS:

5. Enter the Global Configuration mode.

   UltOs# configure terminal
6. Enter firewall configuration mode.

   UltOs(config)# firewall
7. Disable IPS-IDS status.

   UltOs(config-firewall)# ips-ids disable
8. Exit from the Global Configuration mode.

   UltOs(config-firewall)# end

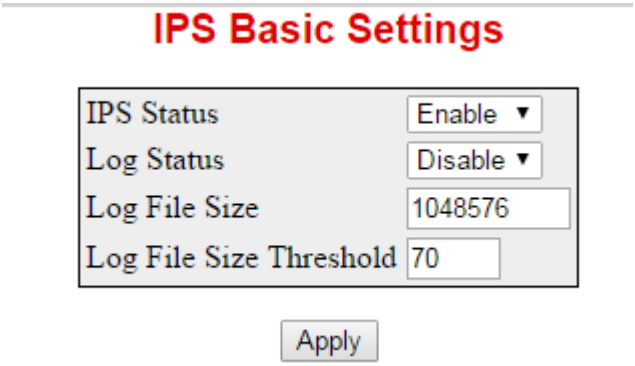
To view the IPS status:

9. UltOs# show ips **config**

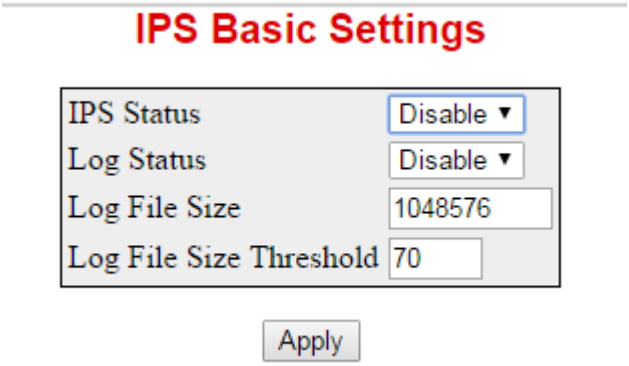
```
IPS Configuration
----------------------


IPS/IDS Status                : Enabled
IDS Logging Status            : Enabled
IPS Log file Size             : 1048576
IPS Log file Size Threshold   : 70
```

10.3.1.2 WEB Configuration

IPS-IDS global status is configured through WEB interface using IPS Basic Settings screen (**Home->Security Management->IPS)**



Screen 10-1: IPS Basic Settings - Enabling IPS-IDS global status



Screen 10-2: IPS Basic Settings - Disabling IPS-IDS global status

10.3.2 Enabling and Disabling IDS Logging

This section describes the steps involved in enabling and disabling the IDS slogging status. By default, IDS logging status is **disabled**.

10.3.2.1 CLI Configuration

To enable IDS Logging:

1. Enter the Global Configuration mode.

   UltOs# configure terminal
2. Enable the Firewall module.

   UltOs(config)# firewall

   UltOs(config-firewall)# enable
3. Enable IPS-IDS status

   UltOs(config-firewall)# ids logging
4. Exit from the Global Configuration mode.

UltOs(config-firewall)# end

To disable IDS Logging:

5. Enter the Global Configuration mode.

   UltOs# configure terminal

6. Enter firewall configuration mode.

   UltOs(config)# firewall

7. Disable IPS-IDS status.

   UltOs(config-firewall)# no ids logging

8. Exit from the Global Configuration mode.

   UltOs(config-firewall)# end

To view the IDS logging status:

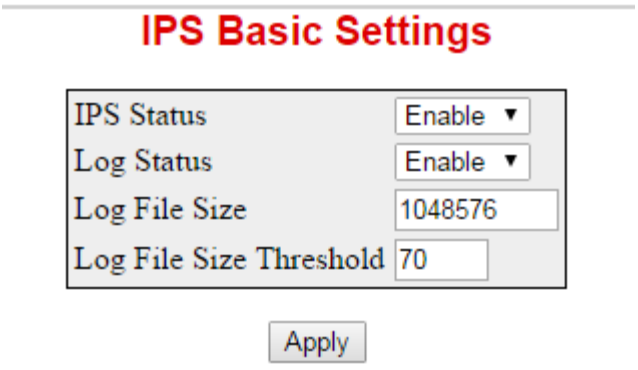
9. UltOs# show ips **config**

```
IPS Configuration
---------------------

IPS/IDS Status                : Enabled
IDS Logging Status            : Enabled
IPS Log file Size             : 1048576
IPS Log file Size Threshold   : 70
```

10.3.2.2 WEB Configuration

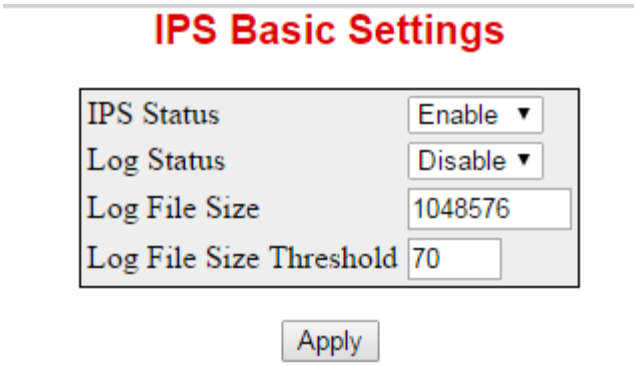
IPS-IDS global status is configured through WEB interface using IPS Basic Settings screen (**Home->Security Management->IPS)**

Enabling IDS logging status through web interface



Screen 10-3: IPS Basic Settings - Enabling IDS logging status

Disabling IDS logging status through web interface



Screen 10-4: IPS Basic Settings - Disabling IDS logging status

10.3.3 Configuring IDS Logging Size and Log Size Threshold

This section describes the steps involved in configuring the IDS logging file size and logging size threshold. By default, the IDS logging file size is 1048576Kb and logging file size threshold is 70%.

10.3.3.1 CLI Configuration

To configure IDS logging file size and threshold:

1. Enter the Global Configuration mode.

   UltOs# configure terminal
2. Enable the Firewall module.

   UltOs(config)# firewall
3. Configure IDS log file size

   UltOs(config-firewall)# ids logging filesize 1045600
4. Configure IDS logging threshold

   UltOs(config-firewall)# ids logging logsize-threshold 80
5. Exit from the Global Configuration mode.

   UltOs(config-firewall)# end

To view the IDS logging file size and threshold:

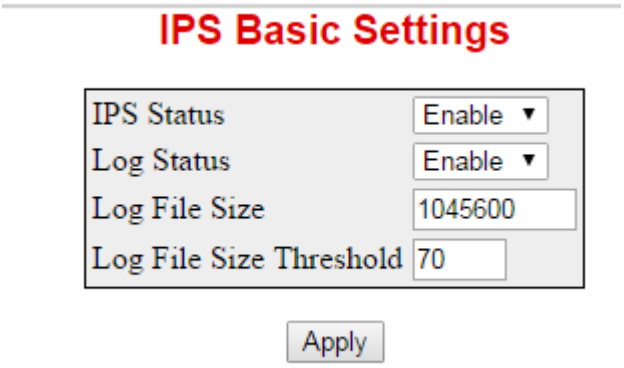
6. **UltOs# show** ips **config**

```
IPS Configuration
----------------------

IPS/IDS Status                : Enabled
IDS Logging Status            : Enabled
IPS Log file Size             : 1045600
IPS Log file Size Threshold   : 80
```

10.3.3.2 WEB Configuration

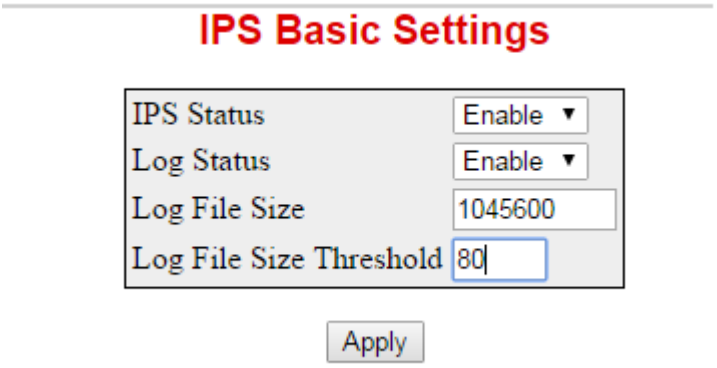
IPS-IDS Logging file size and threshold is configured through WEB interface using IPS Basic Settings screen (**Home->Security Management->IPS)**

Configure IDS logging file size as 1045600 through web interface



Screen 10-5: IPS Basic Settings - Configure IDS logging file size

Configure IDS logging threshold as 80% through web interface



Screen 10-6: IPS Basic Settings - Disabling IDS logging status

10.3.4 Configuring IPS status in firewall access-list

This section describes the steps involved in enabling and disabling the IPS status in the firewall access-list to lookup DPI engine per flow. For creating firewall access-list refer section 15.3.1.5. By default, the IPS status in the firewall access-list is disabled. Refer section 15.3 for interface configuration with packet processing.

10.3.4.1 CLI Configuration

To configure IPS status per firewall access-list:

1. To enable IPS status in access-list:

2. Enter the Global Configuration mode.

   UltOs# configure terminal

3. Enable the Firewall module.

   UltOs(config)# firewall

4. Enable Global IPS status

   UltOs(config-firewall)#ips-ids enable

5. Enable IPS status in firewall access-list

   UltOs(config-firewall)# access-list acl1 lan wan filter1 permit 8 ips enable

6. Exit from the Global Configuration mode.

   UltOs(config-firewall)# end

7. Disable IPS status in firewall access-list
8. Enter the Global Configuration mode.

   UltOs# configure terminal

9. Enable the Firewall module.

   UltOs(config)# firewall

10. Enable Global IPS status

    UltOs(config-firewall)#ips-ids enable

11. Enable IPS status in firewall access-list

    UltOs(config-firewall)# access-list acl1 lan wan filter1 permit 8 ips disable

12. Exit from the Global Configuration mode.

    UltOs(config-firewall)# end

To view the IPS status per firewall access-list:

13. **UltOs# show** firewall access-lists

```
Firewall Access Lists


     ACL Name             From      To       Filter
Combination        Action  Prio-   Fragmented
IPS

                          Zone      Zone
rity   Packet            Status

--------------------      ------    ------   --------
-------------     ------  -----  ----------     ---
-------

acl1                      LAN       WAN      filter1
permit  8      permit          Enable

Def_HTTPS_ACL_LAN_Local   LAN       Local
Def_HTTPS_Filter           permit   9987   permit
Disable

Def_HTTP_ACL_LAN_Local    LAN       Local
Def_HTTP_Filter            permit   9984   permit
Disable
```

```
Def_SNMP_ACL_LAN_Local   LAN      Local
Def_SNMP_Filter           permit  9980   permit
Disable

Def_SNMP_Trap_ACL_LAN_LocalLAN      Local
Def_SNMP_Trap_Filter      permit  9976   permit
Disable

Def_SSH_ACL_LAN_Local    LAN      Local
Def_SSH_Filter            permit  9991   permit
Disable

Def_TELNET_ACL_LAN_Local LAN      Local
Def_TELNET_Filter         permit  9995   permit
Disable

Def_AH_ACL_WAN_Local     WAN      Local
Def_AH_Filter             permit  9967   permit
Disable

Def_ESP_ACL_WAN_Local    WAN      Local
Def_ESP_Filter            permit  9969   permit
Disable

Def_HTTPS_ACL_WAN_Local  WAN      Local
Def_HTTPS_Filter          permit  9989   permit
Disable

Def_IKE_ACL_WAN_Local    WAN      Local
Def_IKE_UDP_Filter        permit  9965   permit
Disable

Def_IKE_NAT_ACL_WAN_LocalWAN      Local
Def_IKE_NAT_UDP_Filter    permit  9963   permit
Disable

Def_SNMP_ACL_WAN_Local   WAN      Local
Def_SNMP_Filter           permit  9982   permit
Disable

Def_SNMP_Trap_ACL_WAN_LocalWAN      Local
Def_SNMP_Trap_Filter      permit  9978   permit
Disable

Def_SSH_ACL_WAN_Local    WAN      Local
Def_SSH_Filter            permit  9993   permit
Disable

Def_HTTPS_ACL_DMZ_Local  DMZ      Local
Def_HTTPS_Filter          permit  9986   permit
Disable

Def_HTTP_ACL_DMZ_Local   DMZ      Local
Def_HTTP_Filter           permit  9983   permit
Disable

Def_SNMP_ACL_DMZ_Local   DMZ      Local
Def_SNMP_Filter           permit  9979   permit
Disable

Def_SNMP_Trap_ACL_DMZ_LocalDMZ      Local
Def_SNMP_Trap_Filter      permit  9975   permit
Disable
```

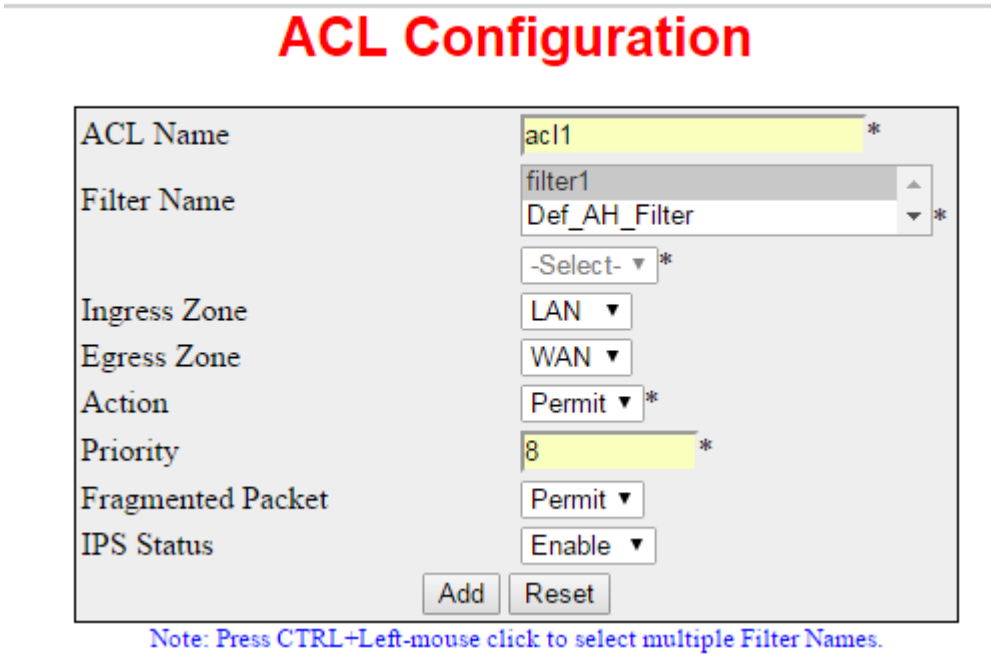
```
Def_SSH_ACL_DMZ_Local    DMZ      Local
Def_SSH_Filter            permit  9990   permit
Disable

Def_TELNET_ACL_DMZ_Local DMZ      Local
Def_TELNET_Filter         permit  9994   permit
Disable

Def_HTTPS_ACL_VPN_Local  VPN      Local
Def_HTTPS_Filter          permit  9988   permit
Disable

Def_HTTP_ACL_VPN_Local   VPN      Local
Def_HTTP_Filter           permit  9985   permit
Disable

Def_SNMP_ACL_VPN_Local   VPN      Local
Def_SNMP_Filter           permit  9981   permit
Disable

Def_SNMP_Trap_ACL_VPN_LocalVPN      Local
Def_SNMP_Trap_Filter      permit  9977   permit
Disable

Def_SSH_ACL_VPN_Local    VPN      Local
Def_SSH_Filter            permit  9992   permit
Disable

Def_TELNET_ACL_VPN_Local VPN      Local
Def_TELNET_Filter         permit  9996   permit
Disable

Def_ACL_ICMP_Local_LAN   Local    LAN
Def_ICMP_Filter           permit  9961   permit
Disable

Def_FTP_ACL_Local_LAN    Local    LAN
Def_FTP_Filter            permit  9999   permit
Disable

Def_SNTP_ACL_Local_LAN   Local    LAN
Def_SNTP_UDP_Filter       permit  9972   permit
Disable

Def_ACL_ICMP_Local_WAN   Local    WAN
Def_ICMP_Filter           permit  9962   permit
Disable

Def_AH_ACL_Local_WAN     Local    WAN
Def_AH_Filter             permit  9968   permit
Disable

Def_ESP_ACL_Local_WAN    Local    WAN
Def_ESP_Filter            permit  9970   permit
Disable

Def_FTP_ACL_Local_WAN    Local    WAN
Def_FTP_Filter            permit  10000  permit
Disable

Def_IKENAT_ACL_Local_WAN Local    WAN
Def_IKE_NAT_UDP_Loc_Filterpermit  9964   permit
Disable
```

```
Def_IKE_ACL_Local_WAN    Local    WAN
Def_IKE_UDP_Loc_Filter    permit  9966   permit
Disable

Def_SNTP_ACL_Local_WAN   Local    WAN
Def_SNTP_UDP_Filter       permit  9974   permit
Disable

Def_ACL_ICMP_Local_DMZ   Local    DMZ
Def_ICMP_Filter           permit  9960   permit
Disable

Def_FTP_ACL_Local_DMZ    Local    DMZ
Def_FTP_Filter            permit  9998   permit
Disable

Def_SNTP_ACL_Local_DMZ   Local    DMZ
Def_SNTP_UDP_Filter       permit  9971   permit
Disable

Def_ACL_ICMP_Local_VPN   Local    VPN
Def_ICMP_Filter           permit  9959   permit
Disable

Def_FTP_ACL_Local_VPN    Local    VPN
Def_FTP_Filter            permit  9997   permit
Disable

Def_SNTP_ACL_Local_VPN   Local    VPN
Def_SNTP_UDP_Filter       permit  9973   permit
Disable
```

10.3.4.2 WEB Configuration

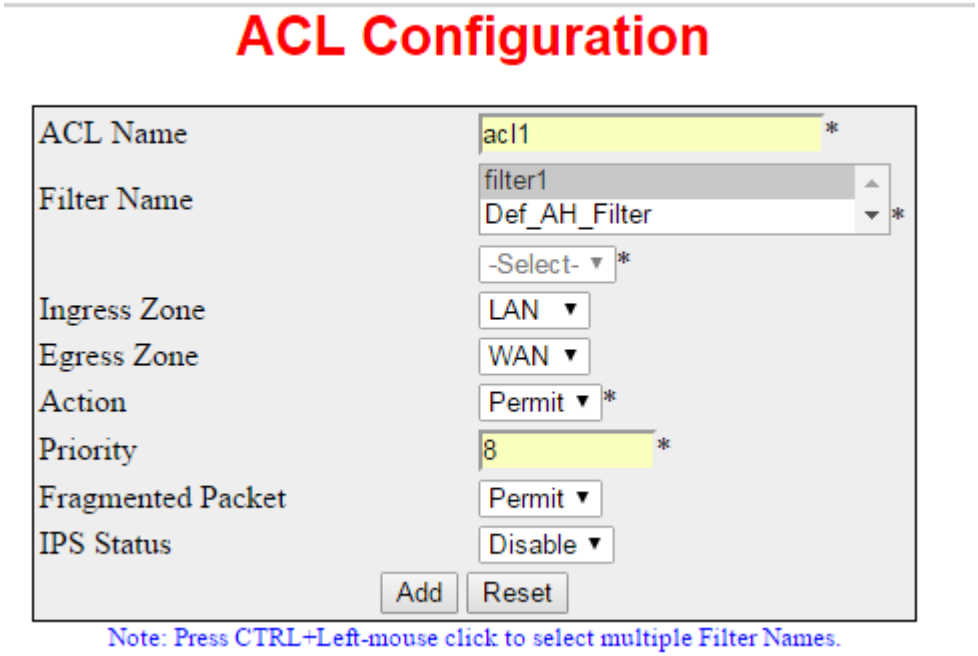
IPS status in firewall access-list is configured through WEB interface using IPS Basic Settings screen (**Home->Security Management->Firewall->Access List)**

Configuring IPS status as enabled in firewall access-list



Screen 10-7: Firewall Access List - Configure IPS status as enabled

Configure IPS status per access-list as disabled through web interface



Screen 10-8: Firewall Access List - Configure IPS status as disabled

To view IPS status in the firewall access-list

Screen 10-9: Firewall Access List – View IPS status

10.3.5 Displaying IPS Categories and IPS Rules

This section describes the steps involved in displaying IPS signature categories and IPS Rules per category. IPS signature files are loaded in the FLASH to view the categories and rules

10.3.5.1 CLI Configuration

To display IPS signature categories:

1. **UltOs# show** ips **categories**

```
IPS Categories


 ==============
not-suspicious
unknown
bad-unknown
attempted-recon
successful-recon-limited
successful-recon-largescale
attempted-dos
successful-dos
attempted-user
unsuccessful-user
successful-user
attempted-admin
successful-admin
rpc-portmap-decode
shellcode-detect
string-detect
suspicious-filename-detect
suspicious-login
system-call-detect
tcp-connection
trojan-activity
```

```
unusual-client-port-connection
network-scan
denial-of-service
non-standard-protocol
protocol-command-decode
web-application-activity
web-application-attack
misc-activity
misc-attack
icmp-event
inappropriate-content
policy-violation
default-login-attempt
sdf
file-format
malware-cnc
client-side-exploit
```

To display signatures per category:

2. **UltOs# show ips rules not-suspicious**

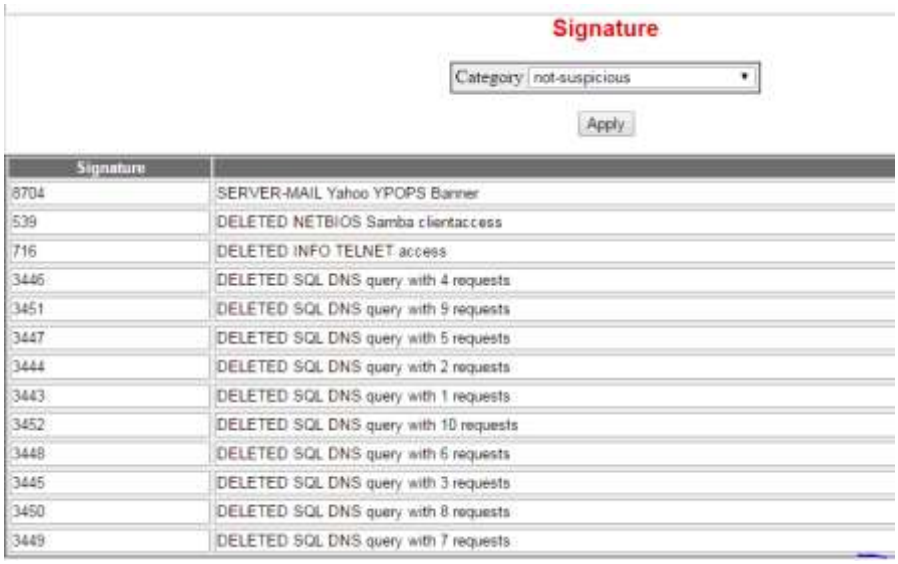
```
IPS Categories Rule List - not-suspicious

 ================================================

 SID     Description

 ======
==================================================
=================
8704     SERVER-MAIL Yahoo YPOPS Banner
539      DELETED NETBIOS Samba clientaccess
716      DELETED INFO TELNET access
3446     DELETED SQL DNS query with 4 requests
3451     DELETED SQL DNS query with 9 requests
3447     DELETED SQL DNS query with 5 requests
3444     DELETED SQL DNS query with 2 requests
3443     DELETED SQL DNS query with 1 requests
3452     DELETED SQL DNS query with 10 requests
3448     DELETED SQL DNS query with 6 requests
```

```
3445      DELETED SQL DNS query with 3 requests
3450      DELETED SQL DNS query with 8 requests
3449      DELETED SQL DNS query with 7 requests
```

10.3.5.2 WEB Configuration

IPS Signature Categories and rules are displayed through WEB interface using IPS Basic Settings screen (**Home->Security Management->IPS->IPS Signature)**

To Display Signatures per category



Screen 100-10: IPS Signature – Display signatures for not-suspicious category

Chapter 11

POE

11.1 Protocol Description

Power over Ethernet technology is a system that transmits electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. The advantage of this technology is that the installers need to run only a single Ethernet cable that carries both power and data to each device. IP telephones, wireless LAN access points, webcams, Ethernet hubs, computers, and other appliances use this technology. Access Points and network devices can be easily located, decreasing installation costs in many cases.

Power over Ethernet is standardized in IEEE 802.3af. This technology offers new options to system designers by providing economical and flexible deployment of networked devices.

POE is supported only in the 6 port Variant of FDN406

11.2 Topology

This network topology explains IP phone and Wireless access point connection to FDN406P. When POE is enabled on these ports, power will be delivered to IP phone and Access point.

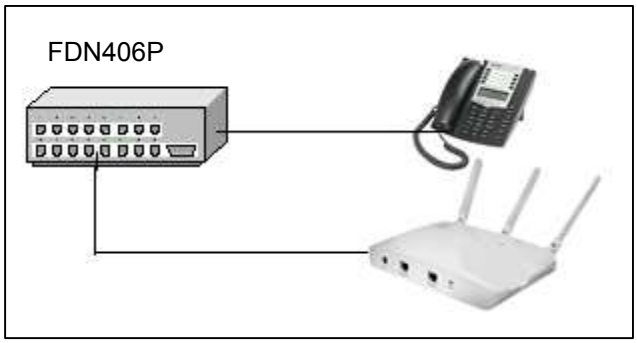


Figure 11-1

11.3 POE Configurations

11.3.1 Enabling POE Module

This section describes steps involved in enabling POE module.

11.3.1.1 CLI Configuration

To enable POE globally

- Enter the Global Configuration mode.

  UltOs# configure terminal
- Enable the POE module.

  UltOs(config)# set poe enable
- Exit from the Global Configuration mode.

  UltOs(config)# end

To view the POE global status

UltOs# show power detail

PSE Status

PoE Global Admin State : Enabled

PSE Oper Status : On

Max Power Supply : 1

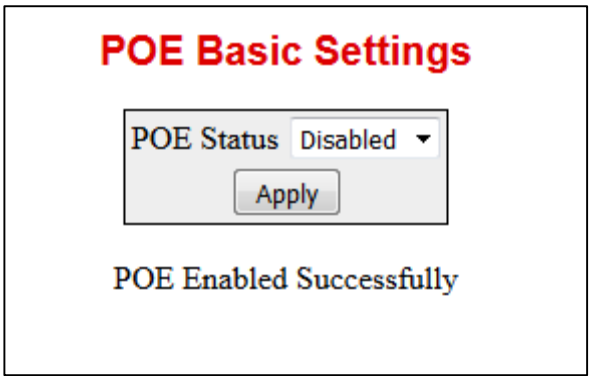
Total Power in (watts) : 30

Total Power Consumed : 0

Pse Usage Threshold : 99

11.3.1.2 WEB Configuration

POE can be enabled / disabled using the **POE Basic Settings** screen (Navigation – **POE> POE Basic Settings)**



Screen 111-1: POE Basic Settings

11.3.2 Enabling POE on port

11.3.2.1 CLI Configuration

To Enable POE on port

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode

  UltOs(config)# interface lan 0/6

- Enable POE on the interface

3. UltOs(config-if)# power inline enable

- Exit from the Interface Configuration mode.

  UltOs(config-if)# end

To View power applied on port

UltOs# show power inline lan 0/6

PoE Port Info

Port Number : 10(lan 0/6)

PoeAdminStatus : Up

PoeDetectionState : Disabled

class : 0

Priority : low

Port Power Mode : Never

Port Power : 0

Actual Pwr Consumed: 0

To view power applied on all the ports

UltOs# show power inline

PoE Port Info

Port-Index PoeAdminState DetectionSts pwrClass priority Mode PwrConfigured ActualPwrConsumed

---

5(lan 0/1) down Disabled class 0 low Never 0 Watts 0 Watts

6(lan 0/2) down Disabled class 0 low Never 0 Watts 0 Watts

7(lan 0/3) down Disabled class 0 low Never 0 Watts 0 Watts

8(lan 0/4) down Disabled class 0 low Never 0 Watts 0 Watts

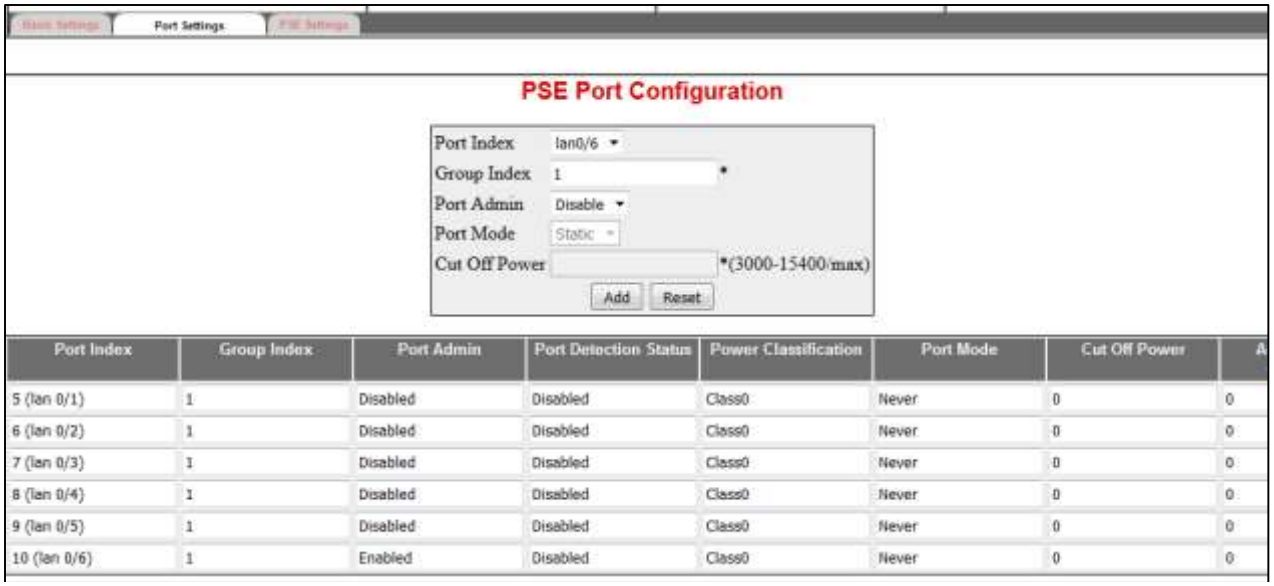
9(lan 0/5) down Disabled class 0 low Never 0 Watts 0 Watts

10(lan 0/6) up Disabled class 0 low Never 0 Watts 0 Watts

11.3.2.2 WEB Configuration

POE functionality on interface can be enabled on PSE Port Configuration page

(Navigation – **POE> Port Settings)**



Screen 111-2: POE Port Configuration

11.3.3 To apply power to a POE device

11.3.3.1 CLI Configuration

To apply power to a POE device

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode

  UltOs(config)# interface lan 0/6

- Apply power on the interface

4. UltOs(config-if)# power inline static 6000

- Exit from the Interface Configuration mode.

  UltOs(config-if)# end

To view the device power status

UltOs# show power inline lan 0/6

PoE Port Info

Port Number : 10(lan 0/6)

PoeAdminStatus : Up

PoeDetectionState : Delivering Power

class : 0

Priority : low

Port Power Mode : Static

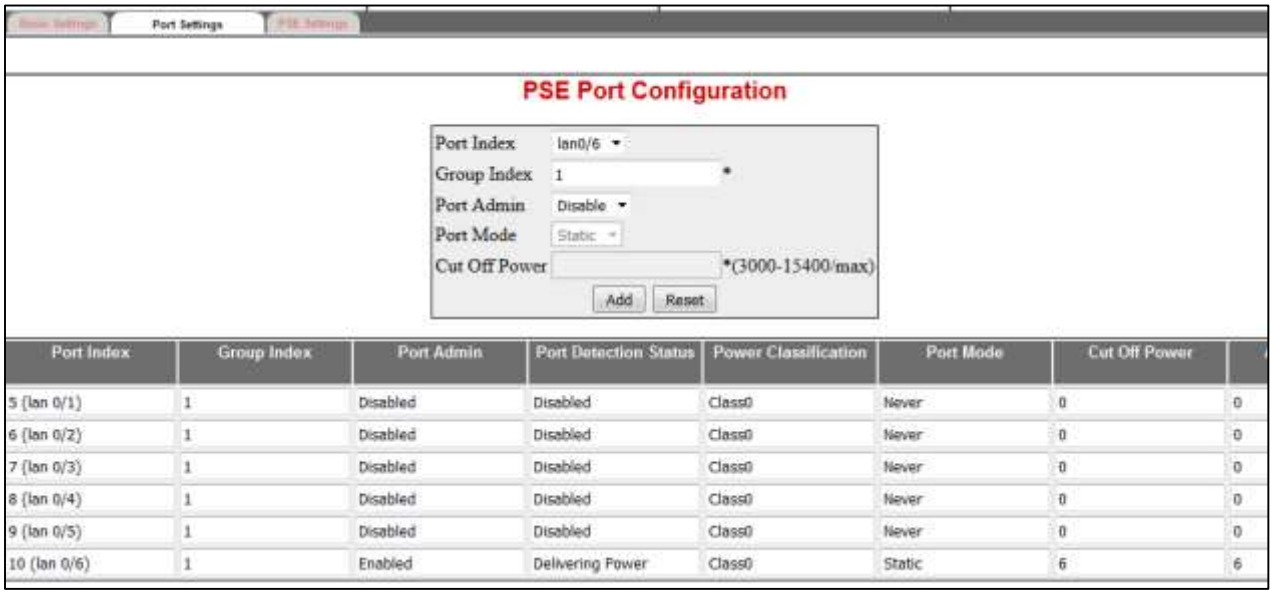
Port Power : 6

Actual Pwr Consumed: 6000

11.3.3.2 WEB Configuration

Power can be applied to a device on PSE Port Configuration page

(Navigation – **POE> Port Settings)**



Screen 111-3: POE Port Configuration

11.3.4 To view the PSE status

11.3.4.1 CLI Configuration

To view the PSE status

UltOs# show power detail

PSE Status

PoE Global Admin State : Enabled

PSE Oper Status : On

Max Power Supply : 1

Total Power in (watts) : 30

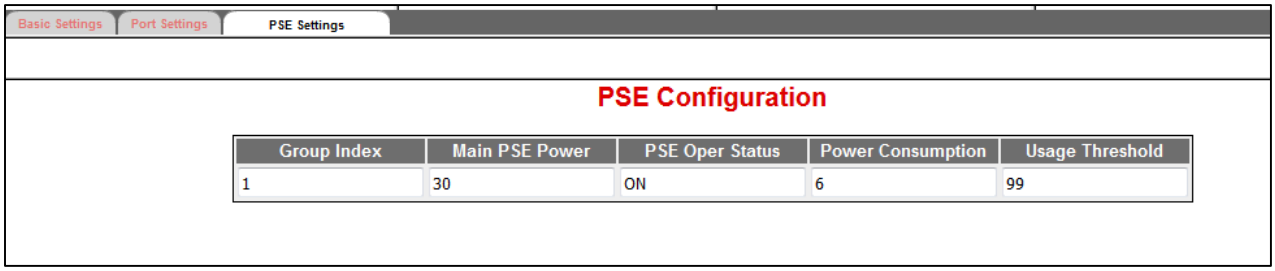
Total Power Consumed : 6

Pse Usage Threshold : 99

11.3.4.2 WEB Configuration

PSE status can be viewed on PSE configuration page

(Navigation – **POE> PSE Settings)**



Screen 111-4: PSE Configuration

Chapter 12

Wi-Fi

12.1 Topology

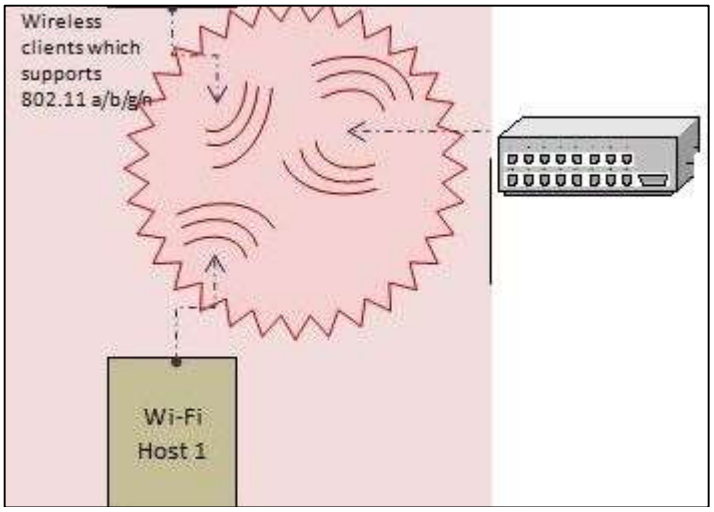


Figure 12-1: Wi-Fi Topology

Table 12-1: Wi-Fi Topology Description

Switch / Host	Interface of FDN40 Switches	WiFi Host 1
FDN40-1(Supports 16 VAPs)	VLAN associated with each VAP	PC/Linux/Mobile with wireless adapter

12.2 Configuration Guidelines

The FDN40 CLI user manual can be referred for the complete set of commands and the various options available for configuring Wi-Fi.

12.3 Wi-Fi Configurations

12.3.1 Enabling WiFi interfaces

12.3.1.1 CLI Configuration

1. Execute the following commands to enable Radio interfaces on the target.

   Enabling the radio0 interface programs the hardware and starts protocol operation.

   – Enter the Global Configuration Mode.

     UltOs# configure terminal

   – Specify the radio interface.

     UltOs(config)# apradio radio0

   – Enable the radio0 interface.

     UltOs(config-apradio0) # no shutdown

   – Exit the radio0 interface Mode

     UltOs(config-apradio0)#end

2. View the Wi-Fi interface status.

   UltOs# show interfaces description

```
Interface     Status    Protocol  Description
---------     ------    --------  -----------
wan0/1        down      down
ApRadio2      up        up
ApRadio3      down      down
lan0/1        down      down
lan0/2        down      down
lan0/3        down      down
lan0/4        down      down
vlan1         up        down
vlan100       up        up
```

   Use the following command to enable the radio1 interface.

   – Enter the Global Configuration Mode.

     UltOs# configure terminal

   – Specify the radio interface.

UltOs(config)# apradio radio1

– Enable the radio1 interface.

UltOs(config-apradio1) # no shutdown

– Exit the radio1 interface Mode

UltOs(config-apradio1)#end

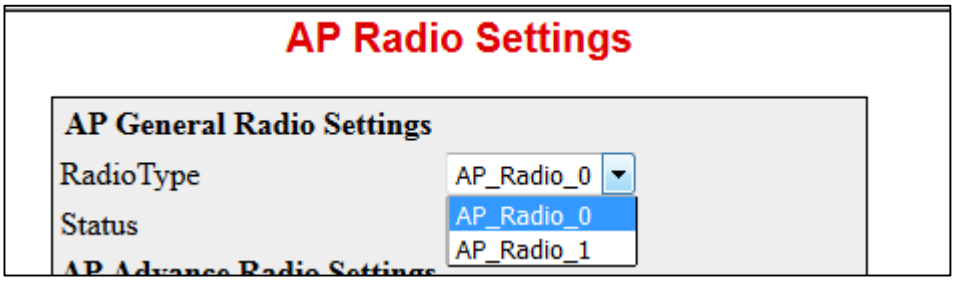
3. View the Wi-Fi interface status.

UltOs# show interfaces description

```
Interface     Status    Protocol  Description
---------     ------    --------  -----------
wan0/1        down      down
ApRadio2      down      down
ApRadio3      up        up
lan0/1        down      down
lan0/2        down      down
lan0/3        down      down
lan0/4        down      down
vlan1         up        down
vlan100       up        up
```

12.3.1.2 WEB Configuration

Radio Interfaces can be enabled through WEB interface using the **AP Radio Setings** screen (Navigation - **Home-> Access Point-> Radio Settings).** Select the radio Interface Radio0/Radio1 from "**RadioType**" tab and set the status to "**On"** in "**Staus**" tab.



Screen 12-1: AP RadioSettings - Enabling Radio Interfaces

12.3.2 Disabling Wi-Fi interface

12.3.2.1 CLI Configuration

1. Execute the following commands to enable Wi-Fi on the target.

Disabling the AP module, stops the protocol operation by deleting the hardware configuration.

- Enter the Global Configuration Mode.

  UltOs# configure terminal

- Specify the radio interface.

  UltOs(config)# apradio radio0

- To configure radio1 interface, use the following command

  UltOs(config)# apradio radio1

- Disable the Wi-Fi interface.

  UltOs(config-apradio) # no shutdown

- Exit the WiFi interface Mode

  UltOs(config-apradio)#exit

- Exit the global configuration Mode.

  UltOs(config)# exit

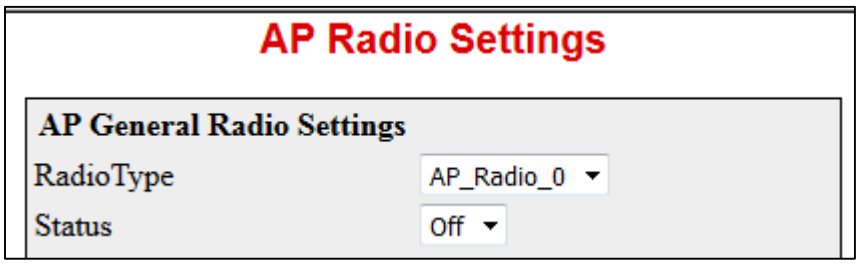
2. View the Wi-Fi interface status.

UltOs# show int desc

```
Interface     Status    Protocol  Description
---------     ------    --------  -----------
wan0/1        down      down
ApRadio2      down      down
ApRadio3      down      down
lan0/1        down      down
lan0/2        down      down
lan0/3        down      down
lan0/4        down      down
vlan1         up        down
vlan100       up        up
```

12.3.2.2 WEB Configuration

Radio Interface can be disabled through WEB interface using the **AP Radio Setings** screen (Navigation - **Home-> Access Point-> Radio Settings).** Select the Radio Interface and set the status to **Off**.



Screen 12-2: AP RadioSettings - Disabling Wi-Fi Interface

12.3.3 VAP creation and VLAN association

12.3.3.1 CLI Configuration

1. Execute the following commands to configure a virtual access point (VAP) on the target.

   This configuration would create a VAP interface to support virtual access point functionality.

   – Enter the Global Configuration Mode.

   UltOs# configure terminal

   – Specify the Radio interface.

   UltOs(config)# apradio radio0

   – Use the following command for configuring radio1 interfaces

   UltOs(config)# apradio radio1

   – Enable the Wi-Fi interface.

   UltOs(config-apradio) # no shutdown

   – Configure a VAP (maximum 31 characters length name)

   UltOs(config-apradio)# ssid *FDN40_ssid*

   – Associate a VLAN with the VAP interface

   UltOs(config-ssid)# vlan *100*

   – Exit the VAP configuration Mode.

   UltOs(config-ssid)# exit

   – Exit the WiFi interface Mode

   UltOs(config-apradio)#exit

   – Exit the global configuration Mode.

   UltOs(config)# exit

2. View the Default configurations for the created VAP in the

   VAP summary table

   UltOs# show apradio radio0 ssid summary

```
SSID : FDN40_ssid
BeaconPeriod :100
DTIM Period :1
Regulatory Domain:Yes
Rate :216700000
RTS threshold :2347
Fragmentation Threshold :2346
Vlan :100
Country :US
Radiomode :802.11an
```

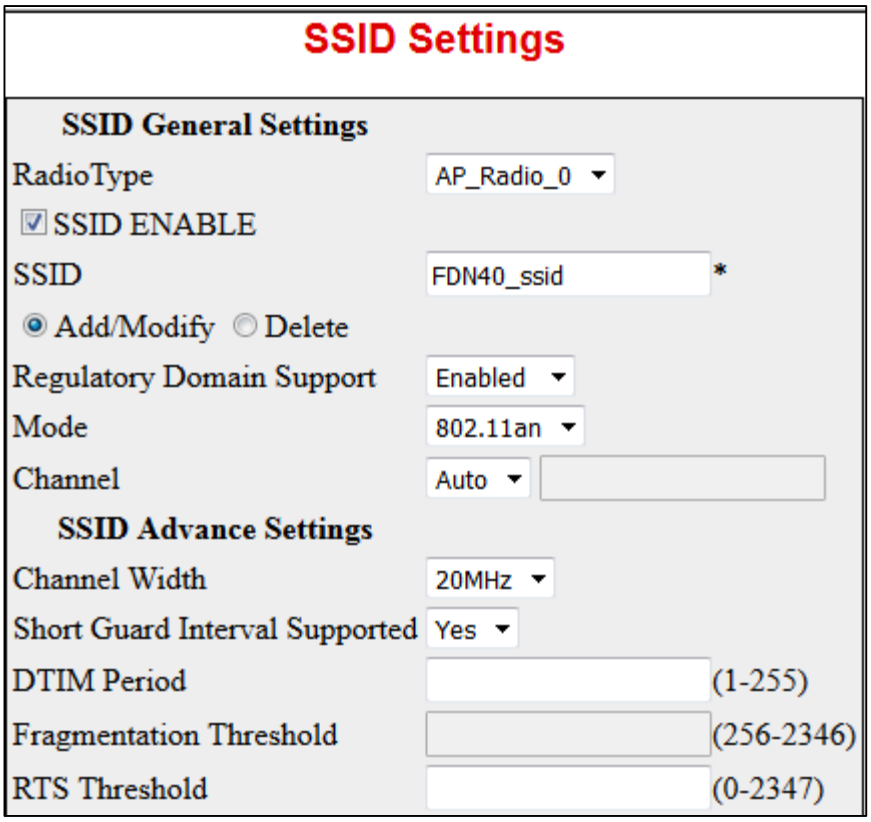
```
Channel :36
Channel Width :Default
Short Guard :Yes
TxPower :17
Security Mode :Open
WMM UAPSD :Enabled
```

12.3.3.2 WEB Configuration

There is an operation mode in which the signals in the 3 chains are not correlated, i.e. the equipment will always have spatial multiplexing across 3 physically independent RF paths.

12.3.3.2.1 VAP (SSID) Creation

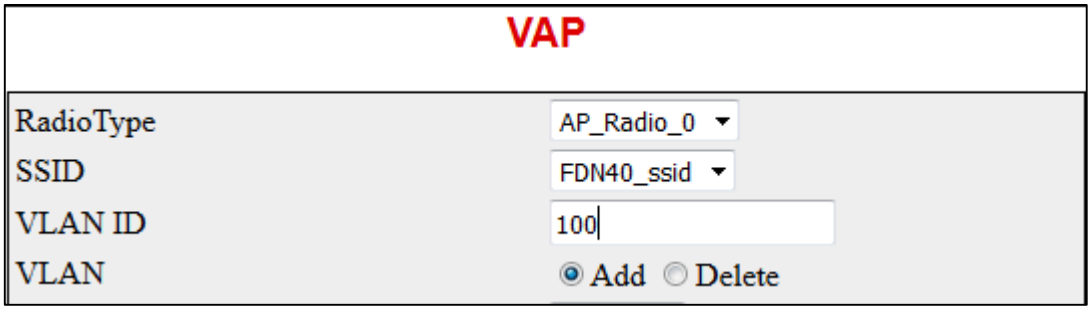
VAP can be created through WEB interface using the **AP Radio Setings** screen (Navigation - **Home-> Access Point-> Radio Settings).** To configure ssid in radio1 interface, Select **AP_Radio_1** in "**RadioType**" tab.



Screen 12-3: AP RadioSettings - Creating VAP (SSID)

12.3.3.2.2 VLAN Association with VAP

VLAN can be associated with VAP through WEB interface using the **VAP** screen (Navigation - **Home-> Access Point-> VAP>Security).** Selec the Radio Type and the corresponding SSIDs are displayed in SSID tab.



Screen 12-4: VAP

12.3.3.2.3 SSID Summary

VAP configurations can be viewed through web interface using the **SSID Summary** screen (Navigation - **Home-> Access Point-> Radio Settings->SSID Summary)**

Screen 12-5: SSID Summary

12.3.4 VAP deletion

12.3.4.1 CLI Configuration

1. Execute the following commands to delete a virtual access point (VAP) on the target.
   - Enter the Global Configuration Mode.

     UltOs# configure terminal
   - Specify the radio interface.

     UltOs(config)# apradio radio0
   - Disable the radio interface before removing a VAP .

     UltOs(config-apradio0)# shutdown
   - Delete the VAP .

     UltOs(config-apradio0)# no ssid *FDN40_ssid*
   - Exit the WiFi configuration Mode. .

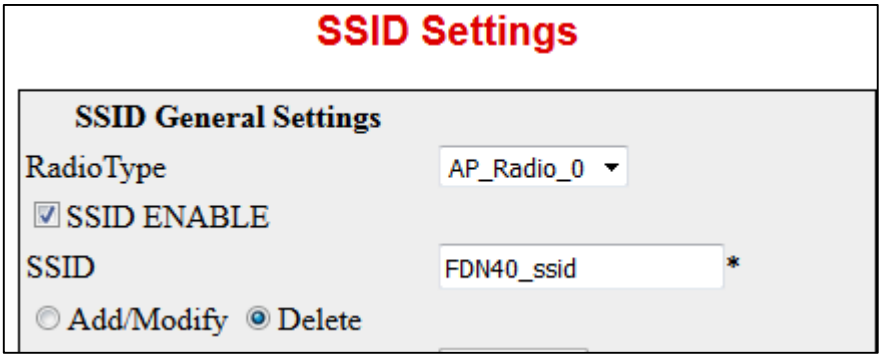
     UltOs(config-apradio0)# exit
   - Exit the global configuration Mode .

     UltOs(config)# exit
   - View in the below command to ensure the VAP is deleted..

UltOs# show apradio radio0 ssid summary

12.3.4.2 WEB Configuration

VAP can be deleted through WEB interface using the **AP Radio Setings** screen (Navigation - **Home-> Access Point-> Radio Settings)**



Screen 12-6: AP RadioSettings - Deleting VAP (SSID)

12.3.5 Rate-limit Configurations

12.3.5.1 CLI Configurations

1. Execute the following commands to configure Rate-limiting configurations on the target.
   - Enter the Global Configuration Mode.

     UltOs# configure terminal
   - Specify the radio interface.

     UltOs(config)# apradio radio1
   - Rate-limit configurations can be applied for interface or for the desired Station.Rate-limit for the interface can be done as :

     UltOs(config-apradio1)# rate-limit interface Cir *1* **Cbs** *1* **Eir** *5000* **Ebs** *8000000* **Coupling-Flag** *enable*
   - Exit the configuration Mode.

     UltOs(config-apradio1)# end
2. View the Rate-limit configurations for the interface.

   UltOs# show apradio radio1 interfacerate-limit

```
CIR           EIR             CBS             EBS
C-Flag          RowStatus

---           ---             ---             ---
------          ---------

1             5000            1               8000000
Enabled         Active
```

3. Rate-limit configurations can be disabled in the WiFi configuration mode.

   UltOs(config-apradio1)# no rate-limit interface
4. Execute the show command to ensure if the Rate-limit configurations are deleted.

UltOs# show apradio radio1 interface rate-limit

5. Rate-limit configurations can be applied for a desired Station .

   UltOs(config-apradio1)# rate-limit station 00:00:00:00:00:01 Cir 1 Cbs 1 eir 5000 ebs 90000 Coupling-Flag Enable

   – Exit the WiFi configuration Mode

   UltOs(config-apradio)# end

6. View the Rate-limit configurations for the station.

   UltOs# show apradio rate-limit

```
Station-Mac   CIR             EIR             CBS
EBS             C-Flag          RowStatus

-----------   ---             ---             ---
---             ------          ---------

00:00:00:00:00:01   1             5000          1
90000        Enabled      Active
```

7. Rate-limit configuration for the station can be removed.

   UltOs(config-apradio1)# no rate-limit station 00:00:00:00:00:01

   – Exit the Wi-Fi configuration Mode.

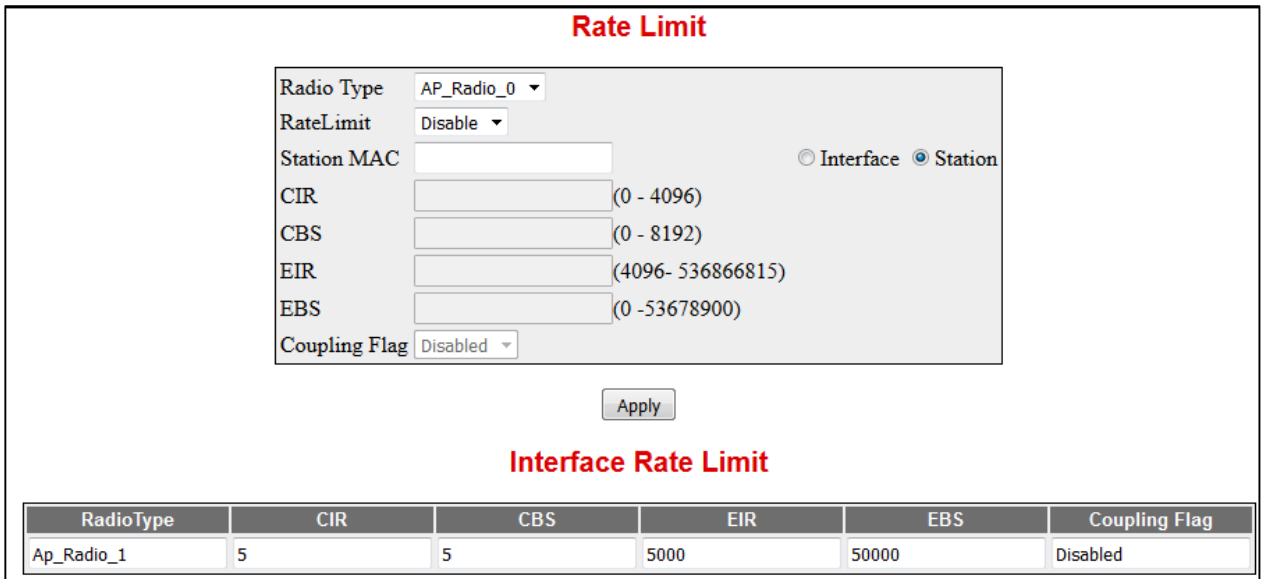
   UltOs(config-apradio1)# end

8. View the Rate-limit configurations for the station.

   UltOs# show apradio rate-limit

12.3.5.2 WEB Configuration

Rate Limit can be configured through WEB interface using the **Rate Limit** screen (Navigation - **Home-> Access Point-> VAP>Rate Limit)**



Screen 12-7: Rate Limit

12.3.6 Configuring Mac-Filtering for VAP

12.3.6.1 CLI Configuration

Execute the following commands to configure Mac-based Filtering in the AP.

1. Enter the VAP configuration Mode for the desired VAP for which the Mac based filtering of stations need to be done.

   UltOs(config-apradio0)# ssid FDN40_ssid

2. Enable Mac based Filtering Mode.

   UltOs(config-ssid)# mac-auth enable

3. Configure the MAC addresses that needs to be allowed in this VAP.Maximum of 32 Mac address can be added beyond which Error will be thrown.

   UltOs(config-ssid)# mac-address *00:00:00:00:00:01*

   UltOs(config-ssid)# mac-address *00:00:00:00:00:02*

   UltOs(config-ssid)# mac-address *00:00:00:00:00:03*

   UltOs(config-ssid)# mac-address *00:00:00:00:00:04*

4. Exit the WiFi configuration Mode

   UltOs(config-ssid)# end

5. View the configurations for the "ALLOWED" stations for the VAP using the following command.

   UltOs# show apradio radio0 stations mac-restricted

```
SSID              Status         Station-Mac
----              ------         -----------
FDN40_ssid         Enabled        00:00:00:00:00:01
FDN40_ssid         Enabled        00:00:00:00:00:02
FDN40_ssid         Enabled        00:00:00:00:00:03
FDN40_ssid         Enabled        00:00:00:00:00:04
```

Mac -addresses can also be removed from the "LIST" for the VAP.

6. Enter the Wi-Fi Configuration Mode and the desired VAP mode.

   UltOs(config-apradio0)# ssid FDN40_ssid

7. Mac-address can be removed from the MAC-filtering list for the VAP.

   UltOs(config-ssid)# no mac-address *00:00:00:00:00:02*

8. Exit the WiFi configuration Mode

   UltOs(config-ssid)# end

9. View the configurations for the "ALLOWED" stations for the VAP using the following command.

   UltOs# show apradio radio0 stations mac-restricted

```
SSID       Status         Station-Mac
----       ------         -----------
FDN40_ssid  Enabled        00:00:00:00:00:01
FDN40_ssid  Enabled        00:00:00:00:00:03
```

```
FDN40_ssid  Enabled        00:00:00:00:00:04
```

10. The Mac- based Filtering Mode can be disabled that would eventually remove the LIST configured for the VAP.

    UltOs(config-ssid)# mac-auth disable

    UltOs(config-ssid)# end

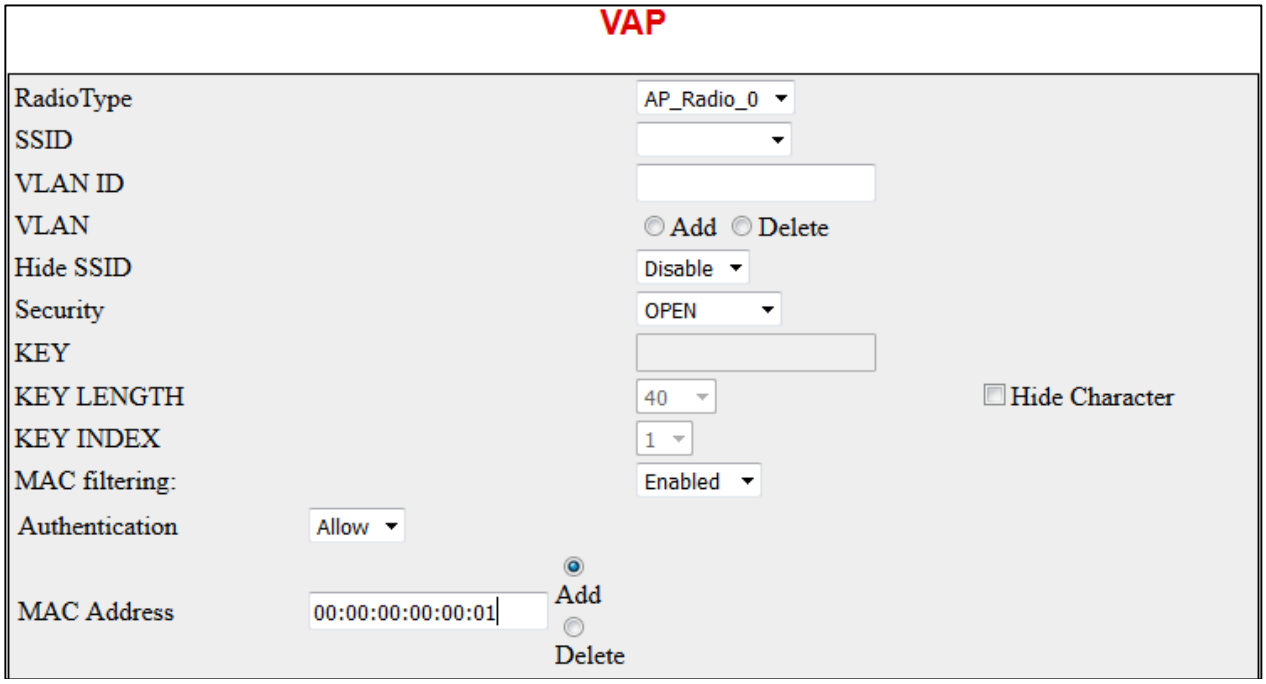
11. -Exit the global configuration Mode and View the Mac-filtered List for the AP.

    UltOs# show apradio radio0 stations mac-restricted

```
SSID      Status          Station-Mac
```

12.3.6.2 WEB Configuration

Mac filtering can be configured through WEB interface using the **VAP** screen (Navigation - **Home-> Access Point-> VAP>Security)**



Screen 12-8: VAP - MAC Filtering

12.3.7 Configuring Authentication Algorithms for VAP

12.3.7.1 CLI Configuration

12.3.7.1.1 Open Authentication

By default , VAP is configured in the "OPEN" Authentication mode.

UltOs# show apradio radio1 ssid summary

```
SSID : FDN40_ssid
BeaconPeriod :100
DTIM Period :1
```

```
Regulatory Domain:Yes
Rate :216700000
RTS threshold :2347
Fragmentation Threshold :2346
Vlan :100
Country :US
Radiomode :802.11ng
Channel :36
Channel Width :Default
Short Guard :Yes
TxPower :17
Security Mode :Open
```

When other algorithms are configured, "OPEN" can be configured using the following command.

UltOs(config-ssid)# security auth open

12.3.7.1.2 WEP Authentication

WEP configurations can be done with the Key size as 40 or 104 bits and the Key index can be one of the four index. :

UltOs(config-ssid)# security static-wep-key encryption key40 ascii hello 1

UltOs(config-ssid)# end

WEP configuration for the VAP is displayed in the display command.

UltOs# show apradio radio1 ssid summary

```
SSID : FDN40_ssid
BeaconPeriod :100
DTIM Period :1
Regulatory Domain:Yes
Rate :0
RTS threshold :2347
Fragmentation Threshold :2346
Vlan :100
Country :US
Radiomode :802.11ng
Channel :36
Channel Width :Default
Short Guard :Yes
TxPower :17
Security Mode :WEP
```

12.3.7.1.3 WPA2 PSK AUTHENTICATION

WPA2 PSK Key size must be 8 to 63 characters length The command is

UltOs(config-ssid)# security wpa2-psk-key encryption 8 password 1

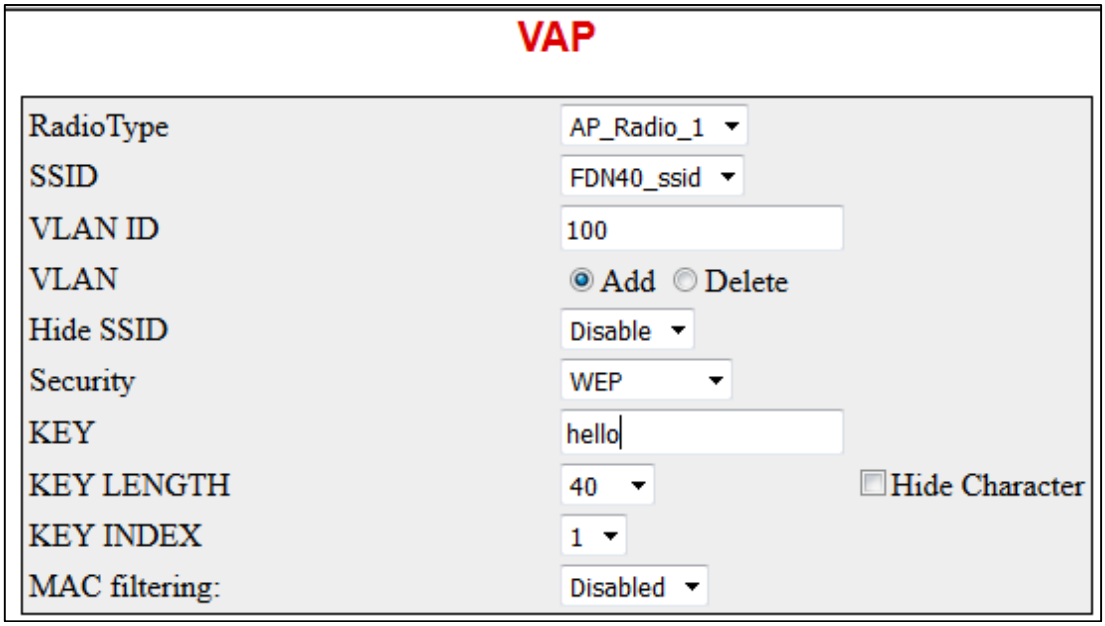
WPA2 PSK Configurations for the VAP interface is displayed as below:

UltOs# show apradio radio1 ssid summary

```
SSID : FDN40_ssid
BeaconPeriod :100
DTIM Period :1
Regulatory Domain:Yes
Rate :216700000
RTS threshold :2347
Fragmentation Threshold :2346
Vlan :100
Country :US
Radiomode :802.11ng
Channel :36
Channel Width :Default
Short Guard :Yes
TxPower :17
Security Mode :WPA2-PSK
```

12.3.7.2 WEB Configuration

Authentication Algorithms can be configured through WEB interface using the **VAP** screen (Navigation - **Home-> Access Point-> VAP>Security)**



Screen 12-9: VAP – Authentication with WEP

12.4 Displaying the Configurations

1. . View the Default configurations for the created VAP in the VAP summary table

UltOs# show apradio {radio0 | radio1} ssid summary

```
SSID : FDN40_ssid
BeaconPeriod :100
DTIM Period :1
Regulatory Domain:Yes
Rate :216700000
RTS threshold :2347
Fragmentation Threshold :2346
Vlan :100
Country :US
Radiomode :802.11an
Channel :36
Channel Width :Default
Short Guard :Yes
TxPower :17
Security Mode :Open
```

2. . View the QOS EDCA Parameters for the AP

UltOs# show apradio {radio0 | radio1}edca params

```
SSID      Queue-Index  CWmin    CWmax          AIFS
```

```
-------- -----------  -----    -----          ----

: FDN40_ssid      0      4          6
3
: FDN40_ssid       1     4         10             7
: FDN40_ssid       2     3         4              1
: FDN40_ssid       3     2        3              1
```

3. The "ALLOWED" stations for the VAP are displayed using the following command.

   UltOs# show apradio {radio0 | radio1} stations mac-restricted

```
SSID          Status         Station-Mac

----          ------         -----------

FDN40_ssid      Enabled        00:00:00:00:00:01

FDN40_ssid      Enabled        00:00:00:00:00:03

FDN40_ssid     Enabled        00:00:00:00:00:04
```

4. Rate -limit Show commands for Interface configuration:

   UltOs# show apradio {radio0 | radio1} interface rate-limit

```
CIR           EIR            CBS            EBS
C-Flag          RowStatus

---           ---            ---            ---
------          ---------

1             5000           1              8000000
Enabled         Active
```

5. Rate-limit station configurations are displayed in the below command:

   UltOs# show apradio {radio0 | radio1} rate-limit

```
Station-Mac  CIR            EIR            CBS
EBS            C-Flag         RowStatus

-----------  ---            ---            ---
---            ------         ---------

00:00:00:00:00:01   1           5000        1
90000       Enabled     Active
```

6. Display for the connected stations to the Access Point

   UltOs# show apradio {radio0 | radio1} connected-stations statistics

```
SSID :FDN40_ssid :: Clients connected : 1

BSSID Mac :04:f0:21:09:04:b1

Assoc UpTime (seconds) :12

Tx Packets :0

Drop -AuthFail :0

Drop- Assoc Fail :0

Rx Packets :0

Station Mac :c0:4a:00:14:44:aa
```

```
Ip Address: 100.0.0.30
Total number of Clients connected :1
```

12.5 Wi-Fi Client Association

12.5.1 CLI Configuration

For a successful association of AP to a Wireless Client, following configurations need to be done in the AP

1. Create a radio1 interface and associate with a VLAN(For radio0 configure with radio0):

   UltOs(config)# apradio radio1

   UltOs(config-apradio1)# no shutdown

   UltOs(config-apradio1)#

   UltOs(config-apradio1)# ssid ZEUS_ssid

   UltOs(config-ssid1)#

   UltOs(config-ssid1)#

   UltOs(config-ssid1)# end

   UltOs#

   UltOs# c t

   UltOs(config)# apradio radio1

   UltOs(config-apradio1)# ssid ZEUS_ssid

   UltOs(config-ssid)# vlan 100

   UltOs(config-ssid)# end

   UltOs# c t

2. Configure a dhcp pool to enable IP address allocation for the Wireless Client

   UltOs(config)# service dhcp-server

   UltOs(config)# ip dhcp pool 1

   UltOs(dhcp-config)# network 100.0.0.30 255.255.255.0 100.0.0.50

   UltOs(dhcp-config)# exit

   UltOs(config)# exit

   UltOs# c t

3. IVR configurations are done to observe switching and routing behavior

   UltOs(config)# int vlan 100

   UltOs(config-if)# ip address 100.0.0.1 255.255.255.0

   UltOs(config-if)# no shutdown

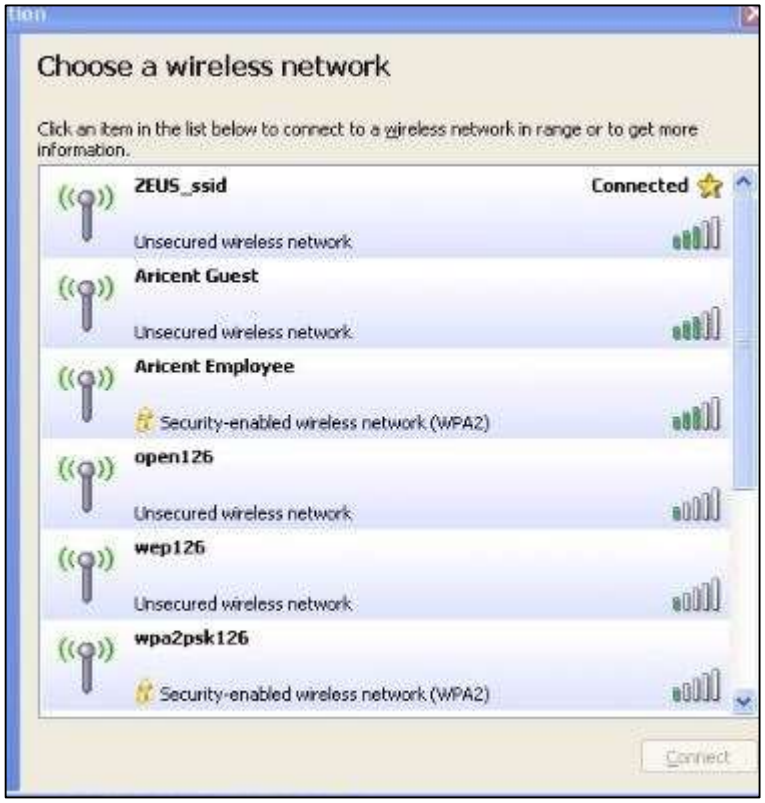
   UltOs(config-if)# end

   UltOs#

4. - Disable Firewall configurations

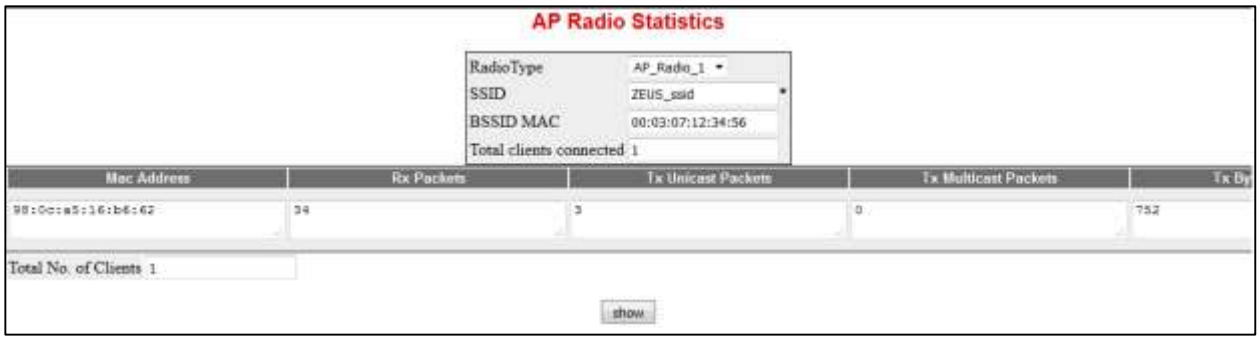
UltOs# c t ; firewall ; disable ; exit ; exit ;

5. **-** Now, the wireless clients can connect to the AP



12.5.2 WEB Configuration

Connection Statistics can be viewed through WEB interface using the **AP Radio Statistics** screen (Navigation - **Home-> Statistics-> ApRadio).** Select the RadioType and provide the SSID Name.



Screen 12-10: AP Radio Statistics

Chapter 13

NTP

13.1 Protocol Description

Network Time Protocol (NTP) message to one or more servers and processes the replies as received. The server interchanges addresses and ports, fills in or overwrites certain fields in the message, recalculates the checksum and returns it immediately. Information included in the NTP message allows each client/server peer to determine the timekeeping characteristics of its other peers, including the expected accuracies of their clocks. Using this information each peer is able to select the best time from possibly several other clocks, update the local clock and estimate its accuracy.

In FDN40, system time is synchronized using NTP daemon (ntpd). ntpd is an operating system daemon which sets and maintains the system time of day in synchronism with Internet standard time servers. It is a complete implementation of the Network Time Protocol. FDN40 will use open source NTP code for NTP functionality. There will be a separate process running for controlling the ntpd daemon.

This process will be responsible for managing the ntpd daemon and sending trap messages to process if NTP server is not reachable.

That way, if the daemon is stopped and restarted, it can reinitialize itself to the previous estimate without spending time re computing the frequency estimate.

ntpd can operate in any of several modes, including symmetric active/passive, client/server broadcast/multicast and manycast.

FDN40 release 1.0 supports only NTP client configuration with maximum of 2 NTP servers for time synchronization. No modification or customization will be done on open source NTP.

13.2 Topology

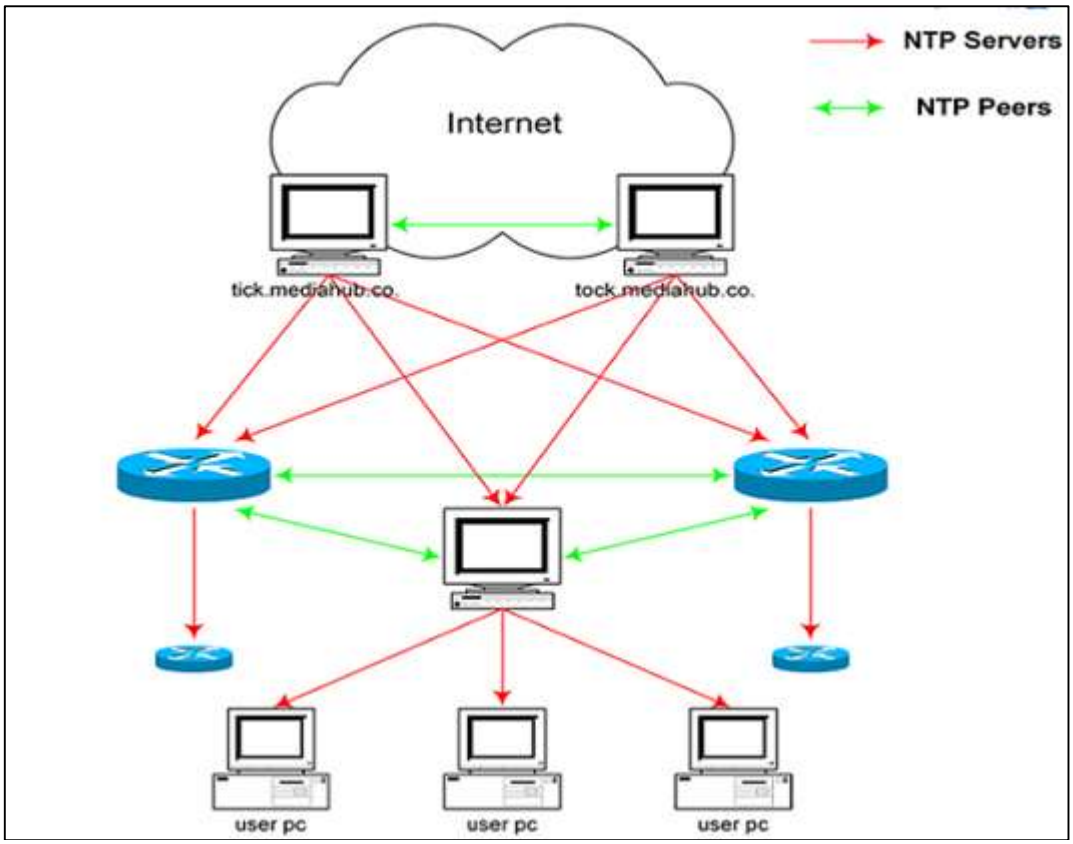


Figure 13-1: NTP Topology

13.3 Configuration Guidelines

The FDN40 CLI user manual can be referred for the complete set of commands and the various options available for configuring NTP.

13.4 Default Configurations

Table 13-2: Default Configurations

Parameter	Default Setting
System Control	Start
NTP mode	Disable
NTP Client mode	Disabled
Default Server IP	0.0.0.0
Default Min Polltime	6

13.5 NTP Configurations

13.5.1 Configuring NTP system

13.5.1.1 Enabling the NTP system

1. Execute the following commands to enable NTP on the target.

   Enabling the NTP module is a two step configuration

   First enable NTP mode and then enabling client mode and further user configuration of server and polltime

   – Enter the Global Configuration Mode.

     UltOs# configure terminal

   – Enter NTP config mode.

     UltOs(config)# ntp

   – Enable NTP mode

     UltOs(config-ntp)# set ntp enable

   – Enable NTP client mode unicast

     set ntp client mode {unicast | multicast | disabled}

     UltOs(config-ntp)# set ntp client mode unicast

   – User can now configure IP and polltime in unicast mode

     UltOs(config-ntp)# exit

2. View the NTP related global information.

   UltOs# show ntp mode

   ```
   NTP SERVICE ENABLE CONFIGURATION:
   NTP SERVICE ENABLE : ENABLED
   ```

   UltOs# show ntp client mode

   ```
   NTP SERVCIE CONFIGURATION INFORMATION:
   NTP CLIENT MODE : UNICAST
   ```

   UltOs# show ntp server

   ```
   NTP SERVER INFO :
   Server Address: 172.30.19.172
   Polltime: 6
   NTP SERVER INFO :
   Server Address: 172.30.19.123
   Polltime: 6
   ```

13.5.1.2 Disabling the NTP system

1. Execute the following commands to disable NTP on the target.

   – Enter the Global Configuration Mode.

     UltOs# configure terminal

- Enter the NTP config mode

  UltOs(config)# ntp

- Disable the NTP client mode

  UltOs(config-ntp)# set ntp client mode disable

- Disable the NTP mode

  UltOs(config-ntp)# set ntp disable

2. View the NTP related global information.

   UltOs# show ntp mode

```
NTP SERVICE ENABLE CONFIGURATION:
NTP SERVICE ENABLE :    DISABLED
```

   UltOs# show ntp client mode

```
NTP SERVCIE CONFIGURATION INFORMATION:
NTP CLIENT MODE : DISABLED
```

13.5.1.3 Configuring the NTP Client Mode

1. Execute the following commands to configure NTP client mode on the target.

   - Enter the Global Configuration Mode.

     UltOs# configure terminal

   - Enter NTP config mode.

     UltOs(config)# ntp

   - Enable NTP mode

     UltOs(config-ntp)# set ntp {enable | disable}

   - Enable NTP client mode unicast

     UltOs(config-ntp)# set ntp client mode unicast

2. View the NTP client mode related global information UNICAST MODE

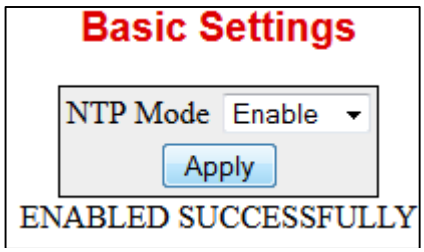
   UltOs# show ntp client mode

```
NTP SERVCIE CONFIGURATION INFORMATION:
NTP CLIENT MODE : UNICAST
```

13.5.1.4 2.WEB Configuration

13.5.1.4.1 Enabling/ Disabling NTP

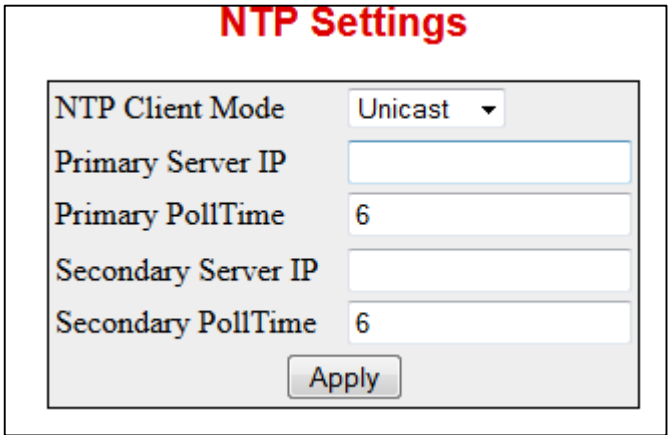
NTP can be enabled/disabled can be viewed through WEB interface using the **Basic Settings** screen (Navigation - **Home-> NTP-> Basic Settings)**



Screen 13-1: NTP Basic Settings

13.5.1.4.2 Configuring NTP Client Mode

NTP Client Mode can be configured through WEB interface using the **NTP Settings** screen (Navigation - **Home-> NTP-> NTP Settings)**



Screen 13-2: NTP Client Mode

13.5.2 Configuring NTP Server

13.5.2.1 CLI Configuration

To Configure NTP Server IP and Polltime the below steps to be followed:

1. Configure NTP Server with Server IP and Polltime (UNICAST MODE)

   UltOs# configure terminal

   UltOs(config)# ntp

   UltOs(config-if)# set ntp enable

   UltOs(config-if)# set ntp client mode unicast

   UltOs(config-if)# set ntp server 1 172.30.19.152 10

   UltOs(config-if)# exit

2. Configure NTP Server IP for any one index (UNICAST MODE)

   UltOs# configure terminal

   UltOs(config)# ntp

   UltOs(config-if)# set ntp enable

   UltOs(config-if)# set ntp client mode unicast

UltOs(config-if)# set ntp server ip 1 172.30.19.152

UltOs(config-if)# exit

3. Configure both the NTP Server IPs. (UNICAST MODE)

   UltOs# configure terminal

   UltOs(config)# ntp

   UltOs(config-if)# set ntp enable

   UltOs(config-if)# set ntp client mode unicast

   UltOs(config-if)# set ntp server ips 172.30.19.152 172.30.19.153

   UltOs(config-if)# exit

4. Configure both the NTP Server Polltime for any one index(UNICAST MODE)

   UltOs# configure terminal

   UltOs(config)# ntp

   UltOs(config-if)# set ntp enable

   UltOs(config-if)# set ntp client mode unicast

   UltOs(config-if)# set ntp server polling 1 10

   UltOs(config-if)# exit

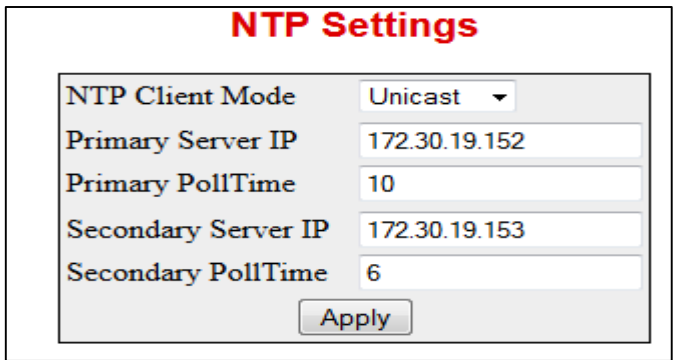
5. View the configuration by executing the show command as mentioned below.

   UltOs# show ntp server

```
NTP SERVER INFO :
Server Address: 172.30.19.152
Polltime: 10
NTP SERVER INFO :
Server Address: 172.30.19.153
Polltime: 6
```

13.5.2.2 Web Configuration

NTP server can be configured through WEB interface using the **NTP Settings** screen (Navigation - **Home-> NTP-> NTP Settings)**



CLIENT MODE	PRIMARY SERVER IP	PRIMARY POLLTIME	SECONDARY SERVER IP	SECONDARY POLLTIME
UNICAST	172.30.19.152	10	172.30.19.153	6

Screen 13-3: NTP Server Configurations

Chapter 14

QOS

14.1 Protocol Description

QoS (Quality of Service) defines the ability to provide different priorities to different applications, users or data flows or the ability to guarantee a certain level of performance to a data flow. QoS at layer 2 involves 802.1p support. QoS also includes support for DiffServ (Differentiated services). This includes the flow based on specific rate limits, scheduling and shaping.

QoS supports 802.1p for mapping VLAN priority to traffic class/queues. It also supports DiffServ features which include scheduling and shaping based on the features supported by the switching silicon used. The realization of QoS is done using the QoSx module on the platforms based on AXM.

14.2 Topology

Figure 14-1: QOS Topology

Table 14-1: QOS Topology Description

Switch / Host	Interface of FDN40 Switches	IPv4 Address / Mask
FDN40-1	VLAN 1	12.0.0.1/255.0.0.0

14.3 Configuration Guidelines

The FDN40 CLI user manual can be referred for the complete set of commands and the various options available for configuring QoS.

14.4 Default Configurations

Table 14-2: Default Configurations

Parameter	Default Setting
System Control	Start
System Control	Enable
Rate Unit	kbps
Rate Granularity	64
Trace Flag	0

14.5 QoS Configurations

14.5.1 Configuring QoS Subsystem

14.5.1.1 Enabling the QoS Subsystem

1. Execute the following commands to enable QoS on the target.

   Enabling the QoS module programs the hardware and starts protocol operation.

   – Enter the Global Configuration Mode.

     UltOs# configure terminal

   – Enable the QoS.

     UltOs(config)# qos enable

   – Exit theGlobal Configuration Mode.

     UltOs(config)# exit

2 View the QoS related global information.

UltOs# show qos global info

```
QoS Global Information
----------------------
System Control : Start
System Control : Enable
Rate Unit : kbps
Rate Granularity : 64
Trace Flag : 0
```

14.5.1.2 Disabling the QoS Subsystem

1. Execute the following commands to disable QoS on the target.

   Disabling the QoS module stops the protocol operation by deleting the hardware configuration.

   – Enter the Global Configuration Mode.

     UltOs# configure terminal

   – Disable the QoS.

     UltOs(config)# qos disable

     UltOs(config)# exit

2. View the QoS related global information.

   UltOs# show qos global info

```
QoS Global Information
----------------------
System Control : Start
System Control : Disable
Rate Unit : kbps
Rate Granularity : 64
Trace Flag : 0
```

14.5.1.3 Making the QoS Subsystem Up

1. Execute the following commands to make the QoS subsystem up.

   When QoS subsystem is set as start, resources required by the QoS module are allocated and QoS module starts running.

   – Enter the global configuration mode.

     UltOs# configure terminal

   – Make the QoS subsystem up.

     UltOs(config)# no shutdown qos

     UltOs(config)# exit

2 View the QoS related global information.

   UltOs# show qos global info

```
QoS Global Information
----------------------
System Control : Start
System Control : Disable
Rate Unit : kbps
Rate Granularity : 64
Trace Flag : 0
```

14.5.1.4 WEB Configuration

QoS can be enabled/ disabled through WEB interface using the **QoS Basic Settings** screen (Navigation - **System-> QoS-> QoSInGress-> Basic Settings)**

Screen 14-1: QoS Basic Settings

14.5.2 Configuring Rate-Limiting at Port level (Ingress port-rate limiting)

14.5.2.1 CLI Configuration

1. Ingress rate-limiting feature helps to rate limit the traffic ingressing on a port.

UltOs# configure terminal

UltOs(config)# interface *lan 0/1*

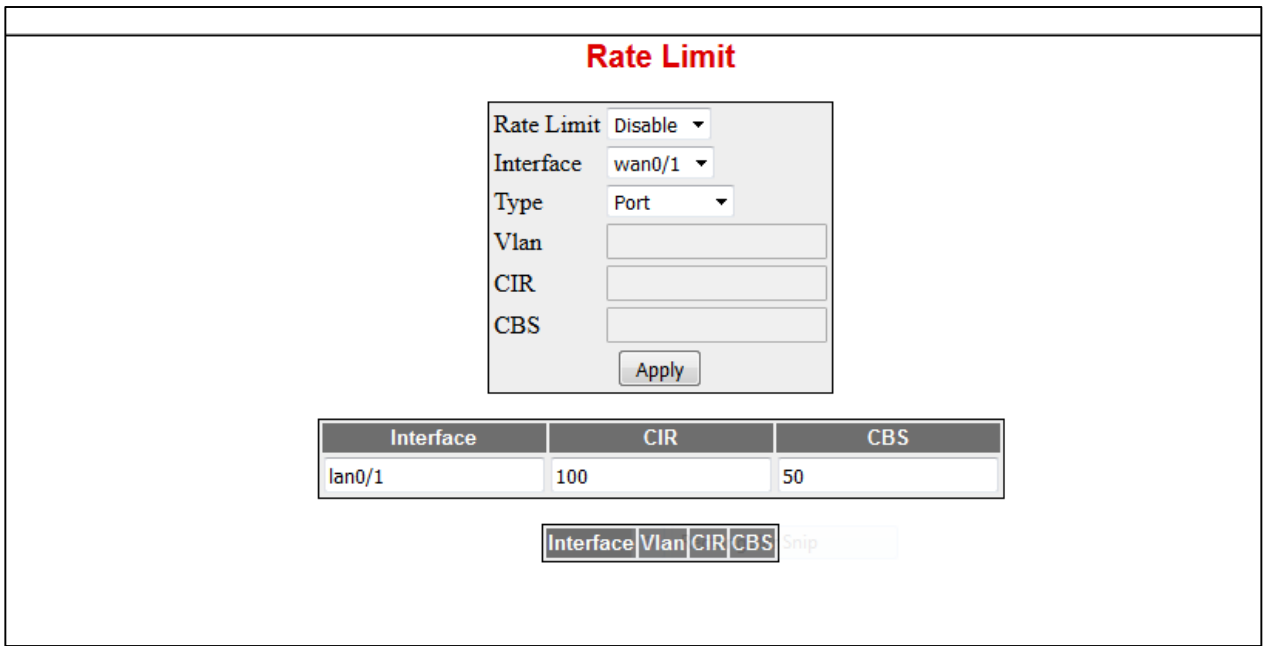
UltOs(config-if)# rate-limit cir 100 cbs 50

UltOs# show rate-limit

```
Vlan                CIR                 CBS
Mode

---------       -----------         ---
---             ----------

--

lan0/1          0                   100
50              ColorBlind
```

14.5.2.2 WEB Configuration

Rate limiting can be configured through WEB interface using the **Rate Limit** screen (Navigation – **System > Qos > QosIngress> Rate Limiting**)



Screen 14-2: Ingress Rate Limiting

Supporting on LAN and WAN ports.

14.5.3 Configuring Storm-Control at Port level (Ingress port-storm control)

14.5.3.1 CLI Configuration

1. Ingress storm control feature helps to control the traffics (DLF, Muliticast and Broadcast) ingressing on a port.

   UltOs# configure terminal

   Storm-Control on WAN ports.

   UltOs(config)# interface *wan 0/1*

   UltOs(config-if)# storm-control bc_dlf_mc cir 100 cbs 50

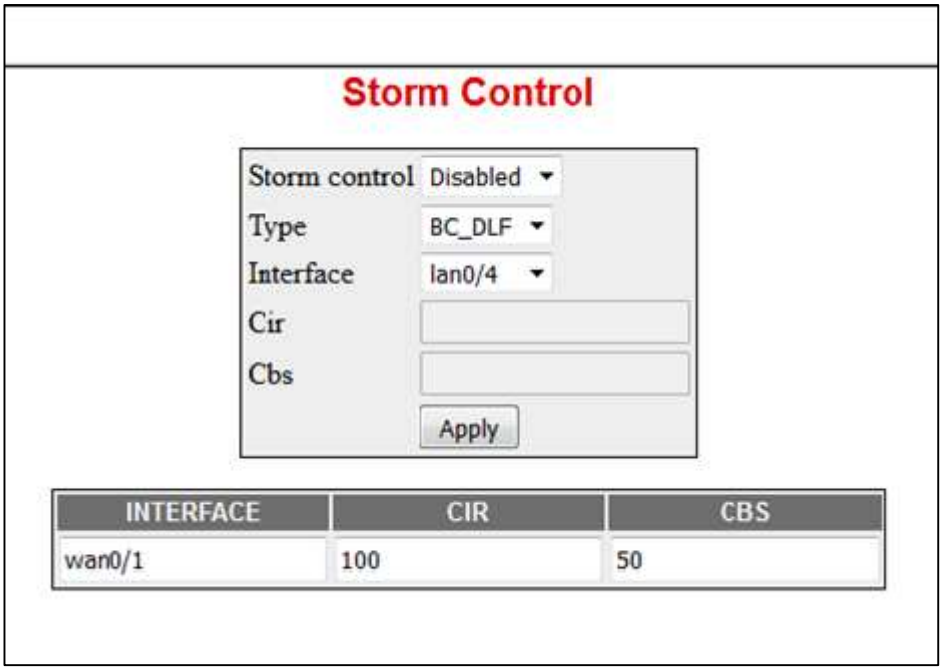
   UltOs(config-if)#exit

2. **UltOs# show storm-control**

```
Interface       CIR                 CBS
---------       ---                 ---
wan0/1          100                 50
```

14.5.3.2 WEB Configuration

Rate limiting can be configured through WEB interface using the **Storm Control** screen (Navigation - **System> Qos> QosIngress> Storm Control**)



Screen 14-3: Storm-Control

14.5.4 Configuring Per Queue Shaping (Egress per- port per- queue shaping)

14.5.4.1 CLI Configuration

1. Shaping can be done per queue by configuring the shape-template values and mapping it to the specific queue.

   UltOs# configure terminal

   UltOs(config)# shape-template 10 cir 100 cbs 50 eir 100 ebs 50

   UltOs(config)# queue *1* **interface** *wan 0/1* **shaper** *10*

   UltOs(config)# end

   Here, the shaper template is created with the value cir = 1000 Kbps.

   The shaper template is associated to the queue. Shaping of traffic on each queue depends on the values of shaper configured for each queue.

2. View the shaping configurations of the queues of an egress interface

   UltOs# show queue interface *wan 0/1*

```
QoS Queue Entries

-----------------

IfIndex  Queue  QTemplate  Scheduler  Weight  Priority
QType  ShapeIdx  GlobalId

-------  -----  ---------  ---------  ------  --------
-----  --------  --------

wan0/1    1        1            0            1         0
UC     10         1
```

```
wan0/1    2        1            0            1         1
UC      none       2

wan0/1    3        1            0            1         2
UC      none       3

wan0/1    4        1            0            1         3
UC      none       4

wan0/1    5        1            0            1         4
UC      none       5

wan0/1    6        1            0            1         5
UC      none       6

wan0/1    7        1            0            1         6
UC      none       7

wan0/1    8        1            0            1         7
UC      none       8
```

3. To disable shaping for a queue, the queue needs to be mapped to shaper 0.

   UltOs# configure terminal

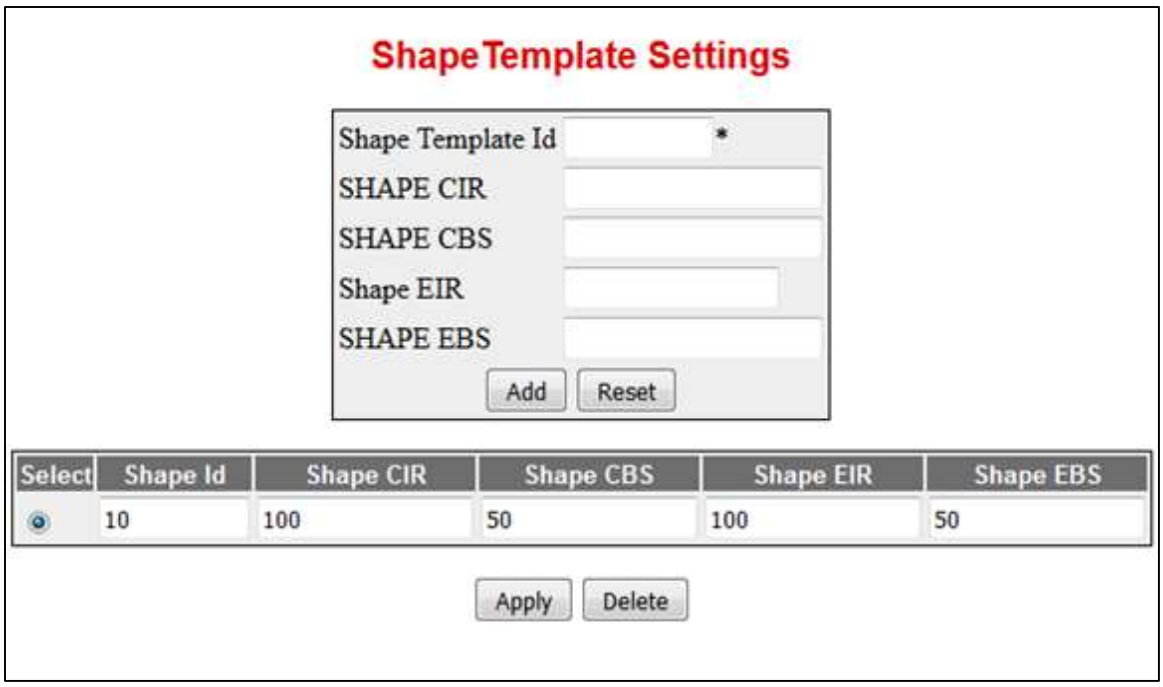
   UltOs(config)# queue *1* **interface** *wan 0/1* **shaper** *0*

   UltOs(config)# end

14.5.4.2 WEB Configuration

14.5.4.2.1 Shape Template

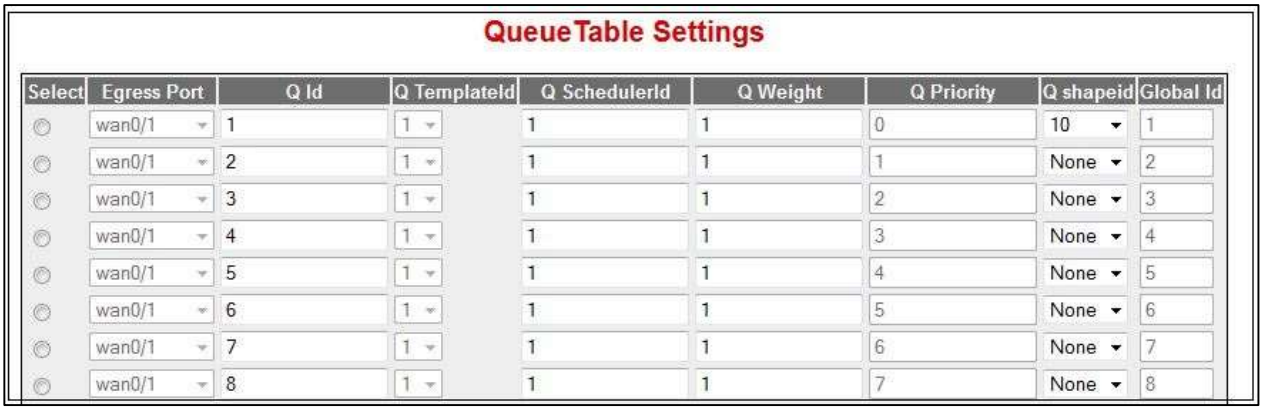
Shape Template can be configured through WEB interface using the **Shape Template Settings** screen (Navigation - **System-> QoS-> QoSEgress-> Shape Template**)



Screen 14-4: Shape Template Configurations

14.5.4.2.2 Queue Table

Queue Table can be configured through WEB interface using the **Queue Table Settings** screen (Navigation - **System-> QoS-> QoSEgress-> Queue Table**)



Screen 14-5: Queue Configurations

14.5.5 Configuring Queue Template

14.5.5.1 CLI Configuration

1. Tail Drop can be done per queue by configuring the queue-template values and mapping it to the specific queue.

   UltOs# configure terminal

   UltOs(config)# queue-type 2

UltOs(config -qtype)# set algo-type tailDrop queue-limit 1

UltOs(config)# end

UltOs(config)# queue *1* **interface** *wan 0/1* **qtype 2**

UltOs(config)# end

The queue template is associated to the queue.

2. View the queue template configurations of the queues of an egress interface

UltOs# show queue interface *wan 0/1*

```
Queue Template Entries
----------------------
Q Template Id                 : 1
Q Limit                       : 256
Drop Type                     : Tail Drop
Drop Algo Status              : Enable
```

3. To disable queue-template for a queue.

UltOs# configure terminal

UltOs(config)# no queue *1* **interface** *wan 0/1*

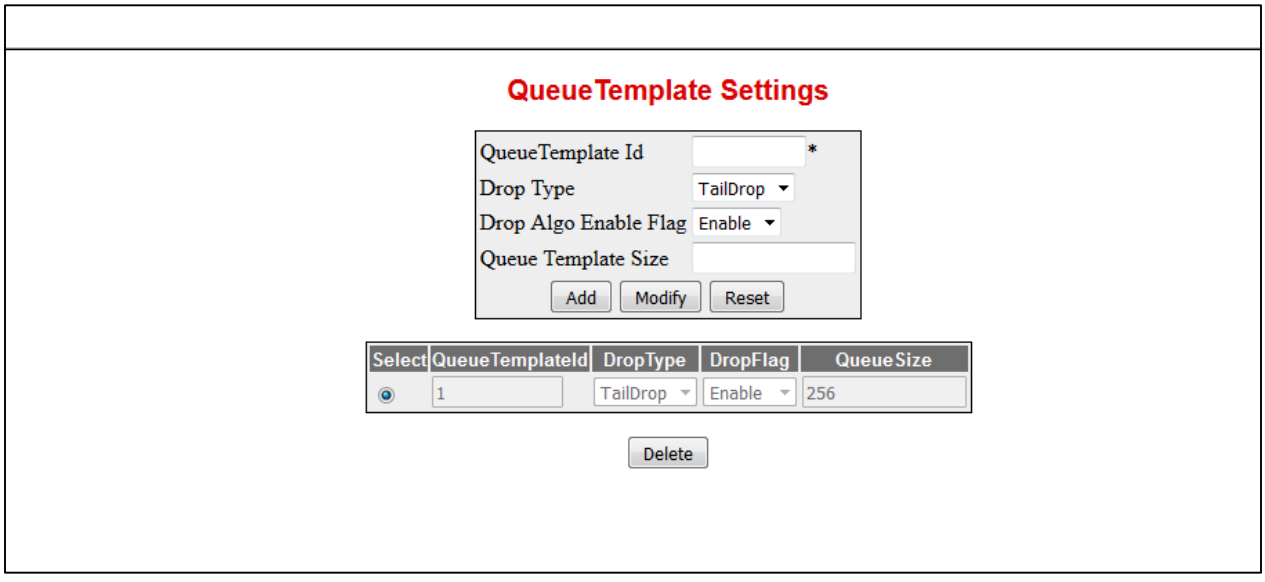
UltOs(config)# end

UltOs(config)#no queue-type 2

14.5.5.2 WEB Configuration

14.5.5.2.1 QueueTemplate

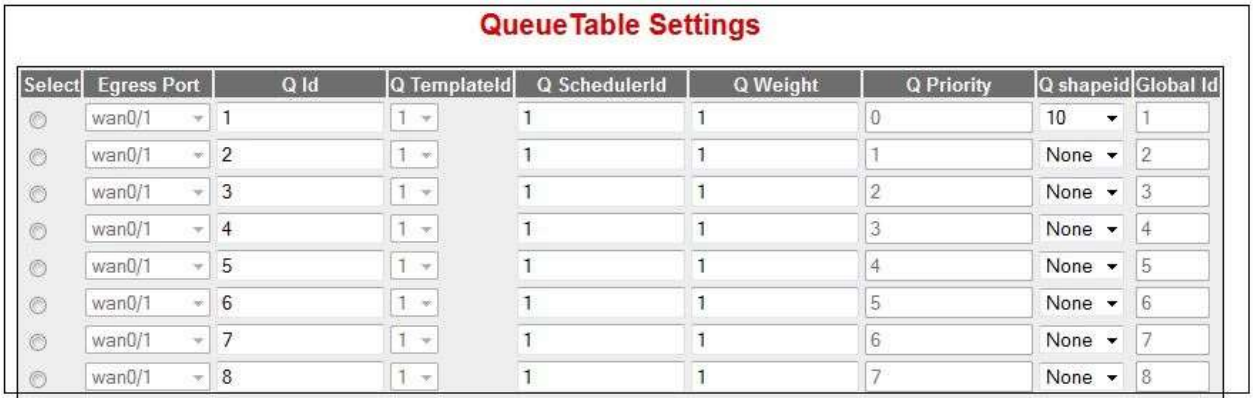
QueueTemplate can be configured through WEB interface using the Queue**Template Settings** screen (Navigation - **System-> QoS-> QoSEgress-> QueueTemplate**)



Screen 14-10: QueueTemplate Configurations

14.5.5.2.2 Queue Table

Queue Table can be configured through WEB interface using the **Queue Table Settings** screen (Navigation - **System-> QoS-> QoSEgress-> Queue Table**)



Screen 14-11: Queue Configurations

14.5.6 Configuring Queue Map

14.5.6.1 CLI Configuration

1. Queue Map can be done per queue by configuring the qmap values and mapping it to the specific queue.

   UltOs# configure terminal

   UltOs(config)# queue-map regn-priority vlanPri 0 interface lan 0/1 queue-id 1

   UltOs(config)# end

   The queue map is associated to the queue.
2. View the queue map configurations of the queues of an egress interface

   UltOs# show queue interface *lan 0/1*

```
Q Template Id                : 1

QoS Queue Map Entries

---------------------

IfIndex     CLASS       PriorityType     Priority Value
Mapped Queue

----------  ----------  ---------------  ---------------
---------------

lan0/1          none             VlanPri                 0
1
```

3. To disable queue-map for a queue.

   UltOs# configure terminal

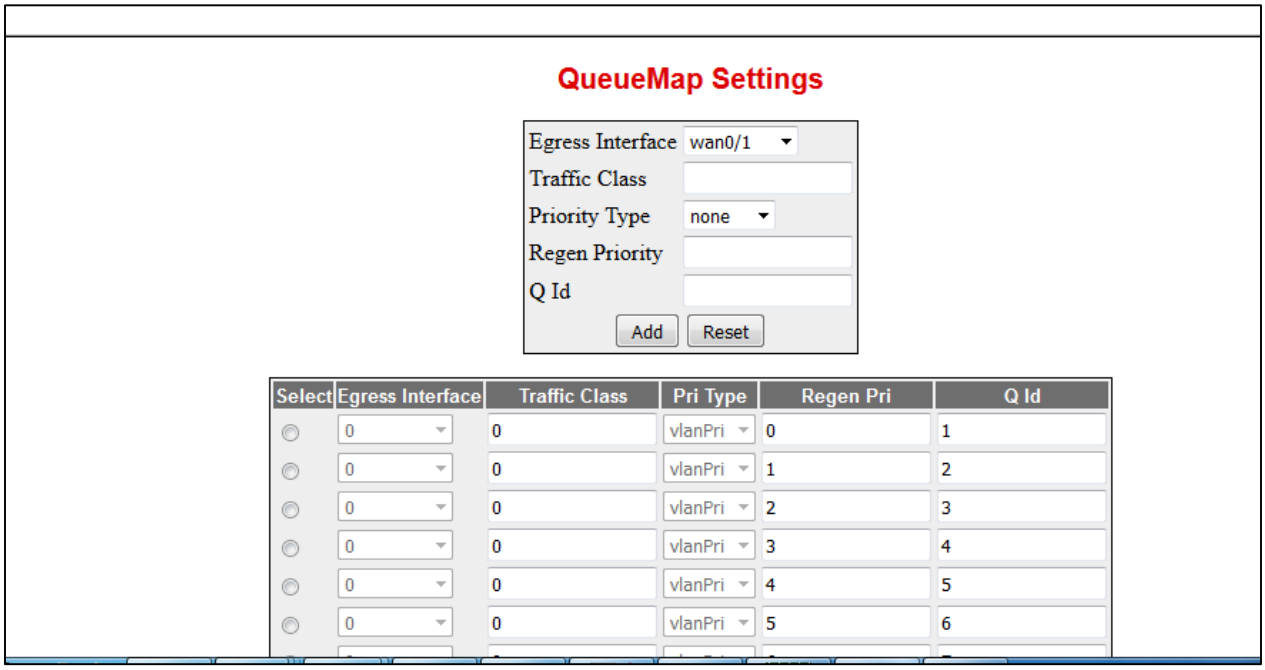
UltOs(config)# no queue-map regn-priority vlanPri 0 interface lan 0/1

UltOs(config)# end

14.5.6.2 WEB Configuration

14.5.6.2.1 QueueTemplate

Queue Map can be configured through WEB interface using the Queue Map screen (Navigation - **System-> QoS-> QoSEgress-> QMap**)



Screen 14-12: Queue Map Configurations

14.5.7 Configuring Scheduler

14.5.7.1 CLI Configuration

The supported scheduling algorithms are:

- Strict-Priority scheduling

1. Configure the scheduling algorithm

UltOs# configure terminal

UltOs(config)# scheduler interface wan 0/1 sched-algo strict-priority

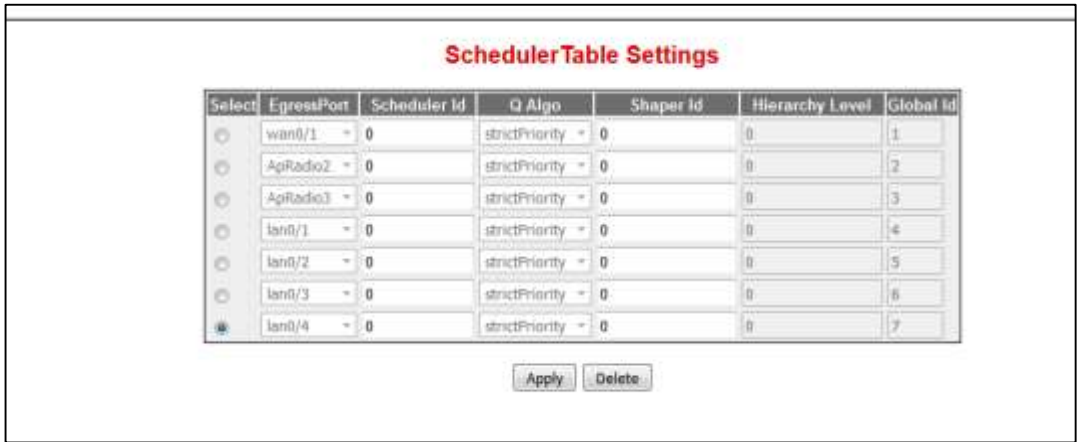
UltOs# show scheduler

```
QoS Scheduler Entries

---------------------

IfIndex     Scheduler Index Scheduler Algo        Shape
Index Scheduler HL  Global
```

```
Id
---------- --------------- -------------------- ------
----- ------------ -------
-----
wan0/1       0                   strictPriority         0
0             1

ApRadio2     0                   strictPriority         0
0             2

ApRadio3     0                   strictPriority         0
0             3

lan0/1       0                   strictPriority         0
0             4

lan0/2       0                   strictPriority         0
0             5

lan0/3       0                   strictPriority         0
0             6

lan0/4       0                   strictPriority         0
0             7
```

14.5.7.2 WEB Configuration

Scheduler Table can be configured through WEB interface using the **Scheduler Table Settings** screen (Navigation - **System-> QoS-> QoSEgress-> Scheduler Table**)



Screen 14-6: Scheduler Configurations

Schedulers are Pre-Created at ports.

Chapter 15

OSPF

15.1 Protocol Description

OSPF (Open Shortest Path First) protocol, is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on the topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links. In addition, it also sends the complete routing structure (topography).

The **OSPF** basic and advanced configuration tasks are described in the following section(s)

15.2 Topology

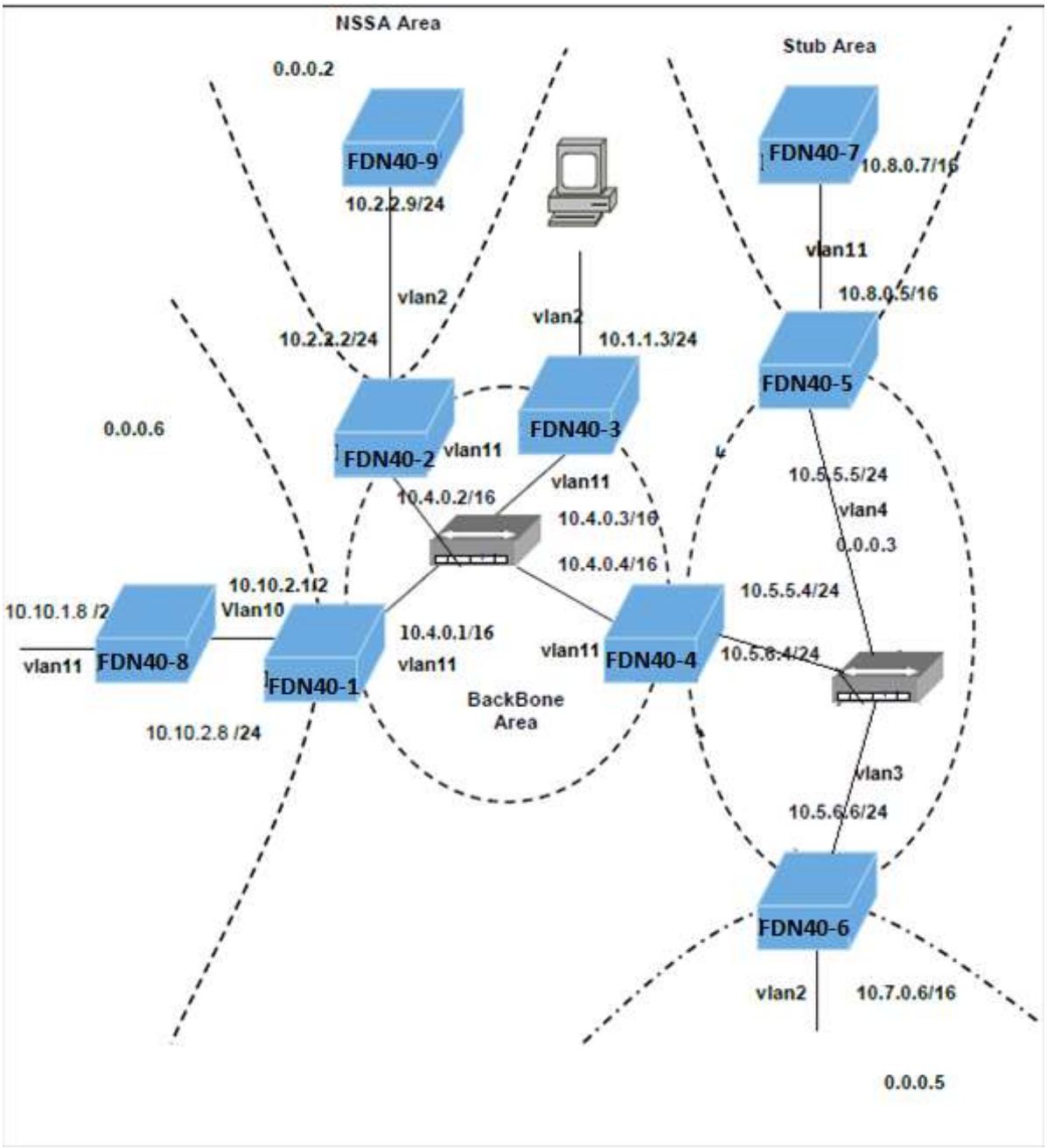


Figure 15-1: OSPF Topology

15.3 Configuration Guidelines

The following sections describe the configuration of **OSPF** running as a part of **ULTERIUS FDN40** product**.**

.This is a prerequisite for configuring the OSPF.

15.3.1 Configuration in FDN40-1

Prerequisite: Configuration of VLAN Interfaces (vlan11 and vlan10)

UltOs# configure terminal

UltOs(config)# vlan 11

UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*

UltOs(config-vlan)# exit

UltOs(config)# interface *vlan 11*

UltOs(config-if)# shut

UltOs(config-if)# ip address *10.4.0.1 255.255.0.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan *10*

UltOs(config-vlan)# ports *wan 0/2* **untagged** *wan 0/2*

UltOs(config-vlan)# exit

UltOs(config)# interface *vlan 10*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.10.2.1 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# interface *wan0/2*

UltOs(config-if)# switchport *pvid 10*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

15.3.2 Configuration in FDN40-2

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal

UltOs(config)# vlan 11

UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*

UltOs(config-vlan)# exit

UltOs(config)# interface vlan 11

UltOs(config-if)# shutdown
UltOs(config-if)# ip address *10.4.0.2 255.255.0.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# vlan *2*
UltOs(config-vlan)# ports *wan 0/2* **untagged** *wan 0/2*
UltOs(config-vlan)# exit
UltOs(config)# interface vlan *2*
UltOs(config-if)# ip address *10.2.2.2 255.255.255.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# interface *wan 0/2*
UltOs(config-if)# no shutdown
UltOs(config-if)# switchport pvid *2*
UltOs(config-if)# exit

15.3.3 Configuration in FDN40-3

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal
UltOs(config)# vlan 11
UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*
UltOs(config-vlan)# exit
UltOs(config)# interface vlan 11
UltOs(config-if)# shutdown
UltOs(config-if)# ip address *10.4.0.3 255.255.0.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# vlan *2*
UltOs(config-vlan)# ports *wan 0/2* **untagged** *wan 0/2*
UltOs(config-vlan)# exit
UltOs(config)# interface vlan *2*
UltOs(config-if)# ip address *10.1.1.3 255.255.255.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# interface *wan 0/2*
UltOs(config-if)# no shutdown

UltOs(config-if)# switchport pvid *2*

UltOs(config-if)# exit

15.3.4 Configuration in FDN40-4

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal

UltOs(config)# interface wan 0/1

UltOs(config-if)# no shutdown

UltOs(config)# exit

UltOs(config)# vlan 11

UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*

UltOs(config-vlan)# exit

UltOs(config)# interface vlan 11

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.4.0.4 255.255.0.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan *3*

UltOs(config-vlan)# ports *wan 0/2*

UltOs(config-vlan)# exit

UltOs(config)# interface vlan 3

UltOs(config-if)# ip address *10.5.6.4 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan *4*

UltOs(config-vlan)# ports add *wan 0/2*

UltOs(config-vlan)# exit

UltOs(config)# interface *vlan 4*

UltOs(config-if)# ip address *10.5.5.4 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

15.3.5 Configuration in FDN40-5

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal

UltOs(config)# vlan 11

UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*
UltOs(config-vlan)# exit
UltOs(config)# interface vlan 11
UltOs(config-if)# shutdown
UltOs(config-if)# ip address *10.8.0.5 255.255.0.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# vlan *4*
UltOs(config-vlan)# ports *wan 0/2* **untagged** *wan 0/2*
UltOs(config-vlan)# exit
UltOs(config)# interface vlan *4*
UltOs(config-if)# ip address *10.5.5.5 255.255.255.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# interface *wan 0/2*
UltOs(config-if)# no shutdown
UltOs(config-if)# switchport pvid *4*
UltOs(config-if)# exit

15.3.6 Configuration in FDN40-6

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal
UltOs(config)# vlan 11
UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*
UltOs(config-vlan)# exit
UltOs(config)# interface vlan 11
UltOs(config-if)# shutdown
UltOs(config-if)# ip address *10.7.0.6 255.255.0.0*
UltOs(config-if)# no shutdown
UltOs(config-if)# exit
UltOs(config)# vlan *3*
UltOs(config-vlan)# ports *wan 0/2* **untagged** *wan 0/2*
UltOs(config-vlan)# exit
UltOs(config)# interface vlan *3*
UltOs(config-if)# ip address *10.5.6.6 255.255.255.0*
UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# interface *wan 0/2*

UltOs(config-if)# no shutdown

UltOs(config-if)# switchport pvid *3*

UltOs(config-if)# exit

15.3.7 Configuration in FDN40-7

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal

UltOs(config)# vlan 11

UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*

UltOs(config-vlan)# exit

UltOs(config)# interface vlan 11

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.8.0.7 255.255.0.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

15.3.8 Configuration in FDN40-6

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal

UltOs(config)# vlan *10*

UltOs(config-vlan)# ports *wan 0/2* **untagged** *wan 0/2*

UltOs(config-vlan)# exit

UltOs(config)# interface vlan *10*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.10.2.8 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# interface *wan 0/2*

UltOs(config-if)# switchport pvid *10*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# vlan 11

UltOs(config-vlan)# ports *wan 0/1* **untagged** *wan 0/1*

UltOs(config-vlan)# exit

UltOs(config)# interface *vlan 11*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.10.1.8 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# interface *wan 0/1*

UltOs(config-if)# switchport pvid *11*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

15.3.9 Configuration in FDN40-9

Prerequisite: Configuration of VLAN Interfaces

UltOs# configure terminal

UltOs(config)# vlan *2*

UltOs(config-vlan)# ports *wan 0/2* **untagged** *wan 0/2*

UltOs(config-vlan)# exit

UltOs(config)# interface vlan *2*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *10.2.2.9 255.255.255.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# interface *wan 0/2*

UltOs(config-if)# switchport pvid *2*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

15.4 Default Configurations

Table 15-1: Default Configurations

Parameter	Default Configuration
Stability interval	40
translation-role	Candidate
compatible rfc1583	Enabled
abr-type	standard
neighbor priority	1
area default-cost	10

area tos	0
area metric	10
area - metric-type	1
area - tos	0
default-information originate always metric	10
default-information originate always metric metric-type	2
Authentication	no authentication
hello-interval	10
retransmit-interval	5
transmit-delay	1
dead-interval	40
tag	2
summary-address	advertise
translation	disabled
redist-config metric-value	10
redist-config metric-type	asExttype2
redist-config tag	manual
nssa asbr-default-route translator	disable

15.5 OSPF Configurations

15.5.1 Enabling and Disabling OSPF

Enabling OSPF takes the user to the Router Configuration Mode from which the router related commands are executed. Disabling OSPF terminates the OSPF process.

15.5.1.1 CLI Configuration

1. Execute the following commands to enable OSPF.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable OSPF globally in the Switch FDN40-1.

     UltOs(config)# router ospf

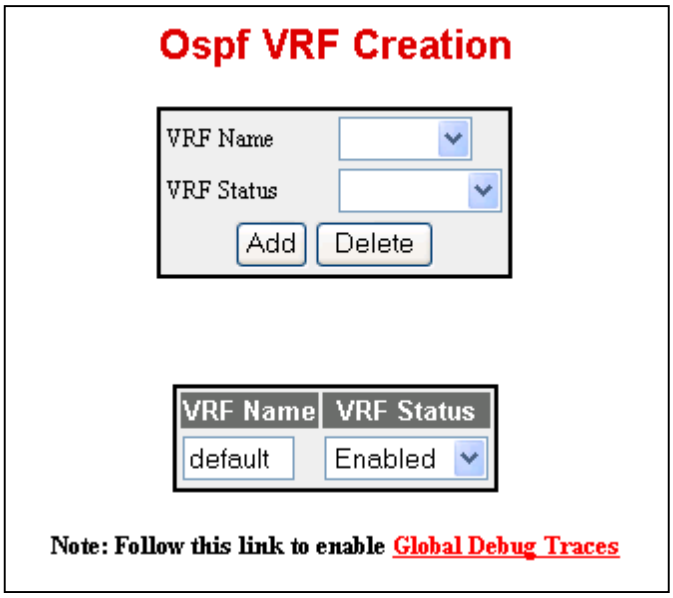
2. This command takes the user to the router configuration mode.

   UltOs(config-router)#

To disable OSPF globally in the switch FDN40-1 by executing the following command. **UltOs(config)# no router ospf**

15.5.1.2 WEB Configuration

OSPF can be enabled/ disabled through WEB interface using the **OSPF VRF Creation** screen (Navigation - **Layer3 Management > OSPF > OSPF VRF Creation**



Screen 15-1: OSPF VRF Creation

15.5.2 Configuring Router-id

The Router-id configured must be one of the IP addresses of the IP interfaces configured in the switch.

15.5.2.1 CLI Configuration

1. Execute the following commands to configure the router-id.
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Enable OSPF globally in the Switch FDN40-1.

     UltOs(config)# router ospf
   - Configure the OSPF router-id.

     UltOs(config-router)# router-id *10.10.2.1*

     It is possible to configure an arbitrary value for the IP address for each router. However, each router ID must be unique. To ensure uniqueness, the router-id must match with one of the IP interface addresses of the router.
   - Exit from the Router Configuration mode.

     UltOs(config-router)# exit

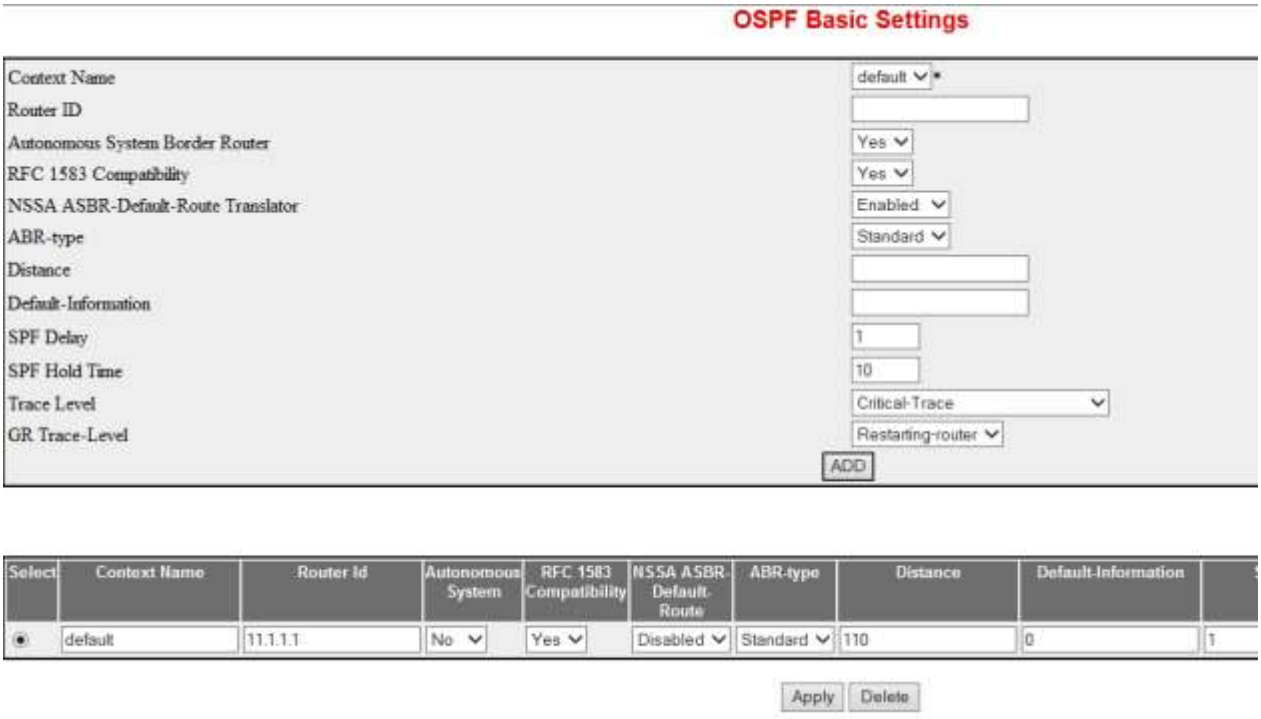
2. View the configuration details by executing the following show command.

   UltOs# show ip ospf

```
OSPF Router ID 10.10.2.1
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 6 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 6 times
```

15.5.2.2 WEB Configuration

Router id can be set to configured through WEB interface using the **OSPF Basic Settings** screen (Navigation - **Layer3 Management > OSPF > Basic Settings)**



Screen 15-2: OSPF Basic Settings

15.5.3 Configuring OSPF Interface

15.5.3.1 CLI Configuration

1. Execute the following commands to configure OSPF interface.

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the Switch FDN40-1.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.10.2.1*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area. VLAN Interfaces VLAN11 and VLAN10 are created as part of the prerequisite configuration.

  UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

  UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

- Enabling OSPF over the VLAN interfaces defines the interfaces on which OSPF runs and the area ID for those interfaces.

2. View the configuration details by executing the following show command.

UltOs# show ip ospf

```
OSPF Router ID 10.10.2.1
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
It is an Area Border Router
Number of Areas in this router is 2
Area is 0.0.0.6
Number of interfaces in this area is 1
SPF algorithm executed 6 times
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 6 times
```

3. View the OSPF interfaces.

UltOs# show ip ospf interface

```
vlan11 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area
0.0.0.0
AS 1, Router ID 10.10.2.1, Network Type BROADCAST,
Cost 1
Transmit Delay is 1 sec, State 4, Priority 1
Designated RouterId 10.10.2.1, Interface address
10.4.0.1
Backup Designated RouterId 10.4.0.4, Interface
address 10.4.0.4
Timer intervals configured, Hello 10, Dead 40, Wait
40, Retransmit 5
Hello due in 8 sec
Neighbor Count is 3, Adjacent neighbor count is 3
Adjacent with the neighbor 10.4.0.4
Adjacent with the neighbor 10.4.0.3
Adjacent with the neighbor 10.4.0.2
vlan10 line protocol is up
Internet Address 10.10.2.1, Mask 255.255.255.0, Area
0.0.0.6
AS 1, Router ID 10.10.2.1, Network Type BROADCAST,
Cost 1
Transmit Delay is 1 sec, State 4, Priority 1
```

```
Designated RouterId 10.10.2.1, Interface address
10.10.2.1

Backup Designated RouterId 10.10.1.8, Interface
address 10.10.2.8

Timer intervals configured, Hello 10, Dead 40, Wait
40, Retransmit 5

Hello due in 6 sec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with the neighbor 10.10.1.8 OSPF Router ID
10.10.2.1
```

Execute the no form of the command to disable OSPF routing for the interfaces defined and to remove the area ID of the interface. **UltOs(config-router)# no network** *10.4.0.1* **area** *0.0.0.0*

PW interface can be configured as OSPF interface similar to router port. For Creating and assigning the IP address to PW interface refer FDN40 configuration user manual.

15.5.3.2 WEB Configuration

Interface can be set to configured through WEB interface using the **OSPF Basic Settings** screen (Navigation - **Layer3 Management > OSPF > Interface**

Screen 15-3: OSPF Interface Configuration

15.5.4 Configuring OSPF Interface Parameters

The interface parameters are configured in the Interface Configuration mode.

15.5.4.1 CLI Configuration

Execute the following commands prior to the configuration of OSPF Interface Parameters.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Enable OSPF over the VLAN interface and associate the interface with an OSPF area. VLAN Interfaces VLAN11 and VLAN10 are created as part of the prerequisite configuration.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

   UltOs(config-router)# exit

5. Enter the Interface Configuration mode.

   UltOs(config)# interface vlan 11

   UltOs(config-if)#

15.5.4.2 WEB Configuration

OSPF Interface Parameters can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2

15.5.5 Configuring OSPF Interface Priority

Configuring OSPF Interface Priority sets the interface priority of the router, which helps to determine the designated router for the link connected to the interface.

15.5.5.1 CLI Configuration

1. Execute the following command to configure the VLAN 11 interface priority as 10.

   UltOs(config-if)#ip ospf priority *10*

2. View the configuration details by executing the following show command.

   UltOs# show ip ospf interface vlan 11

   ```
   vlan11 is line protocol is up
   ```

```
Internet Address 10.4.0.1, Mask 255.255.0.0, Area
0.0.0.0

AS 1, Router ID 10.10.2.1, Network Type BROADCAST,
Cost 1

Transmit Delay is 1 sec, State 4, Priority 10

Designated RouterId 10.10.2.1, Interface address
10.4.0.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait
40, Retransmit 5

Hello due in 4 sec

Neighbor Count is 0, Adjacent neighbor count is 0
```

15.5.5.2 WEB Configuration

OSPF Interface Priority can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

A priority value of 0 signifies that the router is not eligible to become the designated router on a particular network.

The default interface priority value is 1. Restore the default value of the OSPF Interface by executing the following command. **UltOs(config-if)# no ip ospf priority**

15.5.6 Configuring LSA Retransmission Level

Configuring LSA Retransmission Interval specifies the time interval between the successive link-state advertisement (LSA) retransmissions.

15.5.6.1 CLI Configuration

1. Execute the following command to configure the VLAN 11 retransmit-interval as 10 seconds.

   UltOs(config-if)# ip ospf retransmit-interval *10*

2. View the configuration details by executing the following show command.

   UltOs# show ip ospf interface vlan 11

```
vlan11 is line protocol is up

Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0

AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1

Transmit Delay is 1 sec, State 4, Priority 1

Designated RouterId 10.10.2.1, Interface address 10.4.0.1

No backup designated router on this network
```

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 10

Neighbor Count is 0, Adjacent neighbor count is 0

15.5.6.2 WEB Configuration

LSA Retransmission Level can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

Restore the default value of retransmission interval by executing the following command. **UltOs(config-if)# no ip ospf retransmit-interval**

15.5.7 Configuring Hello Interval

Configuring Hello Interval specifies the interval between the hello packets sent on the interface.

15.5.7.1 CLI Configuration

1. Execute the following command to configure the VLAN 11 hello interval as 40 seconds.

   UltOs(config-if)# ip ospf hello-interval *40*

2. View the configuration details by executing the following show command.
   UltOs# show ip ospf interface vlan 11

   vlan11 is line protocol is up

   Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0

   AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1

   Transmit Delay is 1 sec, State 4, Priority 1

   Designated RouterId 10.10.2.1, Interface address10.4.0.1

   No backup designated router on this network

   Timer intervals configured, Hello 40, Dead 40, Wait 40, Retransmit 5

   Hello due in 4 sec

   Neighbor Count is 0, Adjacent neighbor count is 0

15.5.7.2 WEB Configuration

Hello Interval can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

15.5.8 Configuring Dead Interval

Configuring Dead-Interval sets the interval at which hello packets must not be seen before the neighbors declare the router down.

15.5.8.1 CLI Configuration

1. Execute the following command to configure the VLAN 11 dead-interval as 120 seconds.

   UltOs(config-if)# ip ospf dead-interval *120*

2. View the configuration details by executing the following show command.

   UltOs# show ip ospf interface vlan 11

vlan11 is line protocol is up

Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0

AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1

Transmit Delay is 1 sec, State 4, Priority 1

Designated RouterId 10.10.2.1, Interface address 10.4.0.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 120, Wait 120, Retransmit 5

Hello due in 4 sec

Neighbor Count is 0, Adjacent neighbor count is 0

15.5.8.1 WEB Configuration

Dead Interval can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

Restore the default value for dead-interval (40 seconds) by executing the following command. **UltOs(config-if)# no ip ospf dead-interval**

15.5.9 Configuring Network Type

The OSPF network type can be broadcast only. The OSPF network type can not be configured to a type other than the default for a given media.

15.5.10 Configuring Interface Cost

Configuring Interface Cost explicitly specifies the cost of sending a packet on an interface.

15.5.10.1 CLI Configuration

1. Execute the following command to configure the VLAN 11 interface cost as 20.

   UltOs(config-if)# ip ospf cost *20*

2. View the configuration details by executing the following show command.

   UltOs# show ip ospf interface *vlan 11*

vlan11 is line protocol is up

Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0

AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 20

Transmit Delay is 1 sec, State 4, Priority 1

Designated RouterId 10.10.2.1, Interface address 10.4.0.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 120, Wait 120, Retransmit 5

Hello due in 4 sec

Neighbor Count is 0, Adjacent neighbor count is 0

15.5.10.2 WEB Configuration

OSPF Interface Cost can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

Restore the default value for interface cost by executing the following command. **UltOs(config-if)# no ip ospf cost**

15.5.11 Configuring OSPF Authentication

The authentication type for OSPF can be configured as “Simple Password Authentication”, “Message-Digest Authentication” or “Null Authentication”. The following sections describe the configuration of OSPF Authentication.

Authentication related configuration are done in the Interface Configuration mode.

Execute the following commands prior to the configuration of OSPF Authentication.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Enable OSPF over the VLAN interface (VLAN Interfaces vlan11 and vlan10 already created as part of prerequisite configuration) and associate the interface with an OSPF area.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

   UltOs(config-router)# exit

5. Enter the Interface Configuration mode.

   UltOs(config)# interface vlan 11

UltOs(config-if)#

Sample Configuration for Testing Authentication

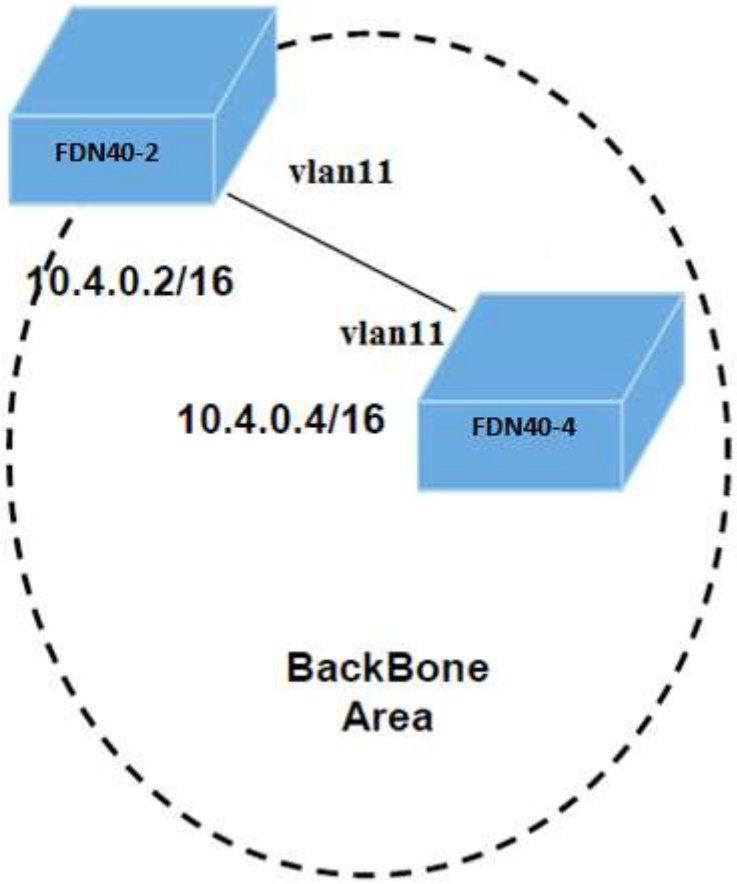


Figure 15-2: Topology for Testing Authentication

Some prerequisite configuration (refer Configuration Guidelines (Prerequisite)) must be done in the switches FDN40-2, FDN40-4 before configuring OSPF.

15.5.11.1 Configuring Simple Password Authentication

For the Simple Password Authentication, a password must be specified which is to be used by the neighboring routers that are using the OSPF simple password authentication.

15.5.11.1.1 CLI Configuration

1. Execute the following commands in FDN40-2 and FDN40-4.

Simple Password authentication

Configuration in FDN40-2:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-2.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.4.0.2*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.4.0.2* **area** *0.0.0.0*

- Exit from the router configuration mode.

  UltOs(config-router)# exit

- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Configure the authentication key for simple password authentication.

  UltOs(config-if)# ip ospf authentication-key *1234*

- Enable simple password authentication.

  UltOs(config-if)# ip ospf authentication

- Exit from the Interface Configuration mode.

  UltOs(config-if)# exit

- Exit from the configuration mode.

  UltOs(config)# exit

Configuration in FDN40-4:

- Enter the Global Configuration mode.
  UltOs# configure terminal
- Enable OSPF globally in the switch FDN40-4.
  UltOs(config)# router ospf
- Configure the OSPF router-id.
  UltOs(config-router)# router-id *10.4.0.4*
- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.
  UltOs(config-router)# network *10.4.0.4* **area** *0.0.0.0*
- Exit from the Router Configuration mode.
  UltOs(config-router)# exit
- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Configure the authentication key for simple password authentication.
  UltOs(config-if)# ip ospf authentication-key *1234*

- Enable simple password authentication.
  UltOs(config-if)# ip ospf authentication
- Exit from the Interface Configuration mode.
  UltOs(config-if)# exit
- Exit from the configuration mode.
  UltOs(config)# exit
  UltOs#

2.View the authentication type configured by executing the following show command.

UltOs# show ip ospf interface
vlan11 is line protocol is up

Internet Address 10.4.0.2, Mask 255.255.0.0, Area 0.0.0.0

AS 1, Router ID 10.4.0.2, Network Type BROADCAST, Cost 1

Transmit Delay is 1 sec, State 5, Priority 1

Designated RouterId 10.4.0.4, Interface address 10.4.0.4

Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 0 sec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with the neighbor 10.4.0.4

Simple password authentication enabled

3.View the adjacency formed between the neighbors (FDN40-2 and FDN40-4) by executing the following command.

UltOs# show ip ospf neighbor detail

Neighbor 10.4.0.4, interface address 10.4.0.4

In the area 0.0.0.0 via interface vlan11

Neighbor priority is 1, State is FULL/BACKUP, 5 state changes

DR is 10.4.0.4 BDR is 10.4.0.2

Options is 0x2

A previously assigned OSPF password can be removed by executing the following command. **UltOs(config-if)# no ip ospf authentication-key**

15.5.11.1.2 WEB Configuration

OSPF Simple Password Authentication can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

A previously assigned OSPF password can be removed by executing the following command. **UltOs(config-if)# no ip ospf authentication-key**

15.5.11.2 Configuring Message-Digest Authentication

Message-Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a “message-digest” that appends to the packet.

15.5.11.2.1 CLI Configuration

1. Execute the following commands to configure the message-digest authentication.

Configuration in FDN40-2:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Delete the authentication key for simple password authentication.

  UltOs(config-if)# no ip ospf authentication-key

- Configure the authentication key for the message-digest authentication.

  UltOs(config-if)# ip ospf message-digest-key *0* **md5** asdf

- Enable message-digest authentication.

  UltOs(config-if)# ip ospf authentication message-digest

- Exit from the Interface Configuration mode.

  UltOs(config-if)# exit

- Exit from the configuration mode.

  UltOs(config)# exit

Configuration in FDN40-4:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Delete the authentication key for simple password authentication.

  UltOs(config-if)# no ip ospf authentication-key

- Configure the authentication key for message-digest authentication.

  UltOs(config-if)# ip ospf message-digest-key *0* **md5** *asdf*

- Enable message-digest authentication.

UltOs(config-if)# ip ospf authentication message-digest

- Exit from the Interface Configuration mode.

  UltOs(config-if)# exit

- Exit from the configuration mode.

  UltOs(config)# exit

2. View the configuration details by executing the following show commands.

In FDN40-2:

View the type of authentication configured.

UltOs# show ip ospf interface

0

vlan11 is line protocol is up

Internet Address 10.4.0.2, Mask 255.255.0.0, Area 0.0.0.0

AS 1, Router ID 10.4.0.2, Network Type BROADCAST, Cost 1

Transmit Delay is 1 sec, State 5, Priority 1

Designated RouterId 10.4.0.4, Interface address 10.4.0.4

Backup Designated RouterId 10.4.0.2, Interface address 10.4.0.2

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 0 sec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with the neighbor 10.4.0.4

Message digest authentication enabled

Youngest key id is 0

View the adjacency formation between the neighbors.

UltOs# show ip ospf neighbor detail

Neighbor 10.4.0.4, interface address 10.4.0.4

In the area 0.0.0.0 via interface vlan11

Neighbor priority is 1, State is FULL/BACKUP, 5 state changes

DR is 10.4.0.4 BDR is 10.4.0.2

Options is 0x2

15.5.11.2.2 WEB Configuration

OSPF Message Digest Authentication can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

15.5.11.3 Configuring Message-Digest with key constants

15.5.11.3.1 CLI Configuration

1. Execute the following commands to configure the message-digest authentication with key constants.
Configuration in FDN40-2:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Delete the authentication key for simple password authentication.

  UltOs(config-if)# no ip ospf authentication-key

- Configure the authentication key for the message-digest authentication.

  UltOs(config-if)# ip ospf message-digest-key *1* **md5** asdf

- Enable message-digest authentication.

  UltOs(config-if)# ip ospf authentication message-digest

Configuration in FDN40-4:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Delete the authentication key for simple password authentication.

  UltOs(config-if)# no ip ospf authentication-key

- Configure the authentication key for the message-digest authentication.

  UltOs(config-if)# ip ospf message-digest-key *1* **md5** asdf

- Enable message-digest authentication.

  UltOs(config-if)# ip ospf authentication message-digest

2. View the configuration details by executing the following show commands.
In FDN40-2:
View the type of authentication configured.

UltOs# show ip ospf interface

vlan11 is line protocol is up

Internet Address 12.0.0.1, Mask 255.0.0.0, Area 0.0.0.0

AS 1, Router ID 12.0.0.1, Network Type BROADCAST, Cost 1

Transmit Delay is 1 sec, State 5, Priority 1

Designated RouterId 12.0.0.2, Interface address 12.0.0.2

Backup Designated RouterId 12.0.0.1, Interface address 12.0.0.1

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 7 sec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with the neighbor 12.0.0.2

Message digest authentication enabled

Youngest key id is 1

Key Start Accept Time is 30 Jan 2012 09:21

Key Start Generate Time is 30 Jan 2012 09:21

Key Stop Generate Time is 30 Jan 2012 09:31

Key Stop Generate Time is 30 Jan 2012 09:31

Connected to VRF default

15.5.11.3.2 WEB Configuration

OSPF Message Digest Authentication can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2.

15.5.11.4 Configuring NULL Authentication

15.5.11.4.1 CLI Configuration

1. Execute the following commands to configure the OSPF authentication type as Null Authentication.

Configuration in FDN40-2:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Delete the authentication key for message digest authentication.

  UltOs(config-if)# no ip ospf message-digest-key *0*

- Enable Null digest authentication.

  UltOs(config-if)# ip ospf authentication null

- Exit from the Interface Configuration mode.

  UltOs(config-if)# exit

- Exit from the configuration mode.

  UltOs(config)# exit

UltOs#

Configuration in FDN40-4:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode.

  UltOs(config)#interface vlan 11

- Delete the authentication key for message digest authentication.

  UltOs(config-if)# no ip ospf message-digest-key *0*

- Enable Null digest authentication.

  UltOs(config-if)# ip ospf authentication null

- Exit from the Interface Configuration mode.

  UltOs(config-if)# exit

- Exit from the configuration mode.

  UltOs(config)# exit

2. View the adjacency formation between the neighbors by executing the following show command.
UltOs# show ip ospf neighbor detail

Neighbor 10.4.0.4, interface address 10.4.0.4

In the area 0.0.0.0 via interface vlan11

Neighbor priority is 1, State is FULL/BACKUP, 5 state changes

DR is 10.4.0.4 BDR is 10.4.0.2

Options is 0x23

15.5.11.4.2 WEB Configuration

OSPF Message Digest Authentication can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2

15.5.12 Configuring Passive Interface

Configuring Passive Interface suppresses routing updates on all interfaces.

15.5.12.1 CLI Configuration

1. Execute the following commands to suppress routing updates on all the interfaces.

- Enter the Global Configuration mode in FDN40-1.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-1.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.10.2.1*

- Suppress routing updates by executing the following command.

  UltOs(config-if)# passive-interface default

  All the OSPF interfaces created after the execution of this command will be passive. This is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

- Enable OSPF over the VLAN interface.

  UltOs(config-if)# network *10.4.0.1* **area** *0.0.0.0*

2. View the configuration details using the following command.

   UltOs# show ip ospf interface vlan 11

```
vlan11 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 2, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
No Hellos (Passive interface)
Neighbor Count is 0, Adjacent neighbor count is 0
```

Restore routing updates on all interfaces by executing the following commands.

UltOs(config-if)# no network *10.4.0.1* **area** *0.0.0.0*
UltOs(config-if)# no passive-interface default

It is also possible to suppress routing updates on a specified interface.

1. Execute the following commands to suppress routing updates on a specified interface.

   - Enter the Global Configuration mode in FDN40-1.

     UltOs# configure terminal

   - Enable OSPF globally in the switch FDN40-1.

     UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.10.2.1*

- Exit from the router configuration mode.

  UltOs(config-router)# exit

- Enter the Interface Configuration Mode for VLAN 11.

  UltOs(config)# interface vlan 11

- Enable OSPF over the VLAN interface.

  UltOs(config-if)# network *10.4.0.1* **area** *0.0.0.0*

- Configure the VLAN 11 interface as passive interface.

  UltOs(config-if)# passive-interface vlan 11

2. View the configuration details by executing the following show command.

UltOs# show ip ospf interface vlan 11.

```
vlan11 is line protocol is up
Internet Address 10.4.0.1, Mask 255.255.0.0, Area 0.0.0.0
AS 1, Router ID 10.10.2.1, Network Type BROADCAST, Cost 1
Transmit Delay is 1 sec, State 2, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
No Hellos (Passive interface)
Neighbor Count is 0, Adjacent neighbor count is 0
```

15.5.12.2 WEB Configuration

OSPF Message Digest Authentication can be configured through WEB interface using the **OSPF Interface** screen. For screenshot, refer section 4.5.3.2

Restore routing updates on interface VLAN 11. **UltOs(config-if)# no passive-interface vlan 11**

15.5.13 Configuring OSPF Area Parameters

Area parameters can be configured only after enabling the OSPF process.

Area parameters are configured in the Router Configuration mode.

15.5.13.1 Configuring Stub Area

Configuring Stub Area specifies an area as a stub area. It also configures other parameters related to that area.

15.5.13.1.1 CLI Configuration

Execute the following commands to configure an area as a stub area.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the OSPF interface.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the area 0.0.0.6 as a stub area.

   UltOs(config-router)# area *0.0.0.6* **stub**

Execute the following command to re-Configure the area 0.0.0.6 as a normal area. **UltOs(config-router)# no area** *0.0.0.6* **stub**

Refer Sample Configuration for Stub area, ASBR and route redistribution.

15.5.13.1.2 WEB Configuration

OSPF Stub Area can be set to configured through WEB interface using the **OSPF Area Configuration** screen (Navigation - **Layer3 Management > OSPF > Area**)

Screen 15-4: OSPF Area Configuration

15.5.13.2 Configuring ASBR Router

Routers that act as gateways (redistribution) between OSPF and other routing protocols (IGRP, EIGRP, RIP, BGP, Static) or other instances of the OSPF routing process are called autonomous system boundary router (ASBR).

15.5.13.2.1 CLI Configuration

Execute the following commands to configure a router as an ASBR router.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the ASBR router.

   UltOs(config-router)# asbr router

Disable the ASBR router by executing the following command. **UltOs(config-router)# no asbr router**

Refer Sample Configuration for Stub area, ASBR and route redistribution.

15.5.13.2.2 WEB Configuration

OSPF ASBR Router can be configured through WEB interface using the **OSPF Area** screen. For screenshot, refer section 15.5.13.1.2

15.5.13.3 Configuring Redistribution

Configuring Redistribution configures the protocol from which the routes have to be redistributed into OSPF.

15.5.13.3.1 CLI Configuration

Execute the following commands to configure redistribution.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the router as ASBR router.

   UltOs(config-router)# asbr router

5. Configure redistribution of all routes.

UltOs(config-router)# redistribute all

Disable redistribution of routes by executing the following command.

UltOs(config-router)# no redistribute all

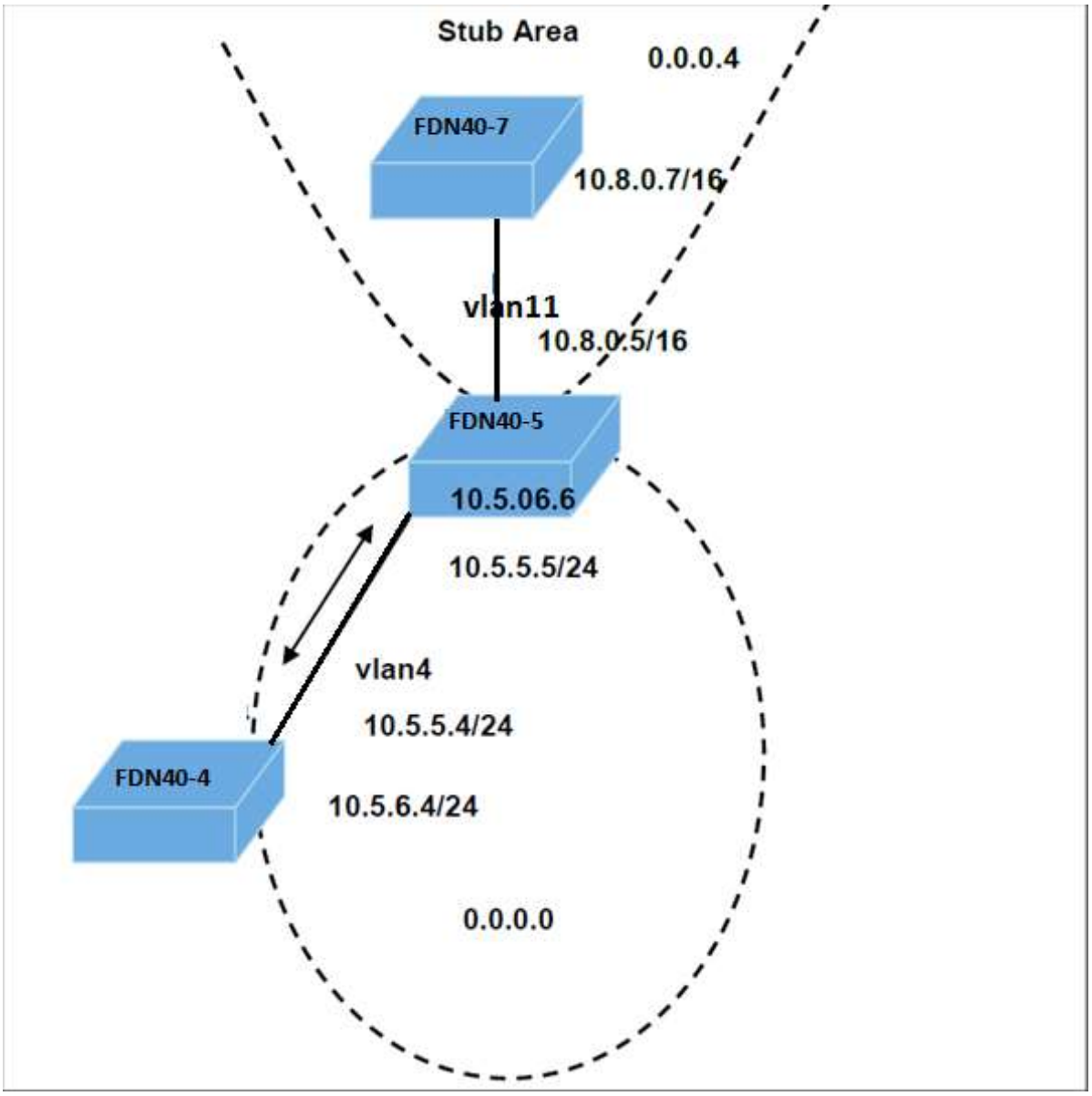


Figure 15-3: Topology For Configuration of stub area, ASBR and route redistribution

Sample Configuration for Stub area, ASBR and route redistribution

Some prerequisite configuration (refer Configuration Guidelines (Prerequisite)) must be done in the switches FDN40-4, FDN40-5, and FDN40-7 before configuring OSPF.

1. Execute the following commands in FDN40-4, FDN40-5 and FDN40-7.

Configuration in FDN40-4:

FDN40-4 is configured as an ASBR router for redistributing the external routes into OSPF domain.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *10.4.0.4*

UltOs(config-router)# asbr router

UltOs(config-router)# redistribute all

UltOs(config-router)# network *10.5.5.4* **area** *0.0.0.0*

UltOs(config-router)# exit

UltOs(config)# ip route *100.0.0.0 255.0.0.0 10.5.5.5*

UltOs(config)# end

Configuration in FDN40-5:

In FDN40-5 area 0.0.0.4 is configured as a stub area.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *10.8.0.5*

UltOs(config-router)# network *10.8.0.5* **area** *0.0.0.4*

UltOs(config-router)# network *10.5.5.5* **area** *0.0.0.0*

UltOs(config-router)# area *0.0.0.4* **stub**

UltOs(config-router)# exit

Configuration in FDN40-7:

In FDN40-7 area 0.0.0.4 is configured as a stub area . External routes are not redistributed into Stub area.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *10.8.0.7*

UltOs(config-router)# network *10.8.0.7* **area** *0.0.0.4*

UltOs(config-router)# area *0.0.0.4* **stub**

UltOs(config-router)# exit

2. View the configuration details by executing the following show commands.

In FDN40-4:

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area
--------- --- -------/--------- ---- ------- ----
10.5.5.0/255.255.255.0 0 0.0.0.0/vlan4 1 IntraArea 0.0.0.0

10.8.0.0/255.255.0.0 0 10.5.5.5/vlan4 2 InterArea 0.0.0.0

UltOs# show ip ospf *0.0.0.0* **database external**

OSPF Router with ID (10.4.0.4)
AS External Link States

LS age : 300

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 10.4.0.0

Advertising Router : 10.4.0.4

LS Seq Number : 0x80000001

Checksum : 0x2a6

Length : 36

Network Mask : 255.255.0.0

Metric Type : 0x80

Metric : 10

Forward Address : 0.0.0.0

Externel Route Tag: 0

AS External Link States

LS age : 300

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 10.5.5.0

Advertising Router : 10.4.0.4

LS Seq Number : 0x80000001

Checksum : 0xbee3

Length : 36

Network Mask : 255.255.255.0

```
Metric Type : 0x80
Metric : 10
Forward Address : 0.0.0.0
Externel Route Tag: 0
```

AS External Link States

LS age : 300
Options : (No ToS Capability, DC)
LS Type : AS External Link
Link State ID : 10.5.6.0
Advertising Router : 10.4.0.4
LS Seq Number : 0x80000001
Checksum : 0xb3ed
Length : 36
Network Mask : 255.255.255.0
Metric Type : 0x80
Metric : 10
Forward Address : 0.0.0.0
Externel Route Tag: 0

AS External Link States

LS age : 300
Options : (No ToS Capability, DC)
LS Type : AS External Link
Link State ID : 100.0.0.0
Advertising Router : 10.4.0.4
LS Seq Number : 0x80000001
Checksum : 0xcd6b
Length : 36
Network Mask : 255.0.0.0
Metric Type : 0x80
Metric : 10
Forward Address : 10.5.5.5
Externel Route Tag: 0

In FDN405:
View the external routes are redistributed in this switch

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--------- --- -------/--------- ---- ------- ----

10.4.0.0/255.255.0.0 0 10.5.5.4/vlan4 10 Type2Ext 0.0.0.0

10.5.5.0/255.255.255.0 0 0.0.0.0/vlan4 1 IntraArea 0.0.0.0

10.5.6.0/255.255.255.0 0 10.5.5.4/vlan4 10 Type2Ext 0.0.0.0

10.8.0.0/255.255.0.0 0 0.0.0.0/vlan11 1 IntraArea 0.0.0.4

100.0.0.0/255.0.0.0 0 10.5.5.5/vlan4 10 Type2Ext 0.0.0.0

UltOs# show ip ospf *0.0.0.0* database external

```
OSPF Router with ID (10.8.0.5)
AS External Link States
----------------------
LS age : 300
Options : (No ToS Capability, DC)
LS Type : AS External Link
Link State ID : 10.4.0.0
Advertising Router : 10.4.0.4
LS Seq Number : 0x80000001
Checksum : 0x2a6
Length : 36
Network Mask : 255.255.0.0
Metric Type : 0x80
Metric : 10
Forward Address : 0.0.0.0
Externel Route Tag: 0
```

AS External Link States

LS age : 300

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 10.5.5.0

Advertising Router : 10.4.0.4

LS Seq Number : 0x80000001

Checksum : 0xbee3

Length : 36

Network Mask : 255.255.255.0

Metric Type : 0x80

Metric : 10

Forward Address : 0.0.0.0

Externel Route Tag: 0

AS External Link States

LS age : 300

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 10.5.6.0

Advertising Router : 10.4.0.4

LS Seq Number : 0x80000001

Checksum : 0xb3ed

Length : 36

Network Mask : 255.255.255.0

Metric Type : 0x80

Metric : 10

Forward Address : 0.0.0.0

Externel Route Tag: 0

In FDN40-7:
View the external routes are not redistributed into the stub area 0.0.0.4.

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--- --- ---/--- ---- --- ---

0.0.0.0/0.0.0.0 0 10.8.0.5/vlan11 2 InterArea 0.0.0.4

10.5.5.0/255.255.255.0 0 10.8.0.5/vlan11 2 InterArea 0.0.0.4

10.8.0.0/255.255.0.0 0 0.0.0.0/vlan11 1 IntraArea 0.0.0.4

UltOs# show ip ospf *0.0.0.4* database external

OSPF Router with ID (10.8.0.7)

15.5.13.3.2 WEB Configuration

OSPF Redistribution can be configured through WEB interface using the **OSPF Area** screen. For screenshot, refer section 15.5.13.1.2

15.5.13.4 Configuring NSSA Area

An NSSA area has the capability to import limited number of external routes.

15.5.13.4.1 CLI Configuration

Execute the following commands to configure an area as an NSSA area.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the OSPF interface.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the area 0.0.0.6 as an nssa area.

   UltOs(config-router)# area *0.0.0.6* **nssa**

Re-Configure the area 0.0.0.6 as a normal area by executing the following command. **UltOs(config-router)# no area** *0.0.0.6* **nssa**

Refer Sample NSSA Configuration, summary address configuration and area-default cost

15.5.13.4.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Area** screen. For screenshot, refer section 15.5.13.1.2

15.5.13.5 Configuring Summary Address

15.5.13.5.1 CLI Configuration

Execute the following commands to configure summary address.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the OSPF interface.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the area 0.0.0.6 as an NSSA area.

   UltOs(config-router)# area *0.0.0.6* **nssa**

6. Configure the summary address for 90.0.0.0/8 in the NSSA area.

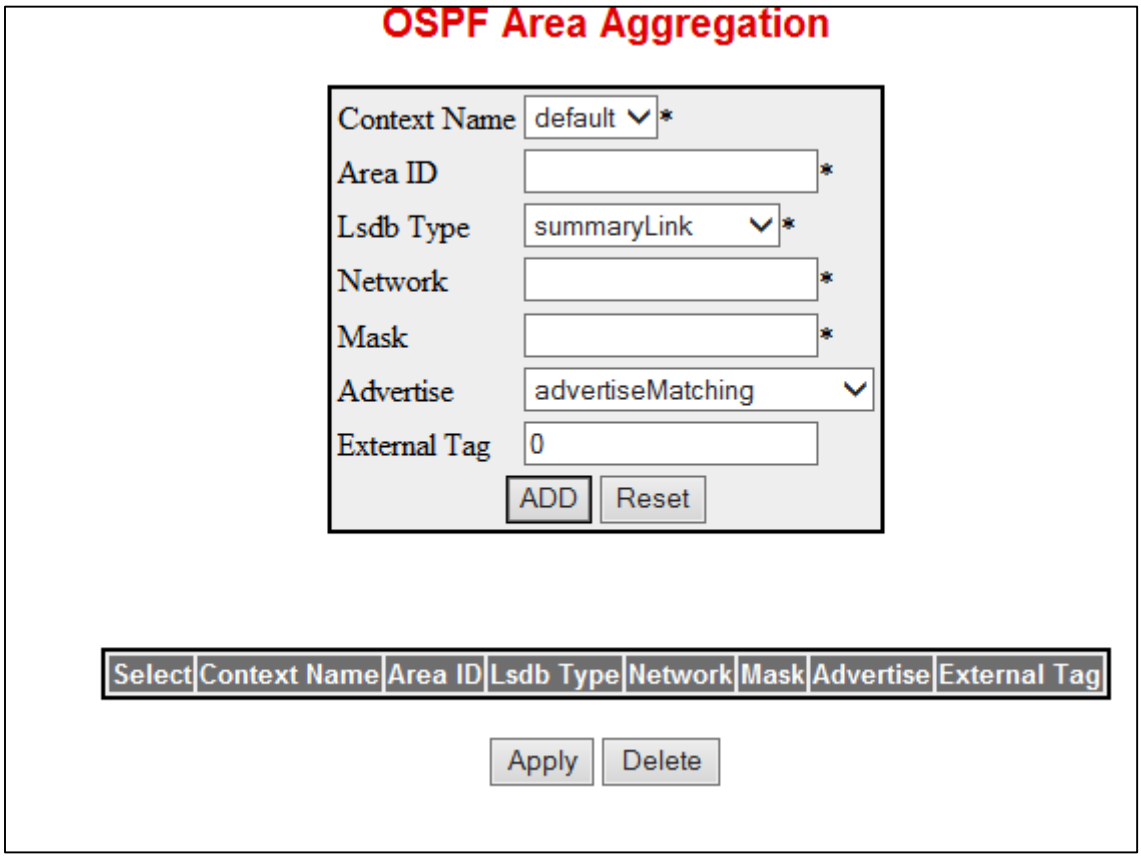
   UltOs(config-router)# summary-address *90.0.0.0 255.0.0.0 0.0.0.6*

Delete the summary address configuration for 90.0.0.0/8 in the NSSA area by executing the following command. **UltOs(config-router)# no summary-address** *90.0.0.0 255.0.0.0 0.0.0.6*

Refer Sample NSSA Configuration, summary address configuration and area-default cost

15.5.13.5.2 WEB Configuration

OSPF Stub Area can be set to configured through WEB interface using the **OSPF Area Configuration** screen (Navigation - **Layer3 Management > OSPF > Aggregation**)



Screen 15-5: OSPF Area Aggregation

15.5.13.6 Configuring Area-default Cost

Configuring Area-default Cost specifies the cost for the default summary route sent into a stub or NSSA.

15.5.13.6.1 CLI Configuration

Execute the following commands to configure the Area-default Cost.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the OSPF interface.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the area 0.0.0.6 as an NSSA area.

   UltOs(config-router)# area 0.0.0.6 nssa

6. Configure the cost for the default summary route sent into the NSSA area.

   UltOs(config-router)# area *0.0.0.6* **default-cost** *50*

Configure the default cost for the default summary route sent into NSSA area by executing the following command.

UltOs(config-router)# no area *0.0.0.6* **default-cost**

Sample NSSA Configuration, summary address configuration and area-default cost

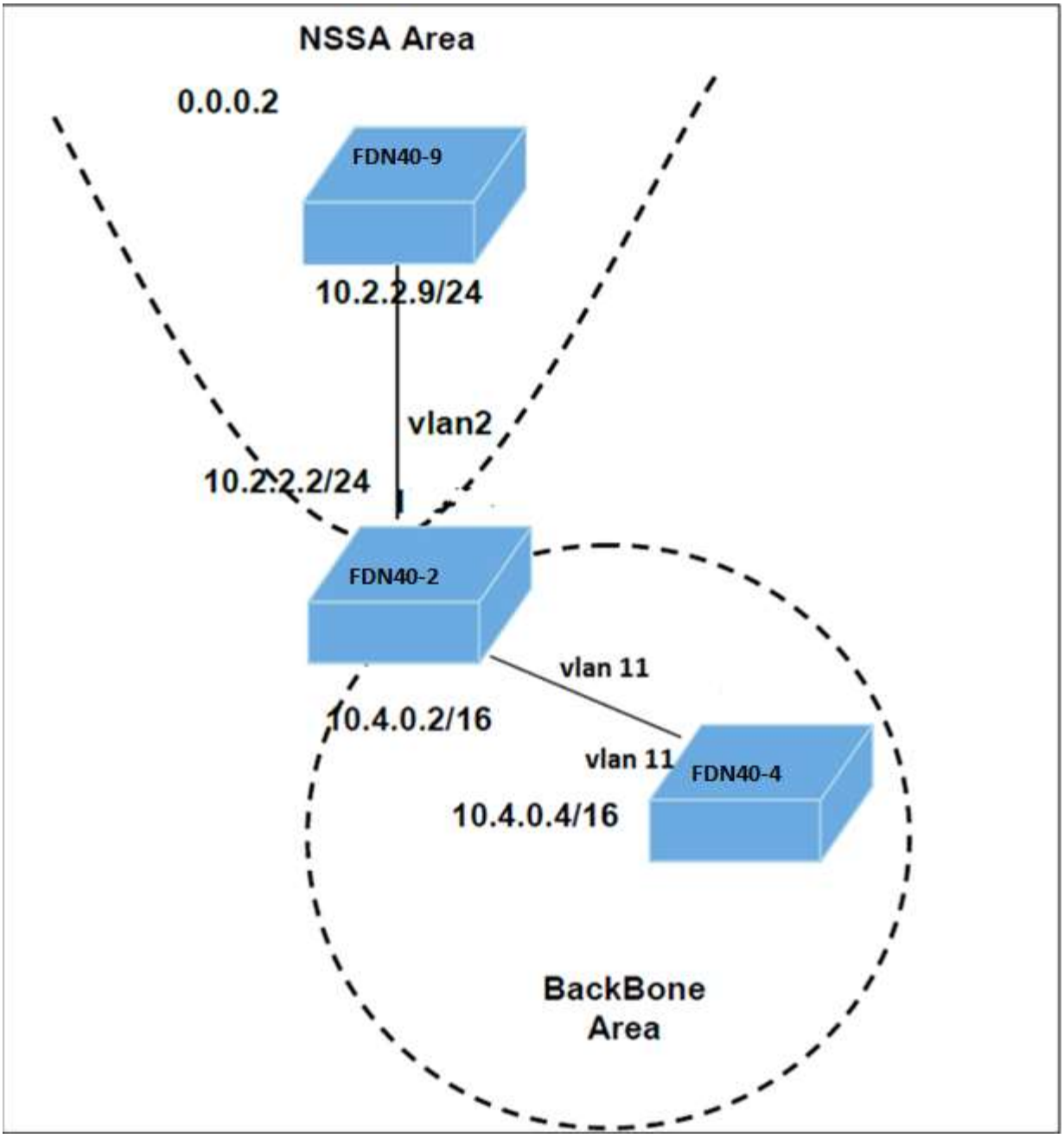


Figure 15-4: Topology For NSSA, summary address and area-default Cost Configuration

Some prerequisite configuration (refer Configuration Guidelines (Prerequisite)) must be done in the switches FDN40-2, FDN40-4, FDN40-9 before configuring OSPF.

1. Execute the following commands in FDN40-2, FDN40-4 and FDN40-9.

Configuration in FDN40-2:

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *10.4.0.2*

UltOs(config-router)# network *10.4.0.2* **area** *0.0.0.0*

UltOs(config-router)# network *10.2.2.2* **area** *0.0.0.2*

- Configure area 0.0.0.2 as an NSSA area.

UltOs(config-router)# area *0.0.0.2* **nssa**

UltOs(config-router)# exit

Configuration in FDN40-4:

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *10.4.0.4*

UltOs(config-router)# network *10.4.0.4* **area** *0.0.0.0*

UltOs(config-router)# end

Configuration in FDN40-9:

UltOs# configure terminal

UltOs(config)# router ospf

- Configure ASBR status and redistribute static routes into the OSPF domain.

UltOs(config-router)# asbr router

UltOs(config-router)# redistribute static

UltOs(config-router)# router-id *10.2.2.9*

UltOs(config-router)# network *10.2.2.9* **area** *0.0.0.2*

Configure the area 0.0.0.2 as an NSSA area.

UltOs(config-router)# area *0.0.0.2* **nssa**

- Configure summary address for the range 90.0.0.0/8 in the area 0.0.0.2.

UltOs(config-router)# summary-address *90.0.0.0 255.0.0.0 0.0.0.2*

UltOs(config-router)# exit

-Configure static routes.

UltOs(config)# ip route *90.1.0.0 255.255.0.0 10.2.2.2*

UltOs(config)# ip route *90.2.0.0 255.255.0.0 10.2.2.2*

UltOs(config)# ip route *90.3.0.0 255.255.0.0 10.2.2.2*

UltOs(config)# ip route *90.4.0.0 255.255.0.0 10.2.2.2*

UltOs(config)# ip route *90.5.0.0 255.255.0.0 10.2.2.2*

UltOs(config)# end

2. View the configuration details by executing the following show commands.

In FDN40-2

View the two nssa-external LSAs one for 90.0.0.0/8 matching the summary range configured and the other for the default external route in the NSSA area.

Another external LSA is generated in the area 0.0.0.0 corresponding to the nssa-external LSA 90.0.0.0/8.

UltOs# show ip ospf database nssa-external

OSPF Router with ID (10.4.0.2)

NSSA External Link States (Area 0.0.0.2)

LS age : 300

Options : (No ToS Capability, DC)

LS Type : NSSA External Link

Link State ID : 90.0.0.0

Advertising Router : 10.2.2.9

LS Seq Number : 0x80000001

Checksum : 0xc84f

Length : 36

NSSA External Link States (Area 0.0.0.2)

LS age : 300

Options : (No ToS Capability, DC)

LS Type : NSSA External Link

Link State ID : 0.0.0.0

Advertising Router : 10.4.0.2

LS Seq Number : 0x80000002

Checksum : 0x120

Length : 36

UltOs# show ip ospf database external

OSPF Router with ID (10.4.0.2)

AS External Link States

LS age : 0

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 90.0.0.0

Advertising Router : 10.4.0.2

LS Seq Number : 0x80000001

Checksum : 0x49fd

Length : 36

Network Mask : 255.0.0.0

Metric Type : 0x80

Metric : 10

Forward Address : 10.2.2.9

Externel Route Tag: 0

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--------- --- -------/--------- ---- ------- ----

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 0.0.0.0/vlan11 1 IntraArea 0.0.0.0

90.0.0.0/255.0.0.0 0 10.2.2.9/vlan2 10 Type2Ext 0.0.0.2

In FDN40-4

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--------- --- -------/--------- ---- ------- ----

10.2.2.0/255.255.255.0 0 10.4.0.2/vlan11 2 InterArea 0.0.0.0

10.4.0.0/255.255.0.0 0 0.0.0.0/vlan11 1 IntraArea 0.0.0.0

90.0.0.0/255.0.0.0 0 10.4.0.2/vlan11 10 Type2Ext 0.0.0.0

In FDN40-9

UltOs# show ip ospf database nssa-external

OSPF Router with ID (10.2.2.9)

NSSA External Link States (Area 0.0.0.2)

LS age : 300

Options : (No ToS Capability, DC)

LS Type : NSSA External Link

Link State ID : 90.0.0.0

Advertising Router : 10.2.2.9

LS Seq Number : 0x80000001

Checksum : 0xc84f

Length : 36

NSSA External Link States (Area 0.0.0.2)

LS age : 300

Options : (No ToS Capability, DC)

LS Type : NSSA External Link

Link State ID : 0.0.0.0

Advertising Router : 10.4.0.2

LS Seq Number : 0x80000002

Checksum : 0x120

Length : 36

UltOs# show ip ospf summary-address

Display of Summary addresses for Type5 and Type7 from redistributed routes

OSPF External Summary Address Configuration Information

Network Mask Area Effect TranslationState

------- ---- ---- ------ ---------------

90.0.0.0 255.0.0.0 0.0.0.2 advertiseMatching enabled

UltOs# show ip route

O 0.0.0.0/0 [2] via 10.2.2.2

C 10.2.2.0/24 is directly connected, vlan2

O 10.4.0.0/16 [2] via 10.2.2.2

C 12.0.0.0/8 is directly connected, vlan11

S 90.1.0.0/16 [1] via 10.2.2.2

S 90.2.0.0/16 [1] via 10.2.2.2

S 90.3.0.0/16 [1] via 10.2.2.2

S 90.4.0.0/16 [1] via 10.2.2.2

S 90.5.0.0/16 [1] via 10.2.2.2

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--------- --- -------/--------- ---- ------- ----

0.0.0.0/0.0.0.0 0 10.2.2.2/vlan2 2 Type1Ext 0.0.0.2

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 10.2.2.2/vlan2 2 InterArea 0.0.0.2

Configuration in FDN40-9:

1. To Test no summary command.

   UltOs# configure terminal

   UltOs(config)# router ospf

   UltOs(config-router)# no summary-address *90.0.0.0 255.0.0.0 0.0.0.2*

2. View the configuration detail in FDN40-9.

   UltOs# show ip ospf summary-address

Display of Summary addresses for Type5 and Type7 from redistributed routes

nssa-external LSA is generated for all the static routes.

UltOs# show ip ospf database

OSPF Router with ID (10.2.2.9)

Router Link States (Area 0.0.0.2)

Link ID ADV Router Age Seq# Checksum Link count

------- ---------- --- ---- -------- ----------

10.4.0.2 10.4.0.2 300 0x80000006 0x1dc6 1

10.2.2.9 10.2.2.9 300 0x80000007 0xec0 1

Network Link States (Area 0.0.0.2)

Link ID ADV Router Age Seq# Checksum

------- ---------- --- ---- --------

10.2.2.9 10.2.2.9 300 0x80000002 0x5290

Summary Link States (Area 0.0.0.2)

Link ID ADV Router Age Seq# Checksum

------- ---------- --- ---- --------

10.4.0.0 10.4.0.2 300 0x80000003 0x56c5

NSSA External Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	Checksum
90.4.0.0	10.2.2.9	300	0x80000001	0x36e4
90.5.0.0	10.2.2.9	300	0x80000001	0x2aef
0.0.0.0	10.4.0.2	300	0x80000003	0xfe21
90.1.0.0	10.2.2.9	300	0x80000001	0x5ac3
90.2.0.0	10.2.2.9	300	0x80000001	0x4ece
90.3.0.0	10.2.2.9	300	0x80000001	0x42d9

In FDN40-2:

3. View the OSPF external routes corresponding to all the NSSA-external LSAs.

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--------- --- -------/--------- ---- ------- ----

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 0.0.0.0/vlan11 1 IntraArea 0.0.0.0

90.1.0.0/255.255.0.0 0 10.2.2.2/vlan2 10 Type2Ext 0.0.0.2

90.2.0.0/255.255.0.0 0 10.2.2.2/vlan2 10 Type2Ext 0.0.0.2

90.3.0.0/255.255.0.0 0 10.2.2.2/vlan2 10 Type2Ext 0.0.0.2

90.4.0.0/255.255.0.0 0 10.2.2.2/vlan2 10 Type2Ext 0.0.0.2

90.5.0.0/255.255.0.0 0 10.2.2.2/vlan2 10 Type2Ext 0.0.0.2

Configuration in FDN40-2:

1. To test the area default-cost command.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# area *0.0.0.2* **default-cost** *50*

In FDN40-9:

FDN40-2 sends a type 7 LSA for the default route with the updated metric as 50. Therefore, the metric for the default route should be 51 in FDN40-9.

2. View the configuration

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--- --- ---/--- ---- --- ---

0.0.0.0/0.0.0.0 0 10.2.2.2/vlan2 51 Type1Ext 0.0.0.2

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 10.2.2.2/vlan2 2 InterArea 0.0.0.2

Configuration in FDN40-2:

1. To Test no area default-cost command.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# no area *0.0.0.2* **default-cost**

In FDN40-9:

FDN40-2 must have sent a type 7 LSA for the default route with the updated default metric as 10. Therefore, the metric for the default route must be 11 in FDN40-9.

2. View the configuration

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--- --- ---/--- ---- --- ---

0.0.0.0/0.0.0.0 0 10.2.2.2/vlan2 11 Type1Ext 0.0.0.2

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 10.2.2.2/vlan2 2 InterArea 0.0.0.2

15.5.13.6.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Area** screen. For screenshot, refer section 15.5.13.1.2

15.5.13.7 Configuring NSSA asbr-default-route translator

Configuring NSSA asbr-default-route translator enables/disables setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR.

15.5.13.7.1 CLI Configuration

Execute the following commands to configure the NSSA asbr-default-route translator.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the ASBR router status.

   UltOs(config-router)#asbr router

5. Configure the OSPF interface.

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

6. Configure the area 0.0.0.6 as an nssa area.

   UltOs(config-router)# area *0.0.0.6* **nssa**

7. Enable nssa asbr-default-route translator.

   UltOs(config-router)# set nssa asbr-default-route translator enable

Disable nssa asbr-default-route translator by executing the following command. **UltOs(config-router)# set nssa asbr-default-route translator disable**

15.5.13.7.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Area** screen. For screenshot, refer section 15.5.13.1.2

15.5.13.8 Configuring NSSA Area Translation Role

Configuring NSSA Area Translation Role configures the translation role for the NSSA as always or candidate.

Execute the following commands to configure the NSSA Area Translation Role.

15.5.13.8.1 CLI Configuration

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the ASBR router status.

   UltOs(config-router)#asbr router

5. Configure the OSPF interface.

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

6. Configure the area 0.0.0.6 as an nssa area.

   UltOs(config-router)# area *0.0.0.6* **nssa**

7. Configure the translation role for the NSSA area 0.0.0.6.

   UltOs(config-router)# area *0.0.0.6* **translation-role always**

Configure the default translation role for the NSSA area 0.0.0.6 by executing the following command. **UltOs(config-router)# no area** *0.0.0.6* **translation-role**

The default translation role is candidate and is configured using the command **no area <area-id> translation-role.**

15.5.13.8.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Area** screen. For screenshot, refer section 15.5.13.1.2

15.5.13.9 Configuring Stability Interval for NSSA

Configuring Stability Interval for the NSSA configures the number of seconds after which an elected translator determines that its services are no longer required, and that it must continue to perform its translation duties for NSSA.

15.5.13.9.1 CLI Configuration

Execute the following commands to configure the Stability Interval for NSSA.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the ASBR router status.

   UltOs(config-router)#asbr router

5. Configure the OSPF interface.

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

6. Configure the area 0.0.0.6 as an nssa area

UltOs(config-router)# area *0.0.0.6* **nssa**

7. Configure the Stability interval for the NSSA area 0.0.0.6 as 120 seconds.

UltOs(config-router)# area *0.0.0.6* **stability-interval** *120*

Configure the default Stability interval for the NSSA area 0.0.0.6 by executing the following command. **UltOs(config-router)# no area** *0.0.0.6* **stability-interval**

The default value for stability interval is 40 seconds and is configured using the command **no area <area-id> stability-interval.**

15.5.13.9.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Area** screen. For screenshot, refer section 15.5.13.1.2

15.5.13.10 Configuring ABR-Type

Configuring abr-type sets the ABR-Type as either standard, or Cisco or IBM.

15.5.13.10.1 CLI Configuration

1. Execute the following commands to configure the abr-type.

- Enter the Global Configuration mode in FDN40-1.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-1.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.10.2.1*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

  UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

- Configure the ABR type as Cisco.

  UltOs(config-router)# abr-type cisco

The default value ABR type is standard.

2. View the configuration details by executing the following show command.

UltOs# show ip ospf

OSPF Router ID 10.10.2.1

Supports only single TOS(TOS0) route

ABR Type supported is Cisco ABR

It is an Area Border Router

Number of Areas in this router is 2

Area is 0.0.0.6

Number of interfaces in this area is 1

SPF algorithm executed 3 times

Area is 0.0.0.0

Number of interfaces in this area is 1

SPF algorithm executed 3 times

15.5.13.10.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Area** For screenshot, refer section 15.5.13.1.2

15.5.13.11 Configuring RFC 1583 Compatibility

Configuring RFC 1583 Compatibility sets the OSPF compatibility list to be compatible with the RFC 1583.

15.5.13.11.1 CLI Configuration

Execute the following commands to configure the RFC 1583 Compatibility.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the rfc1583 compatibility.

   UltOs(config-router)# compatible rfc1583

Disable RFC 1583 compatibility by executing the following command.
UltOs(config-router)# no compatible rfc1583

15.5.13.11.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Basic settings** screen. For screenshot, refer section 15.5.2.2

15.5.13.12 Configuring Default-information Originate Always

Configuring Default-information Originate Always enables generation of a default external route into the OSPF routing domain and other parameters related to that area.

15.5.13.12.1 CLI Configuration

Execute the following commands to configure Default-information Originate Always.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the ASBR router status.

   UltOs(config-router)#asbr router

6. Configure the generation of a default external route.

   UltOs(config-router)# default-information originate always metric *40*

✎ Disable generation of a default external route by executing the following command. **UltOs(config-router)# no default-information originate always**

✎ Refer Sample Configuration for testing default-information originate always and redist-config.

15.5.13.12.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Basic settings** screen. For screenshot, refer section 15.5.2.2

15.5.13.13 Configuring Redist-Config

Configuring redist-config configures the information to be applied to routes learnt from RTM.

15.5.13.13.1 CLI Configuration

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the asbr router.

   UltOs(config-router)# asbr router

5. Configure the redistribution of static routes.

   UltOs(config-router)# redistribute static

6. Configure the redist-config.

   UltOs(config-router)# redist-config *20.0.0.0 255.0.0.0* **metric-value** *100* **metric-type** *asExttype1* **tag** *10*

Delete the information applied to the routes learnt from RTM by executing the following command. **UltOs(config-router)# no redist-config** *20.0.0.0 255.0.0.0*

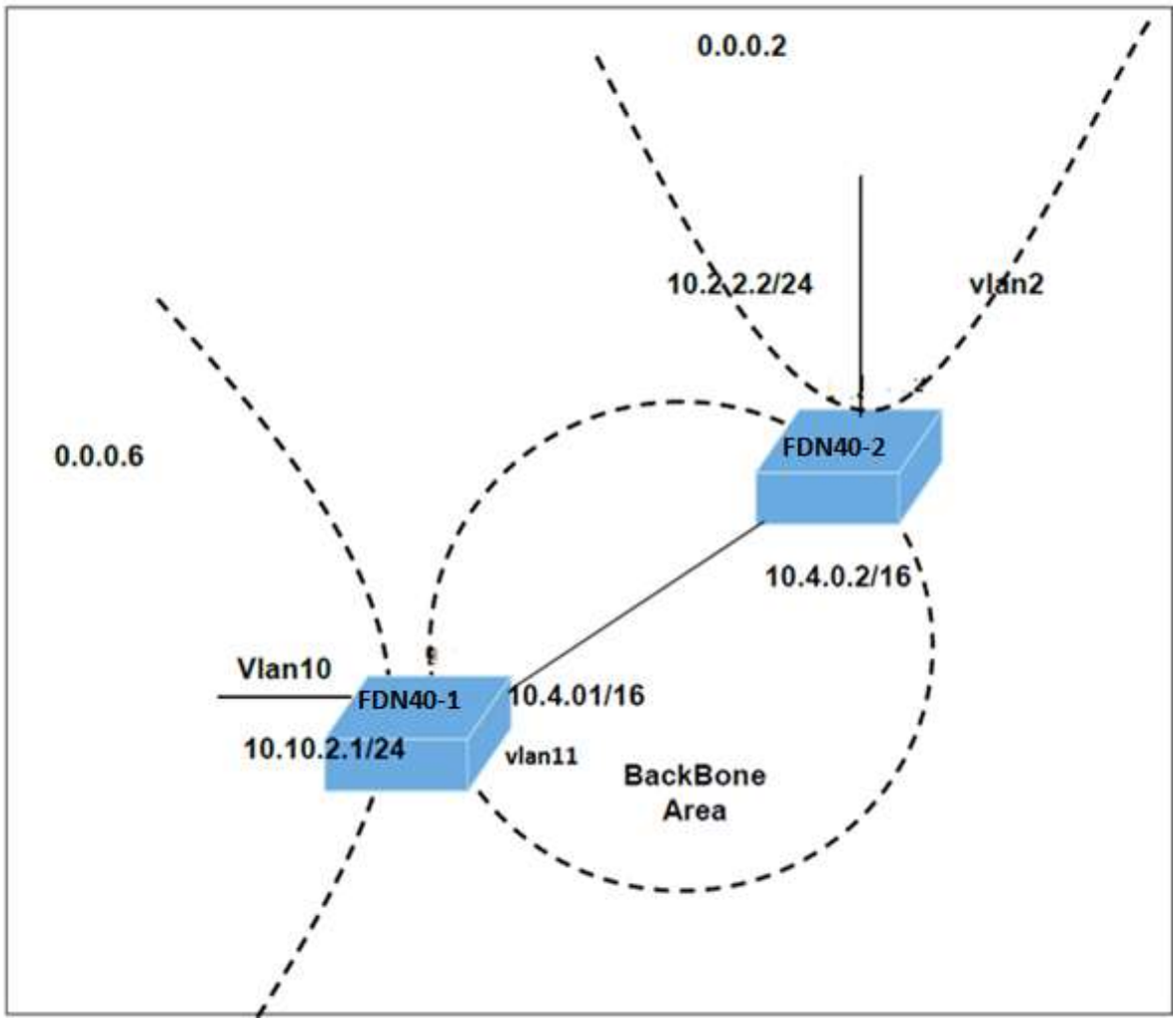


Figure 15-5: Topology For testing default-information originate always and redist-config

Sample Configuration for testing default-information originate always and redist-config.

Some prerequisite configuration (refer Configuration Guidelines (Prerequisite)) must be done in the switches FDN40-1, FDN40-2 before configuring OSPF.

Configuration in FDN40-1:

1. Execute the following commands in FDN40-1 to configure the generation of a default external route.

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-1.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.10.2.1*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

  UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

- Configure the asbr router.

  UltOs(config-router)# asbr router

- Configure the generation of a default external route.

  UltOs(config-router)# default-information originate always metric *40*

- Exit from the router configuration mode.

  UltOs(config-router)# end

  UltOs#

Configuration in FDN40-2:

2. Execute the following commands in FDN40-2

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-2.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.4.0.2*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.4.0.2* **area** *0.0.0.0*

  UltOs(config-router)# network *10.2.2.2* **area** *0.0.0.2*

- Configure area 0.0.0.2 as an NSSA area.

UltOs(config-router)# area *0.0.0.2* **nssa**

- Exit from the router configuration mode.

UltOs(config-router)# end

UltOs#

3. View the configuration details by executing the following show command in FDN40-1.
Type 5 External LSA must be generated for the default route.

UltOs# show ip ospf database external

OSPF Router with ID (10.10.2.1)

AS External Link States

LS age : 0

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 0.0.0.0

Advertising Router : 10.10.2.1

LS Seq Number : 0x80000001

Checksum : 0xb5dd

Length : 36

Network Mask : 0.0.0.0

Metric Type : 0x80

Metric : 40

Forward Address : 0.0.0.0

Externel Route Tag: 0

4. View the configuration details by executing the following show command in FDN40-2.
The route entry for the default route must exist.

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--- --- -------/--- ---- ------- ----

0.0.0.0/0.0.0.0 0 10.4.0.1/vlan11 40 Type2Ext 0.0.0.0

10.2.2.0/255.255.255. 0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 0.0.0.0/vlan11 1 IntraArea 0.0.0.0

10.10.0.0/255.255.0.0 0 10.4.0.1/vlan11 2 InterArea 0.0.0.0

Configuration in FDN40-1:

1. Execute the following commands to disable generation of a default external route.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# no default-information originate always

UltOs(config-router)# end

UltOs#

2. View the configuration detail by executing the following show command.

Type 5 External LSA for the default route must be flushed.

UltOs# show ip ospf database external

OSPF Router with ID (10.10.2.1)

3. Execute the following show command in FDN40-2.

The route entry for the default route must be deleted.

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--- --- ---/--- ---- --- ---

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 0.0.0.0/vlan11 1 IntraArea 0.0.0.0

10.10.0.0/255.255.0.0 0 10.4.0.1/vlan11 2 InterArea 0.0.0.0

Configuration in FDN40-1:

1. Execute the following commands in FDN40-1 to test redist-config.

UltOs# configure terminal

UltOs(config)# router ospf

- Configure redistribution of static routes redist-config.

UltOs(config-router)# redistribute static

- Configure redist-config.

UltOs(config-router)# redist-config *20.0.0.0 255.0.0.0* **metric-value** *100* **metric-type asExttype1 tag** *10*

UltOs(config-router)# exit

- Add a static route for 20.0.0.0/8 network.

UltOs(config)# ip route *20.0.0.0 255.0.0.0 10.4.0.2*

UltOs(config)# end

UltOs#

2. View the configuration details by executing the following show command. An external LSA is generated for 20.0.0.0 with metric as 100, metric type as asExtType1 and tag as 10.

UltOs# show ip ospf database external

OSPF Router with ID (10.10.2.1)

AS External Link States

LS age : 600

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 20.0.0.0

Advertising Router : 10.10.2.1

LS Seq Number : 0x80000001

Checksum : 0xf6b2

Length : 36

Network Mask : 255.0.0.0

Metric Type : 0x0

Metric : 100

Forward Address : 10.4.0.2

Externel Route Tag: 10

In FDN40-2:

3. View the external route 20.0.0.0/8 with metric as 101.

UltOs# show ip ospf route

OSPF Process Routing Table

Dest/Mask TOS NextHop/Interface Cost Rt.Type Area

--- --- -------/---------- ---- ------- ----

10.2.2.0/255.255.255.0 0 0.0.0.0/vlan2 1 IntraArea 0.0.0.2

10.4.0.0/255.255.0.0 0 0.0.0.0/vlan1 1 IntraArea 0.0.0.0

10.10.0.0/255.255.0.0 0 10.4.0.1/vlan1 2 InterArea 0.0.0.0

20.0.0.0/255.0.0.0 0 10.4.0.2/vlan1 101 Type1Ext 0.0.0.0

Configuration in FDN40-1:

1. Execute the following command in FDN40-1 to test no redist-config.

UltOs# configure terminal

UltOs(config)# router ospf

2. Configure no redist-config.

UltOs(config-router)# no redist-config *20.0.0.0 255.0.0.0*

UltOs(config-router)# end

UltOs#

In FDN40-1:

3. View the configuration details by executing the following show command.

The external LSA generated for 20.0.0.0 with metric as 100, metric type as asExtType1 and tag as 10 is flushed and a new external LSA is generated with the default redistribution configuration.

UltOs# show ip ospf database external
OSPF Router with ID (10.10.2.1)

AS External Link States

LS age : 0

Options : (No ToS Capability, DC)

LS Type : AS External Link

Link State ID : 20.0.0.0

Advertising Router : 10.10.2.1

LS Seq Number : 0x80000002

Checksum : 0x3c50

Length : 36

Network Mask : 255.0.0.0

Metric Type : 0x80

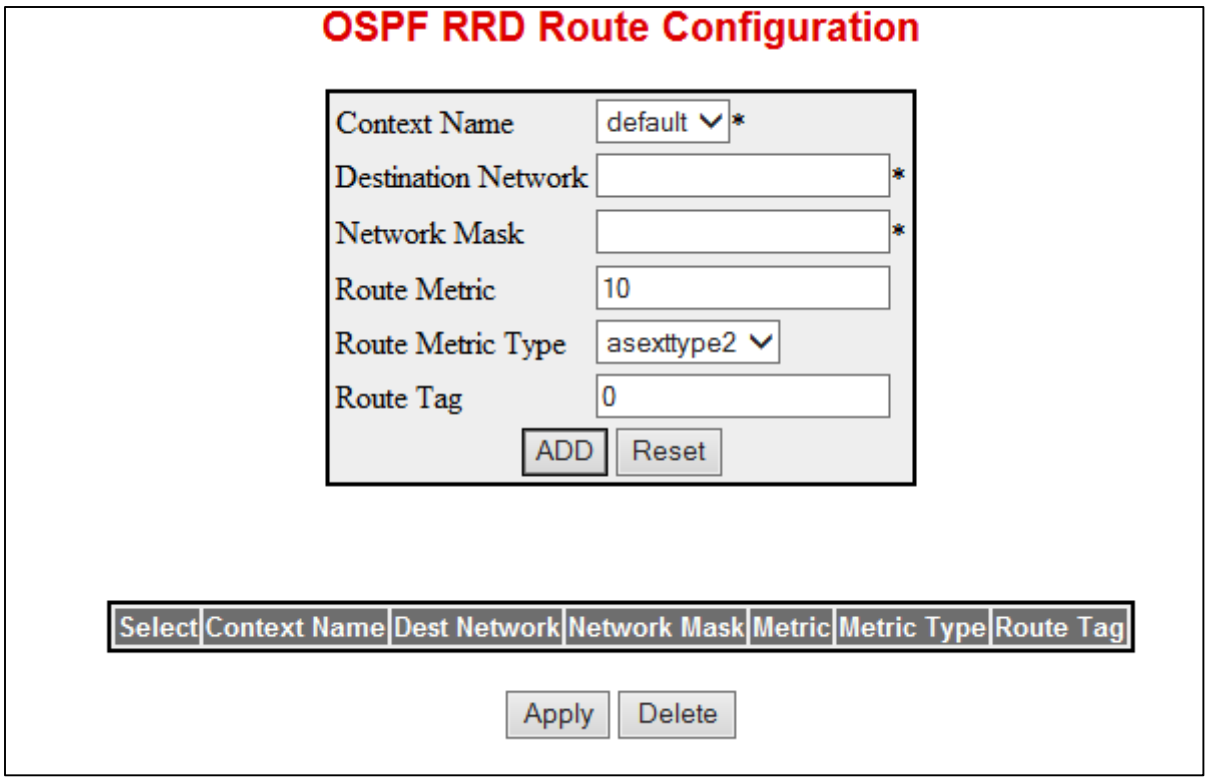
Metric : 10

Forward Address : 10.4.0.2

Externel Route Tag: 0

15.5.13.13.2 WEB Configuration

OSPF Stub Area can be set to configured through WEB interface using the **OSPF RRD Route Configuration** screen (Navigation - **Layer3 Management > OSPF > RRD Route**)



Screen 15-6: OSPF RRD Route Configuration

15.5.13.14 Configuring Neighbor

Configuring Neighbor specifies an NBMA neighbor router and its priority.

15.5.13.14.1 CLI Configuration

Execute the following commands to configure neighbor.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the OSPF interface.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Exit from the Router Configuration mode.

   UltOs(config-router)# exit

6. Enter the Interface Configuration mode.

   UltOs(config)# interface *vlan 11*

7. Configure the network type as NBMA.

   UltOs(config-if)# ip ospf network *non-broadcast*

8. Configure the neighbor with priority.

   UltOs(config-if)# exit

   UltOs(config)# router ospf

   UltOs(config-router)# neighbor *10.4.0.2* **priority** *10*

9. Configure the neighbor with default priority.

   UltOs(config-router)# no neighbor *10.4.0.2* **priority** *10*

Delete the configured neighbor by executing the following command. **UltOs(config-router)# no neighbor** *10.4.0.2*

15.5.13.14.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Basic settings** screen. For screenshot, refer section 15.5.2.2

15.5.13.15 Configuring Virtual link

Configuring Virtual Link defines an OSPF virtual link and its related parameters.

15.5.13.15.1 CLI Configuration

Execute the following commands to configure the Virtual Link.

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the OSPF interface.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.1*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the virtual link.

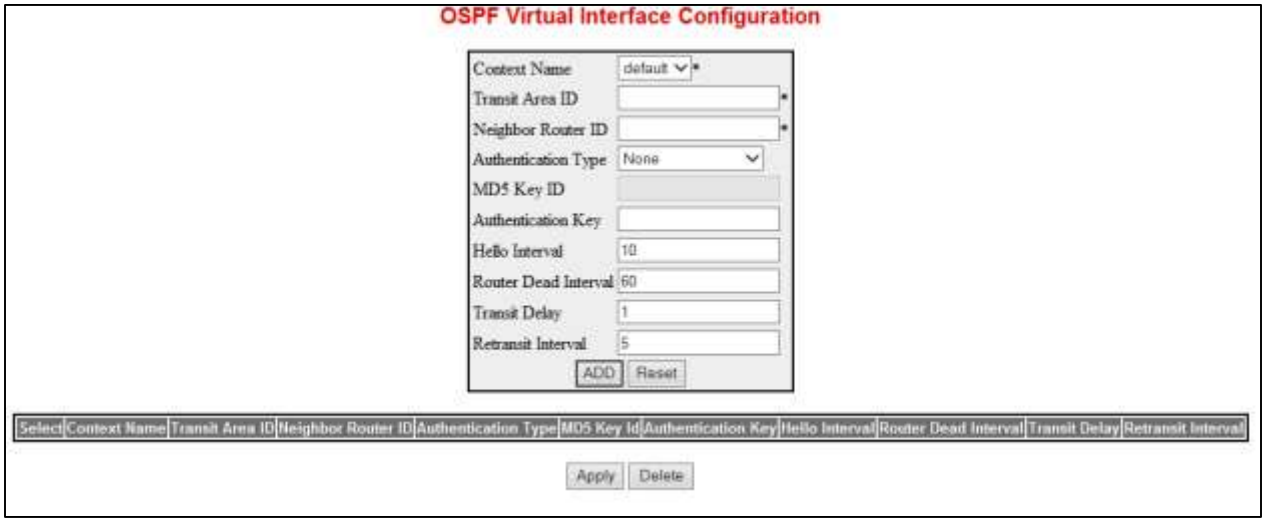
   UltOs(config-router)# area *0.0.0.6* **virtual-link** *20.0.0.1* **authentication** *message-digest* **hello-interval** *100* **retransmit-interval** *100* **transmit-delay** *50* **dead-interval** *200* **authentication-key** *asdf*

Delete the virtual link by executing the following command. **UltOs(config-router)# no area** *0.0.0.6* **virtual-link** *20.0.0.1*

Refer Sample Configuration for testing virtual link and route summarization

15.5.13.15.2 WEB Configuration

OSPF Stub Area can be set to configured through WEB interface using the **OSPF Virtual Interface Configuration** screen (Navigation - **Layer3 Management > OSPF > Virtual Interface**)



Screen 15-7: OSPF Virtual Interface Configuration

15.5.13.16 Configuring Area-range

The area-range is configured to consolidate and summarize routes at an area boundary.

15.5.13.16.1 CLI Configuration

1. Enter the Global Configuration mode in FDN40-1.

   UltOs# configure terminal

2. Enable OSPF globally in the switch FDN40-1.

   UltOs(config)# router ospf

3. Configure the OSPF router-id.

   UltOs(config-router)# router-id *10.10.2.1*

4. Configure the OSPF interface.

   UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

   UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

5. Configure the route summarization at an area border router.

   UltOs(config-router)# area *0.0.0.6* **range** *10.10.0.0 255.255.0.0* **summary**

6. Delete the route summarization information by executing the following command.

   UltOs(config-router)# no area *0.0.0.6* **range** *10.10.0.0 255.255.0.0*

Sample Configuration for testing virtual link and route summarization

Some prerequisite configuration (refer Configuration Guidelines (Prerequisite)) must be done in the switches FDN40-1, FDN40-4, FDN40-5 and FDN40-6 before configuring OSPF.

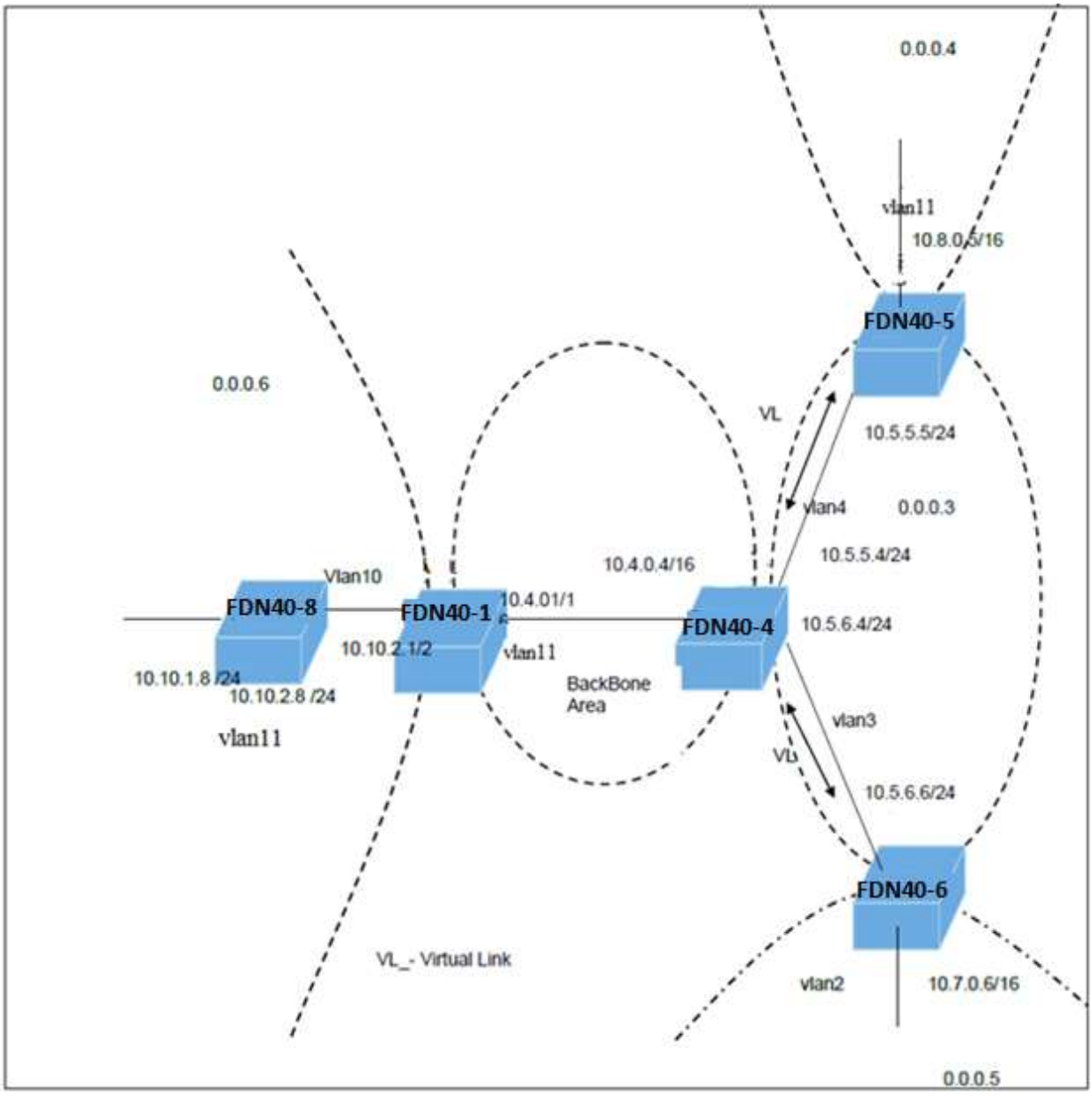


Figure 15-6: Topology For testing virtual link and route summarization

1. Execute the following commands

Configurations in FDN40-1:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-1.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.10.2.1*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.4.0.1* **area** *0.0.0.0*

  UltOs(config-router)# network *10.10.2.1* **area** *0.0.0.6*

- Configure the route summarization at an area border router.

  UltOs(config-router)# area *0.0.0.6* **range** *10.10.0.0 255.255.0.0* **summary**

- Exit from the router configuration mode.
- **UltOs(config-router)# end.**

Configurations in FDN40-4:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-4.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.4.0.4*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.4.0.4* **area** *0.0.0.0*

  UltOs(config-router)# network *10.5.6.4* **area** *0.0.0.3*

  UltOs(config-router)# network *10.5.5.4* **area** *0.0.0.3*

- Configure the virtual link for backbone connectivity.

  UltOs(config-router)# area *0.0.0.3* **virtual-link** *10.7.0.6*

  UltOs(config-router)# area *0.0.0.3* **virtual-link** *10.8.0.5*

- Exit from the router configuration mode.

  UltOs(config-router)# end

Configurations in FDN40-5:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-5.

UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.8.0.5*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.8.0.5* **area** *0.0.0.4*

  UltOs(config-router)# network *10.5.5.5* **area** *0.0.0.3*

- Configure a virtual link for backbone connectivity.

  UltOs(config-router)# area *0.0.0.3* **virtual-link** *10.4.0.4*

- Exit from the router configuration mode.

  UltOs(config-router)# end

Configurations in FDN40-6:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-6.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.7.0.6*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network 10.7.0.6 area 0.0.0.4

  UltOs(config-router)# network 10.5.6.6 area 0.0.0.3

- Configure the virtual link for backbone connectivity.

  UltOs(config-router)# area *0.0.0.3* **virtual-link** *10.4.0.4*

- Exit from the router configuration mode.

  UltOs(config-router)# end

Configurations in FDN40-6:

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable OSPF globally in the switch FDN40-6.

  UltOs(config)# router ospf

- Configure the OSPF router-id.

  UltOs(config-router)# router-id *10.10.1.8*

- Enable OSPF over the VLAN interface and associate the interface with an OSPF area.

  UltOs(config-router)# network *10.10.1.8* **area** *0.0.0.6*

  UltOs(config-router)# network *10.10.2.8* **area** *0.0.0.6*

- Exit from the configuration mode.

  UltOs(config-router)# end

2. View the route summarization information in FDN40-1.
In FDN40-1:

UltOs# show ip ospf area-range

Display of Summary addresses for Type3 and Translated Type5

OSPF Summary Address Configuration Information

Network	Mask	LSAType	Area	Effect	Tag
10.10.0.0	255.255.0.0	Summary	0.0.0.6	Advertise	150746304

3. View the virtual link and the status of the link in FDN40-4.

UltOs# show ip ospf virtual-links

```
Virtual Link to router 10.7.0.6, Interface State is
POINT_TO_POINT
Transit Area 0.0.0.3
Transmit Delay is 1 sec, Neighbor State FULL
Timer intervals configured, Hello 10, Dead 60, Retransmit 5
Virtual Link to router 10.8.0.5, Interface State is
POINT_TO_POINT
Transit Area 0.0.0.3
Transmit Delay is 1 sec, Neighbor State FULL
Timer intervals configured, Hello 10, Dead 60, Retransmit 5
```

4. View the virtual link in FDN40-5.
UltOs# show ip ospf virtual-links

Virtual Link to router 10.4.0.4, Interface State is POINT_TO_POINT

Transit Area 0.0.0.3

Transmit Delay is 1 sec, Neighbor State FULL

Timer intervals configured, Hello 10, Dead 60, Retransmit 5

5. View the virtual link in FDN40-6.

UltOs# show ip ospf virtual-links

Virtual Link to router 10.4.0.4, Interface State is POINT_TO_POINT

Transit Area 0.0.0.3

Transmit Delay is 1 sec, Neighbor State FULL

Timer intervals configured, Hello 10, Dead 60, Retransmit 5

6. View the route available to reach ABR FDN40-1.

UltOs# show ip ospf border-routers

OSPF Process Border Router Information

Destination	TOS	Type	NextHop	Cost	Rt.Type	Area
10.4.0.4	0	ABR	10.5.6.4	1	intraArea	0.0.0.3
10.8.0.5	0	ABR	10.5.6.4	2	intraArea	0.0.0.3
10.10.2.1	0	ABR	255.255.255.255	0		0.0.0.0

15.5.13.16.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF RRD Route** screen. For screenshot, refer section 15.5.13.13.2

15.5.14 Configuring Route Map - OSPF

Ulterius URM (Unified Route Map) is a portable implementation of the route map capability for IPv4 unicast routing software. The URM provides a single interface for the administrator to set up and manage route maps. It also provides a common unified method for routing protocols and static route management software to use route maps for different purposes. The independent nature of the implementation helps to avoid the duplication of the route maps in the different routing modules in a router.

15.5.14.1 Configuring Route Map

This section lists the CLI configuration steps to define a route map with a specified name and the related parameters such as permission and sequence number.

15.5.14.1.1 CLI Configuration

1. Execute the following commands
   - Enter the Global Configuration mode.

     UltOs# configure terminal
   - Configure the route map name, permission and sequence number.

     UltOs(config)# route-map *aa* **permit** *1*
2. View the configured route map

   UltOs# show route-map

Route-map aa, Permit, Sequence 1

Match Clauses:

Set Clauses:

Delete the route map configured.

UltOs(config)# no route-map *aa 1*

15.5.14.1.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF RRD Route** screen. For screenshot, refer section 15.5.13.13.2

15.5.14.2 Configuring Route Map Match Criteria

15.5.14.2.1 CLI Configuration

This section lists the CLI configuration steps to define the filtering criteria for the route map and its related parameters.

1. Execute the following commands

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Configure the route map name, permission and sequence number.

  UltOs(config)# route-map *aa* **permit** *1*

- Configure the route map match destination IP address and the subnet mask.

  UltOs(config-rmap-aa)# match destination ip *91.0.0.1 255.0.0.0*

- Configure the route map match route-type as remote. (Route-type can be configured either as local or remote.)

  UltOs(config-rmap-aa)# match route-type *remote*

- Configure the route map match metric-type. (Metric type can be inter-area / intra-area / type-1-external / type-2-external.)

  UltOs(config-rmap-aa)# match metric-type *inter-area*

- Configure the route map match metric value.

  UltOs(config-rmap-aa)# match metric *44*

- Configure the route map match next-hop IP address.

  UltOs(config-rmap-aa)# match next-hop ip *91.0.0.1*

- Configure the route map match tag.

  UltOs(config-rmap-aa)# match tag *10*

2. View the configured parameters.

UltOs# show running-config route-map

```
Building configuration...
route-map aa permit 1
match destination ip 91.0.0.1 255.0.0.0
match next-hop ip 91.0.0.1
match metric 44
match tag 10
match route-type remote
end
```

Execute the no form of the commands to delete the configurations.

15.5.14.2.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF RRD Route** screen. For screenshot, refer section 15.5.13.13.2

15.5.14.3 Configuring OSPF Distance

15.5.14.3.1 CLI Configuration

This section lists the CLI configuration steps to set the administrative distance for the OSPF router.

1. Execute the following commands

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the OSPF router configuration mode.

  UltOs(config)# router ospf

- Configure the distance for the OSPF routes.

  UltOs(config-router)# distance *130*

2. View the configured distance.

UltOs# show running-config ospf

```
Building configuration...
router ospf
distance 130
!
router ospf
!
```

end

Re-configure the distance to its default value. **UltOs(config-router)# no distance**

15.5.14.3.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF Basic Settings** screen. For screenshot, refer section 15.5.2.2

15.5.14.4 Configuring Redistribution with Route Map

15.5.14.4.1 CLI Configuration

This section lists the CLI configuration steps to configure the protocol from which the routes have to be redistributed into OSPF, by applying the route-map.

1. Execute the following commands

- Enter the Global Configuration mode.
  UltOs# configure terminal
- Enable the OSPF router configuration mode.
  UltOs(config)# router ospf
- Configure the OSPF router ID.
  UltOs(config-router)# router-id *10.10.2.1*
- Configure the router as ASBR (Autonomous System Boundary Router).
  UltOs(config-router)# ASBR Router
- Configure the redistribution of all routes with route-map aa.
  UltOs(config-router)# redistribute all route-map *aa*

2. View the configured parameters.
   UltOs# show running-config ospf

```
Building configuration...
router ospf
router-id 10.10.2.1
ASBR Router
redistribute static route-map aa
redistribute connected route-map aa
redistribute rip route-map aa
redistribute bgp route-map aa
distance 130
```

```
!
router ospf
!
end
```

Disable the redistribution of all routes with route-map. **UltOs(config-router)# no redistribute all route-map** *aa*

15.5.14.4.2 WEB Configuration

OSPF NSSA can be configured through WEB interface using the **OSPF RRD Route** screen. For screenshot, refer section 15.5.13.13.2

15.5.14.5 Topology Configuration for OSPF Testing

This section provides the sample configuration for testing Route map with OSPF.

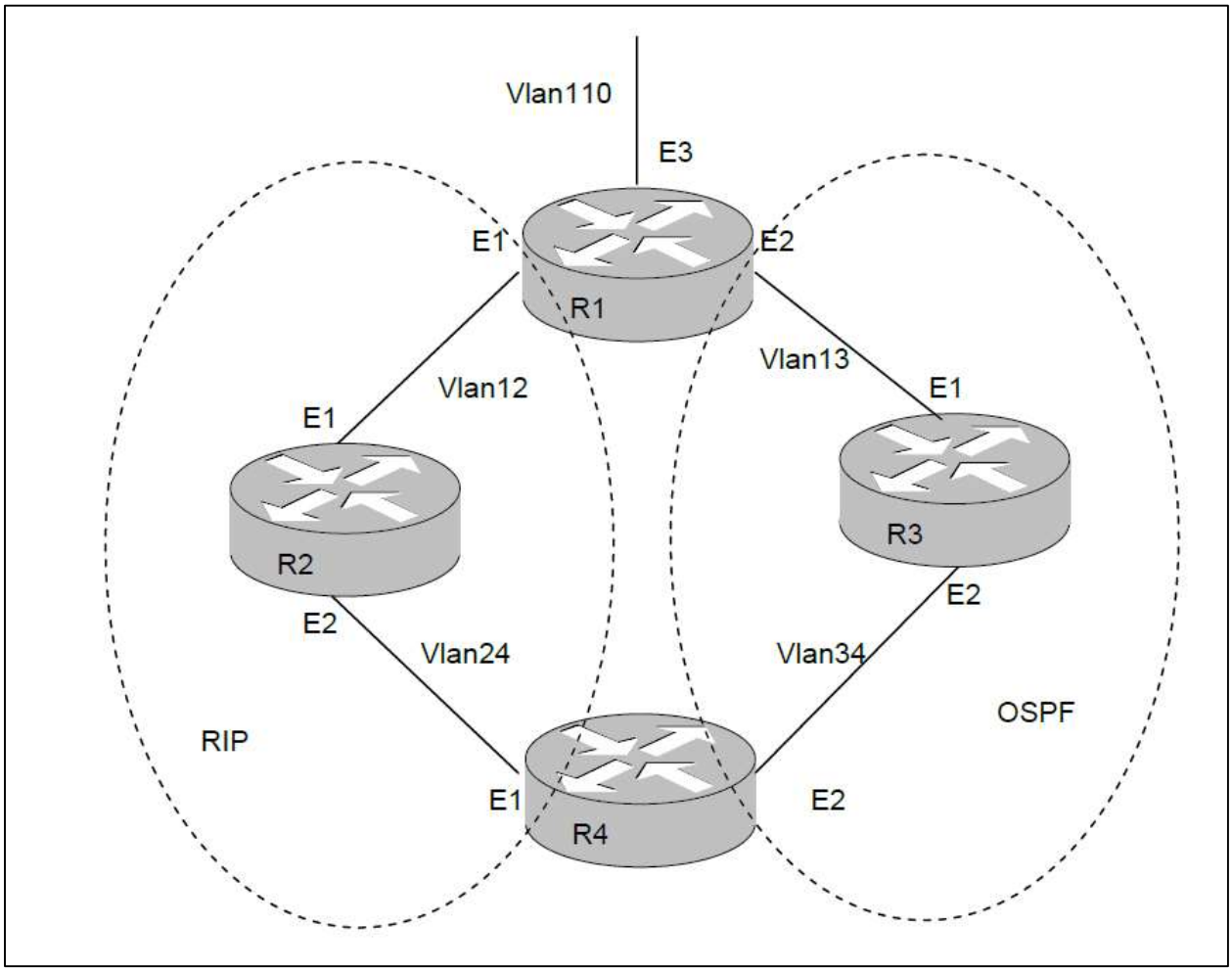


Figure 15-7: Topology Configuration for OSPF Testing

Table 15-2 IPv4 Addresses of Interfaces in the Routers Topology – OSPF Testing

Router	Interface	Ports	IPv4 Address / Mask
R1	Vlan 12	Tagged ports E1	12.0.0.1/8
	Vlan 13	Tagged ports E2	13.0.0.1/8
	Vlan 110	Tagged ports E3	70.0.0.1/8
R2	Vlan 12	Tagged ports E1	12.0.0.2/8
	Vlan 24	Tagged ports E2	24.0.0.2/8
R3	Vlan 13	Tagged ports E1	13.0.0.3/8
	Vlan 34	Tagged ports E2	34.0.0.3/8
R4	Vlan 24	Tagged ports E1	24.0.0.4/8
	Vlan 34	Tagged ports E2	34.0.0.4/8

R1 – ASBR router

All OSPF routers have router-ID 0.0.0.N, where N - number of router.

All OSPF routers use area 0.0.0.0.

Some prerequisite configuration (refer Configuration Guidelines (Prerequisite)) must be done in the switches R1, R2, R3 and R4 before configuring OSPF.

1. To test the behavior of route selection, when distance command is applied to the OSPF router, execute the following commands in R1, R2, R3 and R4.

R1:

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.1*

UltOs(config-router)# ASBR Router

UltOs(config-router)# network *13.0.0.1* **area** *0.0.0.0*

UltOs(config-router)# end

UltOs#

UltOs# configure terminal

UltOs(config)# router rip

UltOs(config-router)# network *12.0.0.1*

UltOs(config-router)#end

UltOs#

R2:

UltOs# configure terminal

UltOs(config)# router rip

UltOs(config-router)# network *12.0.0.2*

UltOs(config-router)# network *24.0.0.2*

UltOs(config-router)#end

UltOs#

R3:

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.2*

UltOs(config-router)# network *13.0.0.3* **area** *0.0.0.0*

UltOs(config-router)# network *34.0.0.3* **area** *0.0.0.0*

UltOs(config-router)# end

UltOs#

R4:

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.3*

UltOs(config-router)# network *34.0.0.4* **area** *0.0.0.0*

UltOs(config-router)# end

UltOs#

UltOs# configure terminal

UltOs(config)# router rip

UltOs(config-router)# network *24.0.0.4*

UltOs(config-router)#end

2. Configure the route-map aa with a match criteria at R4.

UltOs# configure terminal

UltOs(config)# route-map *aa* **permit** *1*

UltOs(config-rmap-aa)# match source ip *34.0.0.3 255.0.0.0*

UltOs(config-rmap-aa)# exit

UltOs(config)# exit

3. Apply redistribute all to RIP and OSPF routers at R4.

UltOs(config)# router ospf

UltOs(config-router)# redistribute all

UltOs(config-router)#end

UltOs#

UltOs(config)# router rip

UltOs(config-router)# redistribute all

UltOs(config-router)#end

4. View the routes at R4.

UltOs# show ip route

Vrf Name: default

C 12.0.0.0/8 is directly connected, vlan1

O 13.0.0.0/8 [2] via 34.0.0.3

O 15.0.0.0/8 [10] via 34.0.0.3

C 24.0.0.0/8 is directly connected, vlan24

C 34.0.0.0/8 is directly connected, vlan34

O 70.0.0.0/8 [10] via 34.0.0.3

5. Set the administrative distance 130 to the OSPF router in R4.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# distance *130* **route-map** *aa*

UltOs(config-router)# exit

6. Force routes updates in R1.

UltOs(config)# router ospf

UltOs(config-router)# no redistribute all

UltOs(config-router)# redistribute all

UltOs(config-router)# exit

UltOs(config)# router rip

UltOs(config-router)# no redistribute all

UltOs(config-router)# redistribute all

UltOs(config-router)# exit

7. View the routes at R4.

UltOs# show ip route

C 12.0.0.0/8 is directly connected, vlan1

O 13.0.0.0/8 [2] via 34.0.0.3

R 15.0.0.0/8 [2] via 24.0.0.2

C 24.0.0.0/8 is directly connected, vlan24

C 34.0.0.0/8 is directly connected, vlan34

R 70.0.0.0/8 [5] via 24.0.0.2

8. Reset the administrative distance to the OSPF router in R4.

UltOs# configure terminal

UltOs(config)# router ospf

UltOs(config-router)# no distance *130* **route-map** *aa*

UltOs(config-router)# exit

9. Force routes updates in R1.

UltOs(config)# router ospf

UltOs(config-router)# no redistribute all

UltOs(config-router)# redistribute all

UltOs(config-router)# exit

UltOs(config)# router rip

UltOs(config-router)# no redistribute all

UltOs(config-router)# redistribute all

UltOs(config-router)# exit

10. View the routes at R4.

UltOs# show ip route

C 12.0.0.0/8 is directly connected, vlan1

O 13.0.0.0/8 [2] via 34.0.0.3

O 15.0.0.0/8 [10] via 34.0.0.3

C 24.0.0.0/8 is directly connected, vlan24

C 34.0.0.0/8 is directly connected, vlan34

O 70.0.0.0/8 [10] via 34.0.0.3

15.5.14.6 Redistribution Topology

This section provides the sample configuration for testing redistribution of routes into OSPF with route map.

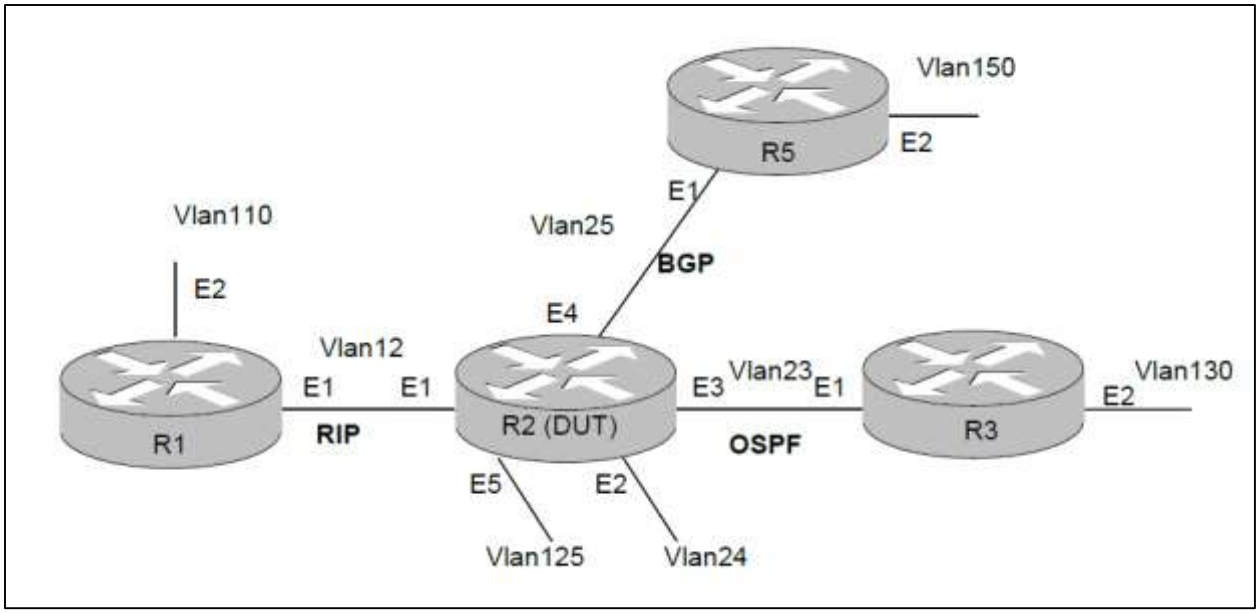


Figure 15-8: Redistribution Topology Configuration

15.5.14.6.1 Redistribution Interface Configuration

Table 15-3: IPv4 Addresses of Interfaces in the Routers – Redistribution Topology

Router	Interface	Port	IPv4 Address / Mask
R1	Vlan 12	Tagged ports E1	140.0.0.1/16
	Vlan 110	Tagged ports E2	70.0.0.1/8
R2	Vlan 12	Tagged ports E1	140.0.0.2/16
	Vlan 23	Tagged ports E3	20.0.0.2/8
	Vlan 24	Tagged ports E2	60.0.0.2/8
	Vlan 25	Tagged ports E4	40.0.0.2/8
	Vlan 125	Tagged ports E5	50.0.0.2/8
R3	Vlan 23	Tagged ports E1	20.0.0.3/8
	Vlan 130	Tagged ports E2	11.0.0.3/8
R5	Vlan 25	Tagged ports E1	40.0.0.5/8
	Vlan 150	Tagged ports E2	14.1.0.5/16

15.5.14.6.2 Redistribution Protocol Configuration

Configuration

Protocol Configuration:

Configure the protocols in the given interfaces in each of the routers as follows:

At R1

Interface Vlan 12

Enable RIPv2.

Enable RIPng.

At R2

Interface Vlan 12

Enable RIPv2.

Enable RIPng.

Interface Vlan 23

Enable OSPFv2 with Area 0. Configure this as the ASBR router.

Enable OSPFv3 with Area 0. Configure this as the ASBR router.

Interface Vlan 25

Enable BGP with peer Vlan 25 interface on R5 with remote AS 300.

At R3

Interface Vlan 23

Enable OSPFv2 with Area 0.

Enable OSPFv3 with Area 0.

At R5

Interface Vlan 25

Enable BGP with peer as VLAN 25 interface on R2 with remote AS 100.

1. To test the following behaviors, execute the following commands:

redistribution of static routes into OSPFv2 with the route map with <match destination ip> clause.

redistribution of static routes into OSPFv2, when the route map is modified or deleted.

redistribution of static routes into OSPFv2, when static routes for redistribution are added or deleted.

Configurations at R1:

UltOs(config)# router rip

UltOs(config-router)# network *140.0.0.1*

UltOs(config-router)# exit

Configurations at R2:

UltOs(config)# router rip

UltOs(config-router)# network *140.0.0.2*

UltOs(config-router)# exit

UltOs(config)#

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.1*

UltOs(config-router)# ASBR Router

UltOs(config-router)# network *20.0.0.2* **area** *0.0.0.0*

UltOs(config-router)# exit

UltOs(config)# as-num *100*

UltOs(config)# router-id *40.0.0.2*

UltOs(config-router)# neighbor *40.0.0.5* **remote-as** *300*

UltOs(config-router)# exit

Configurations at R3

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.2*

UltOs(config-router)# network *20.0.0.3* **area** *0.0.0.0*

UltOs(config-router)# exit

Configurations at R5

UltOs(config)# as-num *300*

UltOs(config)# router-id *40.0.0.5*

UltOs(config-router)# neighbor *40.0.0.2* **remote-as** *100*

UltOs(config-router)# exit

2. Do the following configurations in R2

In R2, create static routes and create a route-map aa.

UltOs(config)# ip route *91.0.0.0 255.0.0.0* **vlan** *24*

UltOs(config)# ip route *92.0.0.0 255.0.0.0* **vlan** *24*

UltOs(config)# route-map *aa* **permit** *1*

UltOs(config-rmap-aa)# match destination ip *91.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)# end

UltOs#configure terminal

UltOs(config)# route-map *aa* **deny** *2*

UltOs(config-rmap-aa)# match destination ip *93.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)#

3. Enable redistribution of static routes into OSPFv2 with route map aa.

UltOs(config)# router ospf

UltOs(config-router)# redistribute static route-map *aa*

4. Verify the route in R3, verify 91.0.0.0/8 is present in the general routing table.

UltOs# show ip route

Vrf Name: default

C 11.0.0.0/8 is directly connected, vlan130

C 12.0.0.0/8 is directly connected, vlan1

C 20.0.0.0/8 is directly connected, vlan23

O 91.0.0.0/8 [10] via 20.0.0.2

5. In R2, modify the route map aa.

UltOs# configure terminal

UltOs(config)# route-map *aa* **permit** *1*

UltOs(config-rmap-aa)# no match destination ip *91.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)# match destination ip *92.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)# exit

6. In R3, verify 91.0.0.0/8 is removed from the general routing table and 92.0.0.0/8 is present in the general routing table.

UltOs# show ip route

Vrf Name: default

C 11.0.0.0/8 is directly connected, vlan130

C 12.0.0.0/8 is directly connected, vlan1

C 20.0.0.0/8 is directly connected, vlan23

O 92.0.0.0/8 [10] via 20.0.0.2

7. In R2, add/remove static routes.

UltOs# configure terminal

UltOs(config)# ip route *93.0.0.0 255.0.0.0* **vlan** *24*

UltOs(config)# no ip route *92.0.0.0 255.0.0.0* **vlan** *24*

UltOs(config)# end

8. In R3, verify 92.0.0.0/8 is removed from the general routing table and verify 93.0.0.0/8 is present in the general routing table.

UltOs# show ip route

Vrf Name: default

C 11.0.0.0/8 is directly connected, vlan130

C 12.0.0.0/8 is directly connected, vlan1

C 20.0.0.0/8 is directly connected, vlan23

O 93.0.0.0/8 [10] via 20.0.0.2

9. Delete the route map aa.

UltOs# configure terminal

UltOs(config)# no route-map *aa 1*

UltOs(config)# no route-map *aa 2*

UltOs(config)# end

10. In R3, verify that all the connected routes and static routes are present in the general routing table.

UltOs# show ip route

Vrf Name: default

C 11.0.0.0/8 is directly connected, vlan130

C 12.0.0.0/8 is directly connected, vlan1

C 20.0.0.0/8 is directly connected, vlan23

O 91.0.0.0/8 [10] via 20.0.0.2

O 93.0.0.0/8 [10] via 20.0.0.2

15.5.14.7 OSPF Inbound Filtering with Route Map

This section provides the sample configuration for testing OSPF inbound filtering with route map.

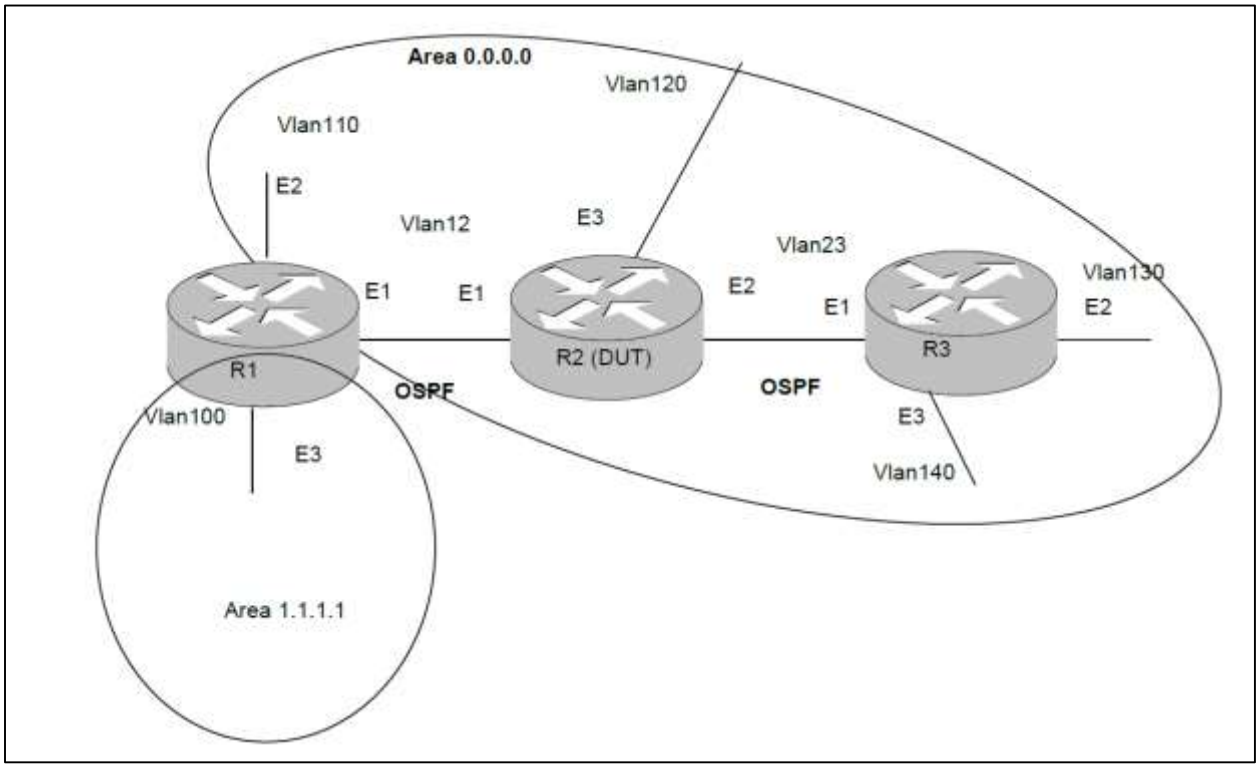


Figure 15-9: Distribute-list In Topology Configurations

15.5.14.7.1 Interface Configuration

Table 15-4: IPv4 Addresses of Interfaces in the Routers – OSPF Inbound Filtering

Router	Interface	Port	IPv4 Address / Mask
R1	Vlan 12	Tagged ports E1	10.0.0.1/8
	Vlan 100	Tagged ports E3	20.0.0.1/8
	Vlan 110	Tagged ports E2	130.0.0.1/8
R2	Vlan 12	Tagged ports E1	10.0.0.2/8
	Vlan 23	Tagged ports E2	30.0.0.2/8
	Vlan 120	Tagged ports E3	100.0.0.2/8
R3	Vlan 23	Tagged ports E1	30.0.0.3/8
	Vlan 130	Tagged ports E2	120.0.0.3/8
	Vlan 140	Tagged ports E3	150.0.0.3/8

15.5.14.7.2 Protocol Configuration

Configure the protocol in the given interfaces in each of the routers as follows:

At R1

Configure this as ASBR router.

Interface Vlan 12

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

Interface Vlan 100

Enable OSPFv2/OSPFv3 with Area 1.1.1.1.

Interface Vlan 110

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

At R2

Interface Vlan 12

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

Interface Vlan 23

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

Interface Vlan 120

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

At R3

Configure this as ASBR router.

Interface Vlan 23

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

Interface Vlan 130

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

Interface Vlan 140

Enable OSPFv2/OSPFv3 with Area 0.0.0.0.

1. Do the following configurations in R1, R2 and R3.

Configurations at R1

Configure R1 as ASBR Router.

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.1*

UltOs(config-router)# network *10.0.0.1* **area** *0.0.0.0*

UltOs(config-router)# network *130.0.0.1* **area** *0.0.0.0*

UltOs(config-router)# network *20.0.0.1* **area** *1.1.1.1*

UltOs(config-router)# exit

Configurations at R2

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.2*

UltOs(config-router)# network *10.0.0.2* **area** *0.0.0.0*

UltOs(config-router)# network *30.0.0.2* **area** *0.0.0.0*

UltOs(config-router)# network *100.0.0.2* **area** *0.0.0.0*

UltOs(config-router)# exit

Configurations at R3

UltOs(config)# router ospf

UltOs(config-router)# router-id *0.0.0.3*

UltOs(config-router)# network *30.0.0.3* **area** *0.0.0.0*

UltOs(config-router)# network *120.0.0.3* **area** *0.0.0.0*

UltOs(config-router)# network *150.0.0.3* **area** *1.1.1.1*

UltOs(config-router)# exit

2. In R3, create static routes and enable redistribution of static routes.

UltOs# configure terminal

UltOs(config)# ip route *91.0.0.0 255.0.0.0 40.0.24.4*

UltOs(config)#

UltOs(config)# router ospf

UltOs(config-router)# redistribute static

UltOs(config-router)# end

3. In R2, shutdown interfaces Vlan12 and Vlan23.

UltOs(config-router)# end

UltOs#configure terminal

UltOs(config)# interface vlan *12*

UltOs(config-if)# shutdown

UltOs(config-if)# end

UltOs# configure terminal

UltOs(config)# interface vlan *23*

UltOs(config-if)# shutdown

UltOs(config-if)#

4. In R2, create route map aa and enable incoming filtering of routes in OSPFv2 with route map aa.

UltOs# configure terminal

UltOs(config)# route-map *aa* **permit** *10*

UltOs(config-rmap-aa)# exit

UltOs(config)# route-map *aa* **deny** *1*

UltOs(config-rmap-aa)# match destination ip *150.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)# match destination ip *91.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)# end

UltOs(config)# router ospf

UltOs(config-router)# distribute-list route-map *aa* **in**

UltOs(config-router)#

5. Start interfaces Vlan12 and Vlan23.

UltOs(config)# interface vlan *12*

UltOs(config-if)# no shutdown

UltOs(config-if)# end

UltOs(config-if)# configure terminal

UltOs(config)# interface vlan *23*

UltOs(config-if)# no shutdown

UltOs(config-if)#end

6. Wait for one minute for all the route updates, and verify the routes in R2.

UltOs# show ip route

Vrf Name: default

C 10.0.0.0/8 is directly connected, vlan12

C 12.0.0.0/8 is directly connected, vlan1

O 20.0.0.0/8 [2] via 10.0.0.1

C 30.0.0.0/8 is directly connected, vlan23

C 100.0.0.0/8 is directly connected, vlan120

O 120.0.0.0/8 [2] via 30.0.0.3

O 130.0.0.0/8 [2] via 10.0.0.1

7. In R2, shutdown interfaces: Vlan12 and Vlan23.

UltOs# configure terminal

UltOs(config)# interface vlan *12*

UltOs(config-if)# shutdown

UltOs(config-if)# end

UltOs# configure terminal

UltOs(config)# interface vlan *23*

UltOs(config-if)# shutdown

8. Modify the route map aa.

UltOs# configure terminal

UltOs(config)# route-map *aa* **deny** *1*

UltOs(config-rmap-aa)# no match destination ip *150.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)# match destination ip *130.0.0.0 255.0.0.0*

UltOs(config-rmap-aa)# end

9. Start interfaces Vlan12 and Vlan23.

UltOs(config)# interface vlan *12*

UltOs(config-if)# no shutdown

UltOs(config-if)# end

UltOs(config-if)# configure terminal

UltOs(config)# interface vlan *23*

UltOs(config-if)# no shutdown

UltOs(config-if)#end

10. Wait for one minute for all the route updates and verify the routes in R2.

UltOs# show ip route

C 10.0.0.0/8 is directly connected, vlan12

C 12.0.0.0/8 is directly connected, vlan1

O 20.0.0.0/8 [2] via 10.0.0.1

C 30.0.0.0/8 is directly connected, vlan23

C 100.0.0.0/8 is directly connected, vlan120

O 120.0.0.0/8 [2] via 30.0.0.3

O 150.0.0.0/8 [2] via 30.0.0.3

11. In R2, shutdown interfaces Vlan12 and Vlan23.

UltOs(config-router)# end; configure terminal

UltOs(config)# interface vlan *12*

UltOs(config-if)# shutdown

UltOs(config-if)# end

UltOs# configure terminal

UltOs(config)# interface vlan *23*

UltOs(config-if)# shutdown

12. Delete the route map aa.

    UltOs# configure terminal

    UltOs(config)# no route-map *aa 1*

    UltOs(config)# end

13. Start interfaces Vlan12 and Vlan23.

    UltOs(config)# interface vlan *12*

    UltOs(config-if)# no shutdown

    UltOs(config-if)# end

    UltOs(config-if)# configure terminal

    UltOs(config)# interface vlan *23*

    UltOs(config-if)# no shutdown

    UltOs(config-if)#end

14. Wait for one minute for all the route updates, and verify the routes in R2.

    UltOs# show ip route

    Vrf Name: default

    C 10.0.0.0/8 is directly connected, vlan12

    C 12.0.0.0/8 is directly connected, vlan1

    O 20.0.0.0/8 [2] via 10.0.0.1

    C 30.0.0.0/8 is directly connected, vlan23

    O 91.0.0.0/8 [10] via 30.0.0.2

    C 100.0.0.0/8 is directly connected, vlan120

    O 120.0.0.0/8 [2] via 30.0.0.3

    O 130.0.0.0/8 [2] via 10.0.0.1

    O 150.0.0.0/8 [2] via 30.0.0.3

Chapter 16

DHCP Relay Agent

16.1 Protocol Description

DHCP relay agent is used to forward the DHCP packets between client and server when they are not in the same subnets. The relay receives packets from the client and inserts certain information like the network in which the packet is received and then forwards it to the server. The Server identifies the client's network from this information and allocates IP accordingly, then sends the reply to the relay. The Relay then strips the information inserted and broadcasts the packets into the client's network.

16.2 Topology

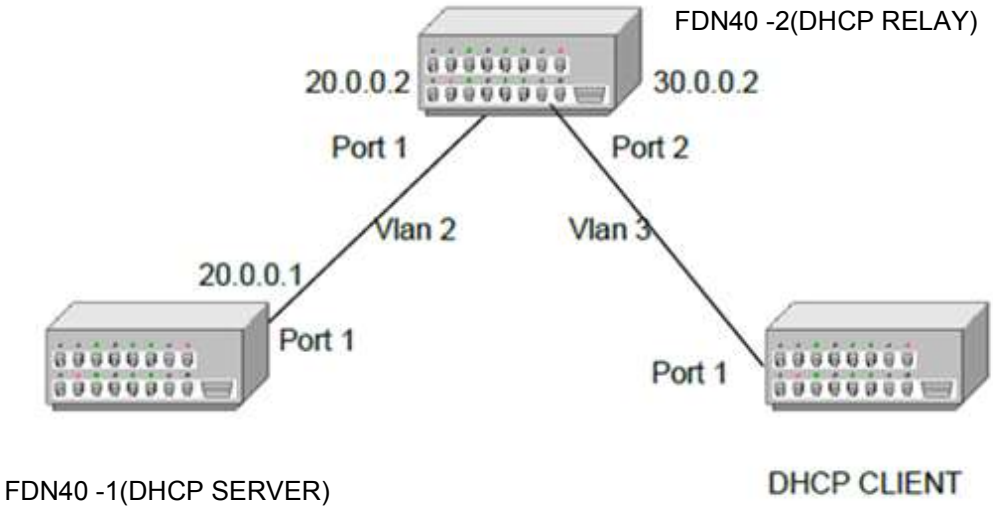


Figure 16-1: DHCP – Topology

16.3 Configuration Guidelines

The following sections describe the configuration of **DHCP** running as a part of **ULTERIUS FDN40.**

- DHCP Server must be disabled before enabling the DHCP Relay agent.
- Only when enabled, the Relay Agent,
  - becomes active
  - forwards the packets from the client to a specific DHCP server
  - does any processing related to Relay Agent Information Options - like inserting the necessary options while relaying a packet from a client to a server and examining/stripping of options when relaying a packet from a server to a client

16.4 Default Configurations

Table 16-1: Default Configurations

Feature	Default Setting
DHCP server status	Disabled
ICMP echo	Disabled
Offer reuse time out	5 seconds

Feature	Default Setting
DHCP next server address	0.0.0.0 (none)
Boot file name	None
DHCP server pool lease time	3600 seconds
DHCP server pool utilization threshold	75%
DHCP server debug level	None
DHCP relay status	Disabled
DHCP relay server address	0.0.0.0 (none)
RAI option	Disabled
DHCP relay debug level	None
DHCP client debug level	None

16.5 Enabling DHCP Relay

16.5.1.1 CLI Configuration

Refer Figure 16-1 for Topology Setup. DHCP relay is disabled by default.

a. Execute the following commands in FDN40-2 to enable DHCP Relay.

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable the DHCP server.

  UltOs(config)# service dhcp-relay

- Exit from the Global configuration mode.

  UltOs(config)# end

b. View the DHCP relay status using the following command.

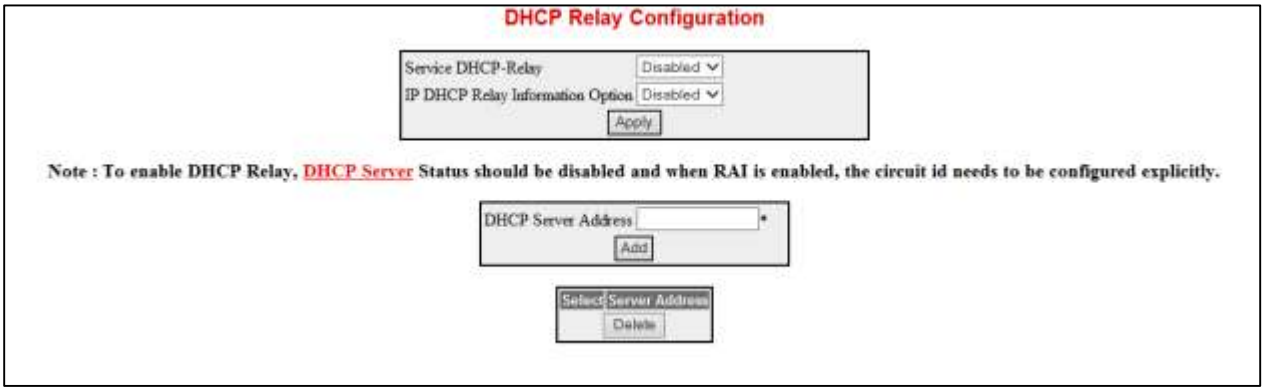
UltOs# show ip dhcp relay information

```
The output in the switch is
Dhcp Relay                  : Enabled
Dhcp Relay Servers only     : Disabled
DHCP server                 : 0.0.0.0
Dhcp Relay RAI option       : Disabled
Default Circuit Id information : router-index
Debug Level                 : 0x1
No of Packets inserted RAI option              : 0
No of Packets inserted circuit ID suboption    : 0
No of Packets inserted remote ID suboption     : 0
No of Packets inserted subnet mask suboption   : 0
```

```
No of Packets dropped                              : 0
No of Packets which did not inserted RAI option : 0
```

16.5.1.2 WEB Configuration

DHCP Relay can be enabled through WEB interface using the **DHCP Relay Configuration** screen (Navigation – **Layer3 Management > DHCP Relay > Basic Settings)**



Screen 16-1: DHCP Relay Configuration

16.6 Configuring a DHCP Server Address

16.6.1.1 CLI Configuration

Refer Figure 16-1 for Topology Setup.

DHCP server address can be configured in the DHCP Relay Agent using the following commands. A maximum of 5 servers can be configured. If no servers are configured, then the DHCP packets will be broadcasted to entire network, except to the network from which packet is received.

1. Execute the following commands to configure a DHCP Server Address.
   - Enter into the global configuration mode.

     UltOs# configure terminal
   - Configure DHCP server address.

     UltOs(config)# ip dhcp server *20.0.0.1*
   - Exit from the Global configuration mode.

     UltOs(config)# end
2. View the server address configured in the relay using the following command.

   UltOs# show ip dhcp relay information

```
The output in the switch is
Dhcp Relay                    : Enabled
Dhcp Relay Servers only       : Enabled
DHCP server 1                 : 20.0.0.1
```

```
Dhcp Relay RAI option       : Disabled
Default Circuit Id information : router-index
Debug Level                 : 0x1
No of Packets inserted RAI option              : 0
No of Packets inserted circuit ID suboption    : 0
No of Packets inserted remote ID suboption     : 0
No of Packets inserted subnet mask suboption   : 0
No of Packets dropped                          : 0
No of Packets which did not inserted RAI option : 0
```

16.6.1.2 WEB Configuration

DHCP Server Address can be configured through WEB interface using the **DHCP Relay Configuration** screen.(Navigation – **Layer3 Management > DHCP Relay > Basic Settings)**

For screenshot, refer section 16.5.1.2

16.7 Enabling Relay Agent Information

16.7.1.1 CLI Configuration

Refer Figure 16-1 for the Topology Setup.

1. Execute the following commands to enable the Relay agent information option in FDN40-2.
   - Enter into the Global configuration mode.

     UltOs# configure terminal
   - Configure DHCP server address.

     UltOs(config)# ip dhcp relay information option
   - Exit from the Global configuration mode.

     UltOs(config)# end
2. View the Relay Agent information option status using the following command.

   UltOs# show ip dhcp relay information

```
The output in the Switch is
Dhcp Relay                  : Enabled
Dhcp Relay Servers only     : Enabled
DHCP server 1               : 20.0.0.1
Dhcp Relay RAI option       : Enabled
Default Circuit Id information : router-index
Debug Level                 : 0x1
No of Packets inserted RAI option              : 0
```

```
No of Packets inserted circuit ID suboption     : 0
No of Packets inserted remote ID suboption      : 0
No of Packets inserted subnet mask suboption    : 0
No of Packets dropped                           : 0
No of Packets which did not inserted RAI option : 0
```

16.7.1.2 WEB Configuration

Relay Agent Information can be enabled through WEB interface using the **DHCP Relay Configuration** screen.(Navigation – **Layer3 Management > DHCP Relay > Basic Settings)**

For screenshot, refer section 16.5.1.2

16.8 Configuring Relay Agent Sub-options

16.8.1.1 CLI Configuration

Refer Figure 16-1 for the Topology Setup.

1. Execute the following commands to configure Circuit-id and Remote-id Relay agent information option in FDN40-2.
   - Enter into the Global Configuration mode.

     UltOs# configure terminal
   - Enter into the VLAN Interface Configuration mode.

     UltOs(config)# interface vlan *1*
   - Execute the following commands to configure the Circuit-id sub-option and the Remote-id sub-option.

     UltOs(config-if)# ip dhcp relay circuit-id *340*

     UltOs(config-if)# ip dhcp relay remote-id *hello*
   - Exit from the VLAN Interface Configuration mode.

     UltOs(config-if)# end
2. Execute the following show command to view the Relay Agent information option.

   UltOs# show ip dhcp relay information

```
The output in the Switch is
Dhcp Relay                  : Enabled
Dhcp Relay Servers only     : Enabled
DHCP server 1               : 20.0.0.1
Dhcp Relay RAI option       : Enabled
Default Circuit Id information : router-index
Debug Level                 : 0x1
No of Packets inserted RAI option              : 0
```

```
No of Packets inserted circuit ID suboption     : 0
No of Packets inserted remote ID suboption      : 0
No of Packets inserted subnet mask suboption    : 0
No of Packets dropped                           : 0
No of Packets which did not inserted RAI option : 0
 Interface  vlan1
Circuit ID : 340
Remote  ID : hello
```

UltOs# show ip dhcp relay information vlan *1*

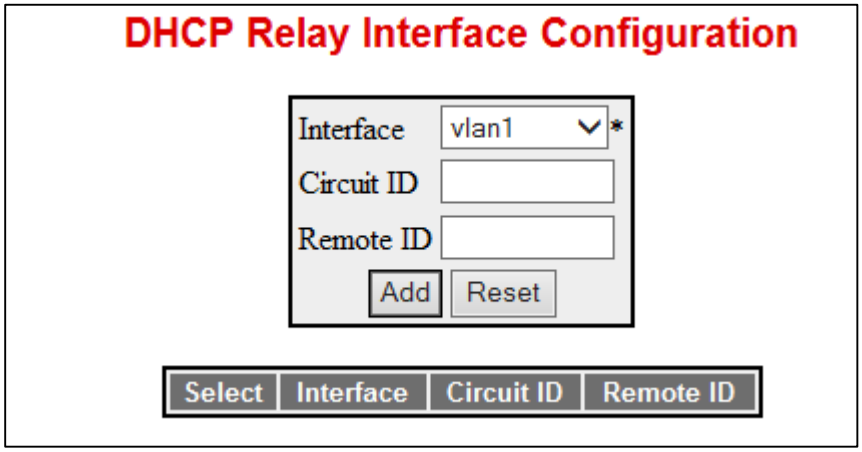
```
Interface vlan1
Circuit ID : 340
Remote ID : hello
```

Configuration of DHCP Relay circuit ID should be greater than the value of the macro DHRL_MAX_L3_IF_INDEX.

The value of the macro DHRL_MAX_L3_IF_INDEX is different for FDN40 packages. For METRO package the value of macro is 1136 and for Enterprise package, the value of macro is 160.

16.8.1.2 WEB Configuration

Relay Agent Sub-options can be configured through WEB interface using the **DHCP Relay Interface Configuration** screen (Navigation – **Layer3 Management > DHCP Relay > Interface Settings)**



Screen 16-2: DHCP Relay Interface Configuration

16.9 Enabling Traces for DHCP Relay

Refer Figure 16-1 for Topology Setup.

1. Execute the following commands in FDN40-2 to enable DHCP relay debug traces.

   UltOs# debug ip dhcp relay *all*

2. View the debug trace level.

UltOs# show ip dhcp relay information

```
Dhcp Relay                    : Enabled
Dhcp Relay Servers only       : Enabled
DHCP server 1                 : 20.0.0.1
Dhcp Relay RAI option         : Enabled
Default Circuit Id information : router-index
Debug Level                   : 0xff
No of Packets inserted RAI option                : 0
No of Packets inserted circuit ID suboption      : 0
No of Packets inserted remote ID suboption       : 0
No of Packets inserted subnet mask suboption     : 0
No of Packets dropped                            : 0
No of Packets which did not inserted RAI option : 0
 Interface  vlan1
Circuit ID : 340
Remote  ID : hello
```

16.10 Acquiring IP from a Server Residing Outside the Client Network

Refer Figure 16-1 for the Topology Setup.

Connect Port 1 of FDN40-1 to Port 1 of FDN40-2 and connect Port 2 of FDN40-2 to Port 1 of DHCP client.

1. Create vlan2 in FDN40-1 with Port 1 as member port. Then, add a route to 30.0.0.0 network though 20.0.0.2 (FDN40-2).

UltOs# configure terminal

UltOs(config)# vlan *2*

UltOs(config-vlan)# ports lan *0/1* **untagged lan** 0/1

UltOs(config-vlan)# exit

UltOs(config)# interface vlan *2*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *20.0.0.1 255.0.0.0*

UltOs(config-if)# no shutdown

UltOs(config-vlan)# exit

UltOs(config)# interface lan *0/1*

UltOs(config-if)# switchport pvid *2*

UltOs(config-vlan)# exit

UltOs(config)# ip route *30.0.0.0 255.0.0.0 20.0.0.2*

UltOs(config) # end

2. View the VLAN configurations and route configuration using the following commands.

UltOs# show ip interface vlan *2*

```
vlan2 is up, line protocol is up
Internet Address is 20.0.0.1/8
Broadcast Address 20.255.255.255
```

UltOs# show vlan id *2*

```
Vlan database
-------------
Vlan ID              : 2
Member Ports         : lan0/1
Untagged Ports       : lan0/1
Forbidden Ports      : None
Name                 : lan
Status               : Permanent
Egress Ethertype     : 0x8100
MacLearning Admin-Status  : Disabled
MacLearning Oper-Status   : Enabled
------------------------------------------------
```

UltOs# show ip route

```
C 12.0.0.0/8 is directly connected, vlan1
C 20.0.0.0/8 is directly connected, vlan2
S 30.0.0.0/8 [1] via 20.0.0.2
```

3. Create vlan2 with port1 as member port and vlan3 with port2 as member port in FDN40-2.

UltOs# configure terminal

UltOs(config)# vlan *2*

UltOs(config-vlan)# ports lan *0/1* **untagged lan** 0/1

UltOs(config-vlan)# exit

UltOs(config)# interface vlan *2*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *20.0.0.2 255.0.0.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# interface lan *0/1*

UltOs(config-if)# switchport pvid *2*

UltOs(config-if)# exit

UltOs(config)# vlan *3*

UltOs(config-vlan)# ports lan *0/2* **untagged lan** *0/2*

UltOs(config-vlan)# exit

UltOs(config)# interface vlan *3*

UltOs(config-if)# shutdown

UltOs(config-if)# ip address *30.0.0.2 255.0.0.0*

UltOs(config-if)# no shutdown

UltOs(config-if)# exit

UltOs(config)# interface lan *0/2*

UltOs(config-if)# switchport pvid *3*

UltOs(config-if)# no shutdown

UltOs(config-if)# end

4. View the configuration using the following commands

UltOs# show vlan id *2*

```
Vlan database
-------------
Vlan ID              : 2
Member Ports         : lan0/1
Untagged Ports       : lan0/1
Forbidden Ports      : None
Name                 : lan
Status               : Permanent
Egress Ethertype     : 0x8100
MacLearning Admin-Status  : Disabled
MacLearning Oper-Status   : Enabled
--------------------------------------------------
```

UltOs# show vlan id *3*

```
Vlan database
-------------
Vlan ID              : 3
Member Ports         : lan0/2
Untagged Ports       : lan0/2
Forbidden Ports      : None
Name                 : lan
```

```
Status              : Permanent
Egress Ethertype    : 0x8100
MacLearning Admin-Status  : Disabled
MacLearning Oper-Status   : Enabled
-------------------------------------------------
```

UltOs# show ip interface vlan *2*

```
vlan2 is up, line protocol is up
Internet Address is 20.0.0.2/8
Broadcast Address 20.255.255.255
```

UltOs# show ip interface vlan *3*

```
vlan3 is up, line protocol is up
Internet Address is 30.0.0.2/8
Broadcast Address 30.255.255.255
```

5. Enable DHCP server in FDN40-1. Since the client is in Vlan3, an address pool with 30.0.0.0 network needs to be configured in the Server.

   UltOs# configure terminal

   UltOs(config)# service dhcp-server

   UltOs(config)# ip dhcp pool *1*

   UltOs(dhcp-config)# network *30.0.0.0*

   UltOs(dhcp-config)# lease *0 0 30*

   UltOs(dhcp-config)# end

6. View the configuration using the following commands.

   UltOs# show ip dhcp server information

```
DHCP server status           : Enable
Send Ping Packets            : Disable
Debug level                  : None
Server Address Reuse Timeout : 5 secs
Next Server Adress           : 0.0.0.0
Boot file name               : None
```

   UltOs# show ip dhcp server pools

```
Pool Id               : 1
---------------------------------
Subnet                : 30.0.0.0
Subnet Mask           : 255.0.0.0
Lease time            : 1800 secs
Utilization threshold : 75%
Start Ip              : 30.0.0.1
```

```
End Ip                : 30.255.255.255


Subnet Options
--------------
Code       :     1, Value      : 255.0.0.0
```

7. Enable DHCP Relay in FDN40-2, which connects the networks between Client and Server.

   UltOs# configure terminal

   UltOs(config)# service dhcp-relay

   UltOs(config)# end

8. View the configuration using the following commands.

   UltOs# show ip dhcp relay information

```
Dhcp Relay              : Enabled
Dhcp Relay Servers only : Disabled
DHCP server             : 0.0.0.0
Dhcp Relay RAI option   : Disabled
Debug Level             : 0x1
No of Packets inserted RAI option               : 0
No of Packets inserted circuit ID suboption     : 0
No of Packets inserted remote ID suboption      : 0
No of Packets inserted subnet mask suboption    : 0
No of Packets dropped                           : 0
No of Packets which did not inserted RAI option : 0
```

9. Configure DHCP server address in FDN40-2.

   UltOs(config)# ip dhcp server *20.0.0.1*

   UltOs(config)# end

10. View the server address configured in the DHCP Relay using the following command.

    UltOs# show ip dhcp relay information

```
The output in the switch is
Dhcp Relay                  : Enabled
Dhcp Relay Servers only     : Enabled
DHCP server 1               : 20.0.0.1
Dhcp Relay RAI option       : Disabled
Default Circuit Id information : router-index
Debug Level                 : 0x1
```

```
No of Packets inserted RAI option                : 0
No of Packets inserted circuit ID suboption      : 0
No of Packets inserted remote ID suboption       : 0
No of Packets inserted subnet mask suboption     : 0
No of Packets dropped                            : 0
No of Packets which did not inserted RAI option : 0
```

11. Enable DHCP Relay Information option in FDN40-2.

    UltOs(config)# ip dhcp relay information option

    UltOs(config)# end

12. In FDN40-2 view the Relay Agent information option status using the following command.

    UltOs# show ip dhcp relay information

```
The output in the Switch is
Dhcp Relay                    : Enabled
Dhcp Relay Servers only       : Enabled
DHCP server 1                 : 20.0.0.1
Dhcp Relay RAI option         : Enabled
Default Circuit Id information : router-index
Debug Level                   : 0x1
No of Packets inserted RAI option                : 0
No of Packets inserted circuit ID suboption      : 0
No of Packets inserted remote ID suboption       : 0
No of Packets inserted subnet mask suboption     : 0
No of Packets dropped                            : 0
No of Packets which did not inserted RAI option : 0
```

13. In FDN40-2 execute the following commands to configure the Circuit-id sub-option and the Remote-id sub-option.

    UltOs(config)# interface vlan *2*

    UltOs(config-if)# ip dhcp relay circuit-id *340*

    UltOs(config-if)# ip dhcp relay remote-id *hello*

    UltOs(config-if)# end

14. In FDN40-2 execute the following show command to view the Relay Agent information option.

    UltOs# show ip dhcp relay information

```
The output in the Switch is
Dhcp Relay                    : Enabled
Dhcp Relay Servers only       : Enabled
DHCP server 1                 : 20.0.0.1
```

```
Dhcp Relay RAI option       : Enabled
Default Circuit Id information : router-index
Debug Level                 : 0x1
No of Packets inserted RAI option              : 0
No of Packets inserted circuit ID suboption    : 0
No of Packets inserted remote ID suboption     : 0
No of Packets inserted subnet mask suboption   : 0
No of Packets dropped                          : 0
No of Packets which did not inserted RAI option : 0
 Interface  vlan2
Circuit ID : 340
Remote  ID : hello
```

UltOs# show ip dhcp relay information vlan *2*

```
Interface vlan2
Circuit ID : 340
Remote ID : hello
```

15. Enable DHCP Client to get the IP address from the DHCP server (FDN40-2) via DHCP Relay (FDN40-1).

Chapter 17

RAVPN

17.1 Protocol Description

RAVPN (acronym for Client to Site VPN) connects individual hosts to private networks. In a Remote Access VPN, every host must have VPN client software. Whenever the host tries to send any traffic, the VPN client software encapsulates and encrypts that traffic before sending it over the Internet to the VPN gateway at the edge of the target network. If the target host inside the private network returns a response, the VPN gateway performs the reverse process to send an encrypted response back to the VPN client over the Internet. These remote access VPNs may use passwords, or other cryptographic methods. The most common secure tunneling protocol IPSec is deployed in RAVPN.

Remote-Access VPNs allow employees to access their company's intranet from home or while traveling outside the office, where as site-to-site VPNs allow employees in geographically disparate offices to share one cohesive virtual network.

17.2 Topology

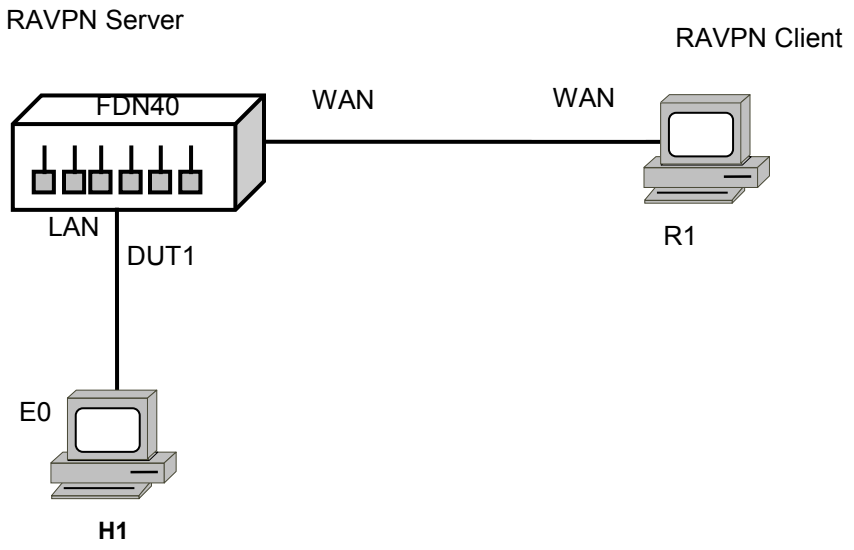


Figure 17-1: RAVPN - Topology

Node	Interface Index/Name	Interface IP Address
DUT1	WAN	35.0.0.1
R1	WAN	35.0.0.2
H1	E0	192.168.1.10
DUT1	LAN	192.168.1.1

17.3 RAVPN Configurations

17.3.1 Enabling VPN Module

The VPN (Virtual Private Network) module is enabled for encryption and decryption of the traffic flows. This section describes the steps involved in enabling the VPN module globally and configuring a VPN policy. This section also describes the verifying of the configuration using corresponding show command.

17.3.1.1 CLI Configuration

To enable VPN globally

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enable the VPN module.

UltOs(config)# set vpn enable

- Exit from the Global Configuration mode.

UltOs(config)# end

To view the VPN global status

- View the global VPN settings.

UltOs# show vpn config

```
VPN Global Configuration
------------------------
IPSecurity Status            : Enabled
Maximum Number of Tunnels    : 100
Number of Tunnels configured : 1
Number of Tunnels Established: 1
```

17.3.1.2 WEB Configuration

VPN can be enabled / disabled using the **VPN Policy** screen (Navigation - **Security Management > VPN > VPN Settings > VPN Policy)**

Screen 17-1: VPN Policy - VPN Module Status

17.3.2 Configuring pool IP address

17.3.2.1 CLI Configuration

To create a pool ip address

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Create the pool IP address

  UltOs# ip ra-vpn pool ravpnpool 192.168.2.1 – 192.168.2.2

- Exit from the Crypto Map Configuration mode.

  UltOs# end

To view the pool IP address

- View the pool ip

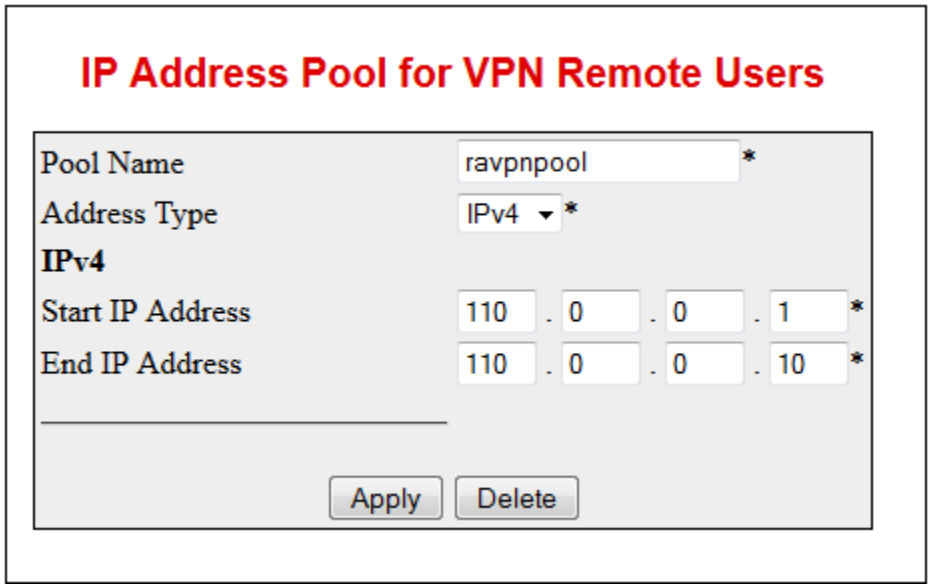
UltOs# show ra-vpn address-pool

```
Address PoolName  Start Ip  End Ip Prefix length
```

```
---------------- ---------- -------- -----------
  ravpnpool      192.168.2.1 192.168.2.2     8
```

17.3.2.2 WEB Configuration

RAVPN Pool can be created using the **Address Pool** screen (Navigation - **Security Management > VPN > Users >Address Pool)**



Screen 17-2: RAVPN Pool IP Address configuration

17.3.3 Configuring RAVPN Policy Type

The VPN policy type defines the policy to be imposed for the authentication of the users. The different policy types available are IPSec manual, preshared key, extended authentication, certificate and RA VPN key.

This section describes the steps involved in configuring VPN policy type.

17.3.3.1 CLI Configuration

To configure RAVPN policy type

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Crypto Map Configuration mode for an existing policy.

  UltOs(config)# crypto map crypto_map_name

- Set the key mode as ravpn preshared key.

  UltOs(config-crypto-map)# crypto key mode ravpn-preshared-key

- Exit from the Crypto Map Configuration mode.

  UltOs(config-crypto-map)# end

To view the RAVPN policy parameters

- View the parameters of the VPN policy.

UltOs# show crypto map

```
                VPN Policy Parameters
                                    ------------------------
Policy Name                       : crypto_map_name
Policy Status                     : Inactive
Policy Type                       : ravpn preshared key
Ike Version                       : v1
Local & Remote Protected N/W's    : None <-- --> None
Security Mode                     : Tunnel
Local & Remote Tunnel Term Addr   : None <== ==> None
Interface Name                    : Not Configured
Policy Protocol                   : any
Policy Action                     : Apply
In/Out bound SPI                  : 0 / 0
Security Protocol                 : ESP
Encryption  Algo                  : Not Configured
Anti Replay                       : Disable
Crypto Session Status             : Inactive
Crypto Session Encr Pkts          : 0
Crypto Session Decr Pkts          : 0
No.of ACTIVE VPN policies         = 0
No.of VPN policies configured     = 1
```

17.3.3.2 WEB Configuration

RA-VPN policy Type can be configured using the **Client termination** screen (Navigation - **Security Management > VPN > Users > Client termination)**

Screen 17-3: RAVPN Policy Type Configuration

17.3.4 Configuring IPSec mode

The mode of the IPSec is configured based on the set up for securing the traffic. The mode can be either Tunnel or Transport.

The Tunnel mode is used to protect traffic between a SG and a host or between two security gateways. The Transport mode is used to protect traffic between a pair of hosts or security gateways.

Only the payload of the IP packet is encrypted and/or authenticated, when in transport mode. The entire IP packet is encrypted and/or authenticated, when in tunnel mode.

This section describes the steps involved in configuring the IPSec mode.

17.3.4.1 CLI Configuration

To configure the VPN policy mode

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Crypto Map Configuration mode for an existing policy.

  UltOs(config)# crypto map crypto_map_name

- Set the IPSec mode.

  UltOs(config-crypto-map)# crypto ipsec mode tunnel

- Exit from the Crypto Map Configuration mode.

  UltOs(config-crypto-map)# end

To view the VPN policy parameters

- View the parameters of the VPN policy.

  UltOs# sh crypto map

```
VPN Policy Parameters
-------------------------
```

```
Policy Name                          : crypto_map_name
Policy Status                        : Inactive
Policy Type                          : IPSec Manual
Ike Version                          : v1
Local & Remote Protected N/W's       : None <-- --> None
Security Mode                        : Tunnel
Local & Remote Tunnel Term Addr      : None <== ==> None
Interface Name                       : Not Configured
Policy Protocol                      : any
Policy Action                        : Apply
In/Out bound SPI                     : 0 / 0
Security Protocol                    : ESP
Encryption  Algo                     : Not Configured
Anti Replay                          : Disable
Crypto Session Status                : Inactive
Crypto Session Encr Pkts             : 0
Crypto Session Decr Pkts             : 0
No.of ACTIVE VPN policies           = 0
No.of VPN policies configured       = 1
```

17.3.5 Configuring Peer Identity

Peer identity refers to the destination address set in the packet during authentication and encryption of outbound datagram. This peer identity is used for IPSec SA negotiations. This section describes the steps involved in configuring the peer identity.

17.3.5.1 CLI Configuration

To configure the peer identity

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Crypto Map Configuration mode for an existing policy.

  UltOs(config)# crypto map crypto_map_name

- Set the peer identity.

  UltOs(config-crypto-map)# set peer *35.0.0.2*

- Exit from the Crypto Map Configuration mode.

  UltOs(config-crypto-map)# end

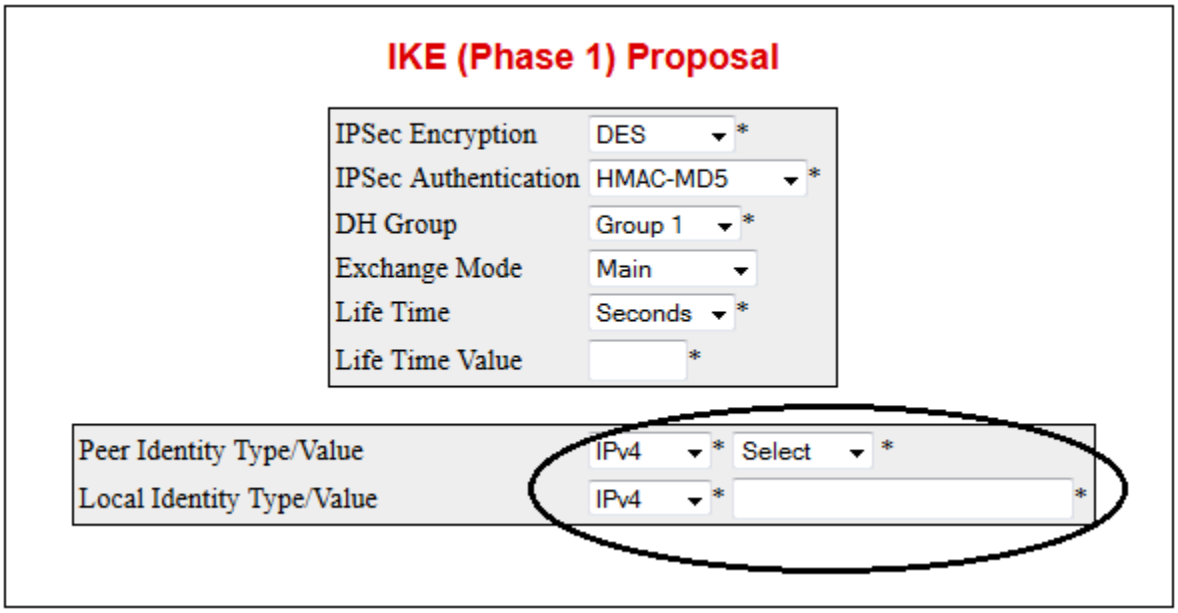
To view the VPN policy parameters

- View the parameters of the VPN policy.

```
UltOs# show crypto map                                    VPN
Policy Parameters

                          -------------------------

 Policy Name                          : crypto_map_name
 Policy Status                        : Inactive
 Policy Type                          : IPSec Manual
 Ike Version                          : v1
 Local & Remote Protected N/W's       :
198.168.1.0/24 <- -    - - > 110.0.0.0/24
 Security Mode                        : Tunnel
 Local & Remote Tunnel Term Addr      : 0.0.0.0 <== ==>
35.0.0.2
 Interface Name                       : Not Configured
 Policy Protocol                      : any
 Policy Action                        : Apply
 In/Out bound SPI                     : 0 / 0
 Security Protocol                    : ESP
 Encryption  Algo                     : Not Configured
 Anti Replay                          : Disable
 Crypto Session Status                : Inactive
 Crypto Session Encr Pkts             : 0
 Crypto Session Decr Pkts             : 0
 No.of ACTIVE VPN policies           = 0
 No.of VPN policies configured       = 1
```

17.3.5.2 WEB Configuration

RA-VPN peer identity can be created using the **Client termination** screen (Navigation - **Security Management > VPN > Users > Client termination)**



Screen 17-4: Peer Identity Configuration

17.3.6 Configuring IPSec Session Keys

The IPSec session keys are configured for a VPN policy to set the security protocol, the authentication and encryption algorithms to be applied, and the inbound and outbound security parameter index that is used to uniquely identify a SA. This section describes the steps involved in configuring the IPSec session keys.

17.3.6.1 CLI Configuration

To configure the IPSec session keys

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Crypto Map Configuration mode for an existing policy.

  UltOs(config)# crypto map crypto_map_name

- Configure the IPSec session key.

  UltOs(config-crypto-map)# set session-key authenticator esp hmac-sha1 *abcdef78123456781234567812345678123456781234567812345678* **esp des cipher** *abcdef7812345678* **outbound** *257* **inbound** *256*

- Exit from the Crypto Map Configuration mode.

  UltOs(config-crypto-map)# end

To view the VPN policy parameters

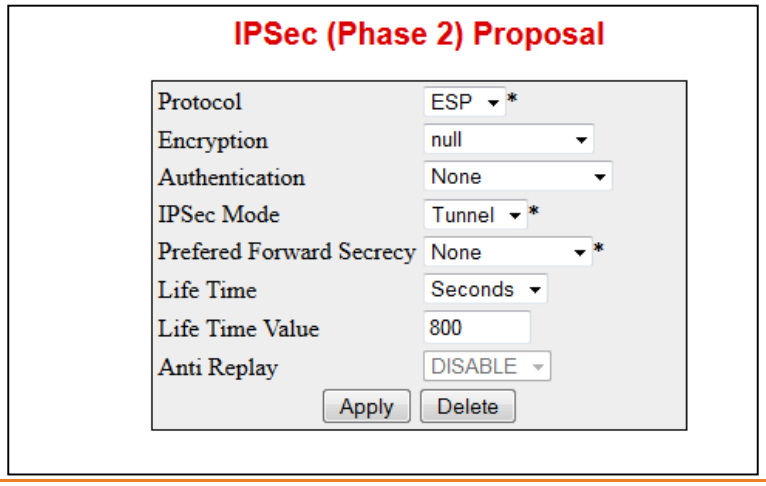
- View the parameters of the VPN policy.

  UltOs# sh crypto map

```
                    VPN Policy Parameters
                   -------------------------

 Policy Name                        : crypto_map_name
 Policy Status                      : Inactive
 Policy Type                        : IPSec Manual
 Ike Version                        : v1
 Local & Remote Protected N/W's     : None <-- --> None
 Security Mode                      : Tunnel
 Local & Remote Tunnel Term Addr    : 0.0.0.0 <== ==>
35.0.0.1
 Interface Name                     : Not Configured
 Policy Protocol                    : any
 Policy Action                      : Apply
 In/Out bound SPI                   : 256 / 257
 Security Protocol                  : ESP
 Authentication Algorithm           : HMAC-SHA1
 Encryption  Algo                   : DES
 Anti Replay                        : Disable
 Crypto Session Status              : Inactive
 Crypto Session Encr Pkts           : 0
 Crypto Session Decr Pkts           : 0
 No.of ACTIVE VPN policies          = 0
 No.of VPN policies configured      = 1
```

17.3.6.2 WEB Configuration

RA-VPN IPSec session keys can be created using the **Client termination** screen (Navigation - **Security Management > VPN > Users > Client termination)**



Screen 17-5: IPSec Session Keys Configuration

17.3.7 Configuring Access List

The access list is configured to specify the traffic type, action to be taken, and source and destination IP address to which the policy is applied. This section describes the steps involved in configuring the access list.

17.3.7.1 CLI Configuration

To configure the access list

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Crypto Map Configuration mode for an existing policy.

  UltOs(config)# crypto map crypto_map_name

- Configure the access list.

  UltOs(config-crypto-map)# access-list 1 apply any source *192.168.1.0 255.255.255.0* **destination** *192.168.2.0 255.255.255.0*

- Exit from the Crypto Map Configuration mode

  UltOs(config-crypto-map)# end

To view the VPN policy parameters

- View the parameters of the VPN policy.

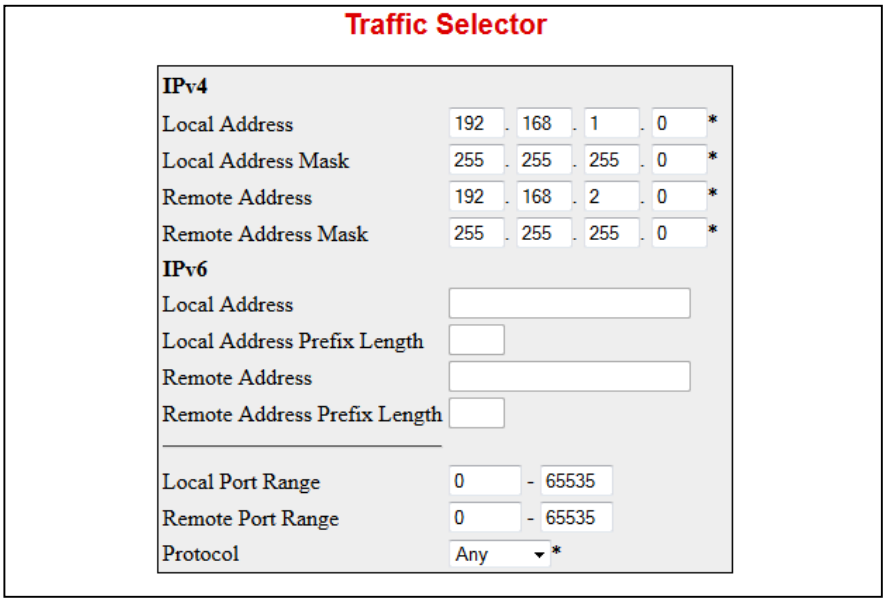
  UltOs# sh crypto map

```
                              VPN Policy Parameters
                             -------------------------

 Policy Name                        : crypto_map_name
 Policy Status                      : Inactive
 Policy Type                        : IPSec Manual
 Ike Version                        : v1
 Local & Remote Protected N/W's     : 192.168.1.0/24 <--
--> 192.168.2.0/24
 Security Mode                      : Tunnel
 Local & Remote Tunnel Term Addr    : 0.0.0.0 <== ==>
35.0.0.1
 Interface Name                     : Not Configured
 Policy Protocol                    : any
 Policy Action                      : Apply
 In/Out bound SPI                   : 256 / 257
 Security Protocol                  : ESP
 Authentication Algorithm           : HMAC-SHA1
 Encryption  Algo                   : DES
```

```
Anti Replay                          : Disable
Crypto Session Status                : Inactive
Crypto Session Encr Pkts             : 0
Crypto Session Decr Pkts             : 0
No.of ACTIVE VPN policies            = 0
No.of VPN policies configured        = 1
```

17.3.7.2 WEB Configuration

RA-VPN policy can be created using the **Client termination** screen (Navigation - **Security Management > VPN > Users > Client termination)**



Screen 17-6: Access List Configuration

17.3.8 Binding of Policy

The configured VPN policy is bound to particular WAN (Wide Area Network) interface for configuring the interface details and local tunnel termination address in the policy and for activating the VPN policy. This section describes the steps involved in binding the policy to the WAN interface

17.3.8.1 CLI Configuration

To bind a policy to a particular WAN Interface

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Enter the Interface Configuration mode.

  UltOs(config)# interface wan *0/1*

- Apply the existing policy to the interface.

UltOs(config-if)# crypto map crypto_map_name

- Exit from the Interface Configuration mode.

UltOs(config-if)# end

To view the VPN policy parameters

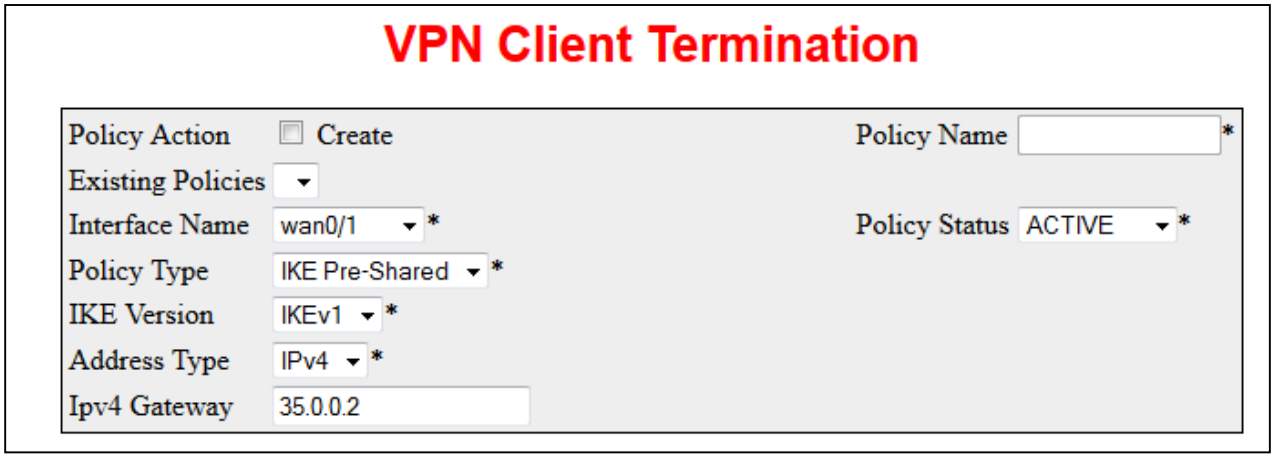
- View the parameters of the VPN policy.

UltOs# show crypto map

```
                VPN Policy Parameters
               -------------------------

 Policy Name                        : crypto_map_name
 Policy Status                      : Active
 Policy Type                        : IPSec Manual
 Ike Version                        : v1
 Local & Remote Protected N/W's     : 192.168.1.0/24 <--
--> 192.168.2.0/24
 Security Mode                      : Tunnel
 Local & Remote Tunnel Term Addr    : 35.0.0.2 <== ==>
35.0.0.1
 Interface Name                     : wan0/1
 Policy Protocol                    : any
 Policy Action                      : Apply
 In/Out bound SPI                   : 256 / 257
 Security Protocol                  : ESP
 Authentication Algorithm           : HMAC-SHA1
 Encryption  Algo                   : DES
 Anti Replay                        : Disable
 Crypto Session Status              : Active
 Crypto Session Encr Pkts           : 0
 Crypto Session Decr Pkts           : 0
 No.of ACTIVE VPN policies          = 1
 No.of VPN policies configured      = 1
```

17.3.8.2 WEB Configuration

VPN policy can be bound over WAN interface using the **Client termination** screen (Navigation - **Security Management > VPN > Users > Client termination)**



Screen 17-7: Binding of Policy

17.3.9 Removing Policy from Interface

The policy assigned to the WAN interface is removed for inactivating the policy. The policy should be inactivated before deleting. Policies assigned to the WAN interface and activated cannot be deleted.

17.3.9.1 CLI Configuration

- **To make the policy inactive**Enter the Global Configuration mode.

  UltOs# configure terminal
- Enter the Interface Configuration mode.

  UltOs(config)#interface wan *0/1*
- Make the policy inactive.

  UltOs(config-if)# no crypto map crypto_map_name
- Exit from the Interface Configuration mode.

  UltOs(config-if)# end

To view the VPN policy parameters

- View the parameters of the VPN policy.

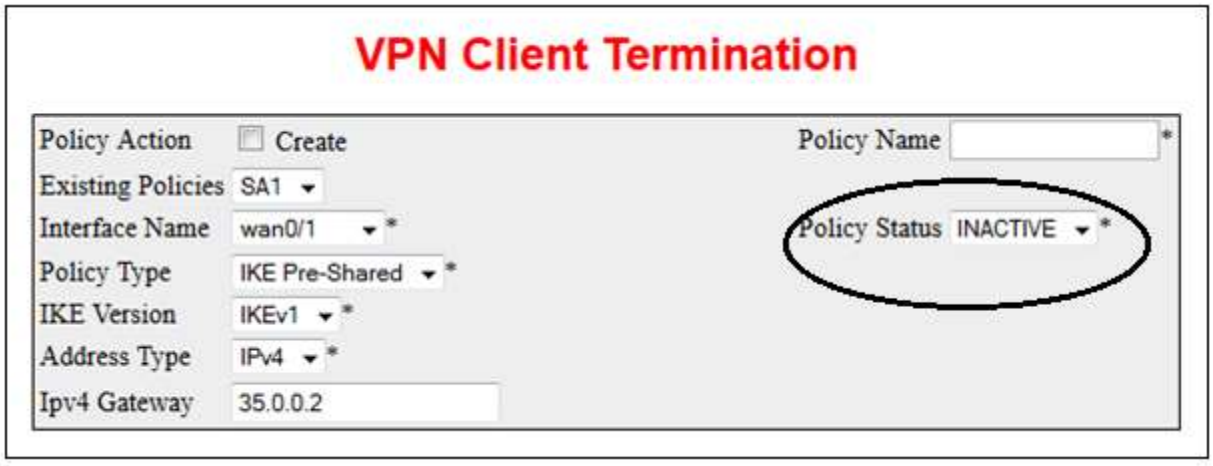
  UltOs# show crypto map crypto_map_name

```
                VPN Policy Parameters

                                  -------------------------

 Policy Name                      : crypto_map_name

 Policy Status                    : InActive

 Policy Type                      : IKE Pre-shared

 Ike Version                      : v1

 Local & Remote Protected N/W's   : 192.168.1.0/24 <--
--> 192.168.2.0/24

 Local & Remote Port Range        : 0-65535 <-- --> 0-
65535
```

```
 Security Mode                        : Tunnel
 Local & Remote Tunnel Term Addr  : 35.0.0.1 <== ==>
35.0.0.2
```

17.3.9.2 WEB Configuration

VPN policy can be removed using the **Client termination** screen (Navigation - **Security Management > VPN > Users > Client termination)**



Screen 17-8: Removal of Policy from Interface

17.3.10 Deleting Policy

This section describes the steps involved in deleting the policy. The policy should be made as inactive before deleting.

17.3.10.1 CLI Configuration

To delete the configured policy

- Enter the Global Configuration mode.

  UltOs# configure terminal

- Delete the configured policy.

  UltOs(config)# no crypto map crypto_map_name

- Exit from the Global Configuration mode.

  UltOs(config)# end

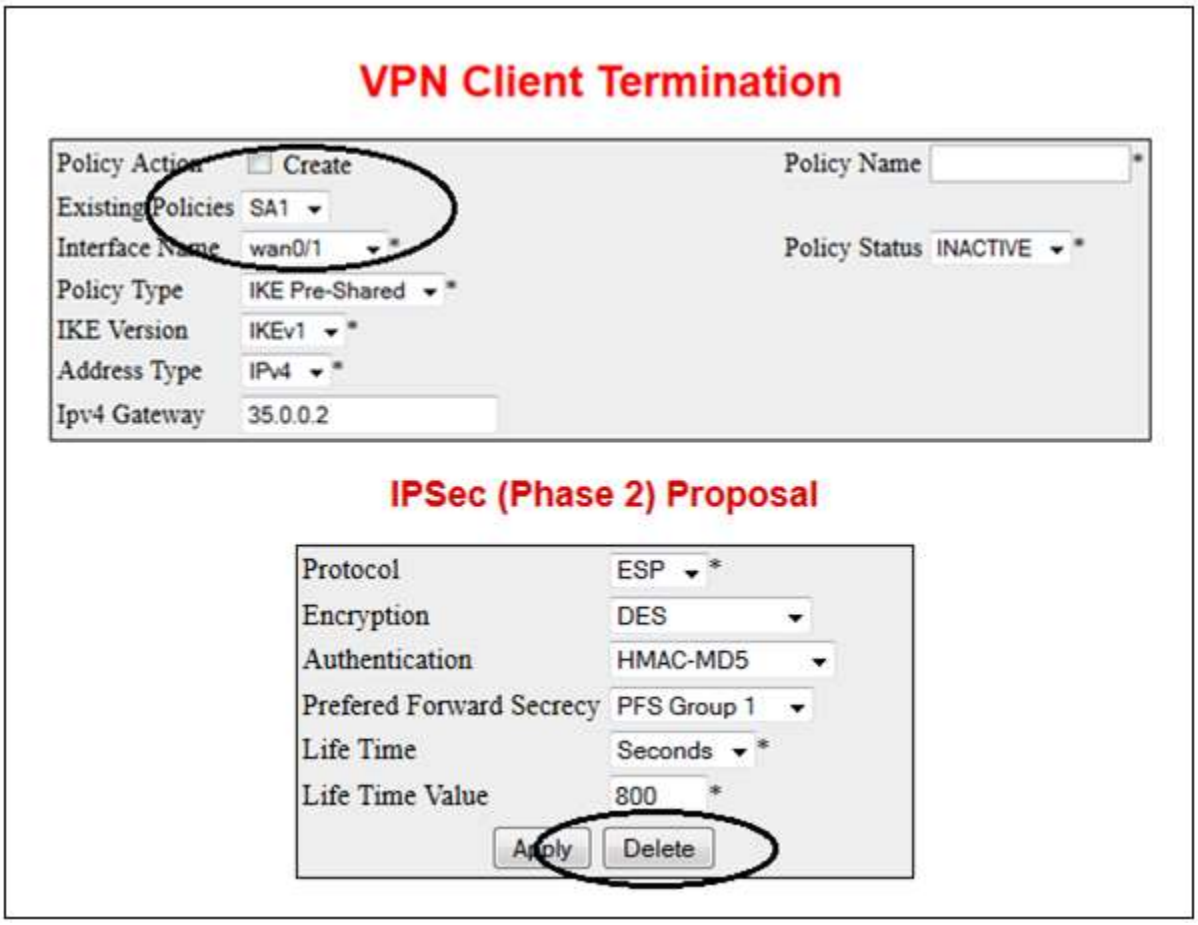
To check the deletion of the policy

- View the parameters of the VPN policy.

  UltOs# show crypto map crypto_map_name

17.3.10.2 WEB Configuration

VPN policy can be created using the **Client termination** screen (Navigation - **Security Management > VPN > Users > Client termination)**



Screen 17-9: Deleting Policy

17.3.11 Sample Configuration

This section describes the sample configuration steps to be performed for configuring the RAVPN module in a switch.

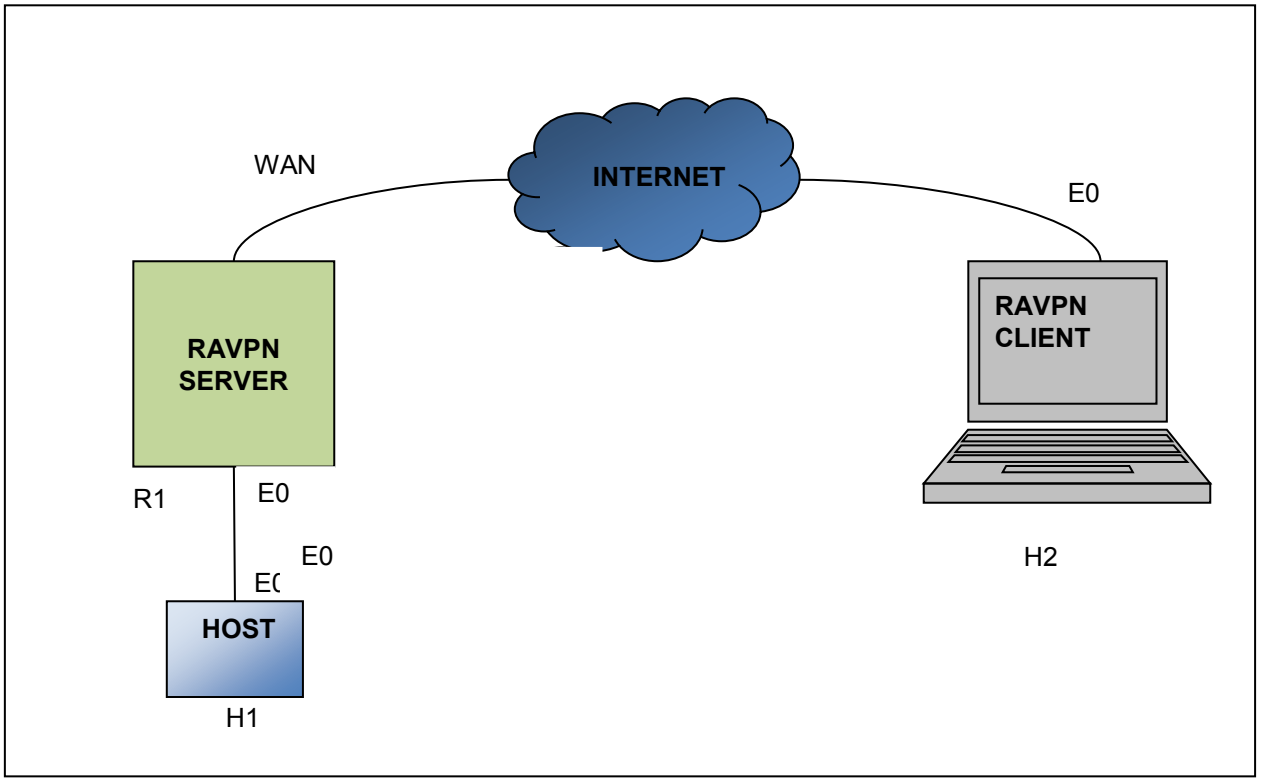


Figure 17-2: RAVPN Topology – Sample Configuration

Node Name	E0 V4 ADDR	WAN V4 ADDR
Host 1(H1)	192.168.1.2	NA
Host 2(H2)	35.0.0.2	NA
FDN40-1(R1)	192.168.1.1	35.0.0.1

17.3.11.1 RAVPN Server Configuration

IPSec RAVPN is installed in the R1 and the below mentioned commands are executed to configure the IPSec policy in IKEv1 mode.

1. Create VLAN interface 100 and assigning an IP

UltOs# configure terminal

UltOs#interface lan 0/1

UltOs#no shutdown

UltOs#exit

UltOs#vlan 100

UltOs#ports add lan 0/1

UltOs#exit

UltOs#interface vlan 100

UltOs#ip address 192.168.1.0 255.255.255.0

UltOs#no shutdown

UltOs#exit

2. Assigning an IP to WAN 0/1 interface

UltOs#interface wan 0/1

UltOs#ip address 35.0.0.1 255.255.255.0

UltOs#no shutdown

UltOs#exit

3. Enable VPN and its parameter

UltOs#set vpn enable

UltOs#vpn remote-access server

UltOs#vpn remote identity keyId CLIENT psk KEY12345

UltOs#ra-vpn username myravpnuser password myravpnpass

UltOs#ip ra-vpn pool myravpnpoolname 192.168.2.1 – 192.168.2.2

4. Create crypto map

UltOs#crypto map sa

UltOs#set ike version v1

UltOs#crypto ipsec mode tunnel

UltOs#crypto key mode ravpn-preshared-key

UltOs#set peer 0.0.0.0

UltOs#isakmp local identity keyId SERVER

UltOs#isakmp peer identity keyId CLIENT

UltOs#isakmp policy encryption DES hash sha1 dh Group2 exch aggressive lifetime Secs 3000

UltOs#crypto map ipsec encryption esp DES authentication esp sha1 lifetime Secs 3000

UltOs#access-list Apply any source 192.168.1.0 255.255.255.0 destination 192.168.2.0 255.255.255.0

UltOs#exit

5. Add default route

   UltOs#ip route 0.0.0.0 0.0.0.0 35.0.0.2

6. Bind crypto map to wan 0/1

   UltOs#interface wan 0/1

   UltOs#crypto map sa

   UltOs#exit

   UltOs#exit

Note: For IKEv2, set the version as v2.

UltOs# set ike version v2

FCC Compliance Statement

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation

FCC Caution!

• Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

• This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Part 15B compliance statements for digital devices:

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected

—Consult the dealer or an experienced radio/TV technician for help.