RADiFlow 3xxx
Service-aware Industrial Ethernet Switches
User Guide

This user guide includes the relevant information for utilizing the RADiFlow 3xxx switches.

The information in this document is subject to change without notice and describes only the product defined in the introduction of this document.

This document is intended for the use of customers of RADiFlow only for the purposes of the agreement under which the document is submitted, and no part of it may be reproduced or transmitted in any form or means without the prior written permission of RADiFlow.

The document is intended for use by professional and properly trained personnel, and the customer assumes full responsibility when using it.

If the Release Notes that are shipped with the device contain information that conflicts with the information in this document or supplements it, the customer should follow the Release Notes.

The information or statements given in this document concerning the suitability, capacity, or performance of the relevant hardware or software products are for general informational purposes only and are not considered binding. Only those statements and/or representations defined in the agreement executed between RADiFlow and the customer shall bind and obligate RADiFlow.

RADiFlow however has made all reasonable efforts to ensure that the instructions contained in this document are adequate and free of material errors and omissions. RADiFlow will, if necessary, explain issues which may not be covered by the document.

RADiFlow sole and exclusive liability for any errors in the document is limited to the documentary correction of errors. RADIFLOW IS NOT AND SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES OR LOSS OF WHATSOEVER KIND, WHETHER DIRECT, INCIDENTAL, OR CONSEQUENTIAL (INCLUDING MONETARY LOSSES), that might arise from the use of this document or the information in it.

This document and the product it describes are the property of RADiFlow, which is the owner of all intellectual property rights therein, and are protected by copyright according to the applicable laws.

Other product and company names mentioned in this document reserve their copyrights, trademarks, and registrations; they are mentioned for identification purposes only

Contents

Introduction

The RADiFlow Service-aware Industrial Ethernet switches, combine a ruggedized Ethernet platform with a unique application-aware processing engine.

As an Industrial Ethernet switch the RADiFlow switches provide a strong Ethernet and IP feature-set with a special emphasis on the fit to the mission-critical industrial environment such as fit to the harsh environmet, high reliabiity and network resliency.

In addition the RADiFlow switches have unique service-aware capabilities that enable an integrated handling of application-level requirements such as implementation of security measures.

Such an integrated solution results in a simple network architecture with an optimized fit to the application requirements.

Key Features

The RADiFlow 3xxx devices offers the following features:

- Wire speed, non-blocking Layer 2 switching
- High-density modular systems (3300/3700) or a compact system (3080)
- Advanced Ethernet and IP feature-set
- Integrated Defense-in-Depth tool-set
- Ethernet and Serial interfaces
- Fit to harsh industrial environment
- Supported by a dedicated industrial service management tool (iSIM)

Using This Document

Documentation Purpose

This user guide includes the relevant information for configuring thenRADiFlow 3xxx functionalities.

It provides the complete syntax for the commands available in the currently-supported software version and describes the features supplied with the device.

For more information regarding the device installation, refer to the *Installation and Maintenance* chapter.

For the latest software updates, see the Release Notes for the relevant release. If the release notes contain information that conflicts with the information in the user guide or supplements it, follow the release notes' instructions.

Intended Audience

This user guide is intended for network administrators responsible for installing and configuring network equipment.

Users must be familiar with the concepts and terminology of Ethernet and local area networking (LAN) to use this User Guide.

Documentation Suite

This document is just one part of the full documentation suite provided with this product.

You are:	Document Function	Function
	Installation Guide	Contains information about installing the hardware and software; including site preparation, testing, and safety information.
➡	User Guide	Contains information on configuring and using the system.
	Release Notes	Contains information about the current release, including new features, resolved issues (bug fixes), known issues, and late-breaking information that supersedes information in other documentation.

Conventions Used

The conventions below are used to inform important information:

NOTE

Indicating special information to which the user needs to pay special attention.

CAUTION

Indicating special instructions to avoid possible damage to the product.

DANGER

Indicating special instructions to avoid possible injury or death.

The table below explains the conventions used within the document text:

Conventions	Description
`commands`	CLI and SNMP commands
command example	CLI and SNMP examples
`<Variable>`	user-defined variables
[Optional Command Parameters]	CLI syntax and coded examples

Organization

The RADiFlow 3xxx User Guide comprises the following list of chapters, each focusing on a different feature or set of features. Each chapter begins with a brief overview of the feature/s, followed by the configuration flow and corresponding commands' configuration section.

Chapter Name	Description
Introduction	Overview of product and document.
Installation and Maintenance	Installing and maintaining the device
Device Administration	Administering RadiFlow devices and using the CLI.
Physical Ports and Logical Interface	Understanding and configuring device interface types including Link Aggregation Groups (LAGs).
RSTP and MSTP	Operating the RSTP and MSTP network resiliency protocols.
VLANs	Understanding and configuring VLANs.
ACLs	Understanding and configuring ACLs, traffic rate-limit, and applying QoS using ACLs.
Quality of Service (QoS)	Understanding and configuring QoS features.
IP Routing	Understanding and configuring the IP routing features.
Application Aware Firewall	Understanding and configuring the application aware firewall.
Secure Remote Access	Understanding and configuring the secure remote access gateway
Serial Tunneling	Understanding and configuration of serial tunneling options
Operations, Administration and Maintenance (OAM)	Understanding and configuring the IEEE 802.1ag Connectivity Fault Management (CFM) tools used for network troubleshooting.
System Log	Understanding and configuring the features used for system troubleshooting

Device Administration

Features Included in this Chapter

This chapter describes how to perform operations to administer your RADiFlow 3xxx devices.

This chapter consists of these sections:

- *MAC-Address Table (FDB)*

  The MAC-address table contains address information that the device uses to forward traffic between ports. The RADiFlow 3xxx devices maintain a database of MAC addresses, manually configured (static) and dynamically learned entries. During troubleshooting, it may be helpful to investigate the entries in the MAC-address table.

- *Files System*

  This section describes some fundamental tasks you perform to maintain the configuration files and system images used by your RADiFlow 3xxx devices.

- Virtual Terminal (VTY) is a logical connection on RADiFlow 3xxx devices. It is used for managing telnet connections.

MAC-Address Table (FDB)

Overview

The MAC (Media Access Control) address is the unique hardware number that identifies the computer on a local area network (LAN) or other network.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length) in the following format:

```
MM:MM:MM:SS:SS:SS
```

Whereas MAC addressing works at the data link layer (layer 2), IP addressing functions at the network layer (layer 3). MAC addresses are also known as *hardware* or *physical* addresses.

The MAC Address table holds the source MAC address, VLAN ID, MAC address priority and port number.

MAC-Address Table Entry Types

The following entry types can exist in the MAC-address table:

- *Dynamic entries*—to learn a dynamic entry, the device examines the packets to determine the source MAC address, VLAN, and port information. Initially, all entries in the database are dynamic, except for certain entries created by the device.

  Dynamic entries are flushed and updated when any of the following occurs:

  - A VLAN is removed
  - A VLAN ID is changed
  - A port mode is changed (tagged/untagged)
  - A port is disabled
  - A port goes down
  - A new dynamic entry is created when the device identifies a source MAC address that does not yet have an entry in the MAC-address table. Dynamic entries are deleted from the database if the device is reset or a power off/on occurs.
- *Static entries*—permanent entries are retained in the database if the device is reset or a power off/on cycle occurs. A permanent entry can be a unicast or multicast MAC address. These entries are created through the CLI.
- *Self entries*—a self entry is automatically created by the device software for various reasons.
- *Filtered entries*—a filtered entry can be created in two ways. One way is to configure filter entry statically for blocking the traffic from and to specific MAC address on the device. The second way is to use the Port Security or the Port Limit feature. The MAC addresses in the filtered entries are the MAC addresses that caused security violation.
- *Multicast entries*—Multicast entries are multicast MAC addresses that were created dynamically by multicast protocol (see the IGMP Snooping chapter of this User Guide).

The MAC-Address Table Configuration Flow

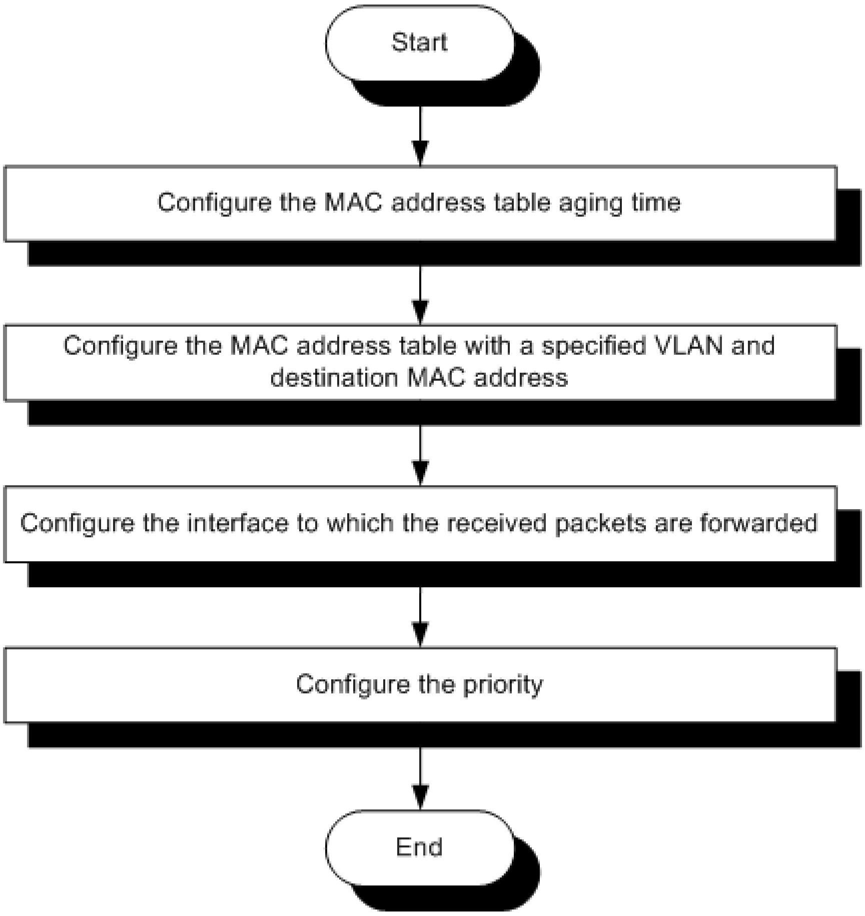

Start
Configure the MAC address table aging time
Configure the MAC address table with a specified VLAN and destination MAC address
Configure the interface to which the received packets are forwarded
Configure the priority
End

Figure 1: The MAC-Address Table Configuration Flow

The MAC-Address Table Commands Hierarchy

```
+ root
        + config terminal
          + [no] port UU/SS/PP
                - [no] learn-new-mac-addresses
          - [no] mac-address-table aging-time <time>
          - [no] mac-address-table static <vlan-id> <mac:hexList>
                - [no] interface UU/SS/PP
                - [no] priority <priority>
                - [no] type {filtered | multicast | secure | self static |
                  unknown}
          - clear mac-address-table
          - show mac-address-table
```

The MAC-Address Table Commands

Table 1: MAC-Address Table Commands

Command	Description
config terminal	Enters the Configuration mode
port *UU/SS/PP*	Enters the Specific Port's Configuration mode
no port [*UU/SS/PP*]	Removes the port configurations
learn-new-mac-addresses	Enables the learning of new MAC addresses in the MAC-address table Default Enabled
no learn-new-mac-addresses	Restores to default
mac-address-table aging-time *<time>*	Defines the length of time that a dynamic entry remains in the MAC-address table since the last time it was updated/used: • *time: in the range of <10-1000000> seconds* Default 300 seconds
no mac-address-table aging-time	Restores to default
mac-address-table static <*vlan-id***> <***mac:hexList***>**	Adds a static MAC address to the MAC-address table: • *vlan-id: the VLAN, in the range of <1-4092>, for which the packet with the specified MAC address is received* • *mac:hexList: the destination unicast/multicast MAC address (HH:HH:HH:HH:HH:HH) added to the MAC-address table* Default None configured
no mac-address-table static <*vlan-id***> <***mac:hexList***>**	Removes a static entry: • *vlan-id: on the specified VLAN in the range of <1-4092>* • *mac:hexList: a specific MAC address (HH:HH:HH:HH:HH:HH)*
interface *UU/SS/PP*	Defines a port to which the received packet is forwarded: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no interface *UU/SS/PP*	Removes the port from forwarding process
priority *<priority>*	Defines the MAC-address table priority: • *priority: in the range of <0-7>* Default 0

Command	Description
no priority	Restores to default
type {filtered | multicast | secure | self | static | unknown}	Specifies the MAC-address learning type: - *filtered, multicast, secure, self static, and unknown* Default Unknown
no type	Restores to default
clear mac-address-table [interface *UU/SS/PP***] [mac** *HH:HH:HH:HH:HH:HH***] [vlan** *<vlan-id>***]**	Removes all or specific entries from the MAC-address table: - *UU/SS/PP: (optional) all MAC addresses for the specified port* - *HH:HH:HH:HH:HH:HH: (optional) a specific MAC address* - *vlan-id: (optional) all MAC addresses for the specified VLAN in the range of <1-4092>*
show mac-address-table	Displays the content of the MAC-address table

Files System

Overview

The Flash file system provides commands for defining, downloading, and deleting software images and configuration files stored in a Flash memory.

The File System Commands Hierarchy

```
+ root

      - file activate-os-image FILE-NAME

      - file backup binary-running-config flash

      - file backup binary-running-config
          PROTOCOL[USER[:PASSWORD]@]IPv4[:PORT]/FILE-NAME

      - file cp os-image PROTOCOL[USER[:PASSWORD]@]IPv4[:PORT]/FILE-NAME

      - file cp FILE-NAME1 PROTOCOL[USER[:PASSWORD]@]IPv4[:PORT]/FILE-NAME2

      - file cp PROTOCOL[USER[:PASSWORD]@]IPv4[:PORT]/FILE-NAME1 FILE-NAME2

      - file cp FILE-NAME1 FILE-NAME2

      - file cp technical-support
          PROTOCOL[USER[:PASSWORD]@]IPv4[:PORT]/FILE-NAME

      - file cp technical-support FILE-NAME

      - file cp running-configuration
          PROTOCOL[USER[:PASSWORD]@]IPv4[:PORT]/FILE-NAME

      - file cp running-configuration FILE-NAME

      - file ls [os-image]

      - file rm [os-image] FILE-NAME

      - file more FILE-NAME

      - file mv FILE-NAME1 FILE-NAME2

      - file replace FILE-NAME

      - file merge FILE-NAME

      - file diff FILE-NAME1 FILE-NAME2

      - file restore binary-running-config flash

      - file restore binary-running-config
          PROTOCOL[USER[:PASSWORD]@]IPv4[:PORT]/FILE-NAME

      - file vi FILE-NAME
```

The File System Configuration Commands

Table 2: File System Commands

Command	Description
`(root)`	
`file activate-os-image` *`FILE-NAME`*	Sets boot statements to load the selected software image on startup: • *FILE-NAME: the file name*
`file backup binary-running-config flash`	Creates a backup file in the local Flash system: Default The name of the backup file is **backup.tar.gz**
`file backup binary-running-config` *`PROTOCOL`*`[`*`USER`*`[:`*`PASSWORD`*`]@]`*`IPv4`*`[:`*`PORT`*`]/`*`FILE-NAME`*	Creates a backup file on a TFTP/FTP server: • *PROTOCOL: the protocol type. For the TFTP server, not need to specify the user, password and port. For the FTP server, no need to specify the port number* • *USER: (optional) the user performing the operation* • *PASSWORD: (optional) the user's password. Symbol @ following the password is required.* • *IPv4: TFTP/FTP server IP address in A.B.C.D format* • *PORT: (optional) the port number* • *FILE-NAME: the name of the file to be backed up*

Command	Description
file cp os-image *PROTOCOL*[*USER*[:*PASSWORD*]@]*IPv4*[:*PORT*]/*FILE-NAME*	Downloads a new software image from a TFTP/FTP server: • *PROTOCOL: the protocol type. For the TFTP server, not need to specify the user, password and port. For the FTP server, no need to specify the port number* • *USER: (optional) the user performing the operation* • *PASSWORD: (optional) the user's password. Symbol @ following the password is required.* • *IPv4: TFTP/FTP server IP address in A.B.C.D format* • *PORT: (optional) the port number* • *FILE-NAME: the file name*
file cp *FILE-NAME1 PROTOCOL*[*USER*[:*PASSWORD*]@]*IPv4*[:*PORT*]/*FILE-NAME2*	Copies a configuration file from the local Flash system to a TFTP/FTP server: • *FILE-NAME1: the source file name* • *PROTOCOL: the protocol type (tftp://A.B.C.D or ftp://user:pass@A.B.C.D). For the TFTP server, not need to specify the user, password and port. For the FTP server, no need to specify the port number* • *USER: (optional) the user performing the operation* • *PASSWORD: (optional) the user's password. Symbol @ following the password is required.* • *IPv4: TFTP/FTP server IP address in A.B.C.D format* • *PORT: (optional) the port number* • *FILE-NAME2: the destination file name*

Command	Description
file cp *PROTOCOL*[*USER*[:*PASSWORD*]@]*IPv4*[:*PORT*]/*FILE-NAME1 FILE-NAME2*	Copies a file from a TFTP/FTP server to the local Flash system: • *PROTOCOL: the protocol type (tftp://A.B.C.D or ftp://user:pass@A.B.C.D). For the TFTP server, not need to specify the user, password and port. For the FTP server, no need to specify the port number* • *USER: (optional) the user performing the operation* • *PASSWORD: (optional) the user's password. Symbol @ following the password is required* • *IPv4: TFTP/FTP server IP address in A.B.C.D format* • *PORT: (optional) the port number* • *FILE-NAME1: the source file name* • *FILE-NAME2: the destination file name*
file cp *FILE-NAME1 FILE-NAME2*	Saves a copy of the active software image to the local Flash system: • *FILE-NAME1: the old file name* • *FILE-NAME2: the new file name*
file cp technical-support *PROTOCOL*[*USER*[:*PASSWORD*]@]*IPv4*[:*PORT*]/*FILE-NAME*	Copies the output of the **show technical-support** command to a TFTP/FTP server: • *PROTOCOL: the protocol type (tftp://A.B.C.D or ftp://user:pass@A.B.C.D). For the TFTP server, not need to specify the user, password and port. For the FTP server, no need to specify the port number* • *USER: (optional) the user performing the operation* • *PASSWORD: (optional) the user's password. Symbol @ following the password is required.* • *IPv4: TFTP/FTP server IP address in A.B.C.D format* • *PORT: (optional) the port number* • *FILE-NAME: the file name*

Command	Description
file cp technical-support *FILE-NAME*	Copies the output of the **show technical-support** command to the local Flash system: • *FILE-NAME: the file name*
file cp running-configuration *PROTOCOL*[*USER*[:*PASSWORD*]@]*IP v4*[:*PORT*]/*FILE-NAME*	Copies the running-configuration file to a TFTP/FTP server: • *PROTOCOL: (optional) the protocol type (tftp://A.B.C.D or ftp://user:pass@A.B.C.D). For the TFTP server, not need to specify the user, password and port. For the FTP server, no need to specify the port number* • *USER: (optional) the user performing the operation* • *PASSWORD: (optional) the user's password. Symbol @ following the password is required.* • *IPv4: TFTP/FTP server IP address in A.B.C.D format* • *PORT: (optional) the port number* • *FILE-NAME: the file name*
file cp running-configuration *FILE-NAME*	Copies the running-configuration file to the local Flash system: • *FILE-NAME: the file name*
file ls [os-image]	Lists the content of the local Flash system, used, and free memory space: • *os-image: (optional) software image version*
file rm [os-image] *FILE-NAME*	Deletes a software image or a specific configuration file from the local Flash system: • *os-image: (optional) software image version* • *FILE-NAME: the file removed from the local Flash system*
file more *FILE-NAME*	Displays the content of a configuration file: • *FILE-NAME: the file's content displayed*
file mv *FILE-NAME1 FILE-NAME2*	Renames the selected configuration file: • *FILE-NAME1: the current file name* • *FILE-NAME2: the new file name*
file replace *FILE-NAME*	Replaces the current running configuration with the selected configuration file: • *FILE-NAME: the file name*

Command	Description
file merge *FILE-NAME*	Merges the content of the selected configuration file with the content of the current running configuration: - *FILE-NAME: the name of the configuration file to be merged*
file diff *FILE-NAME1 FILE-NAME2*	Compares the content of files ignoring case (upper-case and lower-case): - *FILE-NAME1, FILE-NAME2: the names of the files compared*
file restore binary-running-config flash	Restores a specified backup file from the local Flash system: Default The name of the backup file is **backup.tar.gz**
file restore binary-running-config *PROTOCOL*[*USER*[:*PASSWORD*]@]*IP v4*[:*PORT*]/*FILE-NAME*	Restores a specified backup file from a TFTP/FRP server: - *PROTOCOL: the protocol type. For the TFTP server, not need to specify the user, password and port. For the FTP server, no need to specify the port number* - *USER: (optional) the user performing the operation* - *PASSWORD: (optional) the user's password. Symbol @ following the password is required.* - *IPv4: TFTP/FTP server IP address in A.B.C.D format* - *PORT: (optional) the port number* - *FILE-NAME: the name of the file to be restored*
file vi *FILE-NAME*	Edits the content of the selected file: - *FILE-NAME: the file name*

Backup user configuration Files and send files for support

User configurations are saved in 2 different files.

Configurations for serial, security and GRE will be saved in the file *Rf_db.tar.
This file can be saved/uploaded/downloaded using " file cp/rm from.." .
Activation is by deleting older file, downloading new file and restarting the device.

Configurations for standard functionalities as VLAN ,MSTP,LAG ,QOS are saved as a file of the Central Switch.
This file is not displayed when using command "file ls".

For backup : Copy the binary running configuration to a file on TFTP
using : file backup binary-running-config tftp://aa.bb.cc.dd/file_name

For activation : copy the file back to the flash using :

file restore binary-running-config tftp://aa.bb.cc.dd/file_name

System Time and Date

The device internal clock runs from the moment the system starts up and keeps track of the date and time.

The internal clock is set from the following sources:

- Network Time Protocol
- Manual configuration

Network Time Protocol

Network Time Protocol (NTP) provides a reliable way of transmitting and receiving the time over IP networks. NTP is organized as a client-server model. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock connected to a Time server. NTP then distributes this time across the network.

The Time

The time is the number of seconds since 00:00 (midnight) 1 January 1900 GMT, such that the time 1 is 12:00:01 AM on 1 January 1900 GMT; this base serves until the year 2036.

Summer Time (Daylight Saving Time)

You can configure your device to observe the Daylight Saving Time (DST). The DST is followed by the U.S. standards. You can have the device advance the clock one hour at 2:00 a.m. on the first Sunday in April and move back the clock one hour at 2:00 a.m. on the last Sunday in October. You can also explicitly specify the start and end dates and times and whether or not the time adjustment recurs every year.

System Time and Date Command Hierarchy

```
+ root
        + config terminal
          + [no] system
                + [no] time
                      - [no] date CCYY-MM-DDTHH:MM:SS
                      - [no] summer-time recurring [start-at {day-of-the-week
                        DAY | month MONTH | week-of-the-month <week> | time
                        HH:MM:SS} | end-at {day-of-the-week DAY | month MONTH
                        | week-of-the-month <week> | time HH:MM:SS}]
                      - [no] summer-time recurring offset <offset>
                      + [no] ntp
                            + [no] remote-server-ip A.B.C.D
                                  - [no] authentication key-id <key-id> [key-
                                    string STRING]
                            - refresh-interval <interval>
                            - timezone <-12-+12>
                            - [no] time-out <value>
                            - [no] min <min>
                            - [no] shutdown
```

Example for manual setup of time and date using CLI

```
radiflow_3700#config
Entering configuration mode terminal
radiflow_3700#(config)#system
radiflow_3700#(config-system)#time
radiflow_3700#(config-time)#date 2011-06-27T12:33:00
radiflow_3700#(config-time)#commit
radiflow_3700#(config-time)#end
radiflow_3700#system time system-time
date Mon Jun 27 12:33:23 2011
```

The System Time and Date Commands

Table 3: System Time and Date Commands

Command	Description
`config terminal`	Enters the Configuration mode
`system`	Enters the System Configuration Mode
`no system`	Removes the system configurations (system time and date configurations, SNMP, periodic monitoring configurations, and etc.)
`time`	Enters the Time Server Configuration mode
`no time`	Removes the system time configurations
`date` *`CCYY-MM-DDTHH:MM:SS`*	Manually sets the device's system time: • *CCYY-MM-DDTHH:MM:SS: CC represents the century, YY the year, MM the month and DD the day* • *T: date/time separator* • *HH, MM, and SS represent hour, minute and second respectively*
`summer-time recurring {start-at {day-of-the-week` *`DAY`* **`| month`** *`MONTH`* **`| time`** *`HH:MM:SS`* **`| week-of-the-month <`***`week`***`>} | end-at {day-of-the-week`** *`DAY`* **`| month`** *`MONTH`* **`| time`** *`HH:MM:SS`* **`| week-of-the-month <`***`week`***`>}}`**	Defines that the summer time starts and ends on specified days every year: • *start-at: start settings* • *end-at: end settings* • *DAY: the start/end day of the week (Sunday, Monday...)* • *MONTH: the start/end month (January, February...)* • *HH:MM:SS: the start/end time (24-hour format)* • *week: the week of the month to start/end (first, second, third, and forth)* Default The summer time is disabled
`summer-time recurring offset <`*`offset`***`>`**	Defines the number of minutes added during the summer time: • *Offset: in the range of <1-1440>*
`no summer-time recurring`	Restores to default
`ntp`	Configures the device's system time to be synchronized by an NTP server Default Enabled

Command	Description
no ntp	Disables the NTP
remote-server-ip *A.B.C.D*	Defines the NTP server's IP address: • *A.B.C.D: NTP server's IP address*
no remote-server-ip	Removes the NTP server's IP address
authentication key-id <*1-65535***> [key-string** *STRING***]**	Configures the MD5 authentication key used by the device to authenticate the NTP server to prevent rogue server intervention: • *key-id: in the range of <1-65535>* • *key-string STRING: (optional) a string of <1-20> characters (blank spaces and question marks are not allowed)*
no authentication key-id	Removes the MD5 authentication key
refresh-interval <*interval***>**	Defines the number of minutes to synchronize the device's system time to the NTP server: • *interval: in the range of <10-44640> minutes (the upper limit is equivalent to 31 days)*
timezone *<-12-+12>*	Defines the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT): • *-12: the local time zone after (west) of UTC* • *+12: the local time zone before (east) of UTC*
time-out <*value***>**	Defines the NTP server session timeout: • *value: in the range of <2-20> seconds*
no time-out	Removes the timeout
min <*min***>**	Defines the number of minutes before/after UTC: • *min: in the range of <1-59>*
no min	Removes the configured minutes
shutdown	• *Stops the NTP configuration*
no shutdown	• *Starts the NTP configuration*

User Groups

As a security and management measure it might be that the administrator would like to assign new users and password for login in to the system.

+ root

+ config terminal

+ [no] system

+ [no] Security

- [no] user USER_NAME
- [no] member *MEMBER_NAME*
- [no] password *USER_PASSWORD*

Example for manual setup of user

Assignment of user "CTO" with password "CTO" and membership to "admin"

```
radiflow_3700#config
Entering configuration mode terminal
radiflow_3700(config)#system
radiflow_3700(config-system)#security
radiflow_3700(config-security)#user cto
radiflow_3700(config-user-cto)#password cto
radiflow_3700(config-user-cto)#member
(<string>): admin
radiflow_3700(config-user-cto)#commit
Commit complete.
radiflow_3700(config-user-cto)#end
radiflow_3700#logout

Welcome
Please press Enter to activate this console.

Username:cto
Password:cto
3700
cto connected from 127.0.0.1 using tcp on radiflow_3700
radiflow_3700#
```

Changing password to default user "admin"

```
radiflow_3700#config
Entering configuration mode terminal
radiflow_3700(config)#system
radiflow_3700(config-system)#security
radiflow_3700(config-security)#user admin
radiflow_3700(config-user-admin)#password 123
radiflow_3700(config-user-admin)#commit
Commit complete.
radiflow_3700(config-user-admin)#end
radiflow_3700#logout

Welcome
Please press Enter to activate this console.
Username:admin
Password:123
admin connected from 127.0.0.1 using tcp on radiflow_3700
radiflow_3700#
```

VTY (Virtual Terminal)

Virtual Terminal interface (VTY) is used solely to control inbound connections. They are a function of software - there is no hardware associated with them.

VTY Session Command Hierarchy

```
+ root
        - idle-timeout <timeout>
        - screen-length <number-of-rows>
        - screen-width <number-of-columns>
```

VTY Session Configuration Commands

Table 4: VTY Session Commands

Command	Description
idle-timeout *<timeout>*	Defines the VTY connection timeout value: • *timeout: in the range of <0-8192> seconds*
screen-length *<number-of-rows>*	Defines the number of row lines displayed on the terminal screen. • *number-of-rows: in the range of <0-32000>* Default 24 lines
screen-width *<number-of-columns>*	Defines the number of column lines displayed on the terminal screen. • *number-of-columns: in the range of <1-512>*

Physical Ports and Logical Interfaces

Features Included in this Chapter

This chapter describes the RADiFlow 3xxx device interface types and their configuration.

The chapter includes the following sections:

- *Fast and Giga Ethernet Ports*

  This section details the RADiFlow 3xxx device interfaces and the commands to configure them.

- *Link Aggregation Groups (LAGs)*

  This protocol provides increased bandwidth, increased redundancy, and higher availability.

Fast and Giga Ethernet Ports

The RADiFlow 3xxx devices allow service providers to deliver multiple services on separate user ports. Multiple application flows are supported over a single customer port, with each flow being mapped to a different traffic class.

The ports autonegotiate their speed. However, the systems administrator can configure each port for a particular speed (either10 Mbps, 100 Mbps or 1000Mbps).

Gigabit Ethernet ports are statically set to 1 Gbps and you cannot modify their speed.

All ports can be configured for half-duplex or full-duplex operation.

Interface Types

- Device port—device ports are Layer 2-only interfaces associated with a physical port
- IP interface—IP interface is a data structure specifying various interface attributes like its IP address and mask. Thus a single port can have more than one IP interface.

Ports & IP Interfaces Command Hierarchy

NOTE

All the changes to the device's configuration are applied to a copy of the active configuration (called a *candidate configuration*). These changes do not take effect until you commit them, using the `commit` **or** `commit confirm` **command.**

```
+root

        + config terminal

         + port UU/SS/PP

               - [no] description DESCRIPTION

               - [no] speed {10 | 100 | 1000 | 10000 | auto}

               - [no] duplex {auto | full | half}

               - [no] default-vlan <vlan-id>

               - [no] flow-control

               - [no] mtu <mtu-value>

               - [no] mode {access | network}

               - [no] shutdown

         + router

               + [no] interface {eth1 | lo[N] | swN}

                    - [no] description DESCRIPTION

                    - [no] address A.B.C.D/M

                    - [no] shutdown

        - show interface name

        - show interface statistics

        - show port name

        - show port statistics

        - bridge:clear interface name {UU/SS/PP | eth1 | lo[N] | swN}
           statistic
```

IP Interfaces & Ports Commands

Table 1: Ports Configuration Commands

Command	Description
`config terminal`	Enters the Configuration mode
`port` *UU/SS/PP*	Enters the Specific Port's Configuration mode
`description` *DESCRIPTION*	The port's description - *DESCRIPTION: a string of <1-256> characters*
`no description`	Removes the port description
`speed {10 | 100 | 1000 | 10000 | auto}`	Specifies the port's speed Default Auto
`no speed`	Restores to default
`duplex {auto | full | half}`	Specifies the port's duplex parameter Default Auto
`no duplex`	Restores to default
`default-vlan <`*vlan-id*`>`	Specifies the port's default VLAN (only one default VLAN allowed per port) - *vlan-id: in the range of <1-4092>* Default 1
`no default-vlan`	Restores to default
`flow-control`	Enables a technique ((also called Flow Control Mode) for ensuring that a transmitting port does not send too much data to a receiving port at a given time Default Disabled
`no flow-control`	Restores to default
`mtu` *<mtu-value>*	The maximum packet size allowed for the port. This parameter (minus 44 Bytes) is automatically applied on participating IP-interfaces - *mtu-value: in the range of <64-12288>* Default 1544
`no mtu`	Restores to default
`mode {access | network}`	Defines whether the port is an access port (end-host) or a network port (uplink port) - *access: access port's role* - *network: network port's role* Default Network

Command	Description
`shutdown`	Disables the port (the port no longer receives, forwards, or learns)
`no shutdown`	Enables the port

Table 2: IP Interface Configuration Commands

Command	Description
`config terminal`	Enters the Configuration mode
`router`	Enters the Router mode
`interface {eth1 | lo[N] | swN}`	Creates an IP interface and enters the IP-interface's configuration mode • *eth1: an Ethernet network interface* • *lo[N]: an internal logical loopback IP-interface* • *N: (Optional) in the range of <0-9>* • *swN: an IP interface number in the range of <1-9999>*
`no interface {eth1 | lo[N] | swN}`	Removes the created IP interface **NOTE** **Remove the IP interface from all the VLANs it is a member of, in order to remove the created IP interface**
`description DESCRIPTION`	The IP interface description • *DESCRIPTION: a string of up to 256 characters (spaces are allowed)*
`no description`	Removes the IP interface description
`address A.B.C.D/M`	The IP interface's IP address • *A.B.C.D/M: the IP interface's IP address and subnet mask (M) in the range of <1-30>*
`no address`	Removes the IP interface's IP address • *A.B.C.D/M: the IP interface's IP address and subnet mask (M) in the range of <1-30>*
`shutdown`	Disables the interface
`no shutdown`	Enables the interface

Table 3: Commands for Displaying and Clearing Interface Settings and Statistics

Command	Description
show port name *UU/SS/PP*	Displays the status and configuration of the selected port: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
show port statistics	Displays port statistics and packet counters
show interface name {eth1 | lo[*N***] | sw***N***}**	Displays the status and configuration of the selected interface: • *eth1: an Ethernet network interface* • *lo[N]: an internal logical loopback IP-interface. (Optional) N is in the range of <0-9>* • *swN: an IP interface number in the range of <1-9999>*
show interface statistics	Displays interface statistics and packet counters
bridge:clear interface name {*UU/SS/PP* **| eth1 | lo[***N***] | sw***N***} statistic**	Clears all current statistics from the selected interface: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2* • *eth1: an Ethernet network interface* • *lo[N]: an internal logical loopback IP-interface. (Optional) N is in the range of <0-9>* • *swN: an IP interface number in the range of <1-9999>*

Link Aggregation Groups (LAGs)

LAGs provide increased bandwidth and high reliability while saving the cost of upgrading the hardware.

By combining several interfaces in one logical link, LAGs fill the gaps between 10 Mbps, 100 Mbps, and 1 Gbps with intermediate bandwidth values.

LAGs also enable bandwidths beyond 10 Gbps by aggregating multiple Giga ports (as shown in the below figure).

NOTE

The LAGs are numbered from 1 to 14.

Each LAG can consist of up to eight compatibly configured interfaces.

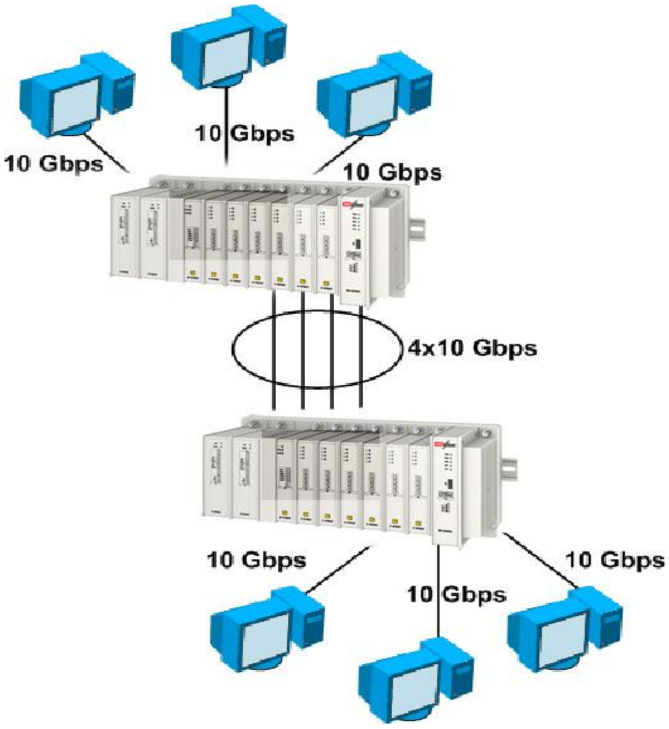


Figure 2: Four Ports Combined into a Link Aggregation Group

There are two LAG types:

- *Static LAGs* consist of individual Gigabit Ethernet links bundled into a single logical link. They provide the ability to treat multiple device ports as one device port. These port groups act as a single logical port for high-bandwidth connections between two network devices. A static LAG balances the traffic load across the links in the channel. If a physical link within the static LAG fails, traffic previously carried over the failed link is moved to the remaining links.

  Most protocols operate over either single ports or aggregated device-ports and do not recognize the physical interface within the port group.

- *Dynamic LAGs* dynamically adapt aggregated links to changes in traffic conditions. This allows load sharing and automatic readjustments in case of LAG link-failures and recovery.

You can configure both static and dynamic LAGs simultaneously, assuming the following restrictions:

- LAG IDs of both static and dynamic LAGs occupy the same available LAG IDs' space
- You cannot define a static LAG and a dynamic LAG with the same LAG ID number
- You can include each port in a single LAG that is either static or dynamic

The LAG Command Hierarchy

```
+ root
       + config terminal
         + [no] ethernet
         + [no] lag
                    - [no] distribution-type {L2 | L3 | L4}
                    + [no] lag-id agN
                         - [no] description DESCRIPTION
                         - [no] mode {access | network}
                         + [no] port {UU/SS/PP}
                              - [no] priority <number>
       - show ethernet lag
       - show ethernet lag lag-id agN [details | statistics]
       - agg:clear lag statistics [lag-id agN]
```

LAG Commands

Table 4: LAG Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
ethernet	Enters the Ethernet Configuration mode
no ethernet	Exits the Ethernet Configuration mode
lag	Enters the LAG Configuration mode
no lag	Exits the LAG Configuration mode
distribution-type {L2 | L3 | L4}	Specifies the LAG packet-distribution between the ports - *L2: distributes packets based on the packets' source and destination MAC addresses* - *L3: distributes packets based on the packets' source and destination IP addresses* - *L4: distributes packets based on the TCP/UDP ports and the source and destination IP addresses for the TCP and UDP packets* Default L2
no lag distribution-type	Restores to default
lag lag-id ag*N*	Mandatory Creates a static LAG and enters the LAG Configuration mode - *agN: LAG ID, where N is in the range of <1-14>*
no lag lag-id ag*N*	Removes the created static LAG
description *DESCRIPTION*	The LAG's description: - *DESCRIPTION: a string of 1-255 characters (spaces are allowed)*
no description	Removes the LAG description
mode {access | network}	Defines whether the group of ports are access ports (end-host) or a network ports (uplink ports) - *access: access role* - *network: network role* Default Network
no mode {access | network}	Restores to default

Command	Description
port *UU/SS/PP*	Mandatory Adds a port to a LAG and enters the LAG Port Configuration mode: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no port *UU/SS/PP*	Removes the selected port from a LAG group: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
priority *<number>*	Specifies an individual port's priority within the LAG: • *number: in the range of <1-65535>* Default 32768
no priority	Restores to default

Table 5: Commands for Displaying and Clearing LAG Settings and Statistics

Command	Description
show ethernet lag	Displays the status and configuration of all LAGs
show ethernet lag lag-id ag*N* **[details | statistics]**	Displays the status and configuration of the selected LAG: • *agN: LAG ID, where N is in the range of <1-14>* • *details: LAG detail information* • *statistics: LAG statistics and packet counters*
agg:clear lag statistics [lag-id ag*N***]**	Clears all current statistics of the selected LAG: • *agN: LAG ID, where N is in the range of <1-14>*

Virtual LANs (VLAN)

VLAN tagging is a standard designed for grouping hosts with common requirements, allowing them to communicate as if they were on the same LAN regardless of their physical location. This allows a logical partition of a physical LAN into different broadcast domains.

This standard also ensures that VLAN traffic is isolated from hosts that are not members of the VLAN.

This technology is based on tagging Ethernet frames with VLAN IDs, assigning each user to a specific VLAN. This prohibits Layer 2 mutual access between workgroups with different VLAN IDs.

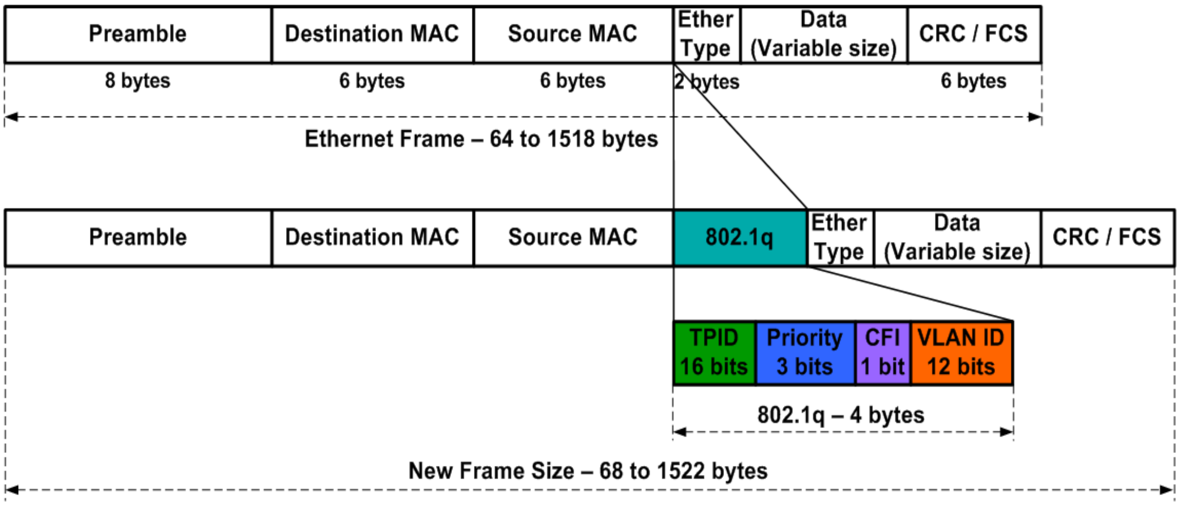
The VLAN Tagging Benefits

Implementing VLANs on the network has the following advantages:

- Flexibility—when a user moves to a different broadcast domain, the system administrator only has to reconfigure the port the user is connected to.
- Security—VLANs provide a greater degree of security than a traditional LAN since data packets of one VLAN are not transmitted to a different VLAN.
- Scalability—VLANs are not limited to a single device, spanning over an enterprise organization or a WAN link.
- Service per VLAN—you can use separate VLANs for different services and features corresponding to each VLAN.

VLAN Traffic Behaviour

VLAN tagging inserts a VLAN ID into the Ethernet frame header, associating each frame with a specific VLAN. Using this method, the port that interconnects devices can carry traffic for multiple VLANs over the same physical connection.



A port can be a member of one or more VLANs. However, only one of these VLANs can be the port's default VLAN. Initially all the device ports are members of a VLAN named *Default* (VLAN ID 1).

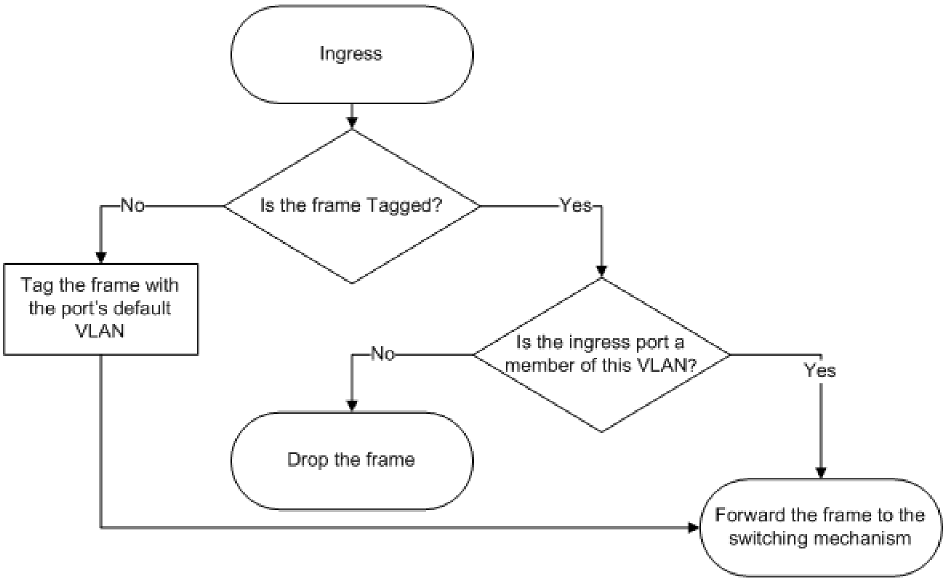
Ports assigned to different VLANs can communicate only through routing (and not on Layer 2).

VLAN Tagging and Ingress Traffic

The VLAN membership and the port's default VLAN affect the incoming (ingress) traffic process as follows:

- When the traffic has a VLAN tagging:
  - if the port is a member of the VLAN, it processes the traffic
  - otherwise, the port drops this traffic

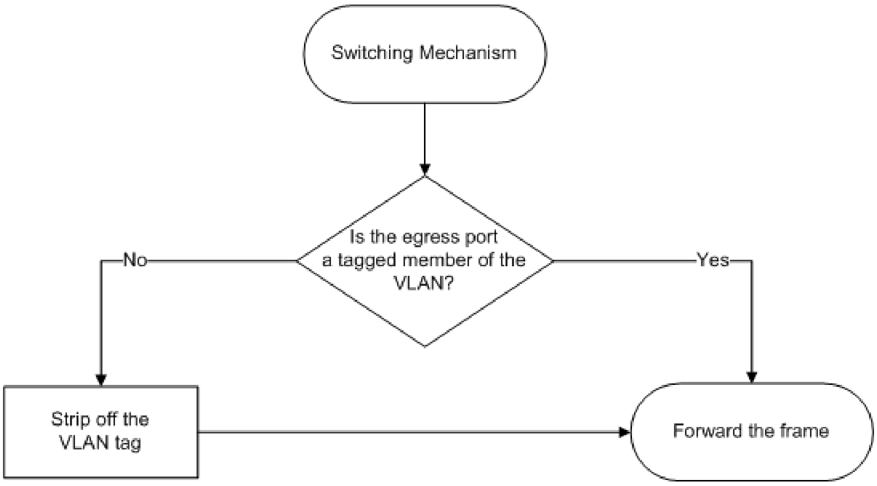
- If the traffic has no VLAN tagging, the port adds its default VLAN ID to the frames and processes them accordingly.


Ingress
Is the frame Tagged?
No
Yes
Tag the frame with the port's default VLAN
Is the ingress port a member of this VLAN?
No
Yes
Drop the frame
Forward the frame to the switching mechanism

VLAN Tagging and Egress Traffic

In addition to the VLANs a port is assigned to, the system administrator defines whether the port is a tagged or an untagged member of a specified VLAN. This affects the outgoing (egress) traffic process:

- If the port is an untagged member of a VLAN, it removes the VLAN ID tagging from this VLAN's frames before forwarding them.
- If the port is a tagged member of a VLAN, it forwards this VLAN's frames with their VLAN ID (without changing the frames).



VLANs Commands Hierarchy

```
+ root
        + config terminal
          + [no] vlan VLAN-NAME <vlan-id>
                - [no] tagged UU/SS/PP
                - [no] untagged UU/SS/PP
                - [no] management
                - [no] routing-interface swN
        - show vlan
```

VLANs Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
vlan *VLAN-NAME <vlan-id>*	Mandatory Creates a VLAN with the specified name and ID (VLAN tag) and enters the VLAN Configuration mode: • *vlan-id: in the range of <1-4092>* • *VLAN-NAME: a string of 1-31 characters*
no vlan *VLAN-NAME <vlan-id>*	Removes the existing VLAN: • *vlan-id: in the range of <1-4092>* • *VLAN-NAME: a string of 1-31 characters*
tagged *UU/SS/PP*	Adds a port as tagged to the specified VLAN: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no tagged [*UU/SS/PP*]	Removes tagged port(s) from the specified VLAN: • *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
untagged *UU/SS/PP*	Adds a port as untagged to the specified VLAN: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*

Command	Description
no untagged [*UU/SS/PP***]**	Removes untagged port(s) from the specified VLAN: • *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
management	Limits the device management access only to the specified VLAN Default Disabled
no management	Specifies the VLAN prohibited from management access
routing-interface *swN*	Attaches an IP interface to the specified VLAN. The sw0 IP interface is attached only to the default VLAN (VLAN ID 1). • *swN: an IP interface number in the range of <01-9999>*
no routing-interface	Detaches the IP interface from the specified VLAN.
show vlan	Displays VLAN configuration information

Spanning Tree (RSTP/MSTP)

Overview

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. An Ethernet network will function properly if only one active path exists between any two stations. STP operation is transparent to end stations, which cannot perceive whether they are connected to a single LAN segment or to a switched LAN with multiple segments.

The fault-tolerant internetworks must have a loop-free path between all the nodes in a network. The spanning tree algorithm calculates the best loop-free path throughout a switched Layer 2 network. Switches send and receive STP frames at regular intervals but they do not forward these frames.

Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages.

The Layer 2 switch relies on MAC addresses for identification of network devices. A switch, essentially a complex bridge, uses bridging tables, which are collections of MAC addresses associated to bridge interfaces or, in the case of a switch, a port number.

STP defines a tree with a root switch and a loop-free path from the root to all switches in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning tree algorithm recalculates the spanning tree topology and activates the standby path.

When two ports on a switch are part of a loop, the STP port priority and path cost settings determine which port is put in the forwarding state and which is put in the blocking state. The STP port priority value represents the location of a port in the network topology and determines how well it is located for passing traffic. The STP path cost value represents media speed.

Bridge ID

Each switch has a unique bridge identifier (bridge ID), which determines the selection of the root switch. The bridge ID of a configuration message is an 8-byte field. The two most-significant bytes are used for the switch priority, and the remaining six bytes are derived from the switch MAC address. Figure 3 shows the bridge ID field architecture.

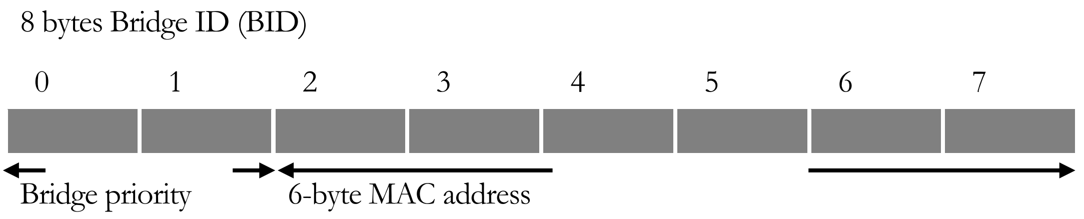


Figure 3: Bridge ID Field of a Bridge Protocol Data Unit

Election of the Root Bridge

The switches in the network exchange data messages called Bridge Protocol Data Units (BPDUs) for information gathering about other switches in the network.

This exchange of messages results in the following actions:

The election of a unique root bridge for each spanning tree instance.

The election of a designated bridge for every switched LAN segment.

The removal of loops in the switched network by blocking ports connected to redundant links.

The bridge with the highest bridge priority (the lowest numerical priority value) is elected as the root switch. If all bridges are configured with the default priority (32768), the bridge with the lowest MAC address in the VLAN becomes the root bridge. The bridge priority value occupies the most significant bits of the bridge ID.

You can change the probability that a bridge will be elected as the root switch by configuring the switch's priority value. Raising the priority value increases the probability; and lowering the value decreases the probability.

The root bridge is the logical center of the STP topology in a switched network. All paths that are not needed for reaching the root bridge from anywhere in the switched network are placed in STP blocking mode.

Path Cost

Switches use an algorithm to determine how close they are to the root bridge. This metric is called the ***Path Cost***. The lower the cost, the closer the switch is to the root. The idea is to traverse the tree using the lowest costs. If two devices have identical path costs in the node of a tree, then the switch with the lowest MAC address value is used for the tiebreaker.

Bridge Protocol Data Units (BPDUs)

BPDUs contain the information about the transmitting switch and its ports, including the switch MAC address, switch priority, port priority, and path cost. STP uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

The BPDU contains information regarding:

Root Bridge ID - Which device is the root bridge

Designated Bridge ID – The transmitting bridge ID.

Path cost - The distance between the root and sender.

Designated port ID - The port ID that identifies the port on the bridge from which the configuration message was originated.

STP Ports States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When a port transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each port on a switch using STP exists in one of these states:

Blocking - The port does not participate in frame forwarding.

Listening - the first transitional state after the blocking state when STP determines that the port should participate in frame forwarding.

Learning - The port prepares to participate in frame forwarding.

Forwarding - The port forwards frames.

Disabled - The port is not participating in STP because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

A port moves through these states:

From initialization to blocking

From blocking to listening or to disabled

From listening to learning or to disabled

From learning to forwarding or to disabled

From forwarding to disabled.

Figure 4 illustrates how a port moves through the states.

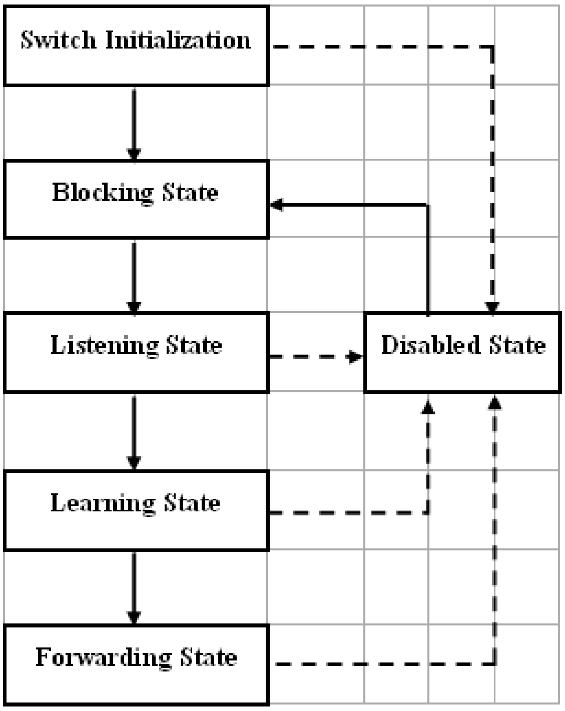


Figure 4: Spanning Tree Port States

When the switch is Powered-up and STP is enabled, every port in the switch goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each port at the forwarding or blocking state.

When the spanning-tree algorithm places a port in the forwarding state, this process occurs:

1. The port is in the listening state while STP waits for protocol information to transition the port to the blocking state.

2. While STP waits for the forward-delay timer to expire, it moves the port to the learning state and resets the forward-delay timer.

3. In the learning state, the port continues to block frame-forwarding as the switch learns end-station location information for the forwarding database.

4. When the forward-delay timer expires, STP moves the port to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A port in the blocking state does not participate in frame-forwarding. After initialization, a BPDU is sent to each port in the switch. A switch initially functions as the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root switch. If there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the ports move to the listening state. A port always enters the blocking state after switch initialization.

A port in the blocking state performs as follows:

Discards frames received on the port

Discards frames switched from another port for forwarding

Does not learn addresses

Receives BPDUs.

Listening State

The listening state is the first state a port enters after the blocking state. The port enters this state when STP determines that the port should participate in frame-forwarding.

A port in the listening state performs as follows:

Discards frames received on the port

Discards frames switched from another port for forwarding

Does not learn addresses

Receives BPDUs.

Learning State

A port in the learning state prepares to participate in frame-forwarding. The port enters the learning state from the listening state.

A port in the learning state performs as follows:

Discards frames received on the port

Discards frames switched from another port for forwarding

Learns addresses

Receives BPDUs.

Forwarding State

A port in the forwarding state forwards frames. The port enters the forwarding state from the learning state.

A port in the forwarding state performs as follows:

Receives and forwards frames received on the port

Forwards frames switched from another port

Learns addresses

Receives BPDUs.

Disabled State

A port in the disabled state does not participate in frame forwarding or STP. A port in the disabled state is non-operational.

A disabled port performs as follows:

Discards frames received on the port

Discards frames switched from another port for forwarding

Does not learn addresses

Does not receive BPDUs.

STP Address Management

IEEE 802.1D specifies 17 multicast addresses, ranging from 0x0180C2000000 to 0x0180C2000010, to be used by different bridge protocols. These addresses are static addresses that cannot be removed.

Regardless of the STP state, the switch receives but does not forward packets destined for addresses between 0x0180c2000000 and 0x0180C200000F.

If STP is enabled, the switch CPU receives packets destined for 0x0180C2000000 and 0x0180C2000010. If STP is disabled, the switch forwards those packets as unknown multicast addresses.

RSTP/MSTP Commands Hierarchy

```
+ root
        + config terminal
          + [no] ethernet
         + [no] spanning tree
               - [no] forward delay <interval>
               - [no] hello-time <interval>
               - [no] max-age <interval>
               - [no] max-age <interval>
              + [no] port UU/SS/PP
                      - [no] edge port
                      - [no] link-type {auto | point-to-point | shared}
                      - [no] mstp instance-id <instance-id>
               - [no] priority <priority>
               - [no] protocol-mstp
               - [no] shutdown
               - [no] vlan-per-instance <vlan-id>
        - show ethernet mstp {details | configuration}
```

RSTP/MSTP Commands

Command	Description
`config terminal ethernet`	Enters the Ethernet Configuration mode
`Spanning-tree`	Enters the RTSP/MSTP Configuration mode
`no Spanning-tree`	Disables spanning tree
`forward-delay <interval>`	Defined the time a port waits in Learning and Listening states before moving to Forwarding state (interval - in seconds)
`no forward-delay`	Restores to default
`hello-time <interval>`	Defines the interval between hello-messages generated by the root

Command	Description
`no hello-time`	Restores to default
`max-age <interval>`	Defines the time a device waits without receiving configuration messages:
`no max-age`	Restores to default
`port UU/SS/PP`	Enters the specific Port's configuration mode
`edge-port`	Setting the port's admin status as an edge port
`no edge-port`	Restores to default
`link-type {auto | point-to-point | shared}`	Defines the port administrative link-type
`mstp instance-id <value>`	Enters the specific MSTP instance Configuration mode for a specified port
`priority <priority>`	Defines the bridge priority
`no priority`	Restores to default
`protocol-mstp`	Enters the MSTP configuration mode
`no protocol-mstp`	Disables MSTP
`shudown`	Disables STP
`no protocol-mstp`	Disables MSTP
`vlan-per-instance <vlan-id>`	Define a VLAN mapped to an instance
`no vlan-per-instance`	Restores to default
`show ethernet mstp [details | configuration]`	Displays the port states and roles

Port Mirroring (Port Monitoring)

Overview

Port Mirroring is a method for monitoring network traffic. Port mirroring forwards all the data transmitted and received by a port to a different location where it can be examined. The port monitoring the traffic has to be connected to a Network Analyzer.

A monitor session includes the following traffic types:

- *Receive (Rx, ingress monitoring)*—the destination port receives a copy of the packets transmitted to the source port, before the source device modifies or processes them.
- *Transmit (Tx, egress monitoring)*—the destination port receives a copy of the packets transmitted by the source port, after the source device modifies and processes them.

NOTE

In egress monitoring, the packets are forwarded to the destination port before the source port changes the packets' 802.1q header. Therefore, the packets transmitted to the destination port may differ from the packets sent out by the source port.

Source Port Characteristics

The RADiflo device can monitor egress traffic, ingress traffic, or both simultaneously.

- The device can monitor any port type such as Fast Ethernet, Gigabit Ethernet, and link-aggregation group.
- The source port cannot be a destination port.
- Source ports can be in the same or different VLANs.

Destination Port Characteristics

The destination port:

- can be any physical Ethernet port
- cannot be a source port
- can participate in only one monitor session at a time (it cannot be a destination port for a second monitor session)
- does not transmit any traffic except the traffic required for the monitoring session
- is limited to its capacity: any traffic exceeding the port's capacity is dropped

Monitor Session Command Hierarchy

```
+ root
        + config terminal
          + [no] system
                - [no] mirror {tx | rx} {destination UU/SS/PP | source
                  UU/SS/PP}
```

The Monitor Session Configuration Commands

Table 6: Monitor Session Commands

Command	Description
`config terminal`	Enters the Configuration mode
`system`	Enters the System Configuration mode
`no system`	Removes the system configurations (system time and date configurations, SNMP, periodic monitoring configurations and etc)
`mirror {tx | rx} {destination UU/SS/PP | source UU/SS/PP}`	Starts a new monitor session: • *tx: configures the session to monitor egress traffic* • *rx: configures the session to monitor ingress traffic* • *destination UU/SS/PP: configures a specific destination port (monitoring port)* • *source UU/SS/PP: configures a list of source (monitored) ports* Default Disabled
`no mirror session {tx | rx}`	Removes the monitor session • *tx: removes the session to monitor egress traffic* • *rx: removes the session to monitor ingress traffic*

Configuration Example

The following example shows how to configure the monitor session on ports. Port 1/4/1 mirrors the traffic on ports 1/4/4, The traffic is monitored both for Rx and Tx.

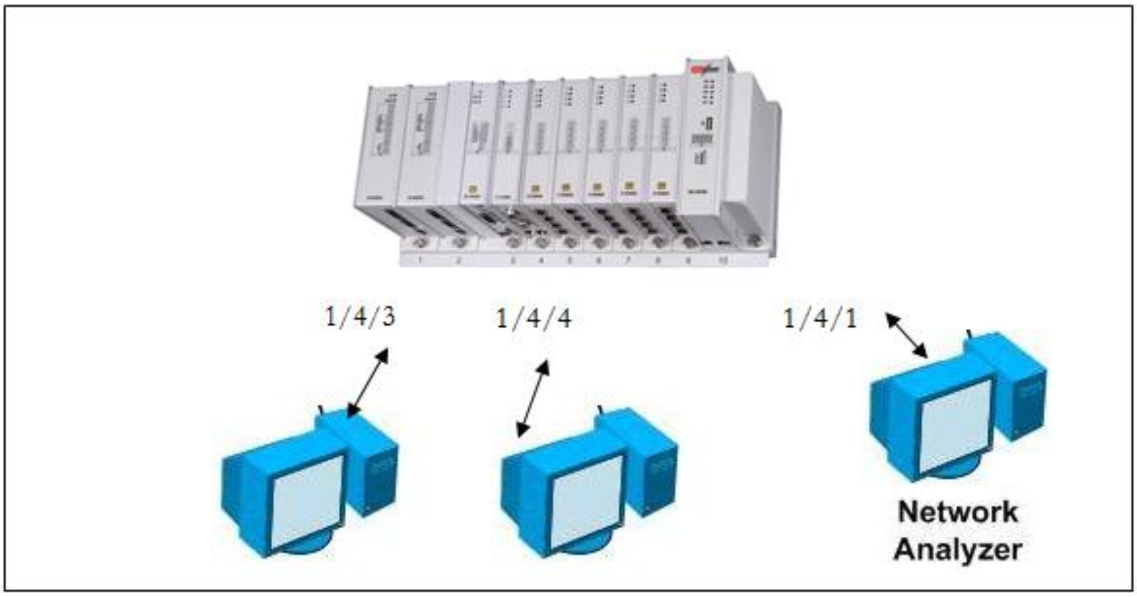


Figure 5: Example of Monitor Session Configuration

1. Set the destination port (sniffer port) for both Rx and Tx:

```
device-name(config)#system mirror tx destination 1/4/1
device-name(config)#system mirror rx destination 1/4/1
```

2. Set the source ports (monitored ports):

```
device-name(config)#system mirror rx source 1/4/4
device-name(config)#system mirror  tx source 1/4/4
```

Access Control Lists (ACLs)

Access Control Lists (ACLs) are sets of numbered rules that process packets going through the device and provide the ability to control network traffic. Using ACLs, system administrators can filter packets that pass through a port by defining different criteria, in order to ensure the network's security, traffic control, and traffic rate-limitation.

These rules are processed in a sequential order, either permitting or denying the traffic, based on the specified ACL conditions. The hardware tests the packets' parameters against the ACLs and acts upon the first condition matched.

The main advantages in using ACLs are:

- Security—by forwarding or dropping ingress traffic, ACLs aid administrators in managing network security policies
- Traffic Control—by enforcing redirection rules, administrators can manipulate network traffic flow, thus reducing bottlenecks and congestions
- Traffic Rate Limitation—using ACLs, administrators can control traffic rate per port or SAP, according to user defined criteria

ACL Types

An ACL is specified by a name or a number. There are four basic ACL types, in predefined range of numbers. Each type matches specific fields in the packets:

- Standard IP ACLs (#1–99,) match the packets' source IP address
- Extended IP ACLs (#100–199) match both the source and destination IP addresses. These ACLs can also match other parameters such as protocol types and TCP/UDP port numbers
- Extended MAC ACLs (#400–499) match both the source and destination MAC addresses. In addition, these ACLs can match VPT and other Layer 2 header fields
- EtherType ACLs (#500–599) match the packets EtherType. These ACLs can match VPT and VLAN options

ACL Process Options

Systems administrators can apply ACLs to both ingress (inbound) traffic and egress (outbound) traffic:

- Ingress ACLs process incoming packets, manipulating permitted packets and forwarding them according to matched ACL conditions. Packets that do not match any of the ACLs are discarded, reducing the load on the outbound interface
- Egress ACLs are mainly used for traffic shaping and statistics collections. They process packets received from the inbound and manipulate them based on ACLs matched

  Egress ACLs do not filter packets originated by the device (such as outgoing Telnet session packets, NTP service packets, and various broadcast packets, such as ARP request).

Access Control Groups (ACG)

An ACG is a collection of ACLs applied to port(s) and SAP(s) determining the process of ingress or egress traffic.

They manipulate permitted ingress packets before forwarding them and discard denied packets, reducing the load on the Outband interface, performing an action that is based on the ACL conditions matched. When configured on egress traffic, they manipulate permitted outgoing packets.

Using ACGs users can:

- filter (drop) traffic
- limit rate of the traffic
- assign a priority to traffic
- remark 802.1p/DSCP bits
- redirect traffic to a specific port
- gather statistics

You can apply multiple ACGs per port and SAP.

ACL Processing Rules

In order to use ACLs effectively, it is essential to understand the ACL processing rules:

- Sequential processing: ACLs are processed sequentially, in the order they are entered
- Once created, users can add new rules to the end of the ACL
- Users cannot selectively add or remove ACL lines from a specific ACL
- The device tests the packets only until it finds the first match, defining whether to permit or deny the packets
- If the packets do not match any of the ACLs:
  - in case of ingress ACL, they are denied. This is due to the fact that the last rule is an implicit deny statement
  - in case of egress ACL, they are permitted (unless the user configures a rule to implicitly deny packets that do not match any of the rules)
- Ordered processing: when applying multiple ACLs, these ACLs are applied in the same order the user applies them. For example, when applying ACL5 and ACL2 to an interface, the device first matches ACL5 rules. If the packets do not match any rules in ACL 5, the device then matches ACL2 rules

Due to the above processing rules, the order of the rules within an ACL and the order the ACLs are applied is crucial.

The total number of conditions for a single ACL rule that can be applied to the ports is limited to 255.

Traffic Remarking

ACLs allow users to impact QoS and its various aspects such as, bandwidth limitation, latency, traffic prioritization, and drop precedence.

Users can also use ACLs to remark the ToS field values by defining a new FC value, and to perform rate control and priority assignment per flow.

Traffic Rate Limit and Shaping

Traffic congestion, caused by heavy network traffic, can cause incoming packet to drop.

To prevent congestion on provider networks, system administrators can use traffic rate-limit and traffic shaping by allocating a specific bandwidth per user port or traffic.

A traffic rate limiter monitors the incoming traffic by:

- forwarding conforming traffic (within the predefined rate)
- dropping non-conforming traffic or marking this traffic as red

Single Rate Three Color Marker (RFC 2697)

The Single Rate Three Color Marker (srTCM) meters a traffic stream and marks it according to three parameters:

- The Committed Information Rate (CIR) determines the long-term average transmission rate
- The Committed Burst Size (CBS) determines how large traffic bursts can be before some of the traffic exceeds the rate limit
- The Excess Burst Size (EBS) determines how large traffic bursts can be before all traffic exceeds the rate limit

The traffic is then marked as follows:

- Traffic within CIR always conforms and is marked green
- Traffic that falls above CIR and below EBS is marked yellow
- Traffic that exceeds CIR and EBS is dropped or marked red

Two Rate Three Color Marker (RFC 2698)

The two rate Three Color Marker (trTCM) meters a traffic stream and marks it according to the below parameters.

- The Committed Information Rate (CIR) determines the long-term average transmission rate
- The Committed Burst Size (CBS), associated with CIR, determines how large traffic bursts can be before some of the traffic exceeds the rate limit
- The Peak Information Rate (PIR) determines the long-term delimiter between yellow packets and red ones
- The Peak Burst Size (PBS), associated with PIR, determines the burst size before the traffic exceeds PIR

The traffic is then marked as follows:

- Traffic within CIR and CBS always conforms and is marked green
- Traffic not conforming to CIR and CBS but conforming to PIR and PSB is marked yellow
- Traffic not conforming to PIR and PSB is dropped or marked red

Exceed Action

Once the packet is classified as exceeding a particular rate limit, the device:

- either drops the packet
- or processes the packet based on congestion avoidance mechanisms, such as wred

Color-Blind and Color-Aware

Rate limiting operates in one of the below two modes:

- in a *Color-Blind* mode, where all packets are considered green upon entering the metering process. They are marked yellow or red if the traffic class exceeds the bandwidth limits configured
- in a *Color-Aware* mode, assuming the packet stream is colored by an upstream device before entering the metering process. In this mode the device forwards green packets and forwards yellow and red packets according to the defined rate-limit

Traffic Redirection

Systems administrators can redirect traffic to separate servers, based on the packet header parameters (such as, IP address, IP protocol, and application).

They can select to redirect traffic to a specified interface or a specified VLAN.

Using this feature, systems administrators can change the traffic's VLAN ID in the VLAN tag header, in order to forward traffic between VLANs.

ACLs Command Hierarchy

IP ACLs

```
+ root
       + config terminal
         + [no] ip access-list standard {NAME | <acl-number>}
               - [no] remark REMARK
               + [no] rule <value>
                    - action {deny | permit}
                    - [no] inner-vlan <vlan-id> [inner-vlan-mask <vlan-mask>]
                    - [no] inner-vpt <priority>
                    - source_ip A.B.C.D/MASK
                    - [no] untagged
                    - [no] vlan <vlan-id> [vlan-mask <vlan-mask>]
                    - [no] vpt <priority>
         + [no] ip access-list extended {NAME | <acl-number>}
               - [no] remark REMARK
               + [no] rule <value>
                    - action {deny | permit}
```

```
           - destination_ip A.B.C.D/MASK
           - [no] inner-vlan <vlan-id> [inner-vlan-mask <vlan-mask>]
           - [no] inner-vpt <priority>
           - [no] precedence TYPE
           - protocol TYPE
                - [no] established
                - [no] icmp-code <value>
                - [no] icmp-type <value>
                - [no] tcp-source-port <value>
                - [no] tcp-destination-port <value>
                - [no] udp-source-port <value>
                - [no] udp-destination-port <value>
           - source_ip A.B.C.D/MASK
           - [no] tos <value>
           - [no] untagged
           - [no] vlan <vlan-id> [vlan-mask <vlan-mask>]
           - [no] vpt <priority>
- [no] access-group-monitoring-profile <profile-id>
      - [no] enables-statistics <statistics-profile>
+ port UU/SS/PP
      + [no] ip-access-group-standard {NAME | <acl-number>} {in | out}
           - [no] fc <value>
                - color {red | green | yellow}
           - [no] monitoring-profile <profile-id>
           + [no] rate-limit {dual | single}
                - cbs <value>
                - cir <value>
                - color-aware
                - ebs <value>
                - pbs <value>
                - pir <value>
           - [no] redirect UU/SS/PP
           - [no] vlan <vlan-id>
      + [no] ip-access-group-extended {NAME | <acl-number>} {in | out}
           + [no] fc <value>
                - color {red | green | yellow}
           - [no] monitoring-profile <profile-id>
           + [no] rate-limit {dual | single}
```

    - **cbs** *<value>*
    - **cir** *<value>*
    - **color-aware**
    - **ebs** *<value>*
    - **pbs** *<value>*
    - **pir** *<value>*
  - **[no] redirect** *UU/SS/PP*
  - **[no] vlan <***vlan-id***>**
- **show port ip-access-group-standard** [*NAME* | *<acl-number>*] **[in | out] [monitoring-profile [statistics [green-bps | green-fps | match-counter-bps | match-counter-fps | not-green-bps | not-green-fps | not-red-bps | not-red-fps | red-bps | red-fps | yellow-bps | yellow-fps]]]**
- **show port ip-access-group-extended** [*NAME* | *<acl-number>*] **[in | out] [monitoring-profile [statistics [green-bps | green-fps | match-counter-bps | match-counter-fps | not-green-bps | not-green-fps | not-red-bps | not-red-fps | red-bps | red-fps | yellow-bps | yellow-fps]]]**
- **show running-config ip access-list**
- **show running-config ip access-list standard** [*NAME* | *<acl-number>*] **[remark** *REMARK* **| rule {***<rule>* **| {action {deny | permit} | inner-vlan <***vlan-id***> [inner-vlan-mask <***VLAN mask***>] | inner-vpt <***priority***> | source_ip** *A.B.C.D/MASK* **| untagged | vlan <***vlan-id***> [vlan-mask <***vlan-mask***>] | vpt** *<priority>***}}]**
- **show running-config ip access-list extended** [*NAME* | *<acl-number>*] **[remark** *REMARK* **| rule {***<rule>* **| {action {deny | permit} | destination_ip** *A.B.C.D/MASK* **| established | icmp-code** *<value>* **| icmp-type** *<value>* | **inner-vlan <***vlan-id***> [inner-vlan-mask <***vlan-mask***>] | inner-vpt <***priority***> | precedence** *TYPE* **| protocol <***type***> | source_ip** *A.B.C.D/MASK* **| tcp-destination-port** *<value>* | **tcp-source-port** *<value>* **| tos <***value***> | udp-destination-port** *<value>* | **udp-source-port** *<value>* **| untagged | vlan <***vlan-id***> [vlan-mask <***vlan-mask***>] | vpt <***priority***>}}]**
- **show running-config access-group-monitoring-profile [<***profile-id***>] [enable-statistics] [match-counter-bps | match-counter-fps | rate-limit-statistics-green-notgreen-bps | rate-limit-statistics-green-notgreen-fps | rate-limit-statistics-green-red-bps | rate-limit-statistics-green-red-fps | rate-limit-statistics-green-yellow-bps | rate-limit-statistics-green-yellow-fps | rate-limit-statistics-red-notred-bps | rate-limit-statistics-red-notred-fps | rate-limit-statistics-red-yellow-bps | rate-limit-statistics-red-yellow-fps]**

MAC ACLs

```
+ root
      + config terminal
        + [no] mac access-list {NAME | <acl-number>}
              - [no] remark REMARK
              + [no] rule <value>
                    - action {deny | permit}
                    - [no] da-type <type>
                    - destination_mac HH:HH:HH:HH:HH:HH destination_mac_mask
                      HH:HH:HH:HH:HH:HH
                    - [no] inner-vlan <vlan-id> [inner-vlan-mask <vlan-mask>]
                    - [no] inner-vpt <priority>
                    - precedence TYPE
                    - source_mac HH:HH:HH:HH:HH:HH source_mac_mask
                      HH:HH:HH:HH:HH:HH
                    - [no] tos <value>
                    - [no] untagged
                    - [no] vlan <vlan-id> [vlan-mask <vlan-mask>]
                    - [no] vpt <priority>
        + port UU/SS/PP
              + [no] mac-access-group {NAME | <acl-number>} {in | out}
                    - [no] fc <value>
                          - color {red | green | yellow}
                    - [no] monitoring-profile <profile-id>
                    + [no] rate-limit {dual | single}
                          - cbs <value>
                          - cir <value>
                          - color-aware
                          - ebs <value>
                          - pbs <value>
                          - pir <value>
                    - [no] redirect UU/SS/PP
                    - [no] vlan <vlan-id>
      - show port mac-access-group [NAME | <acl-number>] [in | out]
          [monitoring-profile [statistics [green-bps | green-fps | match-
          counter-bps | match-counter-fps | not-green-bps | not-green-fps |
          not-red-bps | not-red-fps | red-bps | red-fps | yellow-bps |
          yellow-fps]]]
      - show running-config mac access-list
```

- **show running-config mac access-list** [*NAME* **|** *<acl-number>*] **[remark** *REMARK* **| rule {***<rule>* **| {action {deny | permit} | da-type <***type***> | destination_mac** *HH:HH:HH:HH:HH:HH* **destination_mac_mask** *HH:HH:HH:HH:HH:HH* **| inner-vlan <***vlan-id***> [inner-vlan-mask <***vlan-mask***>] | inner-vpt** *priority***> | precedence** *TYPE* **| source_mac** *HH:HH:HH:HH:HH:HH* **source_mac_mask** *HH:HH:HH:HH:HH:HH* **| tos <***value***> | untagged | vlan <***vlan-id***> [vlan-mask <***vlan-mask***>] | vpt** *<priority>***}}]**

Ethertype ACLs

```
+ root

       + config terminal

         + [no] ether-type access-list {NAME | <acl-number>}

            - [no] remark REMARK

            + [no] rule <rule>

                 - action {deny | permit}

                 - [no] ether-type <type>

                 - [no] inner-vlan <vlan-id> [inner-vlan-mask <vlan-mask>]

                 - [no] inner-vpt <priority>

                 - [no] precedence TYPE

                 - [no] tos <value>

                 - [no] vlan <vlan-id> [vlan-mask <vlan-mask>]

                 - [no] vpt <priority>

         + port UU/SS/PP

            +  [no]  ether-type-access-group  {NAME  |  <acl-number>}  {in  |
               out}

                 - [no] fc <value>

                      - color {red | green | yellow}

                 - [no] monitoring-profile <profile-id>

                 + [no] rate-limit {dual | single}

                      - cbs <value>

                      - cir <value>

                      - color-aware

                      - ebs <value>

                      - pbs <value>

                      - pir <value>

                 - [no] redirect UU/SS/PP

                 - [no] vlan <vlan-id>

       - show port ether-type-access-group [NAME | <acl-number>] [in | out]
           [monitoring-profile [statistics [green-bps | green-fps | match-
           counter-bps | match-counter-fps | not-green-bps | not-green-fps |
           not-red-bps | not-red-fps | red-bps | red-fps | yellow-bps |
           yellow-fps]]]

       - show running-config ether-type access-list

       - show running-config ether-type access-list [NAME | <acl-number>]
           [remark REMARK | rule {<value> | {action {deny | permit} | ether-
           type <type> | inner-vlan <vlan-id> [inner-vlan-mask <vlan-mask>]
           | inner-vpt  <priority> | precedence TYPE | tos <value> | vlan
           <vlan-id> [vlan-mask <vlan-mask>] | vpt <priority>}}]
```

ACLs Commands

Command	Description
config terminal	Enters the Configuration mode
ip access-list standard {*NAME* **|** *<acl-number>***}**	Mandatory Defines a standard IP ACL: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <1-99>*
no ip access-list standard [*NAME* **|** *<acl-number>***]**	Removes the selected standard IP ACL: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <1-99>*
remark *REMARK*	Associates a remark to a standard IP ACL: • *REMARK: a string of <1-30> characters*
no remark	Removes the remark
rule <*value***>**	Mandatory Creates a standard IP ACL rule for filtering traffic: • *value: in the range of <1-255>*
no rule [<*value***>]**	Removes the standard IP ACL rule: • *value: (optional) in the range of <1-255>*
action {deny | permit}	Mandatory Defines the rule conditions: • *deny: denies packets* • *permit: permits packets*
inner-vlan <*vlan-id***> [inner-vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the inner IP-header: • *vlan-id: in the range of <1-4095>* • *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*

Command	Description
no inner-vlan [<*vlan-id***>] [inner-vlan-mask [<***vlan-mask***>]]**	Removes the selected inner-VLAN and inner-mask: • *vlan-id: (optional) in the range of <1-4095>* • *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*
inner-vpt <*priority***>**	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the inner-VLAN tag header: • *priority: in the range of <0-7>*
no inner-vpt [<*priority***>]**	Removes the selected VPT: • *priority: (optional) in the range of <0-7>*
source_ip *A.B.C.D/MASK*	Mandatory Defines the packet's source-address: • *A.B.C.D/MASK: source IP-address/source mask. Use keyword any when source IP-address/source-mask is 0.0.0.0/255.255.255.255 (any host)*
untagged	The ACL rule matches untagged packets only Default Both tagged and untagged
no untagged	Restores to default
vlan <*vlan-id***> [vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the outer IP-header: • *vlan-id: in the range of <1-4095>* • *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*
no vlan [<*vlan-id***>] [vlan-mask [<***vlan-mask***>]]**	Removes the selected outer-VLAN and outer-mask: • *vlan-id: (optional) in the range of 1-4095* • *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*
vpt <*priority***>**	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the outer-VLAN tag header: • *priority: in the range of <0-7>*

Command	Description
no vpt [<*priority***>]**	Removes the selected VPT: • *priority: (optional) in the range of <0-7>*
ip access-list extended {*NAME* **|** *<acl-number>***}**	Mandatory Defines an extended IP ACL: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <100-199>*
no ip access-list extended [*NAME* **|** *<acl-number>***]**	Removes the selected extended IP ACL: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <100-199>*
remark *REMARK*	Associates a remark to an extended IP ACL: • *REMARK: a string of <1-30> characters*
no remark	Removes the remark
rule <*1-255***>**	Mandatory Creates an extended IP ACL rule for filtering traffic: • *value: in the range of <1-255>*
no rule [<*1-255***>]**	Removes the extended IP ACL rule: • *value: (optional) in the range of <1-255>*
action {deny | permit}	Mandatory Defines the rule conditions: • *deny: denies packets* • *permit: permits packets*
destination_ip *A.B.C.D/MASK*	Mandatory Defines the packet's destination-address: • *A.B.C.D/MASK: destination IP-address/destination mask. Use keyword any when destination IP-address/destination-mask is 0.0.0.0/255.255.255.255 (any host)*

Command	Description
inner-vlan <*vlan-id***> [inner-vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the inner IP-header: - *vlan-id: in the range of <1-4095>* - *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*
no inner-vlan [<*vlan-id***>] [inner-vlan-mask [<***vlan-mask***>]]**	Removes the selected inner-VLAN and inner-mask: - *vlan-id: (optional) in the range of <1-4095>* - *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*
inner-vpt <*priority***>**	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the inner-VLAN tag header: - *priority: in the range of <0-7>*
no inner-vpt	Removes the priority
precedence *TYPE*	The ACL rule matches packets by the literal precedence values: - *TYPE: see* **Error! Reference source not found.**
no precedence	Removes the precedence value
protocol *TYPE*	Specifies the name or a number of an IP protocol: - *TYPE: tcp, udp, ip, igmp, icmp or IP protocol numbers in the range of <0-255>, representing an IP protocol number (http://www.iana.org/assignments/protocol-numbers (RFC5237)). To match any Internet protocol, use the keyword ip. Some protocols allow further qualifiers, as described below*
established	(Optional, valid for TCP protocol only) indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The packets that do no match are TCP packets sent to initialize a TCP session.
no established	(valid for TCP protocol only) removes the established connection

Command	Description
icmp-code *<value>*	(Optional, valid for ICMP protocol only) matches ICMP packets by the ICMP message code: - *value: in the range of <0-255> or a valid literal ICMP message code (see* **Error! Reference source not found.***)*
no icmp-code	Removes the ICMP message code
icmp-type *<value>*	(Optional, valid for ICMP protocol only) matches ICMP packets by the ICMP message type: - *value: in the range of <0-255> or a valid literal ICMP message type (see* **Error! Reference source not found.***)*
no icmp-type	Removes the ICMP message type
tcp-source-port *<value>*	(Optional, valid for TCP protocol only) defines the decimal number or a name of source TCP port. Use TCP port's names when filtering TCP packets only: - *value: in the range of <0-65535> or a TCP port literal value (see* **Error! Reference source not found.***)*
no tcp-source-port	Removes the TCP source port's literal value
tcp-destination-port *<value>*	(Optional, valid for TCP protocol only) defines the decimal number or a name of destination TCP port. Use TCP port's names when filtering TCP packets only: - *value: in the range of <0-65535> or a TCP port literal value (see* **Error! Reference source not found.***)*
no tcp-destination-port	Removes the TCP destination port's literal value
udp-source-port *<value>*	(Optional, valid for UDP protocol only) defines the decimal number or a name of source UDP port. Use UDP port's names when filtering UDP packets only: - *value: in the range of <0-65535> or a UDP port literal value (see* **Error! Reference source not found.***)*
no udp-source-port	Removes the UDP source port's literal value

Command	Description
udp-destination-port <*value***>**	(Optional, valid for UDP protocol only) defines the decimal number or a name of a UDP destination port. Use UDP port's names when filtering UDP packets only: - *value: in the range of <0-65535> or a UDP port literal value (see* **Error! Reference source not found.***)*
no udp-destination-port	Removes the UDP destination port's literal value
source_ip *A.B.C.D/MASK*	Mandatory Defines the packet's source-address: - *A.B.C.D/MASK: source IP-address/source mask. Use keyword any when source IP-address/source-mask is 0.0.0.0/255.255.255.255 (any host)*
tos <*value***>**	The ACL rule matches packets by the service level type: - *value: in the range of <0-7> or a valid literal ToS value (see* **Error! Reference source not found.***)*
no tos	Removes the valid literal ToS value
untagged	The ACL rule matches untagged packets only Default Both tagged and untagged
no untagged	Restores to default
vlan <*vlan-id***> [vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the outer IP-header: - *vlan-id: in the range of <1-4095>* - *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*
no vlan [<*vlan-id***>] [vlan-mask [<***vlan-mask***>]]**	Removes the selected outer-VLAN and outer-mask: - *vlan-id: (optional) in the range of <1-4095>* - *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*

Command	Description
vpt <_priority_**>**	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the outer-VLAN tag header: • _priority: in the range of <0-7>_
no vpt [<_priority_**>]**	Removes the selected VPT: • _priority: (optional) in the range of <0-7>_
access-group-monitoring-profile <_profile-id_**>**	Defines a bandwidth-counter profile: • _profile-id: in the range of <1-12>_
no access-group-monitoring-profile [<_profile-id_**>]**	Removes the configured bandwidth-counter profiles: • _profile-id: (optional) in the range of <1-12>_
enable-statistics <_statistics-profile_**>**	Defines statistics: • _statistics-profile:_ see **Error! Reference source not found.**
no enable-statistics [<_statistics-profile_**>]**	Removes the definition: • _statistics-profile: (optional) see_ **Error! Reference source not found.**
port _UU/SS/PP_	Enters the Port's Configuration mode
ip-access-group-standard {_NAME_ **|** _<acl-number>_**} {in | out}**	Mandatory Assigns a IP ACG to a port: • _NAME: a string of <1-10> characters_ • _<acl-number>: in the range of <1-99>_ • _in: filters the ingress traffic only_ • _out: filters the egress traffic only_ Default Deny any
no ip-access-group-standard [_NAME_ **|** _<acl-number>_**] [in | out]**	Removes the specified IP ACG: • _NAME: (optional) a string of <1-10> characters_ • _acl-number: (optional) in the range of <1-99>_ • _in: (optional) filters the ingress traffic only_ • _out: (optional) filters the egress traffic only_ Default Deny any

Command	Description
fc *<value>*	Defines a default mapping of ACG to forwarding class (FC) and color: - *value: FC value (see* **Error! Reference source not found.***)*
no fc [*<value>*]	Restores the mapping: - *value: (optional) FC value*
color {red | green | yellow}	Defines the conforming level: - *red: the non-conforming drop level* - *green: the conforming drop level* - *yellow: the partially conforming level*
monitoring-profile <*profile-id***>**	Enables bandwidth counters per ACL rules: - *profile-id: in the range of <1–12>*
no monitoring-profile [<*profile-id***>]**	Disables the bandwidth monitoring: - *profile-id: (optional) in the range of <1–12>*
rate-limit {dual | single}	Applies a rate-limit on the ACG for the specified port: - *dual: the Two Rate Three Color Marker (RFC 2698)* - *single: the Single Rate Three Color Marker (RFC 2697)*
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: - *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* - *single: (optional)the Single Rate Three Color Marker (RFC 2697)*
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): - *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): - *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): - *value: in the range of <1-1048575> Kbps*

Command	Description
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): • *value: in the range of <1-1048575> Kbps*
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): • *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified port: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP***]**	Removes the traffic redirection from the specified port: • *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: • *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: • *vlan-id: (optional) in the range of <1-4095>*
ip-access-group-extended {*NAME* **| <***acl-number***>} {in | out}**	Mandatory Assigns a IP ACG to a port: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <100-199>* • *in: filters the ingress traffic only* • *out: filters the egress traffic only*
no ip-access-group-extended [*NAME* **| <***acl-number***>] [in | out]**	Removes the specified IP ACG: • *NAME: (optional) a string of 1-10 characters* • *acl-number: (optional) in the range of <1-99>* • *in: (optional) filters the ingress traffic only* • *out: (optional) filters the egress traffic only*

Command	Description
fc *<value>*	Defines a default mapping of ACG to forwarding class (FC) and color: • *value: FC value (see* **Error! Reference source not found.***)*
no fc [*<value>***]**	Restores the mapping: • *value: (optional) FC value*
color {red | green | yellow}	Defines the conforming level: • *red: the non-conforming drop level* • *green: the conforming drop level* • *yellow: the partially conforming level*
monitoring-profile <*profile-id***>**	Enables bandwidth counters per ACL rules: • *profile-id: in the range of <1–12>* Default Disabled
no monitoring-profile [<*profile-id***>]**	Disables the bandwidth monitoring: • *profile-id: (optional) in the range of <1–12>*
rate-limit {dual | single}	Applies a rate-limit on the ACG for the specified port: • *dual: the Two Rate Three Color Marker (RFC 2698)* • *single: the Single Rate Three Color Marker (RFC 2697)*
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: • *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* • *single: (optional)the Single Rate Three Color Marker (RFC 2697)*
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): • *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): • *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): • *value: in the range of <1-1048575> Kbps*

Command	Description
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): • *value: in the range of <1-1048575> Kbps*
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): • *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified port: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP***]**	Removes the traffic redirection from the specified port: • *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: • *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: • *vlan-id: (optional) in the range of <1-4095>*
monitoring-profile <*profile-id***>**	Enables bandwidth counters per ACL rules: • *profile-id: in the range of <1—12>* Default Disabled
no monitoring-profile [<*profile-id***>]**	Disables the bandwidth monitoring: • *profile-id: (optional) in the range of <1—12>*
rate-limit {dual | single}	Applies a rate-limit on the ACG for the specified SAP port: • *dual: the Two Rate Three Color Marker (RFC 2698)* • *single: the Single Rate Three Color Marker (RFC 2697)*
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: • *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* • *single: (optional)the Single Rate Three Color Marker (RFC 2697)*

Command	Description
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): - *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): - *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): - *value: in the range of <1-1048575> Kbps*
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): - *value: in the range of <1-1048575> Kbps*
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): - *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified SAP port: - *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP***]**	Removes the traffic redirection from the specified SAP port: - *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: - *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: - *vlan-id: (optional) in the range of <1-4095>*

Command	Description
ip-access-group-extended {*NAME* **|** **<***acl-number***>} {in | out}**	Mandatory Assigns an IP ACG to a port: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <100-199>* • *in: filters the ingress traffic only* • *out: filters the egress traffic only*
no ip-access-group-extended [*NAME* **|** **<***acl-number***>] [in | out]**	Removes the specified IP ACG: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <100-199>* • *in: (optional) filters the ingress traffic only* • *out: (optional) filters the egress traffic only*
fc *<value>*	Defines a default mapping of ACG to forwarding class (FC) and color: • *value: FC value (see* **Error! Reference source not found.***)*
no fc *<value>*	Restores the mapping: • *value: (optional) FC value*
color {red | green | yellow}	Defines the conforming level: • *red: the non-conforming drop level* • *green: the conforming drop level* • *yellow: the partially conforming level*
monitoring-profile <*profile-id***>**	Enables bandwidth counters per ACL rules: • *profile-id: in the range of <1–12>* Default Disabled
no monitoring-profile [<*profile-id***>]**	Disables the bandwidth monitoring: • *profile-id: (optional) in the range of <1–12>*
rate-limit {dual | single}	Applies a rate-limit on the ACG for the specified port: • *dual: the Two Rate Three Color Marker (RFC 2698)* • *single: the Single Rate Three Color Marker (RFC 2697)*

Command	Description
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: - *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* - *single: (optional)the Single Rate Three Color Marker (RFC 2697)*
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): - *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): - *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): - *value: in the range of <1-1048575> Kbps*
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): - *value: in the range of <1-1048575> Kbps*
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): - *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified port: - *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP***]**	Removes the traffic redirection from the specified port: - *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: - *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: - *vlan-id: (optional) in the range of <1-4095>*

Command	Description
show port ip-access-group-standard [*NAME* **|** *<acl-number>*] **[in | out] [monitoring-profile [statistics [green-bps | green-fps | match-counter-bps | match-counter-fps | not-green-bps | not-green-fps | not-red-bps | not-red-fps | red-bps | red-fps | yellow-bps | yellow-fps]]]**	Displays the standard IP ACGs configured on ports: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <1-99>* • *in: only ingress ACGs* • *out: only egress ACGs* • *monitoring-profile statistics: counts match packets*
show port ip-access-group-extended [*NAME* **|** *<100-199>*] **[in | out] [monitoring-profile [statistics [green-bps | green-fps | match-counter-bps | match-counter-fps | not-green-bps | not-green-fps | not-red-bps | not-red-fps | red-bps | red-fps | yellow-bps | yellow-fps]]]**	Displays information about the extended IP ACGs, filtered by the commands' arguments
show running-config ip access-list	Displays the configured IP ACLs
show running-config ip access-list standard [*NAME* **|** *<1-99>***] [remark** *REMARK* **| rule {***<1-255>* **| {action {deny | permit} | inner-vlan <***vlan-id***> [inner-vlan-mask <***VLAN mask***>] | inner-vpt <***priority***> | source_ip** *A.B.C.D/MASK* **| untagged | vlan <***vlan-id***> [vlan-mask <***vlan-mask***>] | vpt** *<priority>***}}]**	Displays information about the standard IP ACLs, filtered by the commands' arguments
show running-config ip access-list extended [*NAME* **|** *<100-199>***] [remark** *REMARK* **| rule {***<1-255>* **| {action {deny | permit} | destination_ip** *A.B.C.D/MASK* **| established | icmp-code** *<value>* **| icmp-type** *<value>* | **inner-vlan <***vlan-id***> [inner-vlan-mask <***vlan-mask***>] | inner-vpt <***priority***> | precedence** *TYPE* **| protocol <***type***> | source_ip** *A.B.C.D/MASK* **| tcp-destination-port** *<value>* | **tcp-source-port** *<value>* **| tos {<***0-7***> | max-reliability | max-throughput | min-delay | min-monetary-cost | normal} | udp-destination-port** *<value>* | **udp-source-port** *<value>* **| untagged | vlan <***vlan-id***> [vlan-mask <***vlan-mask***>] | vpt <***priority***>}}]**	Displays information about the extended IP ACLs, filtered by the commands' arguments

Command	Description
show running-config access-group-monitoring-profile [<*profile-id***>] [enable-statistics] [match-counter-bps | match-counter-fps | rate-limit-statistics-green-notgreen-bps | rate-limit-statistics-green-notgreen-fps | rate-limit-statistics-green-red-bps | rate-limit-statistics-green-red-fps | rate-limit-statistics-green-yellow-bps | rate-limit-statistics-green-yellow-fps | rate-limit-statistics-red-notred-bps | rate-limit-statistics-red-notred-fps | rate-limit-statistics-red-yellow-bps | rate-limit-statistics-red-yellow-fps]**	Displays information about the monitoring-counter profiles, filtered by the commands' arguments
show sap-access-group-statistics	Displays the IP ACGs configured on SAP ports
mac access-list {*NAME* **|** *<acl-number>***}**	Mandatory Defines an extended MAC ACL: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <400-499>*
no mac access-list [*NAME* **|** *<acl-number>***]**	Removes the selected extended MAC ACL: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <400-499>*
remark *REMARK*	Associates a remark to an extended MAC ACL: • *REMARK: a string of <1-30> characters*
no remark	Removes the remark
rule <*value***>**	Mandatory Creates an extended MAC ACL rule for filtering traffic: • *value: in the range of <1-255>*
no rule [<*value***>]**	Removes the extended MAC ACL rule: • *value: (optional) in the range of <1-255>*

Command	Description
action {deny | permit}	Mandatory Defines the rule conditions: - *deny: denies packets* - *permit: permits packets*
da-type <*type***>**	Defines the traffic type: - *type:* see **Error! Reference source not found.**
no da-type [<*type***>]**	Removes the traffic type: - *type: (optional)* see **Error! Reference source not found.**
destination_mac *HH:HH:HH:HH:HH:HH* **destination_mac_mask** *HH:HH:HH:HH:HH:HH*	Mandatory Defines the destination MAC address and mask the packet is sent to: - *HH:HH:HH:HH:HH:HH: MAC address and mask in hexadecimal format. The any keyword that represents all MAC addresses*
inner-vlan <*vlan-id***> [inner-vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the inner IP-header: - *vlan-id: in the range of <1-4095>* - *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*
no inner-vlan [<*vlan-id***>] [inner-vlan-mask [<***vlan-mask***>]]**	Removes the selected inner-VLAN and inner-mask: - *vlan-id: (optional) in the range of <1-4095>* - *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*
inner-vpt <*priority***>**	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the inner-VLAN tag header: - *priority: in the range of <0-7>*
no inner-vpt [<*priority***>]**	Removes the selected VPT: - *priority: (optional) in the range of <0-7>*
precedence *TYPE*	The ACL rule matches packets by the literal precedence values: - *TYPE:* see **Error! Reference source not found.**
no precedence	Removes the precedence value

Command	Description
source_mac *HH:HH:HH:HH:HH:HH* **source_mac_mask** *HH:HH:HH:HH:HH:HH*	Mandatory Defines the packet's source MAC-address and mask: - *HH:HH:HH:HH:HH:HH: MAC address and mask in hexadecimal format. The any keyword that represents all MAC addresses*
tos <*value***>**	The ACL rule matches packets by the service level type: - *value: in the range of <0-7> or a valid literal ToS value (see* **Error! Reference source not found.***)*
no tos	Removes the valid literal ToS value
untagged	The ACL rule matches untagged packets only Default Both tagged and untagged
no untagged	Restores to default
vlan <*vlan-id***> [vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the outer IP-header: - *vlan-id: in the range of <1-4095>* - *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*
no vlan [<*vlan-id***>] [vlan-mask [<***vlan-mask***>]]**	Removes the selected outer-VLAN and outer-mask: - *vlan-id: (optional) in the range of <1-4095>* - *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*
vpt *<priority>*	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the outer-VLAN tag header: - *priority: in the range of <0-7>*
no vpt [*<priority>***]**	Removes the selected VPT: - *priority: (optional) in the range of <0-7>*
port *UU/SS/PP*	Enters the Port's Configuration mode

Command	Description
mac-access-group {*NAME* | *<acl-number>*} {**in** | **out**}	Mandatory Assigns a MAC ACG to a port: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <400-499>* • *in: filters the ingress traffic only* • *out: filters the egress traffic only*
no mac-access-group [*NAME* | *<acl-number>*] [**in** | **out**]	Removes the specified MAC ACG: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <400-499>* • *in: (optional) filters the ingress traffic only* • *out: (optional) filters the egress traffic only*
fc *<value>*	Defines a default mapping of ACG to forwarding class (FC) and color. • *value: FC value (see* **Error! Reference source not found.***)*
no fc [*<value>*]	Restores the mapping: • *value: (optional) FC value*
color {**red** | **green** | **yellow**}	Defines the conforming level: • *red: the non-conforming drop level* • *green: the conforming drop level* • *yellow: the partially conforming level*
monitoring-profile **<***profile-id***>**	Enables bandwidth counters per ACL rules: • *profile-id: in the range of <1–12>*
no monitoring-profile **[<***profile-id***>]**	Disables the bandwidth monitoring: • *profile-id: (optional) in the range of <1–12>*
rate-limit {**dual** | **single**}	Applies a rate-limit on the ACG for the specified port: • *dual: the Two Rate Three Color Marker (RFC 2698)* • *single: the Single Rate Three Color Marker (RFC 2697)*

Command	Description
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: • *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* • *single: (optional)the Single Rate Three Color Marker (RFC 2697)*
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): • *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): • *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): • *value: in the range of <1-1048575> Kbps*
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): • *value: in the range of <1-1048575> Kbps*
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): • *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified port: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP*]	Removes the traffic redirection from the specified port: • *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: • *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: • *vlan-id: (optional) in the range of <1-4095>*

Command	Description
mac-access-group {*NAME* **|** *<acl-number>***} {in | out}**	Mandatory Assigns a MAC ACG to a SAP: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <400-499>* • *in: filters the ingress traffic only* • *out: filters the egress traffic only*
no mac-access-group [*NAME* **|** *<acl-number>***] [in | out]**	Removes the specified MAC ACG: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <400-499>* • *in: (optional) filters the ingress traffic only* • *out: (optional) filters the egress traffic only*
fc *<value>*	Defines a default mapping of ACG to forwarding class (FC) and color: • *value: FC value (see* **Error! Reference source not found.***)*
no fc [*<value>***]**	Restores the mapping: • *value: (optional) FC value*
color {red | green | yellow}	Defines the conforming level: • *red: the non-conforming drop level* • *green: the conforming drop level* • *yellow: the partially conforming level*
monitoring-profile <*profile-id***>**	Enables bandwidth counters per ACL rules: • *profile-id: in the range of <1–12>*
no monitoring-profile [<*profile-id***>]**	Disables the bandwidth monitoring: • *profile-id: (optional) in the range of <1–12>*
rate-limit {dual | single}	Applies a rate-limit on the ACG for the specified port: • *dual: the Two Rate Three Color Marker (RFC 2698)* • *single: the Single Rate Three Color Marker (RFC 2697)*

Command	Description
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: - *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* - *single: (optional)the Single Rate Three Color Marker (RFC 2697)*
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): - *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): - *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): - *value: in the range of <1-1048575> Kbps*
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): - *value: in the range of <1-1048575> Kbps*
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): - *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified port: - *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP***]**	Removes the traffic redirection from the specified port: - *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: - *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: - *vlan-id: (optional) in the range of <1-4095>*

Command	Description
show port mac-access-group [*NAME* | *<acl-number>*] [**in** | **out**] [**monitoring-profile** [**statistics** [**green-bps** | **green-fps** | **match-counter-bps** | **match-counter-fps** | **not-green-bps** | **not-green-fps** | **not-red-bps** | **not-red-fps** | **red-bps** | **red-fps** | **yellow-bps** | **yellow-fps**]]]	Displays the MAC ACGs: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <400-499>* • *in: only ingress ACGs* • *out: only egress ACGs* • *monitoring-profile: the rate, in frame per second and bytes per second, of transmitted packets that are marked as red, green, or yellow on a selected port* • *statistics: counts match packets*
show running-config mac access-list	Displays information about the extended MAC ACLs
show running-config mac access-list [*NAME* | *<acl-number>*] [**remark** *REMARK* | **rule** {*<value>* | {**action** {**deny** | **permit**} | **da-type** **<***type***>** | **destination_mac** *HH:HH:HH:HH:HH:HH* **destination_mac_mask** *HH:HH:HH:HH:HH:HH* | **inner-vlan** **<***vlan-id***>** [**inner-vlan-mask** **<***vlan-mask***>**] | **inner-vpt** *priority***>** | **precedence** *TYPE* | **source_mac** *HH:HH:HH:HH:HH:HH* **source_mac_mask** *HH:HH:HH:HH:HH:HH* | **tos** {**<***0-7***>** | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **untagged** | **vlan** **<***vlan-id***>** [**vlan-mask** **<***vlan-mask***>**] | **vpt** *<priority>*}}]	Displays information about the extended MAC ACLs, filtered by the commands' arguments
	•
	•

Command	Description
ether-type access-list {*NAME* | *<acl-number>*}	Mandatory Defines an EtherType ACL: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <500-599>*

Command	Description
no ether-type access-list {*NAME* | *<acl-number>*}	Removes the selected EtherType ACL: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <500-599>*
remark *REMARK*	Associates a remark to an EtherType ACL: • *REMARK: a string of <1-30> characters*
no remark	Removes the remark
rule <*value***>**	Mandatory Creates an EtherType ACL rule for filtering traffic: • *value: in the range of <1-255>*
no rule [<*value***>]**	Removes the EtherType ACL rule: • *value: (optional) in the range of <1-255>*
action {deny | permit}	Mandatory Defines the rule conditions: • *deny: denies packets* • *permit: permits packets*
ether-type <*type***>**	Mandatory Matches the 16-bit hexadecimal value specifying the EtherType: • *type: see* **Error! Reference source not found.**
no ether-type [<*type***>]**	Removes the specified EtherType: • *type: (optional) see* **Error! Reference source not found.**
inner-vlan <*vlan-id***> [inner-vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the inner IP-header: • *vlan-id: in the range of <1-4095>* • *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*
no inner-vlan [<*vlan-id***>] [inner-vlan-mask [<***vlan-mask***>]]**	Removes the selected inner-VLAN and inner-mask: • *vlan-id: (optional) in the range of <1-4095>* • *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*

Command	Description
inner-vpt <*priority***>**	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the inner-VLAN tag header: • *priority: in the range of <0-7>*
no inner-vpt [<*priority***>]**	Removes the selected VPT: • *priority: (optional) in the range of <0-7>*
precedence *TYPE*	The ACL rule matches packets by the literal precedence values: • *TYPE: see* **Error! Reference source not found.**
no precedence	Removes the precedence value
tos <*value***>**	The ACL rule matches packets by the service level type: • *value: in the range of <0-7> or a valid literal ToS value (see* **Error! Reference source not found.***)*
no tos	Removes the valid literal ToS value
vlan <*vlan-id***> [vlan-mask <***vlan-mask***>]**	Denies a specific VLAN ID and mask for the outer IP-header: • *vlan-id: in the range of <1-4095>* • *vlan-mask: in hexadecimal format FF:FF:FF:FF. Use 0 for meaningful bits (exact-match) and F for meaningless bits (any)*
no vlan [<*vlan-id***>] [vlan-mask [<***vlan-mask***>]]**	Removes the selected outer-VLAN and outer-mask: • *vlan-id: (optional) in the range of <1-4095>* • *vlan-mask: (optional) in hexadecimal format FF:FF:FF:FF*
vpt *<priority>*	Defines the packet's filtering by the VLAN Priority Tag (VPT) in the outer-VLAN tag header: • *priority: in the range of <0-7>*
no vpt [*<priority>***]**	Removes the selected VPT: • *priority: (optional) in the range of <0-7>*
port *UU/SS/PP*	Enters the Port's Configuration mode

Command	Description
ether-type-access-group {*NAME* **|** *<acl-number>***} {in | out}**	Mandatory Assigns a Ether-type ACG to a port: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <500-599>* • *in: filters the ingress traffic only* • *out: filters the egress traffic only*
no ether-type-access-group [*NAME* **|** *<acl-number>***] [in | out]**	Removes the specified ether-type ACG: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <500-599>* • *in: (optional) filters the ingress traffic only* • *out: (optional) filters the egress traffic only*
fc *<value>*	Defines a default mapping of ACG to forwarding class (FC) and color. • *value: FC value (see* **Error! Reference source not found.** *)*
no fc [*<value>***]**	Restores the mapping: • *value: (optional) FC value*
color {red | green | yellow}	Defines the conforming level: • *red: the non-conforming drop level* • *green: the conforming drop level* • *yellow: the partially conforming level*
monitoring-profile <*profile-id***>**	Enables bandwidth counters per ACL rules: • *profile-id: in the range of <1–12>*
no monitoring-profile [<*profile-id***>]**	Disables the bandwidth monitoring: • *profile-id: (optional) in the range of <1–12>*
rate-limit {dual | single}	Applies a rate-limit on the ACG for the specified port: • *dual: the Two Rate Three Color Marker (RFC 2698)* • *single: the Single Rate Three Color Marker (RFC 2697)*

Command	**Description**
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: - *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* - *single: (optional)the Single Rate Three Color Marker (RFC 2697)*
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): - *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): - *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): - *value: in the range of <1-1048575> Kbps*
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): - *value: in the range of <1-1048575> Kbps*
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): - *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified port: - *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP*]	Removes the traffic redirection from the specified port: - *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: - *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: - *vlan-id: (optional) in the range of <1-4095>*

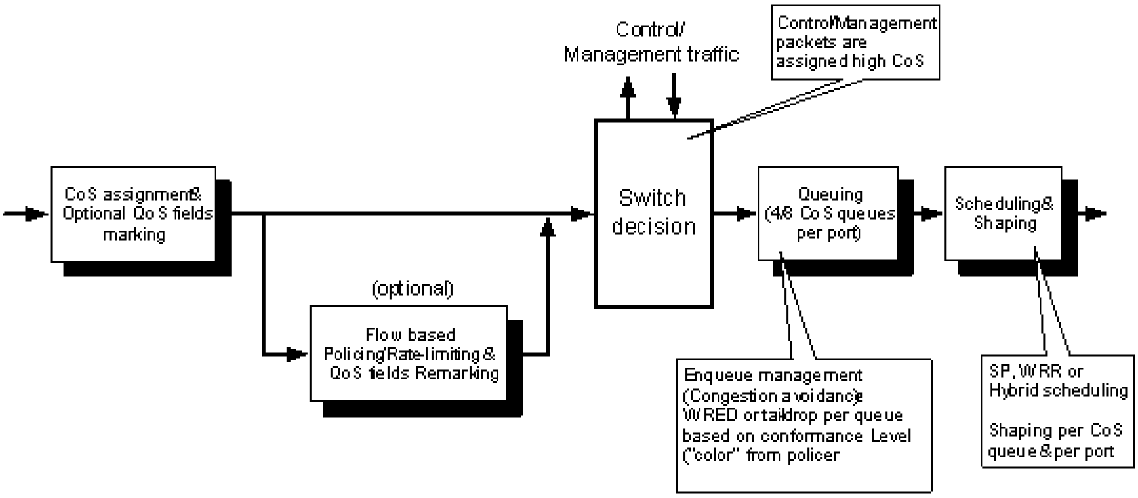
Command	Description
ether-type-access-group {*NAME* **|** *<acl-number>***} {in | out}**	Mandatory Assigns a Ether-type ACG to a SAP: • *NAME: a string of <1-10> characters* • *acl-number: in the range of <500-599>* • *in: filters the ingress traffic only* • *out: filters the egress traffic only*
no ether-type -access-group [*NAME* **|** *<acl-number>***] [in | out]**	Removes the specified ether-type ACG: • *NAME: (optional) a string of <1-10> characters* • *acl-number: (optional) in the range of <500-599>* • *in: (optional) filters the ingress traffic only* • *out: (optional) filters the egress traffic only*
fc *<value>*	Defines a default mapping of ACG to forwarding class (FC) and color: • *value: FC value (see* **Error! Reference source not found.***)*
no fc [*<value>***]**	Restores the mapping: • *value: (optional) FC value*
color {red | green | yellow}	Defines the conforming level: • *red: the non-conforming drop level* • *green: the conforming drop level* • *yellow: the partially conforming level*
monitoring-profile <*profile-id***>**	Enables bandwidth counters per ACL rules: • *profile-id: in the range of <1–12>*
no monitoring-profile [<*profile-id***>]**	Disables the bandwidth monitoring: • *profile-id: (optional) in the range of <1–12>*
rate-limit {dual | single}	Applies a rate-limit on the ACG for the specified port: • *dual: the Two Rate Three Color Marker (RFC 2698)* • *single: the Single Rate Three Color Marker (RFC 2697)*

Command	Description
no rate-limit [dual | single]	Removes the rate limit from the configured ACG: • *dual: (optional) the Two Rate Three Color Marker (RFC 2698)* • *single: (optional)the Single Rate Three Color Marker (RFC 2697)*
cbs *<value>*	(only for single rate) Defines the Committed Burst Size (CBS): • *value: in the range of <1-1048575> Kbps*
cir *<value>*	(only for single rate) Defines the Committed Information Rate (CIR): • *value: in the range of <1-1048575> Kbps*
color-aware	Enables the color-aware mode Default Color blind
ebs *<value>*	(only for single rate) Defines the Excess Information Rate (EBS): • *value: in the range of <1-1048575> Kbps*
pbs *<value>*	(only for dual rate) Defines the Peak Burst Size (PBS): • *value: in the range of <1-1048575> Kbps*
pir *<value>*	(only for dual rate) Defines the Peak Information Rate (PIR): • *value: in the range of <1-1048575> Kbps*
redirect *UU/SS/PP*	Redirects matching traffic to the specified port: • *UU/SS/PP: 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
no redirect [*UU/SS/PP***]**	Removes the traffic redirection from the specified port: • *UU/SS/PP: (optional) 1/1/1-1/1/16, 1/2/1-1/2/8, 1/3/1, 1/3/2, 1/4/1 and 1/4/2*
vlan <*vlan-id***>**	Redirects matching traffic to the specified VLAN by changing the VLAN ID in the packet header: • *vlan-id: in the range of <1-4095>*
no vlan [<*vlan-id***>]**	Removes the traffic redirection: • *vlan-id: (optional) in the range of <1-4095>*

Command	Description
show port ether-type-access-group [*NAME* **|** *<500-599>*] **[in | out] [monitoring-profile [statistics [green-bps | green-fps | match-counter-bps | match-counter-fps | not-green-bps | not-green-fps | not-red-bps | not-red-fps | red-bps | red-fps | yellow-bps | yellow-fps]]]**	Displays information about the EtherType ACGs, filtered by the commands' arguments
show running-config ether-type access-list	Displays information about the EtherType ACLs
show running-config ether-type access-list [*NAME* **|** *<500-599>*] **[remark** *REMARK* **| rule {***<1-255>* **| {action {deny | permit} | ether-type <***type***> | inner-vlan <***vlan-id***> [inner-vlan-mask <***vlan-mask***>] | inner-vpt <***priority***> | precedence** *TYPE* **| tos {<***0-7***> | max-reliability | max-throughput | min-delay | min-monetary-cost | normal} | vlan <***vlan-id***> [vlan-mask <***vlan-mask***>] | vpt** *<priority>***}}]**	Displays information about the EtherType ACLs, filtered by the commands' arguments

Quality of Service (QoS)

The legacy (or 'flat') QoS, supported by most of the equipment used in service provider Carrier Ethernet/IP today (including from RADiFlow). A typical functional model of legacy QoS implementation is shown in the figure below.

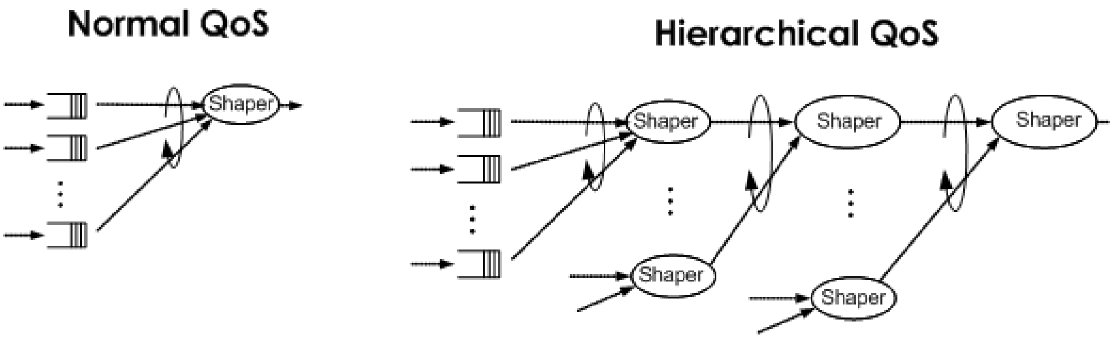

Control/
Management traffic
Control/Management packets are assigned high CoS
CoS assignment & Optional QoS fields marking
Switch decision
Queuing (4/8 CoS queues per port)
Scheduling & Shaping
(optional)
Flow based Policing/Rate-limiting & QoS fields Remarking
Enqueue management (Congestion avoidance) WRED or taildrop per queue based on conformance Level ("color" from policer
SP, WRR or Hybrid scheduling
Shaping per CoS queue & per port

The main characteristics of this model are:

- On ingress - Traffic from each service is classified to its own "flow" for policing and QoS fields marking
- On egress - other packet handling functions are done per CoS (i.e. queuing, scheduling, shaping)

The QoS implementation enhances the 'flat' QoS model by introducing multi-level hierarchy for both flow classification and traffic management by providing per customer/service hierarchical queuing, scheduling and shaping for both service ingress and service egress.

This model allows an SLA to be defined on both customer and service levels, where multiple customers can be connected to each port, and each customer is subscribed to multiple services.



The QoS capabilities are a critical component in providing "hard QoS" guaranties required by current and next generation carrier Ethernet services (e.g. triple-play).

QoS Specifications

- Queuing
  - 24 queues per L2 scheduler - 12096 queues per each direction (504 L2 schedulers * 24 queues per direction)
  - Flexible per service queues allocation:
    - Per forwarding class
    - Separate queues for unicast, multicast and broadcast traffic
    - 24 queues per L2 scheduler (8 queues per traffic type)
- Hierarchical scheduling and shaping
  - 2 scheduling levels per service: Queues → L2 schedules → L1 (root) schedulers
  - 504 ingress and 504 egress (**currently not supported**) L2 schedulers
  - 126 L1 schedulers (63 ingress + 63 egress (**currently not supported**))
  - Each scheduler in the hierarchy supports the following programmable scheduling scheme:
  - 2 priorities support (high/low) with strict priority scheduling
  - For single WFQ only queues is used
- Congestion avoidance and buffer space allocation
  - WRED and buffer allocation per queue and per port

QoS Management

- Policy-based QoS configuration
  - Policy management model allows for flexible and extensive service SLA provisioning:
    - Multi-service
    - Multi-application
  - Policies can be configured once and applied to multiple services for ease of configuration and EMS/NMS integration

QoS Advantages

QoS related mechanism enable the following advantages:

- Per service/customer shaping
  - Improved isolation of traffic between different services/customers with the same CoS assigned
  - Large traffic bursts from a specific service/customer can no longer cause packet loss for traffic from another service/customer with the same CoS
  - Enhanced fairness between services/customers with the same CoS
- Ingress shaping
  - Shaping is done on ingress (after switch decision and packet duplication)
  - As a result in cases where the traffic from a specific customer/service needs to be switched to several network interfaces the shapers on the network ports can't represent the over-all bandwidth profile for that customer/service (or aggregate of customers/services flows)
  - By supporting ingress shaping the device can effectively limit bursts at the UNI level before entering the service provider network
- Hierarchical SLA
  - By utilizing the per service/customer hierarchical queuing, scheduling and shaping capabilities provided with QoS it is possible for the service provider to define and enforce hierarchical SLAs
  - More detailed usage examples are provided in the next section
- Enhanced statistics
  - Granular per flow/queue statistics on both service ingress and service egress all for end-to-end SLA conformance verification

QoS Mechanisms

The following sections describe in detail the various QoS mechanisms as they are implemented by the device.

Weighted Fair Queuing (WFQ) Scheduling

The device uses weighted fair queuing (WFQ) for scheduling transmitted traffic in cases of congestion. WFQ is used for traffic passing through the Network Processor.

During congestion, the WFQ enables each of the participating entities in each scheduling level to receive byte wise fair share of the available bandwidth by using a simple credit calculation as follows. In each time slot, each entity is allowed to transmit X bytes where X is proportional to the relative weight.

For example, if relative weight for all entities in the same scheduling level is equal (weight=1 for all entities), then all entities receive the same credit for transmission resulting in a behavior that is similar to a simple Round Robin fair scheduling. Each entity receives a limited amount of credits for transmission (in this example, 100). The 1st Entity in this example transmits 100 byte frames while the 2nd entity transmits 1k byte frames. After transmitting the first frame, the 1st Entity is left with 0 credits while the 2nd Entity is left with -900 credits. New credits are provisioned … (100, -800), now only the 1st entity has positive amount of credits and is allowed to transmit. Such cycles continue 10 times until the 2nd Entity has positive amount of credits and is again allowed to transmit.

Two instances of WFQ scheduling are applied to L2 schedulers and network queues. One instance is for all in-profile traffic (within the CIR) and a different instance is for all excess traffic (between the CIR and the PIR). Each entity is configured with WFQ profiles including weight for in-profile traffic ('cir-weight') and weight for out-of-profile traffic.

A single instance of WFQ scheduling is used for the service queues. Each service Queue is configured with a single WFQ weight for all traffic.

Shaping (Bandwidth Provisioning)

The device's features shaping for allocating maximum bandwidth guarantee without dropping packets. The QoS shapers described here can be applied only for traffic going through the Network Processor.

The shaping implementation in the device uses dual-rate token based metering. This implementation is similar to the color blind metering described in IETF RFC 2698. CIR and PIR are used for limiting the traffic rate, while CBS and MBS are used for allowing temporary bursts to breach the PIR as part of the SLA.

Weighted Random Early Detection (WRED)

A WRED profile is used for each Queue, consisting of two sets of parameters. One set is used to perform drop decisions for packets marked as 'green' and the second set for packets marked as 'yellow'. The drop decision for each packet is based on drop probability, which is a function of the packet color (yellow or green) and the current average queue depth.

Policy-based QoS Management

The QoS implementation is based on Policies and Profiles, which allow easy and robust management. The idea behind the Policy-based management is that a carrier usually provides a limited number of "packages" to its customers, with multiple customers purchasing the same package. Most of the SLAs with the customers would be based on these "packages" as templates.

For example, a Premium Business package could be a true VPN and triple-play package including VPN, Voice, Video and Internet with 10Mb/s of overall bandwidth. On the other hand, a Basic Business package would include VPN and Internet only, with lower overall bandwidth allocation (e.g. 3Mb/s).

Once a customer subscribes to a package, the network allocates the required resources both for the service(s) and the QoS implementation. For QoS implementation, a set of resources (such as queues, schedulers, buffer space etc.) will be allocated inside the device. In Telco QoS terminology, this is called instantiation of a Policy. Once another customer has subscribed to the same package, the same Policy will be instantiated again, which means additional and identical set of resources will be allocated.

In some cases it makes sense to share a Policy instance between multiple customers. This technique is useful to save resources, although it means no true per-customer SLA assurance can be performed (for example, these customers will share the same shapers, and eventually the same allowed bandwidth).

The device supports several types of Policies (described in detail in the following subsections). Each Policy type includes parameters related to a different set of QoS features. Both non-shared and shared policy instantiation modes are supported, with some limitations as explained in the sub-sections below.

In addition, some of the features are configured using Profiles. Unlike Policies, Profiles are low-level "templates", each defining parameters for a single distinctive QoS feature. Profiles are used not to allocate resources, but rather to configure resources that were already allocated.

For example, a Policy when instantiated could allocate a queue, which would automatically allocate also a WRED instance. A WRED profile would then be used to configure that WRED instance. In this example, there is no direct relation between the number of Queue Policies and the number of WRED Profiles.

Please note that in the current release of the product, only the QoS resources implemented on the 'Network Processor' are managed using Policies.

Service-related Policies

The device supports the following Service-related QoS policies:

- Service Ingress Policy
    - Applied per SAP
    - Defines mapping of VPT / DSCP values to FC and Color
    - Defines mapping of FC to unicast, multicast and broadcast service ingress queues
    - Defines the parent L2 scheduler as well as WFQ and WRED profiles for each queue
- Ingress Scheduling Policy
    - Defines the configuration of service ingress L1 and L2 schedulers, including their WFQ and shaping profiles.

These policies, when applied to SAPs, govern how queues and schedulers are allocated. By managing configuration of these polices and applying them to SAPs you can control how these resources are allocated.

Both shared and dedicated Policy instantiation is supported.

Profiles

Profiles are used within QoS policies. Each profile includes a set of configurable values that can be applied.

The device supports the following QoS profile types:

- WFQ Profile:
    - Applied to service queues, L2 schedulers and network queues
    - Defines WFQ weights for in-profile and out-of-profile traffic
- Shaper Profile:
    - Applied to service-related shapers (L2 or L1), network queues shapers and network port shapers
    - Defines dual-rate shaping parameters (CIR, PIR, CBS, MBS)
- WRED Profile:
    - Applied to service ingress/egress and network egress queues.
    - Defines color-aware WRED parameter for the queue (min. & max. yellow threshold, max. yellow drop probability, min. & max. green threshold and max. green drop probability).

QoS Granularity Table

The following table shows the extent to which a larger entity is subdivided.

QoS parameter	Range allowed by CLI	Step
L2 CIR and PIR	16 Kbps–4096 Kbps	16 Kbps
	4096 Kbps–16384 Kbps	64 Kbps
	16384 Kbps–65536 Kbps	256 Kbps
	65536 Kbps–10 Gbps	4096 Kbps
L2 CBS and MBS	16 KB–256 KB	1 KB
	256 KB–2 MB	8 KB
	2 MB–16 MB	64 KB
	16 MB–32 MB	128 KB
L1 CIR and PIR	80 Kbps–20480 Kbps	80 Kbps
	20480 Kbps–81920 Kbps	320 Kbps
	81920 Kbps–327680 Kbps	1280 Kbps
	327680 Kbps–10 Gbps	20480 Kbps
L1 CBS and MBS	16 KB–256 KB	1 KB
	256 KB–2 MB	8 KB
	2 MB–16 MB	64 KB
	16 MB–64 MB	512 KB

The following table lists cases of inaccuracy in QoS shaper values (currently not supported)

Network egress	Primary tunnel inaccuracy (bytes per packet)	Backup tunnel inaccuracy (bytes per packet)
Qualified SAP and VC type VLAN	+4	+8
Qualified SAP and VC type Ethernet	0	+4
Unqualified SAP and VC type Ethernet	+4	+8

Service egress	Primary tunnel inaccuracy (bytes per packet)	Backup tunnel inaccuracy (bytes per packet)
Qualified SAP and VC type VLAN	0	0
Qualified SAP and VC type Ethernet	0	0
Unqualified SAP and VC type Ethernet	-4	-4

QoS Command Hierarchy

Shaping Profile, WFQ Profile and WRED Profile Commands Hierarchy

```
+ root
        + config terminal
          + qos
                + [no] root-scheduler-shaper-profile ingress <shaping-profile-
                    id>
                     - [no] cbs <cbs>
                     - [no] cir <cir>
                     - [no] pbs <pbs>
                     - [no] pir <pir>
                +  [no]  root-scheduler-shaper-profile  egress  <shaping-profile-
                    id> (currently not supported)
                     - [no] cbs <cbs>
                     - [no] cir <cir>
                     - [no] pbs <pbs>
                     - [no] pir <pir>
```

```
+ [no] scheduler-shaper-profile ingress <shaping-profile-id>
     - [no] cbs <cbs>
     - [no] cir <cir>
     - [no] pbs <pbs>
     - [no] pir <pir>
+ [no] scheduler-wfq-profile ingress <scheduler-wfq-profile-id>
     - [no] cirWeight <cir-weight>
     - [no] weight <weight>
+ [no] service-wfq-profile ingress <service-wfq-profile-id>
     - [no] weight <weight>
+ [no] wred-profile <wred-profile-id>
     - green_max <max>
     - green_min <min>
     - green_prob <prob>
     - yellow_max <max>
     - yellow_min <min>
     - yeloow_prob <prob>
```

Command	Description
`config terminal`	Enters the Configuration mode
`qos`	Enters the QoS Configuration mode
`root-scheduler-shaper-profile ingress <shaping-profile-id>`	Creates a root scheduler shaper profile that is applied to ingress L1 schedulers: - *shaping-profile-id: in the range of <3-16>*
`no root-scheduler-shaper-profile ingress [<shaping-profile-id>]`	Removes root scheduler shaper profiles: - *shaping-profile-id: (optional) in the range of <3-16>*
`scheduler-shaper-profile ingress <shaping-profile-id>`	Creates a scheduler shaper profile that is applied to ingress L2 schedulers: - *shaping-profile-id: in the range of <65-216>*
`no scheduler-shaper-profile ingress [<shaping-profile-id>]`	Removes scheduler shaper profiles: - *shaping-profile-id: (optional) in the range of <65-216>*
`cbs <cbs>`	Mandatory Specifies the Committed Burst Size value: - *cbs: in the range of <16-65535> kbps*
`no cbs`	Removes the CBS

Command	Description
cir *<cir>*	Mandatory Specifies the Committed Information Rate value: • *cir: in the range of <80-1048575> kbps*
no cir	Removes the CIR
pbs *<pbs>*	Mandatory Specifies the Peak Burst Size value: • *pbs: in the range of <16-65535> kbps*
no pbs	Removes the PBS
pir *<pir>*	Mandatory Specifies the Peak Information Rate value: • *pir: in the range of <80-1048575> kbps*
no pir	Removes the PIR
scheduler-wfq-profile ingress *<scheduler-wfq-profile-id>*	Creates a scheduler WFQ profile that is applied to an ingress L2 scheduler: • *scheduler-wfq-profile-id: in the range <1-84>*
no scheduler-wfq-profile ingress [*<scheduler-wfq-profile-id>***]**	Removes WFQ's profiles: • *scheduler-wfq-profile-id: (optional) in the range <1-84>*
cirWeight *<cir-weight>*	Mandatory Defines the weight assigned for committed traffic: • *cir-weight: in the range of <1-220>*
no cirWeight [*<cir-weight>***]**	Removes the weight
weight *<weight>*	Mandatory Defines the weight assigned for excess traffic: • *weight: in the range of <1-220>*
no weight [*<weight>***]**	Removes the weight
service-wfq-profile ingress *<service-wfq-profile-id>*	Creates a service WFQ profile: • *service-wfq-profile-id: in the range of <1-84>*

Command	Description
no service-wfq-profile ingress [*<service-wfq-profile-id>*]	Removes service WFQ profiles: • *<service-wfq-profile-id>: (optional) in the range of <1-84>*
service-wfq-profile egress *<service-wfq-profile-id>*	**Currently not supported.** Creates a service WFQ profile: • *service-wfq-profile-id: in the range of <1-84>*
no service-wfq-profile egress [*<service-wfq-profile-id>*]	Removes service WFQ profiles: • *service-wfq-profile-id: (optional) in the range of <1-84>*
weight *<weight>*	Mandatory Defines the weight assigned for both committed and excess traffic: • *weight: in the range of <1-220>.*
no weight [*<weight>*]	Restores to default
cirWeight *<cir-weight>*	Mandatory Defines the weight assigned for committed traffic: • *cir-weight: in the range of <1-220>* Default
no cirWeight [*<cir-weight>*]	Restores to default
wred-profile *<wred-profile-id>*	Defines a WRED profile: • *wred-profile-id: in the range of <1-64>.* Default 1—for service ingress queues Default 33—for service egress queues Default 57—for network queues
no wred-profile [*<wred-profile-id>*]	Removes WRED profiles: • *wred-profile-id: (optional) in the range of <1-64>. It is not possible to modify or delete default WRED profiles.*
green_max <*max***>**	Mandatory Defines the Maximum Congestion Level for the green traffic: • *max: in the range of <8-32768> KB* Once this value is reached all green packets are dropped.

Command	Description
green_min <*min***>**	Mandatory Defines the Minimum Congestion Level for the green traffic: • *min: in the range of <0-32768> KB* Once this value is reached partial dropping of green packets start according to the drop probability configured for green traffic.
green_prob <*prob***>**	Mandatory Defines the drop probability for green traffic at the Maximum Congestion Level: • *prob: in the range of <0-100> %*
yellow_max <*max***>**	Mandatory Defines the Maximum Congestion Level for the yellow traffic: • *max: in the range of <8-32768> KB*
yellow_min <*min***>**	Mandatory Defines the Minimum Congestion Level for the yellow traffic: • *min: in the range of <0-32768> KB*
yellow_prob <*prob***>**	Mandatory Defines the drop probability for yellow traffic at the Maximum Congestion Level: • *prob: in the range of <0-100> %*

QoS Display Commands Hierarchy

```
+ root
        - show qos service ingress-policy
        - show qos service {ingress | egress} {shaper-profile | wfq-profile}
        - show qos service sap
        - show qos network-policy
        - show qos scheduler-policy
        - show qos wred-profile
```

Command	Description
`show qos service ingress-policy`	Displays service ingress policy configuration
`show qos service {ingress	egress} {shaper-profile	wfq-profile}`	Displays service policy configuration, filtered by the arguments
`show qos service sap`	Displays QoS SAP information
`show qos network-policy`	Displays the network policy configuration.
`show qos scheduler-policy`	Displays scheduler policy information.
`show qos wred-profile`	Displays the WRED profile configuration.

IP Routing

Creating an IP Interface

The routing software and hardware directs IP traffic between router IP interfaces. A router IP interface is simply a VLAN that has an IP address assigned to it. As VLANs with IP addresses belonging to different IP subnets are created, one can also choose the route between the VLANs. Both the VLAN switching and IP routing function occur within the device. Each IP address and mask assigned to a VLAN must represent a unique IP subnet.

The binding between VLAN and IP addresses (IP Interfaces) is done by using the routing-interface ommand in VLAN Configuration mode (see the *VLANs* chapter of the this User Guide).

User SW type IP interfaces

To create IP interfaces ,either for management over IP or for any layer 3 usage please follow bellow commands to establish SW interface type and assignment to the relevant vlan.

```
+ root
        + config terminal
          + router
                + [no] interface SW[0-99]
                     + address aa.bb.cc.dd/M
                     + description <text>
                     + shutdown
```

1. Example for creation of 2 SW IP interfaces named SW0 and SW1 and assignment to predefined vlans.

```
device-name(config)#router
device-name (config-router)#interface sw0
device-name (config-interface-sw0)#address 172.17.212.200/24
device-name (config-interface-sw0)#exit
device-name (config-router)#interface sw1
device-name (config-interface-sw1)#address 192.18.210.100/24
device-name (config-interface-sw1)#top
device-name(config)#vlan default 1
device-name (config-vlan-default/1)#routing-interface sw0
device-name (config-vlan-default/1)#top
device-name(config)#vlan modbus 3001
device-name (config-vlan-modbus/3001)#routing-interface sw1
device-name (config-vlan-modbus/3001)#top
device-name(config)#commit
device-name(config)#end
device-name#show interface
```

Application IP Interface

To use the unique capabilities of RADiflow as the firewall, 101/104 gateway ,serial tunneling IPsec and more ,the use of the APPLICATION CARD is required.

The application card is installed on slot 3 on the RADiflof 3xx switch or is integrated allready with the 3081 switch.

The application card can be assigned an IP interface and a Gateway spcifically used for the relevant services monitored and processed by it.

The IP interface must be associated with a user predefined VLAN. This vlan will be used to forward the processed traffic to the uplink NNI port.

Application IP Interface Commands Hierarchy

```
+ root
       + application connect
         + router
        - interface {create | remove} <IP address> [netmask] [vlan id]
        - default-gw {create | remove} <IP address>
        - show
```

Command	Description
Application connect	*Enter the industrial application menu*
Router	*Enter the application router configuration mode*
interface *create | remove*	*Add or Remove an IP interface for the application engine. The configuration should include:* • *IP address in the format aa.bb.cc.dd* • *netmask for the IP address. example : 255.255.255.0* • *VLAN ID that the application engine will use for this IP interface*
default-gw *create | remove*	*Define or remove the default gateway for an application IP network*
Show	*Show application engine IP interfaces*

Example for creating Application IP Interface

1. Create a vlan to be used for passing the processed traffic from the application to the nni port.
   port 1/3/1 is mendatory to be assigned as tagged.
   port 1/5/1 is givven as an example for chosen nni port.

```
device-name(config)#vlan nni 100
device-name (config-vlan-nni/100)#tagged 1/3/1
device-name (config-tagged-1/3/1)#tagged 1/5/1
device-name (config-tagged-1/5/1)#tagged commit
device-name (config-tagged-1/5/1)#end
device-name#
```

2. Create an IP interface and gateway.

```
device-name#application connect
RADiFlow Application Module
radiflow-app login: ind
Password:ind
Welcome to Radiflow industrial CLI
[/]router interface create address 192.17.212.100 netmask 255.255.255.0 vlan 100
[/]router default-gw create address 192.17.212.200
[/]commit
[/]commit ok
[/]router show
                    Local IP Address          =172.17.212.100/24
                    VLAN                      =100
                    Default gateway           =172.17.212.200
[/]
```

Populating the Routing Table

The RADiFlow 3300, 3700 devices maintain an IP routing table for both network routes and host routes. The table is populated from the following sources:

- Dynamic routes, typically learned from routing protocol packets (see *Dynamic Routes*)
- Static routes, manually entered by the network administrator (see *Static* Routes). They include:
    - Default routes, configured by the network administrator
    - Local routes, of IP interface addresses assigned to the system
    - Other static routes, configured by the network administrator

Dynamic Routes

Dynamic routes are typically learned by the routing protocol OSPF (see the Open Shortest Path First (OSPF) section). Routers that use the routing protocols exchange information in their routing tables by advertising. Using dynamic routes, the routing table only contains accessible networks. Dynamic routes are deleted from the table when either of the following occurs:

- An update for the network is not received for a period of time that is determined by the routing protocol (i.e., the dynamic route is aged out of the table)
- A neighbor sends a command to delete the dynamic routes advertised by the routing protocol OSPF (by setting the route aging time to the maximum and flooding the LSA to the advertiser neighbors)

Static Routes

Static routes are manually entered into the routing table. Static routes are important in the following cases:

- When the router cannot build a route to a particular destination automatically
- When, for security reasons, you need to make changes to the routing table of the router
- When it is necessary to specify a gateway of last resort to which all unroutable packets will be sent

Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the IP subnet is deleted or down, the static route entries using this IP subnet will become inactive and will not be used, although they will be present in the routing table.

The device remembers the *static routes* until they are manually removed. However, the *static routes* decisions can be overridden by the dynamic routing information through prudent assignment of administrative distance values. Each dynamic routing protocol has a default administrative distance, as indicated in *Table 8*.

NOTE

If you want to override a static route by information received from a dynamic routing protocol, simply ensure that the administrative distance of the static route is higher than that of the dynamic protocol.

Special IP Interfaces

A permanent Layer 3 interface (**sw0**) is attached to the default VLAN. All available ports in the system are attached to this VLAN as untagged. For the device to be able to route between the VLANs, the Layer 3 interfaces must be configured with an IP address.

The **lo1-lo9** Layer 3 interfaces are not directly related to a VLAN. These interfaces can never be in a down state. The packets sent through them are looped back to the IP stack and are then routed on a destination-IP-address basis.

The **Eth0** Layer 3 IP interface is destined for debugging purposes and cannot be used to pass data.

The IP Unicast Routing Default Configuration

Table 11: IP Unicast Routing Default Configuration

Parameter	Default Value
Default IP address for sw0 IP interface	Not defined
IP interface multicast flag	Set
The Default Administrative Distances of the Dynamic Routing Protocols	See *Table 8*
IP Forwarding	Enabled

Table 8: Default Administrative Distances of the Dynamic Routing Protocols

Route Source	Default Distance
Connected IP interface	0
OSPF	110
Unknown	255

IP Command Hierarchy

```
+ root
        + config terminal
          - [no] router static-route A.B.C.D/M A1.B1.C1.D1 <distance-value>
        - show routes RouteEntry {flags {blackhole changed | deleted | ibgp |
            internal | mpls_egress | mpls_ingress | outband | selected |
            self_ip | selfroute | static | staticarp | vrrp_ip} | ifname NAME
            | metrics <metric value> | NextHopFlags {active | fib |
            fibset_outband | notready | outband | recursive} | nexthoptype
            {ifindex | ifname | ipv4 | ipv4_ifindex | ipv4_ifname ipv6 |
            ipv6_ifindex | ipv6_ifname} | uptime <duration> | A.B.C.D/M}
```

The IP Configuration Commands

Table 13: Static Routes Commands

Command	Description
`config terminal`	Enters the Configuration mode
`router static-route A.B.C.D/M A1.B1.C1.D1 <distance-value>`	Defines a static route • *A.B.C.D/M: the destination IP address and mask in dotted-decimal format* • *A1.B1.C1.D1: the gateway IP address* • *distance-value: in the range of <0-255>* Default Disabled
`no router static-route [A.B.C.D/M A1.B1.C1.D1 <distance-value>]`	Removes a specific static route or all configured static routes • *A.B.C.D/M: (optional) the destination IP address and mask in dotted-decimal format* • *A1.B1.C1.D1: (optional)the gateway IP address* • *distance-value: (optional)in the range of <0-255>*

Table 14: IP Unicast Routing Display Command

Command	Description
show routes RouteEntry {flags {blackhole | changed | deleted | ibgp | internal | mpls_egress | mpls_ingress | outband | selected | self_ip | selfroute | static | staticarp | vrrp_ip} | ifname *NAME* **| metrics <***metric value***> | NextHopFlags {active | fib | fibset_outband | notready | outband | recursive} | nexthoptype {ifindex | ifname | ipv4 | ipv4_ifindex | ipv4_ifname ipv6 | ipv6_ifindex | ipv6_ifname} | uptime <***duration***> |** *A.B.C.D/M***}**	Displays the static and directly connected (via configured IP interfaces) routes.

Open Shortest Path First (OSPF)

OSPF is an IGP normally implemented on an AS.

This protocol uses the following algorithms:

Shortest Path First (SPF) algorithm—calculates configurable cost metrics and exchanging routing information between routers in large networks.

Constrained Shortest Path First (CSPF) algorithm—(optional) calculates a path that meet not only the topology of the network but but also the attributes of the LSP and the links, and it minimizes congestion by intelligently balancing the network load. CSPF relies on a Traffic Engineering Database (see ***Error! Reference source not found.***) to do the calculations

Upon initialization, each device transmits a Link State Advertisement (LSA) on each of its IP interfaces. OSPF shares information with every router in the network exchanging the status of networks and links. Each device collects the LSAs of all the devices with in a common area, synchronizing their topological databases, and updating their Link-State Database (LSDB). Using OSPF, all the routers within the area maintain identical LSDBs.

Each router constructs a tree of shortest paths to each destination in the AS, based on the LSDB. The cost of a route is described by a single metric. When several equal-cost routes to a destination exist, traffic can be distributed among them.

Area types

OSPF requires dividing the network into a logical star of areas. The topology within an area is hidden from the rest of the AS. Hiding this information significantly reduces LSA traffic and the calculations needed to maintain the LSDB. Routing within the area is determined only by the topology.

- Backbone Area - This area (also called Area 0) connects all other OSPF areas to each other. Any traffic between areas must go through the backbone area. Due to its role, this area has to be robust and stable. It should have internal redundancy and efficient bandwidth to handle the traffic between areas.
- Stub Area – This area is connected to other areas; one of them may be the backbone area. External route information is not distributed into stub areas. Stub areas are used to reduce memory consumption and computation requirements on OSPF routers.
- Normal Area - An area which is not Area 0 or a Stub area.
- Not-So-Stuby-Area (NSSA) - NSSA is an optional area that does not flood all LSAs from the core into the area, but can import and redistribute AS-external routes within the area.

Link State Advertisement

LSA is a data unit describing the local state of a router or network. There are several types of LSAs, designated by names and numbers, as described below:

Table 15: LSA Type Names and Numbers

LSA Number	LSA Name	LSA Description
1	Router-LSAs	Originated by all routers, a router-LSA describes the collected states of the router IP interfaces to an area
2	Network-LSAs	Contains the list of routers connected to the network
3, 4	Summary-LSAs	A summary-LSA describes a route to a destination outside the area, yet still inside the AS (an inter-area route). It is originated by ABRs and flooded throughout the LSAs associated area. Type 3 summary-LSAs describe routes to networks Type 4 summary-LSAs describe routes to ASBR
5	AS-external-LSAs	Originated by ASBR and flooded throughout the AS, each AS-external-LSA describes a route to a destination in another AS. Default routes for the AS can also be described by AS-external-LSAs.

OSPF Neighbors

Upon initialization, routers running OSPF attempt to locate neighboring routers for exchanging LSAs. Routers form adjacencies with neighboring routers before exchanging routing information. The routers check details, such as subnet address, OSPF area number, network type, and authentication passwords before forming an adjacency.

- On broadcast or point-to-point segments, the routers dynamically discover neighbors through the OSPF multicast, 224.0.0.5, using the OSPF Hello protocol.
- On Non-Broadcast Multiple Access (NBMA) networks the system administrators have to configure neighbors manually before the Hello protocol initializes in a unicast fashion, beginning the adjacency forming process.

OSPF Network Types

OSPF has defined standards for communicating across a diverse set of network media:

Broadcast

The Broadcast OSPF network type typically runs on multi-access broadcast IP interfaces such as Ethernet, Token Ring, or FDDI.

Each Broadcast OSPF area includes one Designated Router (DR) and one Backup Designated Router (BDR) elected dynamically on a broadcast segment with which all other routers form adjacencies. The election criteria include router ID, loopback IP interface presence, and router IP interface priority values.

The system administrators can manually configure these criteria to influence the selection process. The DR and BDR are responsible for collecting link state information from all routers on the broadcast segment, compile, and distribute the resulting area map back to each router. This prevents all routers on a common segment from exchanging link state information with every other router on a segment, thus reducing the amount of traffic on a broadcast segment.

Point-to-point

The point-to-point OSPF network type is typically implemented across dedicated WAN circuits, such as T-1 links or on frame relay point-to-point sub-interfaces.

This network type does not have a designated router since each segment includes only two routers. These routers exchange link state information and routes as peers across a common subnet.

Non-Broadcast Multi-Access (NBMA)

The NBMA network type runs on media such as X.25, frame relay, and ATM, where the network cannot dynamically forward broadcast packets to all other routers in a virtual network. Other than manual OSPF neighbor configuration, the router behavior configured with this network type is identical to that of the broadcast type: the Hello protocol elects the DR and DR, forming adjacencies with all non-DR/BDR routers.

It is important to ensure that a hub router is elected to be the DR on a hub-and-spoke partially meshed frame relay network to ensure that adjacencies can be formed with every spoke.

Point-to-Multipoint

The point-to-multipoint network type runs on NBMA networks, such as Frame relay and ATM. Routers are addressed out of a common IP subnet on WAN IP interfaces. However, this network type does not require a full mesh, since it does not include a DR/BDR election.

This network type is well suited for frame relay hub-and-spoke networks, where

- there is a need for IP addresses conservation or
- the minimization of resource impact of logical IP interfaces on hub routers is an issue

Any-to-any spoke connectivity in a partially meshed PVC environment is possible since the hub router advertises itself as the next-hop forwarding address to all spokes for all routes.

Virtual Links

You can configure virtual links between any two backbone routers that have an IP interface to a common non-backbone area. The protocol treats two routers joined by a virtual link as if they were connected by a point-to-point connection in the backbone.

If you cannot physically connect an area to the backbone area, you can use a virtual link to connect to the backbone through a non-backbone area, known as a *transit area.* The transit area must have full routing information; therefore it cannot be a stub area.

In the image below if the connection between ABR1 and the backbone fails, the connection via ABR2 provides redundancy, ensuring communication between ABR1 and the backbone using the virtual link.

Route Redistribution

ASBRs can exchange routes, including static routes between two routing protocols.

OSPF Timers and Authentication

Configuring OSPF timers and authentication on a per-area basis saves time for applying the timers and authentication to each IP interfaces in the area. If you add more networks to the area, you must configure timers and authentication for the new IP interfaces explicitly.

OSPF Command Hierarchy

OSPF Global Commands

```
+ root
        + config terminal
          + router
                + ospf
                     - [no] router-id A.B.C.D
                     - [no] te-router-id A.B.C.D
                     - [no] auto-cost-refbandwidth <ref-value>
                     - [no] compatible-rfc1583 {false,true}
                     - [no] default-info-originate {false,true}
                     - [no] default-metric <metric-value>
                     - [no] external-distance <external-distance>
                     - [no] intra-area-distance <intra-area-distance>
                     - [no] inter-area-distance <inter-area-distance>
                     - [no] abr-type [Alternative Cisco | Alternative IBM |
                       Alternative Shortcut | Standard (RFC2328)]
                     - [no] shutdown
```

OSPF Area-range Commands

```
+ root
        + config terminal
          + router
                + ospf
                     + [no] area-range <range-id> {nssaExternalLink |
                       summaryLink} <range-net> <range-mask>
                          - [no] area-range-effect {advertiseMatching |
                            doNotAdvertiseMatching}
                          - [no] area-range-substitute A.B.C.D/M
```

OSPF Redistributing Commands

```
+ root
        + config terminal
          + router
                + ospf
                     + [no] redistribute {connect | default | kernel | static}
                          - [no] metric-type {1 | 2} <metric-value>
                          - [no] route-map NAME
```

OSPF Neighbor Commands

```
+ root
        + config terminal
          + router
                + ospf
                     - [no] neighbor A.B.C.D
                          - [no] nbr-priority <priority-value>
```

OSPF Virtual Link Commands

```
+ root
        + config terminal
          + router
                + ospf
                     + [no] virtual-link <area-id> A.B.C.D
                          - [no] auth-key <key>
                          - [no] auth-type {md5 | simple}
                          - [no] dead-interval <interval-value>
                          - [no] hello-interval <interval-value>
                          - [no] retry-interval <interval-value>
```

```
            - [no] transit-delay <interval-value>
```

OSPF Area Commands

```
+ root
    + config terminal
     + router
        + ospf
          + [no] area A.B.C.D
            - [no] auth-type {md5 | simple}
            - [no] export-list STRING
            - [no] import-list STRING
            - [no] default-cost <cost-value>
            - [no] metric <metric-value>
            - [no] metric-type {comparableCost | nonComparable |
              ospfMetric}
            - [no] nssa-trans-role {ospfNssaRoleAlways |
              ospfNssaRoleNever | ospfNssaRoleCandidate}
            - [no] summary {noAreaSummary | sendAreaSummary}
            - [no] shortcut-conf {false|true}
            - [no] type {default | nssa | stub}
```

OSPF Interface Commands

```
+ root
    + config terminal
     + router
        + ospf
          + [no] interface A.B.C.D
            - area-id A.B.C.D
            - [no] auth-key-md5 entry <entry value> word STRING
            - [no] auth-key-simple STRING
            - [no] output-cost <cost-value>
            - [no] interface-type {broadcast | none | loopback |
              nbma | pointToMultipoint | pointToPoint |
              virtualLink}
            - [no] priority <priority-value>
            - [no] dead-interval <interval-value>
            - [no] hello-interval <interval-value>
            - [no] retry-interval <interval-value>
            - [no] transit-delay <delay-value>
            - [no] working mode {active | passive}
```

OSPF Timer Commands

```
+ root
        + config terminal
          + router
                + ospf
                     - [no] ext-lsdb-limit <ext-lsdb-limit-value>
                     - [no] ext-overflow-interval <ext-overflow-interval-
                       value>
                     - [no] spf-l2-convergence {false,true}
                     - [no] timers-spf-delay <timers-spf-delay-value>
                     - [no] timers-spf-init-hold <timers-spf-init-hold-value>
                     - [no] timers-spf-max-hold <timers-spf-max-hold-value>
                     - [no] timers-nssa-translator <timers-nssa-translator-
                       value>
```

OSPF Display Commands

```
+ root
        - show router ospf database [area <area-id> | asbr-summary | external
          | max-age | network | nssa-external | opaque | router | self-
          originate | summary]
        - show router ospf interface [name NAME]
        - show router ospf neighbor [all [detail] | detail | id A.B.C.D |
          interface swN [detail]]
        - show router ospf opaque-database
        - show router ospf route
```

OSPF Configuration Commands

Table 16: Global OSPF Configuration Commands

Command	Description
`config terminal`	Enters the Configuration mode
`router`	Enters the Router Configuration mode
`ospf`	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
`router-id` *`A.B.C.D`*	Defines the OSPF fixed-router ID: • *A.B.C.D: fixed-router ID in a dotted-decimal format* Default No OSPF routing process is defined
`no router-id`	Resets the OSPF fixed-router ID to the highest IP address on any of its interfaces
`te-router-id` *`A.B.C.D`*	Enabling the Traffic Engineering (TE): • *A.B.C.D: TE router IP address*
`no te-router-id`	Removes the TE router
`compatible-rfc1583 {false,true}`	Enables OSPF summary and external route calculations in compliance with RFC1583: • *true: enables the RFC 1583 compatibility* • *false: disables the RFC 1583 compatibility* Default False
`no compatible-rfc1583`	Disables the RFC 1583 compatibility and returns to the default method of calculation that is according to RFC 2328

Command	Description
default-info-originate {false,true}	Generates a default route into the OSPF routing domain: • *true: enables the origination of a default route* • *false: disables the origination of a default route* Default False
no default-info-originate	Disables the origination of a default route
default-metric <*metric-value***>**	Defines a default metric value for redistributed routes: • *metric-value: in the range of <0-16777215>* Default 10
no default-metric	Restores to default
external-distance <*external-distance***>**	Defines the external route distance: • *external-distance: in the range of <1-255>* Default 110
no external-distance	Restores to default
intra-area-distance <*intra-area-distance***>**	Defines the intra-area route distance. Intra-area routes are routes within an area: • *intra-area-distance: in the range of <1-255>* Default 110
no intra-area-distance	Restores to default
inter-area-distance <*inter-area-distance***>**	Defines the inter-area route distance. Inter-area routes are routes to other areas: • *inter-area-distance: in the range of<1-255>* Default 110
no inter-area-distance	Restores to default
abr-type [Alternative Cisco | Alternative IBM | Alternative Shortcut | Standard (RFC2328)]	Selects an alternative ABR behavior: • *Alternative Cisco* • *Alternative IBM* • *Alternative Shortcut* • *Standard (RFC2328)* Default RFC2328
no abr-type	Restores to default
shutdown	Disables the OSPF protocol
no shutdown	Enables the OSPF protocol

Table 17: OSPF Area-range Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
router	Enters the Router Configuration mode
ospf	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
area-range <*range-id***> {nssaExternalLink | summaryLink} <***range-net***> <***range-mask***>**	Creates ranges of addresses on the Area Border Router (ABR) for the purpose of route summarization or suppression, and enters the OSPF Area-range Configuration mode: • *range ID: the OSPF area range ID in the range of <0.0.0.0-255.255.255.255>* • *nssaExternalLink: OSPF area as NSSA* • *summaryLink: OSPF area ASBR summary link* • *range-net: the OSPF area range ID, in the range of <0.0.0.0-255.255.255.255>* • *range-mask: the OSPF area range mask in the range of <0.0.0.0-255.255.255.255>*
no area-range [<*range-id***>]**	Deletes a specific OSPF area range: • *range ID: in the range of <0.0.0.0-255.255.255.255>*
area-range-effect {advertiseMatching | doNotAdvertiseMatching}	Defines whether or not to advertise the summarized range of addresses to other areas: • *advertiseMatching: advertises this range* • *doNotAdvertiseMatching: do not advertise this range* Default advertiseMatching
no area-range-effect	Restores to default
area-range-substitute *A.B.C.D/M*	Announces the area range as another: • *A.B.C.D/M: the area range to substitute*
no area-range-substitute	Restores to default

Table 18: OSPF Redistributing Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
router	Enters the Router Configuration mode
ospf	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
redistribute {connect | default | kernel | static}	Redistributes OSPF routes from one routing domain into another routing domain: • *connect: interface routes of the router* • *default: default routes* • *kernel: kernel originated route entries* • *static: static routes* Default Disabled
no redistribute	Restores to default
metric-type{1 | 2} <*metric-value***>**	Defines the external link type associated with the default route advertised into the OSPF routing domain. It can be: • *Type 1 external route* • *Type 2 external route* • *metric-value: in the range of <0-16777215>* Default 0
no metric-type{1 | 2}	Restores to default
route-map *NAME*	Redistributes routes matching the specified route-map conditions: • *NAME: the map name* Default Not configured
no route-map	Restores to default

Table 19: OSPF Neighbor Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
router	Enters the Router Configuration mode
ospf	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
neighbor *A.B.C.D*	Specifies the OSPF router's *neighbors:* • *A.B.C.D: interface's IP address of the neighbor* Default Not configured
no neighbor	Removes the neighbor configuration
nbr-priority <*priority-value***>**	Defines the router priority value of the non-broadcast neighbor associated with the IP address specified: • *priority-value: in the range of <0-255>* Default 0
no nbr-priority	Restores to default

Table 20: OSPF Virtual Link Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
router	Enters the Router Configuration mode
ospf	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
virtual-link <*area-id***>** *A.B.C.D*	Defines a virtual link to connect the area border routers to the backbone via a virtual link: • *area-id: in the range of <0.0.0.0-255.255.255.255>* • *A.B.C.D: neighbor ID, in a dotted-decimal format* Default Not configured
no virtual-link	Removes the virtual link definitions
auth-key <*string***>**	Defines the password for simple authentication: • *string: up to 8 characters* Default Not configured
no auth-key	Removes the password

Command	**Description**
auth-type {md5 | simple}	Specifies the authentication type: • *md5: configured in accordance with RFC 2328* • *simple: simple password (RFC 2328)* Default Simple
no auth-type	Restores to default
dead-interval <*seconds***>**	Defines the time that OSPF waits before declaring a neighbor router down. If no hello packets are received from a neighbor for the duration of the dead interval, the router is assumed to be down. The minimum interval must be two times the hello interval Default 40 seconds
no dead-interval	Restores to default
hello-interval <*interval value***>**	Defines the interval between OSPF hello packets issued on the virtual link: • *hello-interval value: in the range of <1-65535> seconds* Default 10 seconds
no hello-interval	Restores to default
retry-interval <*interval value***>**	Defines the time between retransmitting lost link state advertisements: • *retry-interval value: in the range of <0-3600> seconds* Default 5 seconds
no retry-interval	Restores to default
transit-delay <*delay value***>**	Defines the link state transmit delay: • *transit-delay value: in the range of <0-3600> seconds* Default 1 second
no transit-delay	Restores to default

Table 21: OSPF Area Parameters Commands

Command	Description
config terminal	Enters the Configuration mode
router	Enters the Router Configuration mode
ospf	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
area *A.B.C.D*	Mandatory Defines an OSPF area: • *A.B.C.D: OSPF area's IP address* Default Not defined
no area [*A.B.C.D***]**	Deletes the specified area: • *A.B.C.D: (optional) OSPF area's IP address*
export-list *STRING*	Defines a filter for advertising networks to other areas: • *STRING: filter's name* Default Not configured
no export-list	Removes the filter
import-list *STRING*	Defines a filter for importing networks from other areas to the specified area: • *STRING: filter's name*
no import-list	Removes the filter
auth-type {md5 | simple}	Defines an authentication type: • *md5: configured in accordance with RFC 2328* • *simple: simple password (RFC 2328)* Default Simple
no auth-type	Restores to default
default-cost <*cost-value***>**	Assigns the specified cost to the default summary route used for the stub area: • *cost-value: in the range of <0-16777215>* Default 1
no default-cost	Restores to default
metric <*metric-value***>**	Defines an explicit route cost metric for the selected OSPF area: • *metric-value: in the range of <0-16777215>* Default 10
no metric	Restores to default

Command	Description
metric-type {comparableCost | nonComparable | ospfMetric}	Defines the external link type associated with the default route advertised into the OSPF area: • *comparableCost* • *nonComparable* • *ospfMetric* Default ospfMetric
no metric-type	Restores to default
nssa-trans-role {ospfNssaRoleAlways | ospfNssaRoleNever | ospfNssaRoleCandidate}	Defines the device's role in the OSPF NSSA area: • *ospfNssaRoleAlways* • *ospfNssaRoleNever* • *ospfNssaRoleCandidate* Default Not specified
no nssa-trans-role	Removes the area definition
shortcut-conf {false,true}	Defines the area shortcutting mode: • *true: enabled* • *false: disabled* Default False
no shortcut-conf	Restores to default
summary {noAreaSummary | sendAreaSummary}	Enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR): • *noAreaSummary: prevents injection of inter-area routes into NSSA* • *sendAreaSummary: sends injection of inter-area routes into NSSA* Default noAreaSummary
no summary	Disables sending summary route advertisements and, for stub areas, only the default route is advertised by the ABR
type {default | nssa | stub}	Defines the OSPF area type: • *default: default type* • *nssa: OSPF area as NSSA* • *stub: OSPF area as a stub area* Default Default
no type	Restores to default

Table 22: IP Interface Parameters Commands

Command	Description
config terminal	Enters the Configuration mode
router	Enters the Router Configuration mode
ospf	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
interface *A.B.C.D*	Mandatory Defines an OSPF interface: - *A.B.C.D: OSPF interface's IP address* Default Not activated
no interface [*A.B.C.D*]	Deletes the OSPF interface configuration: - *A.B.C.D: OSPF interface's IP address*
area-id *A.B.C.D*	Mandatory Defines the OSPF area ID in a dotted-decimal format: - *A.B.C.D: in the range of <0.0.0.0-255.255.255.255>*
output-cost <*cost-value*>	Defines the cost of sending a packet on the OSPF IP interface: - *cost-value: in the range of <1-65535>* Default 10
no output-cost	Restores to default
auth-key-md5 entry <*value*> **word** *STRING*	Defines a password for md5 authentication: - *value: in the range of <0 255>* - *STRING: a string of <1-16> characters*
no auth-key-md5 entry <*value*>	Removes the password
auth-key-simple *STRING*	Defines a password for simple authentication (RFC 2328): - *STRING: a string of <1-8> characters*
no auth-key-simple	Removes the password

Command	Description
interface-type {broadcast | none | loopback | nbma | pointToMultipoint | pointToPoint | virtualLink}	Defines the OSPF network type: • *broadcast* • *none* • *loopback* • *nbma* • *pointToMultipoint* • *pointToPoint* • *virtualLink* Default broadcast
no interface-type	Restores to default
priority <*priority-value***>**	Defines the router priority for the configured IP interface to help determine the OSPF designated router for the network: • *priority-value: in the range of <0-255>* Default 1
no priority	Restores to default
dead-interval <*dead-interval value***>**	Defines the number of seconds that a device must wait before it declares a neighbor OSPF router down: • *dead-interval value: in the range of <1-65535> seconds* Default 40 seconds
no dead-interval	Restores to default
hello-interval <*hello-interval value***>**	Defines the length of time between the hello packets that the router sends on an IP interface: • *hello-interval value: in the range of <1-65535> seconds* Default 10 seconds
no hello-interval	Restores to default
retry-interval *<retry-interval value>*	Defines the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an IP interface: • *retry-interval value: in the range of <3-65535> seconds* Default 5 seconds
no retry-interval	Restores to default

Command	Description
transit-delay *<transit-delay value>*	Defines the estimated number of seconds taken to transmit a link state update packet on an IP interface: • *transit-delay value: in the range of <1-65535> seconds* Default 1 seconds
no transit-delay	Restores to default
working-mode {active | passive}	Specifies the working mode: • *active* • *passive* Default Passive
no working-mode	Restores to default

Table 23: Optional OSPF Timers Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
router	Enters the Router Configuration mode
ospf	Enables OSPF and enters the OSPF Router Configuration mode Default Enabled
ext-lsdb-limit <*ext-lsdb-limit-value***>**	Assigns the upper limit to the number of LSAs allowed in the router Link-State Database (LSDB): • *ext-lsdb-limit-value: in the range of <-1—2147483647>* Default 10000
no ext-lsdb-limit	Restores to default
ext-overflow-interval <*ext-overflow-interval value***>**	Defines the time countdown, starting when the router enters *Overflow* state, after which the router attempts to resume transmitting LSAs: • *ext-overflow-interval value: in the range of <0-2147483647> seconds* Default 0 seconds
no ext-overflow-interval	Restores to default
spf-l2-convergence {false,true}	Enables the L2 mode of SPF calculation: • *false: disables the SPF L2-mode calculation* • *true: enables the SPF L2-mode calculation* Default Disabled

Command	**Description**
no spf-l2-convergence	Restores to default
timers-spf-delay <*timers-spf-delay -value***>** **timers-spf-init-hold <***timers-spf-init-hold-value***>** **timers-spf-max-hold <***timers-spf-max-hold-value***>**	Configures three SPF (Shortest Path First) timers: spf-delay, spf-init-holdtime and spf-max-holdtime. • *timers-spf-delay-value, timers-spf-init-hold-value, timers-spf-max-hold-value: in the range of 0-4294967295 seconds* Default SFP delay time 5 seconds Default SFP hold times 10 seconds
no timers-spf-delay **no timers-spf-init-hold** **no timers-spf-max-hold**	Restores to default
timers-nssa-translator <*timers-nssa-translator value***>**	Defines the NSSA Translator Stability interval: • *timers-nssa-translator value: in the range of <1-65535> seconds* Default 40 seconds
no timers-nssa-translator	Restores to default

Table 24: OSPF Display Commands

Command	Description
show router ospf database [area <*area-id***> | asbr-summary | external | max-age | network | nssa-external | opaque | router | self-originate | summary]**	Displays the OSPF database: • *area-id: in the range of <0.0.0.0-255.255.255.255>* • *asbr-summary: the ASBR summary link states* • *external: the external link states* • *max-age: the LSAs in the MaxAge list* • *network: the network link states* • *nssa-external : the NSSA database content per area* • *opaque: the information about TE opaque LSAs* • *router: the router link states* • *self-originate: the self-originated link states* • *summary: the network summary link states*
show router ospf interface [name eth1 | lo[*N***]]**	Displays OSPF interfaces related information: • *lo[N]: an internal logical loopback IP-interface. (Optional) N is in the range of <0-9>* • *swN: an IP interface number in the range of <01-9999>*
show router ospf neighbor [all [detail] | detail | id *A.B.C.D* **| interface sw***N* **[detail]]**	Displays information on OSPF neighbors on a per-interface basis: • *all: (optional) information for all neighbors that are in a down state (neighbors not in full or 2-way state)* • *detail: (optional) detailed information for all neighbors* • *id A.B.C.D: the neighbor's IP address* • *interface swN: an IP interface number in the range of <01-9999>*
show router ospf opaque-database	Display lists of information about the TE opaque LSAs
show router ospf route	Displays all routes received through the OSPF router

Simple Network Management Protocol (SNMP)

Overview

SNMP is an application layer protocol that facilitates the exchange of management information between network devices.

An SNMP-managed network consists of three key components:

- managed device—is a network node that contains an *SNMP Agent* and resides on a managed network
- agent—is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP
- network-management system—executes applications that monitor and control managed devices.

SNMP enables network administrators to manage network performance, find and solve network problems and extend the network.

The below figure displays the communication between an SNMP Agent and Manager.

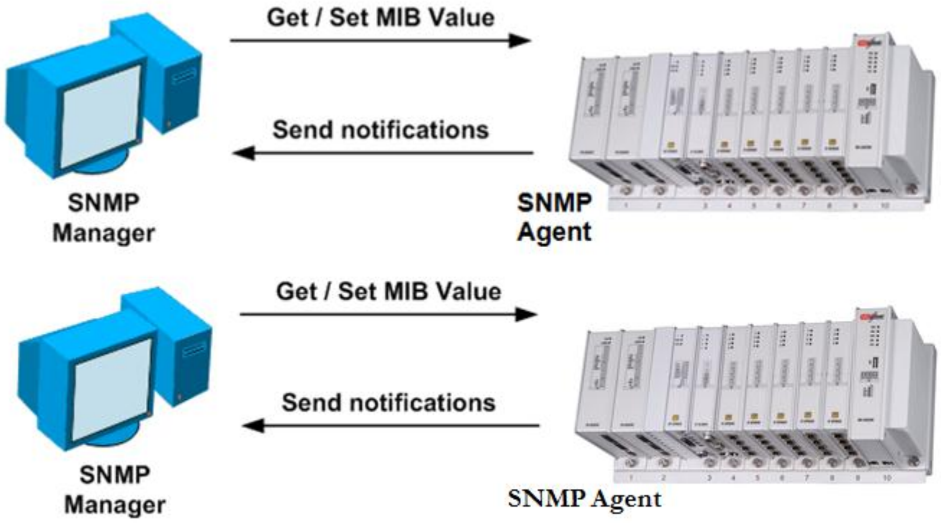


Figure 6: SNMP Agent and Manager Communications

An SNMP Entity is an implementation of the SNMP architecture. Each entity consists of an SNMP Engine and one or more associated applications. An SNMP Engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. The SNMP Engine is identified by the *SNMP Engine ID*. The applications use the services of an SNMP Engine to accomplish specific tasks. They coordinate the processing of management information operations, and may use SNMP messages to communicate with other SNMP Entities.

SNMP Agent

An *Agent* is a network-management software module that resides in a managed device and is responsible for maintaining local management information and delivering that information to a *Manager via SNMP*. A management information exchange can be initiated by the Manager or by the Agent. The SNMP Agent contains MIB variables and these values can be requested or changed by the SNMP Manager. The Agent and MIB reside on the device. The Agent gathers data from the MIB and responds to a Manager's request to get or set data.

Structure of Management Information (SMI)

Management information is a collection of managed objects, residing in a virtual information store, termed the MIB. Collections of related objects are defined in MIB modules. Each type of object has a name, syntax, and an encoding. The name is represented uniquely as an Object Identifier (OID). An OID is an administratively assigned name for identifying one object, regardless of the semantics associated with the object. The encoding of an object type is the way the instances of that object type are represented using the object's type syntax. The names are used to identify managed objects.

SNMP Manager

An SNMP Manager is a software module in a management network responsible for managing part or the entire configuration on behalf of network management applications and users.

The SNMP Manager sends requests to the SNMP Agent to get and set MIB values. Communication among protocol entities is accomplished by the exchange of messages; each of them is entirely and independently represented within a single UDP datagram. A message consists of a version identifier, an SNMP community name, and a protocol data unit (PDU). PDUs are the packets that are exchanged in the SNMP communication.

Management Information Base (MIB)

A MIB consists of a collection of objects organized into groups. Objects have values that represent managed resources. All managed objects in the SNMP environment are arranged in a hierarchical or tree structure. A MIB is the repository for information about device's parameters and network data.

SNMP Engine ID

The *SNMP Engine ID* is a 5 to 32 bytes long, administratively unique identifier of a participant in SNMP communication within a single management domain. The SNMP Manager and SNMP Agent must be configured by an administrator to have unique SNMP Engine IDs.

SNMP View Records

With the community-based authentication defined in SNMPv1, an authorized user is granted access to the whole MIB tree for reading or for reading/writing. With SNMPv1, it is not possible to allow diverse authorized users access to different portions of the MIB database.

This deficiency is overcome in SNMPv3 with the introduction of *views*. A view is a set of rules that define what portion of the MIB database can be *visible* to a specific user. The rules are defined by the OID of a node in the

MIB tree, and the type of rule: ***included*** or ***excluded.*** The OID defines a *view family*—a set of object identifiers that have a common prefix. A single rule (included or excluded) in the view is applied to view family, not only to a single OID.

SNMP Notifications

The *SNMP notification* messages allow devices to send asynchronous messages to the SNMP Managers. Devices can send notifications to SNMP Managers when particular events occur. For example, an Agent might send a message to a Manager when the Agent experiences an error condition.

NOTE

All traps, except the ones sent with SNMPv1, have a request ID as part of the PDU.

SNMP notifications can be sent as traps or Inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. However, an SNMP Manager that receives an Inform request acknowledges the message with an SNMP response PDU. If the sender does not receive a response after a particular time interval, the Inform request is sent again.

Informs consume more resources in the device and in the network but are more reliable. Unlike a trap, which is discarded as soon as it is sent, an Inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an Inform may be retried several times.

Error! Reference source not found. through *Error! Reference source not found.* illustrate the differences between traps and Inform requests.

In *Error! Reference source not found.*, the Agent successfully sends a trap to the SNMP Manager. Although the Manager receives the trap, it does not send any acknowledgment to the Agent. The Agent has no way of knowing whether the trap reached its destination.

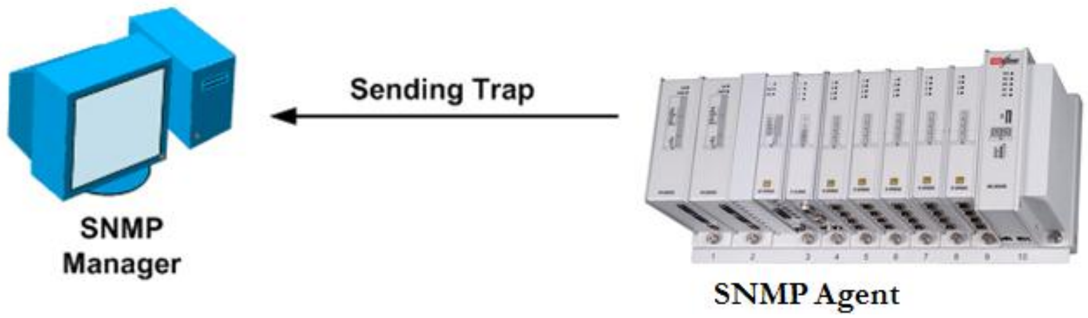


Figure 7: Trap Sent to SNMP Manager Successfully

In Error! Reference source not found., the Agent successfully sends an Inform request to the Manager. When the Manager receives the Inform request, it sends a response back to the Agent. Thus, the Agent knows that the Inform request successfully reached its destination. In this example, twice traffic is generated as in Error! Reference source not found.; however, the Agent is sure that the Manager received the notification.

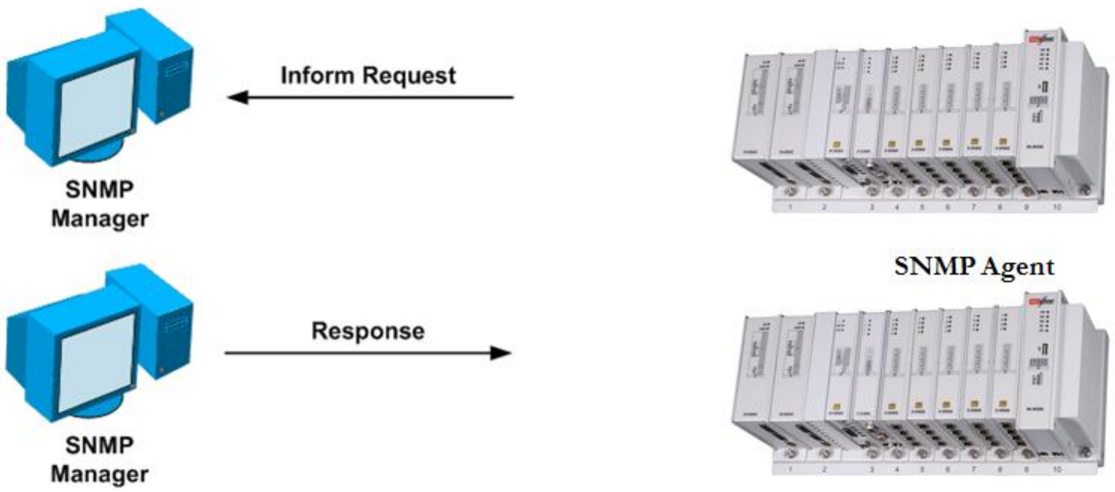


Figure 8: Inform Request Sent to SNMP Manager Successfully

In Error! Reference source not found., the Agent sends a trap to the Manager, but the trap does not reach the Manager. Since the Agent has no way of knowing whether the trap reached its destination, the trap is not sent again. The Manager never receives the trap.

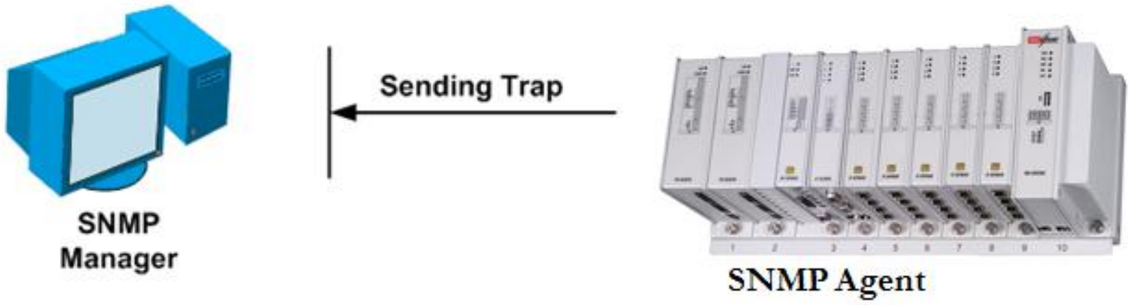


Figure 9: Trap Unsuccessfully Sent to SNMP Manager

In Error! Reference source not found., the Agent sends an Inform request to the Manager, but the Inform request does not reach the Manager. Since the Manager did not receive the Inform request, it does not send a response. After a period of time, the Agent resends the Inform request. This time, the Manager receives the Inform request and replies with a response. In this example, there is more traffic than in Error! Reference source not found.; however, the notification reaches the SNMP Manager.

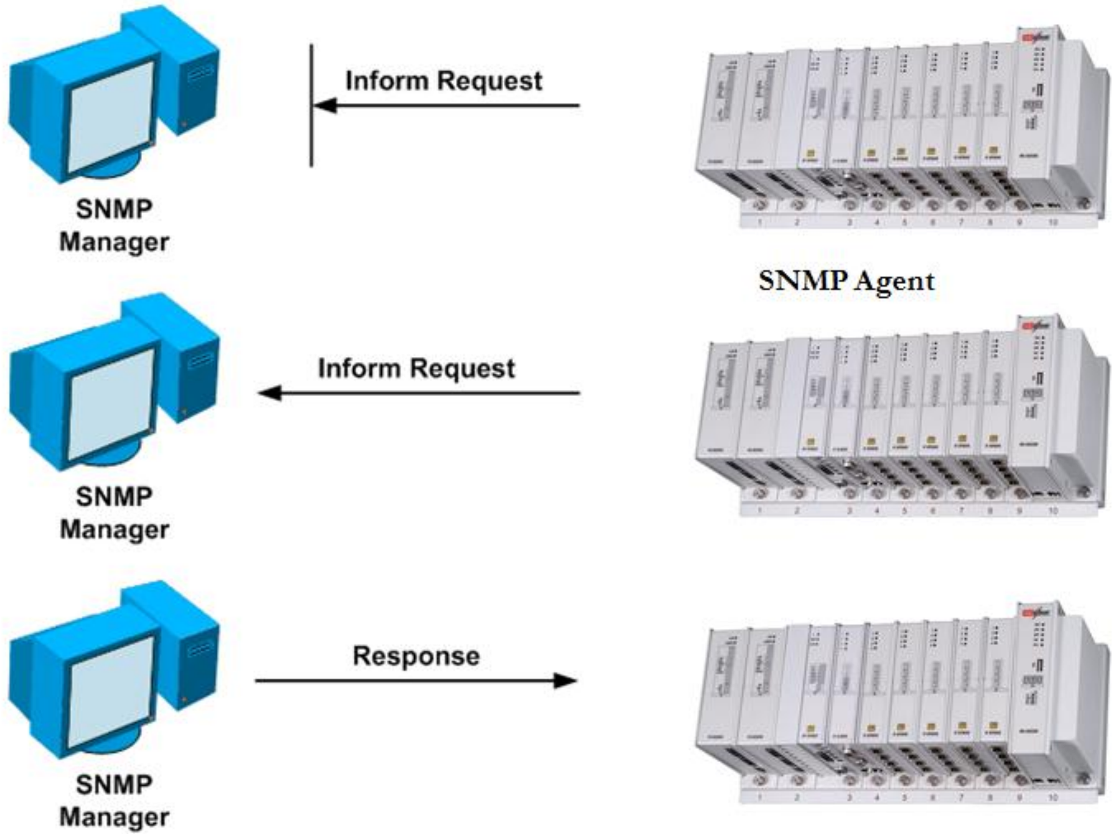


Figure 10: Inform Request Successfully Resent to SNMP Manager

The Discovery Mechanism

To protect the user network against message reply, delay and redirection, one of the SNMP engines involved in each communication is designated to be the authoritative SNMP engine. When an SNMP message contains a payload that expects a response, the receiver of such a message is authoritative. When Inform PDUs are sent, the notification receiver is an authoritative snmpEngineID (the Manager). This implies that the PDUs that are involved in an authenticated/encrypted session between the Agent and the Manager are encoded with keys that are localized with the Manager's snmpEngineID and not with the local application software Agent's snmpEngineID.

To match the described requirements, you need an additional configuration of users, on whose behalf Inform PDUs can be sent. User keys are required to be localized with the snmpEngineID of the Manager (the authoritative side). The keys of these users are localized for the remote side and the Agent cannot process configuration of SNMP requests on their behalf. *GET*, *GET-NEXT*, *GET-BULK*, or *SET* requests from users with a SNMP Engine ID that is different from the Agent SNMP Engine ID cannot be processed. The application software defines as remote those users created with a snmpEngineID different from the Agent's snmpEngineID. Remote users can participate just by sending Inform PDUs.

To create a remote user, specify the snmpEngineID of the notification recipient, where this user is correctly defined. The proper calculation of authentication/encryption keys requires a valid remote user.

To send the Inform PDU to the authoritative side, the Agent needs information for the snmpEngineID of the target-address of the recipient.

To reduce a configuration complexity, the application software Agent implements an auto discovery procedure for obtaining the SNMP Engine IDs of different Inform recipients.

When an event occurs, for example **`LinkUp`**, the Agent sends an Inform PDU to all valid targets for this Inform. The very first Inform PDU actually is not valid as the Agent still does not know the parameters of the Receiver Engine ID—*snmpEngineId, snmpEngineBoots* and *snmpEngineTime.*

In *Error! Reference source not found.*, the Manager reports the PDU with its Engine ID to the Agent.

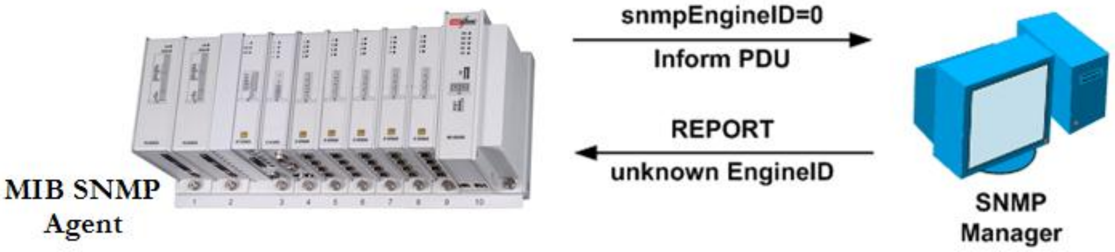


Figure 11: Obtaining the snmpEngineID

The Agent sends an Inform PDU with a valid Engine ID (the Engine ID that is received as shown in *Error! Reference source not found.*), but with incorrect *snmpEngineBoots* and *snmpEngineTime.* These parameters are still unknown to the Agent. The discovery process ends when no authentication/encryption exists for the target address. If authentication/encryption exists, the packet is with the corresponding authentication/encryption—MD5, SHA or DES.

In *Error! Reference source not found.*, the Manager returns an authenticated REPORT PDU (notInTimeWindow) that consists of valid snmpEngineBoots and snmpEngineTime parameters.

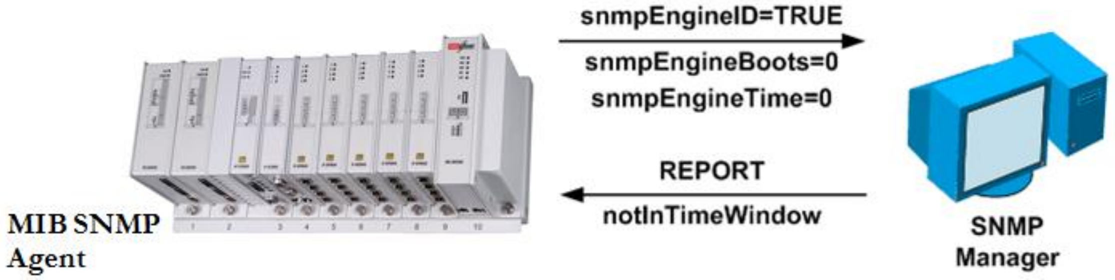


Figure 12: Obtaining the snmpEngineBoots and snmpEngineTime

Finally, when the discovery process is completed, the Agent and the Manager are synchronized and following packets do not discover the Engine ID of the Manager.

Versions of SNMP

The application software supports the following versions of SNMP:

Table 25: SNMP Versions

Variable	Description
SNMPv1	In the SNMP version 1, user can get and set MIB objects, traverse the MIB tree using the *getNext* operation, and enable the management device to receive asynchronous messages from the Agent using the trap mechanism. SNMPv1 bases its security on community strings.
SNMPv2c	SNMP version 2c (the ***c*** stands for community) is the community-string based Administrative Framework. SNMPv2c includes the following improvements over SNMPv1: • Improved performance for getting data using *getBulk*. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information in one PDU, thus minimizing the number of round-trips required. • Improved error handling. SNMPv2 adds many error codes to the five originally defined in SNMPv1. Management devices are provided with more detailed information about the cause of the error. Also, three exceptions are reported with SNMPv2c: **no such object**, **no such instance**, and **end of MIB view** exceptions. • Extended asynchronous reporting. SNMPv2 allows the Agent to send SNMP notifications by **inform** request, as well as by trap messages that are available in SNMPv1. Whereas traps do not provide the Agent with an indication that the message is received, the **inform** request requires the Manager to confirm reception and is therefore more reliable. As for the trap message, its format is changed to match the PDU format of a regular get/set PDU, in order to simplify the protocol. The SNMPv2 protocol requires adding more details to every trap in order to supply the Manager with more information. Generally, MIBs written for Agents that use SNMPv2c or higher versions use SMIv2 instead of version 1 of the SMI. This version adds some new variables types. Both SNMPv1 and SNMPv2c use a community-based form of security.

Variable	Description
SNMPv3 Currently no supported	SNMP version 3 is an interoperable standards-based protocol. It provides secure communication using the USM (User-based Security Model) and access control using the VACM (View-based Access Control). The USM model provides an answer to the following threats: • Replay, interception and retransmission of messages—prevented by using time-stamp. • Masquerading—prevented by authenticating the message sender. • Integrity, interception, changing data, and retransmission of messages—prevented by authenticating the message sender and encryption of the message data. • Disclosure—prevented by encryption of the message data. The SNMPv3 USM allows three levels of security (see *Error! Reference source not found.*): • No Authentication and No Privacy (noAuthNoPriv) • Authentication and No Privacy (AuthNoPriv) • Authentication and Privacy (authPriv)

Table 26: Security Levels Available in the SNMPv3 Security Models

Level	Authentication	Encryption	Explanation
noAuthNoPriv	Username	No	All PDUs are sent unencrypted and not authenticated in the network.
authNoPriv	HMAC-MD5 or HMAC-SHA	No	The PDUs are authenticated with HMAC (keyed-Hashing for Message Authentication Codes). They cannot be altered by an attacker, but can be read.
authPriv	HMAC-MD5 or HMAC-SHA	Cipher Block Chaining—Data Encryption Standard (CBC-DES)	The PDUs are authenticated and encrypted (with CBC-DES Symmetric Encryption Protocol).

You must configure the SNMP Agent to use the version of SNMP supported by the management device. An Agent can communicate with multiple users. For this reason, you can configure the application software to support communications with many users: some users can use the SNMPv1 protocol, some can use the SNMPv2c protocol, and the rest can use SMNPv3.

NOTE

You can participate in different groups, with a different security model in each group. You cannot participate in more than one group with the same security model.

SNMP Command Hierarchy

```
+ root
         + configure terminal
           + system
                  + snmp
                        - [no] engine-id <engineID>
                        - [no] max-packet-size <size>
                        - [no] general-port <port-number>
                        - [no] snmp-address {A.B.C.D | all}
                        - [no] shutdown
                        - [no] authentication-failure-trap
                        - [no] system-name .LINE-TEXT
                        - [no] system-location .LINE-TEXT
                        - [no] system-contact .LINE-TEXT
                        - [no] system-description .LINE-TEXT
                        - [no] view VIEWNAME OID-TREE [MASK | included |
                          excluded]
                        - [no] group GROUPNAME security-model {authNoPriv |
                          authPriv | noAuthNoPriv} read READ-VIEW write WRITE-
                          VIEW notify NOTIFY-VIEW
                        - [no] user USERNAME GROUPNAME {v1 | v2c | v3} [md5 |
                          sha] [AUTHENTICATION-PASSWORD] [ENCRYPTION-PASSWORD]
                        + [no] target-address ADDR-NAME
                              - [no] message-version {v1 | v2c | v3}
                              - [no] security-model {noAuthNoPriv | authNoPriv |
                                authPriv}
                              - [no] address TARGET-ADDRESS
                              - [no] security-name USERNAME
                              - [no] dst-port <port-number>
                              - [no] timeout <value>
                              - [no] retry-count <value>
                              - [no] tag TAGNAME
```

- **show snmp-server [displaylevel** *<level>* **| statistics]**
- **show snmp engine [displaylevel** *<level>***]**
- **show snmp-system [displaylevel** *<level>***]**
- **show snmp views [displaylevel** *<level>***]**
- **show snmp group [displaylevel** *<level>***]**
- **show snmp user [displaylevel** *<level>***]**
- **show snmp target-address [displaylevel** *<level>***]**

SNMP Configuration Commands

Table 27: SNMP Configuration Commands

Command	Description
system	Enters the System Configuration mode.
snmp	Enables SNMP server.
engine-id *<engineID>*	Sets a new value for the Agent's SNMP Engine ID: - *engineID: a string of 10 to 64 characters (represented internally by 5 to 32 bytes), in the format of XX:XX:XX:XX:XX:XX* Default 80 00 02 E2 03 [MAC ADDR]
no engine-id	Restores to default
max-packet-size *<size>*	Sets a new value for the maximum packet size: - *size: in the range of <484-2147483647>* Default 9216
no max-packet-size	Restores to default
general-port *<port-number>*	Sets a new value for the IP SNMP port number: - *port-number: in the range of <161, 1025-65535>* Default 161
no general-port	Restores to default
snmp-address {*A.B.C.D* **| all}**	Defines the SNMP server address: - *A.B.C.D: the IP address* - *all: all IP addresses configured on the device* Default all
no snmp-address	Restores to default
shutdown	Disables SNMP server Default SNMP server is disabled
no shutdown	Mandatory Enables SNMP server
authentication-failure-trap	Sends *authenticationFailure* notifications. This command controls the value of MIB-II mib-2.snmp.snmpEnableAuthTraps Default Enabled
no authentication-failure-	Disables the sending of *authenticationFailure* notifications

Command	Description
trap	
system-name *.LINE-TEXT*	Sets the MIB-II system name: • *.LINE-TEXT: descriptive system name string, up to 255 characters long* Default The default value is the device's model name
no system-name	Removes the defined system name.
system-location *.LINE-TEXT*	Sets the MIB-II system location string: • *.LINE-TEXT: descriptive system location string, up to 255 characters long* Default Empty (null)
no system-location	Restores to default.
system-contact *.LINE-TEXT*	Sets the MIB-II system contact string: • *.LINE-TEXT: descriptive system contact string, up to 255 characters long* Default Empty (null)
no system-contact	Restores to default
system-description *.LINE-TEXT*	Sets the MIB-II system description string: • *.LINE-TEXT: description string, up to 255 characters long* Default Empty (null)
no system-description	Restores to default
view *VIEWNAME OID-TREE* **[***MASK* **| included | excluded]**	Mandatory Defines the subset of all MIB objects accessible to the given view: • *VIEWNAME: the name of the view up to 32 characters* • *OID-TREE: the starting point inside the MIB tree given in dot-notation or as an object name* • *MASK: the mask is typed as a hexadecimal value, and is interpreted as a binary value. A binary 1 in the mask states that the Object ID at the corresponding position has to match, a binary 0 states that the Object ID at the corresponding position is irrelevant—no match is required* • *included: the Object ID subtree is included in the view* • *excluded: the Object ID subtree*

Command	Description
	is excluded from the view
no view *VIEWNAME*	Removes the specified view
group *GROUPNAME* **security-model {authNoPriv | authPriv | noAuthNoPriv} read** *READ-VIEW* **write** *WRITE-VIEW* **notify** *NOTIFY-VIEW*	Mandatory Creates an SNMP group with a specified security model and defines the access-right for this group by associating views to this group: • *GROUPNAME: the name of the group is limited to 32 characters* • *{authNoPriv | authPriv | noAuthNoPriv}: the security level. For more information, refer to Error! Reference source not found.* Default If no security level is specified, **noAuthNoPriv** security level is assumed • *READ-VIEW: the name of the view (not to exceed 32 characters) in which you can only view the contents of the Agent's MIB* • *WRITE-VIEW: the name of the view (not to exceed 32 characters) in which you can type data and configure the contents of the Agent's MIB* • *NOTIFY-VIEW: the name of the view (not to exceed 32 characters) that specifies what portion of the MIB database is accessible for notifications*
no group *GROUPNAME* **security-model {authNoPriv | authPriv | noAuthNoPriv}**	Removes the SNMP group data: • If you specify only the group name, all groups with that name are removed, regardless of their security model and security level. • If you specify the security model, only the group matching all conditions is removed.

Command	Description
user *USERNAME GROUPNAME* **{v1 | v2c | v3} [md5 | sha]** [*AUTHENTICATION-PASSWORD*] [*ENCRYPTION-PASSWORD*]	Mandatory Creates an SNMP local or remote user: • *USERNAME: the name of the user on the host that connects to the Agent. The user name is limited to 32 characters* Default SNMP user is not configured • *GROUPNAME: the name of the group is limited to 32 characters* • *v1, v2, v3: the security model. For more information, refer to Error! Reference source not found.* • *md5: enables HMAC-MD5 (Message Digest 5) authentication* • *sha: enables HMAC-SHA (Secure Hash Algorithm) authentication* • *ENCRYPTION-PASSWORD: the PDUs sent to or received by this user should be encrypted, with the key generated from the encryption password; up to 32 characters* • *AUTHENTICATION-PASSWORD: the authentication password string up to 32 characters*
no user *USERNAME* **group** *GROUPNAME* **{v1 | v2c | v3}**	Removes the specified user definition
target-address *ADDR-NAME* **#traps**	Defines the notification target address: • *ADDR-NAME: the name of the notification target address up to 32 characters*
no target-addr *ADDR-NAME*	Removes the notification target address.
message-version {v1 | v2c | v3}	Defines the security model. It specifies the version of the protocol in which the traps are sent (for more information, refer to *Error! Reference source not found.*): • *v1, with TRAP-V1 PDU type* • *v2c with TRAP-V2 PDU type* • *v3, with TRAP-V2 PDU type)* Default v2c
no message-version	Restores to default

Command	Description
`security-model {noAuthNoPriv | authNoPriv | authPriv}`	Defines the SNMP levels of security: • *authNoPriv, authPriv, noAuthNoPriv: the security level. For more information, refer to Error! Reference source not found.* Default If no security level is specified, **noAuthNoPriv** security level is assumed
`no security-model`	Restores to default
`address` *TARGET-ADDRESS*	Defines the IP address of the target: • *A.B.C.D: the IP address of the target* Default 0.0.0.0
`no address`	Restores to default
`security-name` *USERNAME*	Defines the security name that identifies how SNMP messages will be generated using this entry: • *USERNAME: the security user name up to 32 characters*
`no security-name`	Removes the security name
`dst-port` *<port-number>*	Defines the UDP port number: • *port-number: in the range of <162, 1025-65535>* Default 162
`no dst-port`	Restores to default
`timeout` *<value>*	Defines the time to wait for an acknowledgement before resending an unacknowledged inform PDU: • *value: in the range of <0-600> seconds* Default 15 seconds
`no timeout`	Restores to default
`retry-count` *<value>*	Defines the number of retries if there is not response from the client on the informs: • *value: in the range of <0-255>* Default 3 retries
`no retry-count`	Restores to default
`tag` *TAGNAME*	Defines the notification tag name: • *TAGNAME: the notification tag name up to 255 characters*
`no tag`	Restores to default

Command	Description
`show snmp-server [displaylevel` *`<level>`* **`| statistics]`**	Displays the status of the SNMP server—*enabled* or *disabled*—and the UDP port on which the SNMP is enabled: • *`level: in the range of <0-64>`* • *`statistics: the SNMP server statistics`*
`show snmp engine [displaylevel` *`<level>`***`]`**	Displays the local SNMP Engine ID of the SNMP Agent, all Engine IDs that are known to the Agent, and information about the inform operation values: • *`level: in the range of <0-64>`*
`show snmp-system [displaylevel` *`<level>`***`]`**	Displays the SNMP server system configuration: • *`level: in the range of <0-64>`*
`show snmp views [displaylevel` *`<level>`***`]`**	Displays all configured views and the viewmask of a particular view (if configured): • *`level: in the range of <0-64>`*
`show snmp group [displaylevel` *`<level>`***`]`**	Displays the configured groups, their associated views, and the security model. If the security model is USM (v3), the command displays the security level: • *`level: in the range of <0-64>`*
`show snmp user [displaylevel` *`<level>`***`]`**	Displays the users and their associated engine ID: • *`level: in the range of <0-64>`*
`show snmp target-address [displaylevel` *`<level>`***`]`**	Displays the notification target address: • *`level: in the range of <0-64>`*

Table 28: Notification Argument Values

Argument Value	Description
`authenticationFailure`	The SNMP entity, acting as an Agent, received a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP that is used. • For SNMPv1 and SNMPv2c, authentication failure occurs for packets with an incorrect community string. • For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside of the SNMP engine's time window. The generation of authenticationFailure can also be controlled by the **`authentication-failure-trap`** command.
`cpuTemperatureExceeded`	The sending Agent senses that the internal temperature exceeded the program threshold.
`cpuUtilizationExceeded`	The sending Agent senses that the CPU utilization exceeded the programmed threshold.
`fansTest`	The sending Agent senses that one of the fans changed its status. The trap should be sent once the BiST status of the fan test changes, or when the fan is removed/plugged in.
`linkup`	The SNMP entity, acting as an Agent, detected that the ifOperStatus object for one of its communication links left the down state and transitioned into another state (but not into the notPresent state). The other state is indicated by the included value of ifOperStatus.
`linkDown`	The SNMP entity, acting as an Agent, detected that the ifOperStatus object for one of its communication links entered the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
`powerSupplyTest`	The sending Agent senses that one of the power-supply changed its status. The trap should be sent once the BiST status of the power supply test changes.
`ramFreeSpaceExceeded`	The sending Agent senses that the internal amount of free RAM is lower than a programmed threshold.
`sapCreated`	This trap is sent when a new row is created in the sapBaseInfoTable.
`sapDeleted`	This trap is sent when an existing row is deleted from the sapBaseInfoTable.
`sapStatusChanged`	This trap is generated when there is a change in the administrative or operating status of an SAP.
`sdpCreated`	This trap is sent when a new row is created in the sdpInfoTable.

Argument Value	Description
`sdpDeleted`	This trap is sent when an existing row is deleted from the sdpInfoTable.
`sdpStatusChanged`	This trap is generated when a change occurred in the administrative or operating status of an SDP.
`svcCreated`	This trap is sent when a new row is created in the svcBaseInfoTable.
`svcDeleted`	This trap is sent when an existing row is deleted from the svcBaseInfoTable.
`svcStatusChanged`	This trap is generated when a change occurred in the administrative or operating status of a service.

SNMP Configuration Examples

Creating Users

In this example, an SNMP user is added to the device. The user is named ***tester*** and is attached to a group named ***public***. The SNMPv1 community is parsed by the SNMP Agent as the user name.

1. Enable SNMP:

```
device-name#config terminal
device-name(config)#system
device-name(config-system)#snmp
```

2. Create a view that includes the entire MIB tree from root:

```
device-name(config-snmp)#view all_MIB 1.3 included
```

3. Create a user named ***tester*** that uses ***SNMPv1*** and attach it to a group named ***public*** without authentication and privacy:

```
device-name(config-snmp)#group public security-model noAuthNoPriv read ALL_mib
write all_MIB notify all_MIB
device-name(config-snmp)#user tester public v1
```

4. Enable SNMP server:

```
device-name(config-snmp)#no shutdown
```

5. Commit the configuration:

```
device-name(config-snmp)#commit
Commit complete.
device-name(config-snmp)#end
```

6. Display the SNMP server:

```
device-name #show snmp

SNMP engine configuration
===============================================================================
Local snmpEngineID       : 800002E2030020D2FC296F
snmpEngineBoots          : 3
snmpEngineTime           : 492
snmpEngineMaxMessageSize : 9216
===============================================================================
SNMP Views
===============================================================================
 MIB View name           : all_MIB
 MIB Subtree             : 1.3
 MIB Subtree Mask        :
 MIB Subtree View type   : included
===============================================================================
Number of entries: 1

SNMP Groups table
===============================================================================
 SNMP group name                 : public
 Security-model                  : noAuthNoPriv
 Read-only MIB view              : all_MIB
 Read-write MIB view             : all_MIB
 Accessible-for-notify MIB view  : all_MIB
===============================================================================
Number of entries: 1

SNMP user access configuration
===============================================================================
 SNMP user name                  : tester
 SNMP group name                 : public
 SNMP version                    : SNMPv1
 Authentication type             : N/A
 Authentication password string  : N/A
 Encryption password             : N/A
 Remote Engine ID                : N/A
===============================================================================
Number of entries: 1

SNMP Notification targets
===============================================================================
Number of entries: 0
```

```
device-name #show snmp group
SNMP Groups table
===============================================================================
 SNMP group name                 : public
 Security-model                  : noAuthNoPriv
 Read-only MIB view              : all_MIB
 Read-write MIB view             : all_MIB
 Accessible-for-notify MIB view  : all_MIB
===============================================================================


SNMP server configuration
===============================================================================
SNMP server status           : Running
Bind addresses               : 0.0.0.0
Listen port                  : 161
Authentication failure traps : Enabled
```

Changing Port

The default port used is 161. In this example, we will change the port number as it might be that this port will be occupied by other process.

1. Create

```
device-name(config-snmp)#general-port 1100
device-name(config-snmp)#commit
```

2. Show

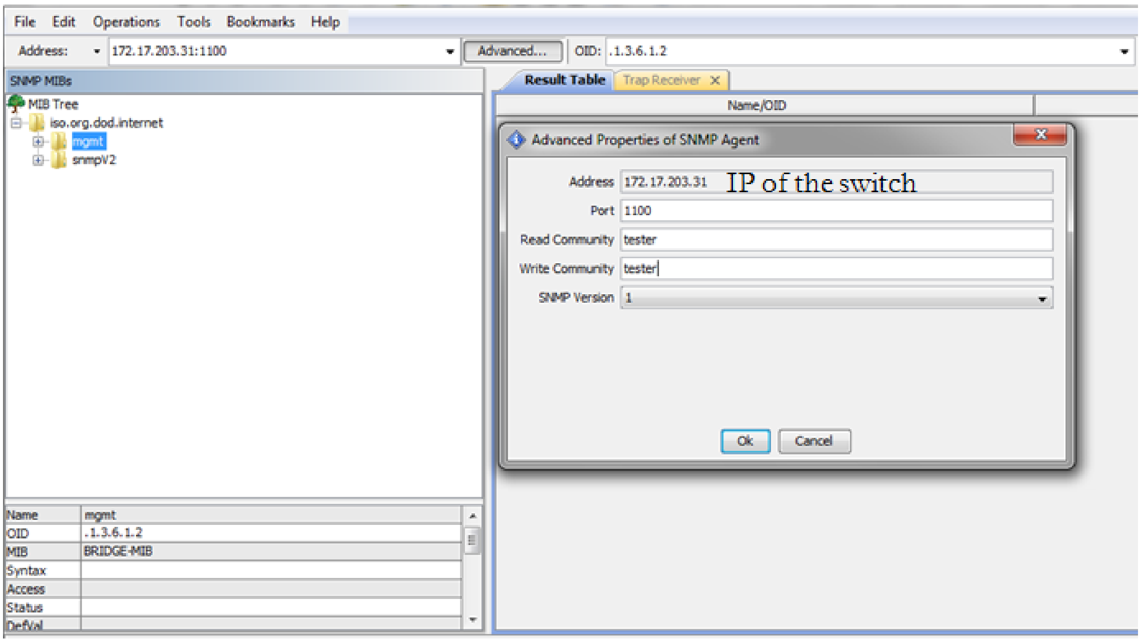
```
device-name#show snmp-server
```

```
SNMP server configuration
===============================================================================
SNMP server status           : Running
Bind addresses               : 0.0.0.0
Listen port                  : 1100
Authentication failure traps : Enabled
```

3. MIB Browser view

Bellow are screen shots of views within an MIB Browser which acts as the SNMP management.

- Configuration of browser:



Address: 172.17.203.31:1100

OID: .1.3.6.1.2

Advanced Properties of SNMP Agent

Address: 172.17.203.31 IP of the switch

Port: 1100

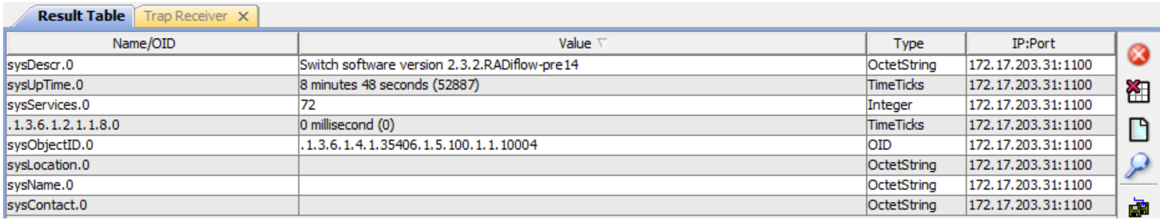
Read Community: tester

Write Community: tester

SNMP Version: 1

Name	mgmt
OID	.1.3.6.1.2
MIB	BRIDGE-MIB
Syntax	
Access	
Status	
DefVal	

- View parameters:



Name/OID	Value	Type	IP:Port
sysDescr.0	Switch software version 2.3.2.RADiflow-pre14	OctetString	172.17.203.31:1100
sysUpTime.0	8 minutes 48 seconds (52887)	TimeTicks	172.17.203.31:1100
sysServices.0	72	Integer	172.17.203.31:1100
.1.3.6.1.2.1.1.8.0	0 millisecond (0)	TimeTicks	172.17.203.31:1100
sysObjectID.0	.1.3.6.1.4.1.35406.1.5.100.1.1.10004	OID	172.17.203.31:1100
sysLocation.0		OctetString	172.17.203.31:1100
sysName.0		OctetString	172.17.203.31:1100
sysContact.0		OctetString	172.17.203.31:1100

SNMP Trap

In this example, a Trap is configured . Target address is set to the IP of the management unit "snmp-mgmt" (user computer) . Destination port on the management unit (computer) is set to 1100.

1. Enable SNMP:

```
device-name#config terminal
device-name(config)#system
device-name(config-system))#snmp
```

2. Assign IP address of target destination:

```
device-name(config-snmp)# target-address snmp-mgmt address 172.17.203.39
```

3. Assign port number at target destination:

```
device-name(config-snmp-mgmt)#dst-port 1100
```

4. Define snmp version model

```
device-name(config-snmp-mgmt)#message-model v1
```

5. Define security name

```
device-name(config-snmp-mgmt)#security-name tester
```

6. Define type of message as Trap:

```
device-name(config-snmp-mgmt)#type trap
```

7. Commit the configuration:

```
device-name(config-snmp-commit)#commit
```

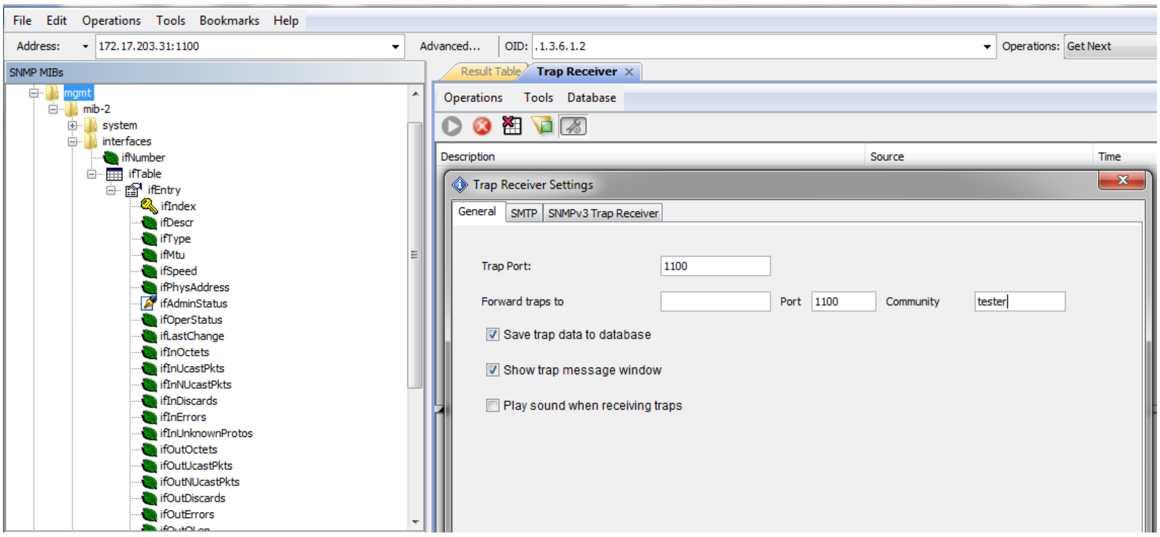
8. Display the SNMP

```
device-name#show running-config system snmp
```

```
SNMP Notification targets
===============================================================================
 Notification target name                : snmp-mgmt
 Security name                           : tester
 Message model                           : v1
 Security level                          : noAuthNoPriv
 Notification target transport type      : IPv4
 Notification target transport address  : 172.17.203.39
 Notification target transport port      : 1100
 Notification target view name           : all_MIB
 Notification target timeout             : 15 seconds
 Notification target retry count        : 3
 Notification type                       : trap
```

9. MIB Browser view

Bellow are screen shots of views within an MIB Browser .



Address: 172.17.203.31:1100

OID: .1.3.6.1.2

Operations: Get Next

Trap Port: 1100

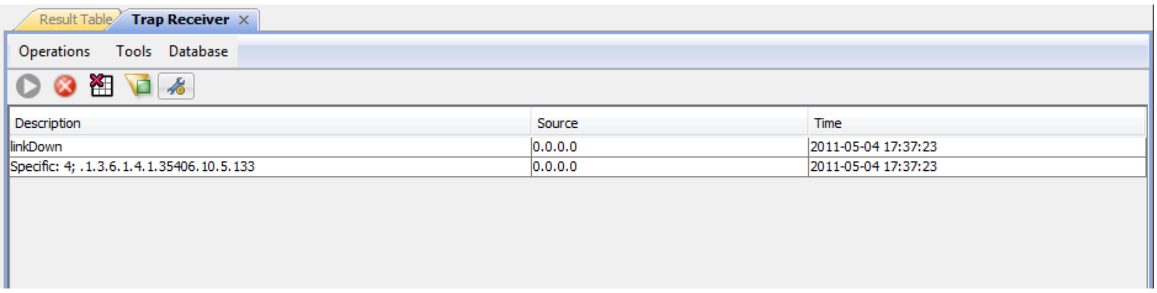
Forward traps to Port 1100 Community tester

☑ Save trap data to database

☑ Show trap message window

□ Play sound when receiving traps

The following trap message apears when dissconencting one of the active link at the switch.



Description	Source	Time
linkDown	0.0.0.0	2011-05-04 17:37:23
Specific: 4; .1.3.6.1.4.1.35406.10.5.133	0.0.0.0	2011-05-04 17:37:23

Supported Standards, MIBs, and RFCs

Feature	Standards	MIBs	RFCs
Simple Network Management Protocol (SNMP)	STD0015, Simple Network Management Protocol STD0016, Structure of Management Information STD0017, Management Information Base STD0058, Structure of Management Information Version 2 (SMIv2) STD0062, Simple Network Management Protocol Version 3 (SNMPv3)	Public MIBs: SNMPV1-MIB MIB-II (RFC1213-MIB) SNMP-COMMUNITY-MIB (RFC2576) SNMPv2-MIB SNMP-VIEW-BASED-ACM-MIB SNMP-USER-BASED-SM-MIB	RFC 1157, SNMPv1—The Simple Network Management Protocol: A full Internet Standard RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II RFC 2579, Textual Conventions for SMIv2 RFC 2580, Conformance Statements for SMIv2 RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) RFC 3413, Simple Network Management Protocol (SNMP) Applications RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) RFC 3417, Transport Mappings for the Simple

Feature	Standards	MIBs	RFCs
			Network Management Protocol (SNMP) RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) RFC 1901, Introduction to Community-based SNMPv2. RFC1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2). RFC1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). RFC3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework

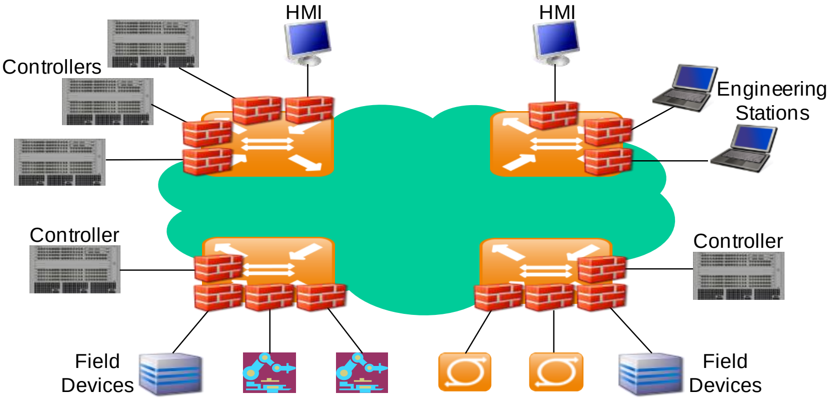
Application Aware Firewall

Overview

The RADiFlow 3xxx switches support remote access contain an integrated firewall on each port, providing a network-based distributed security solution equivalent to the use of personal firewalls on all the industrial devices.

The firewall is "application-aware", meaning that it inspects the contents of the data packets according to the detailed rules regarding the internal parameters of the industrial protocol used.

The resulting distributed service-aware security deployment will monitor all traffic in all the edges of the network and verify that the communication of commands and responses on the application-level between all devices follows the valid application logic as defined by the network operator.



Application-Aware Firewall

The application-aware firewall performs deep application-aware validity checks for specific protocols. This capability is currently supported for Modbus TCP and IEC-60870-5-104 protocols.

TCP/IP Header	Ind. Protocol Header	Function Code	Function Parameters	IP Trailer

For each session the firewall performs several generic validity checks including:

TCP session validity - Check of TCP header fields and check the flow of the TCP session state-machine per session between the source and destination.

Application protocol validity – Check that the packet structure and all its control fields comply to the standard.

Application protocol state-machine – Check that the application-level session flow follows the expected logic as defined in the standard including verification of the master and slave roles, session setup and closing state-machine and command/response interaction.

After the protocol validity tests the firewall checks the application logic. Per each pair of source and destination devices (defined by their IP addresses), the user defines the allowed commands and the optionally also the valid arnges for the command parameters. The firewall will check per flow, each command and its response according to the defined application-level rules.

In addition to the user-defined tests on the application logic the firewall also checks each flow for abnormal behaviour including repetitive usage of specific sensitive commands (device reset, clear diagnostics statistics, etc.), burst of traffic, etc.

Firewall exception handling

Upon each event of a packet violating the security rules several actions are triggered:

Packet Drop - For each rule the user should define whether the violating packets should be dropped or passed as-is with the optional event indications define n this section.

Event Log - The exception event will be logged in the switch in which the exception was spotted. The log entry will include a time-stamp, the packet header and the indication of the rule that was violated.

Counter – Each switch maintains a counter of the firewall security violations per service. The switch increments the appropriate counter for each exception event.

Alarm - An optional alarm for each exception event can be sent from the switch to a management station. In case the iSIM is used a network-wide aggregated view of all security alams is presented.

Simulate Mode

In this mode the firewall will perform all validity checks but will not drop the violating packets. This can be useful for initial activation of the firewall in a network to ensure that the proposed configuration is correct and that valid application sessions are not blocked. Such configuration will override all the "Packet Drop" configurations of the specific rules.

Network-wide operation

The integrated firewall capabilities are best used in a network-wide solution. As such its recommended that the configuration of this solution will be done using the Service Group concept as supported by the dedicated iSIM service management tool that RADiFlow provides.

Service groups are a set of end-devices connected using a specific set of protocols. An end-device can participate in several service groups if there is no overlap in the protocols associated with this service group. Service groups are mapped to separate VLANs in the backbone network so that traffic within a service group reaches only the assigned end-devices.

After defining a service group the user configures a security matrix with detailed security rules for each pair of source and destination IP addresses.

For each such pair the user configures per protocol the following parameters:

State – Allow/Deny/Detailed of traffic in this protocol. In Detailed state the user can further select the allowed commands and their valid parameter ranges.

Rate (Packets/Sec) – The maximum allowed rate of packets in this session.

Master Device – Indication which of the devices is the master in the session (if relevant).

These rules are translated by the iSIM tool to specific security rules for each switch.

Firewall Commands Hierarchy

```
+ root
       + application connect
         + firewall
        - activate mode {disable | simulate | enable }
        - mode show
        - counters show
        - counters clear
        - log show
        - log clear
        - conntrack show
        - conntrack clear
        - rule open
        - rule show
        - rule add <rule>
        - rule delete <rule id>
        - rule save
```

Firewall Commands

Command	Description
Application connect	*Enter the industrial application menu*
Firewall	*Enter the firewall configuration mode*
activate mode **<disable|simulate|enable>**	*Activate firewall in a specific global mode:* • *disable: firewall passes all the traffic* • *simulate: firewall passes all the traffic, but issues logs concerning the traffic* • *enable: firewall filters the traffic according to configured rules and issues logs concerning the traffic*
Show	*Show firewall mode: <disable|simulate|enable>*
counters show	*Show firewall counters*
counters clear	*Clear firewall counters*

Command	Description
`log show`	*Show firewall log*
`log clear`	*Clear firewall log*
`conntrack show`	*Show list of TCP sessions and the session state for each*
`conntrack clear`	*Clear TCP database*
`rule open`	*Read saved firewall rules into the scratch pad for view or edit*
`rule show`	*Show rules currently configured in the scratch pad*
`rule add <rule>`	*Add new firewall rule with the following fields:* *Source IP, Destination IP, Protocol ID, Function Code, Sub function code, Attribute (Pass/Block), Counter number, Log Severity.* *Additional optional 5 triplets of range rules can be added in the following format:* *Range attribute (Pass/Block), Range Low, Range High*
`rule delete <rule id>`	*Delete specified firewall rule*
`rule save`	*Saves rules currently configured in the scratch pad so upon next "firewall activate" command they will take effect*

Secure Remote Access

Overview

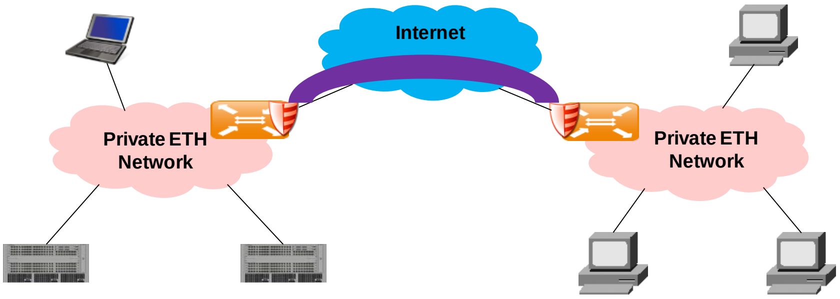
Remote connectivity is one of the main benefits of the usage of Industrial Ethernet infrastructure. Remote access can allow for a distributed deployment in a transparent way and for remote operation and maintenace.

The RADiFlow 3xxx switches contain an 2 mechanisms for secure remote access: Remote user login using a SSH tunnel and inter-site VPN using IPSec.

Inter-site VPN

When a distributed operational network uses public transport links for the inter-site connectivity, the traffic must be encrypted to ensure its confidentiality and its integrity. The RADiFlow 3xxx switches support such a VPN (Virtual Private Network) connection using GRE tunnels (RFC2 2784) over an IPSec encrypted link. The IPSec tunnel can use 3DES or AES encryption according to the user configuration.

The usage of GRE tunneling which supports encapsulation of Ethernet traffic enables the transparent connectivity between the sites as a single Ethernet network without setting up IP routing logic between them. For example such transparent connectivity can be used to preserve the VLAN tagging as a service-indicator or to transfer BPDU between switches in the 2 sites building a common Spanning Tree across the sites.



Remote user login

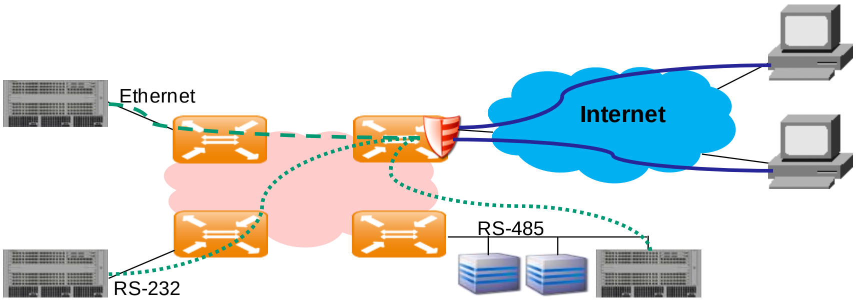
When a remote user needs to access a secure network for operational or maintenance tasks, an encryoted tunnel with limited access rights should be used. The RADiFlow 3xxx switches contain a SSH server for such limited remote access. As such the communication channel between the remote user and the switch is transferred over an encrypted SSH tunnel. Furthermore the system can be configured to use reverse-SSH so that the tunnel is initiated by the server from the secure site outbound. The tunnel is also limited in time with auto-disconnected by the server after the defined period to avoid misuse of tunnels that are left open by the remote user.

After the SSH tunnel is created, the access is controlled per user login authentication and specific access authorizations for each user. The user login is limited according to the remote host from which the session was initiated and for each user there is user-defined set of secure devices to access with specific application protocols.

The SSH tunnel is used as a secure transport for any IP-based protocol with a simple re-route of the traffic in the remote computer to a local-host that is encapsulated over the secure SSH tunnel to the secure network. In this setup the switch acts as a proxy in the application session so that the local network structure in the secure site is not exposed externally and further on-line security checks are performed similar to the functionality of the service-aware firewall. Using the serial gateway capabilities of the switch, remote IP-based sessions can also be translated to serial-based sessions in the local network.

The SSH gateway will log every access (successful and unsuccessful). The logged info includes:

Start Date and Time, End Date and Time, Remote host, User information, Accessed Device, Used protocol, Error code



This access control information is managed in a configuration table which can be manually defined in the switch or can be retrieved from a central RADIUS server.

The configuration table contains several sections:

Global	Maximum amount of concurrent remote sessions and the Timeout period for automatic disconnect of a remote session.
Secure Devices	IP address of the device and its name for remote access
Users	Name and password with a set of Devices and protocols per device that it can access
Remote hosts	IP address, Tunnel initiation method (Normal or using Reverse-SSH) and the list of users that can login from this host

Application IP Interface Commands Hierarchy

```
+ root
        + application connect
          + router
          - interface {create | remove} <IP address> [netmask] [vlan id]
          - default-gw {create | remove} <IP address>
          - show
```

Command	Description
Application connect	*Enter the industrial application menu*
Router	*Enter the application router configuration mode*
interface *create | remove*	*Add or Remove an IP interface for the application engine. The configuration should include:* • *IP address in the format aa.bb.cc.dd* • *netmask for the IP address. example : 255.255.255.0* • *VLAN ID that the application engine will use for this IP interface*
default-gw *create | remove*	*Define or remove the default gateway for an application IP network*
Show	*Show application engine IP interfaces*

GRE Commands Hierarchy

```
+ root
        + application connect
          - tunnel
                - Create [name] <remote end point>
                - Remove [name] <remote end point>
          - clear statistics
          - show
```

GRE Commands

Command	Description
Application connect	*Enter the industrial application menu*
Tunnel	*Enter the tunnel configuration*
Create / remove	• *name* • *remote end point : IP address of remote end point aa.bb.cc.dd*
Clear statistics	*Clears tunnel counters*
Show	*Show application engine IP interfaces*

IPSec Commands Hierarchy

```
+ root
        + application connect
          + ipsec
        association
          - create <from> <to> [algorithm] [key receive] [key transmit]
                [spi]
          - remove <from> <to>
          - update <from> <to> [algorithm] [key receive] [key transmit]
                [spi]
          - show
```

IPsec Commands

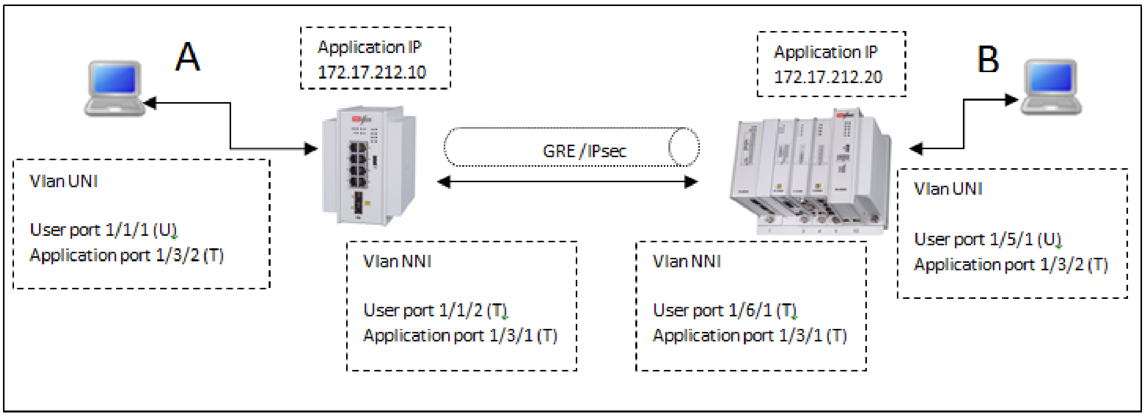
Command	Description
Application connect	*Enter the industrial application menu*
IPsec association	*Enter the IPsec configuration mode*
create	*Add or Remove an IP interface for the application engine. The configuration should include:* • *From: local application IP interface address.* • *To: remote switch application IP interface address.*
Algorithm	• *Optional encryption algorithms are "3des-cbc-192bit", "aes-cbc-160bit", "aes-cbc-220bit".* ▪ *Key receive :* ***"3des-cbc-192bit"** – 24 characters user defined key* ***"aes-cbc-160bit"** – 16 characters user defined key* ***"aes-cbc-220bit"**- 32 characters user defined key* ▪ *Key transmit :* ***"3des-cbc-192bit"** – 24 characters user defined key* ***"aes-cbc-160bit"** – 16 characters user defined key* ***"aes-cbc-220bit"**- 32 characters user defined key* ▪ *Spi : security parameter index Please specify a value ≥256. Must be identical at all remote end of the tunnel.*
remove	• *from: local switch application IP interface address.* • *To: remote switch application IP interface address.*
Show	*Show IPsec*

Example for GRE over IPsec

The following example will demonstrate proper configuration of GRE over secure link using IPsec.

Concept :

- computer A requires secure link with computer B at remote site. 2 RADiflow switchs establish the link between remote sites.
- At each site ,the traffic of the local computer will be directed to the application card in order to be encapsulate it with GRE. Vlan "UNI" will be used.
- An IPsec link will be established between the application IP interfaces of the switchs. please see here for more information on application IP interfaces.
- The traffic will be directed from the application card to the nni port. Vlan "NNI" will be used.
- GRE will run over the IPsec link.
- Note : names and parameters highlighted in bold red are mendatory "as is".



STEP 1 : create the tunnel

Site A :

1. Create vlan UNI to direct traffic from the user port to the application:

```
3080#config terminal
Entering configuration mode terminal
3080(config)#vlan uni 100
3080(config-vlan-uni/100)#tagged 1/3/2
3080(config-tagged-1/3/2)#untagged 1/1/1
3080(config-untagged-1/1/1)#top
3080(config)#port 1/1/1
3080(config-port-1/1/1)#default-vlan 100
3080(config-port-1/1/1)#end
3080#
```

2. Create vlan NNI to direct traffic from the application to the NNI port:

```
3080#config terminal
Entering configuration mode terminal
3080(config)#vlan nni 101
3080(config-vlan-nni/101)#tagged 1/3/1
3080(config-tagged-1/3/1)#tagged 1/1/2
3080(config-port-1/1/2)#end
3080#
```

3. Assign the IP routing interface and correlate it with the NNI vlan

```
3080#application connect
RADiFlow Application Module
radiflow-app login: ind
Password:ind
Welcome to Radiflow industrial CLI
[/]router interface create address 172.17.212.10 netmask 255.255.255.0 vlan 101
[/]commit
committed ok…
[/]router show
                     Local IP Address          =172.17.212.10/24
                     VLAN                      =101

[/]
```

4. Create the tunnel . The remote end point will be the IP of the remote switch application interface.

```
[/]tunnel create name gre remote-end-point 172.17.212.20
[/]commit
Committed ok…
[/]
```

Site B :

5. Create vlan UNI to direct traffic from the user ports to the application:

```
3700#config terminal
Entering configuration mode terminal
3700(config)#vlan uni 100
3700(config-vlan-uni/100)#tagged 1/3/2
3700(config-tagged-1/3/2)#untagged 1/5/1
3700(config-untagged-1/5/1)#top
3700(config)#port 1/5/1
3700(config-port-1/5/1)#default-vlan 100
3700(config-port-1/5/1)#end
3700#
```

6. Create vlan NNI to direct traffic from the application to the NNI port:

```
3700#config terminal
Entering configuration mode terminal
3700(config)#vlan nni 101
3700(config-vlan-nni/101)#tagged 1/3/1
3700(config-tagged-1/3/1)#tagged 1/6/1
3700(config-port-1/6/1)#end
3700#
```

7. Assign the IP routing interface and correlate it with the NNI vlan

```
3700#application connect
RADiFlow Application Module
radiflow-app login: ind
Password:ind
Welcome to Radiflow industrial CLI
[/]router interface create address 172.17.212.20 netmask 255.255.255.0 vlan 101
[/]commit
committed ok…
[/]router show
                     Local IP Address          =172.17.212.20/24
                     VLAN                      =101

[/]
```

8. Create the tunnel . The remote end point will be the IP of the remote switch application interface.

```
[/]tunnel create name gre remote-end-point 172.17.212.10
[/]commit
Committed ok…
[/]
```

At this point the tunnel is established and all traffic between the 2 computers is made in it.

It is not mandatory to add the IPsec for the simple transparent forwarding of the traffic.

STEP 2 : Secure the tunnel using IPsec

Site A :

9. Activate IPsec. The chosen alogorithm is 3des-cbc-192bit .
   24 characters are required as key.
   Transmit key should be idenical to receive key at the remote site B.
   "from" represents local IP of the application interface and "to" reffers to the remote switch application interface.
   "spi" should be identical at both ends.

```
3080#application connect
RADiFlow Application Module
radiflow-app login: ind
Password:ind
Welcome to Radiflow industrial CLI
[/]ipsec association
[ipsec/association/] create from 172.17.212.10 to 172.17.212.20 algorithm
                    3des-cbc-192bit key-transmit 123456789012345678901234 key-receive
                    412345678901234567890123 spi 11111
[/]commit
Commited ok…
[/]
```

Site B :

1. Activate IPsec.

```
3080#application connect
RADiFlow Application Module
radiflow-app login: ind
Password:ind
Welcome to Radiflow industrial CLI
[/]ipsec association
[ipsec/association/] create from 172.17.212.20 to 172.17.212.10 algorithm
                    3des-cbc-192bit key-transmit 412345678901234567890123 key-receive
                    123456789012345678901234 spi 11111
[/]commit
Commited ok…
[/]
```

At this point the tunnel is established over IPsec.

Serial Tunneling

Overview

The serial I/O module of the RADiFlow 3xxx switches connects “legacy” serial-based industrial devices to an Ethernet network. The serial module has 2xRS-232 interfaces and 2xRS-485 interfaces and an internal programmable logic to support a variety of serial protocols.

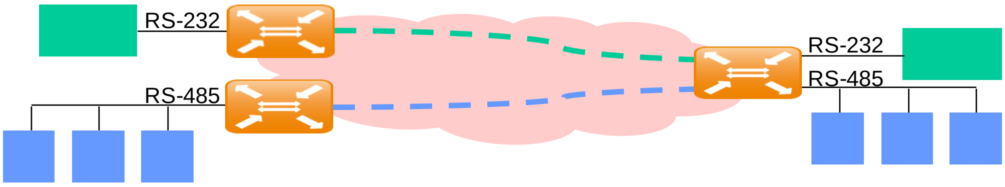
Each of the serial ports can be configured to work in one of three modes of operation: Transparent tunneling, Bridge tunneling or Protocol Gateway.

The configuration of the serial tunnel is done in 2 steps:

- Configuration of the serial bus characteristics including protocol type, baud-rate, assembly time-out, jitter buffer length, etc.
- Configuration of the tunnel parameters including neighbouring IP entities, tunnel VLAN, etc.

Transparent tunneling

This is a simple method of extending indusrtial serial busses over an Ethernet network. In this mode data is transferred through the serial bus to the switch , encapsulated into ethernet packets and sent to the destination switch and then decapsulated and transmitted on the appropariate serial interface to the destination device.



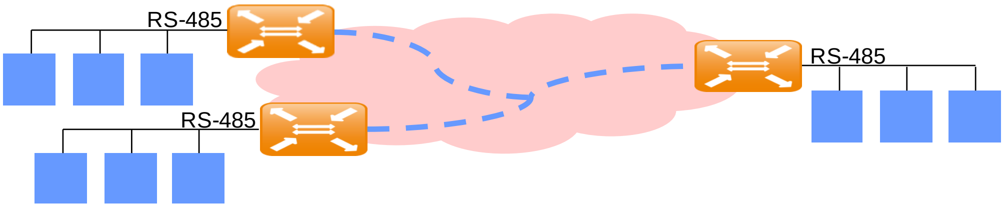
In the transparent mode the switches do not understand the serial protocol so the transmitter collects data bytes and sends them to the other side as is. The packetization is done in blocks of 40 bytes (that fit the data portion of a 64 bytes minimum size Ethernet packet). In case of slow data rates on the serial line or short byte sequences followed by idle periods, packets are also closed on a time-out which is configured by the user. The tunnel packet processing in the transmitter and reciever sides require 50uSec in each side and the additonal network lateny should be taken into account. As a result the latency introduced by the tunnel equals:

Tunnel latency = Min (40*ByteTime, AssemlyTimeout)+2*50uSec+Network latency.

Assuming that the serial tunnel packets are handled in high priority in the network, minimal tolerance in the network latency is introducned due to the potential head-of-line queuing in each switch along the route. To avoid packet timeouts on the serial busses due to the tolerance between the received tunnel packets a jitter buffer is implemented in the receive side of the tunnel. The length of the jitter buffer is user configurable.

Bridge tunneling

This is a more intelligent method for connecting serial busses over the Ethernet network. In this mode the switches understand the industrial protocol used in the serial bus and verify the packet integrity of the packets that are transferred across the Ethernet network. As such in this mode multipoint connections can be used to connect several remote bus segments together.



The following protocols are currently supported in bridging mode: Modbus RTU, Modbus ASCII, Profibus and IEC-60870-5-101. Based on the programmable logic of the tunneling used in the switch additonal protocols with a clearly defined packet structure can be supported per request.

In this mode data is transferred through the serial bus to the switch , encapsulated into ethernet packets and sent to the destination switch and then decapsulated and transmitted on the appropariate serial interface to the destination device.

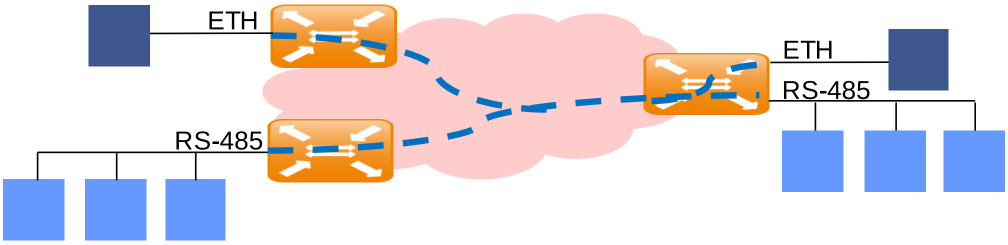
In the bridging mode the switches understand the serial protocol so the transmitter collects data bytes according to the overlay protocol according to the start and stop bytes of the serial packet. To minmize the tunel latency the serial packet is also segmented in blocks of 40 bytes (that fit the data portion of a 64 bytes minimum size Ethernet packet) or according to a user-configurable time-out for slow data rates.

As described in the transparent tunneling mode additional latency of 2*50uSec is introduced bu the tunnel packet processing and the network latency should be also taken into account. The potential tolerance in the network latency is handled by the jitter buffer which is implemented in the receive side of the tunnel with a user-configurable length

Protocol Gateway

The RADiFlow 3xxx switches can act as a protocol gateway converting serial based industrial protocols to their correlating IP based variant, enabling the deployment of a mixed network with serial-based and Ethernet-based devices. In this mode the switch acts as a master on the serial bus and as a server in the IP network for the correlating protocol. This mode is supported The switch takes the “legacy” industrial serial bus protocol and converts it into the relevant IP world,and more specifically, into industrial Ethernet protocol (e.g. Modbus RTU/ASCII to Modbus/TCP, etc.).

The following protocols are currently supported in gateway mode: Modbus RTU/ASCII to Modbus TCP and IEC-60870-5-101 to IEC-60870-5-104.



Serial tunneling Commands Hierarchy

```
+ root
        + application connect
          + serial
               + port
                  - clear counters
                  - create <slot> <port> <baudrate> <parity> <stopbits>
                  - remove <slot> <port>
                  - show
                  - update <slot> <port> <baudrate> <parity> <stopbits>
            + local-end-point
                  - create <slot> <port> <service-id> <position>
                  - remove <slot> <port> <service-id>
                  - show

            +  remote-end-point <service-id>
                  - create <IP address> <service-id> <position>
                  - remove <IP address> <service-id>
                  - show
```

Serial tunneling Commands

Command	Description
Application connect	*Enter the industrial application menu*
Serial port *UU/SS/PP*	*Enter the configuration mode for a specific physical serial ports*
Clear counters	*Clear counters*
Create	*Slot : physical Slot number;* *Port : physical port number.* *Baud rate : 1200,2400,4800,9600,19200,38400, 57600, 115200,230400,460800,921600* *Parity : no, odd, even* *Stopbits : 1,2*
Remove	*Slot : physical Slot number;* *Port : physical port number.*
Show	
Local-end-point	
Create	*Slot : physical Slot number;* *Port : physical port number.* *Service id : numeric value of serial service.* *Position:* *N/A - point to point* *Master – point to multipoint* *Slave – point to multipoint*
Remove	*Slot : physical Slot number;* *Port : physical port number.* *Service id : numeric value of serial service.* *Position:* *N/A - point to point* *Master – point to multipoint* *Slave – point to multipoint*
show	
Remote-end-point	
Create	*address : IP address aa:bb:cc:dd* *Service id : numeric value of serial service.* *Position:* *N/A - point to point* *Master – point to multipoint* *Slave – point to multipoint*

Command	Description
Remove	*address : IP address aa:bb:cc:dd* *Service id : numeric value of serial service.*
show	

Serial interfaces

Note : configuration of the serial interfaces and tunneling and gateway requires the application processor to be installed.

The Serial IO card

A serial io card holds 2 xRS-485 and 2xRS-232 ports.

The interfaces of the RS 485 ports are DB-9 type.
The application cpu maps these ports as :

slot [backplane slot number] port 1

slot [backplane slot number] port 2

The RS 232 interfaces of the ports are RJ-45 type.
The application cpu maps these ports as :

slot [backplane slot number] port 3

slot [backplane slot number] port 4

The serial IO card can be assembled on slots 4 -9 of the backplane so total of 24 serial ports are possible using the 3700 switch. Precondition to use the serial IO is to install the application cpu on slot number 3.
The central switch maps each serial IO card as one IO component and does not regard each port individualy. Adressing specific ports of each IO card (1,2 for RS 485 and 3,4 for RS 232) is done within the application CLI. The central switch identifies the different serial IO cards as they are physicaly assembled on different slots but each card is mapped as one port , allways numbered as '2'.

The following table details the required mapping of the Serial Io card itself and its ports within the central switch and within the application.

backplane slot number	Card mapping at Central Switch CLI	VLAN membership	Ports mapping at Application CLI	Serial foramt	Physical port interface
4	1/4/2	Untagged member of vlan 3500	Slot 4 port 1 Slot 4 port 2 Slot 4 port 3 Slot 4 port 4	RS 485 RS 485 RS 232 RS 232	DB-9 DB-9 RJ-45 RJ-45
5	1/5/2	Untagged member of vlan 3500	Slot 5 port 1 Slot 5 port 2 Slot 5 port 3 Slot 5 port 4	RS 485 RS 485 RS 232 RS 232	DB-9 DB-9 RJ-45 RJ-45
6	1/6/2	Untagged member of vlan 3500	Slot 6 port 1 Slot 6 port 2 Slot 6 port 3 Slot 6 port 4	RS 485 RS 485 RS 232 RS 232	DB-9 DB-9 RJ-45 RJ-45
7	1/7/2	Untagged member of vlan 3500	Slot 7 port 1 Slot 7 port 2 Slot 7 port 3 Slot 7 port 4	RS 485 RS 485 RS 232 RS 232	DB-9 DB-9 RJ-45 RJ-45
8	1/8/2	Untagged member of vlan 3500	Slot 8 port 1 Slot 8 port 2 Slot 8 port 3 Slot 8 port 4	RS 485 RS 485 RS 232 RS 232	DB-9 DB-9 RJ-45 RJ-45
9	1/9/2	Untagged member of vlan 3500	Slot 9 port 1 Slot 9 port 2 Slot 9 port 3 Slot 9 port 4	RS 485 RS 485 RS 232 RS 232	DB-9 DB-9 RJ-45 RJ-45

Serial default VLAN 3500

To create serial tunneling, the serial IO card must be a member of VLAN 3500.

Example for vlan memership assisgnment of the serial IO card:

```
+ root

Config

Vlan serial 3500  //the name "serial" is an example only
                     the value 3500 is mendatory.

Untagged 1/5/2    //the serial IO card which is physically assembled on slot
                     5 of the bacplane is assigned to vlan 3500 as untagged
                     member. The value '2' is mendatory

Tagged 1/3/1      //the application port 1/3/1 must be a tagged member.

Commit

Top

Port 1/5/2

Default-vlan 3500 //vlan 3500 must be the default vlan for the io card.

Commit
```

Declaration of ports

In order to have each one of the 4 ports at the serial IO card be available ,they must be declared within the application CLI.

Example for port declaration:

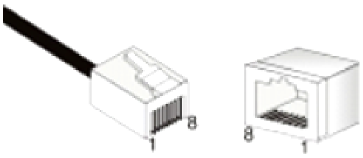
```
+ root

Application connect  //entering application cli

serial

Port create slot 5 port 3  //decleration of port 3 of serial IO card
                           which is assembled on slot 5 of the backplane.

Port create slot 5 port 4  //decleration of port 4 of serial IO card
                           which is assembled on slot 5 of the backplane.

Port create slot 6 port 3  //decleration of port 3 of serial IO card
                           which is assembled on slot 6 of the backplane.

Port create slot 9 port 4  //decleration of port 4 of serial IO card
                           which is assembled on slot 9 of the backplane.

 ..

Commit
```

RS- 232 Serial cables

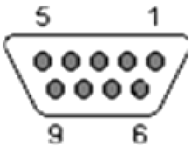
Two types of cables are available to connect the serial interface RS 232 port to DCE and DTE end devices.

The RS-232 ports are of RJ-45 type and so the cables will have one end of male RJ-45 and second end of female DB-9.

Serial port at the switch



DB-9 female conector for end device



Pinout for crossed cable :

cable		Switch port
Female DB-9	Male RJ-45	Female RJ-45
2	6	6 TX
3	5	5 RX
5	4	4 GND

Pinout for straight cable:

cable		Switch port
Female DB-9	Male RJ-45	Female RJ-45
2	5	6 TX
3	6	5 RX
5	4	4 GND

Steps for realizing serial tunneling

1. Create VLAN for each service.
2. For each ,associate port 1/3/1 as tagged. Associate the uplink port as tagged member.
   In bellow example see vlans 850 ,851.
3. Create application routing interface with desired IP address. The vlan associated with the routing interface must be the same one as of the first service.
   In bellow example see vlan 850 used .
4. Establish IP communication between the switches based on Application Routing Interface . check with ping from within the application
5. Create VLAN for the serial ports. Must be numbered 3500.
6. Assign the serial ports to the vlan as untagged 1/x/2 (x- slot number).
   Associate 1/3/1 as tagged member.
   In bellow example see port 1/6/2 and 1/3/1 associated to vlans 850 ,851.
7. Configure serial parameters.
   Assign speed to 1000 and full duplex to serial ports.
   In bellow example see ports 1/6/3 ,1/6/4.
8. Define services to co-relate the IP interface and the serial ports.
   see services 1 and 2.
9. Configure ports position.
   See Master/Slave assignment to ports 1/6/3 ,1/6/4 .
10. Configure local end point
11. Configure remote end point
12. Define ACLs to enabe the network to determine between the different services

Serial tunneling example

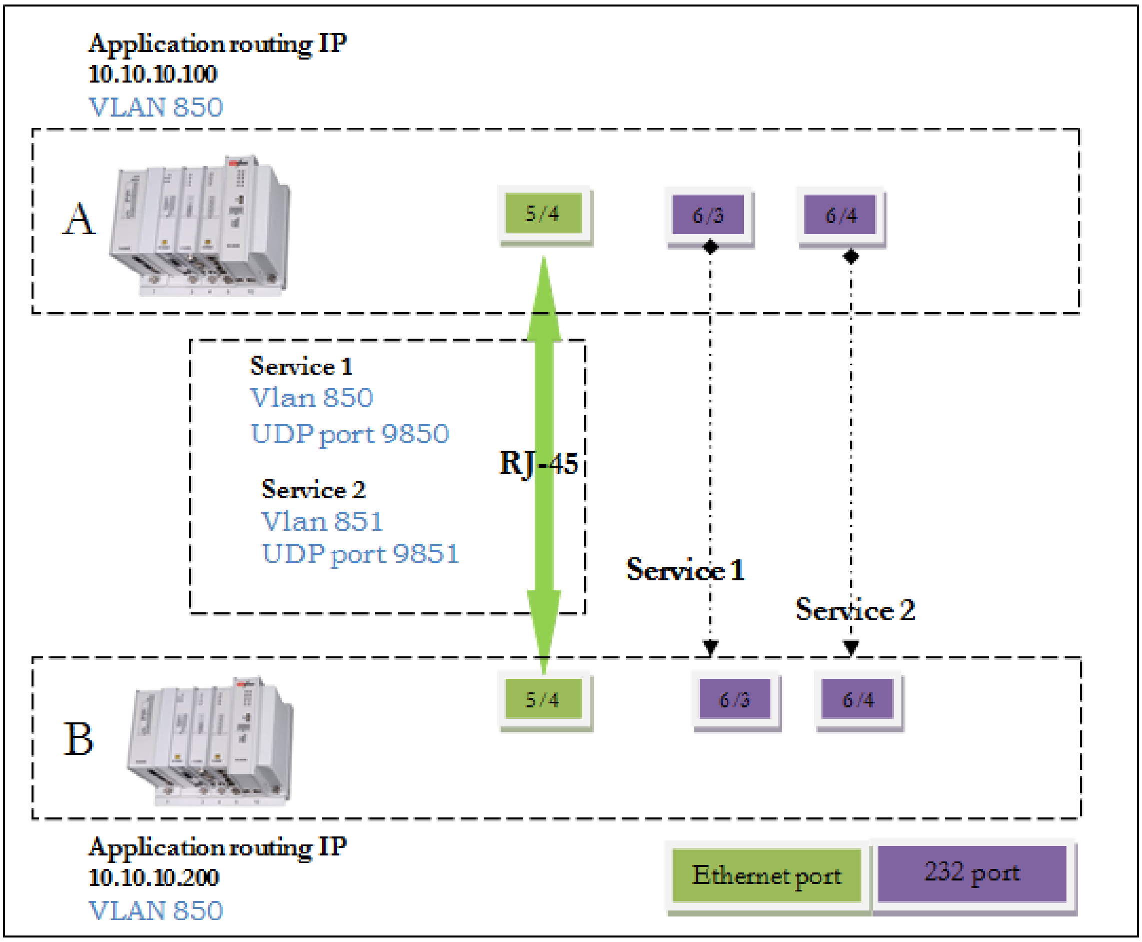
The bellow CLI commands realizes the following topology :

Switch A connected to switch B directly with ports 1/5/4 of each (network port).

Each switch has a serial card at slot 6. Ports 3,4 are used for 232 serial tunneling.

Switch A ports acts as master for the serial services.

2 services (point to point each) are created between the switchs.



For Both Switchs

ACL configuration

```
+ root
config
ip access-list extended 130
remark "850 to 851"
rule 1
action  permit
protocol            udp
source_ip           any
destination_ip      any
udp-source-port     9851
udp-destination-port 9851
vlan                850
top
ip access-list extended 140
remark "851 to 850"
rule 1
action              permit
protocol            udp
source_ip           any
destination_ip      any
udp-source-port     9851
udp-destination-port 9851
vlan                851
top

port 1/3/1
ip-access-group-extended 130 vlan vlan 851
top
port 1/5/4
ip-access-group-extended 140 vlan vlan 850
top
commit
exit
```

VLAN configuration

```
+root
Config
Vlan default 1
No untagged 1/3/1
No untagged 1/5/4
No untagged 1/6/2
Exit
Vlan serial 3500
Tag 1/3/1
Untagged 1/6/2
Vlan service1 850
Tagged 1/3/1
Tagged 1/5/4
Exit
Vlan service2 851
Tagged 1/3/1
Tagged 1/5/4
Exit
Port 1/5/4
Default-vlan 850
Exit
Port 1/6/2
```

```
Default-vlan 3500
duplex full
speed 1000
commit
top
exit
```

SWITCH A

```
Application connect
router interface create address 10.10.10.100 netmask 255.255.255.0 vlan 850
serial
port create slot 6 port 3
port create slot 6 port 4
local-end-point create slot 6 port 3 service-id 1 position master
local-end-point create slot 6 port 4 service-id 2 position master
remote-end-point create address 10.10.10.200 service-id 1 position slave
remote-end-point create address 10.10.10.200 service-id 2 position slave
..
commit
```

SWITCH B

```
Application connect
router interface create address 10.10.10.200 netmask 255.255.255.0 vlan 850
serial
port create slot 6 port 3
port create slot 6 port 4
local-end-point create slot 6 port 3 service-id 1 position slave
local-end-point create slot 6 port 4 service-id 2 position slave
remote-end-point create address 10.10.10.100 service-id 1 position master
remote-end-point create address 10.10.10.100 service-id 2 position master
..
commit
```

Discrete IO Tunneling

Discrete channel interfaces

Discrete signals are very common in industrial application to monitor alarams and indications from the field side.

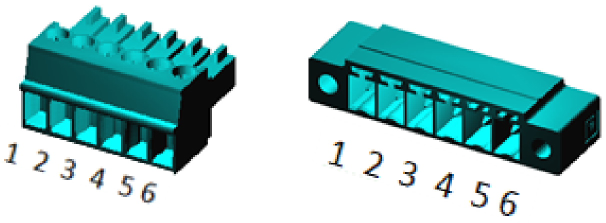
The RADiflow 3x00 switch allows the most effective feature of tunneling these channels over the IP network.

The status of the digital input will be available as digital output at the remote end point configured by th user.

Configuration of the discrete channle tunneling requires the application processor to be installed.

Connection terminal are as shown in bellow figure.

1. Digital output 1
2. Digital output 2
3. Digital output ground
4. Digital Input ground
5. Digital Input 2 (+5v)
6. Digital Input 1 (+5v)



Services

2 services are available at the application card. The relation between the services and physical connection is as follow :

Service ID 1 : relates to either digital input 1 (terminals 6,4) or digital output 1 (terminals 1,3).

Service ID 2 : relates to either digital input 2 (terminals 5,4) or digital output 2 (terminals 2,3).

At each switch ,when declaring the use of a service ,the direction of operation must be determined, as input or output thus associating the the relevant physical hardware to the service ID.

Service			
	Service ID 1	Direction	Hardware terminals
		input	6,4
		output	1,3
	Service ID 2	Direction	Hardware terminals
		input	5,4
		output	2,3

Diagnostics and logic states

1. Within the CLI diagnostics of the discrete chanels can be viewed using the show command

   ```
   device-name(config-snmp)#application connect
   Welcome to Radiflow industrial CLI
   [/]discrete
   [discrete/] show
   ```

2. Status of digital input is either high or low.
   a. Default : low.
   b. If no IP communication : reserve last state.
   c. When Voltage available at the terminals : 'high'
   d. When Voltage unavailable at the terminals : 'low'
3. Status of digital output is either open or closed.
   a. Default – open.
   b. No is not assigned to a service – open.
   c. If is assigned to service ,the local state will be equal to the state of corresponding remote input.
      a. Remote input =High = > local do =closed
      b. Remote input =low = > local do =open
   d. If no IP communication available to remote input – reserve last state.
4. IP Traffic of the discrete services over the routing interface is indicated by constant green flashing of the network led.

Technical data

At digital Inputs please connect a 5v DC source at terminals 6,4 for channel 1 or 5,4 for channel 2.

Digital outputs are dry mechanical relay contacts. Maximum power to be implemented at the contacts :

AC:	Max 250v , 37.5vA.

DC:	Max 220v ,30 watt.

Above mentioned power limitations should not be exceeded .
maximum current allowed at the contacts is 1A.

Discrete IO tunneling Commands Hierarchy

```
    + root
            + application connect
              + discrete
                   + service
                      - create <service id> <direction> <remote end point>
                      - remove <service id> <direction>
                      - show
                   + show
```

Discrete IO tunneling Commands

Command	Description
Application connect	*Enter the industrial application menu*
Discrete	*Enter the configuration mode for a specific physical serial ports*
create	*Service id : valid values 1,2* *Direction : input, output* *Remote end point : ip address of remote end point.*
remove	*Service id : valid values 1,2* *Direction : input, output*
Show	

Steps for realizing serial tunneling

1. Create VLAN for the service.
2. Associate the application port 1/3/1 as tagged. Associate the uplink port as tagged member. In bellow example see vlans 850.
3. Create application routing interface with desired IP address. Associate the routing interface to the service VLAN.
   In bellow example see vlan 850 used .
4. Establish IP communication between the switches based on Application Routing Interface . check with ping from within the application
5. Assign services for discrete channels 1 and/or 2.
6. At each switch assign the service id direction as either input or output.
7. Wire input connection point.
8. Wire output load.

Configuration example

In this example, digital input channel 1 at switch A will be tuuneled to switch B at digital output channel 1. port 1/4/1 is chosen as the uplink (network) port at both switchs.

1. Create a vlan for the discrete services and assign members:

```
device-name#config terminal
device-name(config)#vlan discrete 850
device-name(config- vlan discrete/850)#tagged 1/3/1
device-name(config- vlan discrete/850)#tagged 1/4/1
device-name(config- vlan discrete/850)#commit
```

2. Enter application command line.

```
device-name(config-snmp)#application connect
Welcome to Radiflow industrial CLI
```

3. Create an IP routing interface at switch A:

```
[/]router
[router/]interfcae create address 10.10.10.10 netmask 255.255.255.0 vlan 850
[router/]..
```

4. Create an IP routing interface at switch B :

```
[/]router
[router/]interfcae create address 10.10.10.11 netmask 255.255.255.0 vlan 850
[router/]..
```

5. Create an input service at switch A ,service ID 1:

```
[/]discrete
[discrete/] service create service-id 1 direction input remote-end-point 10.10.10.11
```

6. Create an output service at switch B ,service ID 1:

```
[/]discrete
[discrete/] service create service-id 1 direction output  remote-end-point 10.10.10.10
```

7. Setup is ready.

Operations, Administration, and Maintenance (OAM)

IEEE 802.1ag Connectivity Fault Management (CFM) refers to the ability of a network to monitor the health of an end-to-end service delivered to customers (as oppose to just links or individual bridges). The pre-standard IEEE 802.1ag CFM feature, called MAC ping/trace route, defines the end-to-end OAM capabilities that are intrinsic to Ethernet technology, enabling service providers to monitor the Ethernet service that the customer receives.

The 802.1ag CFM standard specifies protocols, procedures, and managed objects to support transport fault management. These allow:

- the discovery and verification of the frames' path addressed to and from specified network users
- the detection and isolation of a connectivity fault to a specific bridge or LAN

Ethernet CFM defines proactive and diagnostic fault localization procedures for point-to-point and multipoint Ethernet Virtual Connections (EVC) that span one or more links.

CFM-OAM Protocol Functionality

CFM-OAM supports the following basis functionalities:

- *Discovery & Connectivity:* the ability to discover other CFM-OAM enabled devices and verifying the connectivity to these devices
- *Fault Verification:* the ability to verify and test the quality of the service delivered
- *Fault Isolation:* the ability to identify and isolate the point of fault within the service path

CFM Purpose

Bridges are increasingly used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment.

CFM provides capabilities for detecting, verifying, and isolating connectivity failures in such networks, where multiple organizations are involved in providing and using the Ethernet service (such as customers, service providers, and operators).

Customers purchase Ethernet service from service providers. These service providers may utilize their own networks or the networks of other operators to provide connectivity for the requested service. Customers themselves may be service providers. For example, a customer may be an Internet service provider that sells Internet connectivity.

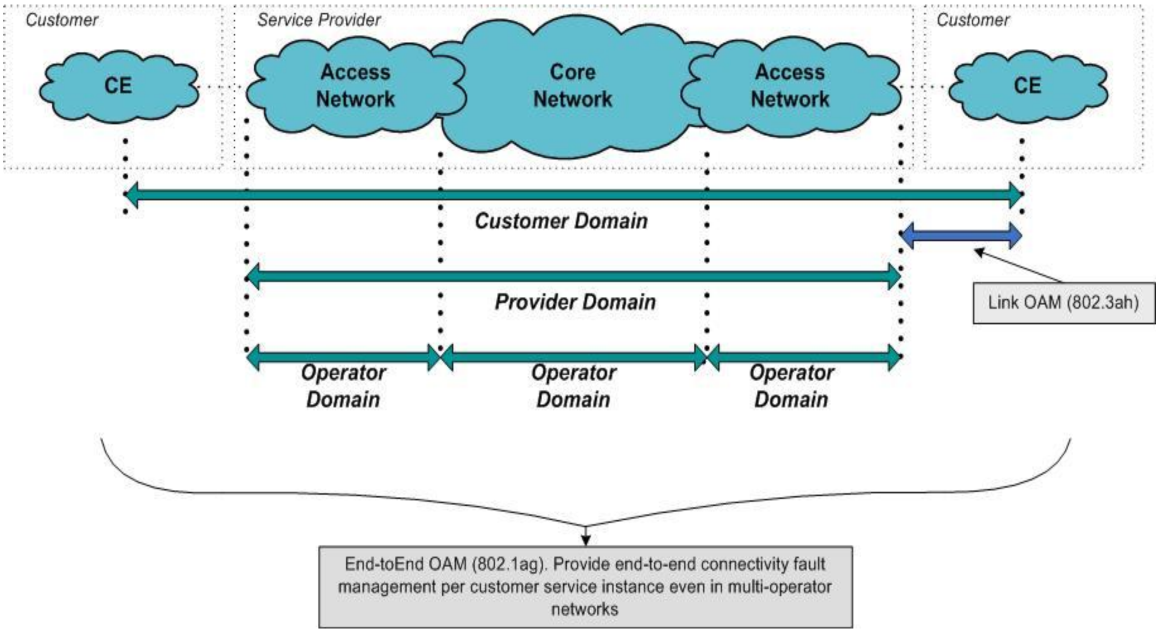


Figure 13: OAM Ethernet Tools

Operators need minimal Ethernet OAM as oppose to providers that need more comprehensive Ethernet OAM for themselves and the ability to provide customers with better monitoring functionality.

In order to validate the service quality and to perform fault verification on Maintenance End Points (MEP) and Maintenance Intermediate Points (MIPs) that belong to the organization, each organization defines its own maintenance domain. These MEPs and MIPs are then linked to the relevant domain creating a Maintenance Association (MA).

Mechanisms of Ethernet 802.1ag OAM

The mechanisms supported by CFM include Connectivity Check Messages (CCM), loopback, link trace and Alarm Indication Signal (AIS).

CFM allows for end-to-end fault management that is generally reactive (through loopback, link trace messages, and Alarm Indication Signals) and connectivity verification that is proactive (through Connectivity Check messages).

CFM Command Hierarchy

```
+ root
     + config terminal
      + oam
          + cfm
              + [no] shutdown
              + [no] domain-name DOMAIN-NAME
                  - level <level>
                  + [no] ma MA-NAME
                      - service <svc-id>
                      - [no] ais-lck
                      - [no] ais-lck-interval {1min | 1sec}
                      - [no] ais-lck-level <level>
                      - [no] ais-lck-priority <priority>
                      - [no] ccm-priority <priority>
                      - clear-remote-mep-table <MEP-id>
                      - [no] fault-alarms-level <detect-priority>
                      - [no] fng-alarm-time <alarm-time>
                      - [no] fng-reset-time <reset-time>
                      - [no] hello-interval <index>
                      - [no] mep <MEP-id> SAPSTRING
                          - [no] shutdown
                          - direction {up | down}
                          - [no] ccm-enabled
                          - [no] ccm-priority <priority>
                      - [no] mip-policy {default | explicit | none}
                      - [no] sender-id-content {chassis-id | chassis-manage-id | manage-id | none}
              + [no] threshold-profile <threshold_profile-id>
                  - [no] one-way-jitter-error <error-value>
                  - [no] one-way-jitter-warning <warning-value>
                  - [no] frame-loss-error <error-threshold>
                  - [no] frame-loss-warning <warning-threshold>
                  - [no] round-trip-jitter-error <error-value>
                  - [no] round-trip-jitter-error-period <period-value>
                  - [no] round-trip-jitter-warning <warning-value>
                  - [no] round-trip-jitter-warning-period <period-value>
```

- [no] **round-trip-latency-error** *<error-value>*
- [no] **round-trip-latency-error-period** *<period-value>*
- [no] **round-trip-latency-warning** *<warning-value>*
- [no] **round-trip-latency-warning-period** *<period-value>*
- [no] **results-bucket-size** *<size>*
- [no] **priority** *<priority>*
- [no] **rate** *<rate>*
- [no] **tlv-size** *<size>*

- [no] **update-interval** *<interval>*
- [no] **test** *<test-id> DOMAIN-NAME MA-NAME <threshold_profile-id>* **[repeat-interval** *number***]**

- **show oam cfm**
- **show oam cfm connectivity [domain-name** *DOMAIN-NAME***] [ma** *MA-NAME***]**
- **show oam cfm connectivity [extended]**
- **show oam cfm domain level** *<level>*
- **show oam cfm test**
- **show oam cfm threshold-profile**

CFM Configuration Commands

Table 1: CFM Configuration Commands

Command	Description
config terminal	Enters the Configuration mode
oam	Enters the OAM Protocol Configuration mode
cfm	Enters the CFM Protocol Configuration mode
shutdown	Disables CFM
no shutdown	Mandatory Enables CFM
domain-name *DOMAIN-NAME*	Mandatory Creates a maintenance domain (MD) and enters a Specific Maintenance Domain mode: • *DOMAIN-NAME: a string of <1-43> characters*
no domain-name *DOMAIN-NAME*	Removes the maintenance domain
level *<level>*	Mandatory Defines a domain's level: • *level: in the range of <0-7>* The domain's levels are: • Operator's MA levels: 0–2 • Provider's MA levels: 3–4 • Customer's MA levels: 5–7
ma *MA-NAME*	Mandatory Creates a maintenance association (MA) and enters a Specific Maintenance Association Configuration mode: • *MA-NAME: a string of <1-45> characters*
no ma *MA-NAME* **service** *<svc-id>*	Removes the created MA
service *<svc-id>*	Mandatory Unique service identifier: • *svc-id: in the range of <1-4294967295>*

Command	Description
ais-lck	Enables Alarm Indication Signal (AIS) and Lock Signal (LCK) functions of Y.1731. MEPs send AIS packets during signal failure detection and LCK packets during tests.
no ais-lck	Disables AIS and LCK functions of Y.1731
ais-lck-interval {1min | 1sec}	Defines a time interval between two successively sent AIS or LCK packets: - *1min: 1 minute interval* - *1sec: 1 second interval* Default 1sec
no ais-lck-interval	Restores to default
ais-lck-level <*level*>	Defines a domain level in which AIS and LCK packets are sent. This level has to be higher than the CFM domain level: - *level: in the range of <0-7>*
no ais-lck-level	Removes the configured AIS-LCK level
ais-lck-priority <*priority*>	Defines a priority used for AIS and LCK sent packets: - *priority: in the range of <0-7>* Default 6
no ais-lck-priority	Restores to default
ccm-priority <*priority*>	Defines the VLAN priority assigned to all CCM and LTM packets, for all MEPs in a MA: - *priority: in the range of <0-7>* Default 6
no ccm-priority	Restores to default
clear-remote-mep-table *<MEP-id>*	Clears a remote MEP: - *MEP-id: in the range of <0-8191>. A value of 0: clears all remote MEPs*
fault-alarms-level *<defect-priority>*	Defines the defect priority for generating fault alarms. Defects are: loss of CCMs or a reception of cross connected CCMs: - *defect-priority: in the range of <1-6>* Default Defect priority is 1 and alarms are generated for all defect conditions

Command	Description
no fault-alarms-level	Restores to default
fng-alarm-time *<alarm-time>*	Defines the time interval that defects must be present before a local MEP generates a Fault Alarm: • *alarm-time: in the range of <250-1000> hundredths of a second* Default 250 hundredths of a second
no fng-alarm-time	Restores to default
fng-reset-time *<reset-time>*	Defines the time interval in which defects are absent before enabling a Fault Alarm again: • *reset-time: in the range of <250-1000> hundredths of a second* Default 1000 hundredths of a second
no fng-reset-time	Restores to default
hello-interval **<***index***>**	Defines the time interval between two successive CCMs sent by a MEP, member of this MA: • *index: in the range of <4-7> as follows: 1sec (4), 10sec (5), 1min (6), and 10min (7)* Default 1 second
no hello-interval	Restores to default
mep *MEP-id SAPSTRING*	Mandatory Adds a SAP port (part of the service where MA was created on) as MEP to a specific MA: • *MEP-id: in the range of <1-8191>* • *SAPSTRING: in UU/SS/PP:<vlan-id>: format* • *UU/SS/PP: the corresponding port* • *vlan-id: in the range of <1-4092>*
no mep <*MEP-id***>**	Removes the MEP from the MA
shutdown	Disables the MEP

Command	Description
no shutdown	Enables the MEP Default Enabled
direction {up | down}	Defines the direction in which the MEP faces on the bridge port: • *up, down*
ccm-enabled	Enables the MEP to generate CCM messages Default Enabled
no ccm-enabled	Restores to default
ccm-priority	Defines the VLAN priority assigned to all CCM and LTM packets, for a specified MEP: • *priority: in the range of <0-7>* Default 6
no ccm-priority	Restores to default
mip-policy {default | explicit | none}	Defines the conditions in which MIPs are automatically created on ports: • *default: always creates MIPs* • *explicit: creates MIPs only if a MEP exists on a lower MD Level* • *none: does not create any MIPs for the specified MA* Default If no MIP creation policy per MA is defined, the default policy is inherited from the domain policy configuration
no mip-policy	Restores to default

Command	Description
sender-id-content {chassis-id | chassis-manage-id | manage-id | none}	Configures the content of the Sender ID Type Length Value (TLV) included in most of the CFM packets the MEPs send: - *chassis-id: the Sender ID TLV includes only the device hostname: the local hostname is visible to all remote sites on the MA but the local management address is hidden* - *chassis-manage-id: the Sender ID TLV includes both the hostname and the management address of the device* - *manage-id: the Sender ID TLV includes only the device's management address: the local management mechanism and management address are visible to all remote sites on the MA but the local hostname is hidden* - *none: does not send the Sender ID TLV to remote MEPs: the chassis ID and management information are hidden from all remote sites* Default None
no sender-id-content	Restores to default
threshold-profile *<threshold-profile id>*	Creates a CFM profile with a specified name and enters the Monitoring Profile Configuration mode: - *threshold-profile id: in the range of <1-64>* Default When the CFM protocol is enabled, a default profile is created automatically
no threshold-profile [*threshold-profile id***]**	Restores to default
one-way-jitter-error *<error-value>*	Defines the one-way jitter error monitoring: - *error-value: in the range of <1-10000> milliseconds* Default 350 milliseconds
no one-way-jitter-error	Restores to default
one-way-jitter-warning *<warning-value>*	Defines the one-way jitter warning monitoring: - *warning-value: in the range of <1-10000>milliseconds* Default 350 milliseconds

Command	Description
no one-way-jitter-warning	Restores to default
frame-loss-error *<error-threshold>*	Defines the two-way frame-loss error monitoring threshold: • *error-threshold: in the range of <1-100> %* Default 10% frame loss
no frame-loss-error	Restores to default
frame-loss-warning *<warning -threshold>*	Defines the two-way frame-loss warning monitoring threshold: • *warning-threshold: in the range of <0-100> %. If you define a value greater than the frame-loss-error value, the frame-loss-warning is disabled* Default 8% frame loss
no frame-loss-warning	Restores to default
round-trip-jitter-error *<error-value>*	Defines the two-way jitter error monitoring: • *error-value: in the range of <1-10000> milliseconds* Default 700 milliseconds
no round-trip-jitter-error	Restores to default
round-trip-jitter-error-period *<period-value>*	Defines the two-way jitter error duration: • *period-value: in the range of <1-3600 >t seconds* Default 90 seconds
no round-trip-jitter-error-period	Restores to default
round-trip-jitter-warning *<warming-value>*	Defines the two-way jitter warning monitoring: • *warning-value: in the range of <1-10000> milliseconds* Default 600 milliseconds
no round-trip-jitter-warning	Restores to default
round-trip-jitter-warning-period *<period-value>*	Defines the two-way jitter warning duration: • *period-value: in the range of <1-3600> seconds* Default 180 seconds

Command	Description
no round-trip-jitter-warning-period	Restores to default
round-trip-latency-error *<error-value>*	Defines the two-way latency error monitoring threshold: • *error-value: in the range of <1-10000> milliseconds* Default 2000 milliseconds
no round-trip-latency-error	Restores to default
round-trip-latency-error-period *<period-value>*	Defines the latency error increase duration: • *1-3600: in the range of <1-3600> seconds* Default 90 seconds
no round-trip-latency-error-period	Restores to default
round-trip-latency-warning *<warning-value>*	Defines the two-way latency warning monitoring threshold: • *warning-value: in the range of <1-10000> milliseconds* Default 1600 milliseconds
no round-trip-latency-warning	Restores to default
round-trip-latency-warning-period *<period-value>*	Defines the latency warning increase duration: • *period-value: in the range of <1-3600> seconds* Default 180 seconds
no round-trip-latency-warning-period	Restores to default
results-bucket-size *<size>*	Defines the number of results to save for jitter calculation • *size: in the range of <2-255>* Default 20 results
no results-bucket-size	Restores to default
priority *<priority>*	Defines the 802.1p class-of-service: • *value: in the range of <0-7>* Default 0
no priority	Restores to default

Command	Description
rate *<rate>*	Defines the number of the Loopback Request packets • *rate: in the range of <1-3>* Default 1 packet
no rate	Restores to default
tlv-size *<size>*	Defines the Loopback Request packets' size, in bytes: • *size: in the range of <0-1462>* Default 0 bytes
no tlv-size	Restores to default
update-interval *<interval>*	Configures the time interval for updating the monitoring parameters (one-way jitter, two-way jitter, latency, and frame loss): • *interval: in the range of <0-65535> seconds. A value 0 suspends the monitoring task and a value different from 0 resumes it* Default 20 seconds
no update-interval	Restores to default
test *<test-id> DOMAIN-NAME MA-NAME <threshold-profile id>* **[repeat-interval** *number***]**	Tests the connectivity: • *test-id: in the range of <1-256>* • *DOMAIN-NAME: a string of <1-43> characters* • *MA-NAME: a string of <1-45> characters* • *threshold-profile id: in the range of <1-64>* • *number: the repeat interval in the range of <1-420>* Default 60
no test *<id> DOMAIN-NAME*	Restores to default
show oam cfm	Displays the current CFM configuration and CFM status
show oam cfm connectivity [domain-name *DOMAIN-NAME***] [ma** *MA-NAME***]**	Displays connectivity statistics for all configured domains: • *DOMAIN-NAME: displays a specified domain connectivity statistics* • *MA-NAME: displays a specified MA connectivity statistics*
show oam cfm connectivity [extended]	Displays information extracted from the Port ID TLV in CCMs

Command	Description
show oam cfm domain level *<level>*	Displays information for MD: • *level: in the range of <0-7>*
show oam cfm test	Displays information about performed tests
show oam cfm threshold-profile	Displays information about CFM profiles

System Log

The application software provides system log messages that are useful to the system administrator for troubleshooting problems in the network:

- The console log routes system messages to a local or remote console, or to the system memory buffer
- Message logging is configurable (for example: what severity levels and where the log is sent)

System Logs Message Format

The logging subsystem takes messages initiated by various software processes within the application software, formats the messages, and writes them to the appropriate log files. These messages come from a local facility or *module* (a hardware device, protocol, or process within the system software).

The logging subsystem:

- provides logging information for monitoring and troubleshooting
- allows configuration of the types of logging information to be captured and the destination (log file or other devices)
- includes system log messages

The system message is stored and displayed based on the following format:

```
DATE TIME SEVERITY PROCESS MESSAGE-TEXT
```

Table 2: System Message Fields

Keyword	Description
DATE and TIME	Indicates when the message is issued
SEVERITY	The literal message's severity level
PROCESS	The name of a system process that generated the message
MESSAGE-TEXT	The textual content of the message

Example

```
Jan  1 01:02:48 info      OSPF  interface 192.168.1.1 join AllSPFRouters Multicast group.
```

Settings and Values

Severity Levels

Trap level for logging should be configured per receiver (buffer, CLI console, SSH console, and Syslog server) and per severity.

By default, only Critical-level messages are stored in buffer. All lower-level trap messages are filtered out.

To change the level of the trap message logging filter, use the **`log buffer severity`** command.

Table 3: Severity Levels

Severity Level	Keyword	Description
0	*`emergency`*	Internal error occurred. The device reached a crash state and cannot continue to operate.
1	*`alert`*	Immediate action needed. The device might operate incorrectly.
2	*`critical`*	Internal error or non-supported event occurred.
3	*`error`*	Error condition (for example, error messages about software or hardware malfunctions).
4	*`warning`*	Warning condition.
5	*`notice`*	Normal but significant condition (for example, interface up/down transitions and system restart messages).
6	*`info`*	Informational message only (for example, reload requests and low-process stack messages).
7	*`debug`*	Debug level messages.

Syslog Facility

A Syslog facility is a setting for the remote Syslog server.

Table 4: Syslog Message Facilities

Keyword	Description
alert	Log alert
audit	Log audit
auth	Security/authorization messages
clock	Clock daemon
cron	Messages generated internally by Syslog
daemon	System daemons
ftp	FTP daemon
local0	Local use 0 (local0)
local1	Local use 1 (local1)
local2	Local use 2 (local5)
local3	Local use 3 (local3)
local4	Local use 4 (local4)
local5	Local use 5 (local5)
local6	Local use 6 (local6)
local7	Local use 7 (local7)
lpr	Line printer subsystem
mail	Mail system
news	Network news subsystem
ntp	NTP subsystem
security	Security/authorization messages
syslog	Messages generated internally by Syslog
user	User-level messages
uucp	UUCP subsystem

NOTE

Some operating systems use facilities `alert`**,** `audit`**, and** `auth` **for security/authorization and audit/alert messages.**

System Logs Command Hierarchy

```
+ root
        + config terminal
          - [no] log cli-console severity <severity level>
          - [no] log ssh-console severity <severity level>
          - [no] log buffer severity <severity level>
          + [no] log syslog-server A.B.C.D
                - [no] facility <facility level>
                - severity <severity level>
        - show syslog
        - show syslog displaylevel <0-64>
        - show syslog message [level <severity level> | process PROCESS |
            text NAME | timestamp NAME] [displaylevel <0-64>]
```

The System Logs Commands

Table 5: Commands for System Logs

Command	Description
`config terminal`	Enters the Configuration mode
`log cli-console severity <severity level>`	Displays system log messages on the CLI console that is attached to the COM port: • *severity level: refer to Keyword column of Table 3. Zero (0) is the highest severity, and 7 is the lowest severity. When you specify a severity level, logging output of the specified level and all lower levels (higher severities) are enabled*
`no log cli-console`	Stops the log output to the CLI console
`log ssh-console severity <severity level>`	Displays system log messages on the SSH console: • *severity level: refer to Keyword column of Table 3*
`no log ssh-console`	Stops the log output to the SSH console
`log buffer severity <severity level>`	Copies system log messages to an internal buffer: • *severity level: refer to Keyword column of Table 3* Default Syslog buffer size is 2000 messages
`no log buffer`	Restores to default
`log syslog-server A.B.C.D`	Enables remote logging using the Syslog server facility: • *A.B.C.D: the IP address of the Syslog server*
`no log syslog-server A.B.C.D [facility]`	Disables the remote logging
`facility <facility level>`	Configures the facility level: • *facility level: refer to Keyword column of Table 4*
`no facility`	Removes the configured facility level
`severity <severity level>`	Configures the severity level: • *severity level: refer to Keyword column of Table 3*
`show syslog`	Displays the logging configuration
`show syslog displaylevel <0-64>`	Displays the detailed logging level configuration: • *0-64: the display level*

Command	Description
`show syslog message [level` *`<severity level>`* **`| process`** *`PROCESS`***`| text`** *`NAME`* **`| timestamp`** *`NAME`***`] [displaylevel`** *`<0-64>`***`]`**	Displays the detailed logging message configuration: • *`severity level: refer to Keyword column of Table 3`* • *`PROCESS: the name of the process to filter on`* • *`NAME: the text name`* • *`NAME: the timestamp name`* • *`0-64: the display level`*

Appendix A: Acronyms Glossary

Acronym	Meaning
AAA	Authentication, Authorization and Accounting
ACG	Access Control Group
ACL	Access Control List
AIS	Alarm Indication Signal
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
BiST	Built-in Self Test
CCM	Continuity Check Message
CFM	Connectivity Fault Management
CLEI	Common Language Equipment Identification
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclical Redundancy Checking
CSPF	Constrained Shortest Path First
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DSCP	Differentiated Services Code Point
FEC	Forwarding Equivalent Class
FRR	Fast Reroute
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ITU-T	International Telecommunications Union-Telecommunications Standard Sector
LAG	Link Aggregation Group
LAN	Local Area Network
LBM	Loopback message
LBR	Loopback Reply
LER	Label Edge Router
LSP	Label Switched Path
LTM	Linktrace Message

Acronym	Meaning
LTR	Linktrace Reply
MA	Maintenance Association
MAC	Media Access Control
MA ID	Maintenance Association Identifier
MC ID	MST Configuration Identifier
MEF	Metro Ethernet Forum
MEP	Maintenance Association End Point
MEP ID	Maintenance association End Point Identifier
MIB	Management Information Base
MIP	Maintenance Intermediate Points
MP	Merge Point
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAS	Network Access Server
NTP	Network Time Protocol
OAM	Operations, Administration, and Maintenance
OAMPDU	OAM Protocol Data Unit
OSPF	Open Shortest Path First
PDU	Protocol Data Unit
PE	Provider Edge
PLR	Point of Local Repair
PVID	Port VLAN Identifier
PW	Pseudowire
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comments
RSVP-TE	Resource Reservation Protocol Traffic Engineering
SD	Signal Degrade
SDP	Service Distribution Path
SF	Signal Failure
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS+	Terminal Access Controller Access Control System Plus
TC	Topology Change
TCP	Transmission Control Protocol

Acronym	Meaning
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
TTL	Time-To-Live
UDP	User Datagram Protocol
VID	VLAN Identifier
VLAN	Virtual LAN
VPN	Virtual Private Network
VTY	Virtual Telnet Type
WAN	Wide Area Network
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin