SIEMENS

User Manual

SURPASS hiD 6615 S223/S323 R1.5

UMN:CLI

A50010-Y3-C150-2-7619

Important Notice on Product Safety

Elevated voltages are inevitably present at specific points in this electrical equipment. Some of the parts may also have elevated operating temperatures.

Non-observance of these conditions and the safety instructions can result in personal injury or in property damage.

Therefore, only trained and qualified personnel may install and maintain the system.

The system complies with the standard EN 60950-1 / IEC 60950-1. All equipment connected has to comply with the applicable safety standards.

The same text in German:

Wichtiger Hinweis zur Produktsicherheit

In elektrischen Anlagen stehen zwangsläufig bestimmte Teile der Geräte unter Spannung. Einige Teile können auch eine hohe Betriebstemperatur aufweisen.

Eine Nichtbeachtung dieser Situation und der Warnungshinweise kann zu Körperverletzungen und Sachschäden führen.

Deshalb wird vorausgesetzt, dass nur geschultes und qualifiziertes Personal die Anlagen installiert und wartet.

Das System entspricht den Anforderungen der EN 60950-1 / IEC 60950-1. Angeschlossene Geräte müssen die zutreffenden Sicherheitsbestimmungen erfüllen.

Trademarks:

All designations used in this document can be trademarks, the use of which by third parties for their own purposes could violate the rights of their owners.

Issued by the Communications Group
Hofmannstraße 51
D-81359 München

Reason for Update

Summary: System software upgrade added

Details:

Chapter/Section	Reason for Update
11	System software upgrade added

Issue History

Issue Number	Date of Issue	Reason for Update
01	07/2006	Initial release
02	08/2006	System software upgrade added

This document consists of a total 381 pages. All pages are issue 2.

Contents

Illustrations

Tables

1 Introduction

1.1 Audience

This manual is intended for SURPASS hiD 6615 S223/S323 single-board Fast Ethernet switch operators and maintenance personnel for providers of Ethernet services. This manual assumes that you are familiar with the following:

- Ethernet networking technology and standards
- Internet topologies and protocols
- Usage and functions of graphical user interfaces.

1.2 Document Structure

Tab. 1.1 briefly describes the structure of this document.

Chapter	Description
1 Introduction	Introduces the overall information of the document.
2 System Overview	Introduces the hiD 6615 S223/S323 system. It also lists the features of the system.
3 Command Line Interface (CLI)	Describes how to use the Command Line Interface (CLI).
4 System Connection and IP Address	Describes how to manage the system account and IP address.
5 Port Configuration	Describes how to configure the Ethernet ports.
6 System Environment	Describes how to configure the system environment and management functions.
7 Network Management	Describes how to configure the network management functions.
8 System Main Functions	Describes how to configure the system main functions.
9 IP Multicast.	Describes how to configure the IP multicast packets.
10 IP Routing Protocol.	Describes how to configure IP routing protocol.
12 Abbreviations	Lists all abbreviations and acronyms which appear in this document.

Tab. 1.1 Overview of Chapters

1.3 Document Convention

This guide uses the following conventions to convey instructions and information.

Information

This information symbol provides useful information when using commands to configure and means reader take note. Notes contain helpful suggestions or references.

Warning

This warning symbol means danger. You are in a situation that could cause bodily injury or broke the equipment. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents by making quick guide based on this guide.

1.4 Document Notation

The following table shows commands used in guide book. Please be aware of each command to use them correctly.

Notation	Description
a	Commands you should use as is.
NAME, PROFILE, VALUE, …	Variables for which you supply values.
PORTS	For entry this variable, see Section 5.1.
[ ]	Commands or variables that appear within square brackets [ ] are optional.
< >	Range of number that you can use.
{ }	A choice of required keywords appears in braces { }. You must select one.
|	Optional variables are separated by vertical bars |.

Tab. 1.2 Command Notation of Guide Book

1.5 CE Declaration of Conformity

The CE declaration of the product will be fulfilled if the construction and cabling is undertaken in accordance with the manual and the documents listed there in, e.g. mounting instructions, cable lists where necessary account should be taken of project-specific documents.

Deviations from the specifications or unstipulated changes during construction, e.g. the use of cable types with lower screening values can lead to violation of the CE requirements. In such case the conformity declaration is invalidated and the responsibility passes to those who have caused the deviations.

1.6 GPL/LGPL Warranty and Liability Exclusion

The Siemens product, SURPASS hiD 6615, contains both proprietary software and “Open Source Software”. The Open Source Software is licensed to you at no charge under the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL). This Open Source Software was written by third parties and enjoys copyright protection. You are entitled to use this Open Source Software under the conditions set out in the GPL and LGPL licenses indicated above. In the event of conflicts between Siemens license conditions and the GPL or LGPL license conditions, the GPL and LGPL conditions shall prevail with respect to the Open Source portions of the software.

The GPL can be found under the following URL:
http://www.gnu.org/copyleft/gpl.html

The LGPL can be found under the following URL:
http://www.gnu.org/copyleft/lgpl.html

In addition, if the source code to the Open Source Software has not been delivered with this product, you may obtain the source code (including the related copyright notices) by sending your request to the following e-mail address: opensrc@dasannetworks.com You will, however, be required to reimburse Siemens for its costs of postage and copying.

Any source code request made by you must be sent within 3 years of your purchase of the product. Please include a copy of your sales receipt when submitting your request. Also please include the exact name and number of the device and the version number of the installed software.

The use of Open Source Software contained in this product in any manner other than the simple running of the program occurs at your own risk, that is, without any warranty claims against Siemens. For more information about the warranties provided by the authors of the Open Source Software contained in this product, please consult the GPL and LGPL.

You have no warranty claims against Siemens when a defect in the product is or could-have been caused by changes made by you in any part of the software or its configuration. In addition, you have no warranty claims against Siemens when the Open Source Software infringes the intellectual property rights of a third party.

Siemens provides no technical support for either the software or the Open Source Software contained therein if either has been changed.

2 System Overview

SURPASS hiD 6615 L3 switch is typical Layer 3 switch intended to construct large-scale network, which provides aggregated function of upgraded LAN network consisted of typical Ethernet switch. Layer 3 switch can connect to PC, web server, LAN equip-ment, backbone equipment, or another switch through various interfaces.

SURPASS hiD 6615 L3 switch supports routing based on VLAN, IP multicasting, and provides Layer 3 switching service such as IP packet filtering or DHCP.

The Fig. 2.1 shows network construction with using hiD 6615 S223/S323.

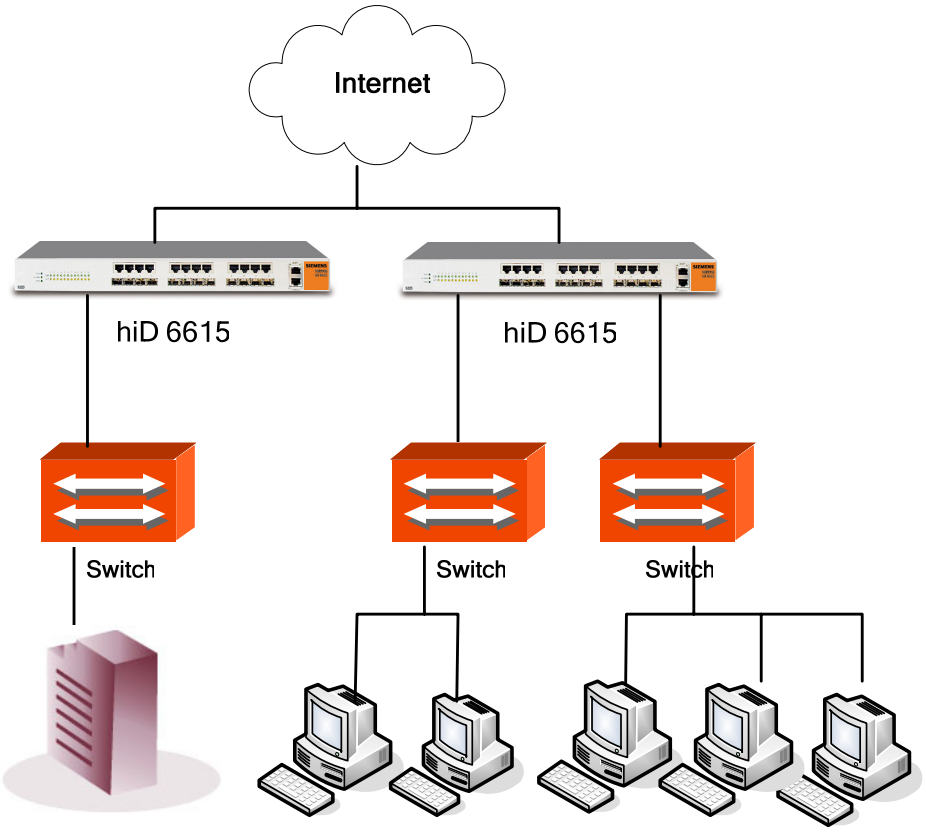


Fig. 2.1 Network Structure with hiD 6615 S223/S323

2.1 System Features

Main features of hiD 6615 S223/S323, having Fast Ethernet switch and Layer 3 switching function which supports both Ethernet switching and IP routing, are follow.

Routing functionalities such as RIP, OSPF, BGP and PIM-SM are only available for hiD 6615 S323. (Unavailable for hiD 6615 S223)

VLAN

Virtual Local Area Network (VLAN) is made by dividing one network into several logical networks. Packet can not be transmitted and received between different VLANs. Therefore it can prevent unnecessary packets accumulating and strengthen security. The hiD 6615 S223/S323 recognizes 802.1q tagged frame and supports maximum 4096 VLANs and Port based, Protocol based, MAC based VLANs.

Quality of Service (QoS)

For the hiD 6615 S223/S323, QoS-based forwarding sorts traffic into a number of classes and marks the packets accordingly. Thus, different quality of service is providing to each class, which the packets belong to. The QoS capabilities enable network managers to protect mission-critical applications and support differentiated level of bandwidth for managing traffic congestion. The hiD 6615 S223/S323 support ingress and egress (shaping) rate limiting, and different scheduling type such as SP (Strict Priority), WRR (Weighted Round Robin) and WFQ (Weighted Fair Queuing).

Multicasting

Because broadcasting in a LAN is restricted if possible, multicasting could be used instead of broadcasting by forwarding multicast packets only to the member hosts who joined multicast group. The hiD 6615 S223/S323 provides IGMP V2, IGMP snooping and PIM-SM for host membership management and multicast routing.

SNMP

Simple Network Management Protocol (SNMP) is to manage Network Elements using TCP/IP protocol. The hiD 6615 S223/S323 supports SNMP version 1, 2, 3 and Remote Monitoring (RMON). Network operator can use MIB also to monitor and manage the hiD 6615 S223/S323.

IP Routing

The hiD 6615 S323 is Layer 3 switch, which has routing table and IP address as router. Therefore, it supports static routing, RIP v1/v2, OSPF v2 and BGP v4 for unicast routing.

DHCP

The hiD 6615 S223/S323 supports DHCP (Dynamic Host Control Protocol) Server that automatically assigns IP address to clients accessed to network. That means it has IP address pool, and operator can effectively utilize limited IP source by leasing temporary IP address. In layer 3 network, DHCP request packet can be sent to DHCP server via DHCP relay and Option 82 function.

Spanning Tree Protocol (STP)

To prevent loop and preserve backup route in layer 2 network, the hiD 6615 S223/S323 supports STP (802.1D). Between STP enabled switches, a root bridge is automatically selected and the network remains in tree topology. But the recovery time in STP is very slow (about 30 seconds), RSTP (Rapid Spanning Tree Protocol) is also provided. IEEE 802.1W defines the recovery time as 2 seconds. If there is only one VLAN in the network, traditional STP works. However, in more than one VLAN network, STP cannot work per VLAN. To avoid this problem, the hiD 6615 S223/S323 supports Multiple Spanning Tree Protocol (MSTP).

Link Aggregation (Trunking)

The hiD 6615 S223/S323 aggregates several physical interfaces into one logical port (aggregate port). Port trunk aggregates interfaces with the standard of same speed, same duplex mode, and same VLAN ID. According to IEEE 802.3ad, the hiD 6615 S223/S323 can configure maximum 8 aggregate ports and up to 12 trunk groups.

LACP

The hiD 6615 S223/S323 supports Link Aggregation Control Protocol (LACP), complying with IEEE 802.3ad, which aggregates multiple links of equipments to use more enlarged bandwidth.

System Management based on CLI

It is easy for users who administer system by using telnet or console port to configure the functions for system operating through CLI. CLI is easy to configure the needed functions after looking for available commands by help menu different with UNIX.

Broadcast Storm Control

Broadcast storm control is, when too much of broadcast packets are being transmitted to network, a situation of network timeout because the packets occupy most of transmit capacity. The hiD 6615 S223/S323 supports broadcast and multicast storm control, which disuses flooding packet, that exceed the limit during the time configured by user.

RADIUS and TACACS+

hiD 6615 S223/S323 supports client authentication protocol, that is RADIUS(Remote Authentication Dial-In User Service) and TACACS+(Terminal Access Controller Access Control System Plus). Not only user IP and password registered in switch but also authentication through RADIUS server and TACACS+ server are required to access. Therefore, security of system and network management is strengthened.

3 Command Line Interface (CLI)

This chapter describes how to use the Command Line Interface (CLI) which is used to configure the hiD 6615 S223/S323 system.

- Command Mode
- Useful Tips

3.1 Command Mode

You can configure and manage the hiD 6615 S223/S323 by console terminal that is installed on user's PC. For this, use the CLI-based interface commands. Connect RJ45-to-DB9 console cable to the hiD 6615 S223/S323.

This chapter explains how CLI command mode is organized before installing. CLI command mode is consisted as follow:

- Privileged EXEC View Mode
- Privileged EXEC Enable Mode
- Global Configuration Mode
- Bridge Configuration Mode
- Rule Configuration Mode
- DHCP Configuration Mode
- DHCP Option 82 Configuration Mode
- Interface Configuration Mode
- RMON Configuration Mode
- Router Configuration Mode
- VRRP Configuration Mode
- Route-Map Configuration Mode

Fig. 3.1 shows hiD 6615 S323 software mode structure briefly.

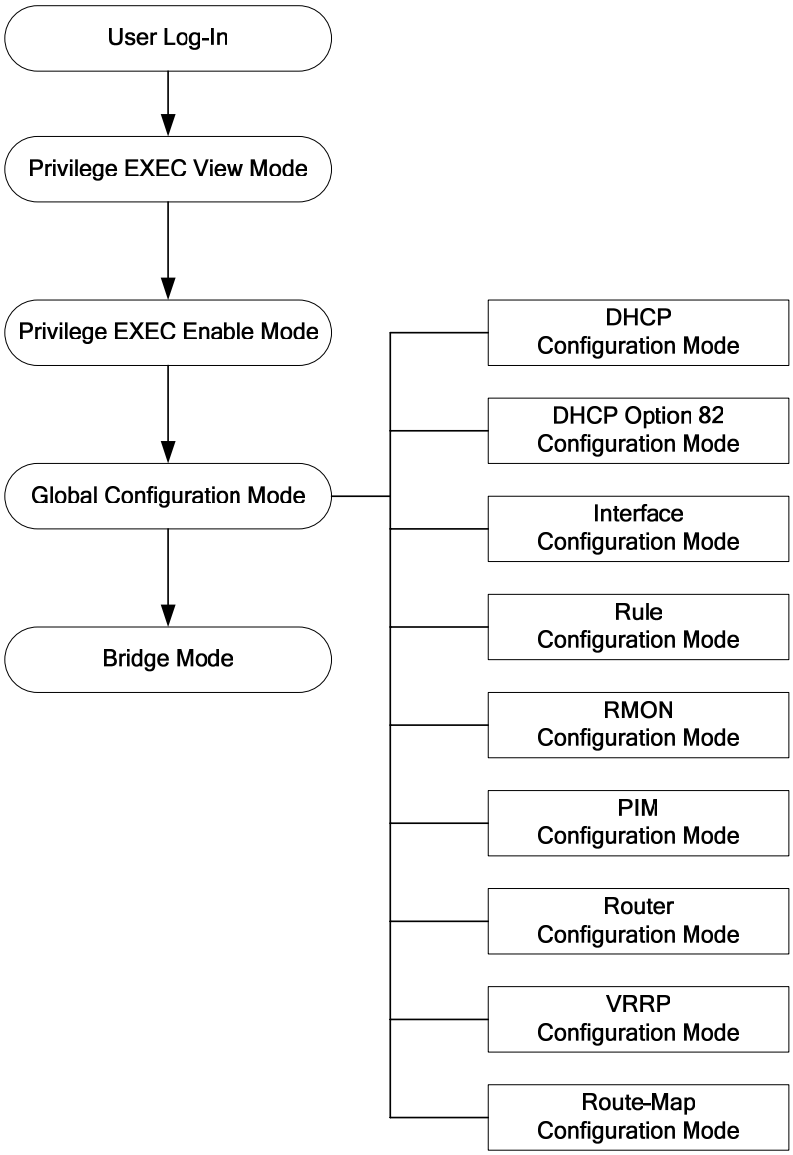


Fig. 3.1 Software mode structure

3.1.1 Privileged EXEC View Mode

When you log in to the switch, the CLI will start with *Privileged EXEC View* mode that is a read-only mode. In this mode, you can see a system configuration and information with several commands.

Tab. 3.1 shows main command of *Privileged EXEC View* mode.

Command	Description
enable	Opens *Privileged EXEC Enable* mode.
exit	Logs out the switch.
show	Shows a system configuration and information.

Tab. 3.1 Main Commands of *Privileged EXEC View* Mode

3.1.2 Privileged EXEC Enable Mode

To configure the switch, you need to open *Privileged EXEC Enable* mode with the **enable** command, then the system prompt will changes from SWITCH> to SWITCH#.

Command	Mode	Description
enable	View	Opens *Privileged EXEC Enable* mode.

You can set a password to *Privileged EXEC Enable* mode to enhance security. Once setting a password, you should enter a configured password, when you open *Privileged EXEC Enable* mode.

Tab. 3.2 shows main commands of *Privileged EXEC Enable* mode.

Command	Description
clock	Inputs time and date in system.
configure terminal	Opens Configuration mode.
telnet	Connects to another device through telnet.
terminal length	Configures the number of lines to be displayed in screen.
traceroute	Traces transmission path of packet.
where	Finds users accessed to system through telnet.

Tab. 3.2 Main Commands of *Privileged EXEC Enable* Mode

3.1.3 Global Configuration Mode

In *Global Configuration* mode, you can configure general functions of the system. You can also open another configuration mode from this mode.

To open *Global Configuration* mode, enter the **configure terminal** command, and then the system prompt will be changed from SWITCH# to SWITCH(config)#.

Command	Mode	Description
configure terminal	Enable	Opens *Global Configuration* mode from *Privileged EXEC Enable* mode.

Tab. 3.3 shows a couple of important main commands of Global Configuration mode.

Command	Description
access-list	Configures policy to limit routing information on the standard of AS.
arp	Registers IP address and MAC address in ARP table.
bgp	Helps BGP configuration.
bridge	Opens *Bridge Configuration* mode.
copy	Makes a backup file for the configuration of the switch.
dot1x	Configures various functions of 802.1x daemon.
end	Closes current mode and returns to *User EXEC* mode.
exit	Closes current mode and returns to previous mode.
hostname	Changes host name of the switch.
exec-timeout	Configures auto-logout function.
fan	Configures fan operation
interface	Opens *Interface Configuration* mode.
ip	Configures various functions of the interface.
passwd	Changes a system password.
qos	Configures QoS.
restore factory-defaults	Restores the default configuration of the switch.
rmon-alarm	Opens *Rmon-alarm* configuration mode.
rmon-event	Opens *Rmon-event* configuration mode.
rmon-history	Opens *Rmon-history* configuration mode.
route-map	Opens *Route-map Configuration* mode.
router	Opens *Router Configuration* mode.(OSPF. RIP, VRRP, PIM, BGP)
snmp	Configures SNMP.
sntp	Configures SNTP
syslog	Configures syslog.
time-zone	Configures time zone.

Tab. 3.3 Main Commands of *Global Configuration* Mode

3.1.4 Bridge Configuration Mode

In *Bridge Configuration* mode, you can configure various Layer 2 functions such as VLAN, STP, LACP, EFM OAM, etc.

To open *Bridge Configuration* mode, enter the **bridge** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(bridge)#.

Command	Mode	Description
bridge	Global	Opens *Bridge Configuration* mode.

Tab. 3.4 shows a couple of main commands of *Bridge Configuration* mode.

Command	Description
auto-reset	Configures the system for automatic rebooting
dhcp-server-filter	Configures packet filtering of DHCP server.
erp	Configures ERP function
lacp	Configures LACP function.
lldp	Configures LLDP function
mac	Manages MAC address
mac-flood-guard	Configures mac-flood-guard.
mirror	Configures mirroring function.
oam	Configures EFM-OAM protocol
port	Sets port configuration
stp	Configures Spanning Tree Protocol
trunk	Configures trunk-function.
vlan	Configures VLAN function.

Tab. 3.4 Main Commands of *Bridge Configuration* Mode

3.1.5 Rule Configuration Mode

You can open *Rule Configuration* mode using the command, **rule** *NAME* **create**, on *Global Configuration* mode.

If you open *Rule Configuration* mode, the system prompt is changed from SWITCH(config)# to SWITCH(config-rule[name])#.

Command	Mode	Description
rule *NAME* **create**	Global	Opens *Rule Configuration* mode.

On the *Rule Configuration* mode, it is possible to configure the condition and operational method for the packets to which the rule function is applied.

Tab. 3.5 shows a couple of important main commands of *Rule Configuration* mode.

Command	Description
apply	Configures rule configuration and applies it to the switch.
mac	Configures a packet condition by MAC address.
match	Configures an operational condition which meets the packet condition.
port	Configures a packet condition by port number.
priority	Configures the priority for rule.
vlan	Configures VLAN.

Tab. 3.5 Main Commands of *Rule Configuration* Mode

3.1.6 DHCP Configuration Mode

To open *DHCP Configuration* mode, use the command, **ip dhcp pool** *POOL*, on *Global Configuration* mode as follow. Then the prompt is changed from SWITCH(config)# to SWITCH(config-dhcp[POOL])#.

Command	Mode	Description
ip dhcp pool *POOL*	Global	Opens *DHCP Configuration mode* to configure DHCP.

DHCP Configuration mode is to configure range of IP address used in DHCP server, group in subnet, and default gateway of subnet.

Command	Description
default-router	Configures a default gateway of subnet.
dns-server	Configures DNS server.
range	Configures a range of IP address used in DHCP server.
subnet	Configures a subnet

Tab. 3.6 Main Commands of *DHCP Configuration* Mode

3.1.7 DHCP Option 82 Configuration Mode

To open *DHCP Option 82 Configuration* mode, use the command, **ip dhcp option82**, on *Global Configuration* mode as follow. Then the prompt is changed from SWITCH(config)# to SWITCH(config-opt82)#.

Command	Mode	Description
ip dhcp option82	Global	Opens *DHCP Option 82 Configuration* mode for DHCP option 82 configuration.

On *DHCP Option 82 Configuration* mode, configure a range of IP address used in DHCP server and designate the group in subnet and configure default gateway of the subnet. Tab. 3.7 is the main commands of *DHCP Option 82 Configuration* mode of hiD 6615 S223/S323.

Command	Description
policy	Configures a rule for option 82 packet.
remote-id	Configures a remote ID.
system-remote-id	Configures the remote ID of the system.
system-circuit-id	Configures the circuit ID of the system.

Tab. 3.7 Main Commands of *DHCP Option 82 Configuration* Mode

3.1.8 Interface Configuration Mode

To open *Interface Configuration* mode, enter the command, **interface** *INTERFACE*, on *Global Configuration* mode, and then the prompt is changed from SWITCH(config)# to SWITCH(config-if)#.

Command	Mode	Description
interface *INTERFACE*	Global	Opens *Interface Configuration* mode.

Interface Configuration mode is to assign IP address in Ethernet interface and to activate or deactivate interface.

Tab. 3.8 shows a couple of main commands of *Interface Configuration* mode.

Command	Description
bandwidth	Configures bandwidth used to make routing information.
description	Makes description of interface.
ip	Assigns IP address.
shutdown	Deactivates interface.
mtu	Sets MTU value to interface.

Tab. 3.8 Main Commands of *Interface Configuration* Mode

3.1.9 RMON Configuration Mode

To open *RMON-Alarm Configuration* mode, enter **rmon-alarm** <1-65534>. To open *RMON-Event Configuration* mode, input **rmon-event** <1-65534>. And to open *RMON-History Configuration* mode, enter **rmon-history** <1-65534>.

Tab. 3.9 shows a couple of important main commands of *RMON Configuration* mode.

Command	Description
active	Enables each RMON configuration.
community	Configures password for trap message transmission right.
description	Describes the RMON event.
falling-event	Configures to generate RMON alarm when object is less than configured threshold.
falling-threshold	Defines the falling threshold
owner	Shows the subject, which configures each RMON and uses related information.
rising-event	Configures to generate RMON alarm when object is more than configured threshold.
requested-buckets	Defines a bucket count for the interval.

Tab. 3.9 Main Commands of *RMON Configuration* Mode

3.1.10 Router Configuration Mode

To open *Router Configuration* mode, use the following command. The system prompt is changed from SWITCH(config)# to SWITCH(config-router)#.

Command	Mode	Description
router *IP-PROTOCOL*	Global	Opens *Router Configuration* mode.

Routing functionalities such as RIP, OSPF, BGP, VRRP and PIM-SM are only available for hiD 6615 S323. (Unavailable for hiD 6615 S223)

According to routing protocol way, *Router Configuration* mode is divided into BGP, RIP, and OSPF. They are used to configure each IP routing protocol.

Tab. 3.10 shows a couple of main commands of *Router Configuration* mode.

Command	Description
distance	Configures distance value to find better route.
neighbor	Configures neighbor router.
network	Configures network to operate each routing protocol.
redistribute	Registers transmitted routing information to another router's table.

Tab. 3.10 Main Commands of *Router Configuration* Mode

3.1.11 VRRP Configuration Mode

To open *VRRP Configuration* mode, use the following command. The system prompt is changed from SWITCH(config)# to SWITCH(config-router)#.

Command	Mode	Description
router vrrp *INTERFACE GROUP-ID*	Global	Opens *VRRP Configuration* mode.

Tab. 3.11 shows a couple of main commands of *Router Configuration* mode.

Command	Description
associate	Configures associated IP address same with virtual router.
authentication	Configures password of virtual router group.
preempt	Activates/deactivates preempt.
track	Configures VRRP track.
vip-access	Configures the function of accessing associated IP address.
vr-priority	Assigns priority to virtual router.
vr-timers	Configures advertisement time, which means the interval that master router distributes its information to another virtual router.

Tab. 3.11 Main Commands of *VRRP Configuration* Mode

3.1.12 Route-Map Configuration Mode

To open *Route-map Configuration* mode, use the following command. The prompt is changed from SWITCH(config)# to SWITCH(config-route-map)#.

Command	Mode	Description
route-map *NAME* {**permit** | **deny**} <1-65535>	Global	Opens *Route-map Configuration* mode.

On *Route-map Configuration* mode, you can configure the place where information is from and sent in routing table.

Tab. 3.12 shows a couple of important main commands of *Route-map Configuration* mode.

Command	Description
match	Transmits routing information to specified place.
set	Configures router address and distance.

Tab. 3.12 Main Commands of *Route-map Configuration* Mode

3.2 Useful Tips

This section provides useful functions for user's convenience while using CLI commands. They are as follow.

- Listing Available Commands
- Calling Command History
- Using Abbreviation
- Using Command of Privileged EXEC Enable Mode
- Exit Current Command Mode

3.2.1 Listing Available Commands

To list available commands, input question mark <**?**>. When you input the question mark <**?**> in each command mode, you can see available commands used in this mode and variables following after the commands.

The following is the available commands on *Privileged EXEC Enable* mode of the hiD 6615 S223/S323.

```
SWITCH# ?
Exec commands:
  clear        Reset functions
  clock        Manually set the system clock
  configure     Enter configuration mode
  copy         Copy from one file to another
  debug        Debugging functions (see also 'undebug')
  disconnect    Disconnect user connection
  enable       Turn on privileged mode command
  erase        Erase saved configuration
  exit         End current mode and down to previous mode
  halt         Halt process
  help         Description of the interactive help system
  no           Negate a command or set its defaults
  ping         Send echo messages
  quote        Execute external command
  rcommand      Management stacking node
  release      Release the acquired address of the interface
  reload       Reload the system
  renew        Re-acquire an address for the interface
  restore      Restore configurations
  show         Show running system information
  ssh          Configure secure shell
  tech-support  Technical Supporting Function for Diagnosis System
 (ommitted)
SWITCH#
```

Question mark <**?**> will not be seen in the screen and you do not need to press <**ENTER**> key to display commands list.

If you need to find out the list of available commands of the current mode in detail, use the following command.

Command	Mode	Description
show list	All	Shows available commands of the current mode.
show cli		Shows available commands of the current mode with tree structure.

The following is an example of displaying list of available commands of *Privileged EXEC Enable* mode.

```
SWITCH# show list
  clear arp
  clear arp IFNAME
  clear ip bgp *
  clear ip bgp * in
  clear ip bgp * in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) in
  clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) out
  clear ip bgp * ipv4 (unicast|multicast) soft
  clear ip bgp * ipv4 (unicast|multicast) soft in
  clear ip bgp * ipv4 (unicast|multicast) soft out
-- more –
```

i Press the <**ENTER**> key to skip to the next list.

In case of the hiD 6615 S223/S323 installed command shell, you can find out commands starting with specific alphabet. Input the first letter and question mark without space. The following is an example of finding out the commands starting "**s**" in *Privileged EXEC Enable* mode of hiD 6615 S223/S323.

```
SWITCH# s ?
  show  Show running system information
  ssh   Configure secure shell
SWITCH# s
```

Also, it is possible to view variables you should input following after commands. After inputting the command you need, make one space and input question mark. The following is an example of viewing variables after the command, **write**. Please note that you must make one space after inputting.

```
SWITCH# write ?
  memory   Write to NV memory
  terminal  Write to terminal
SWITCH# write
```

3.2.2 Calling Command History

In case of installed command shell, you do not have to enter repeated command again. When you need to call command history, use this arrow key <↑>. When you press the arrow key, the latest command you used will be displayed one by one.

The following is an example of calling command history after using several commands.

After using these commands in order: **show clock** → **configure terminal** → **interface** *1* → **exit**, press the arrow key <↑> and then you will see the commands from latest one: **exit** → **interface** *1* → **configure terminal** → **show clock**.

```
SWITCHconfig)# exit
SWITCH# show clock
Mon, 5 Jan 1970 23:50:12 GMT+0000
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# exit
SWITCH(config)# exit
SWITCH# (press the arow key ↑)
            ↓
SWITCH# exit (arrow key ↑)
            ↓
SWITCH# interface 1 (arrow key ↑)
            ↓
SWITCH# configure terminal (arrow key ↑)
            ↓
SWITCH# show clock (arrow key ↑)
```

The hiD 6615 S223/S323 also provides the command that shows the commands used before up to 100 lines.

Command	Mode	Description
show history	Enable	Shows a command history.

3.2.3 Using Abbreviation

Most of the commands can be used also with abbreviated form. The following table shows some examples of abbreviated commands.

Command	Abbreviation
clock	cl
exit	ex
show	sh
configure terminal	con te

Tab. 3.13 Command Abbreviation

3.2.4 Using Command of Privileged EXEC Enable Mode

You can execute the commands of *Privileged EXEC Enable* mode as **show**, **ping**, **telnet**, **traceroute**, and so on regardless of which mode you are located on.

To execute the commands of *Privileged EXEC Enable* mode on another mode, use the following command.

Command	Mode	Description
do *COMMAND*	All	Executes the commands of *Privileged EXEC* mode.

3.2.5 Exit Current Command Mode

To exit to the previous command mode, use the following command.

Command	Mode	Description
exit	All	Exits to the previous command mode.
end		Exits to *Privileged EXEC enable* mode.

If you use the command, **exit**, on *Privileged EXEC View* mode or *Privileged EXEC Enable* mode, you will be logged out!

4 System Connection and IP Address

4.1 System Connection

After installing switch, the hiD 6615 S223/S323 is supposed to examine that each port is rightly connected to network and management PC. And then, user connects to system to configure and manage the hiD 6615 S223/S323. This section provides instructions how to change password for system connection, connect to system through telnet as the following order.

- System Login
- Password for Privileged EXEC Mode
- Changing Login Password
- Management for System Account
- Limiting Number of User
- Telnet Access
- Auto Log-out
- System Rebooting

4.1.1 System Login

After installing the hiD 6615 S223/S323, finally make sure that each port is correctly connected to PC for network and management. And then, turn on the power and boot the system as follow.

Step 1
When you turn on the switch, booting will be automatically started and login prompt will be displayed.

```
SWITCH login:
```

Step 2
When you enter login ID at the login prompt, password prompt will be displayed. And enter password to open *Privileged EXEC View* mode. By default setting, login ID is configured as *admin* and it is possible to access without password.

```
SWITCH login: admin
Password:
SWITCH>
```

Step 3
In *Privileged EXEC View* mode, you can check only the configuration for the switch. To configure and manage the switch, you should begin *Privileged EXEC Enable* mode. The following is an example of beginning *Privileged EXEC Enable* mode.

```
SWITCH> enable
SWITCH#
```

4.1.2 Password for Privileged EXEC Mode

You can configure a password to enhance the security for *Privileged EXEC Enable* mode. To configure a password for *Privileged EXEC Enable* mode, use the following command.

Command	Mode	Description
passwd enable *PASSWORD*	Global	Configures a password to begin *Privileged EXEC Enable* mode.
passwd enable 8 *PASSWORD*		Configures an encrypted password.

password enable does not support encryption at default value. Therefore, it shows the string (or password) as it is when you use the **show running-config** command. In this case, the user's password shown to everyone and has insecure environment.

To encrypt the password which will be shown at running-config, you should use the **service password-encryption** command. And to represent the string (password) is encrypted, input **8** before the encrypted string.

When you use the **password enable** command with **8** and "the string", you will make into *Privileged EXEC Enable* mode with the encrypted string. Therefore, to log in the system, you should do it with the encrypted string as password that you configured after **8**. In short, according to using the **8** option or not, the next string is encrypted or not.

The following is an example of configure the password in *Privileged EXEC Enable* mode as *testpassword*.

```
SWITCH# configure terminal
SWITCH(config)# passwd enable testpassword
SWITCH(config)#
```

The following is an example of accessing after configuring the password.

```
SWITCH login: admin
Password:
SWITCH > enable
Password:
SWITCH#
```

To delete the configured password, use the following command.

Command	Mode	Description
no passwd enable	Global	Deletes the password.

The created password can be displayed with the command, **show running-config**. To encrypt the password not to be displayed, use the following command.

Command	Mode	Description
service password-encryption	Global	Encrypts system password.

To disable password encryption, use the following command.

Command	Mode	Description
no service password-encryption	Global	Disables password encryption.

4.1.3 Changing Login Password

To configure a password for created account, use the following command.

Command	Mode	Description
passwd [*NAME*]	Global	Configures a password for created account.

The following is an example of changing password.

```
SWITCH(config)# passwd Siemens
Changing password for Siemens
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:junior95
Re-enter new password:junior95
Password changed.
SWITCH(config)#
```

The password you are entering won't be seen in the screen, so please be careful not to make mistake.

4.1.4 Management for System Account

4.1.4.1 Creating System Account

For the hiD 6615 S223/S323, the administrator can create a system account. In addition, it is possible to set the security level from 0 to 15 to enhance the system security.

To create a system account, use the following command.

Command	Mode	Description
user add *NAME DESCRIPTION*	Global	Creates a system account.
user add *NAME* **level** <0-15> *DESCRIPTION*		Creates a system account with a security level.

The account of level 0 to level 14 without any configuring authority only can use **exit** and **help** in *Privileged EXEC View* mode and cannot access to *Privileged EXEC Enable* mode. The account with the highest level 15 has a read-write authority.

To delete the created account, use the following command.

Command	Mode	Description
user del *NAME*	Global	Delete the created account.

To display the created account, use the following command.

Command	Mode	Description
show user	Enable/Global	Shows the created account.

4.1.4.2 Configuring Security Level

For the hiD 6615 S223/S323, it is possible to configure the security level from 0 to 15 for a system account. The level 15, as the highest level, has a read-write authority. The administrator can configure from level 0 to level 14. The administrator decides which level user uses which commands in which level. As the basic right from level 0 to level 14, it is possible to use **exit** and **help** command in *Privileged EXEC Enable* mode and it is not possible to access to *Privileged EXEC Enable* mode.

To define the security level and its authority, use the following command.

Command	Mode	Description
privilege bgp level <0-15> {*COMMAND* | **all**}	Global	Uses the specific command of *BGP Configuration* mode in the level.
privilege bridge level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Bridge Configuration* mode in the level.
privilege configure level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Global Configuration* mode in the level.
privilege dhcp-option82 level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Option 82 Configuration* mode in the level.
privilege dhcp-pool level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Configuration* mode in the level.
privilege dhcp-class level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Option 82 Configuration* mode in the level.
privilege dhcp-pool-class level <0-15> {*COMMAND* | **all**}		Uses the specific command of *DHCP Configuration* mode in the level.
privilege enable level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Privileged EXEC* mode in the level.
privilege interface level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Interface Configuration* mode in the level.
privilege ospf level <0-15> {*COMMAND* | **all**}		Uses the specific command of *OSPF Configuration* mode in the level.
privilege pim level <0-15> {*COMMAND* | **all**}		Uses the specific command of *PIM Configuration* mode in the level.
privilege rip level <0-15> {*COMMAND* | **all**}		Uses the specific command of *RIP Configuration* mode in the level.

Command	Mode	Description
privilege rmon-alarm level <0-15> {*COMMAND* | **all**}	Global	Uses the specific command of *RMON Configuration* mode in the level.
privilege rmon-event level <0-15> {*COMMAND* | **all**}		
privilege rmon-history level <0-15> {*COMMAND* | **all**}		Uses the specific command of *RMON Configuration* mode in the level.
privilege route-map level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Route-map Configuration* mode in the level.
privilege rule level <0-15> {*COMMAND* | **all**}		Uses the specific command of *Rule Configuration* mode in the level.
privilege view level <0-15> {*COMMAND* | **all**}		Uses the specific command of *User EXEC* mode in the level.
privilege vrrp level <0-15> {*COMMAND* | **all**}		Uses the specific command of *VRRP Configuration* mode in the level.

The commands that are used in low level can be also used in the higher level. For example, the command in level 0 can be used in from level 0 to level 14.

The commands should be input same as the displayed commands by **show list**. Therefore, it is not possible to input the commands in the bracket separately.

```
SWITCH# show list
  clear arp-inspection mapping counter
  clear arp-inspection statistics
  clear cpu statistics (PORTS|)
  clear ip bgp *
  clear ip bgp * in
  clear ip bgp * in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) in
  clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
  clear ip bgp * ipv4 (unicast|multicast) out
  clear ip bgp * ipv4 (unicast|multicast) soft
  clear ip bgp * ipv4 (unicast|multicast) soft in
  clear ip bgp * ipv4 (unicast|multicast) soft out
  clear ip bgp * out
  clear ip bgp * soft
  clear ip bgp * soft in
  clear ip bgp * soft out
  clear ip bgp * vpnv4 unicast in
  clear ip bgp * vpnv4 unicast out
--More--
(Omitted)
```

It is not possible to input **clear ip bgp * ipv4 unicast in**. You should input like **clear ip bgp * ipv4** {**unicast** | **multicast**} **in**.

The commands starting with the same character are applied by inputting only the starting commands. For example, if you input **show**, all the commands starting with **show** are applied.

To delete a configured security level, use the following command.

Command	Mode	Description
no privilege	Global	Deletes all configured security levels.
no privilege bgp level <0-15> {*COMMAND* | **all**}		Delete a configured security level on each mode.
no privilege bridge level <0-15> {*COMMAND* | **all**}		
no privilege configure level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-option82 level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-pool level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-class level <0-15> {*COMMAND* | **all**}		
no privilege dhcp-pool-class level <0-15> {*COMMAND* | **all**}		
no privilege enable level <0-15> {*COMMAND* | **all**}		
no privilege interface level <0-15> {*COMMAND* | **all**}		
no privilege ospf level <0-15> {*COMMAND* | **all**}		
no privilege pim level <0-15> {*COMMAND* | **all**}		
no privilege rip level <0-15> {*COMMAND* | **all**}		
no privilege rmon-alarm level <0-15> {*COMMAND* | **all**}		
no privilege rmon-event level <0-15> {*COMMAND* | **all**}		
no privilege rmon-history level <0-15> {*COMMAND* | **all**}		
no privilege route-map level <0-15> {*COMMAND* | **all**}		
no privilege rule level <0-15> {*COMMAND* | **all**}		
no privilege view level <0-15> {*COMMAND* | **all**}		
no privilege vrrp level <0-15> {*COMMAND* | **all**}		

To display a configured security level, use the following command.

Command	Mode	Description
show privilege	View Enable Global	Shows a configured security level.
show privilege now		Shows a security level of current mode.

The following is an example of creating the system account *test0* having a security level 10 and *test1* having a security level 1 without password.

```
SWITCH(config)# user add test0 level 0 level0user
Changing password for test0
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:(Enter)
Bad password: too short.
Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# user add test1 level 1 level1user
Changing password for test1
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: (Enter)
Bad password: too short.
Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# show user
=================================================
 User name            Description       Level
=================================================
test0                level0user          0
test1                level1user          1
SWITCH(config)#
```

The following is an example of configuring an authority of the security level 0 and 1.

```
SWITCH(config)# privilege view level 0 enable
SWITCH(config)# privilege enable level 0 show
SWITCH(config)# privilege enable level 1 configure terminal
SWITCH(config)# show privilege

 Command Privilege Level Configuration
 ----------------------------------------------
 Node         All   Level   Command
 EXEC(ENABLE)         1     configure terminal
 EXEC(VIEW)           0     enable
 EXEC(ENABLE)         0     show
 3 entry(s) found.
SWITCH(config)#
```

In the above configuration, as level 0, it is possible to use only show command in *Privi-*

leged EXEC Enable mode; however as level 1, it is possible to use not only the commands in level 1 but also time configuration commands in *Privileged EXEC Enable* mode and accessing commands to *Global Configuration* mode.

4.1.5 Limiting Number of User

For hiD 6615 S223/S323, you can limit the number of user accessing the switch through both console port and telnet. In case of using the system authentication with RADIUS or TACACS+, the configured number includes the number of user accessing the switch via the authentication server.

To set the number of user accessing the switch, use the following command.

Command	Mode	Description
login connect <1-8>	Global	Sets the number of user accessing the switch. Default: 8

4.1.6 Telnet Access

To connect to the host through telnet at remote place, use the following command.

Command	Mode	Description
telnet *DESTINATION* [*TCP-PORT*]	Enable	Connects to a remote host. DESTINATION: IP address or host name

In case of telnet connection, you should wait for **[OK]** message, when you save a system configuration. Otherwise, all changes will be deleted when the telnet session is disconnected.

```
SWITCH# write memory
[OK]
SWITCH#
```

The system administrator can disconnect users connected from remote place. To disconnect a user connected through telnet, use the following command.

Command	Mode	Description
disconnect *TTY-NUMBER*	Enable	Disconnects a user connected through telnet.

The following is an example of disconnecting a user connected from a remote place.

```
SWITCH# where
admin at from console for 4 days 22 hours 15 minutes 24.88 seconds
admin at ttyp0 from 10.0.1.4:1670 for 4 days 17 hours 53 minutes 28.76 seconds
admin at ttyp1 from 147.54.140.133:49538 for 6 minutes 34.12 seconds
SWITCH# disconnect ttyp0
SWITCH# where
admin at from console for 4 days 22 hours 15 minutes 34.88 seconds
admin at ttyp1 from 147.54.140.133:49538 for 6 minutes 44.12 seconds
SWITCH#
```

4.1.7 Auto Log-out

For security reasons of the hiD 6615 S223/S323, if no command is entered within the configured inactivity time, the user is automatically logged out of the system. Administrator can configure the inactivity timer.

To enable auto-logout function, use the following command.

Command	Mode	Description
exec-timeout <1-35791> [<0-59>]	Global	Enables auto log-out. 1-35791: time unit in minutes (by default 10 minutes) 0-59: time unit in seconds
exec-timeout 0		Disables auto log-out.

To display a configuration of auto-logout function, use the following command.

Command	Mode	Description
show exec-timeout	Enable Global	Shows a configuration of auto-logout function.

The following is an example of configuring auto-logout function as 60 seconds and viewing the configuration.

```
SWITCH(config)# exec-timeout 60
SWITCH(config)# show exec-timeout
Log-out time : 60 seconds
SWITCH(config)#
```

4.1.8 System Rebooting

4.1.8.1 Manual System Rebooting

When installing or maintaining the system, some tasks require rebooting the system by various reasons. Then you can reboot the system with a selected system OS.

To restart the system manually, use the following command.

Command	Mode	Description
reload [**os1** | **os2**]	Enable	Restarts the system.

If you reboot the system without saving new configuration, new configuration will be deleted. So, you have to save the configuration before rebooting. Not to make that mistake, hiD 6615 S223/S323 is supported to print the following message to ask if user really wants to reboot and save configuration.

If you want to continue to reboot, press **<y>** key, if you want to save new configuration, press **<n>** key.

```
SWITCH# reload
Do you want to save the system configuration? [y/n]]
```

4.1.8.2 Auto System Rebooting

The hiD 6615 S223/S323 reboots the system according to user's configuration. There are two basises for system rebooting. These are CPU and memory. CPU is rebooted in case CPU Load or Interrupt Load continues for the configured time. Memory is automatically rebooted in case memory low occurs as the configured times.

To enable auto system rebooting function, use the following command.

Command	Mode	Description
auto-reset cpu <50-100> <1-100> *TIME*	Bridge	Configure to reboot the system automatically in case an average of CPU or interrupt load exceeds the configured value during the user-defined time. 50-100: average of CPU load per 1 minute 1-100: average of interrupt load TIME: minute
auto-reset memory <1-120> <1-10>		Configure to reboot the system automatically in case memory low occurs as the configured value. 1-120: time of memory low 1-10: count of memory low(The default is 5)
no auto-reset {**cpu** | **memory**}		Disables auto system rebooting.

To show auto system rebooting configuration, use the following command.

Command	Mode	Description
show auto-reset {**cpu** | **memory**}	Global/ Bridge	Shows a configuration of auto-rebooting function.

The following is an example of configuring auto-restarting function in case CPU load or Interrupt load maintains over 70% during 60 seconds and viewing the configuration.

```
SWITCH(config)# SWITCH(bridge)# auto-reset cpu 70 70 1
SWITCH(bridge)# show auto-reset cpu
------------------------------
 Auto-Reset Configuration(CPU)
------------------------------
auto-reset:         on
cpu load:           70
interrupt load:     70
continuation time:   1
SWITCH(bridge)#
```

4.2 System Authentication

For the enhanced system security, the hiD 6615 S223/S323 provides two authentication methods to access the switch using Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).

4.2.1 Authentication Method

To set the system authentication method, use the following command.

Command	Mode	Description
login {**local** | **remote**} {**radius** | **tacacs** | **host** | **all**} **enable**	Global	Set the system authentication method. local: authentication for console access remote: authentication for telnet access radius: selects RADIUS authentication. tacacs: selects TACACS+ authentication. host: selects nominal system authentication (default). all: selects all the authentication methods.
login {**local** | **remote**} {**radius** | **tacacs** | **host** | **all**} **disable**		Disables a configured system authentication method.

4.2.2 Authentication Interface

If more than 2 interfaces are specified to the hiD 6615 S223/S323, you can designate one specific interface to access RADIUS or TACACS server.

To designate an authentication interface, use the following command.

Command	Mode	Description
login {**radius** | **tacacs**} **interface** *INTERFACE* [*A.B.C.D*]	Global	Designates an authentication interface. radius: selects RADIUS authentication. tacacs: selects TACACS+ authentication. INTERFACE: interface name A.B.C.D: IP address (optional)

4.2.3 Primary Authentication Method

You can set the order of the authentication method with giving the priority to each authentication method. To set the primary authentication method, use the following command

Command	Mode	Description
login {**local** | **remote**} {**radius** | **tacacs** | **host**} **primary**	Global	Set the primary authentication method. local: authentication for console access remote: authentication for telnet access radius: selects RADIUS authentication. tacacs: selects TACACS+ authentication. host: selects nominal system authentication (default).

4.2.4 RADIUS Server

4.2.4.1 RADIUS Server for System Authentication

To add/delete the RADIUS server for system authentication, use the following command.

Command	Mode	Description
login radius server *A.B.C.D KEY*	Global	Adds the RADIUS server with its information. A.B.C.D: RADIUS server address KEY: authentication key value
login radius server *A.B.C.D KEY* **auth_port** *PORT* **acct_port** *PORT*		Adds the RADIUS server with its information. A.B.C.D: RADIUS server address KEY: authentication key value auth_port: Enters authentication port number(optional) acct_port: Enters accounting port number(optional)
no login radius server *A.B.C.D*		Deletes an added RADIUS server.

i You can add up to 5 RADIUS servers.

4.2.4.2 RADIUS Server Priority

To specify the priority of a registered RADIUS server, use the following command.

Command	Mode	Description
login radius server move *A.B.C.D* <1-5>	Global	Specifies the priority of RADIUS server. A.B.C.D: IP address 1-5: priority of RADIUS server

4.2.4.3 Timeout of Authentication Request

After the authentication request, the hiD 6615 S223/S323 waits for the response from the RADIUS server for specified time.

To specify a timeout value, use the following command.

Command	Mode	Description
login radius timeout <1-100>	Global	Specifies a timeout value. 1-100: waiting-time for the response (default: 3)

4.2.4.4 Frequency of Retransmit

If there is no response from RADIUS server, the hiD 6615 S223/S323 is supposed to retransmit an authentication request. To set the frequency of retransmitting an authentication request, use the following command.

Command	Mode	Description
login radius retransmit <1-10>	Global	Sets the frequency of retransmit. 1-10: Enters the times of retry (default: 3)

4.2.5 TACACS Server

4.2.5.1 TACACS Server for System Authentication

To add/delete the TACACS server for system authentication, use the following command.

Command	Mode	Description
login tacacs server *A.B.C.D KEY*	Global	Adds the TACACS server with its information. A.B.C.D: IP address KEY: authentication key value
no login tacacs server *A.B.C.D*		Deletes an added TACACS server. A.B.C.D: IP address

i You can add up to 5 TACACS servers.

After adding the TACACS server, you should register interface of TACACS server connected to user's switch. Use the following command.

Command	Mode	Description
login tacacs interface *NAME A.B.C.D*	Global	Registers interface of TACACS server connected to user's switch.
no login tacacs interface		Clears TACACS server interface

4.2.5.2 TACACS Server Priority

To specify the priority of a registered TACACS server, use the following command.

Command	Mode	Description
login tacacs server move *A.B.C.D* <1-5>	Global	Specifies the priority of RADIUS server. A.B.C.D: TACACS server address 1-5: the priority of TACACS server

4.2.5.3 Timeout of Authentication Request

After the authentication request, the hiD 6615 S223/S323 waits for the response from the TACACS server for specified time.

To specify a timeout value, use the following command.

Command	Mode	Description
login tacacs timeout <1-100>	Global	Specifies a timeout value. 1-100: waiting-time for the response (default: 3)

4.2.5.4 Additional TACACS+ Configuration

The hiD 6615 S223/S323 provides several additional options to configure the system authentication via TACACS server.

TCP Port for the Authentication

To specify TCP port for the system authentication, use the following command.

Command	Mode	Description
login tacacs socket-port <1-65535>	Global	Specifies TCP port for the authentication. 1-65535: TCP port
no login tacacs socket-port		Deleted the configured TCP port for the authentication

Authentication Type

To select the authentication type for TACACS+, use the following command.

Command	Mode	Description
login tacacs auth-type {**ascii** | **pap** | **chap**}	Global	Selects the authentication type for TACACS+. ascii: plain text pap: password authentication protocol chap: challenge handshake authentication protocol
no login tacacs auth-type		Deletes a specified authentication type.

Priority Level

You can define a priority level of user. According to the defined priority level, the user has different authorization to access the DSLAM. This priority must define in the TACACS server in the same way.

To define the priority level of user, use the following command.

Command	Mode	Description
login tacacs priority-level {**min** | **user** | **max** | **root**}	Global	Defines the priority level of user, refer the below information for the order of priority.
no login tacacs priority-level		Deletes a defined priority level.

i The order of priority is **root** = **max** > **user** > **min**.

4.2.6 Accounting Mode

The hiD 6615 S223/S323 provides the accounting function of AAA (Authentication, Authorization, and Accounting). Accounting is the process of measuring the resources a user has consumed. Typically, accounting measures the amount of system time a user has used or the amount of data a user has sent and received.

To set an accounting mode, use the following command.

Command	Mode	Description
login accounting-mode {**none** | **start** | **stop** | **both**}	Global	Sets an accounting mode. none: disables an accounting function. start: measures start point only. stop: measures stop point only. both: measures start and stop point both.

4.2.7 Displaying System Authentication

To display a configured system authentication, use the following command.

Command	Mode	Description
show login	Enable Global	Shows a configured system authentication.

4.2.8 Sample Configuration

[Sample Configuration 1] Configuration RADIUS server

The following is an example of configuring authorization method in SURPASS hiD 6615. It is configured to add RADIUS to default method in case of clients connecting through console and telnet. And, the priority is given to RADIUS in case of clients connecting through console and to default method in case of clients connecting through telnet.

Then, show the configuration. And The following is an example of configuring frequency of retransmit and timeout of response after registering RADIUS server.

```
SWITCH(config)# user add user test1
Changing password for user
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:vertex
Re-enter new password:vertex
Password changed.
SWITCH(config)# login local radius enable
SWITCH(config)# login remote radius enable
SWITCH(config)# login local radius primary
SWITCH(config)# login remote host primary
SWITCH(config)# login radius server add 100.1.1.1 1
SWITCH(config)# login radius retransmit 5
SWITCH(config)# login radius timeout 10
SWITCH(config)# show login
[AUTHEN]
Local login  : radius host
Remote login : host radius
Accounting mode : both
-----------------------------------
[HOST]
maximum_login_counts : 8

-----------------------------------
[RADIUS]
<Radius Servers & Key>
100.1.1.1 1
Radius Retries : 5
Radius Timeout : 10
Radius Interface : default
-----------------------------------
[TACACS]
<Tacacs Servers & Key>
Tacacs Timeout : 3
Tacacs Socket Port : 49
Tacacs Interface : default
Tacacs PPP Id : 1
Tacacs Authen Type : ASCII
Tacacs Priority Level : MIN
SWITCH(config)#
```

Displayed according to priority.

[Sample Configuration 2] Configuration TACACS+ server

The following is an example of configuring authorization method as TACACS+.

```
SWITCH(config)# user add user test1
Changing password for user
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:vertex
Re-enter new password:vertex
Password changed.
SWITCH(config)# login local tacacs enable
SWITCH(config)# login remote tacacs enable
SWITCH(config)# login local tacacs primary
SWITCH(config)# login remote tacacs primary
SWITCH(config)# login tacacs server add 200.1.1.1 1
SWITCH(config)# login tacacs interface default
SWITCH(config)# login tacacs socket-port 1
SWITCH(config)# login tacacs auth-type pap
SWITCH(config)# login tacacs timeout 10
SWITCH(config)# login tacacs priority-level root
SWITCH(config)# show login
[AUTHEN]
Local login  : tacacs host
Remote login : tacacs host
Accounting mode : both
-----------------------------------
[HOST]
maximum_login_counts : 8
-----------------------------------
[RADIUS]
<Radius Servers & Key>
Radius Retries : 3
Radius Timeout : 3
Radius Interface : default
-----------------------------------
[TACACS]
<Tacacs Servers & Key>
200.1.1.1 1
Tacacs Timeout : 10
Tacacs Socket Port : 1
Tacacs Interface : default
Tacacs PPP Id : 1
Tacacs Authen Type : PAP
Tacacs Priority Level : MAX(ROOT)
SWITCH(config)#
```

Displayed according to the priority

4.3 Assigning IP Address

The switch uses only the data's MAC address to determine where traffic needs to come from and which ports should receive the data. Switches do not need IP addresses to transmit packets. However, if you want to access to the hiD 6615 S223/S323 from remote

place with TCP/IP through SNMP or telnet, it requires IP address.

You can enable interface to communicate with switch interface on network and assign IP address as the following:

- Enabling Interface
- Disabling Interface
- Assigning IP Address to Network Interface
- Static Route and Default Gateway
- Displaying Forwarding Information Base(FIB) Table
- Forwarding Information Base(FIB) Retain
- Displaying Interface
- Sample Configuration

4.3.1 Enabling Interface

To assign an IP address to an interface, you need to enable the interface first. If the interface is not enabled, you cannot access it from a remote place, even though an IP address has been assigned.

To display if interface is enabled, use the command, **show running-config**.

Interface Configuration Mode

To open *Interface Configuration* mode of the interface you are about to enable interface, use the following command.

Command	Mode	Description
interface *INTERFACE*	Global	Opens *Interface Configuration* mode of the interface.

To enable the interface, use the following command.

Command	Mode	Description
no shutdown	Interface	Enables the interface on *Interface Configuration* mode.

The following is an example of enabling interface on *Interface Configuration* mode.

```
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# no shutdown
SWITCH(config-if)#
```

4.3.2 Disabling Interface

To disable the interface, use the following commands on *Interface Configuration* mode. Before disabling interface on *Interface Configuration* mode, you should open the mode, and then use the follow command.

Command	Mode	Description
shutdown	Interface	Disables an interface on *Interface Configuration* mode.

4.3.3 Assigning IP Address to Network Interface

After enabling interface, you need to assign IP address. To assign IP address to specified network interface, use the following command.

Command	Mode	Description
ip address *IP-ADDRESS/M*	Interface	Assigns IP address to an interface.
ip address *IP-ADDRESS/M* **secondary**		Assigns secondary IP address to an interface.

To disable the assigned IP address, use the following command.

Command	Mode	Description
no ip address *IP-ADDRESS/M*	Interface	Removes assigned IP address to an interface.
no ip address *IP-ADDRESS/M* **secondary**		Removes assigned secondary IP address to an interface.

To display an assigned IP address, use the following command.

Command	Mode	Description
show ip	Interface	Shows an assigned IP address of the interface.

4.3.4 Static Route and Default Gateway

It is possible to configure the static route. Static route is a route which user configures manually. Packets are transmitted to the destination through static route. Static route includes destination address, neighbor router to receive packet, the number of routes that packets have to go through.

To configure static route, use the following command.

Command	Mode	Description
ip route *A.B.C.D SUBNET-MASK* {*GATEWAY* | **null**} [<1-255>]	Global	Configures static route. A.B.C.D: destination IP prefix GATEWAY: Ip gateway address 1-255: Distance value
ip route *A.B.C.D/M* { *SUBNET-MASK* | **null**} [<1-255> | **src** *IP-ADDRESS*]		
no ip route *A.B.C.D SUBNET-MASK* { *GATEWAY* | **null**} [<1-255>]		Deletes configured static route.
no ip route *IP-ADDRESS/M* { *SUBNET-MASK* | **null**} [<1-255>]		

To configure default gateway, use the following command on *Global Configuration* mode.

Command	Mode	Description
ip route default { *GATEWAY* | **null**} [<1-255>]	Global	Configures default gateway. GATEWAY: Ip gateway address
no ip route default { *GATEWAY* | **null**} [<1-255>]		Deletes default gateway.

The following is an example of configuring static route to reach three destinations, which are not directly connected.

```
SWITCH(config)# ip route 100.1.1.0/24 10.1.1.2
SWITCH(config)# ip route 200.1.1.0/24 20.1.1.2
SWITCH(config)# ip route 172.16.1.0/24 30.1.1.2
```

To display configured static route, use the following command.

Command	Mode	Description
show ip route {*A.B.C.D* | *A.B.C.D/M* | **bgp** | **connected** | **isis** | **kernel** | **ospf** | **rip** | **static** | **summary** | **static**}	Enable Global	Shows configured routing information.
show ip route database static		Shows configured routing information with IP routing table database.

4.3.5 Displaying Forwarding Information Base(FIB) Table

The FIB is a table that contains a mirror image of the forwarding information in the IP routing table. When routing or topology changes occur in the network the route processor updates the IP routing table and CEF updates the FIB. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths, such as fast switching and optimum switching. FIB is used for making IP destination prefix-based switching decisions and maintaining next-hop address information based on the information in the IP routing table.

The forwarding information base (FIB) table contains information that the forwarding processors require to make IP forwarding decisions.

To display Forwarding Information Base table, use the following command.

Command	Mode	Description
show ip route fib	Enable Global Bridge	Displays Forwarding Information Base table.

4.3.6 Forwarding Information Base(FIB) Retain

Use this command to modify the retain time for stale routes in the Forwarding Information Base (FIB) during NSM restart.

Command	Mode	Description
fib retain {**forever | time** <1-65535>}	Global	Configures the retain time for FIB during NSM restart Default: 60sec
no fib retain {**forever | time** <1-65535>}		Restores is as a default

4.3.7 Displaying Interface

To display interface status and configuration, use the following command.

Command	Mode	Description
show interface [*INTERFACE*]	Enable Global Interface	Shows interface status and configuration. INTERFACE: interface name
show ip interface [*INTERFACE*] **brief**	Enable Global	Shows brief information of interface. INTERFACE: interface name

4.3.8 Sample Configuration

[Sample Configuration 1]

The followings are examples of enabling interface 1 in two ways.

① On Configuration Mode

```
SWITCH# configure terminal
SWITCH(config)# interface noshutdown 1
SWITCH(config)#
```

② On Interface Configuration Mode

```
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# no shutdown
SWITCH(config-if)#
```

[Sample Configuration 2]

The following is an example of assigning IP address 192.168.1.10 to 1.

```
SWITCH(config-if)# ip address 192.168.1.10/16
SWITCH(config-if)# show ip
IP-Address        Scope   Status
-------------------------------------
192.168.1.10/16    global
SWITCH(config-if)#
```

[Sample Configuration 3]

The following is an example of configuring default gateway.

```
SWITCH# configure terminal
SWITCH(config)# ip route default 192.168.1.254
SWITCH(config)#
```

4.4 SSH (Secure Shell)

Network security is getting more important according to using network has been generalized between users. However, typical FTP and telnet service has weakness for security. SSH (Secure Shell) is security shell for login. Through SSH, all data are encoded, traffic is compressed. So, transmit rate becomes faster, and tunnel for existing ftp and pop, which are not safe in security, is supported.

4.4.1 SSH Server

The hiD 6615 S223/S323 can be operated as SSH server. You can configure the switch as SSH server with the following procedure.

- Enabling SSH Server
- Displaying On-line SSH Client
- Disconnecting SSH Client
- Displaying Connection History of SSH Client
- Assigning Specific Authentication Key

4.4.1.1 Enabling SSH Server

To enable/disable SSH server, use the following command.

Command	Mode	Description
ssh server enable	Global	Enables SSH server.
ssh server disable		Disables SSH server.

4.4.1.2 Displaying On-line SSH Client

To display SSH clients connected to SSH server, use the following command.

Command	Mode	Description
show ssh	Enable/Global	Shows SSH clients connected to SSH server.

4.4.1.3 Disconnecting SSH Client

To disconnect an SSH client connected to SSH server, use the following command.

Command	Mode	Description
ssh disconnect *PID*	Global	Disconnects SSH clients connected to SSH server. PID: SSH client number

4.4.1.4 Displaying Connection History of SSH Client

To display the connection history of SSH client, use the following command.

Command	Mode	Description
show ssh history	Enable Global	Shows the connection history of SSH clients who are connected to SSH server up to now.

4.4.1.5 Assigning Specific Authentication Key

After enabling ssh server, each client will upload generated key. The ssh server can assign specific key among the uploaded keys from several clients.

To verify Authentication Key, use the following command.

Command	Mode	Description
ssh key verify *FILENAME*	Global	Verifys generated ssh key.

i If the ssh server verify the key for specific client, other clients must download the key file from ssh server to login.

4.4.2 SSH Client

The hiD 6615 S223/S323 can be used as SSH client with the following procedure.

- Login to SSH Server
- File Copy
- Configuring Authentication Key

4.4.2.1 Login to SSH Server

To login to SSH server after configuring the hiD 6615 S223/S323 as SSH client, use the following command.

Command	Mode	Description
ssh login *DESTINATION* [*PUBLIC_KEY*]	Enable	Logins to SSH server. DESTINATION: IP address of SSH server or hostname and account PUBLIC_KEY: Specify public key.

4.4.2.2 File Copy

To copy a file from/to SSH server, use the following command.

Command	Mode	Description
copy {**scp** | **sftp**} **config** {**download** | **upload**} *CONFIG-FILE*	Enable Global	Downloads or uploads a file to through SSH server.

4.4.2.3 Configuring Authentication Key

SSH client can access to server through authentication key after configuring authentication key and informing it to server. It is safer to use authentication key than inputting password every time for login, and it is also possible to connect to several SSH servers with using one authentication key.

To configure authentication key in the hiD 6615 S223/S323, use the following command.

Command	Mode	Description
ssh keygen {**rsa1** | **rsa** | **dsa**}	Global	Configures authentication key. rsa1: SSH ver. 1 public key for the authentication rsa: SSH ver. 2 public key for the authentication dsa: SSH ver. 2 public key for the authentication

To configure authentication key and connect to SSH server with the authentication key, perform the following procedure.

Step 1
Configure the authentication key in the switch.

```
SWITCH_A(config)# ssh keygen dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/etc/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):networks
Enter same passphrase again:networks
Your identification has been saved in /etc/.ssh/id_dsa.
Your public key has been saved in /etc/.ssh/id_dsa.pub.
The key fingerprint is:
d9:26:8e:3d:fa:06:31:95:f8:fe:f6:59:24:42:47:7e root@hiD6615
SWITCH_A(config)#
```

Step 2
Connect to SSH server with the authentication key.

```
SWITCH_A# ssh login 172.16.209.10
Enter passphrase for key '/etc/.ssh/id_dsa': networks
SWITCH_B#
```

To display the configured authentication keys in the hiD 6615 S324, use the following command.

Command	Mode	Description
show key-list	Enable Global	Shows an authentication key of SSH server.

4.5 802.1x Authentication

To enhance security and portability of network management, there are two ways of authentication based on MAC address and port-based authentication which restrict clients attempting to access to port. The port-based authentication (802.1x) decides to give access to RADIUS server having the information about user who tries to access.

802.1x authentication adopts EAP (Extensible Authentication Protocol) structure. In EAP system, there are EAP-MD5 (Message Digest 5), EAP-TLS (Transport Level Security), EAP-SRP (Secure Remote Password), EAP-TTLS(Tunneled TLS) and the hiD 6615 S223/S323 supports EAP-MD5 and EAP-TLS. Accessing with user's ID and password, EAP-MD5 is one-way Authentication based on the password. EAP-TLS accesses through the mutual authentication system of server authentication and personal authentication and it is possible to guarantee high security because of mutual authentication system.

At a request of user Authentication, from user's PC EAPOL-Start type of packets are transmitted to authenticator and authenticator again requests identification. After getting respond about identification, request to approve access to RADIUS server and be authenticated by checking access through user's information.

The following figure explains the process of 802.1x authentication.

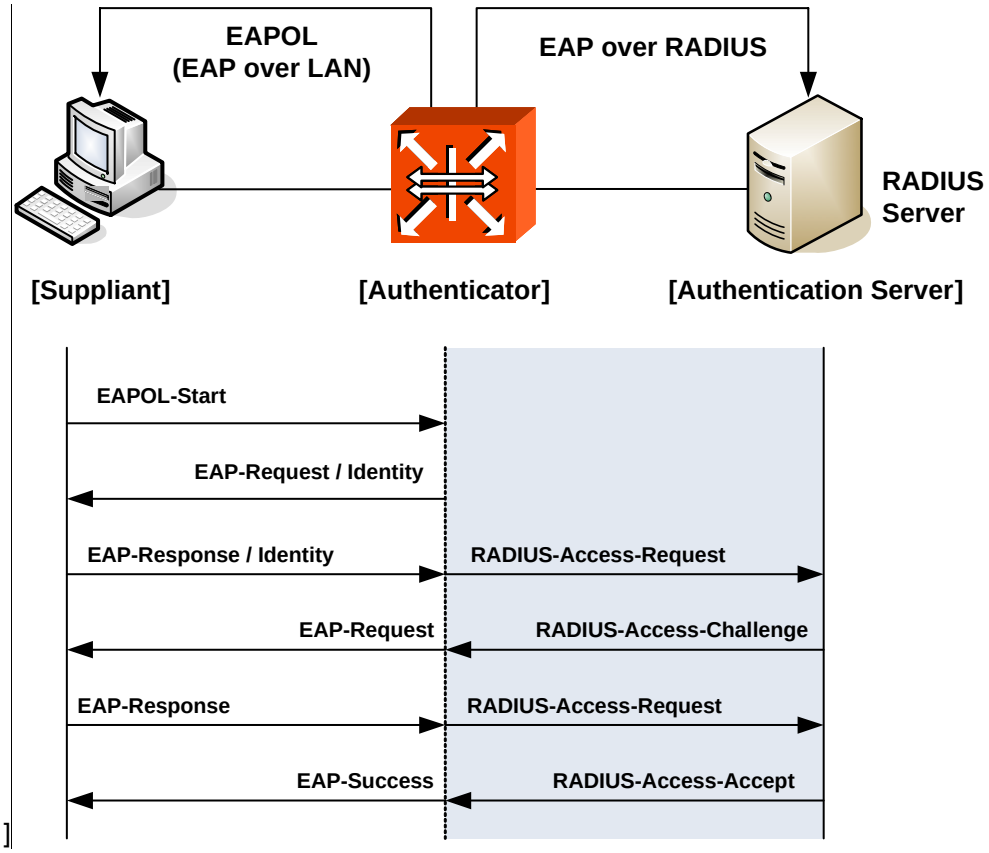


Fig. 4.1 Process of 802.1x Authentication

To enable 802.1x authentication on port of the hiD 6615 S223/S323, you should be able to perform the following tasks.

4.5.1 802.1x Authentication

4.5.1.1 Enabling 802.1x

To configure 802.1x, the user should enable 802.1x daemon first. In order to enable 802.1x daemon, use the following command.

Command	Mode	Description
dot1x system-auth-control	Global	Enables 802.1x daemon.
no dot1x system-auth-control		Disables 802.1x daemon.

4.5.1.2 Configuring RADIUS Server

As RADIUS server is registered in authenticator, authenticator also can be registered in RADIUS server.

Here, authenticator and RADIUS server need extra data authenticating each other besides they register each other's IP address. The data is the key and should be the same value for each other. For the key value, every kinds of character can be used except for the space or special character.

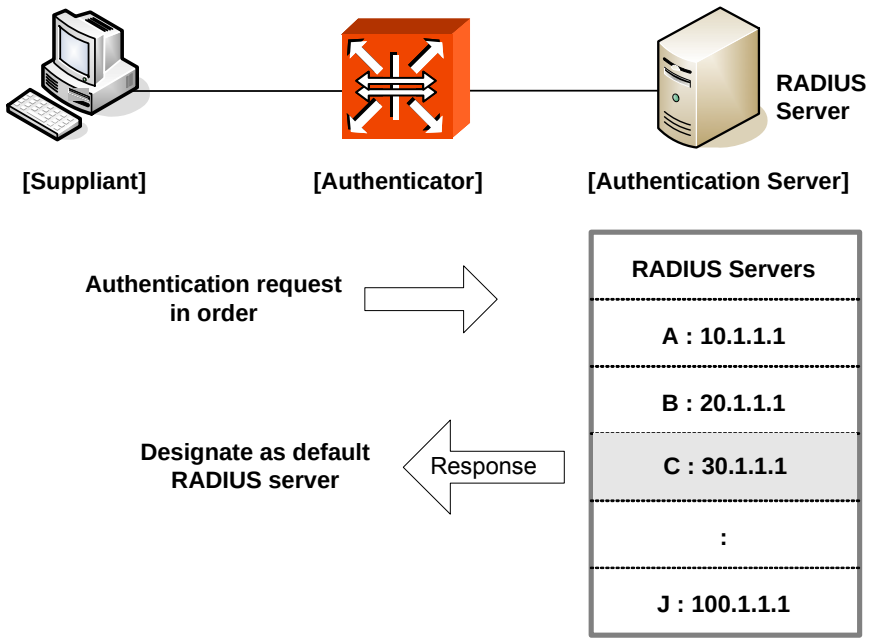


Fig. 4.2 Multiple Authentication Servers

If you register in several servers, the authentication server starts form RADIUS server registered as first one, then requests the second RADIUS server in case there's no response. According to the order of registering the authentication request, the authentication request is tried and the server which responds to it becomes the default server from the point of response time.

After default server is designated, all requests start from the RADIUS server. If there's no response from default server again, the authentication request is tried for RADIUS server designated as next one.

To configure IP address of RADIUS server and key value, use the following command.

Command	Mode	Description
dot1x radius-server host {*IP-ADDRESS* | *NAME*} **auth-port** <0-65535> **key** *KEY*	Global	Registers RADIUS server with key value and UDP port of radius server. IP-ADDRESS: Ip address of radius server NAME: host name 0-65535: UDP port number KEY: the value of key
dot1x radius-server host {*IP-ADDRESS* | *NAME*} **key** *KEY*		Configures IP address of RADIUS server and key value.
no dot1x radius-server host {*IP-ADDRESS* | *NAME*}		Deletes a registered RADIUS server.

i You can designate up to 5 RADIUS servers as authenticator.

The key is authentication information between the authenticator and RADIUS server. The authenticator and RADIUS server must have a same key value, and you can use alphabetic characters and numbers for the key value. The space or special character is not allowed.

You can configure the priority for the radius server that have configured by user.

Command	Mode	Description
dot1x radius-server move {*IP-ADDRESS* | *NAME*} **priority** *PRIORITY*	Global	Configures the priority of radius server. IP-ADDRESS: Ip address of radius server NAME: host name

4.5.1.3 Configuring Authentication Mode

You can change the authentication mode from the port-based to the MAC-based. To change the authentication mode, use the following command.

Command	Mode	Description
dot1x auth-mode mac-base *PORTS*	Global	Sets the authentication mode to the MAC-based.
no dot1x auth-mode mac-base *PORTS*		Restores the authentication mode to the port-based.

i Before setting the authentication mode to the MAC-based, you need to set a MAC filtering policy to deny them for all the Ethernet ports. To configure a MAC filtering policy, see Section 7.12.1

4.5.1.4 Authentication Port

After configuring 802.1x authentication mode, you should select the authentication port.

Command	Mode	Description
dot1x nas-port *PORTS*	Global	Designates 802.1x authentication port.
no dot1x nas-port *PORTS*		Disables 802.1x authentication port.

4.5.1.5 Force Authorization

The hiD 6615 S223/S323 can allow the users to request the access regardless of the authentication from RADIUS server. For example, it is possible to configure not to be authenticated from the server even though a client is authenticated from the server.

To manage the approval for the designated port, use the following command.

Command	Mode	Description
dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**} *PORTS*	Global	Configures the way of authorization to control port whether it has the RADIUS authentication or not.
no dot1x port-control *PORTS*		Deletes the configuration of the way of authorization to control port.

- **auto:** Follows the authentication of RADIUS server.
- **force-authorized:** Gives the authorization to a client even though RADIUS server didn't approve it.
- **force-unauthorized:** Don't give the authorization to a client even though RADIUS server authenticates it.

4.5.1.6 Configuring Interval for Retransmitting Request/Identity Packet

In hiD 6615 S223/S323, it is possible to specify how long the device waits for a client to send back a response/identity packet after the device has sent a request/identity packet. If the client does not send back a response/identity packet during this time, the device retransmits the request/identity packet.

To configure the number of seconds that the switch waits for a response to a request/identity packet, use the following command.

Command	Mode	Description
dot1x timeout tx-period <1-65535> *PORTS*	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: retransmit interval (default: 30)
no dot1x timeout tx-period *PORTS*		Disables the interval for requesting identity.

4.5.1.7 Configuring Number of Request to RADIUS Server

After 802.1x authentication configured as explained above and the user tries to connect with the port, the process of authentication is progressed among user's PC and the equipment as authenticator and RADIUS server. It is possible to configure how many times the device which will be authenticator requests for authentication to RADIUS server.

To configure times of authentication request in the hiD 6615 S223/S323, please use the command in *Global Configuration* mode.

Command	Mode	Description
dot1x radius-server retries <1-10>	Global	Configure times of authentication request to RADIUS server. 1-10: retry number

4.5.1.8 Configuring Interval of Request to RADIUS Server

For the hiD 6615 S223/S323, it is possible to set the time for the retransmission of packets to check RADIUS server. If there's a response from other packets, the switch waits for a response from RADIUS server during the configured time before resending the request.

To set the interval of request to RADIUS server, use the following command.

Command	Mode	Description
dot1x radius-server timeout <1-120>	Global	Configures the interval of request to RADIUS server. 1-120: 1-120 seconds (Default value: 1)

You should consider the distance from the server for configuring the interval of requesting the authentication to RADIUS server. If you configure the interval too short, the authentication couldn't be realized. If it happens, you'd better to reconfigure the interval longer.

4.5.2 802.1x Re-Authentication

In hiD 6615 S223/S323, it is possible to update the authentication status on the port periodically. To enable re-authentication on the port, you should perform the below procedure.

Step 1
Enable 802.1x re-authentication

Step 2
Configure the interval of re-authentication

Step 3
Configuring the interval of requesting re-authentication in case of re-authentication fails.

Step 4
Executing 802.1x re-authenticating regardless of the interval

4.5.2.1 Enabling 802.1x Re-Authentication

To enable 802.1x re-authentication using the following command.

Command	Mode	Description
dot1x reauth-enable *PORTS*	Global	Enables 802.1x re-authentication.
no dot1x reauth-enable *PORTS*		Disables 802.1x re-authentication.

4.5.2.2 Configuring the Interval of Re-Authentication

RAIDIUS server contains the database about the user who has access right. The database is real-time upgraded so it is possible for user to lose the access right by updated database even though he is once authenticated. In this case, even though the user is accessible to network, he should be authenticated once again so that the changed database is applied to. Besides, because of various reasons for managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time. The administrator of hiD 6615 S223/S323 can configure a term of re-authentication.

To configure a term of re-authentication, use the following command.

Command	Mode	Description
dot1x timeout reauth-period <1-4294967295> *PORTS*	Global	Sets the period between re-authentication attempts.
no dot1x timeout reauth-period *PORTS*		Deletes the period between re-authentication attempts.

4.5.2.3 Configuring the Interval of Requesting Re-authentication

When the authenticator sends Request/Identity packet for re-authentication and no response is received from the suppliant for the number of seconds, the authenticator retransmits the request to the suppliant. In hiD 6615 S223/S323, you can set the number of seconds that the authenticator should wait for a response to request/identity packet from the suppliant before retransmitting the request.

To set a period that the authenticator waits for a response, use the following command.

Command	Mode	Description
dot1x timeout quiet-period <1-65535> *PORTS*	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: reattempt interval seconds PORTS: enters port number
no dot1x timeout quiet-period *PORTS*		Disables the interval for requesting identity.

4.5.2.4 802.1x Re-authentication

In 4.5.2.2 Configuring the Interval of Re-Authentication, it is described even though the user is accessible to network, he should be authenticated so that the changed database is applied to.

Besides, because of various reasons managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time.

To implement re-authentication immediately regardless of configured time interval, user

the following command.

Command	Mode	Description
dot1x reauthenticate *PORTS*	Global	Implement re-authentication regardless of the configured time interval.

4.5.3 Initializing Authentication Status

The user can initialize the entire configuration on the port. Once the port is initialized, the supplicants accessing to the port should be re-authenticated.

Command	Mode	Description
dot1x initialize *PORTS*	Global	Initializes the authentication status on the port.

4.5.4 Applying Default Value

To apply the default value to the system, use the following command.

Command	Mode	Description
dot1x default *PORTS*	Global	Applies the default value.

4.5.5 Displaying 802.1x Configuration

To display 802.1x configuration, use the following command.

Command	Mode	Description
show dot1x [*PORTS*]	Enable Global	Shows 802.1x configuration.

4.5.6 802.1x User Authentication Statistic

To display the statistics about the process of 802.1x user authentication, use the following command.

Command	Mode	Description
show dot1x statistics *PORTS*	Global	Shows the statistics of 802.1x user authentication on the port.

To reset statistics by deleting the statistics of 802.1x user authentication, use the following command.

Command	Mode	Description
dot1x clear statistics *PORTS*	Global	Makes reset state by deleting the statistics of 802.1x on the port.

4.5.7 Sample Configuration

The following is to show the configuration after configuring pot number 4 as the authentication port and registering IP address of authentication port and information of RADIUS server.

```
SWTICH(config)# dot1x system-auth-control
SWTICH(config)# dot1x nas-port 4
SWTICH(config)# dot1x port-control force-authorized 4
SWTICH(config)# dot1x radius-server host 10.1.1.1 auth-port 4 key test
SWTICH(config)# show dot1x
802.1x authentication is enabled.
RADIUS Server : 10.1.1.1 (Auth key : test)
-----------------------------------------------------
           |         1         2         3         4
   802.1x  |12345678901234567890123456789012345678901234
-----------------------------------------------------
 PortEnable |...p.....................................
 PortAuthed |...u.....................................
  MacEnable |.....................................
  MacAuthed |.....................................
-----------------------------------------------------
p = port-based, m = mac-based, a = authenticated, u = unauthenticated

SWTICH(config)#
```

The following is configuring a term of re-authentication as 1800 and a tem of re-authentication as 1000 sec.

```
SWTICH(config)# dot1x timeout quiet-period 1000 4
SWTICH(config)# dot1x timeout reauth-period 1800 4
SWTICH(config)# dot1x reauth-enable 4
SWTICH(config)# show dot1x 4
Port 4
  SystemAuthControl : Enabled
  ProtocolVersion   : 0
  PortControl      : Force-Authorized
  PortStatus       : Unauthorized
  ReauthEnabled    : True
  QuietPeriod      : 1000
ReauthPeriod     : 1800
SWTICH(config)#
```

The following is an example of showing the configuration after configuring the authentication based on MAC address.

```
SWTICH(config)# dot1x auth-mode mac-base 4
SWTICH(config)# show dot1x
802.1x authentication is enabled.
RADIUS Server : 10.1.1.1 (Auth key : test)
-----------------------------------------------------
           |         1         2         3         4
   802.1x  |12345678901234567890123456789012345678901234
-----------------------------------------------------
 PortEnable |.....................................
```

```
 PortAuthed |.....................................
  MacEnable |...m.................................
  MacAuthed |...u.................................
-----------------------------------------------------
p = port-based, m = mac-based, a = authenticated, u = unauthenticated

SWTICH(config)#
```

5 Port Configuration

It is possible for user to configure basic environment such as auto-negotiate, transmit rate, and flow control of the hiD 6615 S223/S323 port. Also, it includes instructions how to configure port mirroring and port as basic.

5.1 Port Basic

It is possible to configure default environment of port such as port state, speed. To configure port, you need to open *Bridge Configuration* mode by using the command, **bridge**, on *Global Configuration* mode. When you begin *Bridge Configuration* mode, system prompt will be changed from SWITCH(config)# to SWITCH(bridge)#.

```
SWITCH(config)# bridge
SWITCH(bridge)#
```

The hiD 6615 S223/S323 have 12 electrical and optical combo 100/1000Base-X Ethernet ports. The direction to configure each port is different depending on its features. Read the below instruction carefully and follow it before you configure.

Refer to below figure for front interfaces of hiD 6615 S223/S323.

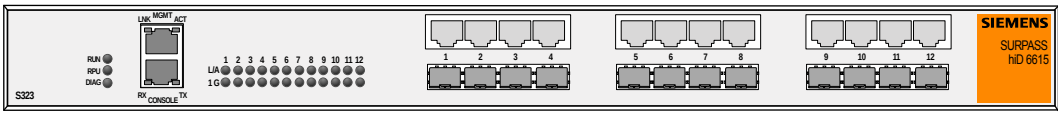


Fig. 5.1 hiD 6615 S223/S323 Interface

To display the configuration of the physical port, use the following command.

Command	Mode	Description
show port [*PORTS*]	Enable Global Bridge	Shows port configuration.

When you use the command, show port command, if you input letter at port-number, the message, “% Invalid port: port’” will be displayed, and if you input wrong number, the message, “% Invalid range: 100 [1-18]” will be displayed.

```
SWITCH(bridge)# show port port
%Invalid port: port
SWITCH(bridge)# show port 100
%Invalid range: 100 [1-18]
SWITCH(bridge)#
```

5.1.1 Selecting Port Type

User should select port type due to the hiD6615 S223/S323 switch ports have two types (RJ45 and SFP). To select port type, use the following command.

Command	Mode	Description
port medium *PORT* {**sfp** | **rj45**}	Bridge	Selects port type (Default: RJ45)

To view the configuration of switch port type, use the following command.

Command	Mode	Description
show port medium	Enable Global Bridge	Shows port type

5.2 Ethernet Port Configuration

5.2.1 Enabling Ethernet Port

To enable/disable a port, use the following command.

Command	Mode	Description
port {**enable** | **disable**} *PORTS*	Bridge	Enables/disables a port, enter a port number. (Default: enable)

The following is an example of disabling the Ethernet port 1 to 3.

```
SWITCH(config)# bridge
SWITCH(bridge)# show port 1-5
-------------------------------------------------------------------
NO    TYPE    PVID    STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 1:  Ethernet     1    Up/Down  Auto/Half/0     Off      N
 2:  Ethernet     1    Up/Down  Auto/Half/0     Off      N
 3:  Ethernet     1    Up/Down  Auto/Half/0     Off      N
 4:  Ethernet     1    Up/Down  Auto/Half/0     Off      N
 5:  Ethernet     1    Up/Down  Auto/Half/0     Off      N
SWITCH(bridge)# port disable 1-3
SWITCH(bridge)# show port 1-5
-------------------------------------------------------------------
NO    TYPE    PVID    STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 1:  Ethernet     1   Down/Down  Auto/Half/0     Off      N
 2:  Ethernet     1   Down/Down  Auto/Half/0     Off      N
 3:  Ethernet     1   Down/Down  Auto/Half/0     Off      N
 4:  Ethernet     1    Up/Down  Auto/Half/0     Off      N
 5:  Ethernet     1    Up/Down  Auto/Half/0     Off      N

SWITCH(bridge)#
```

5.2.2 Auto-negotiation

Auto-negotiation is a mechanism that takes control of the cable when a connection is established to a network device. Auto-negotiation detects the various modes that exist in the network device on the other end of the wire and advertises it own abilities to automatically configure the highest performance mode of interoperation. As a standard technology, this allows simple, automatic connection of devices that support a variety of modes from a variety of manufacturers.

To enable/disable the auto-negotiation on an Ethernet port, use the following command.

Command	Mode	Description
port nego *PORTS* {**on** | **off**}	Bridge	Configures the auto-negotiation of the specified port, enter the port number.

For the hiD 6615 S223/S323, you can configure transmit rate and duplex mode as standard to configure transmit rate or duplex mode of connected equipment even when auto-negotiation is enabled. For example, when you configure transmit rate as 10Mbps with configured auto-negotiation, a port is worked by the standard 10Mbps/full duplex mode.

i By default, auto-negotiation is activated in 10/100/1000Base-TX port of the hiD 6615 S223/S323. However you cannot configure auto-nego in fiber port.

The following is an example of deleting auto-negotiate of port 7 and 8, and showing it.

```
SWITCH(bridge)#
SWITCH(bridge)# port nego 7-8 off
SWITCH(bridge)# show port 7-8
-------------------------------------------------------------------
NO    TYPE    PVID   STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 7:  Ethernet     7    Up/Up   Force/Full/100   Off      Y
 8:  Ethernet     8    Up/Up   Force/Full/100   Off      Y
SWITCH(bridge)#
```

5.2.3 Transmit Rate

To set transmit rate of Ethernet port, use the following command.

Command	Mode	Description
port speed *PORTS* {**10** | **100** | **1000**}	Bridge	Sets transmit rate of Ethernet port as 10/100/1000Mbps, enter the port number.

i When auto-nego is activated, it is impossible to change transmit rate.

The following is an example of configuring transmit rate of port 1 as 10Mbps and showing it.

```
SWITCH(bridge)# show port 1
-------------------------------------------------------------------
NO    TYPE    PVID    STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 1:  Ethernet     1    Up/Up  Force/Half/100    Off      Y
SWITCH(bridge)# port speed 1 10
SWITCH(bridge)# show port 1
-------------------------------------------------------------------
NO    TYPE    PVID    STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 1:  Ethernet     1    Up/Up  Force/Half/10     Off      Y
SWITCH(bridge)#
```

5.2.4 Duplex Mode

Only unidirectional communication is practicable on half duplex mode, and bidirectional communication is practicable on full duplex mode. By transmitting packet for two ways, Ethernet bandwidth is enlarged two times- 10Mbps to 20Mbps, 100Mbps to 200Mbps.

To set duplex mode, use the following command.

Command	Mode	Description
port duplex *PORTS* {**full** | **half**}	Bridge	Sets full or half duplex mode of specified port, enter the port number.

The following is an example of configuring duplex mode of port 1 as half mode and showing it.

```
SWITCH(bridge)# show port 1
-------------------------------------------------------------------
NO    TYPE    PVID    STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 1:  Ethernet     1    Up/Up   Force/Full/100   Off      Y
SWITCH(bridge)# port duplex 1 half
SWITCH(bridge)# show port 1
-------------------------------------------------------------------
NO    TYPE    PVID    STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 1:  Ethernet     1    Up/Down   Force/Half/100    Off      Y
SWITCH(bridge)#
```

5.2.5 Flow Control

Ethernet ports on the switches use flow control to restrain the transmission of packets to the port for a period time. Typically, if the receive buffer becomes full, the port transmits a pause packet that tells remote ports to delay sending more packets for a specified period time. In addition, the Ethernet ports can receive and act upon pause packets from other devices.

To configure flow control of the Ethernet port, use the following command.

Command	Mode	Description
port flow-control *PORTS* {**on** | **off**}	Bridge	Configures flow control for a specified port, enter the port number. (default: off)

The following is an example of configuring flow control to port 25.

```
SWITCH(bridge)# show port 25
-------------------------------------------------------------------------
NO     TYPE     PVID    STATUS       MODE      FLOWCTRL     INSTALLED
                  (ADMIN/OPER)
-------------------------------------------------------------------------
 25   Ethernet     1    Up/Down  Auto/Half/0    Off       Y
SWITCH(bridge)# port flow-control 25 on
SWITCH(bridge)# show port 25
-------------------------------------------------------------------
NO    TYPE    PVID    STATUS       MODE      FLOWCTRL INSTALLED
                (ADMIN/OPER)
-------------------------------------------------------------------
 25:  Ethernet     1    Up/Down  Auto/Half/0     On       Y
SWITCH(bridge)#
```

5.2.6 Port Description

To specify a description of an Ethernet port, use the following command.

Command	Mode	Description
port description *PORTS DESCRIPTION*	Bridge	Specifies a description of an Ethernet port.
no port description *PORTS*		Deletes description of specified port.

To view description of port, use the following command.

Command	Mode	Description
show port description *PORTS*	Enable Global Bridge Interface	Shows description of one port or more.

The following is an example of making description of port 1 and viewing it.

```
SWITCH(bridge)# port description 1 test1
SWITCH(bridge)# show port description 1
-------------------------------------------------------------
 NO   TYPE         STATE       LINK    DESCRIPTION
               (ADM/OPR)
-------------------------------------------------------------
  1 Unknown        Up/Down     0HDX test1
SWITCH(bridge)#
```

5.2.7 Traffic Statistics

5.2.7.1 The Packets Statistics

To display traffic statistic of each port or interface with MIB or RMON MIB data defined, use the following commands.

Command	Mode	Description
show port statistics avg-pkt [*PORTS*]	Enable Global Bridge	Shows traffic statistics of average packet for a specified Ethernet port.
show port statistics avg-pps [*PORTS*]		Shows traffic statistics of average packet type for a specified Ethernet port.
show port statistics interface [*PORTS*]		Shows interface MIB counters of a specified Ethernet port.
show port statistics rmon [*PORTS*]		Shows RMON MIB counters of a specified Ethernet port.

The following is an example of displaying traffic average of port 1.

```
SWITCH(bridge)# show port statistics avg-pkt 1
================================================================================
Slot/Port|       Tx            |        Rx
--------------------------------------------------------------------------------
   Time   | pkts/s |    bits/s    | pkts/s |  bits/s
================================================================================
port 1 ----------------------------------------------------------------------
  5 sec:        1        608        120     61,848
  1 min:        3      3,242        122     62,240
 10 min:        0        440         39     20,272
SWITCH(bridge)#
```

The following is an example of displaying RMON statistic counters of port 1.

```
SWITCH(bridge)# show port statistics rmon 1
Port1
  EtherStatsDropEvents    0
  EtherStatsOctets        5,669,264
  EtherStatsPkts  71,811
  EtherStatsBroadcastPkts 36,368
  EtherStatsMulticastPkts 32,916
  EtherStatsCRCAlignErrors        0
  EtherStatsUndersizePkts 0
  EtherStatsOversizePkts  0
  EtherStatsFragments     0
  EtherStatsJabbers       0
  EtherStatsCollisions    0
  EtherStatsPkts64Octets  165,438
  EtherStatsPkts65to127Octets     12,949
  EtherStatsPkts128to255Octets    1,662
  EtherStatsPkts256to511Octets    31,177
  EtherStatsPkts512to1023Octets   12
  EtherStatsPkts1024to1518Octets  64
  SWITCH(bridge)#
```

Otherwise, to clear all recorded statistics of port and initiate, use the following command.

Command	Mode	Description
clear port statistics {*PORTS* | **all**}	Enable Global Bridge	Clears all recorded port statistics.

5.2.7.2 The CPU statistics

To display CPU statistics of Ethernet port, use the following command.

Command	Mode	Description
show cpu statistics avg-pkt [*PORTS*]	Enable Global Bridge	Shows cpu traffic statistics of average packet for a specified Ethernet port.
show cpu statistics total [*PORTS*]		Shows cpu traffic statistics of Interface group for a specified Ethernet port.

To delete all CPU statistics of specified Ethernet port, use the following command.

Command	Mode	Description
clear cpu statistics [*PORTS*]	Global Bridge	Deletes all CPU statistics for an Ethernet port.

5.2.7.3 The Protocol statistics

To enable/disable protocol statistics

Command	Mode	Description
protocol statistics {**enable** | **disable**} [{**arp** | **icmp** | **ip** | **tcp** | **udp**}]	Global Bridge	

To display protocols' statistics of Ethernet port, use the following command.

Command	Mode	Description
show protocol statistics avg-pkt [*PORTS*]	Enable Global Bridge	Shows protocols (arp, icmp, ip, tcp, udp) statistics of average packet for a specified Ethernet port.
show protocol statistics total [*PORTS*]		Shows protocols (arp, icmp, ip, tcp, udp) statistics of Interface group for a specified Ethernet port.

To delete all protocol statistics of specified Ethernet port, use the following command.

Command	Mode	Description
clear protocol statistics [*PORTS*]	Global Bridge	Deletes all protocols statistics for an Ethernet port.

5.2.8 Port Status

To display a port status, use the following command.

Command	Mode	Description
show port *PORTS*	Enable Global Bridge	Shows configured state of port, enter the port number.
show port description [*PORTS*]		Shows port specific description (max. number of characters is 100), enter the port number.
show port module-info [*PORTS*]		Shows port module information.

The following is an example of displaying port information for port 1 to 12.

```
SWITCH# show port 1-12
--------------------------------------------------------------------------
NO      TYPE      PVID    STATUS        MODE        FLOWCTRL     INSTALLED
                        (ADMIN/OPER)              (ADMIN/OPER)
--------------------------------------------------------------------------
1:    Ethernet     1     Up/Down       Force/Full/0    Off/ Off      Y
2:    Ethernet     1     Up/Down       Force/Full/0    Off/ Off      Y
3:    Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
4:    Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
5:    Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
6:    Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
7:    Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
8:    Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
9:    Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
10:   Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
11:   Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
12:   Ethernet     1     Up/Down       Auto/Full/0     Off/ Off      Y
SWITCH#
```

5.2.9 Initializing Port Statistics

To clear all recorded statistics of port and initiate, use the following command. It is possible to initiate statistics of port and select specific port.

Command	Mode	Function
clear port statistics {*PORT* | **all**}	Global	Initializes port statistics. It is possible to select several ports.

5.3 Port Mirroring

Port mirroring is the function of monitoring a designated port. Here, one port to monitor is called monitor port and a port to be monitored is called mirrored port. Traffic transmitted from mirrored port is sent to monitor port so that user can monitor network traffic.

The following is a network structure to analyze the traffic by port mirroring It analyzes traffic on the switch and network status by configuring Mirrored port and Monitor port connecting the computer, that the watch program is installed, to the port configured as Monitor port.

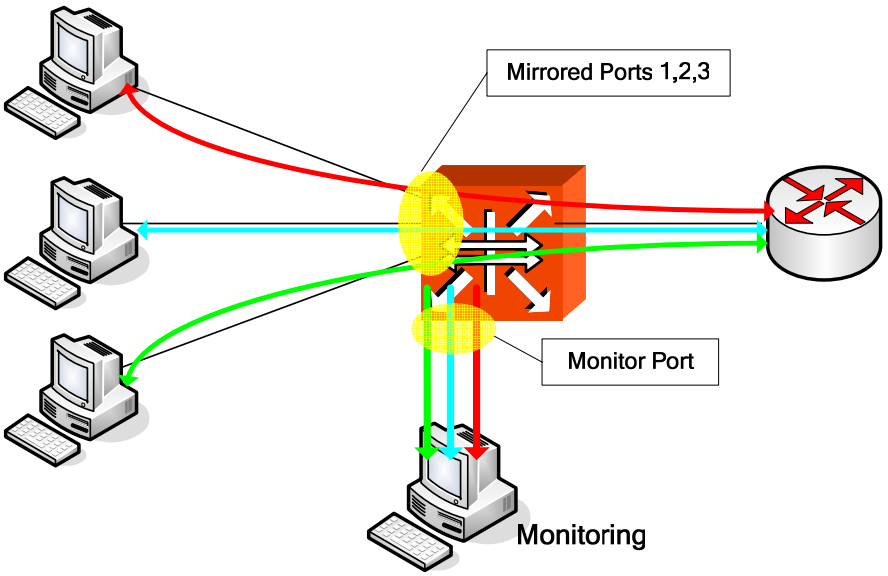


Fig. 5.2 Port Mirroring

To configure port mirroring, designate mirrored ports and monitor port. Then enable port mirroring function. Monitor port should be connected to the watch program installed PC. You can designate only one monitor port but many mirrored ports for one switch.

Step 1
Activate the port mirroring, using the following command.

Command	Mode	Description
mirror enable	Bridge	Activates port mirroring.

Step 2
Designate the monitor port, use the following command.

Command	Mode	Description
mirror monitor {*PORTS* | **cpu**}	Bridge	Designates the monitor port.

Step 3
Designate the mirrored ports, use the following command.

Command	Mode	Description
mirror add *PORTS* [**ingress** | **egress**]	Bridge	Designates the mirrored ports. ingress: ingress traffic egress: egress traffic

Step 4
To delete and modify the configuration, use the following command.

Command	Mode	Description
mirror disable	Bridge	Deactivate monitoring.
mirror del *PORTS* [**ingress** | **egress**]		Delete a port from the mirrored ports.

Step 5
To disable monitoring function, use the following command.

Command	Mode	Description
no mirror monitor	Bridge	Disable port mirroring function.

The following is an example of configuring port mirroring with a port.

Step 1
Connect a motoring PC to the monitor port of the switch.

Step 2
Enable mirroring function.

```
SWITCH(bridge)# mirror enable
SWITCH(bridge)#
```

Step 3
Configure the monitor port 1 and mirroring port 2, 3, 4 and 5.

```
SWITCH(bridge)# mirror monitor 1
SWITCH(bridge)# mirror add 2
SWITCH(bridge)# mirror add 3-5
SWITCH(bridge)#
```

Step 4
Check the configuration.

```
SWITCH(bridge)# show mirror
Mirroring enabled
 Monitor port =
      ----------------------------------
                      |       1
                      |123456789012
      ----------------------------------
      Ingress Mirrored Ports|............
      Egress  Mirrored Ports|............
SWITCH(bridge)#
```

6 System Environment

6.1 Environment Configuration

You can configure a system environment of the hiD 6615 S223/S323 with the following items:

- Host Name
- Time and Date
- Time Zone
- Network Time Protocol
- Simple Network Time Protocol (SNTP)
- Terminal Configuration
- Login Banner
- DNS Server
- Fan Operation
- Disabling Daemon Operation
- System Threshold

6.1.1 Host Name

Host name displayed on prompt is necessary to distinguish each device connected to network.

To set a new host name, use the following command.

Command	Mode	Description
hostname *NAME*	Global	Creates a host name of the switch, enter the name.
no hostname [*NAME*]		Deletes a configured host name, enter the name.

To see a new host name, use the following command.

Command	Mode	Description
show running-config hostname	Global	Shows the host name.

The following is an example of changing hostname to “hiD6615”

```
SWITCH(config)# hostname hiD6615
hiD6615(config)#
```

6.1.2 Time and Date

To set system time and date, use the following command.

Command	Mode	Description
clock *DATETIME*	Enable Global	Sets system time and date.
show clock		Shows system time and date.

The following is an example of setting system time and date as 10:20pm, July 4th, 2005.

```
SWITCH# clock 06 Mar 2006 10:20
Mon, 6 Mar 2006 10:20:00 GMT+0000
SWITCH#
```

6.1.3 Time Zone

The hiD 6615 S223/S323 provides three kinds of time zone, GMT, UCT and UTC. The time zone of the switch is predefined as GMT (Greenwich Mean Time). Also you can set the time zone where the network element belongs.

To set the time zone, use the following command (Refer to the below table).

Command	Mode	Description
time-zone *TIMEZONE*	Global	Sets the time zone.
show time-zone	Enable Global	Shows the world time zone map.

Tab. 6.1 shows the world time zone.

Time Zone	Country/City	Time Zone	Country/City	Time Zone	Country/City
GMT-12	Eniwetok	**GMT-3**	Rio De Janeiro	**GMT+6**	Rangoon
GMT-11	Samoa	**GMT-2**	Maryland	**GMT+7**	Singapore
GMT-10	Hawaii, Honolulu	**GMT-1**	Azores	**GMT+8**	Hong Kong
GMT-9	Alaska	**GMT+0**	London, Lisbon	**GMT+9**	Seoul, Tokyo
GMT-8	LA, Seattle	**GMT+1**	Berlin, Rome	**GMT+10**	Sydney,
GMT-7	Denver	**GMT+2**	Cairo, Athens	**GMT+11**	Okhotsk
GMT-6	Chicago, Dallas	**GMT+3**	Moscow	**GMT+12**	Wellington
GMT-5	New York, Miami	**GMT+4**	Teheran		
GMT-4	George Town	**GMT+5**	New Delhi		

Tab. 6.1 World Time Zone

6.1.4 Network Time Protocol

The Network Time Protocol (NTP) provides a mechanism to synchronize time on computers across an internet. The specification for NTP is defined in RFC 1119.

To enable/disable the NTP function, use the following command.

Command	Mode	Description
ntp *SERVER1* [[*SERVER2*] *SERVER3*]]	Global	Enables the NTP function with specified NTP server. SERVER: server IP address
ntp start		Operates the NTP function with specified NTP server.
no ntp		Disables the NTP function.

To display a configured NTP, use the following command.

Command	Mode	Description
show ntp	Enable Global	Shows a configured NTP function.

The following is an example of configuring 203.255.112.96 as NTP server, running it and showing it.

```
SWITCH(config)# ntp 203.255.112.96
SWITCH(config)# ntp start
SWITCH(config)# show ntp
ntp started
ntp server 203.255.112.96
SWITCH(config)#
```

The following is an example of releasing NTP and showing it.

```
SWITCH(config)# no ntp
SWITCH(config)# show ntp
ntp stoped
SWITCH(config)#
```

6.1.5 NTP (Network Time Protocol)

The hiD 6615 S223/S323 sends and receives the messages constantly with NTP server in order to adjust the recent time. NTP bind-address help NTP server classify the user's swith.

To assign IP address that transmitting the message with NTP server, use the following command.

Command	Mode	Description
ntp bind-address *A.B.C.D*	Global	Assigns IP address which receiving the message from server during transmitting the messages with NTP server.
no ntp bind-address		Deletes the binding-IP address.

6.1.6 Simple Network Time Protocol (SNTP)

NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) are the same TCP/IP protocol in that they use the same UDP time packet from the Ethernet Time Server message to compute accurate time. The basic difference in the two protocols is the algorithms being used by the client in the client/server relationship.

The NTP algorithm is much more complicated than the SNTP algorithm. NTP normally uses multiple time servers to verify the time and then controls the rate of adjustment or slew rate of the PC which provides a very high degree of accuracy. The algorithm determines if the values are accurate by identifying time server that doesn't agree with other time servers. It then speeds up or slows down the PC's drift rate so that the PC's time is

always correct and there won't be any subsequent time jumps after the initial correction. Unlike NTP, SNTP usually uses just one Ethernet Time Server to calculate the time and then it "jumps" the system time to the calculated time. It can, however, have back-up Ethernet Time Servers in case one is not available.

To configure the switch in SNTP, use the following commands.

Command	Mode	Description
sntp *SERVER 1* [*SERVER 2*] [*SERVER 3*]	Global	Specifies the IP address of the SNTP server. It is possible up to three number of server. SERVER: server IP address
no sntp		Disables SNTP function.

To display SNTP configuration, use the following command.

Command	Mode	Description
show sntp	Enable Global	Show SNTP configuration.

The following is to register SNTP server as 203.255.112.96 and enable it.

```
SWITCH(config)# sntp 203.255.112.96
SWITCH(config)# show sntp
==========================
 sntpd is running.
==========================
 Time Servers
--------------------------
 1st : 203.255.112.96
==========================
SWITCH(config)#
```

i You can configure up to 3 servers so that you use second and third servers as backup use in case the first server is down.

6.1.7 Terminal Configuration

By default, the hiD 6615 S223/S323 is configured to display 24 lines composed by 80 characters on console terminal. The maximum line displaying is 512 lines.

To set the number of line displaying on terminal screen, use the following command.

Command	Mode	Description
terminal length <0-512>	Global	Sets the number of line displaying on console terminal, enter the value.
no terminal length		Restores a default line displaying.

6.1.8 Login Banner

It is possible to set system login and log-out banner. Administrator can leave a message to other users with this banner.

To set system login and log-out banner, use the following command.

Command	Mode	Description
banner	Global	Sets a banner before login the system.
banner login		Sets a banner when successfully log in the system.
banner login-fail		Sets a banner when failing to login the system.

To restore a default banner, use the following command.

Command	Mode	Description
no banner	Global	Restores a default banner.
no banner login		
no banner login-fail		

To display a current login banner, use the following command.

Command	Mode	Description
show banner	Enable Global	Shows a current login banner.

6.1.9 DNS Server

To set a DNS server, use the following command.

Command	Mode	Description
dns server *A.B.C.D*	Global	Sets a DNS server.
no dns server *A.B.C.D*		Removes a DNS server.
show dns	Enable Global	Shows a DNS server.

If a specific domain name is registered instead of IP address, user can do telnet, FTP, TFTP and ping command to the hosts on the domain with domain name.

To configure DNS domain name, use the following command.

Command	Mode	Description
dns search *DOMAIN*	Global	Searches a domain name.
no dns search *DOMAIN*		Removes a domain name.

It is possible to delete DNS server and domain name at the same time with the below command.

Command	Mode	Description
no dns	Global	Deletes DNS server and domain name.

6.1.10 Fan Operation

In hiD 6615 S223/S323, it is possible to control fan operation. To control fan operation, use the following command.

Command	Mode	Description
fan operation {**on** | **off**}	Global	Configures fan operation.

i It is possible to configure to start and stop fan operation according to the system temperature. To configure this, refer the Section 6.1.12.3.

6.1.11 Disabling Daemon Operation

You can disable the daemon operation unnecessarily occupying CPU. To disable certain daemon operation, use the following command.

Command	Mode	Description
halt *PID*	Enable	Disables the daemon operation.

You can display PID of daemon with the **show process** command.

```
SWITCH# show process
USER      PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
admin       1  0.0  0.5  1448  592 ?        S    15:56   0:03 init [3]
admin       2  0.0  0.0     0    0 ?        S    15:56   0:00 [keventd]
admin       3  0.0  0.0     0    0 ?        SN   15:56   0:00 [ksoftirqd_CPU0]
admin       4  0.0  0.0     0    0 ?        S    15:56   0:00 [kswapd]
--More--
```

6.1.12 System Threshold

You can configure the switch with various kinds of the system threshold like CPU load, traffic, temperature, etc. Using this threshold, the hiD 6615 S223/S323 generates syslog messages, sends SNMP traps, or performs a related procedure.

6.1.12.1 CPU Load

To set a threshold of CPU load, use the following command.

Command	Mode	Description
threshold cpu <21-100> {**5** | **60** | **600**} [<20-100> {**5** | **60** | **600**}]	Global	Sets a threshold of CPU load in the unit of percent (%). 20-100: CPU load (default: 50) 5 | 60 | 600: time Interval (second)
no threshold cpu		Deletes a configured threshold of CPU load.

To show a configured threshold of CPU load, use the following command.

Command	Mode	Description
show cpuload	All	Shows a configured threshold of CPU load.

6.1.12.2 Port Traffic

To set a threshold of port traffic, use the following command.

Command	Mode	Description
threshold port *PORTS THRESHOLD* {**5** | **60** | **600**} {**rx** | **tx**}	Global	Sets a threshold of port traffic. PORTS: port number (1/1, 1/2, 2/1, …) THRESHOLD: threshold value (unit: kbps) 5 | 60 | 600: time Interval (unit: second)
no threshold port *PORTS* {**rx** | **tx**}		Deletes a configured threshold of port traffic.

The threshold of the port is set to the maximum rate of the port as a default.

To show a configured threshold of port traffic, use the following command.

Command	Mode	Description
show port threshold	Enable Global	Shows a configured threshold of port traffic.

6.1.12.3 Fan Operation

The system fan will operate depending on a configured fan threshold. To set a threshold of port traffic, use the following command.

Command	Mode	Description
threshold fan *START-TEMP STOP-TEMP*	Global	Sets a threshold of fan operation in the unit of centigrade (°C). START-TEMP: starts fan operation. (default: 30) STOP-TEMP: stops fan operation. (default: 0)
no threshold fan		Deletes a configured threshold of fan operation.

When you set a threshold of fan operation, *START-TEMP* must be higher than *STOP-TEMP*.

To show a configured threshold of fan operation, use the following command.

Command	Mode	Description
show status fan	Enable /Global / Bridge	Shows a status and configured threshold of fan operation.

6.1.12.4 System Temperature

To set a threshold of system temperature, use the following command.

Command	Mode	Description
threshold temp *VALUE VALUE*	Global	Sets a threshold of system temperature in the unit of centigrade (°C). VALUE: Threshold temperature between -40 ~ 100
no threshold temp		Deletes a configured threshold of system temperature.

To show a configured threshold of system temperature, use the following command.

Command	Mode	Description
show status temp	Enable Global	Shows a status and configured threshold of system temperature.

6.1.12.5 System Memory

To set a threshold of system memory in use, use the following command.

Command	Mode	Description
threshold memory <20-100>	Global	Sets a threshold of system memory in the unit of per-cent (%). 20-100: system memory in use
no threshold memory		Deletes a configured threshold of system memory.

6.1.13 Enabling FTP Server

FTP server is enabled on hiD 6615 S223/S323 by default. But this configuration can't provide the security serveice becaue it's easy to access to the port #23 by others. If the default configuration is unnecessary on sysem, user can disable the system as FTP server.

To enable/disable the system of hiD S223/S323 as FTP server, use the following command.

Command	Mode	Description
ftp server {**enable** | **disable**}	Global	Enables/ disables the function for FTP serve Default: enable

The follwing is an example of displaying the status of FTP server.

```
SWITCH(config)# ftp server disable
SWITCH(config)# show running-config
(Omitted)
!
ftp server disable
(Omitted)
SWTICH(config)#
```

6.1.14 Assigning IP Address of FTP Client

Serveral IP addresses can be assigned on hiD 6615 S223/S323. But user can specify one source IP address connecting FTP server when the switch is a client. To configure FTP binding address as a source IP address when hiD 6615 S223/S323 as a client connects to FTP server, use the following command.

Command	Mode	Description
ftp bind-address *A.B.C.D*	Global	Binds a source IP address for connecting to FTP server..
no ftp bind-address		Deletes FTP bind-address

i Please be careful that the FTP bind-address is also applied to TFTP server's bind-address.

6.2 Configuration Management

You can verify if the system configurations are correct and save them in the system. This section contains the following functions.

- Displaying System Configuration
- Saving System Configuration
- Auto-Saving
- System Configuration File
- Restoring Default Configuration

6.2.1 Displaying System Configuration

To display a current running configuration of the system, use the following command.

Command	Mode	Description
show running-config	All	Shows a configuration of the system.
show running-config {**admin-rule** | **arp** | **bridge** | **dns** | **full** | **hostname** | **instance** | **interface** *INTERFACE* I **login** | **pm** | **qos** | **rmon-alarm** | **rmon-event** | **rmon-history** | **router** {**bgp** | **pim** | **rip** | **ospf** | **vrrp**} | **rule** | **snmp** | **syslog** | **time-out** | **time-zone** | **time-out**}		Shows a configuration of the system with the specific option.
show running-config router {bgp | ospf | pim | rip | vrrp}		Shows only the configuration that corresponds to each option.

The following is an example to display a configuration of syslog.

```
SWITCH# show running-config syslog
!
syslog start
syslog output info local volatile
syslog output info local non-volatile
!
SWITCH#
```

6.2.2 Saving System Configuration

If you change a configuration of the system, you need to save the changes in the system flash memory. To save all changes of the system, use the following command.

Command	Mode	Description
write memory	All	Saves all changes in the system flash memory.

When you use the command, **write memory**, make sure there is no key input until **[OK]** message appears.

6.2.3 Auto-Saving

In hiD 6615 S223/S323, it is possible to save the configuration automatically. To configure the con-figuration periodically, use the following command.

Command	Mode	Description
write interval <10-1440>	Global	Saves auto-configuration periodically. 10-1440: auto-saving interval (Default: 10 minute)
no write interval		Disables auto-saving function.

6.2.4 System Configuration File

To manage a system configuration file, use the following command.

Command	Mode	Description
copy running-config {*FILENAME* | **startup-config**}	Enable	Copies a running configuration file. FILENAME: configuration file name startup-config: startup configuration file
copy startup-config *FILENAME*		Copies a startup configuration file. FILENAME: configuration file name.
copy *FILENAME* **startup-config**		Copies a specified configuration file to the startup con-figuration file. FILENAME: configuration file name
copy *FILENAME1 FILENAME2*		Copies a specified configuration file to another configu-ration file.
erase *FILENAME*		Deletes a specified configuration file. FILENAME: configuration file name

To back up a system configuration file using FTP or TFTP, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **config upload** {*FILE-NAME* | **startup-config**}	Enable	Uploads a file to ftp or fttp server with a name configured by user.
copy {**ftp** | **tftp**} **config download** {*FILE-NAME* | **startup-config**}		Downloads a file from ftp or fttp server with a name configured by user.
copy {**ftp** | **tftp**} **os upload** {**os1** | **os2**}		Uploads a file to ftp or fttp server with a name of os1 or os2.
copy {**ftp** | **tftp**} **os download** {**os1** | **os2**}		Downloads a file from ftp or fttp server with a name of os1 or os2.

i To access FTP to back up the configuration or use the backup file, you should know FTP user ID and the password. To back up the configuration or use the file through FTP, you can check the file transmission because hash function is automatically turned on.

To display a system configuration file, use the following command.

Command	Mode	Description
show startup-config	Enable	Shows a current startup configuration.
show config-list	Enable Global	Shows a list of configuration files.

The following is an example of displaying a list of configuration files.

```
SWITCH(config)# copy running-config SURPASShiD6615
SWITCH(config)# show config-list
========================
       CONFIG-LIST
========================
l3_default
SURPASShiD6615
SWITCH(config)#
```

To delete backup file, use the following command.

Command	Mode	Description
erase config *FILENAME*	Enable	Deletes backup file.

6.2.5 Restoring Default Configuration

To restore a default configuration of the system, use the following command.

Command	Mode	Description
restore factory-defaults	Global	Restores a factory default configuration.
restore layer2-defaults		Restores an L2 default configuration.
restore layer3-defaults		Restores an L3 default configuration.

i After restoring a default configuration, you need to restart the system to initiate.

The following is an example of restoring a default configuration of the system.

```
SWITCH(config)# restore factory-defaults
You have to restart the system to apply the changes
SWITCH(config)#
```

6.3 System Management

When there is any problem in the system, you must find what the problem is and its solution. Therefore, you should not only be aware of a status of the system but also verify that the system is configured properly.

This section includes the following functions with CLI command.

- Network Connection
- IP ICMP Source-Routing
- Tracing Packet Route
- Displaying User Connecting to
- MAC Table
- Running Time of System
- System Information
- System Memory Information
- Average of CPU Load
- Running Process
- Displaying System Image
- Displaying Installed OS
- Default OS
- Switch Status
- Tech Support

6.3.1 Network Connection

To verify if your system is correctly connected to the network, use the command, **ping**. For IP network, this command transmits echo message to ICMP (Internet Control Message Protocol). ICMP is internet protocol that notifies fault situation and provides information on the location where IP packet is received. When ICMP echo message is received at the location, its replying message is returned to the place where it came.

To perform a ping test to verify network status, use the following command.

Command	Mode	Description
ping [*IP-ADDRESS*]	Enable	Performs a ping test to verify network status.

The following is the basic information to operate ping test.

Items	Description
Protocol [ip]	Supports ping test. Default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to check network status with relative.
Repeat count [5]	Sends ICMP echo message as many as count. Default is 5.
Datagram size [100]	Ping packet size. Default is 100 bytes.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. Default is 2 seconds.
Extended commands [n]	Shows the additional commands. Default is no.

Tab. 6.2 Options for Ping

The following is an example of ping test 5 times to verify network status with IP address 172.16.1.254.

```
SWITCH# ping
Protocol [ip]: ip
Target IP address: 172.16.1.254
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: n
PING 172.16.1.254 (172.16.1.254) 100(128) bytes of data.
Warning: time of day goes back (-394us), taking countermeasures.
108 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=0.058 ms
108 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=0.400 ms
108 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=0.403 ms
108 bytes from 172.16.1.254: icmp_seq=4 ttl=255 time=1.63 ms
108 bytes from 172.16.1.254: icmp_seq=5 ttl=255 time=0.414 ms
--- 172.16.1.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 0.058/0.581/1.632/0.542 ms
SWITCH#
```

When multiple IP addresses are assigned to the switch, sometimes you need to verify the connection status between the specific IP address and network status.

In this case, use the same process as ping test and then input the followings after extended commands. It is possible to verify the connection between specific IP address and network using the following command.

The following is the information to use ping test for multiple IP addresses.

Items	Description
Source address or interface	Designates the address where the relative device should respond in source ip address.
Type of service [0]:	The service filed of QoS (Quality Of Service) in Layer 3 application. It is possible to designate the priority for IP Packet.
Set DF bit in IP header? [no]	Decides whether Don't Fragment (DB) bit is applied to Ping packet or not. Default is no. If the user choose 'yes', when the packets pass through the segment compromised with the smaller data unit, it prevents the packet to be Fragment. Therefore there could be error message.
Data pattern [0xABCD]	Configures data pattern. Default is OxABCD.

Tab. 6.3 Options for Ping for Multiple IP Addresses

The following is to verify network status between 172.16.157.100 and 172.16.1.254 when IP address of the switch is configured as 172.16.157.100.

```
SWITCH# ping
Protocol [ip]:
Target IP address: 172.16.1.254
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: y
Source address or interface: 172.16.157.100
Type of service [0]: 0
Set DF bit in IP header? [no]: no
Data pattern [0xABCD]:
PATTERN: 0xabcd
PING 172.16.1.254 (172.16.1.254) from 172.16.157.100 : 100(128) bytes of data.
108 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=30.4 ms
108 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=11.9 ms
108 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=21.9 ms
108 bytes from 172.16.1.254: icmp_seq=4 ttl=255 time=11.9 ms
108 bytes from 172.16.1.254: icmp_seq=5 ttl=255 time=30.1 ms
--- 172.16.1.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8050ms
rtt min/avg/max/mdev = 11.972/21.301/30.411/8.200 ms
SWITCH#
```

6.3.2 IP ICMP Source-Routing

If you implement PING test to verify the status of network connection, icmp request arrives at the final destination as the closest route according to the routing theory.

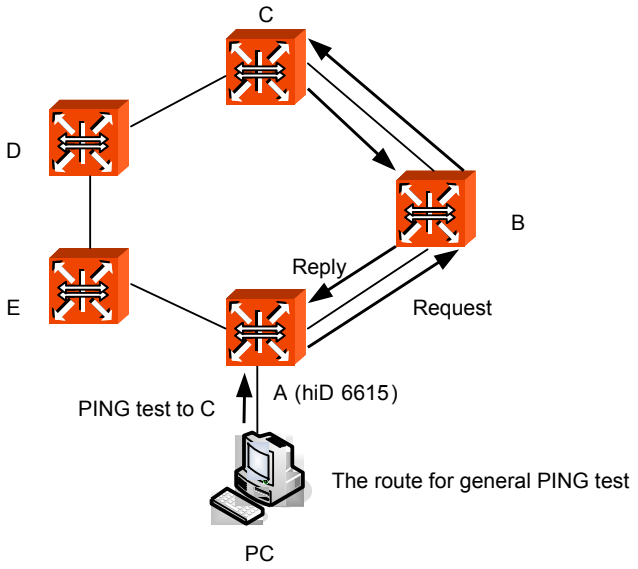


Fig. 6.1 Ping Test for Network Status

In the above figure, if you perform ping test from PC to C, it goes through the route of 「A→B→C」. This is the general case. But, the hiD 6615 S223/S323 can enable to perform ping test from PC as the route of 「A→E→D→C」.

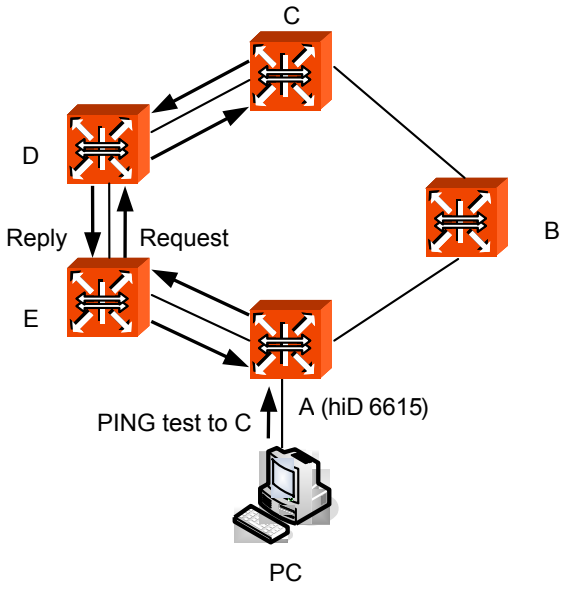


Fig. 6.2 IP Source Routing

To perform ping test as the route which the manager designated, use the following steps.

Step 1
Enable IP source-routing function from the equipment connected to PC which the PING test is going to be performed.

To enable/disable IP source-routing in the hiD 6615 S223/S323, use the following command.

Command	Mode	Description
ip icmp source-route	Global	Enable IP source-routing function.
no ip icmp source-route		Disable IP source-routing function.

Step 2
Performs the ping test from PC as the designate route with the **ping** command

6.3.3 Tracing Packet Route

You can discover the routes that packets will actually take when traveling to their destinations. To do this, the **traceroute** command sends probe datagram and displays the round-trip time for each node.

If the timer goes off before a response comes in, an asterisk (*) is printed on the screen.

Command	Mode	Description
traceroute [*ADDRESS*]	Enable	Traces packet routes through the network. ADDRESS: IP address or host name
traceroute ip *ADDRESS*		

The following is the basic information to trace packet routes.

Items	Description
Protocol [ip]	Supports ping test. Default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to check network status with relative.
Source address	Source IP address which other side should make a response.
Numeric display [n]	Hop is displayed the number instead of indications or statistics.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. Default is 2 seconds.
Probe count [3]	Set the frequency of probing UDP packets.
Maximum time to live [30]	The TTL field is reduced by one on every hop. Set the time to trace hop transmission (The number of maximum hops). Default is 30 seconds.
Port Number [33434]	Selects general UDP port to be used for probing Port. The default is 33434. The command of traceroute depends on the port range of destination host up to base + nhops – 1 through the base.

Tab. 6.4 Options for Tracing Packet Route

The following is an example of tracing packet route sent to 10.2.2.20.

```
SWITCH# traceroute 10.2.2.20
traceroute to 10.2.2.20 (10.2.2.20), 30 hops max, 38 byte packets
1 10.2.2.20 (10.2.2.20) 0.598 ms 0.418 ms 0.301 ms
SWITCH#
```

6.3.4 Displaying User Connecting to System

To display current users connecting to the system from a remote place or via console interface, use the following command.

Command	Mode	Description
where	Enable	Shows current users connecting to the system from a remote place or via console interface.

The following is an example of displaying if there is any accessing user from remote place.

```
SWITCH# where
admin at ttyp0 from 10.20.1.32:2196 for 30 minutes 35.56 seconds
admin at ttyS0 from console for 28 minutes 10.90 seconds
SWITCH#
```

6.3.5 MAC Table

To display MAC table recorded in specific port, use the following command.

Command	Mode	Description
show mac *BRIDGE* [*PORTS*]	Enable Global Bridge	Shows MAC table. BRIDGE: bridge name

The following is an example of displaying MAC table recorded in default.

```
SWITCH(config)# show mac 1

port          mac addr              permission     in use
=================================================================
eth01         00:0b:5d:98:92:da      OK              16.62
eth01         00:14:c2:d9:8a:b5      OK              56.62
eth01         00:01:02:50:d6:b9      OK              72.62
eth01         00:0d:9d:8c:00:ee      OK              72.62
eth01         00:15:00:39:4d:2e      OK              92.62
eth01         00:0e:e8:8b:24:ae      OK             115.48
eth01         00:14:c2:d9:4c:f0      OK             115.48
eth01         00:0b:5d:53:4d:96      OK             124.62
eth01         00:13:20:4b:05:af      OK             132.62
eth01         00:0e:e8:f0:b3:63      OK             152.62
 (skipped)
SWITCH(config)#
```

6.3.6 Configuring Ageing time

SURPASS hiD 6615 records MAC Table to prevent Broadcast packets from transmitting. And unnecessary MAC address that does not response during specified time is deleted from the MAC table automatically. The specified time is called Ageing time.

To specify the Ageing time, use the following command.

Command	Mode	Description
mac aging-time <10-21474830>	Bridge	Specifies the Ageing time. Default: 300sec

6.3.7 Running Time of System

To display running time of the system, use the following command.

Command	Mode	Description
show uptime	Enable Global	Shows running time of the system.

The following is an example of displaying running time of the system.

```
SWITCH# show uptime
10:41am up 15 days, 10:55, 0 users, load average: 0.05, 0.07, 0.01
SWITCH#
```

6.3.8 System Information

To display the system information, use the following command.

Command	Mode	Description
show system	Enable Global	Shows the system information.

The following is an example of displaying the system information of hiD 6615 S223/S323.

```
SWITCH(config)# show system

        SysInfo(System Information)
    Model Name         : SURPASS hiD6615 S323
    Main Memory Size   : 128 MB
    Flash Memory Size  : 8 MB(INTEL 28F640J3), 32 MB(INTEL 28F256J3)
    S/W Compatibility  : 3, 7
    H/W Revision       : DS-T3-07F-A2
    NOS Version        : 3.06
    B/L Version        : 4.69
    H/W Address        : 00:d0:cb:27:01:66
    PLD Version        : 0x10
    Serial Number      : N/A
SWITCH(config)#
```

6.3.9 System Memory Information

To display a system memory status, use the following command.

Command	Mode	Description
show memory	Enable Global	Shows system memory information.
show memory {**bgp** | **dhcp** | **imi** | **lib** | **nsm** | **ospf** | **pim** | **rip**}		Shows system memory information with a specific option.

6.3.10 CPU packet limit

To limit the packets of CPU, use the following command.

Command	Mode	Description
cpu packet limit <500-6000>	Global	

It is possible to display the packet limit of CPU using the following command.

Command	Mode	Description
show cpu packet limit	View Enable Global	

6.3.11 Average of CPU Load

It is possible to display average of CPU load using the following command.

Command	Mode	Description
show cpuload	View Enable Global	Shows threshold of CPU utilization and average of CPU utilization.

6.3.12 Running Process

The hiD 6615 S223/S323 provides a function that shows information of the running processes. The information with this command can be very useful to manage the switch.

To display information of the running processes, use the following command.

Command	Mode	Description
show process	Enable Global	Shows information of the running processes.

The following is an example of displaying information of the running processes.

```
SWITCH# show process
USER     PID  %CPU  %MEM     VSZ   RSS  TTY   STAT   START  TIME  COMMAND
admin      1   0.2   0.2    1448   596  ?     S      20:12  0:05  init [3]
admin      2   0.0   0.0       0     0  ?     S      20:12  0:00  [keventd]
admin      3   0.0   0.0       0     0  ?     SN     20:12  0:00  [ksoftirqd_CPU0]
admin      4   0.0   0.0       0     0  ?     S      20:12  0:00  [kswapd]
admin      5   0.0   0.0       0     0  ?     S      20:12  0:00  [bdflush]
admin      6   0.0   0.0       0     0  ?     S      20:12  0:00  [kupdated]
admin      7   0.0   0.0       0     0  ?     S      20:12  0:00  [mtdblockd]
admin      8   0.0   0.0       0     0  ?     SW<    20:12  0:00  [bcmDPC]
admin      9   1.4   0.0       0     0  ?     SW<    20:12  0:29  [bcmCNTR.0]
admin     10   1.4   0.0       0     0  ?     SW<    20:12  0:29  [bcmCNTR.1]
admin     17   0.0   0.0       0     0  ?     SWN    20:12  0:00  [jffs2_gcd_mtd3]
admin    149   0.0   0.3    1784   776  ?     S      Jan01  0:00  /sbin/syslogd –m
admin    151   0.0   0.2    1428   544  ?     S      Jan01  0:00  /sbin/klogd -c 1
admin    103   2.6   2.0   20552  5100  ?     S      20:12  0:53  /usr/sbin/swchd
--more--
(Omitted)
SWITCH#
```

6.3.13 Displaying System Image

To check a current system image version, use the following command.

Command	Mode	Description
show version	Enable Global	Shows version of system image.

To display a size of the current system image, use the following command.

Command	Mode	Description
show os-size	Enable Global	Shows size of system image.

6.3.14 Displaying Installed OS

To display utilization of flash memory, use the followng command.

Command	Mode	Description
show flash	Enable Global	Shows utilization of flash memory.

6.3.15 Default OS

The hiD 6615 S223/S323 supports dual OS You can show the flash memory by using show system command. When there are two kinds of system images installed, user can

configure one of two as default OS what user wants.

In hiD 6615 S223/S323, a system image saved in **os1** is configured as default OS by default.

To desgnate a default OS, use the following command.

Command	Mode	Description
default-os {**os1** | **os2**}	Enable	Desgnates default OS of switch.

6.3.16 Switch Status

To display temperature of switch, power status, and fan status, use the following command.

Command	Mode	Description
show status fan	Enable Global Bridge	Shows fan status of switch.
show status power		Shows power status.
show status temp		Shows temperature of switch.

6.3.17 Tech Support

In hiD 6615 S223/S323, you can display the configuration and configuration file, log information, register, memory, debugging information using the following commands. By checking tech supporting, check the system errors and use it for solving the problem.

Command	Mode	Description
tech-support {**all** | **crash-info**} **console**	Enable	Check tech support on console.
tech-support {**all** | **crash-info**} **remote** *IP-ADDRESS* {**ftp** | **tftp**}		Save the contents of tech support in a specified address.

Tech support contents displayed on console are showed at once regardless of the number of display lines of terminal screen.

7 Network Management

7.1 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) system is consisted of three parts: SNMP manager, a managed device and SNMP agent. SNMP is an application-layer protocol that allows SNMP manager and agent stations to communicate with each other. SNMP provides a message format for sending information between SNMP manager and SNMP agent. The agent and MIB reside on the switch. In configuring SNMP on the switch, you define the relationship between the manager and the agent. According to community, you can give right only to read or right both to read and to write. The SNMP agent has MIB variables to reply to request from SNMP administrator. And SNMP administrator can obtain data from the agent and save data in the agent. The SNMP agent gets data from MIB, which saves information on system and network.

SNMP agent sends trap to administrator for specific cases. Trap is a warning message to alert network status to SNMP administrator.

The hiD 6615 S223/S323 enhances accessing management of SNMP agent more and limit the range of OID opened to agents.

The following is how to configure SNMP.

- SNMP Community
- Information of SNMP Agent
- SNMP Com2sec
- SNMP Group
- SNMP View Record
- Permission to Access SNMP View Record
- SNMP Version 3 User
- SNMP Trap
- SNMP Alarm
- Displaying SNMP Configuration
- Disabling SNMP

7.1.1 SNMP Community

Only an authorized person can access an SNMP agent by configuring SNMP community with a community name and additional information.

To configure an SNMP community to allow an authorized person to access, use the following command on *Global configuration* mode.

Command	Mode	Description
snmp community {**ro** | **rw**} *COMMUNITY* [*IP-ADDRESS*] [*OID*]	Global	Creates SNMP community. COMMUNITY: community name
no snmp community {**ro** | **rw**} *COMMUNITY*		Deletes a created community. COMMUNITY: community name

i You can configure up to 3 SNMP communities for each read-only and read-write.

To display a configured SNMP community, use the following command.

Command	Mode	Description
show snmp community	Enable Global	Shows a created SNMP community.

The following is an example of creating 2 SNMP communities.

```
SWITCH(config)# snmp community ro public
SWITCH(config)# snmp community rw private
SWITCH(config)# show snmp community

Community List
Type  Community        Source            OID
-----------------------------------------------
ro    public
rw    private

SWITCH(config)#
```

7.1.2 Information of SNMP Agent

You can specify basic information of SNMP agent as administrator, location, and address that confirm its own identity.

To set basic information of SNMP agent, use the following command.

Command	Mode	Description
snmp contact *NAME*	Global	Sets a name of administrator.
snmp location *LOCATION*		Sets a location of SNMP agent.
snmp agent-address *IP-ADDRESS*		Sets an IP address of SNMP agent.
no snmp contact		Deletes specified basic information for each item.
no snmp location		
no snmp agent-address *IP-ADDRESS*		

The following is an example of specifying basic information of SNMP agent.

```
SWITCH(config)# snmp contact Brad
SWITCH(config)# snmp location Germany
SWITCH(config)#
```

To display basic information of SNMP agent, use the following command.

Command	Mode	Description
show snmp contact	Enable Global	Shows a name of administrator.
show snmp location		Shows a location of SNMP agent.
show snmp agent-address		Shows an IP address of SNMP agent.

7.1.3 SNMP Com2sec

SNMP v2 authorizes the host to access the agent according to the identity of the host and community name. The command, **com2sec**, specifies the mapping from the identity of the host and community name to security name.

To configure an SNMP security name, use the following command.

Command	Mode	Description
snmp com2sec *SECURITY* {*IP-ADDRESS* | *IP-ADDRESS/M*} *COMMUNITY*	Global	Specifies the mapping from the identity of the host and community name to security name, enter security and community name. SECURITY: security name COMMUNITY: community name
no snmp com2sec *SECURITY*		Deletes a specified security name, enter the security name. SECURITY: security name
show snmp com2sec	Enable Global	Shows a specified security name.

The following is an example of configuring SNMP com2sec.

```
SWITCH(config)# snmp com2sec TEST 10.1.1.1 PUBLIC
SWITCH(config)# show snmp com2sec

Com2Sec List
         SecName   Source   Community
--------------------------------------
com2sec  TEST     10.1.1.1 PUBLIC

SWITCH(config)#
```

7.1.4 SNMP Group

You can create an SNMP group that can access SNMP agent and its community that belongs to a group.

To create an SNMP group, use the following command.

Command	Mode	Description
snmp group *GROUP* {**v1** | **v2c** | **v3**} *SECURITY*	Global	Creates SNMP group, enter the group name. GROUP: group name SECURITY: security name
no snmp group *GROUP* {**v1** | **v2c** | **v3**} *SECURITY*		Deletes SNMP group, enter the group name. GROUP: group name
show snmp group	Enable Global	Shows a created SNMP group.

7.1.5 SNMP View Record

You can create an SNMP view record to limit access to MIB objects with object identity (OID) by an SNMP manager.

To configure an SNMP view record, use the following command.

Command	Mode	Description
snmp view *VIEW* {**included** | **excluded**} *OID* [*MASK*]	Global	Creates an SNMP view record. VIEW: view record name included: includes sub-tree. excluded: excludes sub-tree. OID: OID number MASK: Mask value (e.g. ff | ff.ff)
no snmp view *VIEW* [*OID*]		Deletes a created SNMP view record. VIEW: view record name

To display a created SNMP view record, use the following command.

Command	Mode	Description
show snmp view	Enable Global	Shows a created SNMP view record.

The following is an example of creating an SNMP view record.

```
SWITCH(config)# snmp view TEST included 410
SWITCH(config)# show snmp view

View list
------------------------------------------------
view TEST included 410

SWITCH(config)#
```

7.1.6 Permission to Access SNMP View Record

To grant an SNMP group to access a specific SNMP view record, use the following command.

Command	Mode	Description
snmp access *GROUP* {**v1** | **v2c**} *READ-VIEW WRITE-VIEW NOTIFY-VIEW*	Global	Grants an SNMP group to access a specific SNMP view record. GROUP: group name
snmp access *GROUP* **v3** {**noauth** | **auth** | **priv**} *READ-VIEW WRITE-VIEW NOTIFY-VIEW*		Grants an SNMP version 3 group to access a specific SNMP view record. GROUP: group name
no snmp access *GROUP*		Deletes a granted SNMP group to access a specific SNMP view record.

To display a granted an SNMP group to access a specific SNMP view record, use the following command.

Command	Mode	Description
show snmp access	Enable Global	Shows a granted an SNMP group to access a specific SNMP view record

The following is an example of permission to accessing an SNMP view record.

```
SWITCH(config)#
SWITCH(config)# snmp access regroup v1 test none none
SWITCH(config)# show snmp access
Access List
GroupName       SecModel SecLevel ReadView       WriteView       NotifyView
--------------------------------------------------------------------------------
rogroup         v1         noauth   TEST           none            none
SWITCH(config)#
```

7.1.7 SNMP Version 3 User

In SNMP version 3, you can register an SNMP agent as user. If you register SNMP version 3 user, you should configure it with the authentication key.

To create/delete SNMP version 3 user, use the following command.

Command	Mode	Description
snmp user *USER* {**md5** | **sha**} *AUTH-KEY* [**des** *PRIVATE-KEY*]	Global	Creates SNMP version 3 user. USER : enters user name AUTH-KEY: Authentication passphrase (min length:8) PRIVATE-KEY: Privacy passphrase (min length: 8)
no snmp user *USER*		Deletes a registered SNMP version 3 user.

To display SNMP version 3 user, use the following command.

Command	Mode	Description
show snmp user	Enable Global	Displays SNMP version 3 user.

7.1.8 SNMP Trap

SNMP trap is an alert message that SNMP agent notifies SNMP manager about certain problems. If you configure SNMP trap, switch transmits pertinent information to network management program. In this case, trap message receivers are called trap host.

7.1.8.1 SNMP Trap Host

To set an SNMP trap host, use the following command.

Command	Mode	Description
snmp trap-host *IP-ADDRESS* [*COMMUNITY*]	Global	Specifies IP address of an SNMP trap host.
snmp trap2-host *IP-ADDRESS* [*COMMUNITY*]		
snmp inform-trap-host *IP-ADDRESS* [*COMMUNITY*]		Specifies IP address of SNMP information trap host.

i You need to configure an SNMP trap host with the **snmp trap2-host** command, if you manage the switch via the ACI-E.

To delete a specified SNMP trap host, use the following command.

Command	Mode	Description
no snmp trap-host *IP-ADDRESS*	Global	Deletes a specified SNMP trap host.
no snmp trap2-host *IP-ADDRESS*		
no snmp inform-trap-host *IP-ADDRESS*		Deletes a specified information trap host.

i You can set maximum 16 SNMP trap hosts with inputting one by one.

The following is an example of setting an SNMP trap host.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)# snmp trap-host 20.1.1.5
SWITCH(config)# snmp trap-host 30.1.1.2
SWITCH(config)#
```

7.1.8.2 SNMP Trap Mode

To select an SNMP trap-mode, use the following command.

Command	Mode	Description
snmp trap-mode {**alarm-report** | **event**}	Global	Selects SNMP trap-mode according to user's network environment. (alarm-report or event)

- **"event" trap-mode** is set by default. It means that Dasan trap OID will be used upon sending the trap if the trap-mode is "event"
- **"alarm-report" trap-mode** will be used form SLE MIB OID which is Siemens private OID.

i In order to manage hiD 6615 S223/S323 using ACI-E, the trap-mode must be set as "alarm-report". Otherwise, ACI-E would not recognize any traps set from the hiD 6615 S223/S323.

7.1.8.3 Enabling SNMP Trap

The system provides various kind of SNMP trap, but it may inefficiently work if all these trap messages are sent very frequently. Therefore, you can select each SNMP trap sent to an SNMP trap host.

i The system is configured to send all the SNMP traps as default.

- **authentication-failure** is shown to inform wrong community is input when user trying to access to SNMP inputs wrong community.
- **cold-start** is shown when SNMP agent is turned off and restarts again.
- **link-up/down** is shown when network of port specified by user is disconnected, or when the network is connected again.
- **memory-threshold** is shown when memory usage exceeds the threshold specified by user. Also, when memory usage falls below the threshold, trap message will be shown to notify it.
- **cpu-threshold** is shown when CPU utilization exceeds the threshold specified by user. Also, when CPU load falls below the threshold, trap message will be shown to notify it.
- **port-threshold** is shown when the port traffic exceeds the threshold configured by user. Also, when port traffic falls below the threshold, trap message will be shown.
- **temperature-threshold** is shown when the system temperature exceeds the threshold configured by user. Also, when system temperature falls below the threshold, trap message will be shown.
- **dhcp-lease** is shown when there is no more IP address can be assigned in subnet of DHCP server. Even if only one subnet does not have IP address to assign when there are several subnets, this trap message will be seen.
- **fan/power/module** is shown when there is any status-change of fan, power, and module.

To enable SNMP trap, use the following command.

Command	Mode	Description
snmp trap auth-fail	Global	Configures the system to send SNMP trap when SNMP authentication is fail.
snmp trap cold-start		Configures the system to send SNMP trap when SNMP agent restarts.
snmp trap link-up *PORTS* [*NODE*]		Configures the system to send SNMP trap when a port is connected to network.
snmp trap link-down *PORTS* [*NODE*]		Configures the system to send SNMP trap when a port is disconnected from network.
snmp trap cpu-threshold		Configures the system to send SNMP trap when CPU load exceeds or falls below the threshold.
snmp trap port-threshold		Configures the system to send SNMP trap when the port traffic exceeds or falls below the threshold.
snmp trap temp-threshold		Configures the system to send SNMP trap when system temperature exceeds or falls below the threshold.

Command	Mode	Description

snmp trap dhcp-lease	Global	Configures the system to send SNMP trap when no more IP address that can be assigned in the subnet of DHCP server is left.
snmp trap fan		Configures the system to send SNMP trap when the fan begins to operate or stops.
snmp trap power		Configures the system to send SNMP trap when any problem occurs in power.
snmp trap module		Configures the system to send SNMP trap when there is any problem in module.

7.1.8.4 Disabling SNMP Trap

To disable SNMP trap, use the following command.

Command	Mode	Description
no snmp trap auth-fail	Global	Disables each SNMP trap.
no snmp trap cold-start		
no snmp trap link-up *PORTS* [*NODE*]		
no snmp trap link-down *PORTS* [*NODE*]		
no snmp trap cpu-threshold		
no snmp trap port-threshold		
no snmp trap temp-threshold		
no snmp trap dhcp-lease		
no snmp trap fan		
no snmp trap power		
no snmp trap module		

When you use the **no snmp** command, all configurations concerning SNMP will be deleted.

7.1.8.5 Displaying SNMP Trap

To display a configuration of SNMP trap, use the following command.

Command	Mode	Description
show snmp trap	Enable Global	Shows a configuration of SNMP trap.

The following is an example of configuring IP address 10.1.1.1 as trap-host, 20.1.1.1 as trap2-host and 30.1.1.1 as inform-trap-host.

```
SWITCH(config)# snmp trap-host 10.1.1.1
SWITCH(config)# snmp trap2-host 20.1.1.1
SWITCH(config)# snmp inform-trap-host 30.1.1.1
SWITCH(config)# show snmp trap
Trap-Host List
            Host        Community
----------------------------------------
inform-trap-host 30.1.1.1
trap2-host      20.1.1.1
trap-host       10.1.1.1
Trap List
Trap-type      Status
-------------------------
auth-fail      enable
cold-start     enable
cpu-threshold   enable
port-threshold  enable
dhcp-lease     enable
power          enable
module         enable
fan           enable|
temp-threshold  enable
SWITCH(config)#
```

7.1.9 SNMP Alarm

The hiD 6615 S223/S323 provides an alarm notification function. The alarm will be sent to a SNMP trap host whenever a specific event in the system occurs through CLI and ACI-E. You can also set the alarm severity on each alarm and make the alarm be shown only in case of selected severity or higher. This enhanced alarm notification allows system administrators to manage the system efficiently.

7.1.9.1 Enabling Alarm Notification

To configure whether the switch enable transmitting SNMP alarm or not, use the following command.

Command	Mode	Description
snmp notify-activity {**enable** | **disable**}	Global	Enables/disables an alarm notification on CLI or ACI-E. (default: disable)

7.1.9.2 Default Alarm Severity

To configure a priority of alarm, use the following command.

Command	Mode	Description
snmp alarm-severity default {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Configures the priority of alarm. (default: minor)

7.1.9.3 Alarm Severity Criterion

You can set an alarm severity criterion to make an alarm be shown only in case of selected severity or higher. For example, if an alarm severity criterion has been set to **major**, you will see only an alarm whose severity is **major** or **critical**.

To configure alarm-severity criteria in CLI, use the following command.

Command	Mode	Description
snmp alarm-severity criteria {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Configures the severity criterion. (default: warning)

The order of alarm severity is **critical** > **major** > **minor** > **warning** > **intermediate**.

The alarm severity option is valid only in ACI-E.

7.1.9.4 Generic Alarm Severity

To configure generic alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity fan-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Configures the priority of fan-fail alarm
snmp alarm-severity cold-start {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of cold-start alarm
snmp alarm-severity broadcast-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of broadcast-over alarm
snmp alarm-severity cpu-load-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of cpu-load-over alarm
snmp alarm-severity dhcp-lease {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of DHCP-lease alarm
snmp alarm-severity dhcp-illegal {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of DHCP-illegal alarm
snmp alarm-severity fan-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of fan-remove alarm
snmp alarm-severity ipconflict {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of IP conflict alarm
snmp alarm-severity memory-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of memory-over alarm
snmp alarm-severity mfgd-block {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of MFGD-block alarm
snmp alarm-severity port-link-down {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of port-link-down alarm
snmp alarm-severity port-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of port-remove alarm
snmp alarm-severity port-thread-over {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of port-thread-over alarm.
snmp alarm-severity power-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of power-fail alarm
snmp alarm-severity power-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of power-remove alarm
snmp alarm-severity rmon-alarm-rising {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of RMON-alarm-rising alarm.
snmp alarm-severity rmon-alarm-falling {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of RMON-alarm-falling alarm.
snmp alarm-severity system-restart {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of system-restart alarm.
snmp alarm-severity module-remove {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of module-remove alarm.
snmp alarm-severity temperature-high {**critical** | **major** | **minor** | **warning** | **intermediate**}		Configures the priority of temperature-high alarm.

If you want to delete a configured alarm severity, use the following command.

Command	Mode	Description
no snmp alarm-severity fan-fail	Global	Deletes a configured alarm severity.
no snmp alarm-severity cold-start		
no snmp alarm-severity broadcast-over		
no snmp alarm-severity cpu-load-over		
no snmp alarm-severity dhcp-lease		
no snmp alarm-severity dhcp-illegal		
no snmp alarm-severity fan-remove		
no snmp alarm-severity ipconflict		
no snmp alarm-severity memory-over		
no snmp alarm-severity mfgd-block		
no snmp alarm-severity port-link-down		
no snmp alarm-severity port-remove		
no snmp alarm-severity port-thread-over		
no snmp alarm-severity power-fail		
no snmp alarm-severity power-remove		
no snmp alarm-severity rmon-alarm-rising		
no snmp alarm-severity rmon-alarm-falling		
no snmp alarm-severity system-restart		
no snmp alarm-severity module-remove		
no snmp alarm-severity temperature-high		

7.1.9.5 ADVA Alarm Severity

To configure a severity of alarms for ADVA status, use the following command.

Command	Mode	Description
snmp alarm-severity adva-fan-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sends alarm notification with the severity when ADVA informs fan-fail.
snmp alarm-severity adva-if-misconfig {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs there's any misconfiguration.
snmp alarm-severity adva-if-opt-thres {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs traffic is over threshold on optical interface.
snmp alarm-severity adva-if-rcv-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs to fail to receive the packets.
snmp alarm-severity adva-if-sfp-mismatch {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs SFP module is mismatched.

Command	Mode	Description
snmp alarm-severity adva-if-trans-fault {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs to fail to transmit the packets.
snmp alarm-severity adva-psu-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs there's any problem on the power.
snmp alarm-severity adva-temperature {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs there is any problem in temperature.
snmp alarm-severity adva-voltage-high {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs the voltage is high.
snmp alarm-severity adva-voltage-low {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when ADVA informs the voltage is low.

If you want to clear a configured ADVA alarm prioirity, use the following command.

Command	Mode	Description
no snmp alarm-severity adva-fan-fail	Global	Clears a configured ADVA alarm prioirity.
no snmp alarm-severity adva-if-misconfig		
no snmp alarm-severity adva-if-opt-thres		
no snmp alarm-severity adva-if-rcv-fail		
no snmp alarm-severity adva-if-sfp-mismatch		
no snmp alarm-severity adva-if-trans-fault		
no snmp alarm-severity adva-psu-fail		
no snmp alarm-severity adva-temperature		
no snmp alarm-severity adva-voltage-high		
no snmp alarm-severity adva-voltage-low		

7.1.9.6 ERP Alarm Severity

To configure a severity of alarms for ERP status, use the following command.

Command	Mode	Description
snmp alarm-severity erp-domain-lotp {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sends alarm notification with the severity when no test packet has been received within 3 test packet intervals in ERP mechanism.
snmp alarm-severity erp-domain-multi-rm {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when a Multiple RM node is created.

Command	Mode	Description
snmp alarm-severity erp-domain-reach-fail {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sends alarm notification with the severity when there is disconnection between ERP domains
snmp alarm-severity erp-domain-ulotp {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when no test packet has been received within 3 test packet intervals in one ERP port while test packets are received in the other port with ERP state.

To delete a configured severity of alarm for ERP status, use the following command.

Command	Mode	Description
no snmp alarm-severity erp-domain-lotp	Global	Deletes a configured severity of alarm for ERP status.
no snmp alarm-severity erp-domain-multi-rm		
no snmp alarm-severity erp-domain-reach-fail		
no snmp alarm-severity erp-domain-ulotp		

7.1.9.7 STP Guard Alarm Severity

To configure a severity of alarm for STP guard status, use the following command.

Command	Mode	Description
snmp alarm-severity stp-bpdu-guard {**critical** | **major** | **minor** | **warning** | **intermediate**}	Global	Sends alarm notification with the severity when there is stp-bpdu-guard problem
snmp alarm-severity stp-root-guard {**critical** | **major** | **minor** | **warning** | **intermediate**}		Sends alarm notification with the severity when there is stp-root-guard problem

To delete a configured severity of alarm for STP guard status, use the following command.

Command	Mode	Description
no snmp alarm-severity stp-bpdu-guard	Global	Deletes a configured severity of alarm for STP guard status.
no snmp alarm-severity stp-root-guard		

7.1.10 Displaying SNMP Configuration

To display all configurations of SNMP, use the following command.

Command	Mode	Description
show snmp	Enable Global	Shows all configurations of SNMP.

To display a configured severity of alarm, use the following commands.

Command	Mode	Description
show snmp alarm-severity	Enable Global	Shows a configured severity of alarm.

To deletes a recorded alarm in the system, use the following command.

Command	Mode	Description
snmp clear alarm-history	Enable Global	Deletes a recorded alarm in the system.

The following is an example of showing the transmitted alarm and delete the records.

```
SWITCH(config)# show snmp alarm-history
cold-start         minor       Fri Mar 25 15:30:56 2005 System booted.
SWITCH(config)# snmp clear alarm-history
SWITCH(config)# show snmp alarm-history
SWITCH(config)#
```

To display a current alarm report, use the following command.

Command	Mode	Description
show snmp alarm-report	Enable Global	Shows a current alarm report.

To deletes a recorded alarm report in the system, use the following command.

Command	Mode	Description
snmp clear alarm-report	Enable Global	Deletes a recorded alarm report in the system.

7.1.11 Disabling SNMP

To disable SNMP feature, use the following command.

Command	Mode	Description
no snmp	Global	Disables SNMP feature.

When you use the above command, all configurations concerning SNMP will be deleted.

7.2 Operation, Administration and Maintenance (OAM)

In the enterprise, Ethernet links and networks have been managed via Simple Network Management Protocol (SNMP). Although SNMP provides a very flexible management solution, it is not always efficient and is sometimes inadequate to the task.

First, using SNMP assumes that the underlying network is operational because SNMP relies on IP connectivity; however, you need management functionality even more when the underlying network is non-operational. Second, SNMP assumes every device is IP accessible. This requires provisioning IP on every device and instituting an IP overlay network even if the ultimate end-user service is an Ethernet service. This is impractical in a carrier environment.

For these reasons, carriers look for management capabilities at every layer of the network. The Ethernet layer has not traditionally offered inherent management capabilities, so the IEEE 802.3ah Ethernet in the First Mile (EFM) task force added the Operations, Administration and Maintenance (OAM) capabilities to Ethernet like interfaces. These management capabilities were introduced to provide some basic OAM function on Ethernet media.

EFM OAM is complementary, not competitive, with SNMP management in that it provides some basic management functions at Layer 2, rather than using Layer 3 and above as required by SNMP over an IP infrastructure. OAM provides single-hop functionality in that it works only between two directly connected Ethernet stations. SNMP can be used to manage the OAM interactions of one Ethernet station with another.

7.2.1 OAM Loopback

For OAM loopback function, both the switch and the host should support OAM function. OAM loopback function enables Loopback function from the user's device to the host, which connected to the user's device and operates it.

To enable/disable local OAM function, use the following command.

Command	Mode	Description
oam local admin enable *PORTS*	Bridge	Enables local OAM.
oam local admin disable *PORTS*		Disables local OAM.

To configure loopback function of the host connected to the switch, use the following command.

Command	Mode	Description
oam remote loopback enable *PORTS*	Bridge	Enables loopback function of peer device.
oam remote loopback disable *PORTS*		Disables loopback function of peer device.
oam remote loopback start *PORTS*		Operates loopback.

7.2.2 Local OAM Mode

To configure Local OAM, use the following command.

Command	Mode	Description
oam local mode {**active** | **passive**} *PORTS*	Bridge	Configures the mode of local OAM.

i Both request and loopback are possible for local OAM active. However, request or loopback is impossible for local OAM passive.

7.2.3 OAM Unidirection

When RX is impossible in local OAM, it is possible to send the information by using TX. To enable/disable the function, use the following command.

Command	Mode	Description
oam local unidirection enable *PORTS*	Bridge	Sends the information by using TX.
oam local unidirection disable *PORTS*		Disables to transmit the information by using TX.

7.2.4 Remote OAM

To enable/disable remote OAM, use the following command.

Command	Mode	Description
oam remote oam admin <1-2> **enable** *PORTS*	Bridge	Enables remote OAM.
oam remote oam admin <1-2> **disable** *PORTS*		Disables remote OAM.

To configure the mode of remote OAM, use the following command.

Command	Mode	Description
oam remote oam mode <1-2> {**active** | **passive**} *PORTS*	Bridge	Configures the mode of remote OAM.

To display the information of peer host using OAM function, use the following command.

Command	Mode	Description
oam remote alarm optical <1-3> <0-65535> *PORTS*	Bridge	Shows the information of peer host using OAM function.
oam remote alarm temperature <0-255> *PORTS*		
oam remote alarm voltage {**min** | **max**} <0-65535> *PORTS*		
oam remote electrical mode {**full** | **half**} *PORTS*		
oam remote general autonego <1-4> {**enable** | **disable**} *PORTS*		
oam remote general forwarding <3-4> {**enable** | **disable**} *PORTS*		
oam remote general speed <1-4> <0-4294967295>*PORTS*		
oam remote general user <1-4> *STRING PORTS*		
oam remote system interface {**unforced** | **forceA** | **forceB**} *PORTS*		
oam remote system interval <0-255> *PORTS*		
oam remote system mode {**master** | **slave**} *PORTS*		
oam remote system reset *PORTS*		

7.2.5 Displaying OAM Configuration

To display OAM configuration, use the following command.

Command	Mode	Description
show oam	Enable Global Bridge	Shows OAM configuration.
show oam local [*PORTS*]		Shows local OAM configuration.
show oam remote [*PORTS*]		Shows remote OAM configuration.
show oam remote variable <0-255> <0-255> *PORTS*		Shows remote OAM variable.
show oam remote variable specific <0-255> <0-255> <0-4> *PORTS*		Shows remote OAM specific variable.

The following is to configure to enable OAM loopback function through 25 port of the switch and operate once.

```
SWITCH(bridge)# oam local admin enable 25
SWITCH(bridge)# oam remote loopback enable 25
SWITCH(bridge)# show oam local 25
  LOCAL PORT[25]
-----------------------------------------
      item       |     value
-----------------------------------------
  admin          |     ENABLE
  mode           |     ACTIVE
  mux action     |     FORWARD
  par action     |     DISCARD
  variable       |     UNSUPPORT
  link event     |     UNSUPPORT
  loopback       |     SUPPORT(disable)
  uni-direction  |     UNSUPPORT(disable)
-----------------------------------------
SWITCH(bridge)# show oam remote 25
  REMOTE PORT[25]
-----------------------------------------
      item       |     value
-----------------------------------------
  mode           |     ACTIVE
  MAC address    |     00:d0:cb:27:00:94
  variable       |     UNSUPPORT
  link event     |     UNSUPPORT
  loopback       |     SUPPORT(enable)
  uni-direction  |     UNSUPPORT
-----------------------------------------
SWITCH(bridge)# oam remote loopback start 25
PORT[25]: The remote DTE loopback is success.
SWITCH(bridge)#
```

7.3 Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) is the function of transmitting data for network management for the switches connected in LAN according to IEEE 802.1ab standard.

7.3.1 LLDP Operation

The hiD 6615 S223/S323 supporting LLDP transmits the management information between near switches. The information carries the management information that can recognize the switches and the function. This information is saved in internal MIB (Management Information Base)

When LLDP starts to operate, the switches send their information to near switches. If there is some change in local status, it sends their changed information to near switch to inform their status. For example, if the port status is disabled, it informs that the port is disabled to near switches. And the switch that receives the information from near switches processes LLDP frame and saves the information of the other switches. The information received from other switches is aged.

7.3.2 LLDP Operation Type

If you activated LLDP on a port, configure LLDP operation type.

Each LLDP operation type works as the follow:
- **both**: sends and receive LLDP frame.
- **tx_only**: only sends LLDP frame.
- **rx_only**: only receives LLDP frame.
- **disable**: does not process any LLDP frame.

To configure how to operate LLDP, use the following command.

Command	Mode	Description
lldp adminstatus *PORTS* {**both** | **tx_only** | **rx_only** | **disable**}	Bridge	Configurs LLDP operation type. (default: disable)

7.3.3 Basic TLV

LLDP is transmitted through TLV. There are mandatory TLV and optional TLV. In optional TLV, there are basic TLV and organizationally specific TLV. Basic TLV must be in the switch where LLDP is realized, specific TLV can be added according to the feature of the switch.

In hiD 6615 S223/S323, the administrator can enable and disable basic TLV by selecting it. To enable basic TLV by selecting it, use the following command.

Command	Mode	Description
lldp enable *PORTS* {**portdescription** | **sysname** | **sysdescription** | **syscap**}	Bridge	Selects basic TLV that is sent in the port. portdescription: Port's description syscap: System's capablility sysname: System's name sysdescription: System's description
lldp disable *PORTS* {**portdescription** | **sysname** | **sysdescription** | **syscap**}		Disables basic TLV configured as sent in the port.

7.3.4 LLDP Message

In hiD 6615 S223/S323, it is possible to configure the interval time and times of sending LLDP message. To configure the interval time and times of LLDP message, use the following command.

Command	Mode	Description
lldp msg txinterval <5-32768>	Bridge	Configures the interval of sending LLDP message. The unit is second.
lldp msg txhold <2-10>		Configures the periodic times of LLDP message.

i Default for sending LLDP message is 4 times in every 30 seconds.

7.3.5 Interval and Delay Time

In hiD 6615 S223/S323, the administrator can configure the interval time of enabling LLDP frame after configuring LLDP operation type. To configure the interval time of enabling LLDP frame after configuring LLDP operation type, use the following command.

Command	Mode	Description
lldp reinitdelay <1-10>	Bridge	Configures the interval time of enabling LLDP frame from the time of configuring not to process LLDP frame. (default: 2)

To configure delay time of transmitting LLDP frame, use the following command.

Command	Mode	Description
lldp txdelay <1-8192>	Bridge	Configures delay time of transmitting LLDP frame. (default: 2)

7.3.6 Displaying LLDP Configuration

To display LLDP configuration, use the following command.

Command	Mode	Description
show lldp config *PORTS*	Enable Global Bridge	Shows LLDP configuration.
show lldp remote *PORTS*		Show statistics for remote entries.
show lldp statistics *PORTS*		Shows LLDP operation and statistics.

To delete an accumulated statistics on the port, use the following command.

Command	Mode	Description
clear lldp statistics *PORTS*	Global Bridge	Deletes an accumulated statistics on the port.

The following is to configure to enable LLDP function on *Bridge Configuration* mode-through port number 10 of the switch and operate it.

```
SWITCH(bridge)# show lldp config 10
GLOBL:
-------------------------------------------------------------------------
MsgTxInterval   = 30
MsgTxHold      = 4   =>  txTTL = 120
ReInitDelay     = 2
TxDelay        = 2
-------------------------------------------------------------------------
PORTS active   adminStat|optTLVs
   10: disable    Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
SWITCH(bridge)# lldp enable 10
SWITCH(bridge)# lldp disable 10 portdescription
SWITCH(bridge)# lldp adminstatus 10 tx_only
SWITCH(bridge)# lldp msg txinterval 50
SWITCH(bridge)# lldp msg txhold 8
SWITCH(bridge)# show lldp config 10
GLOBL:
-------------------------------------------------------------------------
MsgTxInterval   = 50
MsgTxHold       = 8   =>  txTTL = 400
ReInitDelay     = 2
TxDelay         = 2
-------------------------------------------------------------------------
PORTS active   adminStat|optTLVs
  10: enable     Tx only |0xe= SysName, SysDesc, SysCap
SWITCH(bridge)#
```

7.4 Remote Monitoring (RMON)

Remote Monitoring (RMON) is a function to monitor communication status of devices connected to Ethernet at remote place. While SNMP can give information only about the device mounted SNMP agent, RMON gives information about overall segments including devices. Thus, user can manage network more effectively. For instance, in case of SNMP it is possible to be informed traffic about certain ports but through RMON you can monitor traffics occurred in overall network, traffics of each host connected to segment and current status of traffic between hosts.

Since RMON processes quite lots of data, its processor share is very high. Therefore, administrator should take intensive care to prevent performance degradation and not to overload network transmission caused by RMON. There are nine defined RMON MIB groups in RFC 1757: Statistics, History, Alarm, Host, Host Top N, Matrix, Filter, Packet Capture and Event. The system supports two MIB groups of them, most basic ones: Statistics (only for uplink ports) and History.

7.4.1 RMON History

RMON history is periodical sample inquiry of statistical data about each traffic occurred in Ethernet port. Statistical data of all ports are pre-configured to be monitored at 30-minute interval, and 50 statistical data stored in one port. It also allows you to configure the time interval to take the sample and the number of samples you want to save.

The following is an example of displaying the default configuration of RMON history.

```
SWITCH(config)# show rmon-history config 5

RMON History configuration:
===========================
history index      : 5
data source        : 0/1 (1)
buckets requested  : 50
buckets granted    : 50
interval time (s)  : 1800
owner              : none
status             : under create
SWITCH(config)#
```

To open *RMON-history* mode, use the following command.

Command	Mode	Description
rmon-history <1-65535>	Global	Opens *RMON-history Configuration* mode. 1-65535: index number

The following is an example of opening *RMON-history Configuration* mode with index number 5.

```
SWITCH(config)# rmon-history 5
SWITCH(config-rmonhistory[5])#
```

Input a question mark <**?**> at the system prompt on *RMON Configuration* mode if you

want to list available commands.

The following is an example of listing available commands on *RMON Configuration* mode.

```
SWITCH(config-rmonhistory[5])# ?
RMON history configuration commands:
  active              Activate the history
  data-source         Set data source port
  do                  To run exec commands in config mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  interval            Define the time interval for the history
  owner               Assign the owner who define and is using the history
                      resources
  requested-buckets   Define the bucket count for the interval
  show                Show running system information
SWITCH(config-rmonhistory[5])#
```

7.4.1.1 Source Port of Statistical Data

To specify a source port of statistical data, use the following command.

Command	Mode	Description
data-source *NAME*	RMON	Specifies a data object ID. NAME: enters a data object ID. (ex. ifindex.n1/port1)

7.4.1.2 Subject of RMON History

To identify subject using RMON history, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject using related data, enter the name (max. 32 characters).

7.4.1.3 Number of Sample Data

To configure the number of sample data of RMON history, use the following command.

Command	Mode	Description
requested-buckets <1-65535>	RMON	Defines a bucket count for the interval, enter the number of buckets. 1-65535: bucket number (default: 50)

7.4.1.4 Interval of Sample Inquiry

To configure the interval of sample inquiry in terms of second, use the following command.

Command	Mode	Description
interval <1-3600>	RMON	Defines the time interval for the history (in seconds), enter the value. (default: 1800)

i 1 sec is the minimum time which can be selected. But the minimum sampling interval currently is 30 sec, i.e., all intervals will be round up to a multiple of 30 seconds.

7.4.1.5 Activating RMON History

To activate RMON history, use the following command.

Command	Mode	Description
active	RMON	Activates RMON history.

i Before activating RMON history, check if your configuration is correct. After RMON history is activated, you cannot change its configuration. If you need to change configuration, you need to delete the RMON history and configure it again.

7.4.1.6 Deleting Configuration of RMON History

When you need to change a configuration of RMON history, you should delete an existing RMON history.

To delete RMON history, use the following command.

Command	Mode	Description
no rmon-history <1-65535>	RMON	Deletes RMON history of specified number, enter the value for deleting.

7.4.1.7 Displaying RMON History

To display RMON history, use the following command.

Command	Mode	Description
show running-config rmon-history	All	Shows a configured RMON history.

i Always the last values will be displayed but no more than the number of the granted buckets.

The following is an example of displaying RMON history.

```
SWITCH(config-rmonhistory [5])# show running-config rmon-history
!
rmon-history 5
 owner test
 data-source ifindex.hdlc1
 interval 60
 requested-buckets 25
 active
!
SWITCH(config-rmonhistory [5])#
```

7.4.2 RMON Alarm

There are two ways to compare with the threshold: absolute comparison and delta comparison.

- **Absolute Comparison**: Comparing sample data with the threshold at configured interval, if the data is more than the threshold or less than it, alarm is occurred
- **Delta Comparison**: Comparing difference between current data and the latest data with the threshold, if the data is more than the threshold or less than it, alarm is occurred.

You need to open *RMON Alarm Configuration* mode first to configure RMON alarm.

Command	Mode	Description
rmon-alarm <1-65535>	Global	Opens *RMON Alarm Configuration* mode. 1-65535: index number

The following is an example of listing available commands on *RMON-alarm Configuration* mode.

```
SWITCH(config)# rmon-alarm 1
SWITCH(config-rmonalarm[1])# ?

RMON alarm configuration commands:

  active              Activate the event
  do                  To run exec commands in config mode
  exit                End current mode and down to previous mode
  falling-event       Associate the falling threshold with an existing RMON
                      event
  falling-threshold   Define the falling threshold
  help                Description of the interactive help system
  owner               Assign the owner who define and is using the history
  resources
  rising-event        Associate the rising threshold with an existing RMON
                      event
  rising-threshold    Define the rising threshold
  sample-interval     Specify the sampling interval for RMON alarm
  sample-type         Define the sampling type
  sample-variable     Define the MIB Object for sample variable
  show                Show running system information
  startup-type        Define startup alarm type (default : rising)
  write               Write running configuration to memory or terminal
SWITCH(config-rmonalarm[1])#
```

7.4.2.1 Subject of RMON Alarm

User needs to configure RMON alarm and identify subject using many kinds of data from alarm. To identify subject of alarm, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject using related data, enter the name (max. 32 characters).

7.4.2.2 Object of Sample Inquiry

User needs object value used for sample inquiry to provide RMON Alarm. The following is rule of object for sample inquiry. To assign object used for sample inquiry, use the following command.

Command	Mode	Description
sample-variable *MIB-OBJECT*	RMON	Assigns MIB object used for sample inquiry.

7.4.2.3 Absolute Comparison and Delta Comparison

It is possible to select the way to compare MIB object used for sample inquiry in case of configuring RMON Alarm. Absolute comparison directly compares object selected as sample with the threshold. For instance, when you want to know the point of 30,000 times of sample inquiry, if you configure apSvcConnections as 30,000, it is for Absolute comparison. To compare object selected as sample with the threshold, use the following command.

Command	Mode	Description
sample-type absolute	RMON	Compares object with the threshold directly.

Delta comparison compares difference between current data and the latest data with the threshold. For instance, in order to know the point of variable notation rule 100,000 more than the former rule, configure apCntHits as Delta comparison. To configure delta comparison, use the following command.

Command	Mode	Description
sample-type delta	RMON	Compares difference between current data and the latest data with the threshold.

7.4.2.4 Upper Bound of Threshold

If you need to occur alarm when object used for sample inquiry is more than upper bound of threshold, you have to configure the upper bound of threshold. To configure upper bound of threshold, use the following command.

Command	Mode	Description
rising-threshold *VALUE*	RMON	Configures upper bound of threshold. VALUE: 0-2147483647

After configuring upper bound of threshold, configure to generate RMON event when object is more than configured threshold. Use the following command.

Command	Mode	Description
rising-event <1-65535>	RMON	Configures to generate RMON event when object is more than configured threshold. 1-65535: event index

7.4.2.5 Lower Bound of Threshold

If you need to occur alarm when object used for sample inquiry is less than lower bound of threshold, you should configure lower bound of threshold. To configure lower bound of threshold, use the following command.

Command	Mode	Description
falling-threshold *NUMBER*	RMON	Configures lower bound of threshold.

After configuring lower bound of threshold, configure to generate RMON event when object is less than configured threshold. Use the following command.

Command	Mode	Description
falling-event <1-65535>	RMON	Configures to generate RMON alarm when object is less than configured threshold.

7.4.2.6 Configuring Standard of the First Alarm

It is possible for users to configure the standard the first time alarm is occurred. The user can select the first point when object is more than threshold, or the first point when object is less than threshold, or the first point when object is more than threshold or less than threshold.

To configure the first RMON alarm to occur when object is less than lower bound of threshold first, use the following command.

Command	Mode	Description
startup-type falling	RMON	Configures the first RMON Alarm to occur when object is less than lower bound of threshold first.

To configure the first alarm to occur when object is firstly more than upper bound of threshold, use the following command.

Command	Mode	Description
startup-type rising	RMON	Configures the first Alarm to occur when object is firstly more than upper bound of threshold.

To configure the first alarm to occur when object is firstly more than threshold or less than threshold, use the following command.

Command	Mode	Description
startup-type rising-and-falling	RMON	Configures the first Alarm to occur when object is firstly more than threshold or less than threshold.

7.4.2.7 Interval of Sample Inquiry

The interval of sample inquiry means time interval to compare selected sample data with upper bound of threshold or lower bound of threshold in terns of seconds.

To configure interval of sample inquiry for RMON alarm, use the following command.

Command	Mode	Description
sample-interval <0-65535>	RMON	Configures interval of sample inquiry. (unit: second)

7.4.2.8 Activating RMON Alarm

After finishing all configurations, you need to activate RMON alarm. To activate RMON alarm, use the following command.

Command	Mode	Description
active	RMON	Activates RMON alarm.

7.4.2.9 Deleting Configuration of RMON Alarm

When you need to change a configuration of RMON alarm, you should delete an existing RMON alarm.

To delete RMON alarm, use the following command.

Command	Mode	Description
no rmon-alarm <1-65535>	Global	Deletes RMON history of specified number, enter the value for deleting.

7.4.2.10 Displaying RMON Alarm

To display RMON alarm, use the following command.

Command	Mode	Description
show running-config rmon-alarm	All	Shows a configured RMON alarm.

7.4.3 RMON Event

RMON event identifies all operations such as RMON alarm in the switch. You can configure event or trap message to be sent to SNMP management server when sending RMON alarm.

You need to open *RMON Event Configuration* mode to configure RMON event.

Command	Mode	Description
rmon-event <1-65535>	Global	Opens *RMON Event Configuration* mode. 1-65535: index number

7.4.3.1 Event Community

When RMON event is happened, you need to input community to transmit SNMP trap message to host. Community means a password to give message transmission right.

To configure community for trap message transmission, use the following command.

Command	Mode	Description
community *NAME*	RMON	Configures password for trap message transmission right. NAME: community name

7.4.3.2 Event Description

It is possible to describe event briefly when event is happened. However, the description will not be automatically made. Thus administrator should make the description.

To make a description about event, use the following command.

Command	Mode	Description
description *DESCRIPTION*	RMON	Describes the event. Max: 126 character

7.4.3.3 Subject of RMON Event

You need to configure event and identify subject using various data from event. To identify subject of RMON event, use the following command.

Command	Mode	Description
owner *NAME*	RMON	Identifies subject of event. You can use maximum 126 characters and this subject should be same with the subject of RMON alarm.

7.4.3.4 Event Type

When RMON event happened, you need to configure event type to arrange where to send event.

To configure event type, use the following command.

Command	Mode	Description
type log	RMON	Configures event type as log type. Event of log type is sent to the place where the log file is made.
type trap		Configures event type as trap type. Event of trap type is sent to SNMP administrator and PC.
type log-and-trap		Configures event type as both log type and trap type.
type none		Configures none event type.

7.4.3.5 Activating RMON Event

After finishing all configurations, you should activate RMON event. To activate RMON event, use the following command.

Command	Mode	Description
active	RMON	Activates RMON event.

7.4.3.6 Deleting Configuration of RMON Event

Before changing the configuration of RMON event, you should delete RMON event of the number and configure it again.

To delete RMON event, use the following command.

Command	Mode	Description
no rmon-event <1-65535>	Global	Delete RMON event of specified number.

7.4.3.7 Displaying RMON Event

To display RMON alarm, use the following command.

Command	Mode	Description
show running-config rmon-event	All	Shows a configured RMON event.

7.5 Syslog

The syslog is a function that allows the network element to generate the event notification and forward it to the event message collector like a syslog server. This function is enabled as default, so even though you disable this function manually, the syslog will be enabled again.

This section contains the following contents.

- Syslog Output Level
- Facility Code
- Syslog
- Disabling Syslog
- Displaying Syslog Message
- Displaying Syslog Configuration

7.5.1 Syslog Output Level

Syslog Output Level without a Priority

To set a syslog output level, use the following command.

Command	Mode	Description
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **console**	Global	Generates a syslog message of selected level or higher and forwards it to the console.
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **local** {**volatile** | **non-volatile**}		Generates a syslog message of selected level or higher in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **remote** *IP-ADDRESS*		Generates a syslog message of selected level or higher and forwards it to a remote host.

To disable a specified syslog output, use the following command.

Command	Mode	Description
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **console**	Global	Deletes a specified syslog output.
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **local** {**volatile** | **non-volatile**}		
no syslog output {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info** | **debug**} **remote** *IP-ADDRESS*		

Syslog Output Level with a Priority

To set a user-defined syslog output level with a priority, use the following command.

Command	Mode	Description
syslog output priority {**auth** | **authpriv** | **cron** | **daemon** | **kern** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **console**	Global	Generates a user-defined syslog message with a priority and forwards it to the console.
syslog output priority {**auth** | **authpriv** | **cron** | **daemon** | **kern** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **local** {**volatile** | **non-volatile**}		Generates a user-defined syslog message with a priority in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
syslog output priority {**auth** | **authpriv** | **cron** | **daemon** | **kern** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **remote** *IP-ADDRESS*		Generates a user-defined syslog message with a priority and forwards it to a remote host.

To disable a user-defined syslog output level, use the following command.

Command	Mode	Description
no syslog output priority {**auth** | **authpriv** | **cron** | **daemon** | **kern** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **console**	Global	Deletes a specified user-defined syslog output level with a priority.
no syslog output priority {**auth** | **authpriv** | **cron** | **daemon** | **kern** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **local** {**volatile** | **non-volatile**}		
no syslog output priority {**auth** | **authpriv** | **cron** | **daemon** | **kern** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**} {**emerg** | **alert** | **crit** | **err** | **warning** | **notice** | **info**} **remote** *IP-ADDRESS*		

i The order of priority is **emergency** > **alert** > **critical** > **error** > **warning** > **notice** > **info** > **debug**. If you set a specific level of syslog output, you will receive only a syslog message for selected level or higher. If you want receive a syslog message for all the levels, you need to set the level to **debug**.

The following is an example of configuring syslog message to send all logs higher than notice to remote host 10.1.1.1 and configuring local1.info to transmit to console.

```
SWITCH(config)# syslog output notice remote 10.1.1.1
SWITCH(config)# syslog output priority local1 info console
SWITCH(config)# show syslog
System logger on running!

info                local volatile
info                local non-volatile
notice              remote 10.1.1.1
local1.info         console
SWITCH(config)#
```

7.5.2 Facility Code

You can set a facility code of the generated syslog message. This code make a syslog message distinguished from others, so network administrator can handle various syslog messages efficiently.

To set a facility code, use the following command.

Command	Mode	Description
syslog local-code <0-7>	Global	Sets a facility code.
no syslog local-code		Deletes a specified facility code.

The following is an example of configuring priority of all syslog messages which is transmitted to remote host 10.1.1.1, as the facility code 0.

```
SWITCH(config)# syslog output err remote 10.1.1.1
SWITCH(config)# syslog local-code 0
SWITCH(config)# show syslog
System logger on running!

info                local volatile
info                local non-volatile
err                 remote 10.1.1.1
local_code          0
SWITCH(config)#
```

7.5.3 Syslog Bind Address

You can specify IP address to attach to the syslog message for its identity. To specify IP address for syslog identity, use the following command.

Command	Mode	Description
syslog bind-address *A.B.C.D*	Global	Specifies IP address for a syslog message identity.
no syslog bind-address		Deletes a specified binding IP address.

7.5.4 Debug Message for Remote Terminal

To display a syslog debug message to a remote terminal, use the following command.

Command	Mode	Description
terminal monitor	Enable	Enables a terminal monitor function.
no terminal monitor		Disables a terminal monitor function.

i Terminal monitor is not possible to be operational in local console.

7.5.5 Disabling Syslog

To disable the syslog manually, use the following command.

Command	Mode	Description
no syslog	Global	Disables the syslog.

7.5.6 Displaying Syslog Message

To display a received syslog message in the system memory, use the following command.

Command	Mode	Description
show syslog local {**volatile** | **non-volatile**} [*NUMBER*]	Enable Global	Shows a received syslog message. volatile: removes a syslog message after restart. non-volatile: reserves a syslog message. NUMBER: shows the last N syslog messages.
show syslog local {**volatile** | **non-volatile**} **reverse**		Shows the syslog messages from the latest one.
clear syslog local {**volatile** | **non-volatile**}	Enable Global	Removes a received syslog message.

7.5.7 Displaying Syslog Configuration

To display a configuration of the syslog, use the following command.

Command	Mode	Description
show syslog	Enable Global	Shows a configuration of the syslog.
show syslog {**volatile** | **non-volatile**} **information**		

7.6 Rule and QoS

The hiD 6615 S223/S323 provides rule and QoS feature for traffic management. The rule classifies incoming traffic, and then processes the traffic according to user-defined policies. You can use the physical port, 802.1p priority (CoS), VLAN ID, DSCP, and so on to classify incoming packets.

You can configure the policy in order to change some data fields within a packet or to relay packets to a mirror monitor by a “Rule” function. QoS (Quality of Service) is one of useful functions to provide the more convenient service of network traffic for users. It is very serviceable to prevent overloading and delaying or failing of sending traffic by giving priority to traffic.

By the way, you need to be careful for other traffics not to be failed by the traffic configured as priority by user. QoS can give a priority to a specific traffic by basically offering the priority to the traffic or limiting the others. When processing data, data are usually supposed to be processed in time-order like first in, first out.

This way, not processing specific data first, might lose all data in case of overloading traffics. However, in case of overloading traffics QoS can apply processing order to traffic by reorganizing priorities according to its importance. By favor of QoS, you can predict network performance in advance and manage bandwidth more effectively.

7.6.1 How to Operate Rule and QoS

For the hiD 6615 S223/S323, rules operate as follows.

- Rule Creation
  To classify the packets according to the specific basis, configure the policies about them first. The basis used to classify the packets is 802.1p priority (CoS), VLAN ID, DSCP and port number. Additionally, a unique name needs to be assigned to each rule.
- Rule Priority
  Assigns a priority to a rule (precedence to other rules).
- Packet Classification
  Configures the policy to adjust how and what is to be classified within transmitted packets.
- Rule Match
  Configures the policy classifying the action(s) to be performed if the configured rule classification fits transmitted packet(s).
  − **mirror** transmits the classified traffic to monitor port.
  − **redirect** transmits the classified traffic to specified port.
  − **permit** allows traffic matching given characteristics.
  − **deny** blocks traffic matching given characteristics.
- Rule Apply
  Applies the just configured rule. Configured values will be checked and the rule becomes activated within the system.

An already applied rule can not be modified. It needs to be deleted and then created again with changed values.

- Scheduling Algorithm
  To handle overloading of traffics, you need to configure differently processing orders of graphic by using scheduling algorithm. The hiD 6615 S223/S323 provides:
  − Strict Priority Queuing (SPQ)
  − Weighted Round Robin (WRR)
  − Weighted Fair Queuing (WFQ).
- Queue Weight
  Queue weight can be used to additionally adjust the scheduling mode per queue in WRR or WFQ mode.
  − Queue weight controls the scheduling precedence of the internal packet queues. The higher the weight value the higher the scheduling precedence of this queue.

7.6.2 Rule Configuration

7.6.2.1 Rule Creation

For the hiD 6615 S223/S323, you need to open *Rule Configuration* mode first. To open *Rule Configuration* mode, use the following command.

Command	Mode	Description
rule *NAME* **create**	Global	Opens *Rule Configuration* mode, enter rule name.

After opening *Rule Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-rule[name])#.

After opening *Rule Configuration* mode, a rule can be configured by user. The rule priority, rule match, rule action, and action parameter(s) can be configured for each rule.

1. The rule name must be unique. Its size is limited to 63 significant characters.
2. The order in which the following configuration commands will be entered is arbitrary.
3. The configuration of a rule being configured can be changed as often as wanted (inclusive rule type) until the command, **apply**, will be entered.
4. Use the command, **show rule-profile**, to display the configuration entered up to now.

You can not create the rule name which started with alphabet ‘a’ If you try to enter ‘a’, the error message will be appeared. .

7.6.2.2 Rule Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first.

To set a priority for a rule, use the following command.

Command	Mode	Description
priority {**low** | **medium** | **high** | **highest**}	Rule	Sets a priority for a rule.

7.6.2.3 Packet Classification

After configuring a packet classification for a rule, then configure how to process the packets. To specify a packet-classifying pattern, use the following command.

When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

Command	Mode	Description
port {*SRC-PORT* | **any**} {*DST-PORT* | **cpu** | **any**}	Rule	Classifies a physical port: SRC-PORT: source port number DST-PORT: destination port number cpu: CPU port any: any physical port (ignore)
vlan {*VID* | **any**}		Classifies a VLAN: VLAN: 1-4094 any: any VLAN (ignore)
dscp {<0-63> | **any**}		Classifies a DSCP value: 0-63: DSCP value any: any DSCP (ignore)
cos {<0-7> | **any**}		Classifies the IEEE 802.1p priority: 0-7: 802.1p priority value any: any 802.1p priority value (ignore)
tos {<0-255> | **any**}		Classifies all ToS field: 0-255: ToS value any: any ToS value (ignore)
ip-prec {<0-7> | **any**}		Classifies an IP precedence: 0-7: IP precedence value any: any IP precedence value (ignore)
length {<21-65535> | **any**}		Classifies a packet length: 21-65535: IP packet length any: any IP packet length (ignore)
ethtype {*TYPE-NUM* | **arp** | **any**}		Classifies the Ethernet type: TYPE-NUM: Ethernet type field (hex, e.g. 0800 for IPv4) arp: address resolution protocol any: any Ethernet type (ignore)
mac {*SRC-MAC-ADDRESS* | *SRC-MAC-ADDRESS / MASK-BITS* | **any**} {*DST-MAC-ADDRESS* I*DST-MAC-ADDRESS/ MASK BITS* I **any**}		Classifies MAC address: SRC-MAC-ADDRESS: source MAC address DST-MAC-ADDRESS: destination MAC address any: any source/destination MAC address (ignore)
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} [0-255]		Classifies an IP address: A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number

Command	Mode	Description
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp**	Rule	Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp** {<0-255> | **any**} [<0-255> | **any**]		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP 0-255: ICMP message type number 0-255: ICMP message code number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**} {<0-65535> | **any**} {<0-65535> | **any**}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP 0-65535: TCP/UDP source/destination port number any: any TCP/UDP source/destination port
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **tcp** {<0-65535> | **any**} {<0-65535> | **any**} {*TCP-FLAG* | **any**}		Classifies an IP protocol (TCP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP 0-65535: TCP source/destination port number any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag

To delete a specified packet-classifying pattern, use the following command.

Command	Mode	Description
no vlan	Rule	Deletes a specified packet-classifying pattern for each option.
no cos		
no tos		
no length		
no ethtype		
no mac		
no ip		

7.6.2.4 Rule Action

To specify a rule action (**match**) for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
match deny	Rule	Denies a packet.
match permit		Permits a packet.
match redirect *PORT*		Redirects to specified egress port: PORT: uplink port number
match mirror		Sends a copy to mirror monitoring port.
match dscp <0-63>		Changes DSCP field, enter DSCP value.
match cos <0-7>		Changes 802.1p class of service, enter CoS value. 0-7: CoS value
match cos <0-7> **overwrite**		Overwrites 802.1p CoS field in the packet. 0-7: CoS value
match cos same-as-tos overwrite		Overwrites 802.1p CoS field in the packet same as IP ToS precedence bits.
match ip-prec <0-7>		Changes IP ToS precedence bits in the packet. 0-7: ToS precedence value
match ip-prec same-as-cos		Changes IP ToS precedence bits in the packet, same as 802.1p CoS value.
match bandwidth *BANDWIDTH*		Determines maximum allowed bandwidth (Mbps).
match vlan <1-4094>		Specifies matched-packet VLAN ID 1-4094: VLAN ID
match copy-to-cpu		Copies to CPU.
match counter		Counts how many times the packets come into configured Rule.
match egress filter *PORT*		Deletes a specified egress port.
match egress port *PORT*		Overwrites a specified egress port

To delete a specified rule action (**match**), use the following command.

Command	Mode	Description
no match deny	Rule	Deletes a specified rule action.
no match permit		
no match redirect		
no match mirror		
no match dscp		
no match cos		
no match ip-prec		
no match bandwidth		
no match vlan		
no match copy-to-cpu		
no match counter		
no match egress		

To specify a rule action (**no-match**) for the packets **not** matching configured classifying patterns, use the following command.

Command	Mode	Description
no-match deny	Rule	Denies a packet.
no-match redirect *PORT*		Redirects to specified egress port: PORT: uplink port number (e.g. 25-28)
no-match mirror		Sends a copy to mirror monitoring port.
no-match dscp <0-63>		Changes DSCP field, enter DSCP value.
no-match cos <0-7>		Changes 802.1p class of service, enter CoS value. 0-7: CoS value
no-match cos <0-7> **overwrite**		Overwrites 802.1p CoS field in the packet. 0-7: CoS value
no-match cos same-as-tos-over-write		Overwrites 802.1p CoS field in the packet same as IP ToS precedence bits.
no-match ip-prec <0-7>		Changes IP ToS precedence bits in the packet. 0-7: ToS precedence value
no-match ip-prec same-as-cos		Changes IP ToS precedence bits in the packet, same as 802.1p CoS value.
no-match copy-to-cpu		Copies to CPU.

To delete a specified rule action (**no-match**), use the following command.

Command	Mode	Description
no no-match deny	Rule	Deletes a specified rule action.
no no-match redirect		
no no-match mirror		
no no-match dscp		
no no-match cos		
no no-match ip-prec		
no no-match copy-to-cpu		

7.6.2.5 Applying Rule

After configuring rule using the above commands, apply it to the system with the following command. If you do not apply the rule to the system, all specified rules will be lost.

To save and apply a rule, use the following command.

Command	Mode	Description
apply	Rule	Applies a rule to the system.

i

1. The switch performs a detailed plausibility check and rejects the rule if the configuration is incomplete, contains bad or unsupported values or conflicts to other rules. In this case, the switch informs about the reason and the operator may correct the values
2. The switch may reject a rule with the message “% Already exist rule” allthough the name will not be listed by command, **show rule**. Unfortunately, the entered name in this case interferes with the name of an internally managed rule.
   Remedy: Select another name for the rule (e.g. add a prefix).
3. All previously entered values remain valid after successful (or unsuccessful) execution of command, **apply**. That is, if several rules being different only in one value should be created, then only the one changed value needs to be entered again.

7.6.2.6 Modifying and Deleting Rule

To modify a rule, use the following command.

Command	Mode	Description
rule *NAME* **modify**	Global	Modifies a rule, enter a rule name.

To delete a rule, use the following command.

Command	Mode	Description
no rule [*NAME*]	Global	Deletes a rule, enter a rule name optionally.

7.6.2.7 Displaying Rule

The following command can be used to show a certain rule by its name, all rules of a certain type, or all rules at once sorted by rule type.

Command	Mode	Description
show rule *NAME*	Enable Global	Shows a rule, enter a rule name. NAME: rule name
show rule		Shows all rules sorted by type.
show rule all		Shows all rules and admin access rules sorted by type.
show rule statistics		Shows rule statistics.
show rule-profile	Rule	Shows a current configuration of a rule.

The following is an example of configuring specific rule action on rule profile and showing it.

```
SWITCH# configure terminal
SWITCH(config)# rule jean create
SWITCH(config-rule[jean])# priority low
SWITCH(config-rule[jean])# match copy-to-cpu
SWITCH(config-rule[jean])# apply
SWITCH(config-rule[jean])# exit
SWITCH(config)# rule jean create
% Already exist rule
SWITCH(config)# show rule
rule jean
  priority low
  port any any
  match copy-to-cpu
SWITCH(config)# rule jean modify
SWITCH(config-rule[jean])no match copy-to-cpu
SWITCH(config-rule[jean]) show rule
rule jean
  priority low
  port any any
SWITCH(config-rule[jean])
```

7.6.3 QoS

For hiD 6615 S223/S323, it is possible to use Strict Priority Queuing, Weighted Round Robin and Weighted Fair Queuing for a packet scheduling mode.

The following steps explain how QoS can be configured.

- Scheduling Algorithm
- Qos Weight
- 802.1p Priory-to-queue Mapping
- Queue Parameter
- Displaying QoS

7.6.3.1 Scheduling Algorithm

To process incoming packets by the queue scheduler, the hiD 6615 S223/S323 provides the scheduling algorithm as Strict Priority Queuing (SP), Weighted Round Robin (WRR) and Weighted Fair Queuing (WFQ).

Weighted Round Robin (WRR)

WRR processes packets as much as weight. Processing the packets that have higher priority is the same way as strict priority queuing. However, it passes to next stage after processing as configured weight so that it is possible to configure for packet process not to be partial to the packets having higher priority. However, there is a limitation of providing differentiated service from those existing service.

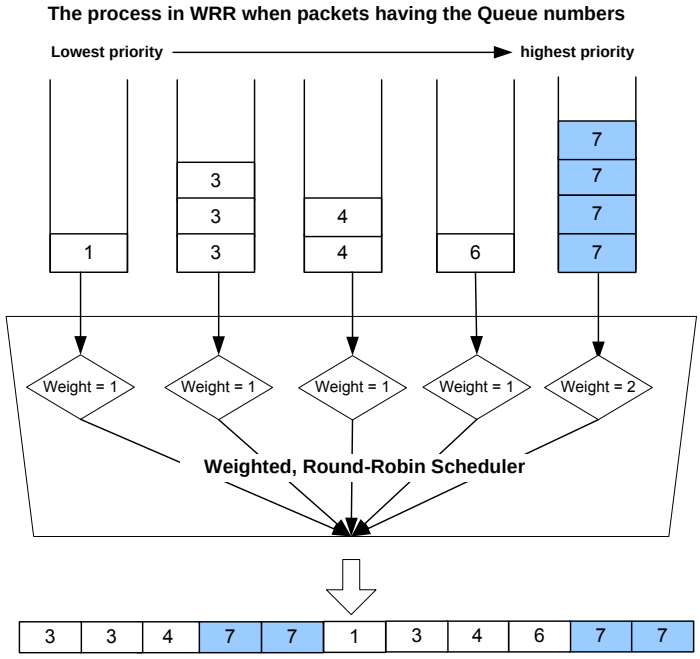


Fig. 7.1 Weighted Round Robin

Weighted Fair Queuing (WFQ)

Weighted fair queuing (WFQ) provides automatically sorts among individual traffic streams without requiring that you first define access lists. It can manage one way or two way streams of data: traffic between pairs of applications or voice and video.

In WFQ, packets are sorted in weighted order of arrival of the last bit, to determine transmission order. Using order of arrival of last bit emulates the behavior of Time Division Multiplexing (TDM), hence "fair"

From one point of view, the effect of this is that WFQ classifies sessions as high- or low-bandwidth. Low-bandwidth traffic gets priority, with high-bandwidth traffic sharing what's left over. If the traffic is bursting ahead of the rate at which the interface can transmit, new high-bandwidth traffic gets discarded after the configured or default congestive-messages threshold has been reached. However, low-bandwidth conversations, which include control-message conversations, continue to enquire data.

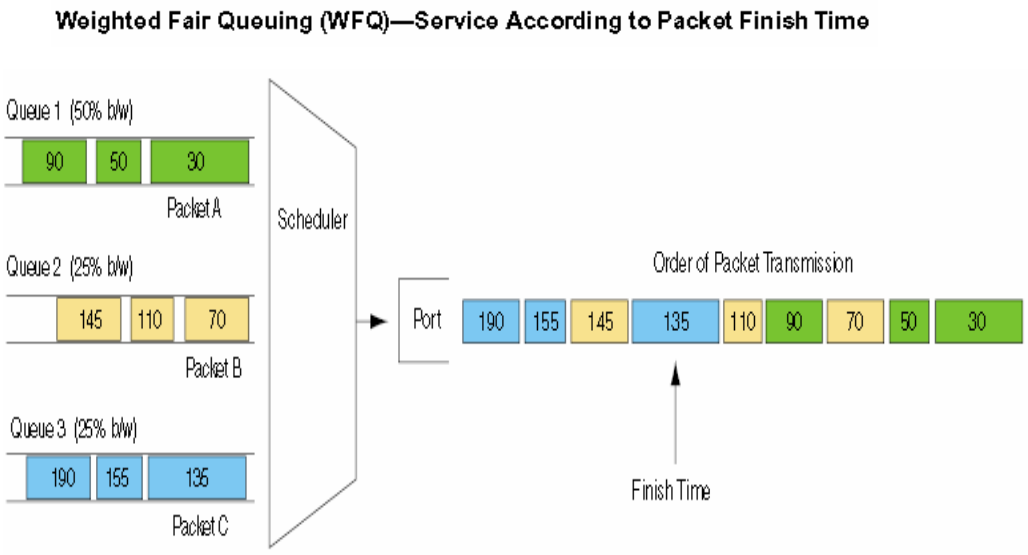


Fig. 7.2 Weighted Fair Queuing

Strict Priority Queuing (SP)

SPQ processes first more important data than the others. Since all data are processed by their priority, data with high priority can be processed fast but data without low priority might be delayed and piled up. This method has a strong point of providing the distinguished service with a simple way. However, if the packets having higher priority enter, the packets having lower priority are not processed.

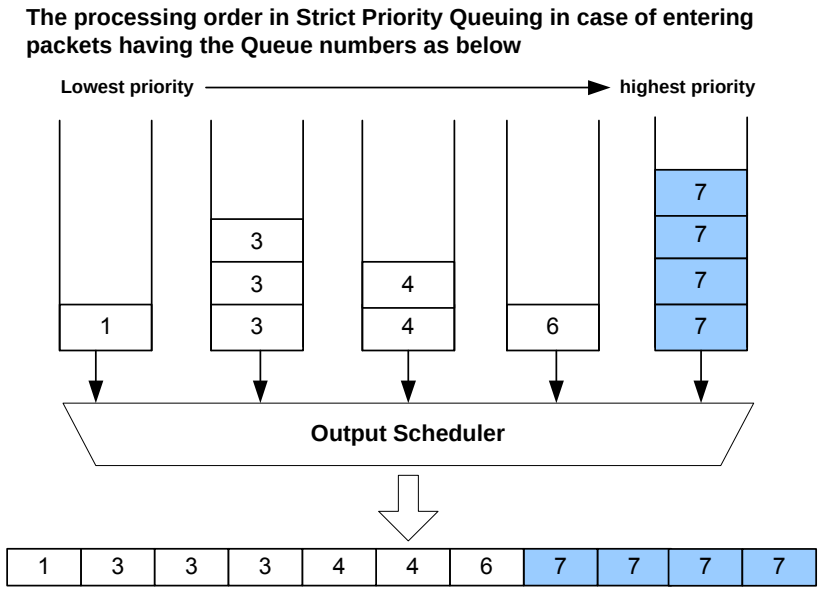


Fig. 7.3 Strict Priority Queuing

To select a packet scheduling mode, use the following command.

Command	Mode	Description
qos scheduling-mode {**sp** | **wrr**}	Global	Selects a packet scheduling mode for a ports: sp: strict priority queuing wrr: weighted round robin
qos cpu scheduling-mode sp		Selects a scheduling mode for handling CPU packets sp: strict priority queuing

i The default scheduling mode is **WRR**. And it is possible to assign a different scheduling mode to each port.

7.6.3.2 Qos Weight

To set a weight for WRR scheduling mode only, use the following command.

Command	Mode	Description
qos weight *PORTS* <0-3> {<1-15> | **unlimited**}	Global	Sets a weight for each port and queue: PORTS: port numbers 0-7: queue number 1-15: weight value (default: 1) unlimited: strict priority queuing

7.6.3.3 802.1p Priory-to-queue Mapping

For the hiD 6615 S223/S323, it is possible to configure how packets having a certain 802.1p priority will be stored into which queue. Default mapping is shown as below (default values).

CoS (802.1p Priority)	Description	Queue Mapping (8 Queues)	Reduced Queue Mapping (4 Queues)
0	Lowest: Best Effort IP (be)	2	1
1	Background (bg)	0	0
2	Spare (spare)	1	0
3	Excellent Effort (ee)	3	1
4	Controlled Load (cl)	4	2
5	Video (video)	5	2
6	Voice (voice)	6	3
7	Highest: Network Control (ctrl)	7	3

Tab. 7.1 Default 802.1p Priory-to-queue Map

To define an 802.1p priory-to-queue map for 8 queues, use the following command.

Command	Mode	Description
qos map <0-7> <0-3>	Global	Priority to queue number mapping, priority value (0-7) according to 802.1p: 0 = lowest: best effort (be) 1: background (bg) 2: spare (spare) 3: excellent effort (ee) 4: controlled load (cl) 5: video (video) 6: voice (voice) 7: network control (ctrl) Queue value: 0-3: queue number

7.6.3.4 Queue Parameter

To configure a queue parameter, use the following command.

Command	Mode	Description
qos ibp *PORTS* <1-8191>	Global	Sets a ingress back-pressure: PORTS: port numbers
qos pktlimit *PORTS* <0-3> <4-2047>		Sets a maximum packet size per queue for egress port: PORTS: port numbers 0-3: queue number
qos seglimit *PORTS* <0-3> <1-8191>		Sets a maximum segment per queue for egress port: PORTS: port numbers 0-3: queue number
no qos ibp *PORTS*		Restroes it as a default.
no qos pktlimit *PORTS* <0-3>		
no qos seglimit *PORTS* <0-3>		

7.6.3.5 Displaying QoS

To display a configuration of QoS, enter following command.

Command	Mode	Description
show qos	Enable Global Bridge	Shows the configuration of QoS for all ports.
show qos *PORTS*		Shows the configuration of QoS per each port.
show qos buffer *PORTS*		Shows the configuration of a buffer per each port.
show qos cpu		Shows the configuration of QoS for CPU packets.

7.6.4 Admin Access Rule

For the hiD 6615 S223/S323, it is possible to block a specific service connection like telnet, FTP, ICMP, etc with an admin access rule function.

7.6.4.1 Rule Creation

For the hiD 6615 S223/S323, you need to open *Admin Access Rule Configuration* mode first. After opening *Admin Access Rule Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-admin-rule[NAME])#.

To open *Rule Configuration* mode, use the following command.

Command	Mode	Description
rule *NAME* **create admin**	Global	Opens *Admin Access Rule Configuration* mode, enter rule name.

After opening *Admin Access Rule Configuration* mode, a rule can be configured by user. The rule priority, packet classification and rule action(s) can be configured for each rule.

1. The rule name must be unique. Its size is limited to 63 significant characters.
2. The order in which the following configuration commands will be entered is arbitrary.
3. The configuration of a rule being configured can be changed as often as wanted (inclusive rule type) until the command, **apply**, will be entered.
4. Use the command, **show rule-profile**, to display the configuration entered up to now.

7.6.4.2 Rule Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first.

To set a priority for an admin access rule, use the following command.

Command	Mode	Description
priority {**low** | **medium** | **high** | **highest**}	Admin-rule	Sets a priority for a rule. (Defaul: low)

7.6.4.3 Packet Classification

After configuring a packet classification for a rule, then configure how to process the packets. To specify a packet-classifying pattern, use the following command.

When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

Command	Mode	Description
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} [0-255]	Admin-rule	Classifies an IP address: A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp**		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **icmp** {<0-255> | **any**} {<0-255> | **any**}		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP 0-255: ICMP message type number 0-255: ICMP message code number
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} {**tcp** | **udp**} {<1-65535> | **any**} {<1-65535> | **any**}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP 0-65535: TCP/UDP source/destination port number any: any TCP/UDP source/destination port
ip {*A.B.C.D* | *A.B.C.D/M* | **any**} {*A.B.C.D* | *A.B.C.D/M* | **any**} **tcp** {<0-65535> | **any**} {<0-65535> | **any**} {*TCP-FLAG* | **any**}		Classifies an IP protocol (TCP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP 0-65535: TCP source/destination port number any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag

7.6.4.4 Rule Action

To specify a rule action (**match**) for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
match deny	Admin-rule	Denies a packet.
match permit		Permits a packet.

To delete a specified rule action (**match**), use the following command.

Command	Mode	Description
no match deny	Admin-rule	Deletes a specified rule action.
no match permit		

To specify a rule action (**no-match**) for the packets **not** matching configured classifying patterns, use the following command.

Command	Mode	Description
no-match deny	Admin-rule	Denies a packet.
no-match permit		Permits a packet.

To delete a specified rule action (**no-match**), use the following command.

Command	Mode	Description
no no-match deny	Admin-rule	Deletes a specified rule action.
no no-match permit		

7.6.4.5 Applying Rule

After configuring rule using the above commands, apply it to the system with the following command. If you do not apply a rule to the system, all specified rules will be lost.

To save and apply an admin access rule, use the following command.

Command	Mode	Description
apply	Admin-rule	Applies an admin access rule to the system.

i

1. The switch performs a detailed plausibility check and rejects the rule if the configuration is incomplete, contains bad or unsupported values or conflicts to other rules. In this case, the switch informs about the reason and the operator may correct the values
2. The switch may reject a rule with the message “% Already exist rule” allthough the name will not be listed by command, **show rule**. Unfortunately, the entered name in this case interferes with the name of an internally managed rule.
   Remedy: Select another name for the rule (e.g. add a prefix).
3. All previously entered values remain valid after successful (or unsuccessful)

execution of command, **apply**. That is, if several rules being different only in one value should be created, then only the one changed value needs to be entered again.

7.6.4.6 Modifying and Deleting Rule

To modify a rule, use the following command.

Command	Mode	Description
rule *NAME* **modify admin**	Global	Modifies an admin access rule, enter a rule name.

To delete a rule, use the following command.

Command	Mode	Description
no rule admin	Global	Deletes an admin access rule, enter a rule name optionally.
no rule all		Deletes all rules and admin access rules.

7.6.4.7 Displaying Rule

The following command can be used to show a certain rule by its name, all rules of a certain type, or all rules at once sorted by rule type.

Command	Mode	Description
show rule admin	Enable Global	Shows all admin access rules sorted by type.
show rule all		Shows all rules and admin access rules sorted by type.
show rule statistics		Shows rule statistics.
show rule-profile	Admin-rule	Shows a current configuration of a rule.

7.7 NetBIOS Filtering

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN). NetBIOS is used in Ethernet, included as part of NetBIOS Extended User Interface (NetBEUI). Resource and information in the same network can be shared with this protocol.

But the more computers are used recently, the more strong security is required. To secure individual customer's information and prevent information leakages in the LAN environmen, the hiD 6615 S223/S323 provides NetBIOS filtering function.

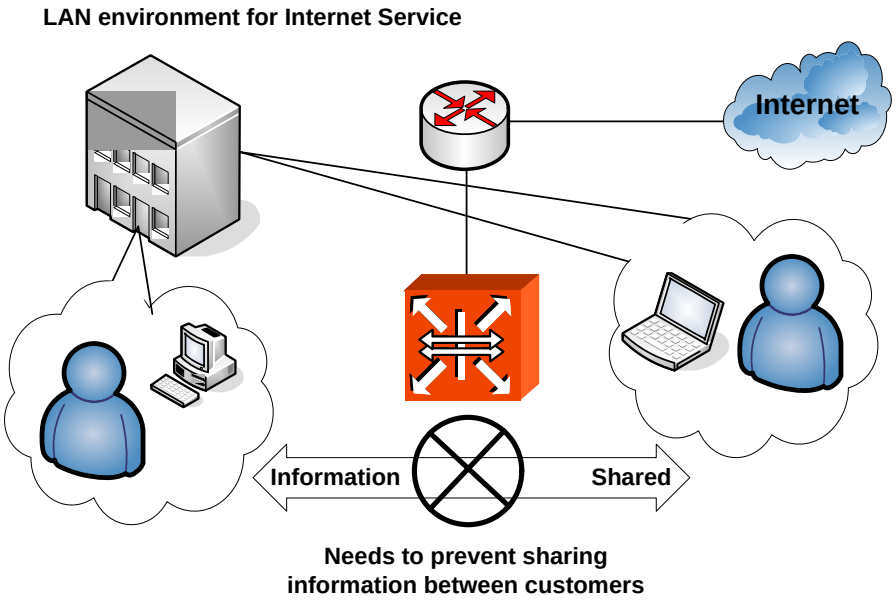


Fig. 7.4 NetBIOS Filtering

Without NetBIOS filtering, customer's data may be opened to each other even though the data should be kept. To keep customer's information and prevent sharing information in the above case, NetBIOS filtering is necessary.

Command	Mode	Description
netbios-filter *PORTS*	Bridge	Configures NetBIOS filtering to a specified port.

To disable NetBIOS filtering according to user's request, use the following command.

Command	Mode	Description
no netbios-filter *PORTS*	Bridge	Disables NetBIOS filtering from a specified port.

To display a configuration of NetBIOS filtering, use the following command.

Command	Mode	Description
show netbios-filter	Global Bridge	Shows a configuration of NetBIOS filtering.

The following is an example of configuring NetBIOS filtering in port 1~5 and showing it.

```
SWITCH(bridge)# netbios-filter 1-5
SWITCH(bridge)# show netbios-filter
o:enable .:disable
-------------------------
       1       2
12345678901234567890123456|
-------------------------
ooooo.....................
-------------------------
SWITCH(bridge)#
```

7.8 Martian Filtering

It is possible to block packets, which trying to bring different source IP out from same network. If packet brings different IP address, not its source IP address, then it is impossible to know it makes a trouble. Therefore, you would better prevent this kind of packet outgoing from your network. This function is named as Martian filter.

To block packets which try to bring different source IP out from same network, use the following command.

Command	Mode	Description
ip martian-filter *INTERFACE*	Global	Blocks packets which bring different source IP address from specified interface. INTERFACE: enter the interface name.

i It is not possible to configure both QoS and Martian filter at the same time.

To disable the configured Martian filter function, use the following command.

Command	Mode	Description
no ip martian-filter *INTERFACE*	Global	Disables a configured Martian filter function. INTERFACE: enter an interface name.

i To see a configuration of Martian filter, use the **show running-config** command.

7.9 Max Host

You can limit the number of users by configuring maximum number of users also named as max hosts for each port. In this case, you need to consider not only the number of PCs in network but also devices such as switches in network.

For the hiD 6615 S223/S323, you have to lock the port like MAC filtering before configuring max hosts. In case of ISPs, it is possible to arrange billing plan for each user by using this configuration.

To configure max host, use the following command.

Command	Mode	Description
max-hosts *PORTS* <1-16>	Bridge	Limits the number of connection to a port by setting maximum host: PORTS: enter the port number. 1-16: enter the maximum MAC number.
no max-hosts *PORTS*		Deletes configured max-host, enter the port number.

The following is an example of configuring to allow two MAC addresses to port 3, and five addresses to port 1, 2, and to ten addresses to port 7.

```
SWITCH(bridge)# max-hosts 3 2
SWTICH(bridge)# max-hosts 1 5
SWTICH(bridge)# max-hosts 2 5
SWTICH(bridge)# max-hosts 7 10
SWTICH(bridge)#
```

To display configured max host, use the following command.

Command	Mode	Description
show max-hosts	Enable Global Bridge	Shows configured max host.

The following is an example of displaying configured max hosts.

```
SWITCH(bridge)# show max-hosts
port  1 :     0/5          (current/max)
port  2 :     0/5          (current/max)
port  3 :     0/2          (current/max)
port  4 :     0/Unlimited (current/max)
port  5 :     0/Unlimited (current/max)
port  6 :     0/Unlimited (current/max)
port  7 :     0/10         (current/max)
port  8 :     0/Unlimited (current/max)
port  9 :     0/Unlimited (current/max)
port 10 :     0/Unlimited (current/max)
```

7.9.1 Max New Hosts

Max-new-hosts feature is to limit the number of users by configuring the number of MAC address that can be learned on the system and on the port for a second. The number of MAC address that can be learned on the system has the priority.

To configure max new hosts, use the following command.

Command	Mode	Description
max-new-hosts *PORTS MAX-MAC-NUMBER*	Bridge	The number of MAC address that can be learned on the port for a second.
max-new-hosts system *PORTS MAX-MAC-NUMBER*		The number of MAC address that can be learned on the system for a second.

To delete configured max new hosts, use the following command.

Command	Mode	Description
no max-new-hosts *PORTS*	Bridge	Deletes the number of MAC address that can be learned on the port.
no max-new-hosts system		Deletes the number of MAC address that can be learned on the system.

To display configured max new hosts, use the following command.

Command	Mode	Description
show max-new-hosts	Enable Global Bridge	Shows the configured Max-new-hosts.

If MAC that already counted disappears before passing 1 second and starts learning again, it is not counted. In case the same MAC is detected on the other port also, it is not counted again. For example, if MAC that was learned on port 1 is detected on port 2, it is supposed that MAC moved to the port 2. So, it is deleted from the port 1 and learned on the port 2 but it is not counted.

7.10 Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the PCs that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the PC attached to that port is assured the full bandwidth of the port.

7.10.1 Port Security on Port

Step 1
Enable port security on the port.

Command	Mode	Description
port security *PORTS*	Bridge	Enables port security on the port. PORT: selects port number

Step 2
Set the maximum number of secure MAC address for the port.

Command	Mode	Description
port security *PORTS* **maximum** <1-16384>	Bridge	Sets a maximum number of secure MAC address for the port. 1-16384: Maximum number of addresses (default: 1)

Step 3
Set the violation mode and the action to be taken.

Command	Mode	Description
port security *PORTS* **violation** {**shutdown** | **protect** | **restrict**}	Bridge	Selects a violation mode.

When configuring port security, note that the following information about port security violation modes:

- **protect** drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict** drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the Security Violation counter to increment.
- **shutdown** puts the interface into the error-disabled state immediately and sends an SNMP trap notification

Step 4
Enter a secure MAC address for the port.

Command	Mode	Description
port security *PORTS* **mac-address** *MACADDR* **vlan** *NAME*	Bridge	Sets a secure MAC address for the port. PORTS: select the port number. MACADDR: enter the MAC address. NAME: vlan name

To disable the configuration of port secure, use the following command.

Command	Mode	Description
no port security *PORTS*	Bridge	Disables port security on the port.
no port security *PORTS* **mac-address** *MACADDR* **vlan** *NAME*		Deletes a secure MAC address for the port. PORTS: enter the port number MACADDR: enter the MAC address.
no port security *PORTS* **maximum**		Returns to the default number of secure MAC address. (default: 1)
no port security *PORTS* **violation**		Returns to the violation mode to the default. (shutdown mode)

To display the configuration of port security, use the following command.

Command	Mode	Description
show port security [*PORTS*]	Bridge	Shows port security on the port.

This is an example of configuring port security on port 7.

```
SWITCH(config)# bridge
SWITCH(bridge)# port security 7
SWITCH(bridge)# port security 7 maximum 10000
SWITCH(bridge)# port security 7 violation protect
SWITCH(bridge)# port security 7 mac-address 00:02:a5:74:9b:17 vlan 1
SWITCH(bridge)# show port security 7
=============================================================================
port  security  violation  aging    type     static   maximum  current
=============================================================================
  7   enabled   protect      -   absolute       -     10000       1
=============================================================================
port    vlan    secure-mac-addr        status      in use
=============================================================================
  7       1    00:02:a5:74:9b:17      static          -
SWITCH(bridge)# no port security 7 maximum
SWITCH(bridge)# no port security 7 violation
SWITCH(bridge)# show port security 7
=============================================================================
port  security  violation  aging    type     static   maximum  current
=============================================================================
  7   enabled   shutdown     -   absolute       -         1       0
=============================================================================
port    vlan    secure-mac-addr        status      in use
=============================================================================
SWITCH(bridge)#
```

7.10.2 Port Security Aging

Port security aging is to set the aging time for all secure addresses on a port. Use this feature to remove and add PCs on a secure port without manually deleting the existing secure MAC addresses while still limiting the number of secure addresses on a port.

Command	Mode	Description
port security *PORTS* **aging static**	Bridge	Enables aging for configured secure addresses.
port security *PORTS* **aging time** <1-1440>		Configures aging time in minutes for the port. All the secure addresses age out exactly after the time.
port security *PORTS* **aging type** {**absolute** | **inactivity**}		Configures aging type.

- **absolute** all the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list.
- **inactivity** the secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.

To disable the configuration of port secure aging, use the following command.

Command	Mode	Description
no port security *PORTS* **aging static**	Bridge	Disables aging for only statistically configured secure addresses.
no port security *PORTS* **aging time**		Disables port secure aging for all secure addresses on a port.
no port security *PORTS* **aging type**		Returns to the default condition. (absolute)

To display the configuration of port security, use the following command.

Command	Mode	Description
show port security [*PORTS*]	Enable Global Bridge	Shows port security on the port.

7.11 MAC Table

A dynamic MAC address is automatically registered in the MAC table, and it is removed if there is no access to/from the network element corresponding to the MAC address during the specified MAC aging time. On the other hand, a static MAC address is manually registered by user. This will not removed regardless of the MAC aging time before removing it manually.

To manage MAC table in the switch, use the following command.

Command	Mode	Description
mac *NAME PORT MACADDR*	Bridge	Specifies a static MAC address in the MAC table. NAME: enter the bridge name. PORT: enter the port number. MACADDR: enter the MAC address.
mac aging-time <10-21474830>		Specifies MAC aging time: 10-21474830: aging time (default: 300)

To remove registered dynamic MAC addresses from the MAC table, use the following command.

Command	Mode	Description
clear mac	Enable Global Bridge	Clears dynamic MAC addresses.
clear mac *NAME*		Clears dynamic MAC addresses.
clear mac *NAME PORT*		Clears dynamic MAC addresses. NAME: enter the bridge name. PORT: enter the port number.
clear mac *NAME PORT MACADDR*		Clears dynamic MAC addresses. NAME: enter the bridge name. PORT: enter the port number. MACADDR: enter the MAC address.

To remove static MAC addresses manually registered by user from the MAC table, use the following command.

Command	Mode	Description
no mac	Bridge	Deletes static MAC addresses.
no mac *NAME*		Deletes static MAC addresses, enter the bridge name.
no mac *NAME PORT*		Deletes static MAC addresses. NAME: enter the bridge name. PORT: enter the port number.
no mac *NAME PORT MACADDR*		Deletes a specified static MAC address. NAME: enter the bridge name. PORT: enter the port number. MACADDR: enter the MAC address.

To display a MAC table in the switch, use the following command.

Command	Mode	Description
show mac *NAME* [*PORT*]	Enable Global Bridge	Shows switch MAC address, selection by port number (subscriber port only): NAME: enter the bridge name PORT: select the port number.

There are more than a thousand of MAC addresses in MAC table. And it is difficult to find information you need at one sight. So, the system shows certain amount of addresses displaying –**more**– on standby status. Press any key to search more. After you find the information, you can go back to the system prompt without displaying the other table by pressing <**q**>.

7.12 MAC Filtering

It is possible to forward frame to MAC address of destination. Without specific performance degradation, maximum 4,096 MAC addresses can be registered.

7.12.1 Default Policy of MAC Filtering

The basic policy of filtering based on system is set to allow all packets for each port. However the basic policy can be changed for user's requests.

After configuring basic policy of filtering for all packets, use the following command on Bridge mode to show the configuration.

Command	Mode	Description
mac-filter default-policy {**deny** | **permit**} *PORTS*	Bridge	Configures basic policy of MAC Filtering in specified port.

By default, basic filtering policy provided by system is configured to permit all packets in each port.

Sample Configuration

This is an example of blocking all packets in port 1~3 and port 7.

```
SWTICH(bridge)#  mac-filter default-policy deny 5-10
SWTICH(bridge)#  mac-filter default-policy permit 2
SWTICH(bridge)# show mac-filter default-policy
  -------------------------
  PORT POLICY | PORT POLICY
  ------------+------------
     1 PERMIT |    2 PERMIT
     3 PERMIT |    4 PERMIT
     5  DENY  |    6  DENY
     7  DENY  |    8  DENY
     9  DENY  |   10  DENY
    11 PERMIT |   12 PERMIT
    13 PERMIT |   14 PERMIT
    15 PERMIT |   16 PERMIT
    17 PERMIT |   18 PERMIT
    19 PERMIT |   20 PERMIT
    21 PERMIT |   22 PERMIT
    23 PERMIT |   24 PERMIT
    25 PERMIT |   26 PERMIT
    27 PERMIT |   28 PERMIT
SWITCH(bridge)#
```

7.12.2 Adding Policy of MAC Filter

You can add the policy to block or to allow some packets of specific address after configuring the basic policy of MAC Filtering. To add this policy, use the following commands on *Bridge Configuration* mode.

Command	Mode	Description
mac-filter add *MACADDR* {**deny** | **permit**}	Bridge	Allows or blocks packet which brings configured mac address to specified port.

Variable MAC-ADDRESS is composed of twelve digits number in Hexa decimal. It is possible to check it by using the **show mac** command. 00:d0:cb:06:01:32 is an example of MAC address.

7.12.3 Deleting MAC Filter Policy

To delete MAC filtering policy, use the following command.

Command	Mode	Description
mac-filter del *SOURCE-MACADDR* [<1-4094>]	Bridge	Deletes filtering policy for specified MAC address.

To delete MAC filtering function, use the following command.

Command	Mode	Description
no mac-filter	Bridge	Deletes all MAC filtering functions.

7.12.4 Listing of MAC Filter Policy

If you need to make many MAC filtering policies at a time, it is hard to input command one by one. In this case, it is more convenient to save MAC filtering policies at “/etc/mfdb.conf” and display the list of MAC filtering policy. To view the list of MAC filtering policy at /etc/mfdb.conf, use the following command.

Command	Mode	Description
mac-filter list	Bridge	Shows the list of MAC filtering policy at /etc/mfdb.conf.

7.12.5 Displaying MAC Filter Policy

To show a configuration about MAC filter policy, use the following command.

Command	Mode	Description
show mac-filter default-policy	Enable / Global / Bridge	Shows MAC filter policy.
show mac-filter		

Sample Configuration

The latest policy is recorded as number 1. The following is an example of permitting MAC address 00:02:a5:74:9b:17 and 00:01:a7:70:01:d2 and showing table of filter policy.

```
SWITCH(bridge)# mac-filter add 00:02:a5:74:9b:17 permit
SWITCH(bridge)# mac-filter add 00:01:a7:70:01:d2 permit
SWITCH(bridge)# show mac-filter
================================
 ID |        MAC      | ACTION
================================
   1  00:01:a7:70:01:d2   PERMIT
   2  00:02:a5:74:9b:17   PERMIT
SWITCH(bridge)#
```

The following is an example of displaying one configuration.

```
SWITCH(bridge)# show mac-filter 1
================================
 ID |        MAC      | ACTION
================================
   1  00:01:a7:70:01:d2   PERMIT
SWITCH(bridge)#
```

7.13 Address Resolution Protocol (ARP)

Device connected to IP network has two addresses, LAN address and network address. LAN address is sometimes called as data link because it is used in Layer 2 level, but more commonly the address is known as MAC address. Ethernet Switch needs 48-bit-MAC address to transmit packets. In this case, the process of finding proper MAC address from IP address is called as address resolution.

On the other hand, the progress of finding proper IP address from MAC address is called as reverse address resolution. Siemens switches find MAC address from IP address through address resolution protocol (ARP).

This chapter consists of these sections:
- ARP Table
- ARP Alias
- Gratuitous ARP
- Proxy-ARP

7.13.1 ARP Table

Hosts typically have an ARP table, which is a cache of IP/MAC address mappings. The ARP Table automatically maps the IP address to the MAC address of a switch. In addition to address information, the table shows the age of the entry in the table, the encapsulation method, and the switch interface (VLAN ID) where packets are forwarded.

The hiD 6615 ARP saves IP/MAC addresses mappings in ARP table for quick search. Referring to the information in ARP table, packets attached IP address is transmitted to network. When configuring ARP table, it is possible to do it only in some specific interfaces.

7.13.1.1 Registering ARP Table

The contents of ARP table are automatically registered when MAC address corresponds to MAC address is founded. The network administrator could use MAC address of specific IP address in Network by registering on ARP table.

To make specific IP address to be accorded with MAC address, use the following command.

Command	Mode	Description
arp *A.B.C.D MACADDR*	Global	Sets a static ARP entry, enter the IP address and the MAC address. MACADDR: enter the MAC address.
arp *A.B.C.D MACADDR INTERFACE*		Sets a static ARP entry, enter the IP address, the MAC address and enter an interface name. INTERFACE: enter an interface name. MACADDR: enter the MAC address.

To delete registered IP address and MAC address or change all the contents of ARP table, use one of the following command.

Command	Mode	Description
no arp *A.B.C.D*	Global	Negates a command or set sets its default
no arp *A.B.C.D INTERFACE*		Negates a command or set sets its default, enter the IP address and enter the interface name.
clear arp	Enable Global	Deletes all the contents of ARP table.
clear arp *INTERFACE*		Deletes all the contents of ARP table, enter the interface name.

7.13.1.2 Displaying ARP Table

To display ARP table registered in switch, use one of the following command.

Command	Mode	Description
show arp	Enable Global	Shows ARP table.
show arp {*INTERFACE* | *A.B.C.D*}		Shows ARP table for specified interface, enter the interface name or IP address. (br1, br2, ...).

The following is an example of registering 10.1.1.1 as IP address and 00:d0:cb:00:00:01 as MAC address. This command displays ARP table.

```
SWITCH(config)# arp 10.1.1.1 00:d0:cb:00:00:01
SWITCH(config)# show arp
------------------------------------------------------------
   Address            HWaddress         Type     Interface
------------------------------------------------------------
10.254.254.105     00:bb:cc:dd:ee:05    DYNAMIC     br4094
10.2.2.1           00:00:cd:01:82:d0    DYNAMIC     br2
SWITCH(config)#
```

7.13.2 ARP Alias

Although clients are joined in same client switch, it may be impossible to communicate between clients for their private security. When you need to make them communicate each other, the hiD 6615 S223/S323 supports ARP alias, which responses ARP request from client net through concentrating switch.

To register address of client net range in ARP alias, use the following command.

Command	Mode	Description
arp-alias *A.B.C.D A.B.C.D* [*MACADDR*]	Global	Registers IP address range and MAC address in ARP alias to make user's equipment response ARP request.

i Unless you input MAC address, MAC address of user's equipment will be used for ARP response.

To delete registered IP address range of ARP alias, use the following command.

Command	Mode	Description
no arp-alias *START-IP-ADDRESS END-IP-ADDRESS*	Global	Deletes a registered IP address range of ARP alias.

To display ARP alias, use the following command.

Command	Mode	Description
show arp-alias	Enable Global	Shows a registered ARP alias.

7.13.3 ARP Inspection

ARP provides IP communication by mapping an IP address to a MAC address. But a malicious user can attack ARP caches of systems by intercepting traffic intended for other hosts on the subnet. For example, Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. If Host C responses with an IP address of Host A (or B) and a MAC address of Host C, Host A and Host B can use Host C's MAC address as the destination MAC address for traffic intended for Host A and Host B.

ARP Inspection is a security feature that validates ARP packets in a network. It intercepts and discards ARP packets with invalid IP-MAC address binding.

To enable and disable ARP Inspection on the hiX 5430 system, use the following command.

Command	Mode	Description
ip arp inspection vlan *VLAN*	Global	Enables ARP-inspection function on a VLAN.
no ip arp inspection vlan *VLAN*		Disables ARP-inspection function on a VLAN.

You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP address and the source MAC address.

Command	Mode	Description
ip arp inspection validate {**src-mac** | **dst-mac** | **ip**}	Global	Inspects specific check on incoming ARP packets. src-mac: checks the source MAC address. Packets with different MAC addresses are classified as invalid are dropped. dst-mac: checks the destination MAC address. Packets with different MAC addresses are classified as invalid are dropped. ip: checks the unexpected IP address.
ip arp inspection filter *NAME* **vlan** *VLAN*		Applies ARP ACL to the VLAN. NAME: ARP ACL name. It is created with the **arp access-list** *NAME* command.
ip arp inspection trust port *PORTS*		Configures a connection between switches as trusted. PORTS: trusted port number.

To remove the specific ARP Inspection configuration, use the following commands

Command	Mode	Description
no ip arp inspection validate {**src-mac** | **dst-mac** | **ip**}	Global	Removes specific ARP inspection configuration.
no ip arp inspection filter *NAME* **vlan** *VLAN*		
no ip arp inspection trust port *PORTS*		

To display checking and statistics, use the following command.

Command	Mode	Description
show ip arp inspection [**vlan** *VLAN*]	Enable Global Bridge	Displays the information of ARP inspection.
show ip arp inspection statistics [**vlan** *VLAN*]		
show ip arp inspection trust [**port** *PORTS*]		

To clear ARP inspection mapping counter and statistics, use the following command.

Command	Mode	Description
clear ip arp inspection statistics [**vlan** *VLAN*]	Global Bridge	Clears ARP inspection statistics.

7.13.4 Gratuitous ARP

Gratuitous ARP is a broadcast packet like an ARP request. It containing IP address and MAC address of gateway, and the network is accessible even though IP addresses of specific host's gateway are repeatedly assigned to the other.

Configure Gratuitous ARP interval and transmission count using following commands. And configure transmission delivery-start in order to transmit Gratuitous ARP after ARP reply.

Gratuitous ARP is transmitted after some time from transmitting ARP reply.

Command	Mode	Description
arp-patrol *TIME COUNT* [*TIME*]	Global	Configures a gratuitous ARP. TIME: transmit interval COUNT: transmit count
no arp-patrol		Disables a gratuitous ARP.

The following is an example of configuring the transmission interval as 10 sec and transmission times as 4 and showing it.

```
SWITCH(config)# arp-patrol 10 4
SWITCH(config)# show running-config
Building configuration...
Current configuration:
hostname SWITCH
(Omitted)
arp-patrol 10 4
!
no snmp
!
SWITCH(config)#
```

7.13.5 Proxy-ARP

To configure Proxy-ARP, you need to enter *Interface configuration* mode and use the following command.

Command	Mode	Description
ip proxy-arp	Interface	Sets proxy-ARP at specified Interface
no ip proxy-arp		Removes the configured proxy-ARP from the interface.

7.14 ICMP Message Control

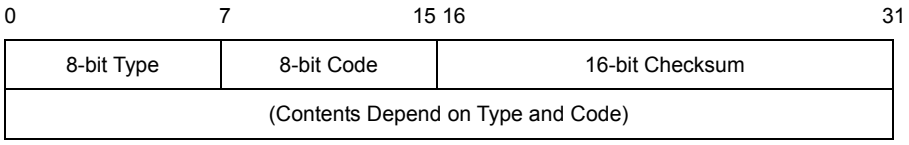
ICMP stands for Internet Control Message Protocol. When it is impossible to transmit data or configure route for data, ICMP sends error message about it to host. The first 4 bytes of all ICMP messages are same, but the other parts are different ac-cording to type field value and code field value. There are fifteen values of field to distinguish each different ICMP message, and code field value helps to distinguish each type in detail.

The following table shows explanation for fifteen values of ICMP message type.

Type	Value	Type	Value
ICMP_ECHOREPLY	0	ICMP_DEST_UNREACH	3
ICMP_SOURCE_QUENCH	4	ICMP_REDIRECT	5
ICMP_ECHO	8	ICMP_TIME_EXCEEDED	11
ICMP_PARAMETERPROB	12	ICMP_TIMESTAMP	13
ICMP_TIMESTAMPREPLY	14	ICMP_INFO_REQUEST	15
ICMP_INFO_REPLY	16	ICMP_ADDRESS	17
ICMP_ADDRESSREPLY	18		

Tab. 7.2 ICMP Message Type

The following figure shows simple ICMP message construction.



It is possible to control ICMP message through user's configuration. You can configure to block the echo reply message to the partner who is doing ping test to device and interval to transmit ICMP message.

7.14.1 Blocking Echo Reply Message

It is possible to configure block echo reply message to the partner who is doing ping test to switch. To block echo reply message, use the following commands.

Command	Mode	Description
ip icmp ignore echo all	Global	Blocks echo reply message to all partners who are taking ping test to device.
ip icmp ignore echo broadcast		Blocks echo reply message to partner who is taking broadcast ping test to device.

To release the blocked echo reply message, use the following commands.

Command	Mode	Description
no ip icmp ignore echo all	Global	Releases blocked echo reply message to all partners who are taking ping test to device.
no ip icmp ignore echo broadcast		Releases blocked echo reply message to partner who is taking broadcast ping test to device.

7.14.2 Interval for Transmit ICMP Message

User can configure the interval for transmit ICMP message. After you configure the interval, ICMP message will be blocked until the period based on the last message is up. For example, if you configure the interval as 1 second, ICMP will not be sent within 1 second after the last message has been sent.

To configure interval to transmit ICMP message, the administrator should configure the type of message and the interval time.

Use the following command, to configure the interval for transmit ICMP message.

Command	Mode	Description
ip icmp interval rate-mask *MASK*	Global	Configures the interval for transmit ICMP message. MASK: user should input hexadecimal value until 0xFFFFFFFF. The default is 0x1818.

If mask that is input as hexadecimal number is calculated as binary number “1” means “Status ON”, “0” means “Status OFF”. In binary number, if the digit showed as “1” matches with the value of ICMP message. It means ICMP Message is selected as “Status ON”. Digit value starts from 0.

For example, if hexadecimal number “8” is changed as binary number, it is “1000”. In 1000, 0 digit is “0” and 1 digit is “0”, 2 digit is “0” and 3 digit is “1”. The digit showed as “1” is “3” and ICMP_DEST_UNREACH means ICMP value is “3”. Therefore, ICMP_DEST_UNREACH is chosen the message of limiting the transmission time.

Default is 0x1818. If 1818 as hexadecimal number is changed as binary number, it is 1100000011000. By calculating from 0 digit, 3 digit, 4 digit, 11 digit, 12 digit is “1” and it is “STATUS ON”. Therefore, the message that corresponds to 3, 4, 11, and 12 is chosen as the message limiting the transmission rate.

Tab. 7.3 shows the result of mask calculation of default value.

Type	Status
ICMP_ECHOREPLY (0)	OFF
ICMP_DEST_UNREACH (3)	ON
ICMP_SOURCE_QUENCH (4)	ON
ICMP_REDIRECT (5)	OFF
ICMP_ECHO (8)	OFF
ICMP_TIME_EXCEEDED (11)	ON
ICMP_PARAMETERPROB (12)	ON
ICMP_TIMESTAMP (13)	OFF
ICMP_TIMESTAMPREPLY (14)	OFF
ICMP_INFO_REQUEST (15)	OFF
ICMP_INFO_REPLY (16)	OFF
ICMP_ADDRESS (17)	OFF
ICMP_ADDRESSREPLY (18)	OFF

Tab. 7.3 Mask Calculation of Default Value

To configure the limited ICMP transmission time, use the following command.

Command	Mode	Description
ip icmp interval rate-limit *INTERVAL*	Global	Configures a limited ICMP transmission time. INTERVAL: 0-2000000000 (unit: 10 ms)

i The default ICMP interval is 1 second (100 ms).

To return to default ICMP configuration, use the following command.

Command	Mode	Description
ip icmp interval default	Global	Returns to default configuration.

To display ICMP interval configuration, use the following command.

Command	Mode	Description
show ip icmp interval	Enable Global	Shows ICMP interval configuration.

7.14.3 Transmitting ICMP Redirect Message

User can configure to transmit ICMP Redirect Message. Transmitting ICMP Redirect Message is one of the ways preventing DoS(Denial of Service), and this can make the switch provide the constant service to the hosts.SURPASS hiD 6615 transmits more optimized route to the host than the present route between the host connected to the switch and the specific destination.

To activate the function transmitting ICMP Redirect Message, use the following command.

Command	Mode	Description
ip redirects	Global	Activates the function transmitting ICMP Redirect Message
no ip redirecs		Deactivates the function transmitting ICMP Redirect Message.

The following is an example for configuring ICMP Redirect Message and checking the configuration.

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

(omitted)

interface 1
 ip address 222.121.68.247/24
!
!
!
SWITCH(config)# ip redirects
SWITCH(config)# show running-config

(omitted)

interface 1
 ip address 222.121.68.247/24
!!
ip redirects
!
!
SWITCH(config)#
```

7.14.4 The policy of unreached messages

When the packets can't reach Destination host or the network, the switch is supposed to bring them back to the source IP address. What if too many unreached packets are coming into the system, it might cause slow down the system operation.

Not to bring these messages back to source IP address on a specific interface, use the following command on *Interface Configuration* mode.

Command	Mode	Description
ip unreachables	Interface	Configures not to bring unreached messages back to their source IP address on interface.
no ip unreachables		Brings all unreached messages back to their source IP address on interface.

7.15 IP TCP Flag Control

TCP (Transmission Control Protocol) header includes six kinds of flags that are URG, ACK, PSH, RST, SYN, and FIN. For the hiD 6615 S223/S323, you can configure RST and SYN as the below.

7.15.1 RST Configuration

RST sends a message when TCP connection can not be done to a person who tries to make it. However, it is also possible to configure to block the message. This function will

help prevent that hackers can find impossible connections.

To configure not to send the message that informs TCP connection can not be done, use the following command.

Command	Mode	Description
ip tcp ignore rst-unknown	Global	Configures to block the message that informs TCP connection can not be done.
no ip tcp ignore rst-unknown		Responds the message again that informs TCP connection is not possible.

7.15.2 SYN Configuration

SYN sets up TCP connection. The hiD 6615 S223/S323 transmits cookies with SYN to a person who tries to make TCP connection. And only when transmitted cookies are returned, it is possible to permit TCP connection. This function prevents connection overcrowding because of accessed users who are not using and helps the other users use service.

To permit connection only when transmitted cookies are returned after sending cookies with SYN, use the following command.

Command	Mode	Description
ip tcp syncookies	Global	Permits only when transmitted cookies are returned after sending cookies with SYN.
no ip tcp syncookies		Disables configuration to permit only when transmitted cookies are returned after sending cookies with SYN.

7.16 Packet Dump

Failures in network can occur by certain symptom. Each symptom can trace to one or more problems by using specific troubleshooting tools. The hiD 6615 S223/S323 switch provides the debug command to dump packet. Use debug commands only for problem isolation. Do not use it to monitor normal network operation. The debug commands produce a large amount of processor overhead.

7.16.1 Verifying Packet Dump

You can configure a packet dump type to verify dumped packets as the follows.

- Packet Dump by Protocol
- Packet Dump with Option

The hiD 6615 S223/S323 also provides debug command for Layer 3 routing protocols (BGP, OSPF, RIP and PIM). If you want to debug about them, refer to the each configuration chapter.

7.16.1.1 Packet Dump by Protocol

You can see packets about BOOTPS, DHCP, ARP and ICMP using the following command.

Command	Mode	Description
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **protocol** {**bootps** | **dhcp** | **arp** | **icmp**} {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*}	Enable	Shows packet dump by protocol.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **host** {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*} {**src-port** <1-65535> | **dest-port** <1-65535>}		Shows host packet dump.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **multicast** {**src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*}		Shows multicast packet dump.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **src-ip** *A.B.C.D* | **dest-ip** *A.B.C.D*}		Show packet dump by source IP address or destination IP address.
debug packet {**interface** *INTERFACE* | **port** *PORTS*} **dest-ip** *A.B.C.D*		

7.16.1.2 Packet Dump with Option

You can verify packets with TCP dump options using the following command.

Command	Mode	Description
debug packet *OPTION*	Enable	Shows packet dump using options.

Tab. 7.4 shows the options for packet dump.

Option	Description
-a	Change Network & Broadcast address to name.
-d	Change the complied packet-matching code to readable letters and close it
-e	Output link-level header of each line
-f	Output outer internet address as symbol
-l	Buffer output data in line. This is useful when other application tries to receive data from tcpdump.
-n	Do not translate all address (e.g. port, host address)
-N	When output host name, do not print domain.
-O	Do not run packet-matching code optimizer. This option is used to find bug in optimizer
-p	Interface is not remained in promiscuous mode
-q	Reduce output quantity of protocol information. Therefore, output line is shorter.
-S	Output TCP sequence number not relative but absolute
-t	Time is not displayed on each output line
-v	Display more information
-w	Save the captured packets in a file instead of output
-x	Display each packet as hexacode
-c *NUMBER*	Close the debug after receive packets as many as the number
-F *FILE*	Recieves file as filter expression. All additional expressions on command line are ignored.
-i *INTERFACE*	Desinate the interface where the intended packets are transmitted. If not designated, it automatically select a interface which has the lowest number within the system interfaces (Loopback is excepted)
-r FILE	Read packets from the file which created by '-w' option.
-s *SNAPLEN*	This is used to configure sample packet except the 68 byte default value. The 68 byte is appropriate value for IP, ICMP, TCP and UDP, but it can truncate protocol information of Name server or NFS packets. If sample size is long, the system should take more time to inspect and packets can be dropped for small buffer size. On the contrary, if the sample size is small, information can be leaked as the amount. Therefore, user should adjust the size as header size of protocol.
-T TYPE	Display the selected packets by conditional expression as the intended type. rpc (Remote Procedure Call) rtp (Real-time Transport Protocol) rtcp (Real-time Transport Control Protocal) vat (Visual Audio Tool) wb (distributed White Board)
EXPRESSION	Conditional expression

Tab. 7.4 Options for Packet Dump

7.16.2 Debug Packet Dump

The hiD 6615 S223/S323 provides network debugging function to prevent system overhead for unknown packet inflow. Monitoring process checks CPU load per 5 seconds. If there is more traffic than threshold, user can capture packets using TCP Dump and save it to file. User can download the dump file with the name of file-number.dump after FP connection to the system. Verify the dumped packet contents with a packet analyze promgram.

To debug packet dump, use the following command.

Command	Mode	Description
debug packet log *COUNT VALUE TIME* [1-10]	Enable	Debug with according to the conditions COUNT: packet counting VALUE: CPU-threshold 1-10: file number
no debug packet log		Release the debug configuration

i Basically, user can save current configuration with **write memory** command. However, the dump file is not saved.

7.17 Displaying the usage of the packet routing table

The packet routing based on host uses L3 table as it's memory. It searches the information of destination addess in L3 table to get the Nexthop information and transmits packets through Rewriting process.

If it does not find the information of destination in L3 table, it refers to CPU routing table and records Nexthop information in L3 table and then transmits the packets through Rewriting process. hiD 6615 provides 4k of L3 table.

The packet routing based on network complements the ineffectual process of recording with packet unit.

hiD 6615 uses LPT table as it's memory and it provides 16k of LPM table.

To show the usage of L3 table, LPM table or interface used in packet routing, use the following command.

Command	Mode	Description
show ip tables summary	Enable	Show the usage of L3 table or LPM table or interface

8 System Main Functions

8.1 VLAN

The first step in setting up your bridging network is to define VLAN on your switch. VLAN is a bridged network that is logically segmented by customer or function. Each VLAN contains group of ports called VLAN members. On the VLAN network, packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 switching device to route traffic between the VLANs. These VLANs improve performance because they reduce the propagation of local traffic, and they improve security benefits because they completely separate traffic.

Enlarged Network Bandwidth

Users belonged in each different VLAN can use more enlarged bandwidth than no VLAN composition because they do not receive unnecessary Broadcast information. A properly implemented VLAN will restrict multicast and unknown unicast traffic to only those links necessary to only those links necessary to reach members of the VLAN associated with that multicast (or unknown unicast) traffic.

Cost-Effective Way

When you use VLAN to prevent unnecessary traffic loading because of broadcast, you can get cost-effective network composition since switch is not needed.

Strengthened Security

When using a shared-bandwidth LAN, there is no inherent protection provided against unwanted eavesdropping. In addition to eavesdropping, a malicious user on a shared LAN can also induce problems by sending lots of traffic to specific targeted users or network as a whole. The only cure is to physically isolate the offending user. By creating logical partitions with VLAN technology, we further enhance the protections against both unwanted eavesdropping and spurious transmissions. As depicted in Figure, a properly implemented port-based VLAN allows free communication among the members of a given VLAN, but does not forward traffic among switch ports associated with members of different VLANs. That is, a VLAN configuration restricts traffic flow to a proper subnet comprising exactly those links connecting members of the VLAN. Users can eavesdrop only on the multicast and unknown unicast traffic within their own VLAN presumably the configured VLAN comprises a set of logically related users.

User Mobility

By defining a VLAN based on the addresses of the member stations, we can define a workgroup independent of the physical location of its members. Unicast and multicast traffic (including server advertisements) will propagate to all members of the VLAN so that they can communicate freely among themselves.

8.1.1 Port-Based VLAN

The simplest implicit mapping rule is known as port-based VLAN. A frame is assigned to a VLAN based solely on the switch port on which the frame arrives. In the example depicted in Figure, frames arriving on ports 1 through 4 are assigned to VLAN 1, frame from ports 5 through 8 are assigned to VLAN 2, and frames from ports 9 through 12 are assigned to VLAN 3.

Stations within a given VLAN can freely communicate among themselves using either unicast or multicast addressing. No communication is possible at the Data Link layer between stations connected to ports that are members of different VLANs. Communication among devices in separate VLANs can be accomplished at higher layers of the architecture, for example, by using a Network layer router with connections to two or more VLANs.

Multicast traffic, or traffic destined for an unknown unicast address arriving on any port, will be flooded only to those ports that are part of the same VLAN. This provides the desired traffic isolation and bandwidth preservation. The use of port-based VLANs effectively partitions a single switch into multiple sub-switches, one for each VLAN.

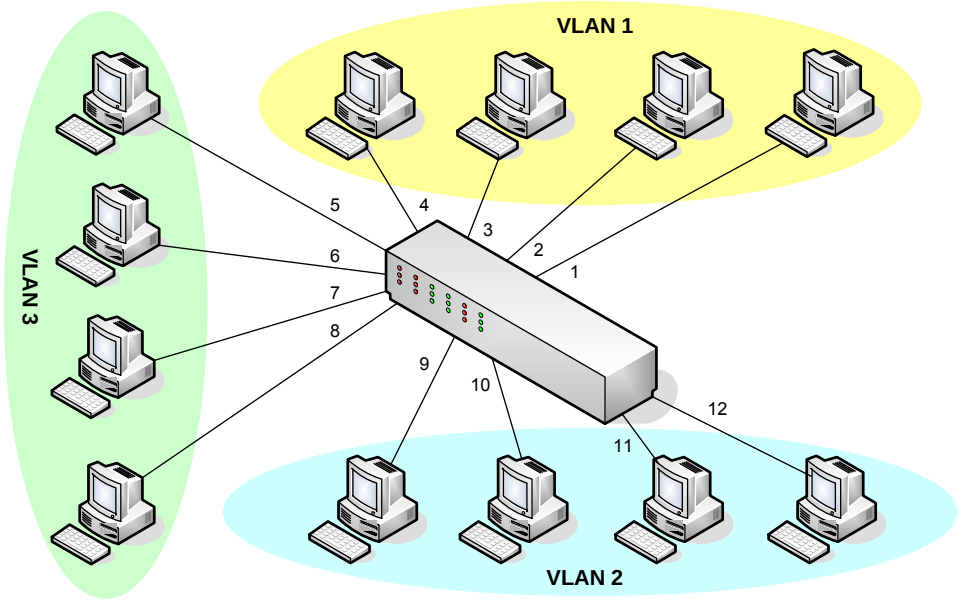


Fig. 8.1 Port-based VLAN

The IEEE 802.1q based ports on the switches support simultaneous tagged and untagged traffic. An 802.1q port is assigned a default port VLAN ID (PVID), and all untagged traffic is assumed to belong to the port default PVID. Thus, the ports participating in the VLANs accept packets bearing VLAN tags and transmit them to the port VLAN ID.

The below functions are explained.

- Creating VLAN
- Specifying PVID
- Assigning Port to VLAN
- Deleting VLAN
- Displaying VLAN

8.1.1.1 Creating VLAN

To configure VLAN on user's network, use the following command.

Command	Mode	Description
vlan create *VLANS*	Bridge	Creates new VLAN by assigning VLAN ID: VLANS: enter the number of VLAN ID (from 1 to 4094).

i The variable VLANS is a particular set of bridged interfaces. Frames are bridged only among interfaces in the same VLAN.

8.1.1.2 Specifying PVID

By default, PVID 1 is specified to all ports. You can also configure PVID. To configure PVID in a port, use the following command.

Command	Mode	Description
vlan pvid *PORTS PVIDS*	Bridge	Configures VLAN PVID: PORTS: enter the port numbers. PVIDS: enter the PV IDs (1 to 4094 multiple entries possible).

8.1.1.3 Assigning Port to VLAN

To assign a port to VLAN, use the following command.

Command	Mode	Description
vlan add *VLANS PORTS* {**tagged** | **untagged**}	Bridge	Assigns a port to VLAN: VLANS: enter the VLAN ID. PORTS: enter the port number.
vlan del *VLANS PORTS*		Deletes associated ports from specified VLAN: VLANS: enter the VLAN ID. PORTS: enter the port number to be deleted.

i When you assign several ports to VLAN, you have to enter each port separated by a comma without space or use dash mark "-" to arrange port range.

8.1.1.4 Deleting VLAN

To delete VLAN, use the following command.

Command	Mode	Description
no vlan *VLANS*	Bridge	Deletes VLAN, enter the VLAN ID to be deleted.

i When you delete VLAN, all ports must be removed from VLAN before, see the below procedure.

8.1.1.5 Displaying VLAN

To display a configuration of VLAN, use the following command.

Command	Mode	Description
show vlan [*VLANS*]	Enable Global Bridge	Shows the configuration for specific VLAN, enter VLAN ID.

8.1.2 Protocol-Based VLAN

User can use a VLAN mapping that associates a set of processes within stations to a VLAN rather than the stations themselves. Consider a network comprising devices supporting multiple protocol suites. Each device may have an IP protocol stack, an AppleTalk protocol stack, an IPX protocol stack and so on.

If we configure VLAN-aware switches such that they can associate a frame with a VLAN based on a combination of the station's MAC source address and the protocol stack in use, we can create separate VLANs for each set of protocol-specific applications.

To configure protocol-based VLAN, follow these steps.

1. Configure VLAN groups for the protocols you want to use.
2. Create a protocol group for each of the protocols you want to assign to a VLAN.
3. Then map the protocol for each interface to the appropriate VLAN

Command	Mode	Description
vlan pvid *PORTS* [**ethertype** *ETHERTYPE*] <1-4094>	Bridge	Configures protocol based VLAN. PORTS: input a port number ETHERTYPE: 0x800 1-4094: Vlan ID
no vlan pvid *PORTS* **ethertype** [*ETHERTYPE*]		Removes protocol based VLAN.

Because Protocol Based VLAN and normal VLAN run at the same time, Protocol Based VLAN operates only matched situation comparing below two cases.

1. When Untagged Frame comes in and matches with Protocol VLAN Table, tags PVID which configured on Protocol VLAN. But in no matched situation, tags PVID which configured on and operates VLAN.
2. When Tagged Frame comes in and VID is 0, it switches by Protocol VLAN Table. But if VID is not 0, it switches by normal VLAN Table.

8.1.3 MAC address-based VLAN

In order to configure VLAN based on MAC address, user should designate MAC address. use the following command.

Command	Mode	Description
vlan macbase *MAC-ADDRESS* <1-4094>	Bridge	Configure VLAN based on MAC address
no vlan macbase *MAC-ADDRESS*		Clears configured VLAN based on MAC address.

8.1.4 Subnet-based VLAN

In order to configure VLAN based on Subnet, user should designate Subnet. use the following command.

Command	Mode	Description
vlan subnet *IP-ADDRESS/M* <1-4094>	Bridge	Configure VLAN based on Subnet
no vlan subnet {*IP-ADDRESS*}		Clears configured VLAN based on Subnet.

To make precedence between MAC address and Subnet based VLAN, user can choose one of both with below command.

Command	Mode	Description
vlan precedence {*MAC / SUBNET*}	Bridge	Configure precedence between MAC based VLAN and Subnet based VLAN.

8.1.5 Tagged VLAN

In a VLAN environment, a frame's association with a given VLAN is soft; the fact that a given frame exists on some physical cable does not imply its membership in any particular VLAN. VLAN association is determined by a set of rules applied to the frames by VLAN-aware stations and/or switches.

There are two methods for identifying the VLAN membership of a given frame:
- Parse the frame and apply the membership rules (implicit tagging).
- Provide an explicit VLAN identifier within the frame itself.

VLAN Tag

A VLAN tag is a predefined field in a frame that carries the VLAN identifier for that frame. VLAN tags are always applied by a VLAN –aware device. VLAN-tagging provides a number of benefits, but also carries some disadvantages.

Advantages	Disadvantages
VLAN association rules only need to be applied once.	Tags can only be interpreted by VLAN aware devices.
Only edge switches need to know the VLAN association rules.	Edge switches must strip tags before forwarding frames to legacy devices or VLAN-unaware domains.
Core switches can get higher performance by operating on an explicit VLAN identifier.	Insertion or removal of a tag requires recalculation of the FCS, possibly compromising frame integrity.
VLAN-aware end stations can further reduce the performance load of edge switches.	Tag insertion may increase the length of a frame beyond the maximum allowed by legacy equipment.

Tab. 8.1 Advantages and Disadvantages of Tagged VLAN

Mapping Frames to VLAN

From the perspective the VLAN-aware devices, the distinguishing characteristic of a VLAN is the means used to map a given frame to that VLAN. In the case of tagged frame, the mapping is simple – the tag contains the VLAN identifier for the frame, and the frame is assumed to belong to the indicated VLAN. That's all there is to it.

To configure the tagged VLAN, use the following command.

Command	Mode	Description
vlan add *VLANS PORTS* **tagged**	Bridge	Configures tagged VLAN on a port: VLANS: enter the VLAN ID. PORTS: enter the port number

8.1.6 VLAN Description

You can describe each VLAN with the following command

Command	Mode	Description
vlan description *VLANS DESC*	Bridge	Describes VLAN characteristic: VLANS: enter the VLAN ID. DESC: enter the detail description
no vlan description *VLANS*		Deletes the description about specified VLAN ID.

8.1.7 Displaying VLAN Information

User can display the VLAN information about Port based VLAN, Protocol based VLAN and QinQ.

Command	Mode	Description
show vlan	Enable Global Bridge	Shows all VLAN configurations.
show vlan *VLANS*		Shows a configuration for specific VLAN.
show vlan description		Shows a description for specific VLAN.
show vlan dot1q-tunnel		Shows QinQ configuration.
show vlan protocol		Shows VLAN based on protocol.

8.1.8 QinQ

QinQ or Double Tagging is one way for tunneling between networks

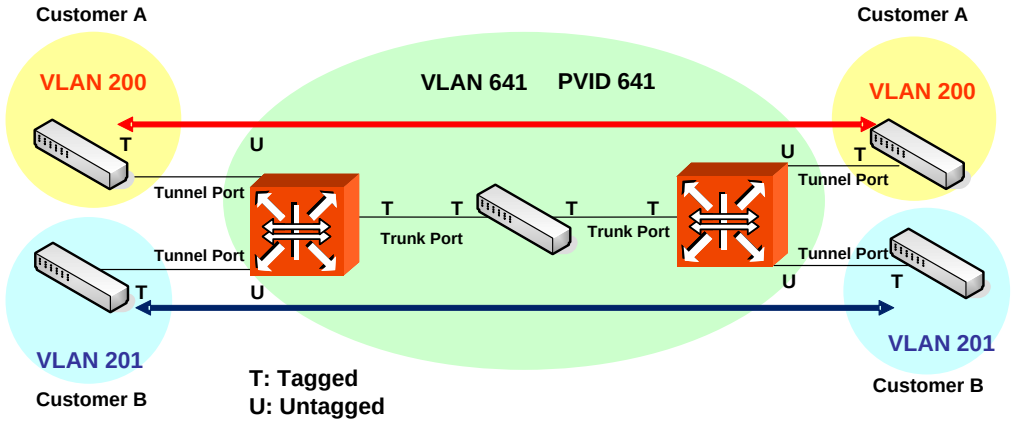


Fig. 8.2 Example of QinQ Configuration

If QinQ is configured on the hiD 6615 S223/S323, it transmits packets adding another Tag to original Tag. Customer A group and customer B group can guarantee security because telecommunication is done between each VLANs at Double Tagging part.

Double tagging is implemented with another VLAN tag in Ethernet frame header.

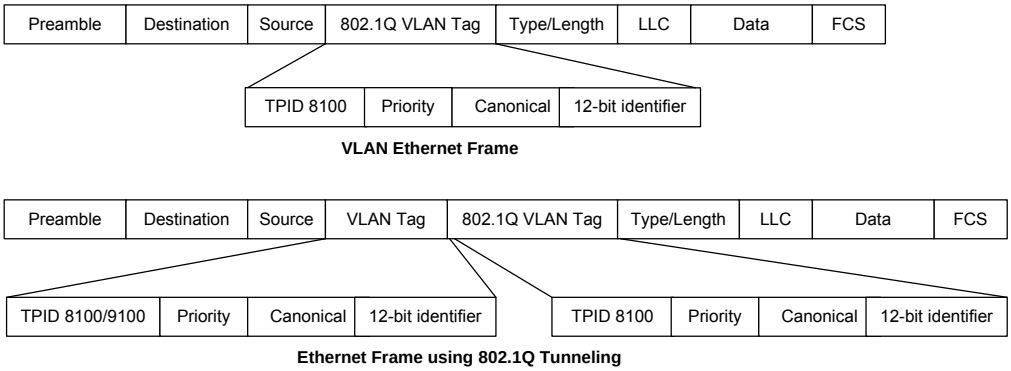


Fig. 8.3 QinQ Frame

Port which connected with Service Provider is Uplink port (internal), and which connected with customer is Access port (external).

Tunnel Port

By tunnel port we mean a LAN port that is configured to offer 802.1Q-tunneling support. A tunnel port is always connected to the end customer, and the input traffic to a tunnel port is always 802.1Q tagged traffic. The different customer VLANs existing in the traffic to a tunnel port shall be preserved when the traffic is carried across the network

Trunk Port

By trunk port we mean a LAN port that is configured to operate as an interswitch link/port,

able of carrying double-tagged traffic. A trunk port is always connected to another trunk port on a different switch. Switching shall be performed between trunk ports and tunnels ports and between different trunk ports.

8.1.8.1 Double Tagging Operation

Step 1
If there is no SPVLAN Tag on received packet, SPVLAN Tag is added.
SPVLAN Tag = TPID : Configured TPID
VID : PVID of input port

Step 2
If received packet is tagged with CVLAN, the switch transmits it to uplink port changing to SPVLAN + CVLAN. When TPID value of received packet is same with TPID of port, it recognizes as SPVLAN, and if not as CVLAN.

Step 3
If Egress port is Access port (Access port is configured as Untagged), remove SPVLAN. If egress port is uplink port, transmit as it is.

Step 4
The hiD 6615 S223/S323 switch has 0x8100 TPID value as default and other values are used as hexadecimal number.

8.1.8.2 Double Tagging Configuration

Step 1
Designate the QinQ port.

Command	Mode	Description
vlan dot1q-tunnel enable *PORTS*	Bridge	Configures a qinq port. PORTS: selects port number qinq to be enabled

Step 2
Configure the same PVID with the VLAN of peer network on the designated qinq port.

Command	Mode	Description
vlan pvid *PORTS* <1-4094>	Bridge	Configures a qinq port. PORTS: selects port number qinq to be enabled <1-4094>: VLAN ID

To disable double tagging, use the following command

Command	Mode	Description
vlan dot1q-tunnel disable *PORTS*	Bridge	Configures a qinq port. PORTS: a port qinq to be disabled

i When you configure Double tagging on the hiD 6615 S223/S323, consider the below attention list.

- DT and HTLS cannot be configured at the same time. (If switch should operate as DT, HTSL has to be disabled.)
- TPID value of all ports on switch is same.
- Access Port should be configured as Untagged, and Uplink port as Tagged.
- Ignore all tag information of port which comes from untagged port (Access Port).
- Port with DT function should be able to configure Jumbo function also

8.1.8.3 TPID Configuration

TPID (Tag Protocol Identifier) is a kind of Tag protocol, and it indicates the currently used tag information. User can change the TPID. By default the port which is configured as 802.1q (0x8100) cannot work as VLAN member.

Use the following command to set TPID on a QinQ port.

Command	Mode	Description
vlan dot1q-tunnel tpid *TPID*	Bridge	Configures TPID.

8.1.9 Layer 2 Isolation

Private VLAN is a kind of LAN Security function using by Cisco products, and it can be classified to Private VLAN and Private edge. Until now, there is no standard document of it.

Private VLAN Edge

Private VLAN edge (protected port) is a function in local switch. That is, it cannot work on between two different switches with protected ports. A protected port cannot transmit any traffic to other protected ports.

Private VLAN

Private VLAN provides L2 isolation within the same Broadcast Domain ports. That means another VLAN is created within a VLAN. There are three type of VLAN mode.

- **Promiscuous**: A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- **Isolated**: An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is for warded only promiscuous ports.
- **Community**: Community ports communicate among themselves and with their promiscuous ports. These interfaces separate at Layer 2 from all other interfaces in-other communities or isolated ports within their PVLAN.

The difference between Private VLAN and Private VLAN edge is that PVLAN edge guarantees security for the ports in a VLAN using protected port and PVLAN guarantees port security by creating sub-VLAN with the three types (Promiscuous, Isolation, and Community). And because PVLAN edge can work on local switch, the isolation between two switches is impossible.

The hiD 6615 S223/S323 provides Private VLAN function like Private VLAN edge of Cisco product. Because it does not create any sub-VLAN, port security is provided by port

isolation. If you want to configure Private VLAN on the hiD 6615 S223/S323 switch, refer to Port Isolation configuration.

8.1.9.1 Port Isolation

The Port Isolation feature is a method that restricts L2 switching between isolated ports in a VLAN. Nevertheless, flows between isolated port and non-isolated port are not restricted. If you use the **port protected** command, packet cannot be transmitted between protected ports. However, to non-protected ports, communication is possible.

To configure Port Isolation, use the following command.

Command	Mode	Description
port protected *PORTS*	Bridge	Enables port isolation.
no port protected [*PORTS*]		Disables port isolation.

8.1.9.2 Shared VLAN

This chapter is only for Layer 2 switch operation. The hiD 6615 S223/S323 is Layer 3 switch, but it can be used for Layer 2 also. Because there is no routing information in Layer 2 switch, each VLAN cannot communicate. Especially, the uplink port should receive packets from all VLANs. Therefore, when you configure the hiD 6615 S223/S323 as Layer 2 switch, the uplink ports have to be included in all VLANs.

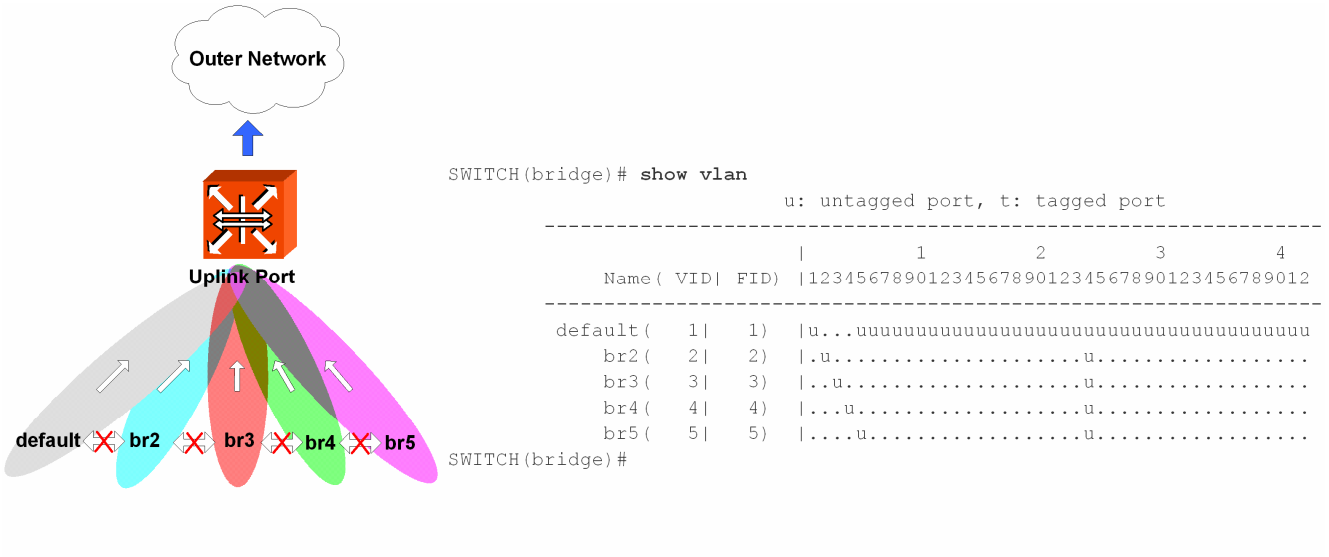


Fig. 8.4 In Case Packets Going Outside in Layer 2 environment

As above configuration with untagged packet, if an untagged packet comes into port 1, it is added with **tag 1** for PVID 1. And the uplink port 24 is also included in the default VLAN; it can transmit to port 24.

However, a problem is possible to occur for coming down untagged packets to uplink ports. If an untagged packet comes to uplink ports from outer network, the system does not know which PIVD it has and where should it forward.

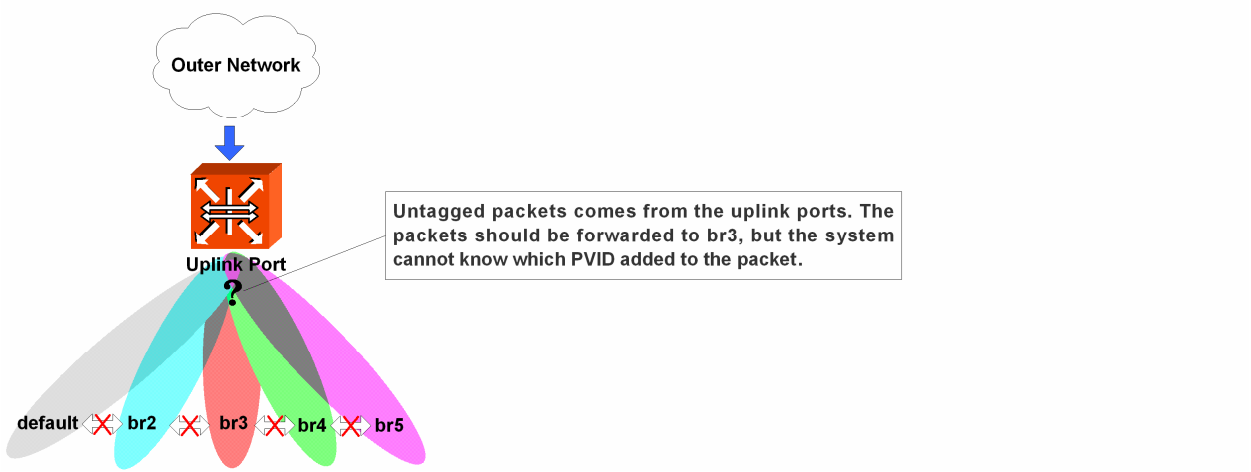
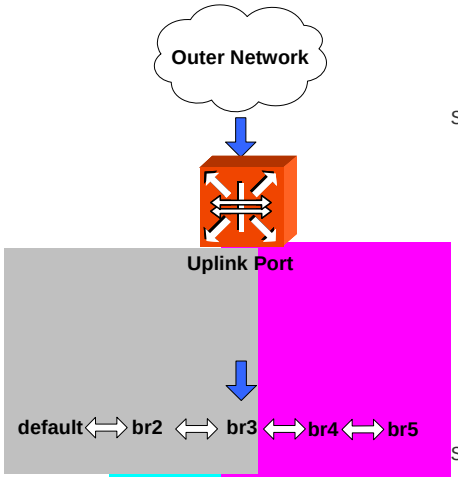


Fig. 8.5 In Case External Packets Enter under Layer 2 environment (1)

To transmit the untagged packet from uplink port to subscriber, a new VLAN should be created including all subscriber ports and uplink ports. This makes the uplink ports to recognize all other ports.

FID helps this packet forwarding. FDB is MAC Address Table that recorded in CPU. FDB table is made of FID (FDB Identification). Because the same FID is managed in the same MAC table, it can recognize how to process packet forwarding. If the FID is not same, the system cannot know the information from MAC table and floods the packets.




```
SWITCH(bridge)# show vlan
                                u: untagged port, t: tagged port
-------------------------------------------------------------------------
                          |          1         2         3         4
    Name( VID| FID) |1234567890123456789012345678901234567890123456789012
-------------- ---- ----------------------------------------------------
 default(   1|   6) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
     br2(   2|   6) |.u.....................u..................
     br3(   3|   6) |..u.....................u.................
     br4(   4|   6) |...u.....................u................
     br5(   5|   6) |....u.....................u...............
     br6(   6|   6) |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
SWITCH(bridge)#
```

Fig. 8.6 In Case External Packets Enter under Layer 2 environment (2)

In conclusion, to use the hiD 6615 S223/S323 as Layer 2 switch, user should add the uplink port to all VLANs and create new VLAN including all ports. If the communication between each VLAN is needed, FID should be same.

To configure FID, use the following command.

Command	Mode	Description
vlan fid *VLANS FID*	Bridge	Configures FID. VLANS: enters VLAN name FID: enters FID value

8.1.10 VLAN Translation

VLAN Translation is simply an action of Rule. This function is to translate the value of specific VLAN ID which classified by Rule. The switch makes Tag adding PVID on Untagged packets, and use Tagged Packet as it is. That is, all packets are tagged in the Switch, and VLAN Translation is to change the VLAN ID value of Tagged Packet in the Switch. This function is to adjust traffic flow by changing the VLAN ID of packet.

Step 1
Open *Rule Configuration* mode using **rule** *NAME* **create** command..

Step 2
Classify the packet that VLAN Translation will be applied by Rule..

Step 3
Designate the VLAN ID that will be changed in the first step by the **match vlan** <1-4094> command.

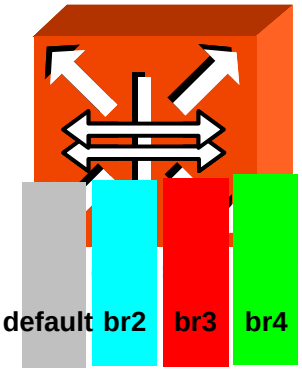
Step 4
Open *Bridge Configuration* mode using the **bridge** command.

Step 5
Add the classified packet to VLAN members of the VLAN ID that will be changed.

8.1.11 Sample Configuration

[Sample Configuration 1] Configuring Port-based VLAN

The following is assigning vlan id of 2,3 and 4 to port 2, port 3, and port 4.




```
SWITCH(bridge)# vlan create 2
SWITCH(bridge)# vlan create 3
SWITCH(bridge)# vlan create 4
SWITCH(bridge)# vlan del default 2-4
SWITCH(bridge)# vlan add 2 2 untagged
SWITCH(bridge)# vlan add 3 3 untagged
SWITCH(bridge)# vlan add 4 4 untagged
SWITCH(bridge)# vlan pvid 2 2
SWITCH(bridge)# vlan pvid 3 3
SWITCH(bridge)# vlan pvid 4 4
SWITCH(bridge)# show vlan
                        u: untagged port, t: tagged port
      ----------------------------------------------------------------
```

```
                        |         1         2         3         4
           Name( VID| FID) |12345678901234567890123456789012345678901234567890123456
        ------------------------------------------------------------------------------
         default(   1|   1) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
             br2(   2|   2) |.u......................................................
             br3(   3|   3) |..u.....................................................
             br4(   4|   4) |...u....................................................
SWITCH(bridge)#
```

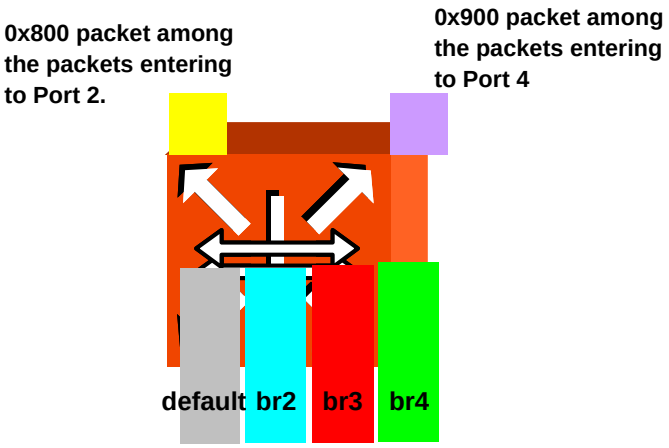
[Sample Configuration 2] Deleting Port-based VLAN

The following is deleting vlan id 3 among configured VLAN.

```
SWITCH(bridge)# vlan del 3 3
SWITCH(bridge)# exit
SWITCH(config)# interface 3
SWITCH(interface)# shutdown
SWITCH(interface)# exit
SWITCH(config)# bridge
SWITCH(bridge)# no vlan 3
SWITCH(bridge)# show vlan
                      u: untagged port, t: tagged port
        ------------------------------------------------------------------------------
                        |         1         2         3         4
           Name( VID| FID) |12345678901234567890123456789012345678901234567890123456
        ------------------------------------------------------------------------------
         default(   1|   1) |u.u.uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
             br2(   2|   2) |.u......................................................
             br4(   4|   4) |...u....................................................
SWITCH(bridge)#
```

[Sample Configuration 3] Configuring Protocol-based VLAN

The following is an example of configuring protocol based VLAN on the port 2 and port 4




```
SWITCH(bridge)# vlan pvid 2 ethertype 0x800 5
SWITCH(bridge)# vlan pvid 4 ethertype 0x900 6
SWITCH(bridge)# show vlan protocol
```

```
          ------------------------------------------------------------
                          |         1         2         3         4
           Ethertype | VID |1234567890123456789012345678901234567890123
          ------------------------------------------------------------
              0x0800     5  .p.....................................
              0x0900     6  ...p....................................
SWITCH(bridge)#
```

With above configuration, the packets from port number 2 and 4 are decided according to the protocol. In case the protocol is incongruous, the route is decided according to the port based VLAN.

[Sample Configuration 4] Configuring QinQ

10 port of SWITCH 1 and 11 port of SWITCH 2 are connected to the network where different VLANs are configured. To communicate without changing VLAN configuration of SWITCH 1 and SWITCH 2 which communicate with PVID 10, configure it as follows.

i You should configure the ports connected to network communicating with PVID 11 as Tagged VLAN port.

< SWITCH 1 >

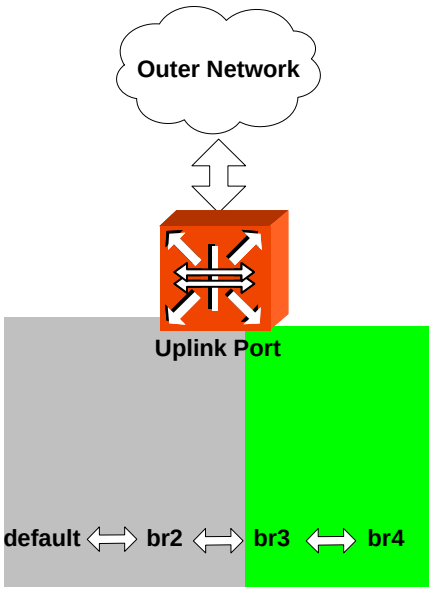
```
SWITCH(bridge)# vlan dot1q-tunnel enable 10
SWITCH(bridge)# vlan pvid 10 11
SWITCH(bridge)# show vlan dot1q-tunnel
          Tag Protocol Id : 0x8100 (d: double-tagging port)
         ------------------------------------------------------
               |       1       2       3       4
          Port |12345678901234567890123456789012345678901234
         ------------------------------------------------------
          dtag  .........d.............................
SWITCH(bridge)#
```

< SWITCH 2 >

```
SWITCH(bridge)# vlan dot1q-tunnel enable 11
SWITCH(bridge)# vlan pvid 11 11
SWITCH(bridge)# show vlan dot1q-tunnel
          Tag Protocol Id : 0x8100 (d: double-tagging port)
         ------------------------------------------------------
               |       1       2       3       4
          Port |12345678901234567890123456789012345678901234
         ------------------------------------------------------
          dtag  .........d.............................
SWITCH(bridge)#
```

[Sample Configuration 5] Configuring Shared VLAN with FID

Configure br2, br3, br4 in the hiD 6615 S223/S323 configured Layer 2 environment and 24 ports as Uplink port is configured. To transmit untagged packet through Uplink port rightly, follow below configuration.




```
SWITCH(bridge)# vlan create br2
SWITCH(bridge)# vlan create br3
SWITCH(bridge)# vlan create br4
SWITCH(bridge)# vlan del default 3-8
SWITCH(bridge)# vlan add br2 3,4 untagged
SWITCH(bridge)# vlan add br3 5,6 untagged
SWITCH(bridge)# vlan add br4 7,8 untagged
SWITCH(bridge)# vlan add br2 24 untagged
SWITCH(bridge)# vlan add br3 24 untagged
SWITCH(bridge)# vlan add br4 24 untagged
SWITCH(bridge)# vlan create br5
SWITCH(bridge)# vlan add br5 1-42 untagged
SWITCH(bridge)# vlan fid 1-5 5
SWITCH(bridge)# show vlan
                      u: untagged port, t: tagged port
       ------------------------------------------------------------------
                         |         1         2         3         4
          Name( VID| FID) |12345678901234567890123456789012345678901234
       ------------------------------------------------------------------
        default(   1|   5)  |uu.....uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
            br2(   2|   5)  |..uu..................u.....................
            br3(   3|   5)  |....uu................u.....................
            br4(   4|   5)  |......uu..............u.....................
            br5(   5|   5)  |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
SWITCH(bridge)#
```

8.2 Link Aggregation

Link Aggregation Control Protocol (LACP) complying with IEEE 802.3ad bundles several physical ports together to one logical port so that user can get enlarged bandwidth.

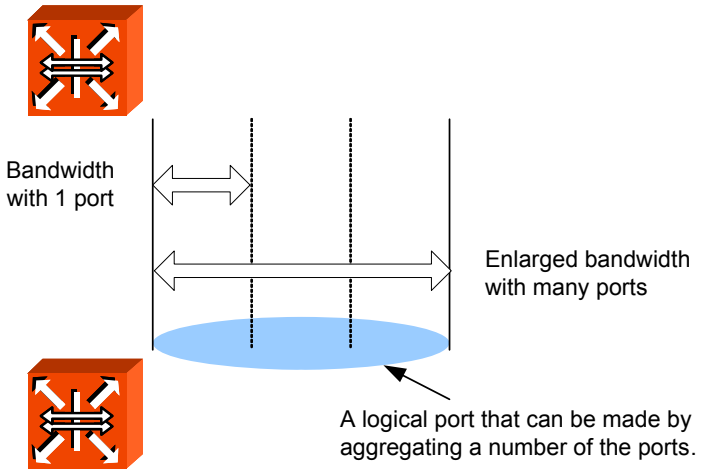


Fig. 8.7 Link Aggregation

The hiD 6615 S223/S323 supports two kinds of link aggregation as port trunk and LACP. There's a little difference in these two ways. In case of port trucking, it is quite troublesome to set the configuration manually and the rate to adjust to the network environment changes when connecting to the switch using logical port. However, if the user configures physical port aggregated with the logical port in each switches, the switches are connected as the configuration. Therefore it is easier for user to configure comparing to the port trunk and could quickly respond to the environmental changes.

8.2.1 Port Trunk

Port trucking enables you to dynamically group similarly configured interfaces into a single logical link (aggregated port) to increase bandwidth, while reducing the traffic congestion.

8.2.1.1 Configuring Port Trunk

To make logical port by aggregating the ports, use the following command.

Command	Mode	Description
trunk <0-5> *PORT*	Bridge	Adds a port to the aggregation port group.
trunk distmode <0-5> *PORTS* {**dstip** | **dstmac** | **srcdstip** | **srcdstmac** | **srcip** | **srcmac**}		Adds a port to the aggregation group and designates physical port as logical port and decide which packets are transmitted to the aggregated port. 1-5: Trunk Group ID

i For the hiD 6615 S223/S323, source destination MAC address is basically used to decide packet route.

If packets enter to logical port aggregating several ports and there's no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively. Therefore hiD 6615 S223/S323 is configured to decide the way of packet route in order to divide on member port effectively when packets

enter. It is decided with Source IP address, Destination IP address, Source MAC address, Destination Mac address and the user could get information of packets to decided packet route.

- **dstip**: Destination IP address
- **dstmac:** Destination MAC address
- **srcdstip:** Refer to both Source IP address and Destination IP address
- **srcdstmac:** Refer to both Source MAC address and Destination MAC address
- **srcip:** Source IP address
- **srcmac:** Source MAC address.

The port designated as member port of port trunk is automatically deleted from existing VLAN. Therefore, if member port and aggregated port exist in other VLAN, VLAN configuration should be changed for the aggregated port.

8.2.1.2 Disabling Port Trunk

To remove the configured port trunk from specified trunk group, use the following command.

Command	Mode	Description
no trunk<0-5> *PORTS*	Bridge	Releases a configured trunk port.
no trunk distmode <0-5>		

i If the user deleted member port from logical port or release port trunk, they are automatically contained as default VLAN.

8.2.1.3 Displaying Port Trunk Configuration

To display a configuration of port trunk, use the following command.

Command	Mode	Description
show trunk	Enable Global Bridge	Shows a configuration for trunk.

8.2.2 Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) is the function of using wider bandwidth by aggregating more than two ports as a logical port as previously stated port trunk function. If the integrated port by configuring from port trunk is in other VLAN which is different from VLAN where existing member port is originally belong to, it should be moved to VLAN where the existing member port is belong to. However, the integrated port configured by LACP is automatically added to appropriate VLAN.

i The LACP aggregator from LACP could support up to 14 so that it is possible to input aggregator number from 0 to 13, and group ID of port trunk and aggregator number of LACP cannot be configured repeatedly.

The following explains how to configure LACP.

- Configuring LACP
- Packet Route
- Operating Mode of Member Port
- Priority of Switch
- Identifying Member Ports within LACP
- BPDU Transmission Rate
- Key value of Member Port
- Priority
- Displaying LACP Configuration

8.2.2.1 Configuring LACP

Step 1
Activate LACP function, using the following command.

Command	Mode	Description
lacp aggregator *AGGREGATIONS*	Bridge	Enables LACP of designated Aggregator-number: AGGREGATIONS: select aggregator ID that should be enabled for LACP (valid value from 0 to 13).
no lacp aggregator *AGGREGATIONS*		Disables LACP for designated Aggregator-number, select the aggregator ID that should be disabled for LACP.

Step 2
Configure the physical port that is a member of aggregated port. In order to configure the member port, use the following command.

Command	Mode	Description
lacp port *PORTS*	Bridge	Configures physical port that is member port of aggregator; select the port number(s) that should be enabled for LACP.
no lacp port *PORTS*		Deletes member port of Aggregator, select the port number(s) that should be disabled for LACP.

8.2.2.2 Packet Route

When packets enter to logical port integrating several ports, if there's no process to decide the packet route, it is not possible to use logical port effectively from focusing packets on a particular member port.

If these packets enter to logical port aggregating several ports and there's no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively.

Therefore the hiD 6615 S223/S323 is configured to decide the way of packet route in order to divide on member port effectively when packets are transmitted. It can be selected with Source IP address, destination IP address, source MAC address, destination MAC address and the user could get the information of packets to decided packet route.

- **dstip**: Destination IP address
- **dstmac:** Destination MAC address
- **srcdstip:** Runs by reference to both Source IP address and Destination IP address
- **srcdstmac:** Source MAC address and Destination MAC address
- **srcip:** Source IP address
- **srcmac:** Source MAC address.

i For the hiD 6615 S223/S323, **srcdstmac** (source MAC address and destination MAC address) is basically used to decide packet route.

After configuring aggregator, you should configure packets transmitting aggregator port. The following is the command of configuring packets transmitting aggregator port.

Command	Mode	Description
lacp aggregator distmode *AGGREGETIONS* {**srcmac** | **dstmac** | **srcdstmac** | **srcip** | **dstip** | **srcdstip**}	Bridge	Defines packets transmitted by way of aggregator which is a logical aggregated port: AGGREGATIONS: select the aggregator ID <0-13>.

To disable configuring packets, use the following command.

Command	Mode	Description
no lacp aggregator *AGGREGETIONS*	Bridge	Deletes destination MAC address, select the aggregator ID.

8.2.2.3 Operating Mode of Member Port

After configuring member port, configure the mode of member port. There are two kinds of mode *Active* mode and *Passive* mode in member port. The port of *Passive* mode starts LACP when there's *Active* mode on the port of opposite switch. The priority of *Active* mode is higher that that of *Passive* mode so that the port of *Passive* mode follows the port of *Active* mode.

i If each member port of the connected switch is configured as *Active* mode and *Passive* mode, *Active* mode is the standard. If both switches are configured as *Passive* mode, link for member ports of two switches is not realized.

To configure the mode of member port, use the following command.

Command	Mode	Description
lacp port activity *PORTS* {**active** | **passive**}	Bridge	Configure the mode of member port, select the member port number. (default: active)

To delete an operating mode of configured member port, use the following command.

Command	Mode	Description
no lacp port activity *PORTS*	Bridge	Deletes operation mode of configured member port, select the member port number.

8.2.2.4 Identifying Member Ports within LACP

The port configured as member port is basically configured to aggregate to LACP. However, even though the configuration as member port is not released, they could operate as independent port without being aggregated to LACP. These independent ports cannot be configured as trunk port because they are independent from being aggregated to LACP under the condition of being configured as member port.

To configure member port to aggregate to LACP, use the following command.

Command	Mode	Description
lacp port aggregation *PORTS* {**aggregatable** | **individual**}	Bridge	Designates whether a member port joins LACP or not, select the member port should be included. (default: aggregatable)

To clear aggregated to LACP of configured member port, use the following command.

Command	Mode	Description
no lacp port aggregation *PORTS*	Bridge	Deletes the configured member port in LACP, select the member port.

8.2.2.5 BPDU Transmission Rate

Member port transmits BPDU with its information. For the hiD 6615 S223/S323, it is possible to configure the BPDU transmission rate, use the following command.

Command	Mode	Description
lacp port timeout *PORTS* {**short** | **long**}	Bridge	Configures BPDU transmission rate: PORTS: select the port number. short: fast rate (once every 1 sec) long: slow rate (30 sec: default)

To clear BPDU transmission rate, use the following command (clear means long timeout).

Command	Mode	Description
no lacp port timeout *PORTS*	Bridge	Deletes BPDU transmission rate of configured member port, select the port number.

8.2.2.6 Key value of Member Port

Member port of LACP has key value. All member ports in one aggregator have same key values. To make an aggregator consisted of specified member ports, configure different key value with key value of another port.

Command	Mode	Description
lacp port admin-key *PORTS* <1-15>	Bridge	Configures key value of member port: PORTS: select the port number. 1-15: select the port key value. (default: 1)

To delete key value of configured member port, use the following command.

Command	Mode	Description
no lacp port admin-key *PORTS*	Bridge	Deletes key value of selected member port, select the member port number.

8.2.2.7 Priority of Member Port

To configure priority of LACP member port, use the following command.

Command	Mode	Description
lacp port priority *PORTS* <1-65535>	Bridge	Sets the LACP priority of member port, select the port number. (default: 32768)

To remove port priority of configured member port, use the following command.

Command	Mode	Description
no lacp port priority *PORTS*	Bridge	Deletes port priority of selected member port, select the member port number.

8.2.2.8 Priority of Switch

In case the member ports of connected switches are configured as Active mode (LACP system enabled), it is required to configure which switch would be a standard for it. For this case, the user could configure the priority on switch. The following is the command of configuring the priority of the switch in LACP function.

Command	Mode	Description
lacp system priority <1-65535>	Bridge	Sets the priority of the switch in LACP function, enter the switch system priority. (default: 32768)

To delete the priority of configured switch, use the following command.

Command	Mode	Description
no lacp system priority	Bridge	Clears the priority of the configured switch.

8.2.2.9 Displaying LACP Configuration

To display a configured LACP, use the following command.

Command	Mode	Description
show lacp aggregator	Enable Global Bridge	Shows the information of aggregated port.
show lacp aggregator *AGGRE-GATIONS*		Shows the information of selected aggregated port.
show lacp port		Shows the information of member port.
show lacp port *PORTS*		Shows the information of appropriated member port.
show lacp statistics		Shows aggregator statistics.

To clear LACP statistics information, use the following command.

Command	Mode	Description
clear lacp statistics	Enable Global Bridge	Clears the information of statistics.

8.3 Spanning-Tree Protocol (STP)

LAN, which is composed of double-path like token ring, has the advantage that it is possible to access in case of disconnection with one path. However, there is another problem named Loop when you always use the double-path.

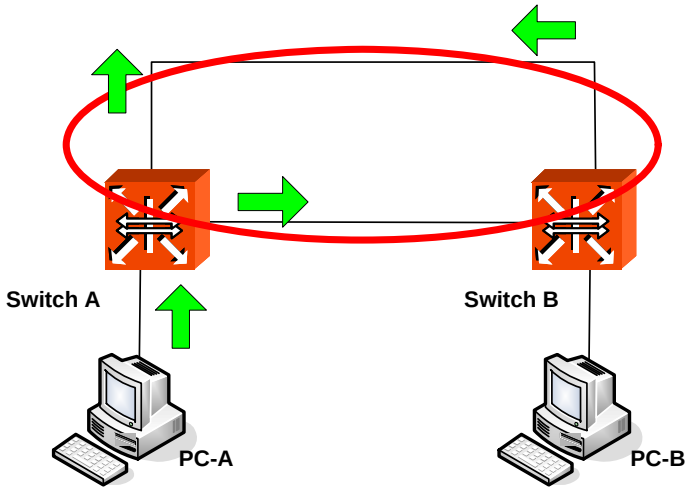


Fig. 8.8 Example of Loop

Loop is when there are more than one path between switches (SWITCH A, B), PC A sends packet through broadcast or multicast and then the packet keeps rotating. It causes superfluous data-transmission and network fault.

STP (Spanning-Tree Protocol) is the function to prevent Loop in LAN with more than two paths and to utilize the double-path efficiently. It specify in IEEE 802.1d. If STP is configured, there is no Loop since it chooses more effective path of them and closes the other path. In other words, when SWITCH C in the below figure sends packet to SWITCH B, path 1 is chosen and path 2 is blocked.

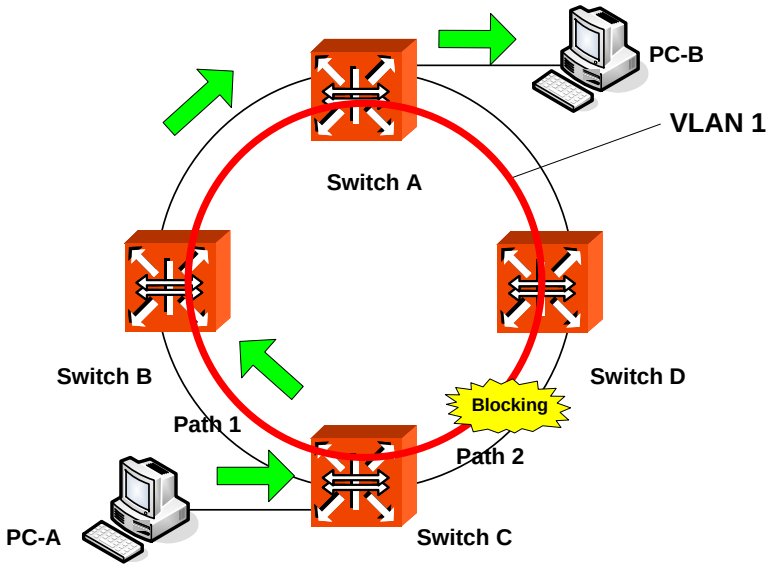


Fig. 8.9 Principle of Spanning Tree Protocol

Meanwhile, RSTP (Rapid Spanning-Tree Protocol) defined in IEEE 802.1w innovate reduces the time of network convergence on STP (Spanning-Tree Protocol). It is easy and fast to configure new protocol.

Also, 802.1w includes 802.1d inside, so it can provide compatibility with 802.1d. For more detail description of STP and RSTP, refer to the following.

- STP Operation
- RSTP Operation
- MSTP Operation
- Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required)
- Configuring STP/RSTP/MSTP
- Configuring PVSTP/PVRSTP
- Root Guard
- Restarting Protocol Migration
- Bridge Protocol Data Unit Configuration
- Sample Configuration

8.3.1 STP Operation

The 802.1d STP defines port state as blocking, listening, learning, and forwarding. When STP is configured in LAN with double-path, switches exchange their information including bridge ID. It is named as BPDU (Bridge Protocol Data Unit). Switches decide port state based on the exchanged BPDU and automatically decide optimized path to communicate with the root switch.

Root Switch

The most important information to decide the root switch is bridge ID. Bridge ID is composed of 2 bytes-priority and 6 bytes-MAC address. The root switch is decided with the lowest bridge ID.

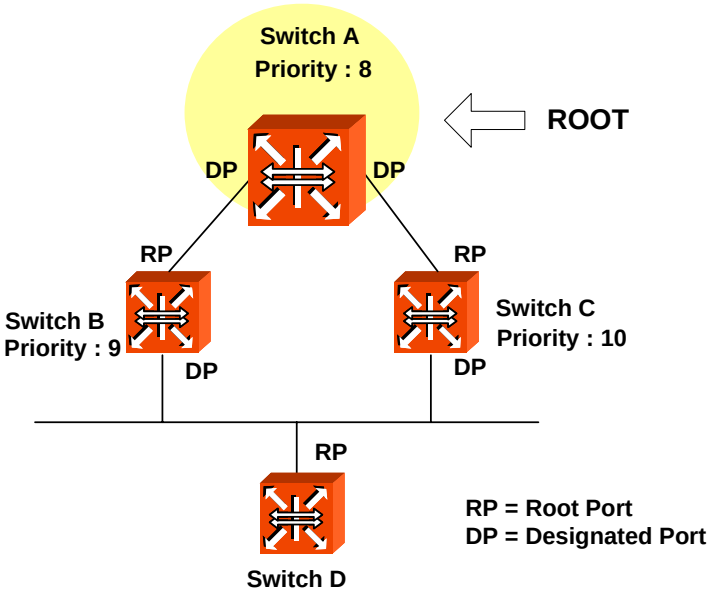


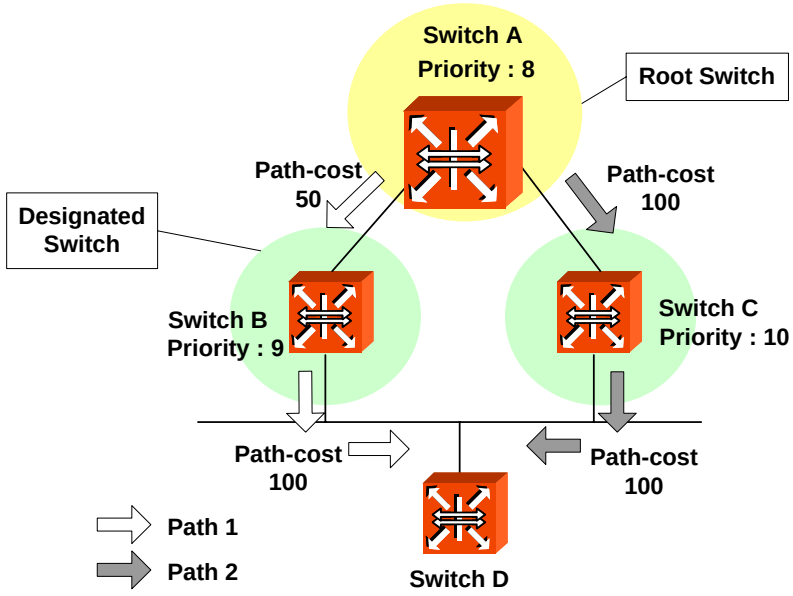
Fig. 8.10 Root Switch

After configuring STP, these switches exchange their information. The priority of SWITCH A is 8, the priority of SWITCH B is 9 and the priority of SWITCH C is 10. In this case, SWITCH A is automatically configured as a root switch.

Designated Switch

After deciding a root switch, while SWITCH A transmits packets to SWITCH C, SWITCH A compares exchanged BPDU to decide the path. The most important information to decide path is the path-cost. Path-cost depends on transmission rate of LAN interface and path with lower path-cost is selected.

The standard to decide designated switch is total root path-cost which is added with path-cost to root. Path-cost depends on transmit rate of switch LAN interface and switch with lower path-cost is selected to be designated switch.



(PATH 1 = 50 + 100 = 150, PATH 2 = 100 + 100 = 200, PATH 1 < PATH 2, ∴ **PATH 1 selected**

Fig. 8.11 Designated Switch

In case of the above picture showing SWITCH C sends packet, path-cost of PATH 1 is 150 and path- cost of PATH 2 is total 200(100 + 100 ; path-cost of SWITCH C to B + path-cost of SWITCH B to C). Therefore lower path-cost, PATH 1 is chosen. In this case, port connected to Root switch is named Root port. In the above picture, port of SWITCH C connected to SWITCH A as Root switch is Root port. There can be only one Root port on equipment.

The standard to decide designated switch is total root path-cost which is added with path-cost to root. Switch with lower path-cost is selected to be designated switch. When root path-costs are same, bridge ID is compared.

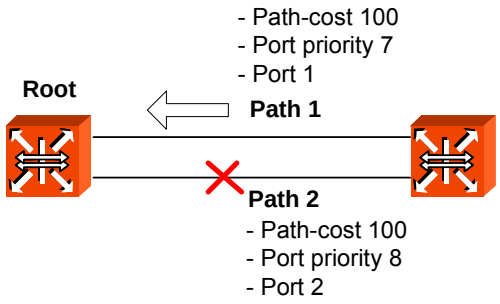
Designated Port and Root Port

A Root Port is the port in the active topology that provides connectivity from the Designated Switch toward the root. A Designated Port is a port in the active topology used to forward traffic away from the root onto the link for which this switch is the Designated Switch. That is; except root port in each switch, selected port to communicate is designated port.

Port Priority

Meanwhile, when path-costs of two paths are same, port-priority is compared. As the below picture, suppose that two switches are connected. Since the path-costs of two paths are 100, same, their port priorities are compared and port with smaller port priority is selected to transmit packet.

i All these functions are automatically performed by BPDU, which is the information of switch. It is also possible to configure BPDU to modify root switch or path manually.



(path-cost of PATH 1 = path-cost of PATH 2 = 100 ∴ unable to compare
PATH 1 port priority = 7, PATH 2 port priority = 8, PATH 1 < PATH 2, ∴ **PATH 1 is chosen**)

Fig. 8.12 Port Priority

Port States

Each port on a switch can be in one of five states.

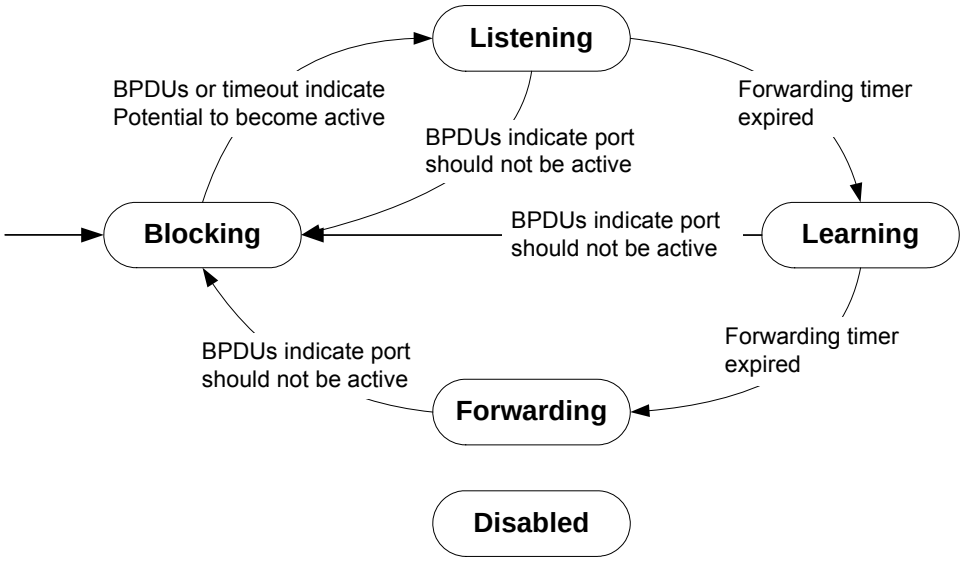


Fig. 8.13 Port State

- **Blocking**
  a port that is enabled, but that is neither a Designated port nor a Root port, will be in the blocking state. A blocking port will not receive or forward data frames, nor will it transmit BPDUs, but instead it will listen for other's BPDUs to determine if and when the port should consider becoming active in the spanning tree.
- **Listening**
  the port is still not forwarding data traffic, but is listening to BPDUs in order to compute the spanning tree. The port is comparing its own information (path cost, Bridge Identifier, Port Identifier) with information received from other candidates and deciding which is best suited for inclusion in the spanning tree.
- **Learning**
  the port is preparing to forward data traffic. The port waits for a period of time to build its MAC address table before actually forwarding data traffic. This time is the forwarding delay.
- **Forwarding**
  After some time learning address, it is allowed to forward data frame. This is the steady state for a switch port in the active spanning tree.
- **Disabled**
  When disabled, a port will neither receive nor transmit data or BPDUs. A port is in this state because it is broken or disabled by administrator.

8.3.2 RSTP Operation

STP or RSTP is configured on network where Loop can be created. However, RSTP is more rapidly progressed than STP at the stage of reaching to the last topology. This section describes how the RSTP more improved than STP works. It contains the below sections.

- Port States
- BPDU Policy
- Rapid Network Convergence
- Compatibility with 802.1d.

Port States

RSTP defines port states as discarding, learning, and forwarding. Blocking of 802.1d and listening is combined into discarding. Same as STP, root port and designated port are decided by port state. But a port in blocking state is divided into alternate port and backup port. Alternate port means a port blocking BPDUs of priority of high numerical value from other switches, and backup port means a port blocking BPDUs of priority of high numerical value from another port of same equipment.

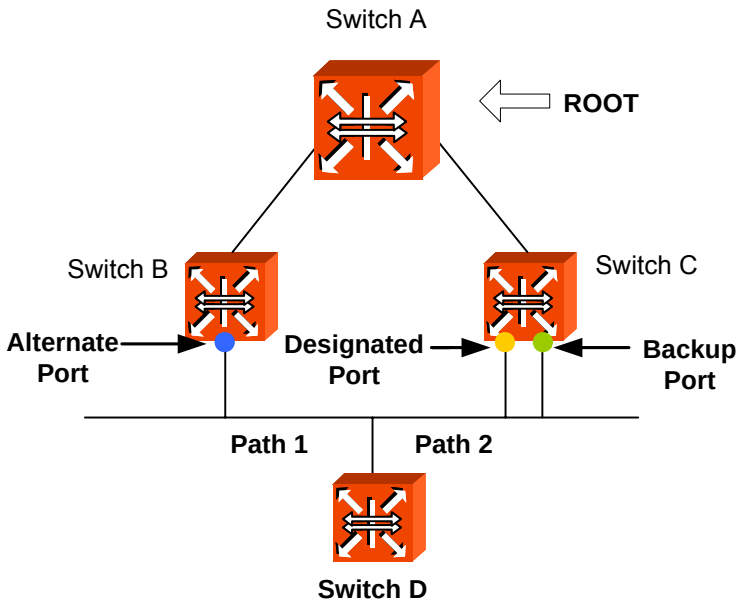


Fig. 8.14 Alternate Port and Backup port

The difference of between alternate port and backup port is that alternate port can alternate path of packet when there is a problem between Root switch and SWITCH C but Backup port cannot provide stable connection in that case.

BPDU Policy

802.1d forwards BPDU following Hello-time installed in root switch and the other switch except root switch its own BPDU only when receiving BPDU from root switch. However, in 802.1w not only root switch but also all the other switches forward BPDU following Hello-time. BPDU is more frequently changed than the interval root switch exchanges, but with 802.1w it becomes faster to be master of the situation of changing network.

By the way, when low BPDU is received from root switch or designated switch, it is immediately accepted. For example, suppose that root switch is disconnected to SWITCH B. Then, SWITCH B is considered to be root because of the disconnection and forwards BPDU.

However, SWITCH C recognizes root existing, so it transmits BPDU including information of root to Bridge B. Thus, SWITCH B configures a port connected to SWITCH C as new root port.

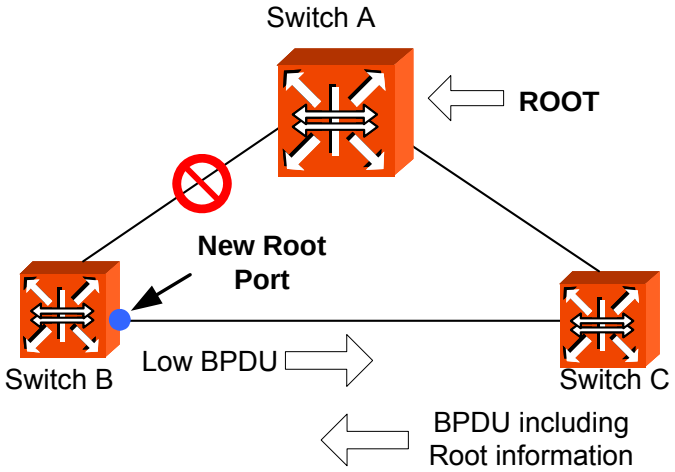


Fig. 8.15 Example of Receiving Low BPDU

Rapid Network Convergence

A new link is connected between SWITCH A and root. Root and SWITCH A is not directly connected, but indirectly through SWITCH D. After SWITCH A is newly connected to root, packet cannot be transmitted between the ports because state of two switches becomes listening, and no loop is created.

In this state, if root transmits BPDU to SWITCH A, SWITCH A transmits new BPDU to SWITCH A and SWITCH C, switch C transmits new BPDU to SWITCH D. SWITCH D, which received BPDU from SWITCH C makes port connected to SWITCH C Blocking state to prevent loop after new link.

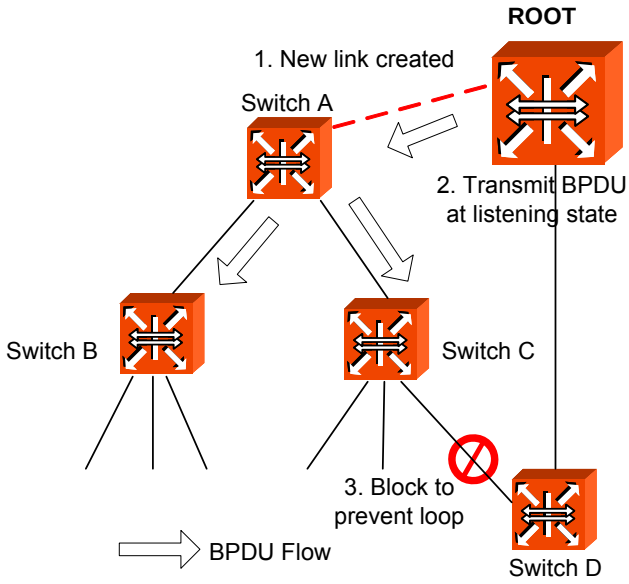


Fig. 8.16 Convergence of 802.1d Network

This is very an epochal way of preventing a loop. The matter is that communication is disconnected during two times of BPDU Forward-delay till a port connected to switch D and SWITCH C is blocked. Then, right after the connection, it is possible to transmit BPDU although packet cannot be transmitted between switch A and root.

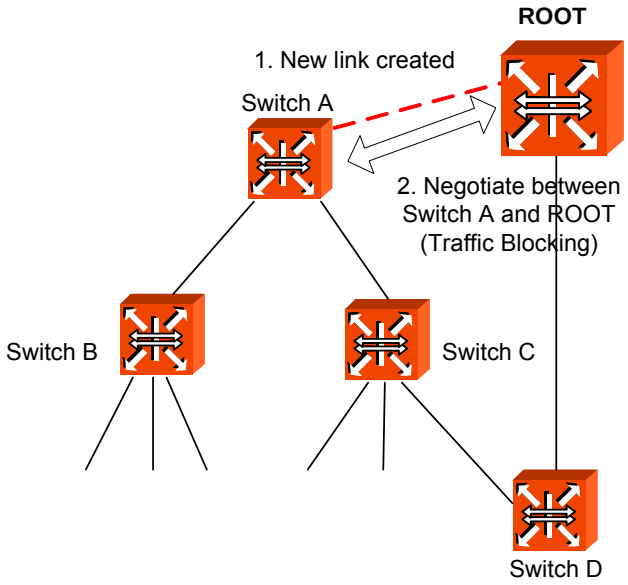


Fig. 8.17 Network Convergence of 802.1w (1)

SWITCH A negotiates with root through BPDU. To make link between SWITCH A and root, port state of non-edge designated port of SWITCH is changed to blocking. Although SWITCH A is connected to root, loop will not be created because SWITCH A is blocked to SWITCH Band C. In this state, BPDU form root is transmitted to SWITCH B and C through SWITCH A. To configure forwarding state of SWITCH A, SWITCH A negotiates with SWITCH B and SWITCH C.

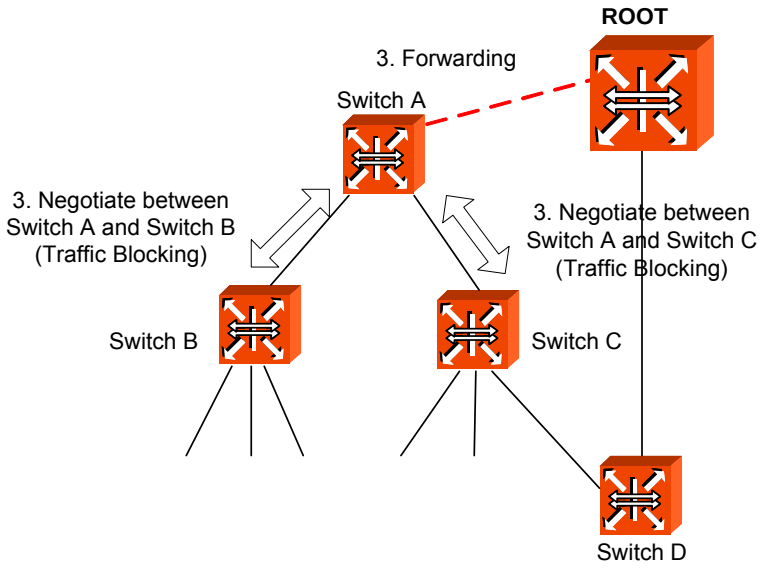


Fig. 8.18 Network Convergence of 802.1w (2)

SWITCH B has only edge-designated port. Edge designated does not cause loop, so it is defined in 802.1w to be changed to forwarding state. Therefore, SWITCH B does not need to block specific port to forwarding state of SWITCH A. However since SWITCH C has a port connected to SWITCH D, you should make blocking state of the port.

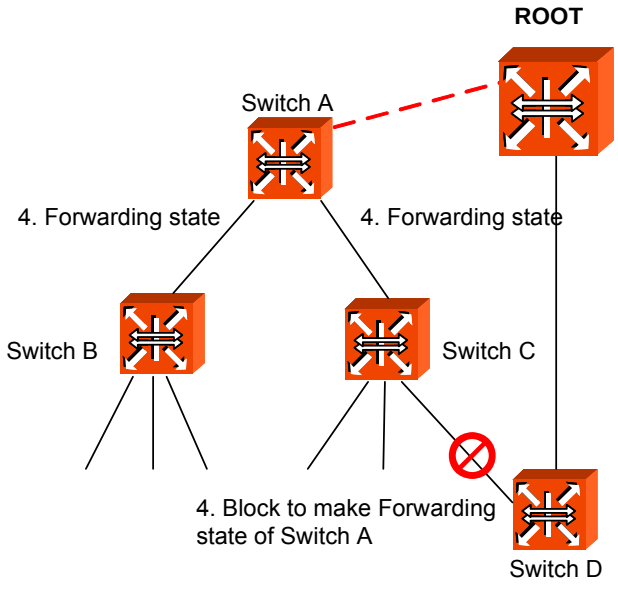


Fig. 8.19 Network Convergece of 802.1w (3)

It is same with 802.1d to block the connection of SWITCH D and SWITCH C. However, 802.1w does not need any configured time to negotiate between switches to make forwarding state of specific port. So it is very fast progressed. During progress to forwarding state of port, listening and learning are not needed. These negotiations use BPDU.

Compatibility with 802.1d

RSTP internally includes STP, so it has compatibility with 802.1d. Therefore, RSTP can recognize BPDU of STP. But, STP cannot recognize BPDU of RSTP. For example, assume that SWITCH A and SWITCH B are operated as RSTP and SWITCH A is connected to SWITCH C as designated switch. Since SWITCH C, which is 802.1d ignores RSTP BPDU, it is interpreted that switch C is not connected to any switch or segment.

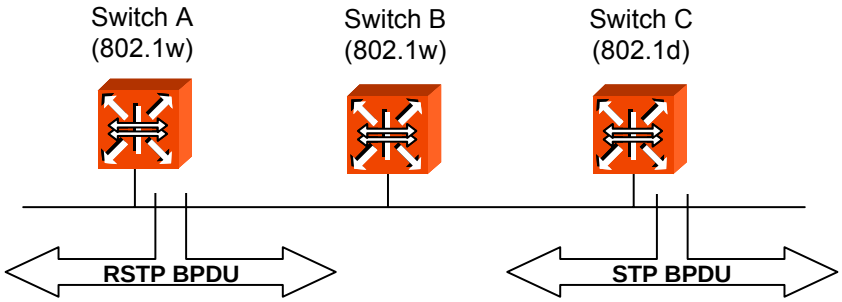


Fig. 8.20 Compatibility with 802.1d (1)

However, SWITCH A converts a port received BPDU into RSTP of 802.1d because it can read BPDU of SWITCH C. Then SWITCH C can read BPDU of SWITCH A and accepts SWITCH A as designated switch.

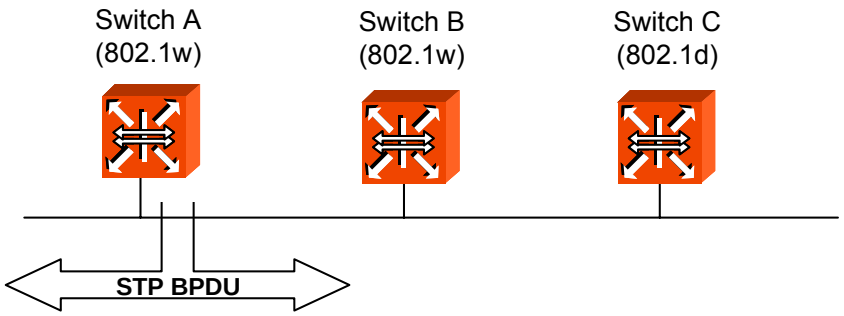


Fig. 8.21 Compatibility with 802.1d (2)

8.3.3 MSTP Operation

To operate the network more effectively, the hiD 6615 S223/S323 uses MSTP (Multiple Spanning-Tree Protocol). It constitutes the network with VLAN subdividing existing LAN domain logically and configure the route by VLAN or VLAN group instead of existing routing protocol.

Operation

Here explains how STP/MSTP differently operates on the LAN. Suppose to configure 100 of VLAN from Switch A to B, C. In case of STP, there's only a STP on all of VLAN and it does not provide multiple instances.

While existing STP is a protocol to prevent Loop in a LAN domain establishes STP per VLAN in order to realize routing suitable to VLAN environment.

It does not need to calculate all STP for several VLAN so that traffic overload could be reduced. By reducing unnecessary overload and providing multiple transmission route for data forwarding, it realizes load balancing and provides many VLAN through Instances.

MSTP

In MSTP, VLAN is classified to groups with same Configuration ID. Configuration ID is composed of Revision name, Region name and VLAN/Instance mapping. Therefore, to have same configuration ID, all of these tree conditions should be the same. VLAN classified with same configuration ID is called MST region. In a region, there's only a STP so that it is possible to reduce the number of STP comparing to PVSTP. There's no limitation for region in a network environment but it is possible to generate Instances up to 64. Therefore instances can be generated from 1 to 64. Spanning-tree which operates in each region is IST (Internal Spanning-Tree). CST is applied by connecting each spanning-tree of region. Instance 0 means that there is not any Instance generated from grouping VLAN, that is, it does not operate as MSTP. Therefore Instance 0 exists on all the ports of the equipment. After starting MSTP, all the switches in CST exchanges BPDU and CST Root is decided by comparing their BPDU. Here, the switches that don't operate with MSTP have instance 0 so that they can also join BPUD exchanges. The operation of deciding CST Root is CIST (Common & Internal Spanning-Tree).

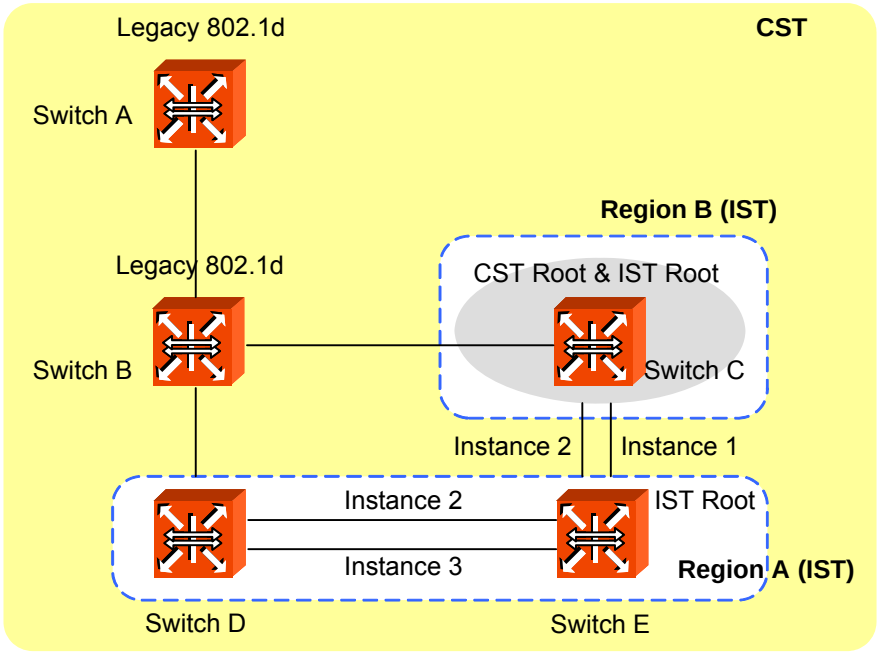


Fig. 8.22 CST and IST of MSTP (1)

In CST, A and B are the switches operating with STP and C, D and, E are those operating with MSTP. First, in CST, CIST is established to decide CST Root. After CST root is decided, the closest switch to CST root is decided as IST root of the region. Here, CST root in IST is IST root.

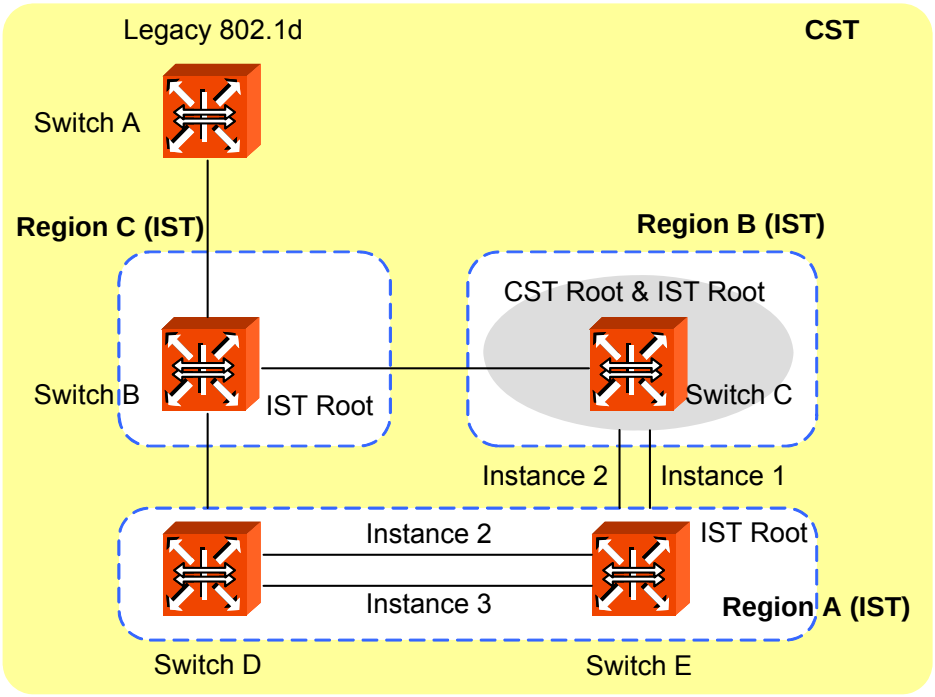


Fig. 8.23 CST and IST of MSTP (2)

In above situation, if B operates with MSTP, B will send it's BPDU to CST root and IST root in order to request itself to be CST root. However, if any BPDU having higher priority than that of B is sent, B cannot be CST root.

For the hiD 6615 S223/S323, the commands configuring MSTP are also used to configure STP and RSTP.

8.3.4 Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required)

First of all, you need to configure force-version to decide the mode before STP is configured. To decide force-version of the switch, use the following command.

Command	Mode	Description
stp force-version {stp | rstp | mstp | pvstp | pvrstp}	Bridge	Configures Force-version in the bridge.

To delete STP configuration from the switch, use the following command.

Command	Mode	Description
no stp force-version	Bridge	Removes force-version configuration.

8.3.5 Configuring STP/RSTP/MSTP

To configure STP and RSTP, use the following steps.

Step 1
Decide STP mode using the **stp force-version** {**stp** | **rstp**} command.

Step 2
Activate MST daemon using the **stp mst enable** command.

Step 3
Configure detail options if specific commands are required.

8.3.5.1 Activating STP/RSTP/MSTP

To enable/disable STP, RSTP, and MSTP in the force-version, use the following command.

Command	Mode	Description
stp mst {**enable** | **disable**}	Bridge	Enables/disables STP, RSTP or MSTP function.

Even though STP function does not operated, loop event does not occur in a switch which belongs to the non-dual path LAN environment.

8.3.5.2 Root Switch

To establish STP, RSTP, or MSTP function, first of all, root switch should be decided. In STP or RSTP, it is named as root switch and in MSTP it is as IST root switch. Each switch has its own bridge ID, and root switch on same LAN is decided by comparing their bridge ID. However, the user can modify root switch by configuring priority for it. The switch having the lowest priority is decided as root switch.

To change root switch by configuring priority for it, use the following command.

Command	Mode	Description
stp mst priority *MSTID-RANGE* <0-61440>	Bridge	Configures the priority of the switch: MSTID-RANGE: select instance number 0. 0-61440: priority value in steps of 4096 (default: 32768)
no stp mst priority *MSTID-RANGE*		Clears the Priority of the switch, enter the instance number.

8.3.5.3 Path-cost

After deciding root switch, you need to decide to which route you will forward the packet. To do this, the standard is path-cost.

Generally, path cost depends on transmission speed of LAN interface in the switch. The following table shows path cost according to transmit rate of LAN interface.

You can use same commands to configure STP and RSTP, but their path-costs are totally different. Please be careful not to make mistake.

Transmit Rate	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

Tab. 8.2 STP Path-cost

Transmit Rate	Path-cost
4M	20,000,000
10M	2,000,000
100M	200,000
1G	20,000
10G	2,000

Tab. 8.3 RSTP Path-cost

When the route decided by path-cost gets overloading, you would better take another route. Considering these situations, it is possible to configure path-cost of root port so that user can configure route manually.

To configure path-cost, use the following command.

Command	Mode	Description
stp mst path-cost *MSTID-RANGE PORTS* <1-200000000>	Bridge	Sets the path-cost to configure route: MSTID_RANGE: select instance number (0-64). PORTS: select the port number. 1-200000000: enter the path cost value.
no stp mst path-cost *MSTID-RANGE PORTS*		Deletes the configured path-cost, enter the instance number and the port number.

8.3.5.4 Port-priority

When all conditions of two switches are same, the last standard to decide route is port-priority. It is also possible to configure port priority so that user can configure route manually. In order to configure port-priority, use the following command.

Command	Mode	Description
stp mst port-priority *MSTID-RANGE PORTS* <0-240>	Bridge	Configures port-priority.
no stp mst port-priority *MSTID-RANGE PORTS*		Disables port priority configuration.

8.3.5.5 MST Region

If MSTP is established in the hiD 6615 S223/S323, decide which MST region the switch is going to belong to by configuring MST configuration ID. Configuration ID contains region name, revision, VLAN map.

To set configuration ID, use the following command.

Command	Mode	Description
stp mst config-id name *NAME*	Bridge	Designate the name for the region: name: set the MST region name. NAME: enter name to give the MST region.
stp mst config-id map <1-64> *VLAN-RANGE*		Configure the range of VLAN that is going to be grouping as a region: 1-64: select an instance ID number. VLAN-RANGE: enter a number of the VLANs to be mapped to the specified instance.
stp mst config-id revision <0-65535>		Configure the switches in the same MST boundary as same number: 0-65535: set the MST configuration revision number.

i In case of configuring STP and RSTP, you don't need to configure configuration ID. If it is configured, error message is displayed.

To delete configuration ID, use the following command.

Command	Mode	Description
no stp mst config-id	Bridge	Delete the entire configured configuration ID.
no stp mst config-id name		Deletes the name of region, enter the MST region name.
no stp mst config-id map <1-64> [*VLAN-RANGE*]		Deletes entire VLAN-map or part of it, select the instance ID number and the number of the VLANs to remove from the specified instance.
no stp mst config-id revision		Deletes the configured revision number.

After configuring configuration ID in the hiD 6615 S223/S323, you should apply the configuration to the switch. After changing or deleting the configuration, you must apply it to the switch. If not, it does not being injected into the switch.

To apply the configuration to the switch after configuring configuration ID, use the following command.

Command	Mode	Description
stp mst config-id commit	Bridge	Commits the configuration of the region.

i After deleting the configured configuration ID, apply it to the switch using the above command.

8.3.5.6 MSTP Protocol

MSTP protocol has a backward compatibility. MSTP is compatible with STP and RSTP. If some other bridge runs with STP mode and send BPDU version of STP or RSTP, MSTP automatically changes to STP mode. STP mode can not be changed to MSTP mode automatically. If administrator wants to change network topology to MSTP mode, administrator has to clear previous detected protocol manually.

To configure the protocol, use the following command.

Command	Mode	Description
stp clear-detected-protocol *PORTS*	Bridge	Clears detected protocol and trys administrative protocol. PORTS: select the port number.

8.3.5.7 Point-to-point MAC Parameters

The internal sub layer service makes available a pair of parameters that permit inspection of, and control over, the administrative and operational state of the point-to-point status of the MAC entity by the MAC relay entity.

To configure the point-to-point status, use the following command.

Command	Mode	Description
stp point-to-point-mac *PORTS* {**auto** | **force-true** | **force-false**}	Bridge	Sets point-to-point MAC: PORTS: select the port number auto: auto detect force-true: force to point-to-point MAC force-false: force to shared MAC (not point-to point MAC)

True means, the MAC is connected to a point-to-point LAN, i.e., there is at most one other system attached to the LAN. False means, the MAC is connected to a non point-to-point LAN, i.e., there can be more than one other system attached to the LAN.

To delete the point-to-point configuration, use the following command.

Command	Mode	Description
no stp point-to-point-mac *PORT*	Bridge	Deletes point-to-point MAC configuration: PORT: select the port number.

8.3.5.8 Edge Ports

Edge ports are used for connecting end devices. There are no switches or spanning-tree bridges after the edge port.

To configure edge port mode, use the following command.

Command	Mode	Description
stp edge-port *PORTS*	Bridge	Sets port edge mode: PORTS: select the port number.

To delete the edge port mode, use the following command.

Command	Mode	Description
no stp edge-port *PORTS*	Bridge	Deletes port edge mode: PORTS: select the port number.

8.3.5.9 Displaying Configuration

To display the configuration after configuring STP, RSTP, and MSTP, use the following command.

Command	Mode	Description
show stp	Enable Global Bridge	Shows the configuration of STP/RSTP/MSTP.
show stp mst		Shows the configuration when it is configured as MSTP.
show stp mst *MSTID-RANGE*		Shows the configuration of specific Instance, enter the instance number.
show stp mst *MSTID-RANGE* {**all** | *PORTS*} [**detail**]		Shows the configuration of the specific Instance for the ports: MSTID_RANGE: select the MST instance number. all: select all ports. PORTS: select port number. detail: show detail information (as option).

i In case STP or RSTP is configured in the SURPASS hiD 6615 S223/S323, you should configure *MSTID-RANGE* as 0.

To display a configured MSTP of the switch, use the following command.

Command	Mode	Description
show stp mst config-id {**current** | **pending**}	Enable Global Bridge	Shows the MSTP configuration identifier: current: shows the current configuration as it is used to run MST. pending: shows the edited configuration.

i For example, after the user configures configuration ID, if you apply it to the switch with **stp mst config-id commit** command, you can check configuration ID with the **show stp mst config-id current** command.

i However, if the user did not use the **stp mst config-id commit** command in order to apply to the switch after configuration, the configuration could be checked with the **show stp mst config-id pending** command.

8.3.6 Configuring PVSTP/PVRSTP

STP and RSPT are designed with one VLAN in the network. If a port becomes blocking state, the physical port itself is blocked. But PVSTP (Per VLAN Spanning Tree Protocol) and PVRSTP (Per VLAN Rapid Spanning Tree Protocol) maintains spanning tree instance for each VLAN in the network. Because PVSTP treats each VLAN as a separate network, it has the ability to load balance traffic by forwarding some VLANs on one trunk and other VLANs. PVRSTP provides the same functionality as PVSTP with enhancement.

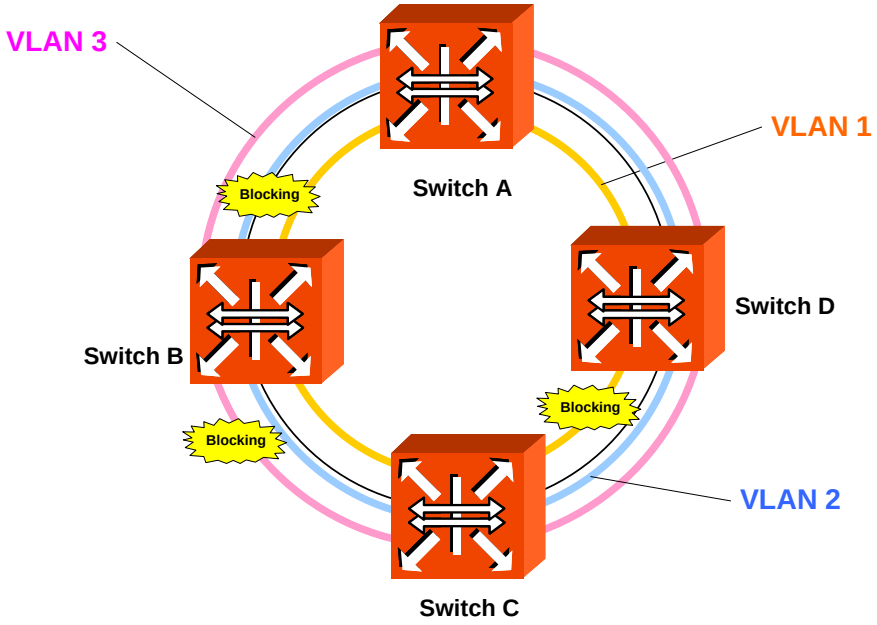


Fig. 8.24 Example of PVSTP

8.3.6.1 Activating PVSTP/PVRSTP

To configure PVSTP or PVRSTP, configure force-version in order to decide the mode. In order to decide force-version, use the following command.

Command	Mode	Description
stp pvst enable *VLAN-RANGE*	Bridge	Activates PVSTP or PVRSTP function. VLAN-RANGE : Vlan name

PVSTP is activated after selecting PVSTP in Force-version using the above command and PVRSTP is activated after selecting PVRSTP using the above commands. In PVSTP and PVRSTP, it is possible to configure only the current VLAN. If you input VLAN that does not exist, error message is displayed.

For the switches in LAN where dual path doesn't exist, Loop does not generate even though STP function is not configured. To disable configured PVSTP, PVRSTP, use the following command.

Command	Mode	Description
stp pvst disable	Bridge	Disables PVSTP or PVRSTP in VLAN.

8.3.6.2 Root Switch

In order establish PVSTP, PVRSTP function, first of all, Root switch should be decided. Each switch has its own Bridge ID and Root switch on same LAN is decided by comparing their Bridge ID. However, the user can change Root switch by configuring Priority for it. The switch having the lowest priority is decided as Root switch.

To change Root switch by configuring Priority for it, use the following command.

Command	Mode	Description
stp pvst priority *VLAN-RANGE* <0-61440>	Bridge	Configures a priority of switch.
no stp pvst priority *VLAN-RANGE*		Clears a priority of switch.

8.3.6.3 Path-cost

After deciding Root switch, you need to decide to which route you will forward the packet. To do this, the standard is path-cost. Generally, path-cost depends on transmission speed of LAN interface in switch. In case the route is overload based on Path-cost, it is better to take another route.

By considering the situation, the user can configure Path-cost of Root port in order to designate the route on ones own. To configure Path-cost, use the following command.

Command	Mode	Description
stp pvst path-cost *VLAN-RANGE PORTS* <1-200000000>	Bridge	Configures path-cost to configure route on user's own.
no stp pvst path-cost *VLAN-RANGE PORTS*		Clears path-cost configuration.

8.3.6.4 Port-priority

When all conditions of two switches are same, the last standard to decide route is port-priority. It is also possible to configure port priority so that user can configure route manually. To configure port priority, use the following command.

Command	Mode	Description
stp pvst port-priority *VLAN-RANGE PORTS* <0-240>	Bridge	Configures port-priority.
no stp pvst port-priority *VLAN-RANGE PORTS*		Disables port priority configuration.

8.3.7 Root Guard

The standard STP does not allow the administrator to enforce the position of the root bridge, as any bridge in the network with lower bridge ID will take the role of the root bridge. Root guard feature is designed to provide a way to enforce the root bridge placement in the network. Even if the administrator sets the root bridge priority to zero in an effort to secure the root bridge position, there is still no guarantee against bridge with priority zero and a lower MAC address.

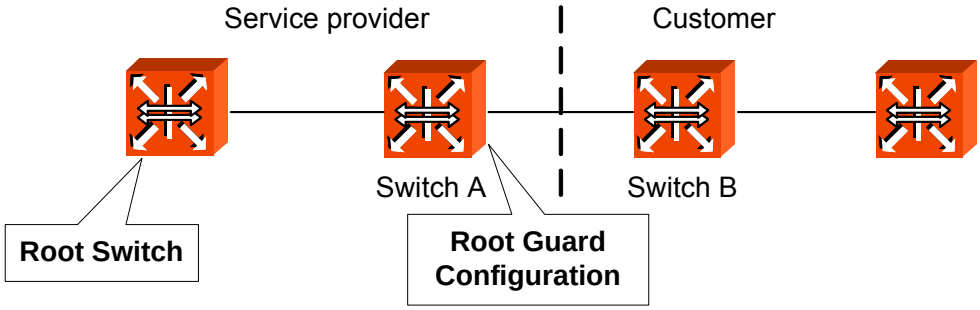


Fig. 8.25 Root Guard

Software-based bridge applications launched on PCs or other switches connected by a customer to a service-provider network can be elected as root switches. If the priority of bridge B is zero or any value lower than that of the root bridge, device B will be elected as a root bridge for this VLAN. As a result, network topology could be changed. This may lead to sub-optimal switching. But, by configuring root guard on switch A, no switches behind the port connecting to switch A can be elected as a root for the service provider's switch network. In which case, switch A will block the port connecting switch B.

To configure Root-Guard, use the following command.

Command	Mode	Description
stp pvst root-guard *VLAN-RANGE PORTS*	Bridge	Configures Root Guard on PVST network.
stp mst root-guard *MSTID-RANGE PORTS*		Configures Root Guard on MST network.
no stp pvst root-guard *VLAN-RANGE PORTS*		Disables Root Guard.
no stp mst root-guard *MSTID-RANGE PORTS*		

8.3.8 Restarting Protocol Migration

There are two switches which configured as STP and RSTP. Usually, in this case, STP protocol is used between two switches. But if someone configures the STP switch to RSTP mode, what happens? Because the RSTP switch already received STP protocol packet, the two switches still can work with STP mode even though RSTP is enabled at both. If you enable this command, the switch checks STP protocol packet once again.

To clear configured Restarting Protocol Migration, use the following command.

Command	Mode	Description
stp clear-detected-protocol *PORTS*	Bridge	Configures restarting protocol migration function.

8.3.9 Bridge Protocol Data Unit Configuration

Bridge Protocol Data Unit (BPDU) is a transmission message in LAN in order to configure, maintain the configuration for STP/RSTP/MSTP. Switches that STP is configured exchange their information BPDU to find best path. MSTP BPDU is general STP BPDU having additional MST data on it's end. MSTP part of BPDU does not rest when it is out of Region.

- **Hello Time**
  Hello time decides an interval time when a switch transmits BPDU. It can be configured from 1 to 10 seconds. The default is 2 seconds.
- **Max Age**
  Root switch transmits new information every time based on information from another switches. However, if there are many switches on network, it takes lots of time to transmit BPDU. And if network status is changed while transmitting BPDU, this information is useless. To get rid of useless information, max age is identified in each information.
- **Forward Delay**
  Switches find location of another switches connected to LAN though received BPDU and transmit packets. Since it takes certain time to receive BPDU and find the location before transmitting packet, switches send packet at regular interval. This interval time is named forward delay.

i The configuration for BPDU is applied as selected in force-version. The same commands are used for STP, RSTP, MSTP, PVSTP and PVRSTP.

8.3.9.1 Hello Time

Hello time decides an interval time when a switch transmits BPDU. To configure hello time, use the following command.

Command	Mode	Description
stp mst hello-time <1-10>	Bridge	Configures hello time to transmit the message in STP, RSTP and MSTP: 1-10: set the hello time. (default: 2)
stp pvst hello-time *VLAN-RANGE* <1-10>		Configures hello time to transmit the message in PVSTP and PVRSTP: 1-10: set the hello time. (default: 2)

To clear configured hello-time, use the following command.

Command	Mode	Description
no stp mst hello-time	Bridge	Returns to the default hello time value of STP, RSTP and MSTP.
no stp pvst hellow-time *VLAN-RANGE*		Returns to the default hello time value of PVSTP and PVRSTP.

8.3.9.2 Forward Delay

It is possible to configure forward delay, which means time to take port status from listening to forwarding. To configure forward delay, use the following command.

Command	Mode	Description
stp mst forward-delay <4-30>	Bridge	Modifies forward-delay in STP, RSTP or MSTP, enter a delay time value. (default: 15)
stp pvst forward-delay *VLAN-RANGE* <4-30>		Modifies forward-delay in PVSTP and PVRSTP, enter a delay time value of VLAN. (default: 15)

To delete a configured forward delay, use the following command.

Command	Mode	Description
no stp mst forward-delay	Bridge	Returns to the default value of STP, RSTP and MSTP.
no stp pvst forward-delay *VLAN-RANGE*		Returns to the default value of PVSTP and PVRSTP per VLAN.

8.3.9.3 Max Age

Max age shows how long path message is valid. To configure max age to delete useless messages, use the following command.

Command	Mode	Description
stp mst max-age <6-40>	Bridge	Configures max age of route message of STP, RSTP or MSTP, enter a max age time value. (default: 20)
stp pvst max-age *VLAN-RANGE* <6-40>		Configures max age of route message of PVSTP, PVRSTP, enter a max age time value of VLAN. (default: 20)

i It is recommended that max age is configured less than twice of forward delay and more than twice of hello time.

To delete a configured max age, use the following command.

Command	Mode	Description
no stp mst max-age	Bridge	Returns to the default max-age value of STP, RSTP and MSTP.
no stp pvst max-age *VLAN-RANGE*		Returns to the default max-age value of PVSTP and PVRSTP.

8.3.9.4 BPDU Hop

In MSTP, it is possible to configure the number of hop in order to prevent BPDU from wandering. BPDU passes the switches as the number of hop by this function.

To configure the number of hop of BPDU in MSTP, use the following command.

Command	Mode	Description
stp mst max-hops <1-40>	Bridge	Configures the number of hop for BPDU, set the number of possible hops in the region.
no stp mst max-hops		Deletes the number of hop for BPDU in MSTP.

8.3.9.5 BPDU Filter

BPDU filtering allows you to avoid transmitting on the ports that are connected to an end system. If the BPDU Filter feature is enabled on the port, then incoming BPDUs will be filtered and BPDUs will not be sent out of the port. To set the BPDU filter on the port, use the following command.

Command	Mode	Description
stp bpdu-filter {**enable** | **disable**} *PORTS*	Bridge	Forbids all STP BPDUs to go out the specific port and not to recognize incoming STP BPDUs the specific port.

By default, it is disabled. The BPDU filter-enabled port acts as if STP is disabled on the port. This feature can be used for the ports that are usually connected to an end system or the port that you don’t want to receive and send unwanted BPDU packets. Be cautious about using this feature on STP enabled uplink or trunk port. If the port is removed from VLAN membership, correspond BPDU filter will be automatically deleted.

8.3.9.6 BPDU Guard

BPDU guard has been designed to allow network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports with STP enabled are not allowed to influence the STP topology. This is achieved by disabling the port upon receipt of BPDU. This feature prevents Denial of Service (DoS) attack on the network by permanent STP recalculation. That is caused by the temporary introduction and subsequent removal of STP devices with low (zero) bridge priority.

To configure BPDU guard in the switch, perform the following procedure.

Step 1
Configure the specific port as edge-port.

Command	Mode	Description
stp edge-port *PORTS*	Bridge	Configures the port as Edge port.
no stp edge-port *PORTS*		Disables Edge port configuration.

Step 2
Configure BPDU Guard.

Command	Mode	Description
stp bpdu-guard	Bridge	Configures BPDU Guard function on switch.
no stp bpdu-guard		Disables BPDU Guard function.

However, BPDU Guard can be corrupted by unexpected cause. In this case, the edge port is blocked immediately and remains at this state until user recovers it. To prevent this problem, the hiD 6615 S223/S323 switch provides BPDU guard auto-recovery function. When an edge port is down for BPDU packet which came from other switch, the port is recovered automatically after configured time.

To configure BPDU Guard auto-recovery, use the following command.

Command	Mode	Description
stp bpdu-guard auto-recovery	Bridge	Configures BPDU Guard auto-recovery on switch.
stp bpdu-guard auto-recovery-time <10-1000000>		Configures BPDU Guard auto-recovery-time.
no stp bpdu-guard auto-recovery		Disables BPDU Guard auto-recovery function.
no stp bpdu-guard auto-recovery-time		

To recover a blocked port by manually, use the following command.

Command	Mode	Description
stp bpdu-guard err-recovery *PORTS*	Bridge	Recovers a blocked port by manually.

8.3.9.7 Self Loop Detection

Although there is no double path in user's equipment, loop can be caused by network environment and cable condition connected to equipment. To prevent this, the hiD 6615 S223/S323 has self loop detection to perceive that outgoing packet is got back. Through the self loop detection, you can prevent packet, which comes back because it blocks the port.

To enable/disable self loop detection, use the following command.

Command	Mode	Description
self-loop-detect {**enable** | **disable**}	Bridge	Enables/disables self loop detection function.

To display a configuration for BPDU, use the following command.

Command	Mode	Description
show self-loop-detect	Enable Global Bridge	Shows status of self loop detection and a port where loop is happed.
show self-loop-detect {**all** | *PORTS*}		Shows self loop detection status on specified ports: all: all the ports PORTS: selected port

8.3.9.8 Displaying BPDU Configuration

To display the configuration for BPDU, use the following command.

Command	Mode	Description
show stp mst *MSTID-RANGE* {**all** | *PORTS*} [**detail**]	Enable Global Bridge	Shows a configuration for BPDU for STP, RSTP and MSTP.
show stp mst *MSTID-RANGE* **all** [**detail**]		
show stp mst *MSTID-RANGE PORTS* [**detail**]		
show stp pvst *VLAN-RANGE* [**all** | *PORTS*] [**detail**]		Shows a configuration for BPDU for PVSTP and PVRSTP.

8.3.10 Sample Configuration

Backup Route

When you design layer 2 network, you must consider backup route for stable STP network. This is to prevent network corruption when just one additional path exits.

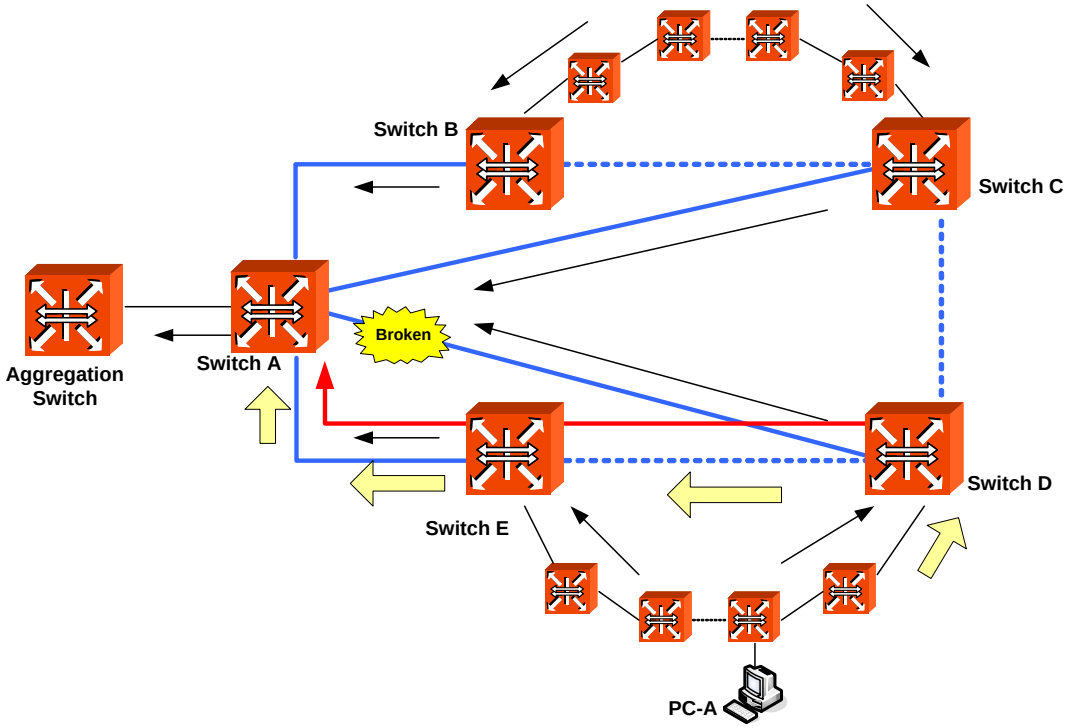


Fig. 8.26 Example of Layer 2 Network Design in RSTP Environment

In ordinary case, data packets go to Root switch A through the blue path. The black arrows describe the routine path to the Aggregation Switch. And the dot lines are in blocking state. But if there is a broken between Switch A and Switch B, the data from PC-A should find another route at Switch D. Switch D can send the data to Switch C and Switch E. Because Switch E has shorter hop count than Switch B, the data may go through the Switch E and A as the red line. And we can assume Switch E is also failed at the same time. In this case, since Switch D can has the other route to Switch C, the network can be stable than just one backup route network.

MSTP Configuration

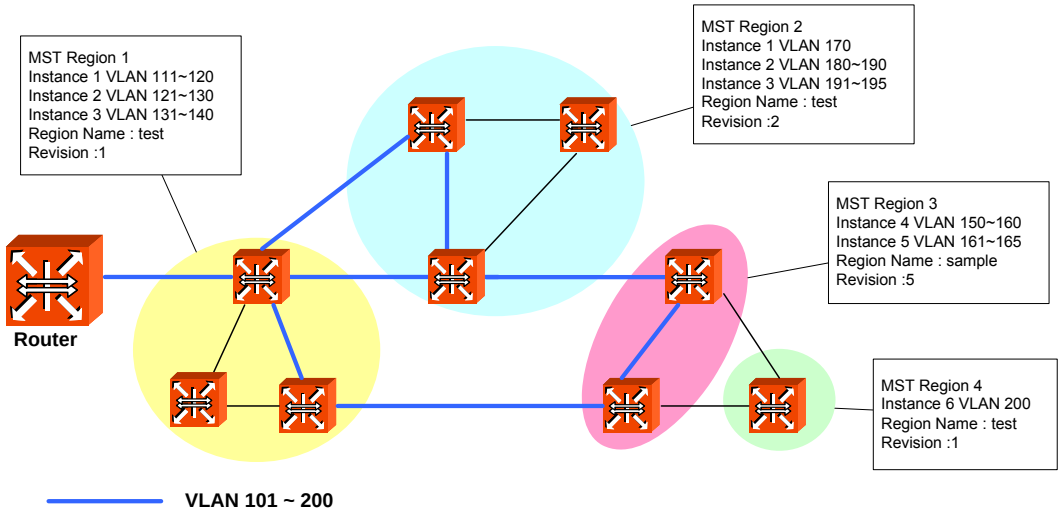


Fig. 8.27 Example of Layer 2 Network Design in MSTP Environment

The following is an example of configuring MSTP in the switch.

```
SWITCH(bridge)# stp force-version mstp
SWITCH(bridge)# stp mst enable
SWITCH(bridge)# stp mst config-id map 2 1-50
SWITCH(bridge)# stp mst config-id name 1
SWITCH(bridge)# stp mst config-id revision 1
SWITCH(bridge)# stp mst config-id commit
SWITCH(bridge)# show stp mst

Status              enabled
bridge id           8000.00d0cb000183
designated root     8000.00d0cb000183
root port           0                   path cost 0
max age             20.00               bridge max age          20.00
hello time          2.00                bridge hello time       2.00
forward delay       15.00               bridge forward delay    15.00
CIST regional root  8000.00d0cb000183   CIST path cost          0
max hops            20
name                TEST
revision            1
instance vlans
------------------------------------------------------------------------
CIST     51-4094
  2      1-50
------------------------------------------------------------------------
SWITCH(bridge)#
```

8.4 Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is configuring Virtual router (VRRP Group) consisted of VRRP routers to prevent network failure caused by one dedicated router. You can configure maximum 255 VRRP routers in VRRP group of hiD 6615 S323. First of all, decide which router plays a roll as Master Virtual Router. The other routers will be Backup Virtual Routers. After you give priority to these backup routers, the router serves for Master Virtual Router when there are some problems in Master Virtual router. When you configure VRRP, configure all routers in VRRP with unified Group Id and assign unified Associated IP to them. After that, decide Master Virtual Router and Backup Virtual Router. A router which has the highest priority is supposed to be Master and Backup Virtual Routers also get orders depending on priority.

⚠ Routing functionalities such as RIP, OSPF, BGP, VRRP and PIM-SM are only available for hiD 6615 S323. (Unavailable for hiD 6615 S223)

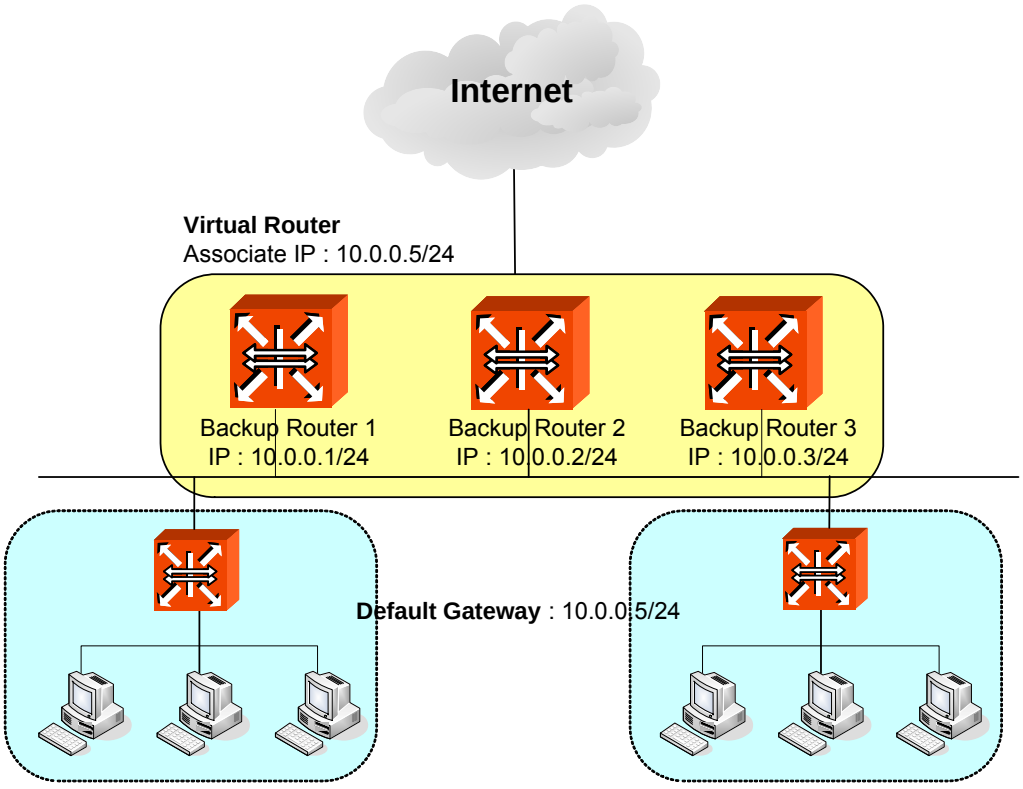


Fig. 8.28 VRRP Operation

In case routers have same priorities, then a router, which has lower IP address, gets the precedence. Fig. 8.28 shows an example of configuring three routers which have IP addresses, 10.0.0.1/24, 10.0.0.2/24 and 10.0.0.3/24 for each one as Virtual router by Associated IP, 10.0.0.5/24. If these three routers have same Priority, a router, which has the smallest IP, address, 10.0.0.1/24 is decided to be Master Router. Also, switches and PCs connected to the Virtual Router are to have IP address of Virtual Router, 10.0.0.5/24 as default gateway.

8.4.1 Configuring VRRP

To configure the hiD 6615 S323 as device in Virtual Router, use the following command on *Global Configuration* mode. Then you can configure VRRP by opening *VRRP Configuration* mode.

Command	Mode	Description
router vrrp *INTERFACE GROUP-ID*	Global	Configures Virtual Router (VRRP Group). GROUP-ID: 1-255

To display a configuration of VRRP, use the following command.

Command	Mode	Description
show vrrp	Enable Global Bridge VRRP	Shows current configuration of VRRP.
show vrrp *INTERFACE*		Shows current configuration of specified interface VRRP.

To delete the VRRP configuration, use the following command.

Command	Mode	Description
no router vrrp <1-255>	Global	Configures Virtual Router (VRRP Group). 1-255: group ID

8.4.1.1 Associated IP Address

After configuring a virtual router, you need to assign an associated IP address to the virtual router. Assign unified IP address to routers in one group.

To assign an associate IP address to routers to a virtual router or delete a configured associate IP address, use the following command.

Command	Mode	Description
associate *A.B.C.D*	VRRP	Assigns an associated IP address to a virtual router.
no associate [*A.B.C.D*]		Deletes an assigned associated IP address from a virtual router.

8.4.1.2 Access to Associated IP Address

If you configure the function of accessing Associated IP address, you can access to Associated IP address by the commands such as ping.

To configure the function of accessing Associated IP address, use the following command.

Command	Mode	Description
vip-access [**enable** | **disable**]	VRRP	Configures the function of accessing associated IP address.

8.4.1.3 Master Router and Backup Router

The hiD 6615 S323 can be configured as Master Router and Backup Router by comparing Priority and IP address of devices in Virtual Router. First of all, it compares Priority. A device, which has higher Priority, is to be higher precedence. And when devices have same Priority, then it compares IP address. A device, which has lower IP address, is to be higher precedence. If a problem occurs on Master Router and there are more than two routers, one of them is selected as new Master Router according to their precedence.

To configure Priority of Virtual Router or delete the configuration, use the following commands.

Command	Mode	Description
vr-priority <1-254>	VRRP	Configures Priority of Virtual Router.
no vr-priority		Deletes configured Priority of Virtual Router.

Priority of Virtual Backup Router can be configured from 1 to 254.

To set VRRP timers or delete the configuration, use the following command.

Command	Mode	Description
vr-timers advertisement <1-10>	VRRP	Sets VRRP timers. 1-10: advertisement time in the unit of second
no vr-timers advertisement		Clears a configured VRRP time.

The following is an example of configuring Master Router and Backup Router by comparing their Priorities: Virtual Routers, Layer 3 SWITCH 1 – 101 and Layer 3 SWITCH 2 – 102. Then, regardless of IP addresses, one that has higher Priority, Layer 3 SWITCH 2 becomes Master Router.

<Layer 3 SWITCH1: IP Address - 10.0.0.1/24>

```
SWTICH1(config)# router vrrp default 1
SWITCH1(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr-priority 101
SWITCH1(config-router)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
-------------------------------------------
state                     backup
virtual mac address         00:00:5E:00:01:01
advertisement interval       1 sec
preemption                 enabled
priority                   101
master down interval         3.624 sec
 [1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWTICH2(config)# router vrrp default 1
SWITCH2(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr-priority 102
SWITCH2(config-router)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
-------------------------------------------
state                     master
virtual mac address         00:00:5E:00:01:01
advertisement interval       1 sec
preemption                 enabled
priority                   102
master down interval         3.620 sec
 [1] associate address : 10.0.0.5
```

SWITCH 2 with higher priority is configured as Master.

By default, Priority of the hiD 6615 S323 is configured as “100”. So, unless you configure specific Priority, this switch becomes Master Router because a device, which has lower IP address, has higher precedence.

Also, when there are more than two Backup Routers, IP addresses are compared to decide order. The following is an example of configuring Master Router and Backup Router by comparing IP addresses: Virtual Routers, Layer 3 SWITCH 1 – 10.0.0.1 and Layer 3 SWITCH 2 – 10.0.0.2.

<Layer 3 SWITCH1: IP address - 10.0.0.1/24>

```
SWTICH1(config)# router vrrp default 1
SWITCH1(config-router)# associate 10.0.0.5
SWITCH1(config-router)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
-------------------------------------------
state                     master
virtual mac address         00:00:5E:00:01:01
advertisement interval       1 sec
preemption                 enabled
priority                   100
master down interval         3.624 sec
 [1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWTICH2(config)# router vrrp default 1
SWITCH2(config-router)# associate 10.0.0.5
SWITCH2(config-router)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
-------------------------------------------
state                     backup
virtual mac address         00:00:5E:00:01:01
advertisement interval       1 sec
preemption                 enabled
priority                   100
master down interval         3.620 sec
 [1] associate address : 10.0.0.5
```

In case of same priorities, SWITCH 1 with lower IP address is configured as Master.

8.4.1.4 VRRP Track Function

When the link connected to Master Router of VRRP is off as below, if link of Master Router is not recognized, the users on the interface are not able to communicate because the interface is not able to access to Master Router.

In the condition that Link to VRRP's master router is down as the figure shown below, or the link of Master Router cannot be recognized, the communication would be impossible.

For the hiD 6615 S323, you can configure Master Router to be changed by giving lower Priority to Master Router when the link of Mater Router is disconnected. This function is VRRP Track.

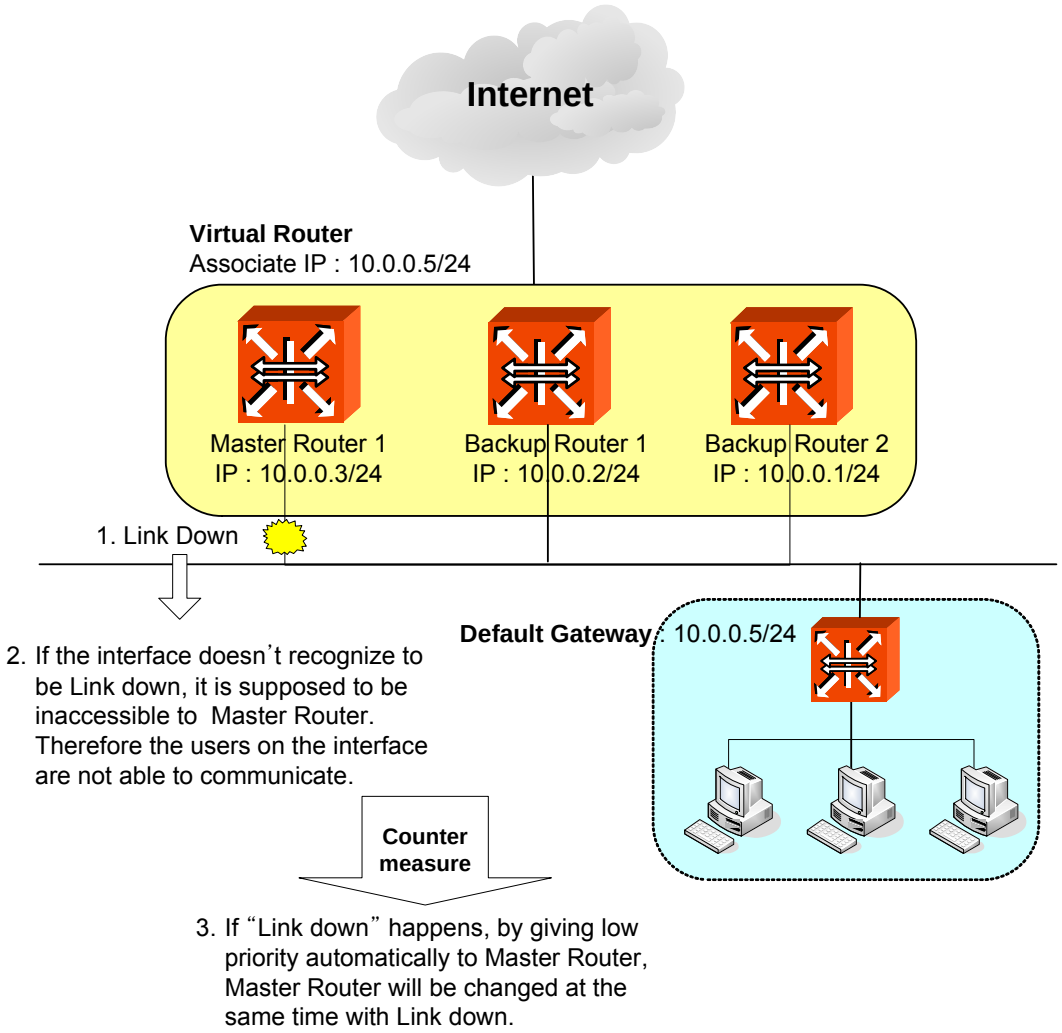


Fig. 8.29 VRRP Track

To configure VRRP Track, use the following command.

Command	Mode	Description
track interface *INTERFACE* **priority** <1-254>	VRRP	Configures VRRP Track. The Priority becomes lower as the configured value.

To release VRRP Track configuration, use the following command.

Command	Mode	Description
no track interface *INTERFACE*	VRRP	Disables VRRP Track configuration.

8.4.1.5 Authentication Password

If anyone knows Group ID and Associated IP address, he can configure another device as a Virtual Router. To prevent this, user needs to configure a password, named authentication password that can be used only in Virtual Router user configured.

To configure an authentication password for security of Virtual Router, use the following command on VRRP configuration mode.

Command	Mode	Description
authentication clear_text *PASSWORD*	VRRP	Configures an authentication password.
no authentication		Deletes a configured authentication password.

Authentication password can be configured with maximum 7 digits.

The following is an example of configuring Authentication password in Virtual Router as network and showing it.

```
SWITCH(config-vrrp)# authentication clear_text network
SWITCH(config-vrrp)# show running-config
Building configuration...
(Omitted)
vrrp default 1
 authentication clear_text network
 associate 10.0.0.5
no snmp
SWITCH(config-vrrp)#
```

8.4.1.6 Preempt

Preempt is a function that an added device with the highest Priority user gave is automatically configured as Master Router without rebooting or specific configuration when you add an other device after Virtual Router is configured.

To configure Preempt, use the following command on VRRP configuration mode.

Command	Mode	Description
preempt {**enable** | **disable**}	VRRP	Enables or disables Preempt. (default: enable)

The following is an example of disabling Preempt.

```
SWITCH(config-vrrp)# preempt disable
SWITCH(config-vrrp)# exit
SWITCH(config)# show vrrp

default - virtual router 1
------------------------------------------
state                     master
virtual mac address         00:00:5E:00:01:01
advertisement interval       1 sec
preemption                  disabled
priority                   100
master down interval         3.624 sec
 [1] associate address : 10.0.0.5

SWITCH(config)#
```

Also, to make Preempt “enable” as default setting, use the following command on VRRP configuration mode.

Command	Mode	Description
no preempt	VRRP	Deletes the former configuration of Preempt to enable it.

8.4.1.7 VRRP Statistics

To display the VRRP statistics that packets have been sent and received, use the following command.

Command	Mode	Description
show vrrp stat	Enable Global Bridge VRRP	Shows statistics of packets in Virtual Router Group.

The following is an example of viewing statistics of packets in Virtual Router Group.

```
SWITCH(config)# show vrrp stat
 VRRP statistics :
  VRRP packets rcvd with invalid TTL       0
  VRRP packets rcvd with invalid version    0
  VRRP packets rcvd with invalid VRID      0
  VRRP packets rcvd with invalid size      0
  VRRP packets rcvd with invalid checksum   0
  VRRP packets rcvd with invalid auth-type  0
  VRRP packets rcvd with interval mismatch  0

SWITCH(config)#
```

To clear the VRRP statistics information, use the following command.

Command	Mode	Description
clear vrrp stat	Enable Global Bridge VRRP	Clears statistics of packets in Virtual Router Group.

8.5 Rate Limit

User can customize port bandwidth according to user’s environment. By this configuration, you can prevent a certain port to monopolize whole bandwidth so that all ports can use bandwidth equally. Egress and ingress can be configured both to be same and to be different.

The hiD 6615 S223/S323 can apply the rate limit and support ingress policing and egress shaping.

8.5.1 Configuring Rate Limit

To set a port bandwidth, use the following command.

Command	Mode	Description
rate *PORTS RATE* [**egress** | **ingress**]	Bridge	Sets port bandwidth. If you input egress or ingress, you can configure outgoing packet or incoming packet. The unit is 64 Kbps.
no rate *PORTS*		Clears rate configuration of a specific port.
no rate *PORTS* [**egress** | **ingress**]		Clears rate configuration of a specific port by transmitting direction.

Unless you input neither egress nor ingress, they are configured to be same. To switch, egress is incoming packet. To display the configured bandwidth, use the following command.

Command	Mode	Description
show rate	Global	Shows the configured bandwidth.

8.5.2 Sample Configuration

The following is an example of showing the configuration after setting the bandwidth of 64Mbps to port number 1 and 128Mbps to the port number 2.

```
SWTICH(bridge)# rate 1 64
SWTICH(bridge)# rate 2 128
SWTICH(bridge)# show rate
 unit : kbps E : Enhanced
--------------------------------------------------------------------------------
Port |   Ingress   |    Egress    | Port |   Ingress   |    Egress
-----------------------------------------+-------------------------------------
   1  |       64    |       64     |   2  |      128    |      128
   3  |      N/A    |      N/A     |   4  |      N/A    |      N/A
   5  |      N/A    |      N/A     |   6  |      N/A    |      N/A
   7  |      N/A    |      N/A     |   8  |      N/A    |      N/A
SWTICH(bridge)#
```

8.6 Flood Guard

Flood-guard limits number of packets, how many packets can be transmitted, in configured bandwidth, whereas Rate limit controls packets through configuring width of bandwidth, which packets pass through. This function prevents receiving packets more than configured amount without enlarging bandwidth.

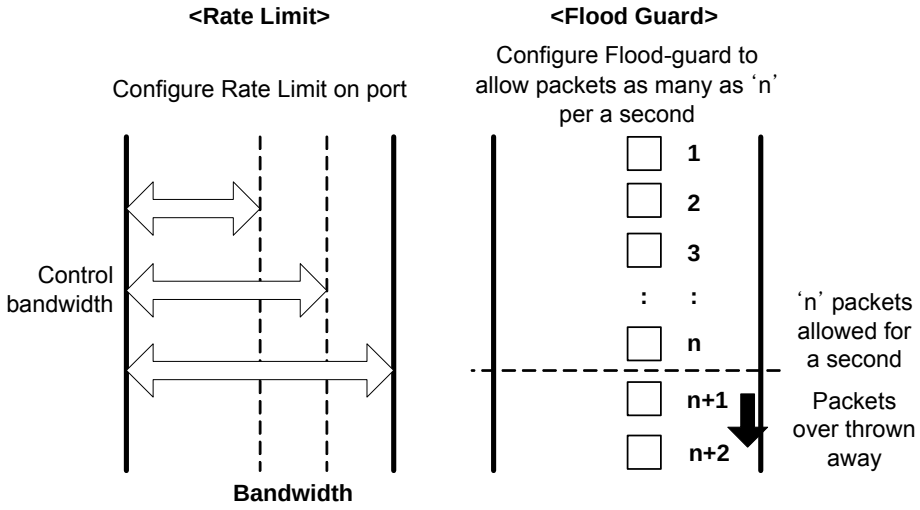


Fig. 8.30 Rate Limit and Flood Guard

8.6.1 Configuring Flood-Guard

To configure the number of packets, which can be transmitted in a second, use the following command.

Command	Mode	Description
mac-flood-guard *PORTS* <1-2000000>	Bridge	Limits the number of packets which can be transmitted to the port for 1 second.
no mac-flood-guard *PORTS*		Clears the configured Flood Guard.

To display a configuration of flood guard, use the following command.

Command	Mode	Description
show mac-flood-guard [**macs**]	Bridge	Shows the configured Flood Guard.

8.6.2 Sample Configuration

The following is an example of showing the configuration after limiting the number of packets transmitted to the port number 1 as 10,000.

```
SWITCH(bridge)# mac-flood-guard 1 10000
SWITCH(bridge)# show mac-flood-guard
--------------------------------
 Port Rate(fps) | Port Rate(fps)
---------------+----------------
   1    10000    |   2  Unlimited
   3  Unlimited |   4  Unlimited
   5  Unlimited |   6  Unlimited
   7  Unlimited |   8  Unlimited
   9  Unlimited |  10  Unlimited
  11  Unlimited |  12  Unlimited
  13  Unlimited |  14  Unlimited
  15  Unlimited |  16  Unlimited
(Omitted)

SWITCH(bridge)#
```

8.7 Bandwidth

Routing protocol uses bandwidth information to measure routing distance value. To configure bandwidth of interface, use the following command.

Command	Mode	Description
bandwidth *BANDWIDTH*	Interface	Configures bandwidth of interface, enter the value of bandwidth.

i The bandwidth can be from 1 to 10,000,000 Kbits. This bandwidth is for routing information implement and it does not concern physical bandwidth.

To delete a configured bandwidth, use the following command.

Command	Mode	Description
no bandwidth *BANDWIDTH*	Interface	Deletes configured bandwidth of interface, enter the value.

The following is an example of configuration to bandwidth as 1000.

```
SWITCH(config-if)# bandwidth 1000
SWITCH(config-if)# show running-config interface 1
!
interface default
 bandwidth 1m
 ip address 10.27.41.181/24
!
SWITCH(config-if)#
```

8.8 Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is a TCP/IP standard for simplifying the administrative management of IP address configuration by automating address configuration for network clients. The DHCP standard provides for the use of DHCP servers as a way to manage dynamic allocation of IP addresses and other related configuration details to DHCP-enabled clients on the network.

Every device on a TCP/IP network must have a unique IP address in order to access the network and its resources. The IP address (together with its related subnet mask) identifies both the host computer and the subnet to which it is attached. When you move a computer to a different subnet, the IP address must be changed. DHCP allows you to dynamically assign an IP address to a client from a DHCP server IP address database on the local network.

The DHCP provides the following benefits:

Saving Cost

Numerous users can access the IP network with a small amount of IP resources in the environment that most users do not have to access the IP network at the same time all day long. This allows the network administrators to save the cost and IP resources.

Efficient IP Management

By deploying DHCP in a network, this entire process is automated and centrally managed. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it logs on to the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

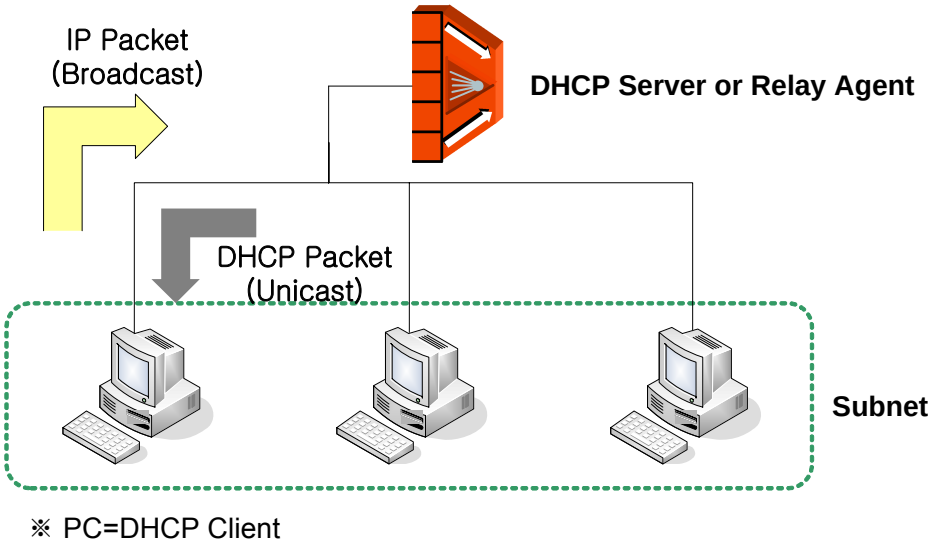


Fig. 8.31 DHCP Service Structure

The hiD 6615 S223/S323 flexibly provides the functions as the DHCP server or DHCP relay agent according to your DHCP configuration.

This chapter contains the following sections:

- DHCP Server
- DHCP Address Allocation with Option 82
- DHCP Lease Database
- DHCP Relay Agent
- DHCP Option 82
- DHCP Client
- DHCP Snooping
- IP Source Guard
- DHCP Filtering
- Debugging DHCP

8.8.1 DHCP Server

This section describes the following DHCP server related features and configurations:

- DHCP Pool Creation
- DHCP Subnet
- Range of IP Address
- Default Gateway
- IP Lease Time
- DNS Server
- Manual Binding
- Domain Name
- DHCP Server Option
- Static Mapping
- Recognition of DHCP Client
- IP Address Validation
- Authorized ARP
- Prohibition of 1:N IP Address Assignment
- Ignoring BOOTP Request
- DHCP Packet Statistics
- Displaying DHCP Pool Configuration

To activate/deactivate the DHCP function in the system, use the following command.

Command	Mode	Description
service dhcp	Global	Activates the DHCP function in the system.
no service dhcp		Deactivates the DHCP function in the system.

i Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

8.8.1.1 DHCP Pool Creation

The DHCP pool is a group of IP addresses that will be assigned to DHCP clients by DHCP server. You can create various DHCP pools that can be configured with a different network, default gateway and range of IP addresses. This allows the network administrators to effectively handle multiple DHCP environments.

To create a DHCP pool, use the following command.

Command	Mode	Description
ip dhcp pool *POOL*	Global	Creates a DHCP pool and opens *DHCP Pool Configuration* mode.
no ip dhcp pool *POOL*		Deletes a created DHCP pool.

The following is an example of creating the DHCP pool as *sample*.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])#
```

8.8.1.2 DHCP Subnet

To specify a subnet of the DHCP pool, use the following command.

Command	Mode	Description
network *A.B.C.D/M*	DHCP Pool	Specifies a subnet of the DHCP pool. A.B.C.D/M: network address
no network *A.B.C.D/M*		Deletes a specified subnet.

The following is an example of specifying the subnet as 100.1.1.0/24.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])#
```

i You can also specify several subnets in a single DHCP pool.

8.8.1.3 Range of IP Address

To specify a range of IP addresses that will be assigned to DHCP clients, use the following command.

Command	Mode	Description
range *A.B.C.D A.B.C.D*	DHCP Pool	Specifies a range of IP addresses. A.B.C.D: start/end IP address
no range *A.B.C.D A.B.C.D*		Deletes a specified range of IP addresses.

The following is an example for specifying the range of IP addresses.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])#
```

You can also specify several inconsecutive ranges of IP addresses in a single DHCP pool, e.g. 100.1.1.1 to 100.1.1.62 and 100.1.1.129 to 100.1.1.190.

When specifying a range of IP address, the start IP address must be prior to the end IP address.

8.8.1.4 Default Gateway

To specify a default gateway of the DHCP pool, use the following command.

Command	Mode	Description
default-router *A.B.C.D1* [*A.B.C.D2*] ... [*A.B.C.D8*]	DHCP Pool	Specifies a default gateway of the DHCP pool. A.B.C.D: default gateway IP address
no default-router *A.B.C.D1* [*A.B.C.D2*] ... [*A.B.C.D8*]		Deletes a specified default gateway.
no default-router all		Deletes all the specified default gateways.

The following is an example of specifying the default gateway 100.1.1.254.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])#
```

8.8.1.5 IP Lease Time

Basically, the DHCP server leases an IP address in the DHCP pool to DHCP clients, which will be automatically returned to the DHCP pool when it is no longer in use or expired by IP lease time.

To specify IP lease time, use the following command.

Command	Mode	Description
lease-time default <120-2147483637>	DHCP Pool	Sets default IP lease time in the unit of second. (default: 3600)
lease-time max <120-2147483637>		Sets maximum IP lease time in the unit of second. (default: 3600)
no lease-time {**default** | **max**}		Deletes specified IP lease time.

The following is an example of setting default and maximum IP lease time.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])# lease-time default 5000
SWITCH(config-dhcp[sample])# lease-time max 10000
SWITCH(config-dhcp[sample])#
```

8.8.1.6 DNS Server

To specify a DNS server to inform DHCP clients, use the following command.

Command	Mode	Description
dns-server *A.B.C.D1* [*A.B.C.D2*] ... [*A.B.C.D8*]	DHCP Pool	Specifies a DNS server. Up to 8 DNS servers are possible. A.B.C.D: DNS server IP address
no dns-server *A.B.C.D1* [*A.B.C.D2*] ... [*A.B.C.D8*]		Deletes a specified DNS server.
no dns-server all		Deletes all the specified DNS servers.

The following is an example of specifying a DNS server.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])# network 100.1.1.0/24
SWITCH(config-dhcp[sample])# default-router 100.1.1.254
SWITCH(config-dhcp[sample])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[sample])# lease-time default 5000
SWITCH(config-dhcp[sample])# lease-time max 10000
SWITCH(config-dhcp[sample])# dns-server 200.1.1.1 200.1.1.2 200.1.1.3
SWITCH(config-dhcp[sample])#
```

If you want to specify a DNS server for all the DHCP pools, use the **dns server** command. For more information, see Section 6.1.9.

8.8.1.7 Manual Binding

To manually assign a static IP address to a DHCP client who has a specified MAC address, use the following command.

Command	Mode	Description
fixed-address *A.B.C.D* *MAC-ADDRESS*	DHCP Pool	Assigns a static IP address to a DHCP client. A.B.C.D: static IP address MAC-ADDRESS: MAC address
no fixed-address *A.B.C.D*		Deletes a specified static IP assignment.

8.8.1.8 Domain Name

To set a domain name, use the following command.

Command	Mode	Description
domain-name *DOMAIN*	DHCP Pool	Sets a domain name.
no domain-name		Deletes a specified domain name.

8.8.1.9 DHCP Server Option

If a DHCP server option is specified, the DHCP server will respond only to DHCP messages that carry the same option information.

To specify a DHCP server option, use the following command.

Command	Mode	Description
option <1-254> [<1-8>] {**ip** *A.B.C.D* | **hex** *HEXSTRING* | **text** *STRING*}	DHCP Pool	Specifies a DHCP option. 1-254: DHCP option code 1-8: instance number of the option code ip | hex | text: DHCP option information
no option <1-254> [<1-8>]		Deletes a specified DHCP option.

The already-defined DHCP option codes or the DHCP option codes only for the DHCP client cannot be specified with this command, e.g. **option 82**.

8.8.1.10 Static Mapping

The hiD 6615 S223/S323 provides a static mapping function that enables to assign a static IP address without manually specifying static IP assignment by using a DHCP lease database in the DHCP database agent.

To perform a static mapping, use the following command.

Command	Mode	Description
origin file *A.B.C.D FILE*	DHCP Pool	Performs a static mapping. A.B.C.D: DHCP database agent address FILE: file name of DHCP lease database
no origin file		Cancels a static mapping.

For more information of the file naming of a DHCP lease database, see Section 8.8.3.1.

8.8.1.11 Recognition of DHCP Client

Normally, a DHCP server recognizes DHCP clients with a client ID. However, some DHCP clients may not have their own client ID. In this case, you can select the recognition method as a hardware address instead of a client ID.

To select a recognition method of DHCP clients, use the following command.

Command	Mode	Description
ip dhcp database-key {**client-id** | **hardware-address**}	Global	Selects a recognition method of DHCP clients

8.8.1.12 IP Address Validation

Before assigning an IP address to a DHCP client, a DHCP server will validate if the IP address is used by another DHCP client with a ping or ARP. If the IP address does not respond to a requested ping or ARP, the DHCP server will realize that the IP address is not used then will assign the IP address to the DHCP client.

To select an IP address validation method, use the following command.

Command	Mode	Description
ip dhcp validate {**arp** | **ping**}	Global	Selects an IP address validation method.

You can also set a validation value of how many responses and how long waiting (timeout) for the responses from an IP address for a requested ping or ARP when a DHCP server validates an IP address.

To set a validation value of how many responses from an IP address for a requested ping or ARP, use the following command.

Command	Mode	Description
ip dhcp {**arp** | **ping**} **packet** <0-20>	Global	Sets a validation value of how many responses. 0-20: response value (default: 2)

To set a validation value of timeout for the responses from an IP address for a requested ping or ARP, use the following command.

Command	Mode	Description
ip dhcp {**arp** | **ping**} **timeout** <100-5000>	Global	Sets a validation value of timeout for the responses in the unit of millisecond. 100-5000: timeout value (default: 500)

8.8.1.13 Authorized ARP

The authorized ARP is to limit the leasing of IP addresses to authorized users. This function strengthens security by blocking ARP responses from unauthorized users at the DHCP server.

To disacrd an ARP response from unauthorized user, use the following command.

Command	Mode	Description
ip dhcp authorized-arp <120-2147483637>	Global	Discards an ARP response from unauthorized user. 120-2147483637: starting time (multiples of 30)
no ip dhcp authorized-arp		Disables the authorized ARP function.

To display a list of valid or invalid (blocked) IP addresses, use the following command.

Command	Mode	Description
show ip dhcp authorized-arp valid	Enable Global Bridge	Shows a list of valid IP addresses.
show ip dhcp authorized-arp invalid		Shows a list of invalid (discarded) IP addresses.

To delete a list of invalid (blocked) IP addresses, use the following command.

Command	Mode	Description
clear ip dhcp authorized-arp invalid	Enable Global Bridge	Deletes a list of invalid (discarded) IP addresses.

8.8.1.14 Prohibition of 1:N IP Address Assignment

The DHCP server may assign plural IP addresses to a single DHCP client in case of plural DHCP requests from the DHCP client which has the same hardware address. Some network devices may need plural IP addresses, but most DHCP clients like personal computers need only a single IP address. In this case, you can configure the hiD 6615 S223/S323 to prohibit assigning plural IP addresses to a single DHCP client.

To prohibit assigning plural IP addresses to a DHCP client, use the following command.

Command	Mode	Description
ip dhcp check client-hardware-address	Global	Prohibits assigning plural IP addresses.
no ip dhcp check client-hardware-address		Permits assigning plural IP addresses.

8.8.1.15 Ignoring BOOTP Request

To allow a DHCP server to ignore received bootstrap protocol (BOOTP) request packets, use the following command.

Command	Mode	Description
ip dhcp bootp ignore	Global	Ignores BOOTP request packets.
no ip dhcp bootp ignore		Permits BOOTP request packets.

8.8.1.16 DHCP Packet Statistics

To display DHCP packet statistics of the DHCP server, use the following command.

Command	Mode	Description
show ip dhcp server statistics	Enable Global Bridge	Shows DHCP packet statistics.
clear ip dhcp statistics		Deletes collected DHCP packet statistics.

The following is an example of displaying DHCP packet statistics.

```
SWITCH(config)# show ip dhcp server statistics

 ========================================
 Message            Recieved/Error(0/0)
 ----------------------------------------
 DHCP DISCOVER              0
 DHCP REQUEST               0
 DHCP DECLINE               0
 DHCP RELEASE               0
 DHCP INFORM                0

 ======================================
 Message            Sent/Error(0/0)
 --------------------------------------
 DHCP OFFER                 0
 DHCP ACK                   0
 DHCP NAK                   0

SWITCH(config)#
```

8.8.1.17 Displaying DHCP Pool Configuration

To display a DHCP pool configuration, use the following command.

Command	Mode	Description
show ip dhcp pool [*POOL*]	Enable Global Bridge	Shows a DHCP pool configuration.
show ip dhcp pool summary [*POOL*]		Shows a summary of a DHCP pool configuration. POOL: pool name

The following is an example of displaying a DHCP pool configuration.

```
SWITCH(config)# show ip dhcp pool summary
[Total -- 1 Pools]
 Total     0                                0.00 of total
 Available 0                                0.00 of total
 Abandon   0                                0.00 of total
 Bound     0                                0.00 of total
 Offered   0                                0.00 of total
 Fixed     0                                0.00 of total

[sample]

 Total     0           0.00% of the pool    0.00 of total
 Available 0           0.00% of the pool    0.00 of total
 Abandon   0           0.00% of the pool    0.00 of total
 Bound     0           0.00% of the pool    0.00 of total
 Offered   0           0.00% of the pool    0.00 of total
 Fixed     0           0.00% of the pool    0.00 of total

SWITCH(config)#
```

8.8.2 DHCP Address Allocation with Option 82

The DHCP server provided by the hiD 6615 S223/S323 can assign dynamic IP addresses based on DHCP option 82 information sent by the DHCP relay agent.

The information sent via DHCP option 82 will be used to identify which port the DHCP_REQUEST came in on. The feature introduces a new DHCP class capability, which is a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside. The DHCP class can be configured with option 82 information and a range of IP addresses.

8.8.2.1 DHCP Class Capability

To enable the DHCP server to use a DHCP class to assign IP addresses, use the following command.

Command	Mode	Description
ip dhcp use class	Global	Enables the DHCP server to use a DHCP class to assign IP addresses.
no ip dhcp use class		Disables the DHCP server to use a DHCP class.

8.8.2.2 DHCP Class Creation

To create a DHCP class, use the following command.

Command	Mode	Description
ip dhcp class *CLASS*	Global	Creates a DHCP class and opens *DHCP Class Configuration* mode. CLASS: DHCP class name
no ip dhcp class [*CLASS*]		Deletes a created DHCP class.

8.8.2.3 Relay Agent Information Pattern

To specify option 82 information for IP assignment, use the following command.

Command	Mode	Description
relay-information remote-id ip *A.B.C.D* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]	DHCP Class	Specifies option 82 information for IP assignment.
relay-information remote-id hex *HEXSTRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		
relay-information remote-id text *STRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		

To delete specified option 82 information for IP assignment, use the following command.

Command	Mode	Description
no relay-information remote-id ip *A.B.C.D* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]	DHCP Class	Deletes specified option 82 information for IP assignment.
no relay-information remote-id hex *HEXSTRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		
no relay-information remote-id text *STRING* [**circuit-id** {**hex** *HEXSTRING* | **index** <0-65535> | **text** *STRING*}]		

To delete specified option 82 information for IP assignment, use the following command.

Command	Mode	Description
no relay-information remote-id all	DHCP Class	Deletes all specified option 82 information that contains only a remote ID.
no relay-information all		Deletes all specified option 82 information.

8.8.2.4 Associating DHCP Class

To associate a DHCP class with a current DHCP pool, use the following command.

Command	Mode	Description
class *CLASS*	DHCP Pool	Associates a DHCP class with a DHCP pool and opens *DHCP Pool Class Configuration* mode. CLASS: DHCP class name
no class [*CLASS*]		Releases an associated DHCP class from a current DHCP pool.

8.8.2.5 Range of IP Address for DHCP Class

To specify a range of IP addresses for a DHCP class, use the following command.

Command	Mode	Description
address range *A.B.C.D A.B.C.D*	DHCP Pool Class	Specifies a range of IP addresses. A.B.C.D: start/end IP address
no address range *A.B.C.D A.B.C.D*		Deletes a specified range of IP addresses.

A range of IP addresses specified with the **address range** command is valid only for a current DHCP pool. Even if you associate the DHCP class with another DHCP pool, the specified range of IP addresses will not be applicable.

8.8.3 DHCP Lease Database

8.8.3.1 DHCP Database Agent

The hiD 6615 S223/S323 provides a feature that allows to a DHCP server automatically saves a DHCP lease database on a DHCP database agent.

The DHCP database agent should be a TFTP server, which stores a DHCP lease database as numerous files in the form of **leasedb.***MAC-ADDRESS*, e.g. **leasedb.***0A:31:4B:1A:77:6A*. The DHCP lease database contains a leased IP address, hardware address, etc.

To specify a DHCP database agent and enable an automatic DHCP lease database back-up, use the following command.

Command	Mode	Description
ip dhcp database *A.B.C.D INTERVAL*	Global	Specifies a DHCP database agent and back-up interval. A.B.C.D: DHCP database agent address INTERVAL: 120-2147483637 (unit: second)
no ip dhcp database		Deletes a specified DHCP database agent.

i Upon entering the **ip dhcp database** command, the back-up interval will begin.

To display a configuration of the DHCP database agent, use the following command.

Command	Mode	Description
show ip dhcp database	Enable Global Bridge	Shows a configuration of the DHCP database agent.

8.8.3.2 Displaying DHCP Lease Status

To display current DHCP lease status, use the following command.

Command	Mode	Description
show ip dhcp lease {**all** | **bound** | **abandon** | **offer** | **fixed** | **free**} [*POOL*]	Enable Global Bridge	Shows current DHCP lease status. all: all IP addresses bound: assigned IP address abandon: illegally assigned IP address offer: IP address being ready to be assigned fixed: manually assigned IP address free: remaining IP address POOL: pool name
show ip dhcp lease detail [*A.B.C.D*]		

8.8.3.3 Deleting DHCP Lease Database

To delete a DHCP lease database, use the following command.

Command	Mode	Description
clear ip dhcp leasedb *A.B.C.D/M*	Enable Global	Deletes a DHCP lease database a specified subnet.
clear ip dhcp leasedb pool *POOL*		Deletes a DHCP lease database of a specified DHCP pool.
clear ip dhcp leasedb all		Deletes the entire DHCP lease database.

8.8.4 DHCP Relay Agent

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. The DHCP relay agents are used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. The DHCP relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently.

By contrast, DHCP relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The DHCP relay agent sets the gateway address and, if configured, adds the DHCP option 82 information in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing the DHCP option 82 information.

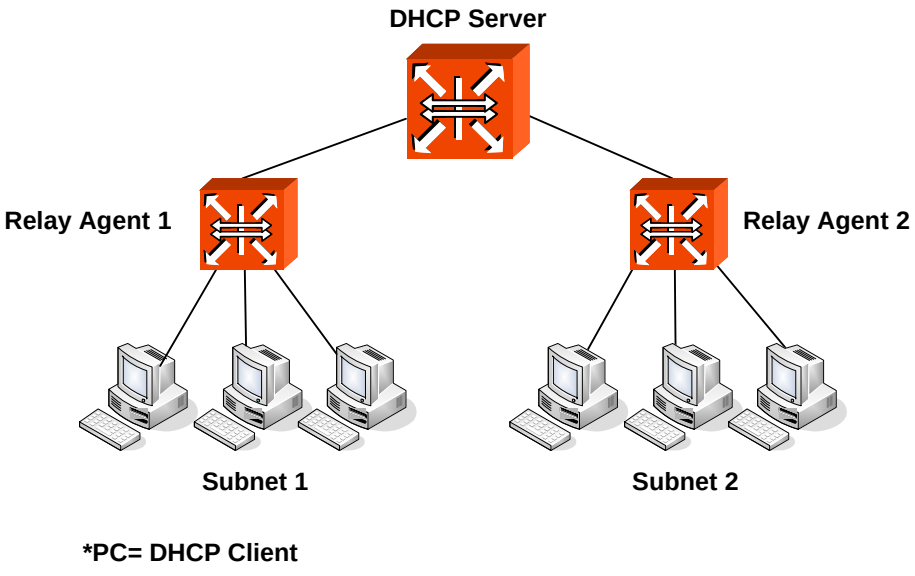


Fig. 8.32 Example of DHCP Relay Agent

To activate/deactivate the DHCP function in the system, use the following command.

Command	Mode	Description
service dhcp	Global	Activates the DHCP function in the system.
no service dhcp		Deactivates the DHCP function in the system.

Before configuring DHCP server or relay, you need to use the **service dhcp** command first to activate the DHCP function in the system.

8.8.4.1 Packet Forwarding Address

A DHCP client sends DHCP_DISCOVER message to a DHCP server. DHCP_DISCOVER message is broadcasted within the network to which it is attached. If the client is on a network that does not have any DHCP server, the broadcast is not forwarded because the switch is configured to not forward broadcast traffic. To solve this problem, you can configure the interface that is receiving the broadcasts to forward certain classes of broadcast to a helper address.

To specify a packet forwarding address, use the following command.

Command	Mode	Description
ip dhcp helper-address *A.B.C.D*	Interface	Specifies a packet forwarding address. More than one address is possible. A.B.C.D: DHCP server address
no ip dhcp helper-address {*A.B.C.D* | **all**}		Deletes a specified packet forwarding address.

If a packet forwarding address is specified on an interface, the hiD 6615 S223/S323 will enable a DHCP relay agent.

You can also specify an organizationally unique identifier (OUI) when configuring a packet forwarding address. The OUI is a 24-bit number assigned to a company or organization for use in various network hardware products which is a first 24 bits of a MAC address. If an OUI is specified, a DHCP relay agent will forward DHCP_DISCOVER message to a specific DHCP server according to a specified OUI.

To specify a packet forwarding address with an OUI, use the following command.

Command	Mode	Description
ip dhcp oui *XX:XX:XX* **helper-address** *A.B.C.D*	Interface	Specifies a packet forwarding address with an OUI. More than one address is possible. XX:XX:XX: OUI (first 24 bits of a MAC address in the form of hexadecimal) A.B.C.D: DHCP server address
no ip dhcp oui *XX:XX:XX* [**helper-address** *A.B.C.D*]		Deletes a specified packet forwarding address.

8.8.4.2 Smart Relay Agent Forwarding

Normally, a DHCP relay agent forwards DHCP_DISCOVER message to a DHCP server only with a primary IP address on an interface, even if there is more than one IP address on the interface.

If the smart relay agent forwarding is enabled, a DHCP relay agent will retry sending DHCP_DISCOVER message with a secondary IP address, in case of no response from the DHCP server.

To enable the smart relay agent forwarding, use the following command.

Command	Mode	Description
ip dhcp smart-relay	Global	Enables a smart relay.
no ip dhcp smart-relay		Disables a smart relay.

8.8.5 DHCP Option 82

In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the DHCP option 82, a DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP relay agent will automatically add the circuit ID and the remote ID to the option 82 field in the DHCP packets and forward them to the DHCP server.

The DHCP option 82 resolves the following issues in an environment in which untrusted hosts access the internet via a circuit based public network:

Broadcast Forwarding

The DHCP option 82 allows a DHCP relay agent to reduce unnecessary broadcast flooding by forwarding the normally broadcasted DHCP response only on the circuit indicated in the circuit ID.

DHCP Address Exhaustion

In general, a DHCP server may be extended to maintain a DHCP lease database with an IP address, hardware address and remote ID. The DHCP server should implement policies that restrict the number of IP addresses to be assigned to a single remote ID.

Static Assignment

A DHCP server may use the remote ID to select the IP address to be assigned. It may permit static assignment of IP addresses to particular remote IDs, and disallow an address request from an unauthorized remote ID.

IP Spoofing

A DHCP client may associate the IP address assigned by a DHCP server in a forwarded DHCP_ACK message with the circuit to which it was forwarded. The circuit access device may prevent forwarding of IP packets with source IP addresses, other than, those it has associated with the receiving circuit. This prevents simple IP spoofing attacks on the central LAN, and IP spoofing of other hosts.

MAC Address Spoofing

By associating a MAC address with a remote ID, a DHCP server can prevent offering an IP address to an attacker spoofing the same MAC address on a different remote ID.

Client Identifier Spoofing

By using the agent-supplied remote ID option, the untrusted and as-yet unstandardized client identifier field need not be used by the DHCP server.

Fig. 8.33 shows how the DHCP relay agent with the DHCP option 82 operates.

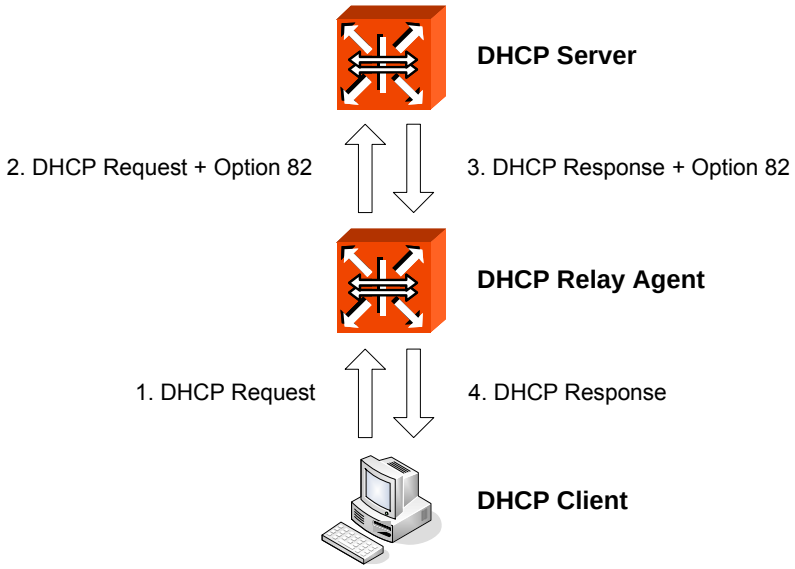


Fig. 8.33 DHCP Option 82 Operation

8.8.5.1 Enabling DHCP Option 82

To enable/disable the DHCP option 82, use the following command.

Command	Mode	Description
ip dhcp option82	Global	Enables the system to add the DHCP option 82 field.
no ip dhcp option82		Disables the system to add the DHCP option 82 field.

8.8.5.2 Option 82 Sub-Option

The DHCP option 82 enables a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement security and IP address assignment policies.

There are 2 sub-options for the DHCP option 82 information as follows:

- **Remote ID**
  This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits and have mechanisms to identify the remote host of the circuit. Note that, the remote ID must be globally unique.
- **Circuit ID**
  This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits. It encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by DHCP relay agents in forwarding DHCP responses back to the proper circuit.

To specify a remote ID, use the following command.

Command	Mode	Description
system-remote-id hex *HEXSTRING*	Option 82	Specifies a remote ID. (default: system MAC address)
system-remote-id ip *A.B.C.D*		
system-remote-id text *STRING*		

To specify a circuit ID, use the following command.

Command	Mode	Description
system-circuit-id *PORTS* **hex** *HEXSTRING*	Option 82	Specifies a circuit ID. (default: port number)
system-circuit-id *PORTS* **index** <0-65535>		
system-circuit-id *PORTS* **text** *STRING*		

To delete a specified remote and circuit ID, use the following command.

Command	Mode	Description
no system-remote-id	Option 82	Deletes a specified remote and circuit ID
no system-circuit-id *PORTS*		

8.8.5.3 Option 82 Reforwarding Policy

A DHCP relay agent may receive a DHCP packet from a DHCP server or another DHCP relay agent that already contains relay information. You can specify a DHCP option 82 reforwarding policy to be suitable for the network.

To specify a DHCP option 82 reforwarding policy, use the following command.

Command	Mode	Description
policy {**replace** | **keep**}	Option 82	Specifies a DHCP option 82 reforwarding policy. replace: replaces an existing DHCP option 82 information with a new one. keep: keeps an existing DHCP option 82 information (default).
policy drop {**normal** | **option82** | **none**}		normal: DHCP packet option82: DHCP option 82 packet none: no DHCP packet (default)

8.8.5.4 Option 82 Trust Policy

Default Trust Policy

To specify the default trust policy for DHCP packets, use the following command.

Command	Mode	Description
trust default {**deny** | **permit**}	Option 82	Specifies the default trust policy for a DHCP packet.

i If you specify the default trust policy as **deny**, the DHCP packet that carries the information you specifies below will be permitted, and vice versa.

Trusted Remote ID

To specify a trusted remote ID, use the following command.

Command	Mode	Description
trust remote-id hex *HEXSTRING*	Option 82	Specifies a trusted remote ID.
trust remote-id ip *A.B.C.D*		
trust remote-id text *STRING*		

To delete a specified trusted remote ID, use the following command.

Command	Mode	Description
no trust remote-id hex *HEXSTRING*	Option 82	Deletes a specified trusted remote ID.
no trust remote-id ip *A.B.C.D*		
no trust remote-id text *STRING*		

Trusted Physical Port

To specify a trusted physical port, use the following command.

Command	Mode	Description
trust port *PORTS* {**normal** | **option82** | **all**}	Option 82	Specifies a trusted physical port. normal: DHCP packet option82: DHCP option 82 packet all: DHCP + option 82 packet
no trust port {**all** | PORTS} {**normal** | **option82** | **all**}		Deletes a specified trusted port.

8.8.5.5 Simplified DHCP Option 82

In case of a DHCP option 82 environment, when forwarding DHCP messages to a DHCP server, a DHCP relay agent normally adds a relay agent information option to the DHCP messages and replaces a gateway address in the DHCP messages with a relay agent address.

On the other hand, in case of a simplified DHCP option 82 environment, a DHCP relay agent adds a relay agent information option to the DHCP messages without replacement of a gateway address field in the DHCP messages. This allows an enhanced security and efficient IP assignment in the Layer 2 environment with a relay agent information option.

To enable/disable the simplified DHCP option 82, use the following command.

Command	Mode	Description
ip dhcp simplified-opt82	Interface	Enables the simplified DHCP option 82.
no ip dhcp simplified-option82		Disables the simplified DHCP option 82.

8.8.6 DHCP Client

An interface of the hiD 6615 S223/S323 can be configured as a DHCP client, which can obtain an IP address from a DHCP server. The configurable DHCP client functionality allows a DHCP client to use a user-specified client ID, class ID or suggested lease time when requesting an IP address from a DHCP server. Once configured as a DHCP client, the hiD 6615 S223/S323 cannot be configured as a DHCP server or relay agent.

8.8.6.1 Enabling DHCP Client

To configure an interface as a DHCP client, use the following command.

Command	Mode	Description
ip address dhcp	Interface	Enables a DHCP client on an interface.
no ip address dhcp		Disables a DHCP client.

8.8.6.2 DHCP Client ID

To specify a client ID, use the following command.

Command	Mode	Description
ip dhcp client client-id hex *HEXSTRING*	Interface	Specifies a client ID.
ip dhcp client client-id text *STRING*		
no ip dhcp client client-id		Deletes a specified client ID.

8.8.6.3 DHCP Class ID

To specify a class ID, use the following command.

Command	Mode	Description
ip dhcp client class-id hex *HEXSTRING*	Interface	Specifies a class ID. (default: system MAC address)
ip dhcp client class-id text *STRING*		
no ip dhcp client class-id		Deletes a specified class ID.

8.8.6.4 Host Name

To specify a host name, use the following command.

Command	Mode	Description
ip dhcp client host-name *NAME*	Interface	Specifies a host name.
no ip dhcp client host-name		Deletes a specified host name.

8.8.6.5 IP Lease Time

To specify IP lease time that is requested to a DHCP server, use the following command.

Command	Mode	Description
ip dhcp client lease <120-2147483637>	Interface	Specifies IP lease time in the unit of second (default: 3600).
no ip dhcp client lease		Deletes a specified IP lease time.

8.8.6.6 Requesting Option

To configure a DHCP client to request an option from a DHCP server, use the following command.

Command	Mode	Description
ip dhcp client request {**domain-name** | **dns**}	Interface	Configures a DHCP client to request a specified option.

To configure a DHCP client not to request an option, use the following command.

Command	Mode	Description
no ip dhcp client request {**domain-name** | **dns**}	Interface	Configures a DHCP client not to request a specified option.

8.8.6.7 Forcing Release or Renewal of DHCP Lease

The hiD 6615 S223/S323 supports two independent operation: immediate release a DHCP lease for a DHCP client and force DHCP renewal of a lease for a DHCP client.

To force a release or renewal of a DHCP release for a DHCP client, use the following command.

Command	Mode	Description
release dhcp *INTERFACE*	Enable	Forces a release of a DHCP lease.
renew dhcp *INTERFACE*		Forces a renewal of a DHCP lease.

8.8.6.8 Displaying DHCP Client Configuration

To display a DHCP client configuration, use the following command.

Command	Mode	Description
show ip dhcp client *INTERFACE*	Enable Global Interface	Shows a configuration of DHCP client.

8.8.7 DHCP Snooping

For enhanced security, the hiD 6615 S223/S323 provides the DHCP snooping feature. The DHCP snooping filters untrusted DHCP messages and maintains a DHCP snooping binding table. An untrusted message is a message received from outside the network, and an untrusted interface is an interface configured to receive DHCP messages from outside the network.

The DHCP snooping basically permits all the trusted messages received from within the network and filters untrusted messages. In case of untrusted messages, all the binding entries are recorded in a DHCP snooping binding table. This table contains a hardware address, IP address, lease time, VLAN ID, interface, etc.

It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

8.8.7.1 Enabling DHCP Snooping

To enable the DHCP snooping on the system, use the following command

Command	Mode	Description
ip dhcp snooping	Global	Enables the DHCP snooping on the system.
no ip dhcp snooping		Disables the DHCP snooping on the system. (default)

Upon entering the **ip dhcp snooping** command, the DHCP_OFFER and DHCP_ACK messages from all the ports will be discarded before specifying a trusted port.

To enable the DHCP snooping on a VLAN, use the following command

Command	Mode	Description
ip dhcp snooping vlan *VLANS*	Global	Enables the DHCP snooping on a specified VLAN.
no ip dhcp snooping vlan *VLANS*		Disables the DHCP snooping on a specified VLAN.

You must enable DHCP snooping on the system before enabling DHCP snooping on a VLAN.

8.8.7.2 DHCP Trust State

To define a state of a port as trusted or untrusted, use the following command.

Command	Mode	Description
ip dhcp snooping trust *PORTS*	Global	Defines a state of a specified port as trusted.
no ip dhcp snooping trust *PORTS*		Defines a state of a specified port as untrusted.

Note that, the DHCP snooping only sees the DHCP_OFFER and DHCP_ACK messages which are received from untrusted interfaces.

8.8.7.3 DHCP Rate Limit

To set the number of DHCP packet per second (pps) that an interface can receive, use the following command.

Command	Mode	Description
ip dhcp snooping limit-rate *PORTS* <1-255>	Global	Sets a rate limit for DHCP packets. (unit: pps)
no ip dhcp snooping limit-rate *PORTS*		Deletes a rate limit for DHCP packets.

Normally, the DHCP rate limit is specified to untrusted interfaces and 15 pps is recommended for a proper value. However, if you want to set a rate limit for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value.

8.8.7.4 DHCP Lease Limit

The number of entry registration in DHCP snooping binding table can be limited. If there are too many DHCP clients on an interface and they request IP address at the same time, it may cause IP pool exhaustion.

To set the number of entry registration in DHCP snooping binding table, use the following command.

Command	Mode	Description
ip dhcp snooping limit-lease *PORTS* <1-2147483637>	Global	Enables a DHCP lease limit on a specified untrusted port. 1-2147483637: the number of entry registration
no ip dhcp snooping limit-lease *PORTS*		Deletes a DHCP lease limit.

You can limit the number of entry registration only for untrusted interfaces, because the DHCP snooping binding table only contains the information for DHCP messages from untrusted interfaces.

8.8.7.5 Source MAC Address Verification

The hiD 6615 S223/S323 can verify that the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

To enable the source MAC address verification, use the following command.

Command	Mode	Description
ip dhcp snooping verify mac-address	Global	Enables the source MAC address verification.
no ip dhcp snooping verify mac-address		Disables the source MAC address verification.

8.8.7.6 DHCP Snooping Database Agent

When DHCP snooping is enabled, the system uses the DHCP snooping binding database to store information about untrusted interfaces. Each database entry (binding) has an IP address, associated MAC address, lease time, interface to which the binding applies and VLAN to which the interface belongs.

To maintain the binding when reload the system, you must use DHCP snooping database agent. If the agent is not used, the DHCP snooping binding will be lost when the switch is rebooted. The mechanism for the database agent saves the binding in a file at a remote location. Upon reloading, the switch reads the file to build the database for the binding. The system keeps the current file by writing to the file as the database changes.

Specifying DHCP Snooping Database Agent

To specify a DHCP database agent and enable an automatic DHCP snooping database back-up, use the following command.

Command	Mode	Description
ip dhcp snooping database *A.B.C.D INTERVAL*	Global	Specifies a DHCP snooping database agent and back-up interval. A.B.C.D: DHCP snooping database agent address INTERVAL: 120-2147483637 (unit: second)
no ip dhcp snooping database		Deletes a specified DHCP snooping database agent.

To request snooping binding entries from a DHCP snooping database agent, use the following command.

Command	Mode	Description
ip dhcp snooping database renew *A.B.C.D*	Global	Requests snooping binding entries from a DHCP snooping database agent. A.B.C.D: DHCP snooping database agent address

Specifying DHCP Snooping Binding Entry

The DHCP snooping binding table contains a hardware address, IP address, lease time, VLAN ID, and port information that correspond to the untrusted interfaces of the system.

To manually specify a DHCP snooping binding entry, use the following command.

Command	Mode	Description
ip dhcp snooping binding <1-4094> *PORT A.B.C.D MAC-ADDR* <120-2147483637>	Global	Configures binding on DHCP snooping table. 1-4094: VLAN ID PORT: port number A.B.C.D: IP address MAC-ADDR: MAC address 120-2147483637: lease time (unit: second)
clear ip dhcp snooping binding *PORT* {*A.B.C.D* | **all**}		Releases configured binding on DHCP snooping table.

i The DHCP snooping database agent should be TFTP server.

8.8.7.7 Displaying DHCP Snooping Configuration

To display DHCP snooping table, use the following command.

Command	Mode	Description
show ip dhcp snooping	Enable Global	Shows a DHCP snooping configuration.
show ip dhcp snooping binding		Shows DHCP snooping binding entries.

8.8.8 IP Source Guard

IP source guard is similar to DHCP snooping. This function is used on DHCP snooping untrusted Layer 2 port. Basically, except for DHCP packets that are allowed by DHCP snooping process, all IP traffic comes into a port is blocked. If an authorized IP address from the DHCP server is assigned to a DHCP client, or if a static IP source binding is configured, the IP source guard restricts the IP traffic of client to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding will be filtered out. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.

IP source guard supports the Layer 2 port only, including both access and trunk. For each untrusted Layer 2 port, there are two levels of IP traffic security filtering:

- **Source IP Address Filter**
  IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted. An IP source address filter is changed when a new IP source entry binding is created or deleted on the port, which will be recalculated and reapplied in the hardware to reflect the IP source binding change. By default, if the IP filter is enabled without any IP source binding on the port, a default policy that denies all IP traffic is applied to the port. Similarly, when the IP filter is disabled, any IP source filter policy will be removed from the interface.
- **Source IP and MAC Address Filter**
  IP traffic is filtered based on its source IP address as well as its MAC address; only IP traffic with source IP and MAC addresses matching the IP source binding entry are permitted. When IP source guard is enabled in IP and MAC filtering mode, the DHCP snooping option 82 must be enabled to ensure that the DHCP protocol works properly. Without option 82 data, the switch cannot locate the client host port to forward the DHCP server reply. Instead, the DHCP server reply is dropped, and the client cannot obtain an IP address.

8.8.8.1 Enabling IP Source Guard

After configuring DHCP snooping, configure the IP source guard using the provided command. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

To enable IP source guard, DHCP snooping needs to be enabled.

To enable IP source guard with a source IP address filtering on a port, use the following command.

Command	Mode	Description
ip dhcp verify source *PORTS*	Global	Enables IP source guard with a source IP address filtering on a port.
no ip dhcp verify source *PORTS*		Disables IP source guard.

To enable IP source guard with a source IP address and MAC address filtering on a port, use the following command.

Command	Mode	Description
ip dhcp verify source port-security *PORTS*	Global	Enables IP source guard with a source IP address and MAC address filtering on a port.
no ip dhcp verify source port-security *PORTS*		Disables IP source guard.

You cannot configure IP source guard with the **ip dhcp verify source** and **ip dhcp verify source port-security** commands together.

8.8.8.2 Static IP Source Binding

The IP source binding table has bindings that are learned by DHCP snooping or manually specified with the **ip dhcp verify source binding** command. The switch uses the IP source binding table only when IP source guard is enabled.

To specify a static IP source binding entry, use the following command.

Command	Mode	Description
ip dhcp verify source binding <1-4094> *PORT A.B.C.D MAC-ADDR*	Global	Specifies a static IP source binding entry. 1-4094: VLAN ID PORT: port number A.B.C.D: IP address MAC-ADDR: MAC address
no ip dhcp verify source binding {*A.B.C.D* | **all**}		Deletes a specified static IP source binding.

8.8.8.3 Displaying IP Source Guard Configuration

To display IP source binding table, use the following command.

Command	Mode	Description
show ip dhcp verify source binding	Enable Global	Shows IP source binding entries.

8.8.9 DHCP Filtering

8.8.9.1 DHCP Packet Filtering

For the hiD 6615 S223/S323, it is possible to block the specific client with MAC address. If the blocked MAC address by administrator requests IP address, the server does not assign IP. This function is to strength the security of DHCP server.

The following is the function of blocking to assign IP address on a port.

Command	Mode	Description
ip dhcp filter-port *PORTS*	Global	Configures a port in order not to assign IP.
no ip dhcp filter-port *PORTS*		Disables DHCP packet filtering.

The following is to designate MAC address which IP address is not assigned.

Command	Mode	Description
ip dhcp filter-address *MAC-ADDR*	Global	Blocks a MAC address in case of requesting IP address. MAC-ADDR: MAC address
no ip dhcp filter-address *MAC-ADDR*		Disables DHCP MAC filtering.

8.8.9.2 DHCP Server Packet Filtering

Dynamic host configuration protocol (DHCP) makes DHCP server assign IP address to DHCP clients automatically and manage the IP address. Most ISP operators provide the service as such a way. At this time, if a DHCP client connects with the equipment that can be the other DHCP server such as Internet access gateway router, communication failure might be occurred.

DHCP filtering helps to operate DHCP service by blocking DHCP request which enters through subscriber's port and goes out into uplink port or the other subscriber's port and DHCP reply which enters to the subscriber's port.

In the Fig. 8.34, server A has the IP area from 192.168.10.1 to 192.168.10.10. Suppose a user connects with client 3 that can be DHCP server to A in order to share IP address from 10.1.1.1 to 10.1.1.10.

Here, if client 1 and client 2 are not blocked from client 3 of DHCP server, client 1 and client 2 will request and receive IP from client 3 so that communication blockage will be occurred. Therefore, the filtering function should be configured between client 1 and client 3, client 2 and client 3 in order to make client 1 and client 2 receive IP without difficulty from DHCP server A.

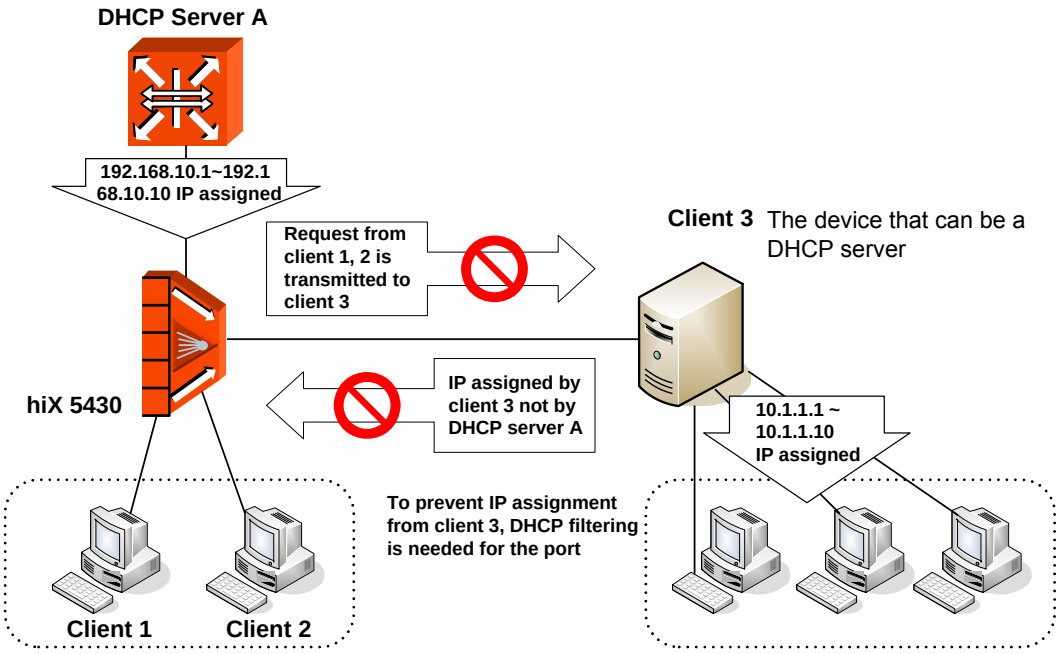


Fig. 8.34 DHCP Server Packet Filtering

To enable the DHCP server packet filtering, use the following command.

Command	Mode	Description
dhcp-server-filter *PORTS*	Bridge	Enables the DHCP server packet filtering.
no dhcp-server-filter *PORTS*		Disables the DHCP server packet filtering.

To display a status of the DHCP server packet filtering, use the following command.

Command	Mode	Description
show dhcp-server-filter	Enable Global Bridge	Show a status of the DHCP server packet filtering.

8.8.10 Debugging DHCP

To enable/disable a DHCP debugging, use the following command.

Command	Mode	Description
debug dhcp {**filter** | **lease** | **packet** | **service** | **all**}	Enable	Enables a DHCP debugging.
no debug dhcp {**filter** | **lease** | **packet** | **service** | **all**}		Disables a DHCP debugging.

8.9 Ethernet Ring Protection (ERP)

The ERP is a Siemens protection protocol and procedure to protect Ethernet ring topologies. It is a fast failure detection and recovery so that it decreases the time to prevent Loop under 50ms.

The main characteristics of the ERP are the follows:

- It required no additional underlying protection mechanism within the ring configuration, the complete functionality is implemented on the interface units of the system and does not require additional dedicated hardware which may raise network complexity and costs.
- It is a unique robustness functionality which runs on every network element involved in the ring configurations. It means each system is active part of the ring protection mechanism. Therefore, it guarantees a maximum of 50 ms to switch over towards a new configuration after link or system failures.
- ERP and STP cannot be configured at once.

8.9.1 ERP Operation

Ethernet Ring Protection (ERP) is a concept and protocol optimized for fast failure detection and recovery on Ethernet ring topologies. The Protection of fast failure detection and recovery occurs on RM Node. An Ethernet ring consists of two or more switches. One of the nodes on the ring is designated as redundancy manager (RM) and the two ring ports on the RM node are configured as primary port and secondary port respectively.

The RM blocks the secondary port for all non-control traffic belongs to this ERP domain. Here, if Line failure occurs, the Nodes detecting Link Failure transmit Link Down message and Link Failure port becomes Blocking status. When the RM nodes receive this link-down message, it immediately declares failed state, and opens the logically blocked protected VLANs on the secondary port. Then, Ethernet Ring restarts the communication.

The following is ERP operation when Link Failure occurs.

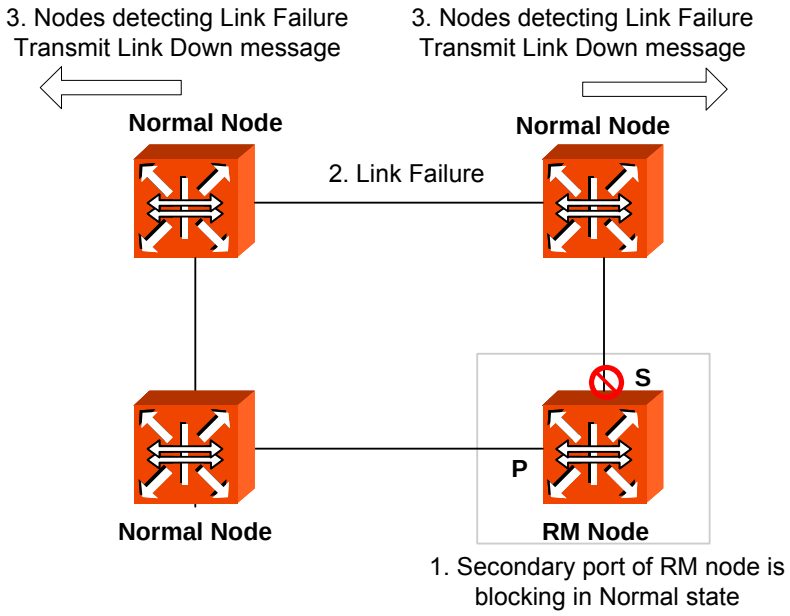


Fig. 8.35 Ethernet Ring Protocol Operation in Failure State

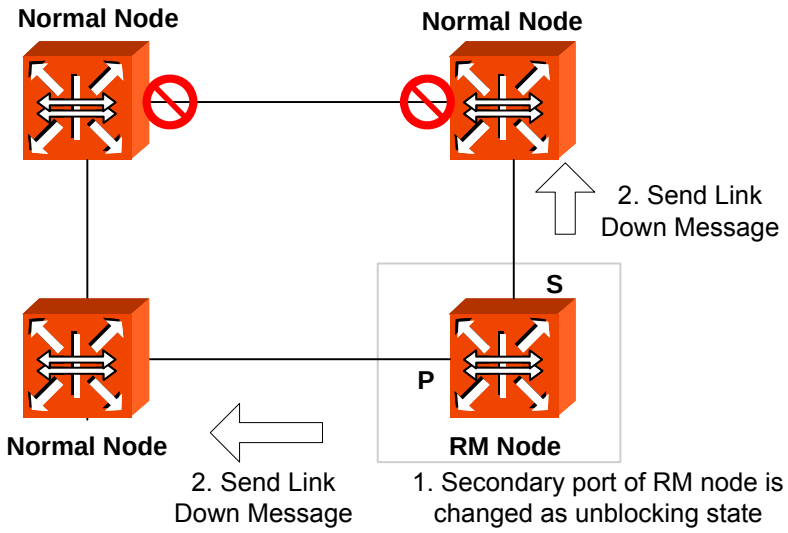


Fig. 8.36 Ring Protection

When a Link Failure is recovered, a temporary loop may occur. To rectify this condition, ERP sends a “link up” message to the RM. The RM will logically block the protected VLANs on its secondary port and generate a “RM link up” packet to make sure that all transit nodes are properly reconfigured. This completes fault restoration and the ring is back in normal state.

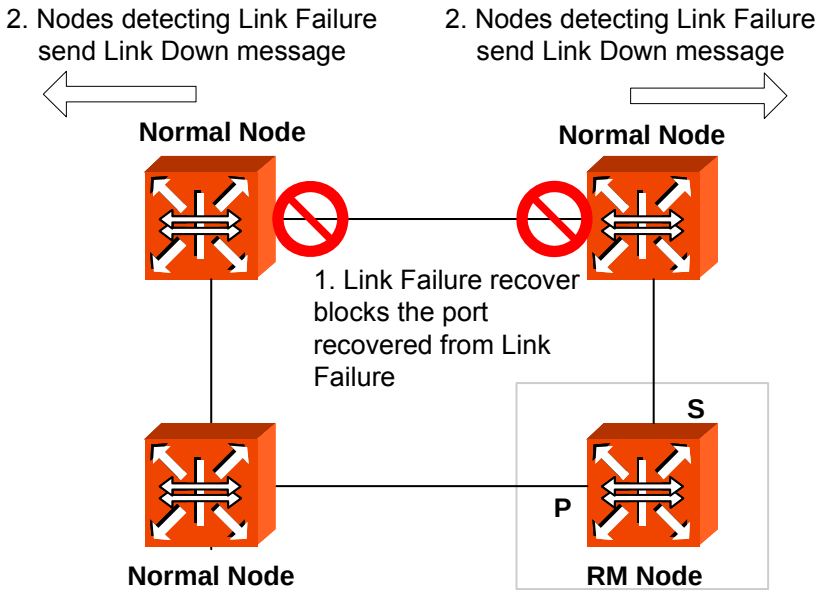


Fig. 8.37 Link Failure Recovery

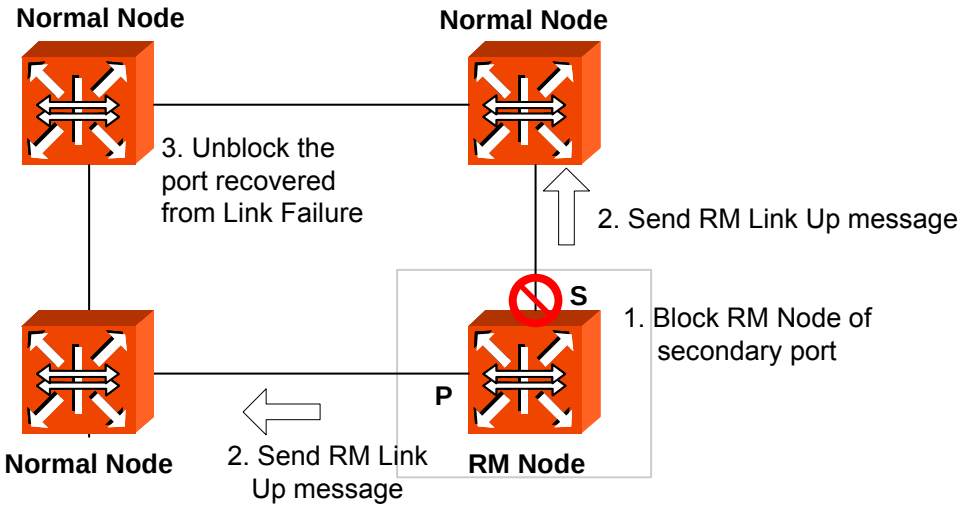


Fig. 8.38 Ring Recovery

8.9.2 Loss of Test Packet (LOTP)

ERP recognizes the Link Failure using Loss of Test Packet (LOTP). RM Node regularly sends RM Test Packet message. If the message is not retransmitted to RM Node through Ethernet Ring, it means that Loop doesn't occur. Therefore, RM Node unblocks Secondary port. The condition that RM Test Packet from RM Node doesn't return is LOTP state.

On the other hand, if RM Test Packet is retransmitted to RM Note through Ethernet Ring, Loop may occur. In this condition, RM Node blocks Secondary port.

8.9.3 Configuring ERP

8.9.3.1 ERP Domain

To realize ERP, you should fist configure domain for ERP. To configure the domain, use the following command.

Command	Mode	Description
erp domain *DOMAIN-ID*	Bridge	Creates ERP domain. DOMAIN-ID: control VLAN ID of domain <1-4094>
no erp domain {**all** | *DOMAIN-ID*}		Deletes ERP domain.

To specify a description for configured domain, use the following command.

Command	Mode	Description
erp description *DOMAIN-ID DESCRIPTION*	Bridge	Specifies a description of domain.

8.9.3.2 RM Node

To configure RM Node, use the following command.

Command	Mode	Description
erp rmnode *DOMAIN-ID*	Bridge	Configures RM node of ERP node mode.
no erp rmnode *DOMAIN-ID*		Configures ERP node mode as normal node.

8.9.3.3 Port of ERP domain

To configure Primary Port and Secondary port of RM Node, use the following command.

Command	Mode	Description
erp port *DOMAIN-ID* **primary** *PORT* **secondary** *PORT*	Bridge	Configures ports of ERP domain

i Primary port and secondary port should be different.

8.9.3.4 Protected VLAN

To configure Protected VLAN of ERP domain, use the following command.

Command	Mode	Description
erp protections *DOMAIN-ID VID*	Bridge	Configures protected VLAN of ERP domain VID: VLAN ID

To delete the configured Protected VLAN, use the following command.

Command	Mode	Description
no erp protections *VID*	Bridge	Deletes protected VLAN of ERP domain. VID: VLAN ID

8.9.3.5 Protected Activation

To configure ERP Protected Activation, use the following command.

Command	Mode	Description
erp activation *DOMAIN-ID*	Bridge	Configures ERP Protected Activation.

To disable ERP Protected Activation, use the following command

Command	Mode	Description
no erp activation *DOMAIN-ID*	Bridge	Disables ERP Protected Activation.

8.9.3.6 Manual Switch to Secondary

To configure Manual Switch to Secondary, use the following command.

Command	Mode	Description
erp ms-s *DOMAIN-ID*	Bridge	Configures ERP manual switch to secondary

To disable Manual Switch to Secondary, use the following command.

Command	Mode	Description
no erp ms-s *DOMAIN-ID*	Bridge	Disables ERP manual switch to secondary

8.9.3.7 Wait-to-Restore Time

To configure Wait-to-Restore Time, use the following command.

Command	Mode	Description
erp wait-to-restore *DOMAIN-ID* <1-720>	Bridge	Configures ERP wait-to-restore time 1-720: Wait to restore time in second

To return the configured Wait-to-Restore Time as Default, use the following command.

Command	Mode	Description
no erp wait-to-restore *DOMAIN-ID*	Bridge	Configures ERP wait-to-restore time as default value

8.9.3.8 Learning Disable Time

To configure ERP Learning Disable Time, use the following command.

Command	Mode	Description
erp learn-dis-time *DOMAIN-ID* <0-500>	Bridge	Configures ERP learning disable time 0-500: learning disabling time (unit: millisecond)

To return the configured Learning Disable Time as Default, use the following command.

Command	Mode	Description
no erp learn-dis-time *DOMAIN-ID*	Bridge	Configures ERP learning disable time as default value

8.9.3.9 Test Packet Interval

To configure ERP Test Packet Interval, use the following command.

Command	Mode	Description
erp test-packet-interval *DOMAIN-ID* <10-500>	Bridge	Configures ERP test packet interval 10-500: packet interval (unit: millisecond)

To return ERP Test Packet Interval as Default, use the following command.

Command	Mode	Description
no erp test-packet-interval *DOMAIN-ID*	Bridge	Configures ERP test packet interval as default value

8.9.3.10 Displaying ERP Configuration

To display a configuration for ERP, use the following command.

Command	Mode	Description
show erp {**all** | *DOMAIN-ID*}	Enable Global Bridge	Shows the information of ERP

8.10 Stacking

It is possible to manage several switches with one IP address by using stacking. If there's a limitation for using IP addresses and there are too many switches which you must manage, you can manage a number of switches with a IP address using this stacking function.

Switch stacking technology available in the industry today provides two main benefits to customers. The first benefit is the ability to manage a group of switches using a single IP address. The second benefit is the ability to interconnect two or more switches to create a distributed fabric, which behaves in the network as a unified system. The hiD 6615 S223/S323 provides the stacking technology's benefits for the customer.

i It is possible to configure stacking function for switches from 2 to 16.

The following is an example of the network where stacking is configured.

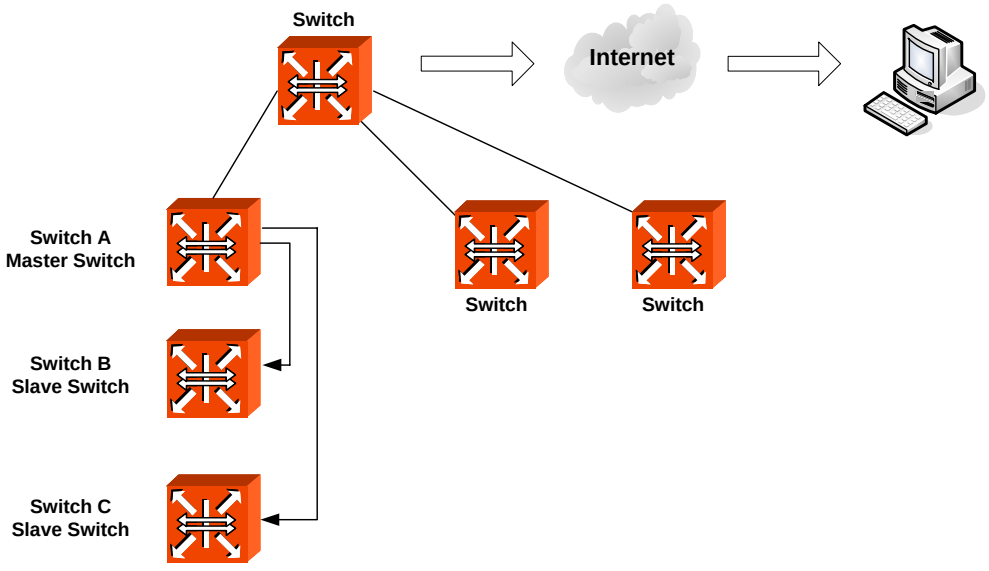


Fig. 8.39 Example of Stacking

A switch, which is supposed to manage the other switches in stacking is named as Master switch and the other switches managed by Master switch are named as Slave switch. Regardless of installed place or connection state, Master switch can check and manage all Slave switches.

The below steps are provided to configure stacking.

8.10.1 Switch Group

You should configure all the switches configured with stacking function to be in the same VLAN. To configure the switches as a switch group belongs in the same VLAN, use the following command.

Command	Mode	Description
stack device *NAME*	Global	Configures device name or VID

i For managing the stacking function, the port connecting Master switch and Slave switch must be in the same VLAN.

8.10.2 Designating Master and Slave Switch

Designate Mater switch using the following command.

Command	Mode	Description
stack master	Global	Designates Master switch

After designating Master switch, register Slave switch for Master switch. To register Slave switch or delete the registered Slave switch, use the following command.

Command	Mode	Description
stack add *MACADDR* [*DESCRIPTION*]	Global	Registers slave switch. MACADDR: MAC address
stack del *MACADDR*		Deletes slave switch.

i To make stacking operate well, it is required to enable the interface of Slave switch. The switches in different VLANs can not be added to the same switch group.

You should designate Slave switch registered in Master Switch as Slave Switch. To designate Slave switch, use the following command.

Command	Mode	Description
stack slave	Global	Designates as a slave switch

8.10.3 Disabling Stacking

To disable stacking, use the following command.

Command	Mode	Description
no stack	Global	Disables the stacking function

8.10.4 Displaying Stacking Status

Command	Mode	Description
show stack	Enable Global	Shows a configuration of stacking

8.10.5 Accessing to Slave Switch from Master Switch

After configuring all stacking configurations, it is possible to configure and mange by accessing to Slave switch from Master switch.

To access to Slave switch from Mater switch, use the following command in Bridge configuration mode.

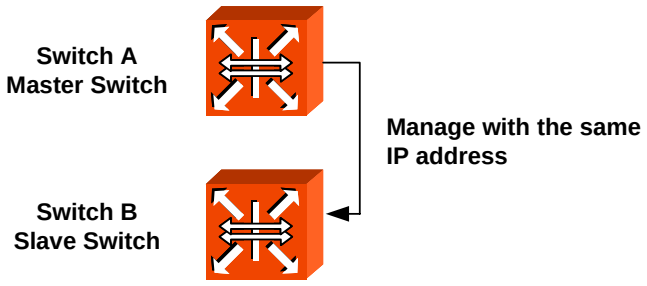
Command	Mode	Description
rcommand *NODE*	Global	Accesses to a slave switch. NODE: node number

NODE means node ID from configuring stacking in Slave switch. If you input the above command in Mater switch, Telnet connected to Slave switch is displayed and it is possible to configure Slave switch using DSH command. If you use the exit command in Telnet, the connection to Slave switch is down.

8.10.6 Sample Configuration

[Sample Configuration 1] Configuring Stacking

The following is a stacking configuration by designating SWITCH A as a master and SWITCH B as a slave.



Step 1
Assign IP address in Interface configuration mode of Switch and enable interface using “no shutdown” command. In order to enter into *Interface configuration* mode, you should

open *Interface configuration* mode of VLAN to register as a switch group for stacking.

The following is an example of configuring Interface of switch group as 1.

```
SWITCH_A# configure terminal
SWITCH_A(config)# interface 1
SWITCH_A(interface)# ip address 192.168.10.1/16
SWITCH_A(interface)# no shutdown
SWITCH_A(interface)#
```

i If there are several switches, rest of them are managed by a single IP address of Master switch. Therefore you don't need to configure IP address in Slave switch.

Step 2
Configure Switch A as Master switch. Configure VLAN to belong in the same switch group after registering Slave switch, configure it as a Master switch.

<Switch A – Master Switch>

```
SWITCH_A(config)# stack master
SWITCH_A(config)# stack device default
SWITCH_A(config)# stack add 00:d0:cb:22:00:11
```

Step 3
Configure VLAN in order to belong to the same switch group in Switch B registered by Master switch as Slave switch and configure as a Slave switch.

<Switch B – Slave Switch>

```
SWITCH_B(config)# stack slave
SWITCH_B(config)# stack device default
```

Step 4
Check the configuration. The information you can check in Master switch and Slave switch is different as below.

<Switch A – Master Switch>

```
SWITCH_A(config)# show stack
device  : default
node ID : 1
node   MAC address        status   type             name        port
   1   00:d0:cb:0a:00:aa    active   SURPASS hiD 6615 S223/S323 SWITCH_A     24
   2   00:d0:cb:22:00:11    active   SURPASS hiD 6615 S223/S323 SWITCH_B     24
SWITCH_A(config)#
```

<Switch B – Slave Switch>

```
SWITCH_B(config)# show stack
device  : default
node ID : 2
SWITCH_B(config)#
```

[Sample Configuration 2] Accessing from Master Switch to Slave Switch

The following is an example of accessing to Slave switch from Master switch configured in [Sample Configuration 1]. If you show the configuration of Slave switch in [Sample Configuration 1], you can recognize node-number is 2.

```
SWITCH(bridge)# rcommand 2
Trying 127.1.0.1(23)...
Connected to 127.1.0.1.
Escape character is '^]'.
SWITCH login: admin
Password:
SWITCH#
```

To disconnect, input as below.

```
SWITCH# exit
Connection closed by foreign host.
SWITCH(bridge)#
```

8.11 Broadcast Storm Control

The hiD 6615 S223/S323 supports broadcast storm control for broadcast packets. Broadcast storm is overloading situation of broadcast packets since they need major part of transmit capacity. Broadcast storm may be often occurred because of difference of versions. For example, when there are mixed 4.3 BSD and 4.2 BSD, or mixed AppleTalk Phase I and Phase II in TCP/IP, Storm may occur

In addition, when information of routing protocol regularly transmitted from router incorrectly recognized by system, which does not support the protocol, Broadcast Storm may be occurred.

Broadcast Storm Control is operated by system counts how many Broadcast packets are there for a second and if there are packets over configured limit, they are discarded.

The hiD 6615 S223/S323 provides not only broadcast storm but also control of multicast and DLF (Destination Lookup Fail) storm. In order to use control of multicast and DLF storm, use the following commands. Then all configurations of Broadcast storm control will be equally applied to all VLANs.

To enable multicast storm control and DLF storm control, use the following command.

Command	Mode	Description
storm-control {**broadcast** | **multicast** | **dlf**} *RATE* [*PORTS*]	Bridge	Enables broadcast, multicast, or DLF storm control respectively in a port with a user defined rate. Rate value is from 1 to 262142 for FE, and from 1 to 2097150 for GE

i By default, DLF storm control is enabled and multicast storm control is disabled.

To disable multicast storm control and DLF storm control, use the following commands

Command	Mode	Description
no storm-control {**broadcast** | **multicast** | **dlf**} [*PORTS*]	Bridge	Disables broadcast, multicast, or DLF storm control respectively.

To display a configuration of storm control, use the following command.

Command	Mode	Description
show storm-control	Enable Global Bridge	Displays storm control configuration.

8.12 Jumbo-frame Capacity

The packet range that can be capable to accept is from 64 bytes to 1518 bytes. Therefore, packets not between these ranges will not be taken. However, the hiD 6615 S223/S323 can accept Jumbo-frame larger than 1518 bytes through user's configuration.

To configure to accept Jumbo-frame larger than 1518 bytes, use the following command.

Command	Mode	Description
jumbo-frame *PORTS* <1518-9000>	Bridge	Configures to accept jumbo-frame between specified ranges. 1518-9000: Max packet length

To disable configuration to accept Jumbo-frame, use the following command.

Command	Mode	Description
no jumbo-frame *PORTS*	Bridge	Disables configuration to accept jumbo-frame on specified port.

To display the configuration of Jumbo-frame, use the following command.

Command	Mode	Description
show jumbo-frame	Enable Global Bridge	Shows a configuration of jumbo frame.

Sample Configuration

The following is an example of configuration to accept Jumbo-frame under 2200 bytes in port 1~10.

```
SWITCH# configure terminal
SWITCH(config)# bridge
SWITCH(bridge)# jumbo-frame 1-10 2200
SWITCH(bridge)# show jumbo-frame
         Name : Current/Default
       port01 :   2200/  1518
```

```
        port02 :   2200/  1518
        port03 :   2200/  1518
        port04 :   2200/  1518
        port05 :   2200/  1518
        port06 :   2200/  1518
        port07 :   2200/  1518
        port08 :   2200/  1518
        port09 :   2200/  1518
        port10 :   2200/  1518
        port11 :   1518/  1518
        port12 :   1518/  1518
SWITCH(bridge)#
```

8.13 Blocking Direct Broadcast

RFC 2644 recommends that system blocks broadcast packet of same network bandwidth with interfaceof equipment, namely Direct broadcast packet. Hereby, SURPASS hiD 6615 supposed to block Direct broadcast packet by default setting. However, you can enable or disable it in SURPASS hiD 6615. In order to block Direct broadcast packet, use the following command.

Command	Mode	Description
no ip forward direct-broadcast	Global	Enables blocking Direct broadcast packet. (Default)
ip forward direct-broadcast		Disables blocking Direct broadcast packet.

The following is an example of blocking Direct broadcast packet and showing it.

```
SWITCH(config)# ip forward direct-broadcast
SWITCH(config)# show running-config
Building configuration...
(omitted)
!
ip forward direct-broadcast
!
no snmp
!
SWITCH(config)#
```

8.14 Maximum Transmission Unit (MTU)

Maximum value for the length of the data payload can be transmitted. User can control Maximum Transmission Unit (MTU) with below command.

Command	Mode	Description
mtu <68-1500>	Interface	Configures maximum MTU size.
no mtu		Returns to the default MTU size.

The following is an example of configuration to mtu size as 100.

```
SWITCH(config-if)# mtu 100
SWITCH(config-if)# show running-config interface 1
!
interface default
 mtu 100
 bandwidth 1m
 ip address 10.27.41.181/24
SWITCH(config-if)
```

9 IP Multicast

Traditional IP network provided unicast transmission a host to send packets to a single host or broadcast transmission. But multicast provides group transmission a host to send packets to a group of all hosts. In the multicast environment, multicast packets are delivered to a group by duplicating multicast packets.

Multicasting is divided into Layer 3 multicast routing and Layer 2 IGMP snooping. The hiD 6615 S323 supports PIM-SM/SSM of multicast routing, and V1, V2 and V3 of IGMP snooping.

Fig. 9.1 shows the example of IGMP snooping configuration network. In Layer 2 network, the hiD 6615 S223/S323 is configured only for IGMP Snooping.

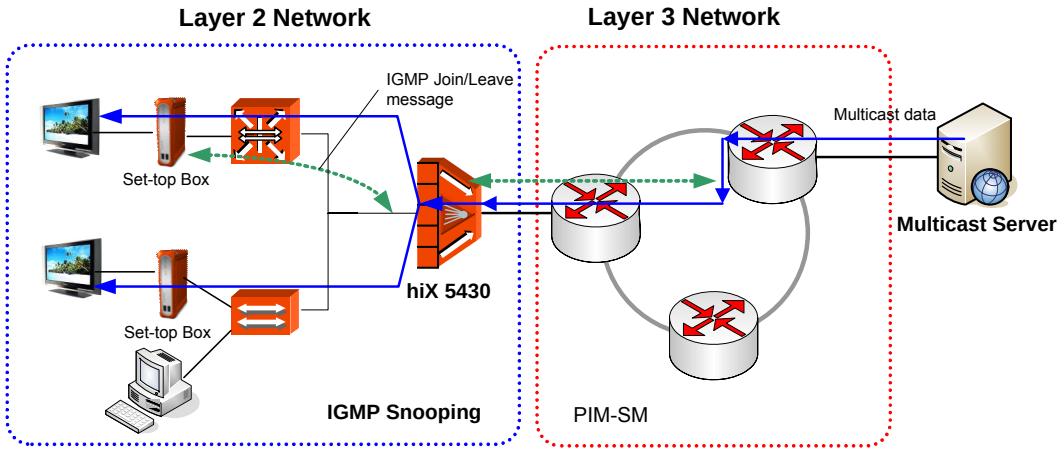


Fig. 9.1 IGMP Snooping Configuration Network

If the hiD 6615 S323 is installed within Layer 3 network, PIM-SM should be configured. Below the hiD 6615 S223/S323, there is a switch that performs IGMP snooping function for subscribers.

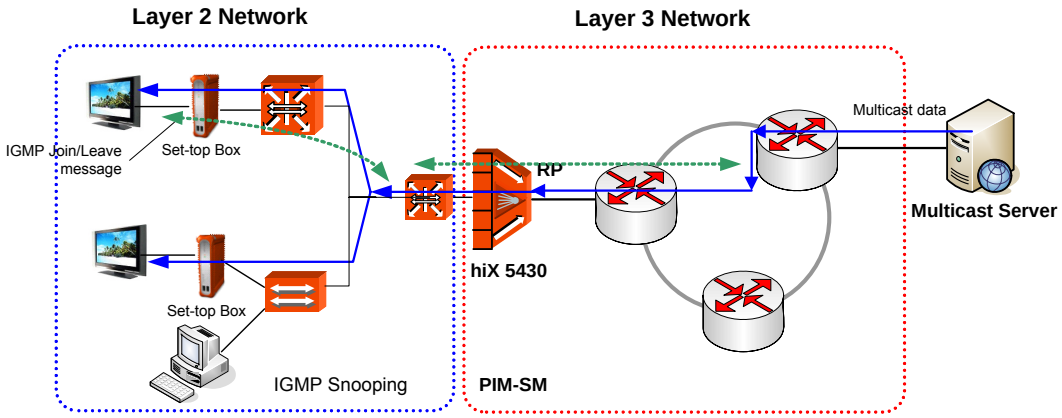


Fig. 9.2 PIM-SM Configuration Network

You can configure IGMP Snooping with PIM-SM as Fig. 9.3. If more than one port are on the same interface and the hiD 6615 S323 is located in Layer 3 boundary, IGMP Snoop-

ing and PIM-SM should be configured at the same time.

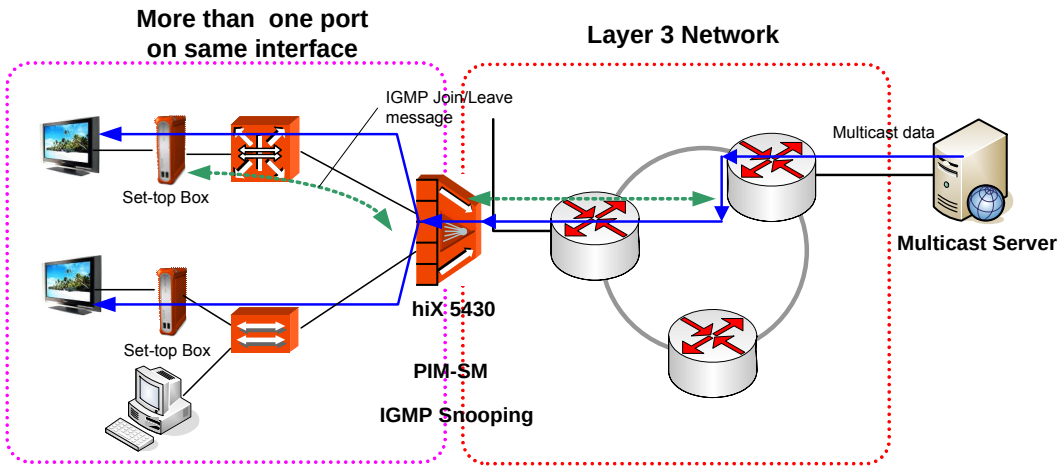


Fig. 9.3 IGMP Snooping and PIM-SM Configuration Network

9.1 Multicast Routing Information Base

In this chapter, you can configure the common multicast commands for multicast routing information base.

9.1.1 Enabling Multicast Routing (Required)

To provide multicast service on the hiD 6615 S323, you should use the **ip multicast-routing** command necessarily. If you disable the multicast routing, the multicast protocol daemon remains present, but does not perform multicast functions.

Enable the multicast routing function, using the following command.

Command	Mode	Description
ip multicast-routing	Global	Enables multicast routing function.
no ip multicast-routing		Disables multicast routing function. (default)

9.1.2 Limitation of MRIB Routing Entry

You can limit the number of multicast routes that can be added to a switch, and generate an error message when the limit is exceeded.

To configure the limitation of MRIB routing entry, use the following command.

Command	Mode	Description
ip multicast route-limit *LIMIT* [*THRESHOLD*]	Global	Enables multicast routing function. LIMIT: 1-214783647 (number of routes) THRESHOLD: 1-214783647
no ip multicast route-limit		Disables the limitation configuration of MRIB routing entry.

9.1.3 Clearing MRIB Information

Clearing Total or Partial Group Entry of MRIB

If you use the **clear ip mroute** command, the MRIB clears the multicast route entries in its multicast route table, and removes the entries from the multicast forwarder. Each multicast protocol has its own clear multicast route command. The protocol-specific **clear** command clears multicast routes from the protocol, and also clears the routes from the MRIB.

To delete the multicast route entries, use the following command.

Command	Mode	Description
clear ip mroute *	Enable Global Bridge	Deletes all multicast routes entries.
clear ip mroute *GROUP-ADDR* [*SRC-IP-ADDRESS*]		Deletes specific multicast routes entries. GROUP-ADDR: group IP address SRC-IP-ADDRESS: source IP address

Clearing Statistics of Multicast Routing Table

To delete the multicast route statistics entries from IP multicast routing table, use the following command.

Command	Mode	Description
clear ip mroute statistics *	Enable Global Bridge	Deletes all multicast routes statistics entries.
clear ip mroute statistics *GROUP-ADDR* [*SRC-IP-ADDRESS*]		Deletes specific multicast routes statistics entries. GROUP-ADDR: group IP address SRC-IP-ADDRESS: source IP address

Clearing MFC and Tree Information Base which are produced by PIM-SM

To clear all Multicast Forwarding Cache (MFC) and TIB entries in the PIM-SM protocol level, use the following command.

Command	Mode	Description
clear ip mroute * pim sparse-mode	Enable Global	Deletes all MFC and TIB entries in the PIM-SM.
clear ip mroute *GROUP-ADDR* [*SRC-IP-ADDRESS*] **pim sparse-mode**		Deletes specific MFC and TIB entries in the PIM-SM. GROUP-ADDR: group IP address SRC-IP-ADDRESS: source IP address

9.1.4 Displaying MRIB Information

To display MRIB information, use the following commands

Command	Mode	Description
show ip mroute {**dense** | **sparse**} {**count** | **summary**}	Enable Global Bridge	Displays multicast routes entries. GROUP-ADDR: group IP address SRC-IP-ADDRESS: source IP address
show ip mroute *GROUP-ADDR* [*SRC-IP-ADDRESS*] {**dense** | **sparse**} {**count** | **summary**}		
show ip mroute *GROUP-ADDR* [*SRC-IP-ADDRESS*] *GROUP-ADDR* [*SRC-IP-ADDRESS*]{**dense** | **sparse**} {**count** | **summary**}		
show ip mroute *GROUP-ADDR*/M {**dense** | **sparse**} {**count** | **summary**}		

To display the contents of the MRIB VIF table, use this command.

Command	Mode	Description
show ip mvif [*IFNAME*]	Enable	Displays IP multicast interface.

9.1.5 Multicast Time-To-Live Threshold

Use this command to configure the time-to-live (TTL) threshold of packets being forwarded out of an interface.

Command	Mode	Description
ip multicast ttl-threshold <0-255>	interface	Configures the time-to-live threshold for multicast packet Default: 1
no ip multicast ttl-threshold		Restores is as a default.

9.1.6 MRIB Debug

Use this command to debug events in the multicast RIB.

Command	Mode	Description
debug nsm mcast {**all** | **fib-msg** | **mrt** | **register** | **stats** | **vif**}	Enable	Debugs event in the multicast RIB. all : all Ipv4 multicast debugging fib-msg: multicast FIB messages mrt: multicast routes register: multicast PIM register messages stats: multicast statitics vif: multicast interface
no debug nsm mcast {**all** | **fib-msg** | **mrt** | **register** | **stats** | **vif**}		Disables the debug event.

9.1.7 Multicast Aging

L2 and L3 Join information about Multicast Group used to apply on the chipset without Multicast Stream, which makes dissatisfaction for Maximum Multicast Entry. Multicast Aging is to optimize Multicast Entry management using Multicast L2 Aging. When Multicast Stream comes in, L2 filtering port (igmp snooping, pim snooping) would be written on the chip. In addition, verify the hitbit about Entry after the Aging time to reset the aging time or delete Entry to manage the Multicast Entry efficiently.

To configure the multicast againg, use the following command.

Command	Mode	Description
ip mcfdb aging-time < 10-21474830>	Global	Configures Aging tiem for Multicast Stream (Default:300sec)
ip mcfdb aging-limit <256-65535>		Configures Maximun Multicast Stream for Aging (Default:5000)
no ip mcfdb aging-time		Restores it as a default
no ip mcfdb aging-limit		

To delete Muticast Stream Entry that has done the Aging, use the following command.

Command	Mode	Description
clear ip mcfdb {**vlan** *VLAN*}	Global	Deletes Multicast Stream Entry after Aging per vlan or all
clear ip mcfdb vlan *VLAN* **group** *A.B.C.D* **source** *A.B.C.D*		Deletes Multicast Stream Entry after Aging per vlan or group, source

To display about Againg information, use the following command.

Command	Mode	Description
show ip mcfdb	Enable Global Bridge	Displays L2 Aging information (aging-time, aging-limit information)
show ip mcfdb aging-entry {**vlan** *VID* | **group** *A.B.C.D*} [**mac-based** | **detail]**		Displays L2 Aging information
show ip mfib {**vlan** *VID* | **group** *A.B.C.D*} [**detail**]		Displays L3 Aging Entry information as Input interface (RPF) and Output Interface Detail: displays input/output Port for each interface and user for each port
show ip mfib hidden {**reserved** | **dstuser**}		Displays reserved information and destination user information as a hidden command

9.2 Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is used by hosts and routers that support multicasting. All the systems on a network can know which hosts belong to which multicast groups. IGMP is not multicast routing protocol but group management protocol.

Multicast routers can receive thousands of multicast packets from other group. If a router does not have the information of host membership, it has to broadcast the packets. This is bandwidth waste. To solve this problem, one group list of members is maintained. IGMP helps multicast router to create and renew the list.

The hiD 6615 S223/S323 supports IGMP Version 1, 2 and 3.

9.2.1 IGMP Basic Configuration

This chapter explains how to configure basic IGMP features such as IGMP version, IGMP DB and Debugging method.

9.2.1.1 IGMP Version per Interface

You can configure the IGMP Protocol version on an interface. To configure the IGMP Protocol version, use the following command.

Command	Mode	Description
ip igmp version <1-3>	Interface	Selects an IGMP version. 1: version 1 2: version 2 3: version 3 (default)
no ip igmp version		Returns to the default setting. (version 3)

- **IGMP Version 1**
  Provides basic Query-Response mechanism that allows the multicast router to determine which multicast groups are active an other processes that enable hosts to join and leave a multicast group.
- **IGMP Version 2**
  Extends IGMP features as IGMP leave process, group-specific queries and explicit maximum query response time. It added support for "low leave latency", that is, a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network.
- **IGMP Version 3**
  Version 3 of IGMP adds support for "source filtering", that is, the ability for a system to report interest in receiving packets ‘only’ from specific source addresses, or from ‘all but’ specific source addresses, sent to a particular multicast address. That information may be used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested receivers

9.2.1.2 Removing IGMP Entry

To clear IGMP interface entries, use the following command.

Command	Mode	Description
clear ip igmp interface *INTERFACE*	Enable	Clears IGMP interface entries on an interface.
clear ip igmp group {***** | *A.B.C.D* [*INTERFACE*]}		Deletes IGMP group cache entries. *: all IGMP group A.B.C.D: IGMP group address

9.2.1.3 IGMP Debug

To enable debugging of all IGMP or a specific feature of IGMP, use the following command.

Command	Mode	Description
debug igmp {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}	Enable	Enables debugging of IGMP. all: debug all IGMP decode: debug IGMP decoding encode: debug IGMP encoding events: debug IGMP events fsm: debug IGMP Finite State Machine (FSM) tib: debug IGMP Tree Information Base (TIB)
no debug igmp {**all** | **decode** | **encode** | **events** | **fsm** | **tib**}		Disables the IGMP debugging configuration.

9.2.1.4 IGMP Robustness Value

To change the Querier Robustness Variable value on an interface, use the following command.

Command	Mode	Description
ip igmp robustness-variable <2-7>	Interface	Configures the querier robustness variable value on an interface.
no ip igmp robustness-variable		Returns to the default value. (default: 2)

9.2.2 IGMP Version 2

IGMP v2 consists of three message type, query, membership report and leave report. This chapter describes how to configure these IGMP v2 features.

9.2.2.1 IGMP Static Join Setting

If there is no group member on a network segment and you want to transmit multicast packet to that network segment, you can configure to pull multicast traffic down to a network segment using the **ip igmp static-group** command. With this command, the switch does not accept the packets, but forwards them. The outgoing interface appears in the

IGMP cache, but the switch is not a member. Therefore it can support fast switching.

To configure IGMP static Join, use the following command.

Command	Mode	Description
ip igmp static-group *A.B.C.D* **vlan** *VLAN* **port** *PORT* **reporter** *A.B.C.D*	Global	Configures IGMP static join setting. A.B.C.D: group address
no ip igmp static-group [*A.B.C.D*] [**vlan** *VLAN*]		Disables the IGMP static join configuration.
no ip igmp static-group *A.B.C.D* **vlan** *VLAN* **port** *PORT* **reporter** *A.B.C.D*		

9.2.2.2 Maximum Number of Groups

Hosts on a subnet serviced by a particular interface have the access to join certain multicast groups. These multicast groups can be controlled by the **ip igmp access-group** command.

To control the multicast groups on an interface, use the following command.

Command	Mode	Description
ip igmp access-group {<1-99> | *WORD*}	Interface	Sets an IGMP access group. 1-99: access list number WORD: IP named standard access list
no ip igmp access-group		Disables groups on interfaces.

9.2.2.3 IGMP Query Configuration

Multicast routers send host membership query messages (host query messages) to discover which multicast groups have members on the attached networks of the router. Hosts respond with IGMP report messages indicating that they wish to receive multicast packets for specific groups (indicating that the host wants to become a member of the group). Host query messages are addressed to the all-hosts multicast group, which has the address 224.0.0.1, and has an IP time-to-live (TTL) value of 1.

The designated router for a LAN is the only router that sends IGMP host query messages. For IGMP Version 2, the designated querier is the router with the lowest IP address on the subnet. If the router hears no queries for the timeout period, it becomes the querier.

To configure an IGMP query interval, use the following command.

Command	Mode	Description
ip igmp query-interval <1-18000>	Interface	Configures the IGMP query interval. 1-18000: frequency at which IGMP host query messages are sent (unit: second)
no ip igmp query-interval		Returns to the default value. (125)

Use this command to configure the timeout period before the router takes over as the

querier for the interface after the previous querier has stopped querying.

Command	Mode	Description
ip igmp querier-timeout <60-300>	Interface	Configures the IGMP queier timeout. 60-300: number of seconds that router waits after the previous querier has stopped querying before it takes over as the querier
no ip igmp querier-timeout		Returns to the default value. (255)

IGMP Maximum Response Time

To configure the maximum response time advertised in IGMP queries, use the following command. If the router is running IGMP v2, you can change this value.

Command	Mode	Description
ip igmp query-max-response-time <1-240>	Interface	Configures the IGMP queier timeout. 1-240: Maximum response time (in seconds) advertised in IGMP queries.
no ip igmp query-max-response-time		Returns to the default value. (10)

IGMP v2 Group-specific or IGMP v3 Group-source-specific Query Message

The Last Member Query Count is the number of Group-Specific Queries sent before the router assumes there are no local members. The Last Member Query Count is also the number of Group-and-Source-Specific Queries sent before the router assumes there are no listeners for a particular source.

To configure the last member query count, use the following command.

Command	Mode	Description
ip igmp last-member-query-count <2-7>	Interface	Configures the IGMP last member query count. 2-7: last member query count value
no ip igmp last-member-query-count		Returns to the default value. (2)

When a router receives an IGMP Version 2 leave group message on an interface, it waits twice the query interval specified by the **ip igmp last-member-query-interval** command; after which, if no receiver has responded, the router drops the group membership on that interface.

To configure the last member query interval, use the following command

Command	Mode	Description
ip igmp last-member-query-interval <1000-25500>	Interface	Configures the IGMP last member query interval. 1000-25500: frequency at which IGMP group-specific host query messages are sent. (unit: millisecond)
no ip igmp last-member-query-interval		Returns to the default value. (1000 milliseconds)

9.2.2.4 IGMP v2 Fast Leave

In IGMP version 2, you can minimize the leave latency of IGMP memberships. This command is used when only one receiver host is connected to each interface.

When this command is not configured, the router sends an IGMP group-specific query message upon receipt of an IGMP Version 2 group leave message. The router stops forwarding traffic for that group only if no host replies to the query within the timeout period. The timeout period is determined by the **ip igmp last-memberquery-interval** command and the IGMP robustness variable, which is defined by the IGMP specification. By default, the timeout period is 2 seconds.

When the **ip igmp immediate-leave** command is enabled on an interface, the router does not send IGMP group specific host queries on receiving an IGMP Version 2 leave group message from that interface. Instead, the router immediately removes the interface from the IGMP cache for that group, and informs the multicast routing protocols.

To configure the IGMP v2 fast leave, use the following command.

Command	Mode	Description
ip igmp immediate-leave group-list {<1-99> | <1300-1999> | *WORD*}	Interface	Configures the IGMP fast leave function. 1-99: access list number 1300-1999: access list number (expanded range) WORD: IP named standard access list
no ip igmp immediate-leave		Disables the fast leave configuration.

9.2.2.5 Displaying the IGMP Configuration

To display the multicast groups and related information, use the following command.

Command	Mode	Description
show ip igmp groups [**detail**]	Enable Global Bridge	Displays the multicast groups with receivers directly connected to the router and learned through IGMP.
show ip igmp groups *A.B.C.D* [**detail**]		
show ip igmp groups *INTERFACE* [**detail**]		
show ip igmp groups *INTERFACE A.B.C.D* [**detail**]		
show ip igmp interface		Displays multicast-related information about an interface.
show ip igmp interface *INTERFACE*		

9.2.3 L2 MFIB

Occasionally, unknown multicast traffic is flooded because a MAC address has timed out or has not been learned by the switch. To guarantee that no multicast traffic is flooded to the port, use the following command.

Command	Mode	Description
ip unknown-multicast block	Global	Configures the blocking of unknown multicast traffic.
ip unknown-multicast port *PORTS* **block**		Configures the blocking of unknown multicast traffic for a specific port.
no ip unknown-multicast block		Returns to the normal forwarding states.
no ip unknown-multicast port *PORTS* **block**		

9.2.4 IGMP Snooping Basic Configuration

9.2.4.1 Enabling IGMP Snooping per VLAN

The hiD 6615 S223/S323 supports 256 Snooping Membership Group Table that are managed by each VLAN. Snooping supports Enable/Disable by VLAN independently. By default, IGMP snooping is globally disabled on the switch.

To enable/disable global IGMP, use the following steps.

Step 1
Open *Global Configuration* mode using the **configure terminal** command.

Step 2
Execute the **ip multicast-routing** command.

Step 3
Enable IGMP snooping in all existing VLAN interfaces.

Command	Mode	Description
ip igmp snooping	Global	Enables IGMP snooping globally.

Step 4
Return to *Privileged EXEC Enable* mode using **exit** command. To globally disable IGMP snooping on all VLAN interfaces, use the **no ip igmp snooping** command. In *Global Configuration* mode, follow these steps to enable IGMP snooping on a VLAN interface.

Step 1
Open *Global Configuration* mode using the **configure terminal** command.

Step 2
Execute the **ip multicast-routing** command.

Step 3
Enable IGMP snooping on a VLAN interface.

Command	Mode	Description
ip igmp snooping vlan *VLANS*	Global	Enables IGMP snooping on a VLAN interface. VLANS: 1-4094

Step 4
Return to *Privileged EXEC Enable* mode using the **exit** command.

To diable IGMP snooping on a VLAN interface, use the **no ip igmp snooping vlan** *VLANS* command for the specified VLAN number.

To display global IGMP, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*]	Enable Global Bridge	Shows IGMP snooping configuration.

9.2.4.2 Robustness Count for IGMP v2 Snooping

Configure the robustness variable on a VLAN basis, using the following command.

Command	Mode	Description
ip igmp snooping [**vlan** *VLANS*] **robustness-variable** <1-7>	Global	Configures the robustness variable.
no ip igmp snooping [**vlan** *VLANS*] **robustness-variable**		Returns to the default value.

9.2.5 IGMP v2 Snooping

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those associated with IP multicast devices. Internet Group Management Protocol (IGMP) is the internet protocol that helps to inform multicast groups to multicast router. In the multicast network, multicast router sends only IGMP query massage that quest whether receive multicast packet when multicast packet is transmitted. If a switch sends the join massage to multicast router, multicast router transmits the multicast packet only to that switch.

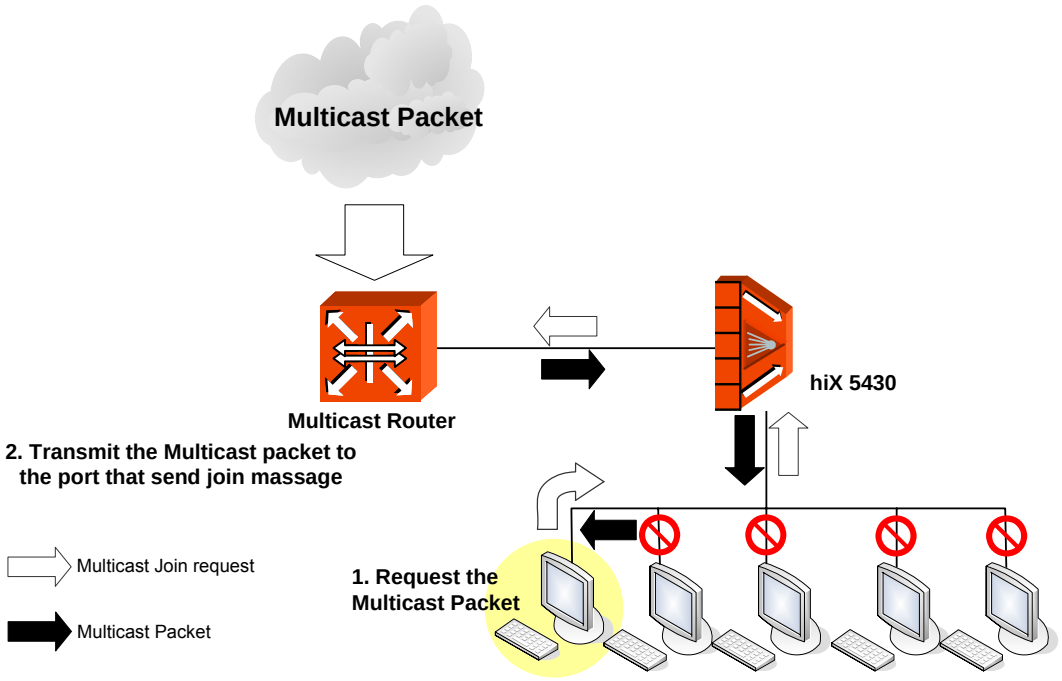


Fig. 9.4 IP Multicasting

IGMP Snooping is a function that finds port, which sends 「**Join message**」 to join in specific multicast group to receive multicast packet or 「**Leave message**」 to get out of the multicast group because it does not need packets.

Only when the switch is connected to multicast router, IGMP Snooping can be enabled.

9.2.5.1 IGMP v2 Snooping Fast Leave

If the Multicast client sends the leave massage to leave out Multicast group, Multicast router sends IGMP Query massage to the client again, and when the client does not respond, delete the client from the Multicast group.

In IGMP v2, even after Host sent Leave Message, it receives Multicast Traffic until sending Specific Query. In Snooping Fast-Leave Enable mode, it sends no more Multicast Traffic immediately by deleting from Membership Table when receive Leave Message without sending Specific Query.

Command	Mode	Description
ip igmp snooping immediate-leave	Global	Configures the fast-leave on the system.
ip igmp snooping vlan *VLANS* **immediate-leave**		Configures the fast-leave on a VLAN interface.

To disable IGMP snooping fast-leave, use the following command.

Command	Mode	Description
no ip igmp snooping immediate-leave	Global	Deletes the fast-leave.
no ip igmp snooping vlan *VLAN-ID* **immediate-leave**		Deletes the fast-leave on a VLAN interface.

To display IGMP snooping Immediate Leave configuration, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*]	Enable Global Bridge	Shows that the IGMP snooping Immediate leave is enabled.

9.2.5.2 IGMP v2 Snooping Querier

You can use the hiD 6615 S223/S323 as IGMP querier without multicast router, because IGMP query daemon has been installed in the hiD 6615 S223/S323. Legacy equipments used IGMP Querier of PIM but not developed Querier for IGMP Snooping. Because of this, to operate Querier on IGMP Snooping, IP Address was mandatory and Specific Query was operated by IGMP Querier.

The hiD 6615 S223/S323 implemented IGMP Snooping Querier and it operates differently with IGMP Query. IGMP Snooping Querier can send General Query from Snooping Switch and it should be distinguished with Specific Query. IGMP Snooping Querier also uses Source IP Address 0.0.0.0, if there is no IP Address on Switch.

Enabling IGMP Snooping Querier

To enable the IGMP Snooping querier, use the following command.

Command	Mode	Description
ip igmp snooping querier address *A.B.C.D*	Global	Enables the IGMP snooping querier on the system. A.B.C.D: Source address for IGMP v2 snooping querier
ip igmp snooping vlan *VLANS* **querier address** *A.B.C.D*		Enables the IGMP snooping querier on a VLAN interface. VLANS: VLAN ID

To disable IGMP querier, use the following command.

Command	Mode	Description
no ip igmp snooping querier address	Global	Disables the IGMP snooping querier.
no ip igmp snooping vlan *VLAN-NAME* **querier address**		Disables the IGMP snooping querier on a VLAN interface.

The Query Interval of IGMP v2 Snooping Querier

To configure a query interval of the querier, use the following command.

Command	Mode	Description
ip igmp snooping querier query-interval <1-1800>	Global	Configures the IGMP snooping querier query interval on the system. 1-1800: IGMP snooping querier query interval in seconds
ip igmp snooping vlan *VLANS* **querier query-interval** <1-1800>		Enables the IGMP snooping querier on a VLAN interface. VLANS: VLAN ID

To disable the query interval of the querier, use the following command.

Command	Mode	Description
no ip igmp snooping querier query-interval	Global	Disables the IGMP snooping querier interval.
no ip igmp snooping vlan *VLANS* **querier query-interval**		Disables the IGMP snooping querier interval on a VLAN interface.

The Timeout Value of IGMP v2 Snooping Querier's General Query

Use this following command to configure the max response time in which the reply for the IGMP snooping query being sent should be received.

Command	Mode	Description
ip igmp snooping querier max-response-time <1-25>	Global	Configures the IGMP snooping max-response-time interval on the system. 1-25: The maximum response time in seconds
ip igmp snooping vlan *VLANS* **querier max-response-time** <1-25>		Enables the IGMP snooping max-response-time on a VLAN interface. VLANS: VLAN ID

To disable the max-response-time, use the following command.

Command	Mode	Description
no ip igmp snooping querier max-response-time	Global	Disables the IGMP snooping max-response-time interval.
no ip igmp snooping vlan *VLANS* **querier max-response-time**		Disables the IGMP snooping max-response-time on a VLAN interface.

To display IGMP query parameter, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*] **querier** [**detail**]	Enable Global Bridge	Verifies that the IGMP snooping querier is enabled.

9.2.5.3 IGMP v2 Snooping Last-Member-Interval

When receive Leave Message from host in IGMP v2, Querier sends Specific Query and check whether there is Multicast Group Member. Basically, if Membership Report about First Specific Query does not come, after 1 second, send second Specific Query. If there is no response also, it deleted from Membership Table. Last-member-interval is the value to regulate gap between first Specific Query and second Specific Query. By limiting Interval value, IGMP v2 function and fast Leave can be implemented.

To send IGMP Query message and configure the respond time, use the following command.

Command	Mode	Description
ip igmp snooping last-member-query-interval <100-10000>	Global	Configures the time of registering in multicast group after sending Join message on the system. (unit: ms)
ip igmp snooping vlan *VLANS* **last-member-query-interval** <100-10000>		Configures the time of registering in multicast group after sending Join message on a VLAN interface.

i If you configure **ip igmp snooping fast-leave**, it is meaningless to register time as multicast group.

To release the waiting time for respond after sending IGMP Query message, use the following command.

Command	Mode	Description
no ip igmp snooping last-member-query-interval	Global	Returns to the default time of registering Join message in multicast group after sending it.
no ip igmp snooping vlan *VLANS* **last-member-query-interval**		Returns to the default time of registering Join message after sending it on a VLAN interface.

9.2.5.4 IGMP v2 Snooping Report Method

When IGMP report suppression is enabled, the switch forwards only one IGMP report per multicast router query. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers.

Command	Mode	Description
ip igmp snooping report-suppression	Global	Configures the IGMP report suppression on the system.
ip igmp snooping vlan *VLANS* **report-suppression**		Configures the IGMP report suppression on a VLAN interface.

IGMP report suppression is supported only when the multicast query has IGMP v1 and IGMP v2 reports. This feature is not supported when the query includes IGMP v3 reports.

To disable IGMP snooping report suppression, use the following command.

Command	Mode	Description
no ip igmp snooping report-suppression	Global	Deletes the IGMP report suppression on the system.
no ip igmp snooping vlan *VLANS* **report-suppression**		Deletes the IGMP report suppression on a VLAN interface.

To display the IGMP Report Suppression configuration, use the following command.

Command	Mode	Description
show ip igmp snooping [**vlan** *VLANS*]	Enable Global Bridge	Shows that the IGMP report suppression is enabled

9.2.5.5 Mrouter Port

Configuring Mrouter Port per VLAN

You can designate, to which port, the multicast router is connected. If you designate multicast router is connected to where, it is possible to transmit multicast packet or message only to that port.

To designate the port connected to multicast router, use the following command.

Command	Mode	Description
ip igmp snooping mrouter port {*PORTS* | **cpu**}	Global	Designates the port where multicast router is connected to on the system. PORTS: logical port number ID to use cpu: identifies the CPU port to use.
ip igmp snooping vlan *VLANS* **mrouter port** {*PORTS* | **cpu**}		Designates the port where multicast router is connected to on a VLAN interface.

To disable the port where multicast router is connected, use the following command.

Command	Mode	Description
no ip igmp snooping mrouter port {*PORTS* | **cpu**}	Global	Disables the port where multicast router is connected on the system
no ip igmp snooping vlan *VLANS* **mrouter port** {*PORTS* | **cpu**}		Disables the port where multicast router is connected on a VLAN interface.

Mrouter Port Learning Method

For the hiD 6615 S323, multicast-capable router ports are added to the forwarding table for every Layer 2 multicast entry. The switch learns such ports through snooping on PIM packets. The switch snoops on PIM packets on all VLANs.

To configure Mrouter port learning method, use the following commands.

Command	Mode	Description
ip igmp snooping mrouter learn pim	Global	Configures the mrouter port learning method on the system.
ip igmp snooping vlan *VLANS* **mrouter learn pim**		Configures the mrouter port learning method on a VLAN interface.
no ip igmp snooping mrouter learn pim		Disables the mrouter port learning method on the system.
no ip igmp snooping vlan *VLANS* **mrouter learn pim**		Disables the mrouter port learning method on a VLAN interface.

Displaying Mrouter Configuration

To display IGMP snooping mrouter configuration, use the following command.

Command	Mode	Description
show ip igmp snooping mrouter	Enable Global Bridge	Shows the mrouter configuration on the system.
show ip igmp snooping vlan *VLANS* **mrouter**		Shows the mrouter configuration and detail information on a VLAN interface.

9.2.5.6 Multicast TCN Flooding

An IGMP snooping-disabled switch does not flood multicast traffic to all ports in a VLAN when a spanning-tree Topology Change Notification (TCN) is received. A topology can change in a VLAN and it may invalidate previously learned IGMP snooping information. A host that was on one port before the topology change may move to another port after the topology change. The hiD 6615 S223/S323 switch helps to deliver multicast traffic is delivered to all multicast receivers in that VLAN when the topology changes. When the spanning tree protocol is running in a VLAN, a spanning tree topology change notification (TCN) is issued by the root switch in the VLAN.

To flood multicast traffic when TCN packet is received, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood	Global	Designates the port where multicast router is connected to on the system.
ip igmp snooping tcn vlan *VLANS* **flood**		Designates the port where multicast router is connected to on a VLAN interface.

With the **ip igmp snooping tcn flood query count** command, you can enable multicast flooding on a switch for a short period of time following a topology change by configuring an IGMP query threshold.

Command	Mode	Description
ip igmp snooping tcn flood query count <1-10>	Global	Configures IGMP snooping TCN flood query count. 1-10: number of IGMP queries

To configure the interval of incoming IGMP General Query, use the following command.

Command	Mode	Description
ip igmp snooping tcn flood query interval <1-1800>	Global	Configures IGMP snooping TCN flood query Interval. 1-1800: Seconds

With the **ip igmp snooping tcn query solicit** command, you can direct a non-spanning tree root switch to issue the same query solicitation.

Command	Mode	Description
ip igmp snooping tcn query solicit [**address** *A.B.C.D*]	Global	Configures the switch to send a query solicitation when a TCN is detected on the system. address: query solicitation source IP address

To stop the switch from sending a query solicitation, enter the **no ip igmp snooping tcn query solicit** command.

To diable the configured TCN flood settings, use the following commands.

Command	Mode	Description
no ip igmp snooping tcn flood	Global	Disables multicast flooding on the switch.
no ip igmp snooping tcn vlan *VLANS* **flood**		Disables multicast flooding on a VLAN interface.
no ip igmp snooping tcn flood query count		Returns to the default number of IGMP queries.
no ip igmp snooping tcn flood query interval		Returns to the default interval of IGMP queries.
no ip igmp snooping tcn query solicit [**address**]		Stops the switch from sending a query solicitation.

9.2.6 IGMP v3 Snooping

This chapter consists of these sections
- IGMP Snooping Version
- Join Host Management
- Immediate Block

9.2.6.1 IGMP Snooping Version

The reports sent to the multicast router are sent based on the version of that interface. A user can administratively configure the version of the port as 1 or 2. If the user has configured the version specifically, the reports are always sent out with only this version. If the user has not administratively configured the version value, and a v1 query is received on an interface, this interface is made a v1 interface, and all reports sent out of this interface are v1 reports. If no v1 query is received on an interface for the v1 router present timeout period (400 seconds), the interface version goes back to its default value (2).

To configure the version of the IGMP reports sent out of a port, use the following command.

Command	Mode	Description
ip igmp snooping version <1-3>	Global	Configures the version of IGMP report on the system. 1-3: IGMP report version
ip igmp snooping vlan *VLANS* **version** <1-3>		Configures the version of IGMP report on a VLAN interface.

To return to the default version of IGMP report, use the **no** parameter command.

9.2.6.2 Join Host Management

Explicit host tracking is supported only with IGMP v3 hosts.

With explicit host tracking enabled, the switch is in its proxy-reporting mode. In proxy-reporting mode, the switch forwards the first report only for a source-multicast group pair to the router, and suppresses all other reports for the same pair. With IGMP v3 proxy reporting, the switch does proxy reporting for unsolicited reports and reports that are received in the general query interval. By enabling explicit tracking, the router might not be able to track all the hosts that are behind a VLAN interface.

With proxy reporting disabled, the switch works in transparent mode, and updates the IGMP snooping database as it receives reports, then forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

To enable explicit host tracking on a VLAN, use the following command.

Command	Mode	Description
ip igmp snooping explicit-tracking	Global	Enables explicit host tracking on the system.
ip igmp snooping vlan *VLANS* **explicit-tracking**		Enables explicit host tracking on a VLAN interface.

To display a configuration, use the following command.

Command	Mode	Description
show ip igmp snooping explicit-tracking {**vlan** *VLANS* | **port** *PORTS* | **group** *A.B.C.D*}	Enable Global Bridge	Shows a configuration.

9.2.6.3 Immediate Block

For a Layer 2 IGMP v2 host interface to join an IP multicast group, a host sends an IGMP membership report for the IP multicast group. For a host to leave a multicast group, it can either ignore the periodic IGMP general queries or it can send an IGMP leave message. When the switch receives an IGMP leave message from a host, it sends out an IGMP group-specific query to determine whether any devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the table entry for that Layer 2 multicast group so that only those hosts interested in receiving multicast traffic for the group are listed.

However, IGMP v3 hosts send IGMP v3 membership reports (with the allow group record mode) to join a specific multicast group. When IGMP v3 hosts send membership reports (with the block group record) to reject traffic from all sources in the previous source list, the last host on the port will be removed by immediate-leave.

To configure the Immediate Block, use the following command.

Command	Mode	Description
ip igmp snooping immediate-block	Global	Enables immediate block on the system.
ip igmp snooping vlan *VLANS* **immediate-block**		Enables immediate block on a VLAN interface.

9.2.7 Multicast VLAN Registration (MVR)

Multicast VLAN Registration (MVR) is for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service provider network. MVR allows a subscriber on a port to subscribe or not to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network with subscribers remaining in separate VLANs. MVR helps to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscribers subscribe or not (join and leave) these multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP version-2-compatible host. Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other feature. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.

9.2.7.1 Enabling MVR

To use the MVR, enable the MVR function with the following command.

Command	Mode	Description
mvr	Global	Enables MVR on the system.
no mvr		Disables MVR on the system.

9.2.7.2 MVR Group Address

Statically configure a VLAN interface to receive multicast traffic sent to the multicast VLAN and the IP multicast address. An interface statically configured as a member of a group remains a member of the group until statically removed.

Command	Mode	Description
mvr vlan *VLAN* **group** *GROUP-ADDR*	Global	Configures MVR group address. GROUP-ADDR: specific group address (ex: a.b.c.d or a.b.c.d-x.y.z.w)

To delete the statically configured MVR group address, use the following command.

Command	Mode	Description
no mvr vlan *VLAN* **group** *GROUP-ADDR*	Global	Deletes a MVR group address. GROUP-ADDR: specific group address (ex: a.b.c.d or a.b.c.d-x.y.z.w)

9.2.7.3 MVR IP Address

Statically configure a VLAN interface to receive multicast traffic sent to the multicast VLAN and the IP multicast address. An interface statically configured as a member of a group remains a member of the group until statically removed.

When a multicast server belongs to different network from user's network, a multicast router operates as Layer 3 forwarding for each MVR VLAN. In this case, when an IGMP packet of a subscriber is transmitted to the multicast server, a source address of the IGMP packet may not match the network address of MVR VLAN. To handle such a problem, you can replace a source address of an IGMP packet with one of the IP addresses of MVR VLAN.

To configure a helper address to replace a source address of an IGMP packet, use the following command.

Command	Mode	Description
mvr vlan *VLAN* **helper** *IP-ADDRESS*	Global	Configures MVR group address. IP ADDRESS: specific IP address

To delete the statically configured MVR group address, use the following command.

Command	Mode	Description
no mvr vlan *VLAN* **helper**	Global	Deletes a MVR group address. IP ADDRESS: specific IP address

9.2.7.4 Send and Receive Port

Statically configure a VLAN interface to receive multicast traffic sent to the multicast VLAN and the IP multicast address. An interface statically configured as a member of a group remains a member of the group until statically removed.

Command	Mode	Description
mvr port *PORTS* **type** {**receiver** | **source**}	Global	Configures MVR port. PORTS: port number

- **Source**
  This configures uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN.
- **Receiver**
  This configures a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.

To delete the statically configured MVR port, use the following command.

Command	Mode	Description
no mvr port *PORTS*	Global	Deletes a MVR port.

9.2.7.5 Displaying MVR Configuration

To display an MVR configuration, use the following command.

Command	Mode	Description
show mvr	Enable Global	Shows a configuration.
show mvr port		
show mvr vlan *VLANS*		

9.2.8 IGMP Filtering and Throttling

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is

dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only group specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic.

9.2.8.1 Creating IGMP Profile

You can create or modify the IGMP profile to be used for filtering IGMP join requests from a port. The system prompt will be changed to SWITCH(config-igmp-profile[N])# from SWITCH(config)#.

Command	Mode	Description
ip igmp profile <1-2147483647>	Global	Configures IGMP profile.

To delete the created IGMP profile, use the **no ip igmp profile** <1-2147483647> command on global mode.

To display the IGMP profile, use the following command.

Command	Mode	Description
show ip igmp profile [<1-2147483647>]	Enable Global Bridge	Shows IGMP profile.

9.2.8.2 Policy of IGMP Profile

Configure the action to permit or deny access to the IP multicast address using the following command.

Command	Mode	Description
{**permit** | **deny**}	IGMP Profile	Configures the action of IGMP profile.

9.2.8.3 Group Range of IGMP Profile

Configure the group range of IGMP Profile using the following command.

Command	Mode	Description
range *A.B.C.D* [*A.B.C.D*]	IGMP Profile	Configures a group range. A.B.C.D: low IP multicast address A.B.C.D: high IP multicast address
no range *A.B.C.D* [*A.B.C.D*]		Deletes a configured group range.

9.2.8.4 Applying IGMP Profile to the Filter Port

To apply the configured IGMP Profile to the filter port, use the following command.

Command	Mode	Description
ip igmp filter port *PORTS* **profile** <1-2147483647>	Global	Configures IGMP profile. PORTS: port number 1-2147483647: number of configured IGMP profile

To cancel the applying of the profile, use the following command.

Command	Mode	Description
no ip igmp filter port *PORTS*	Global	Disables an applied IGMP profile. PORTS: port number

To display the IGMP filter configuration, use the following command.

Command	Mode	Description
show ip igmp filter [**port** *PORTS*]	Enable Global Bridge	Shows a configuration.

9.2.8.5 Max Number of IGMP Join Group

You can configure the maximum number of IGMP groups that a Layer 2 interface can join. To configure the maximum number of IGMP groups per port, use the following command.

Command	Mode	Description
ip igmp max-groups port *PORTS* **count** <0-2147483647>	Global	Configures the maximum number of IGMP groups. PORTS: port number 0-2147483647: maximum number of IGMP groups that the port can join

To return to the default setting, use the following command.

Command	Mode	Description
no ip igmp max-groups port *PORTS* **count**	Global	Returns to the default of no maximum. PORTS: the number of port

9.2.9 Displaying IGMP Snooping Table

To display an IGMP snooping table, use the following command.

Command	Mode	Description
show ip igmp snooping groups [*IP-ADDRESS*]	Enable Global Bridge	Shows a configuration.
show ip igmp snooping groups port [*PORT*| **cpu**]		
show ip igmp snooping groups vlan *VLANS*		
show ip igmp snooping groups mac-based		

9.3 PIM-SM (Protocol Independent Multicast-Sparse Mode)

IGMP is the protocol to help multicast communication between switch and host, but PIM is the protocol for multicast communication between router and router. There are two kinds of PIM, PIM-DM (Protocol Independent Multicast–Dense Mode) and PIM-SM (Protocol Independent Multicast–Sparse Mode), the hiD 6615 S323 supports PIM-SM only.

Protocol of dense mode can send information about data packet and member to interface, which is not connected to multicast source or receiver, and multicast router saves connection state to all the nodes. In this case, when most hosts are belonged to multicast group and there is enough bandwidth to support flow of controlling message between constituent members, these overheads are acceptable, but the other cases are inefficient.

Contrary to dense mode, PIM-SM receives multicast packet only when request comes from specific host in multicast group. Therefore PIM-SM is proper when constituent members of group are dispersed in wide area or bandwidth used for the whole is small. Sparse mode is the most useful on WAN and can be used on LAN. For standard of PIM-SM, you can refer to RFC 2362.

RPT and SPT

RP (Rendezvous Point) works in a central role for PIM-SM. Viewing the below chart, multicast packet is transmitted to D as RP from A as source, through B and C. And D (RP) transmits multicast packet after receiving join message from E or F. That is, all multicast packets are transmitted with passing through RP (Rendezvous Point). For instance, even though F needs multicast packet, the packet is passed through 『A→B→C→D→C→F』, not 『A→B→C→F』.

Like this, route made with focusing on RP is RPT (Rendezvous Point Tree) or shared tree. There is only one RP in one multicast group. RPT has (*, G) entry because receiver can send a message to RP without knowing source. “G” means multicast group.

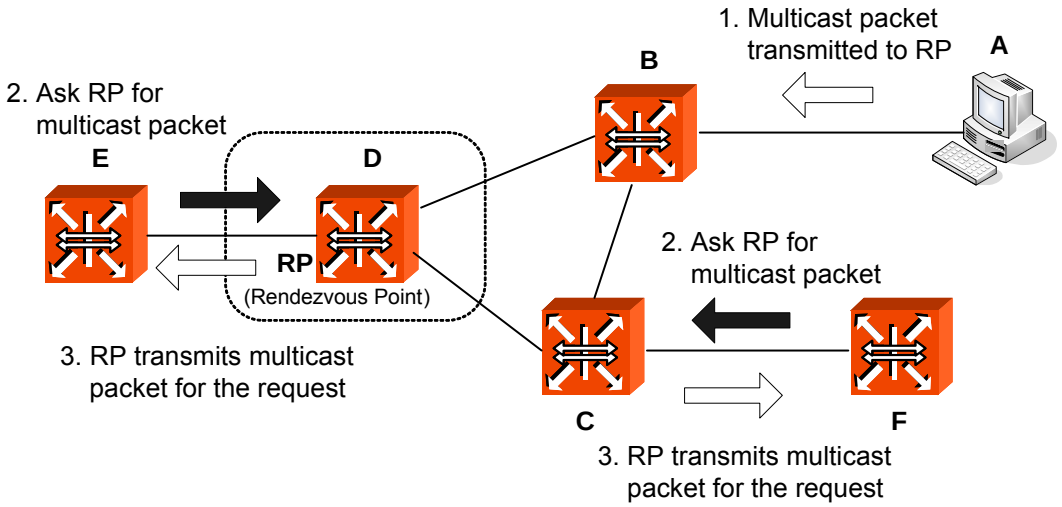


Fig. 9.5 RPT of PIM-SM

Also, routers on packet route automatically optimize route by deleting unnecessary hops when traffic exceeds certain limit. After route to source and multicast group connected to the source are constituted, all sources have route to connect to receiver directly.

In the below figure, packets are usually transmitted through『A→B→C→D』, but packets are transmitted through faster route『A→C→F』when traffic is increased. SPT (Shortest-Path Tree) selects the shortest route between source and receiver regardless of RP, it is called source based tree or short path tree. SPT has (S, G) entry, “S” means source address and “G” means multicast group.

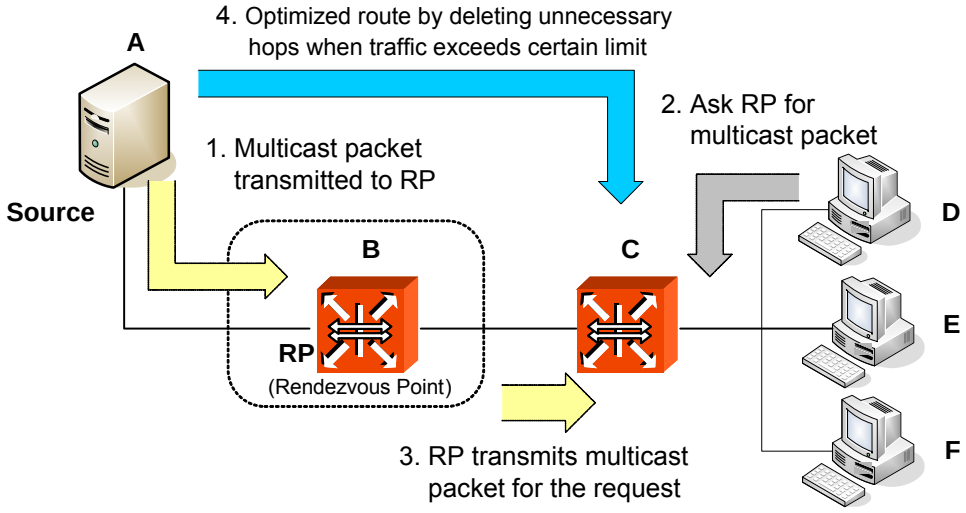


Fig. 9.6 STP of PIM-SM

9.3.1 PIM Common Configuration

Routing functionalities such as RIP, OSPF, BGP and PIM-SM are only available for hiD 6615 S323. (Unavailable for hiD 6615 S223)

9.3.1.1 PIM-SM and Passive Mode

You need to open *Interface Configuration* mode of specified interface for activating PIM-SM on Ethernet interface. To open *Interface Configuration* mode, use the following command.

Command	Mode	Description
interface *INTERFACE*	Global	Opens *Interface Configuration* mode of specified interface.

To disable *Interface Configuration* mode, use the following command.

Command	Mode	Description
no interface *INTERFACE*	Global	Disables a specified interface.

To activate PIM-SM after opening the *Interface Configuration* mode, use the following command.

Command	Mode	Description
ip pim sparse-mode [**passive**]	Interface	Activates PIM-SM on specified interface.

The **ip pim sparse-mode passive** command enables passive mode operation for local members on the interfaces. Passive mode essentially stops PIM transactions on the interface, allowing only IGMP mechanism to be active. To turn off passive mode, use the **ip pim sparse-mode passive** or the **ip pim sparse-mode** command.

To disable PIM-SM, use the following command.

Command	Mode	Description
no ip pim sparse-mode [**passive**]	Interface	Disables PIM-SM from specified interface.

9.3.1.2 DR Priority

To set the priority for which a router is elected as the designated router (DR), use the following command in interface configuration mode.

Command	Mode	Description
ip pim dr-priority <0-4294967294>	Interface	Configures the priority for router. 0-4294967294: priority value
no ip pim dr-priority		Returns to the default value 1.

The router with the highest priority value configured on an interface will be elected as the DR. If this priority value is the same on multiple routers, then the router with the highest IP address configured on an interface will be elected as the DR. If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers with this priority status, then the router with the highest IP address configured on an interface will be elected as

the DR.

9.3.1.3 Filters of Neighbor in PIM

Enable filtering of neighbors on the interface. When configuring a neighbor filter-PIM-SM will either not establish adjacency with the neighbor, or terminate adjacency with the existing neighbors-if denied by filtering access list.

To configure the filtering of neighbor in PIM, use the following command.

Command	Mode	Description
ip pim neighbor-filter {<1-99> | *ACCESS-LIST*}	Interface	Configures the filtering of neighbor in PIM. 1-99: simple access list ACESS-LIST: IP named standard access list
no ip pim neighbor-filter {<1-99> | *ACCESS-LIST*}		Disables the filtering configuration.

9.3.1.4 PIM Hello Query

To configure a query hold time, use the following command.

Command	Mode	Description
ip pim query-holdtime <1-65535>	Interface	Configures the query hold time. 1-65535: hello message hold time (unit: second)
no ip pim query-holdtime		Disables the query hold time configuration.

When configuring query hold time, if the configured value is less than the current query interval, it is refused.

To configure the frequency of hello interval value, use the following command.

Command	Mode	Description
ip pim query-interval <1-18724>	Interface	Configures the frequency of hello time. 1-18724: hello message interval (unit: second)
no ip pim query-interval		Disables the hello message interval configuration.

9.3.1.5 PIM Debug

To activate PIM-SM debugging, use the following command.

Command	Mode	Description
debug pim {**all** | **events** | **nexthop** | **mib** | **mfc** | **nsm** | **packet** [**in** | **out**] | **state** | **timer**}	Enable	Activates PIM debugging. all : all PIM debugging events: PIM events nexthop: PIM-SM nexthop communications mib: PIM-SM MIBs mfc: MFC add/delete/update nsm: PIM-SM network service module communications packet: incoming and/or outgoing packets state: state transition on all PIM-SM FSMs
debug pim timer assert [**at**]		Enables the PIM-SM assert timers debugging.
debug pim timer bsr [**bst** | **crp**]		Enables the PIM-SM BSR timer's debugging.
debug pim timer hello [**ht** | **nlt** | **tht**]		Enables the PIM-SM Hello timer's debugging.
debug pim timer joinprune [**jt** | **et** | **ppt** | **kat** | **ot**]		Enables the PIM-SM JoinPrune timer's debugging.
debug pim timer register [**rst**]		Enables the PIM-SM register timer's debugging.

9.3.2 BSR and RP

There are two ways to decide RP as central of PIM-SM on multicast network. One is that network administrator manually decides RP and the other way is that RP is automatically decided by exchanging information between multicast routers installed on network. The information transmitted between multicast routers in the automatic way is called Bootstrap message and the router, which sends this Bootstrap message, is called BSR (Bootstrap Router). All PIM routers existing on multicast network can be BSR.

Routers that want to be BSP are named as candidate-BSR and one router, which has the highest priority, becomes BSR among them. If there are routers, which have same priority, then one router, which has the highest IP address, becomes BSR. Bootstrap message includes priority to decide BSR, hash-mark to be used in Hash, and RP information. After deciding BSR, routers, which support RP, transmit candidate-RP message to BSR. Candidate-RP message includes priority, IP address, and multicast group. Then BSR adds candidate-RP message to Bootstrap message and transmits it to another PIM router. Through this transmitted Bootstrap message, RP of multicast group is decided.

User's equipment belonged in PIM-SM network can be candidate-BSR and BSR is decided among them. Candidate-BSR transmits Bootstrap message to decide BSR. You can configure priority to decide BSR among Bootstrap messages and Hash-mask.

9.3.3 Bootstrap Router (BSR)

The information transmitted between multicast routers in the automatic way is called Bootstrap message and the router, which sends this Bootstrap message, is called BSR (Bootstrap Router). All PIM routers existing on multicast network can be BSR. Routers, which want to be BSP, are named candidate-BSR and one router, which has the highest

priority, becomes BSR among them. If there are routers, which have same priority, then one router, which has the highest IP address, becomes BSR.

It is possible to configure the following messages, which are included in candidate-BSR message.

Since it is possible to assign several IP addresses in hiD 6615 S323, the switch may have several IP addresses assigned. User can select one IP address among several IP addresses to be used in switch as candidate-BSR.

When there are same priorities to compare candidate-BSR, IP address is compared through Hash. User can configure Hash-mask to apply Hash.

If you decide BSR among candidate-BSRs, priority in Bootstrap message is compared to decide it. The highest priority of candidate-BSR becomes BSR. In order to configure priority of Bootstrap message, use the following command.

To configure candidate-BSR, use the following command.

Command	Mode	Description
ip pim bsr-candidate *INTERFACE* [<0-32>] [<0-255>]	Global	Gives the switch the candidate BSR status. INTERFACE: interface name 0-32: hash mask length for RP selection 0-255: priority for candidate bootstrap switch

To disable assigned IP address in candidate-BSR, use the following command.

Command	Mode	Description
no ip pim bsr-candidate	Global	Disables .the configuration of BSR-candidate.

You can clear all RP sets learned through the PIM Bootstrap Router (BSR) using the following command.

Command	Mode	Description
clear ip pim sparse-mode bsr rp-set *	Global	Clears all RP sets.

9.3.4 RP Information

After deciding BSR on multicast network, candidate-RP routers send RP message to BSR. Candidate-RP message includes priority, IP address, and multicast group. Then, BSR adds the received candidate-RP information to Bootstrap message and transmit to another PIM router. Through this Bootstrap message, RP of multicast group is decided. All routers belonged in multicast network can become candidate-RP and routers which generally consist candidate-BSR are supposed to consist candidate-RP. It is possible to configure the following information, which is included in candidate-RP message.

9.3.4.1 Static RP for Certain Group

You can configure several IP addresses on the hiD 6615 S323. Therefore, you need to

decide which IP address to be used as candidate-RP. This command is used to statically configure the RP address for multicast groups.

To configure IP address to be used in candidate-RP, use the following command.

Command	Mode	Description
ip pim rp-address *A.B.C.D* [<1-99> | <1300-1999>] [**override**]	Global	Configures RP address for multicast groups statically. A.B.C.D: IP address 1-99: IP standard access list 1300-1999: IP standard access list (expanded range) override: override dynamically RP mappings

- If RP-address configured through BSR and RP-address configured statically are both available for a group range, the RP-address configured through BSR is chosen.
- If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.

To delete configured IP address, use the following command.

Command	Mode	Description
no ip pim rp-address *A.B.C.D*	Global	Deletes configured IP address.

9.3.4.2 Enabling Transmission of Candidate RP Message

Use this command to give the router the candidate RP status using the IP address of the specified interface.

Command	Mode	Description
ip pim rp-candidate *INTERFACE* [**group-list** <1-99>] [**interval** <1-16383>] [**priority** <0-255>]	Global	Configures a message for a candidate RP. INTERFACE: interface name 1-99: IP standard access list 1-16383: advertisement interval (unit: second) 0-255: priority value

To delete configured priority of candidate-RP, use the following command.

Command	Mode	Description
no ip pim rp-candidate	Global	Unconfigures the entire setting of candidate-RP.
no ip pim rp-candidate *INTERFACE*		Deletes the setting of candidate-RP of specific interface.
no ip pim rp-candidate *INTERFACE* **group-list** <1-99>		

9.3.4.3 KAT (Keep Alive Time) of RP

You can configure KAT for (S, G) states at RP to monitor PIM Register packets, overriding the generic KAT timer value.

Command	Mode	Description
ip pim rp-register-kat <1-65535>	Global	Configures Keep Alive Time. 1-65535: time
no ip pim rp-register-kat		Disables a KAT configuration.

9.3.4.4 Ignoring RP Priority

To ignore the RP-SET priority value, and use only the hashing mechanism for RP selection, use the following command. It is used to inter-operate with older Cisco IOS versions.

Command	Mode	Description
ip pim ignore-rp-set-priority	Global	Ignores the PR-SET priority value.
no ip pim ignore-rp-set-priority		Deletes the priority ignoring configuration.

9.3.5 PIM-SM Registration

9.3.5.1 Rate Limit of Register Message

You can configure the rate of register packets sent by the designated router (DR), in units of packets per second. Enabling this command will limit the load on the DR and RP at the expense of dropping those register messages that exceed the set limit. Receivers may experience data packet loss within the first second in which register messages are sent from bursty sources.

The configured rate is per (S, G) state, not a system wide rate.

Command	Mode	Description
ip pim register-rate-limit <1-65535>	Global	Configures the rate of register packets. 1-65535: the maximum number of packets that can be sent per second.
no ip pim register-rate-limit		Disables the limit configuration.

9.3.5.2 Registeration Suppression Time

Use this command to configure the register-suppression time, in seconds, overriding the default value of 60 seconds. Configuring this value modifies register-suppression time at the DR, and configuring this value at the RP modifies the RP-keepalive-period value if the **ip pim re-register-kat** command is not used.

To configure the registration suppression time, use the following command.

Command	Mode	Description
ip pim register-suppression <1-65535>	Global	Configures the time of registration suppression. 1-65535: The register suppression on time in seconds.
no ip pim register-suppression		Disables the registration suppression time.

9.3.5.3 Filters for Register Message from RP

One network may include different multicast groups and routers that are not members of multicast group. Therefore it can happen that routers, which are members of another network or not members of multicast group, apply for RP and transmit candidate-RP message.

To prevent this case, user can block candidate-RP message of another router by making only candidate-RP in multicast group communicate. In order to block candidate-RP message from routers which are not members, perform the below tasks.

Step 1
Configure filtering out multicast sources.

Command	Mode	Description
ip pim accept-register list {<100-199> | <2000-2699> | *ACCESS-LIST*}	Global	Configures multicast source filtering function. 100-199: IP extended access-list 2000-2699: IP extended access list (expanded range) ACCESS-LIST: IP named Standard Access List

Step 2
Allow or deny only the transmitted packets by routers that exchange candidate-RP message.

Command	Mode	Description
access-list {<100-199> | <2000-2699>} {**deny** | **permit**} **ip** {*A.B.C.D* | **any**}	Global	Configures multicast source filtering function. 100-199: IP extended access list 2000-2699: IP extended access list (expanded range) A.B.C.D: address to match

To delete the above configuration, use the following command.

Command	Mode	Description
no ip pim accept-register	Global	Releases blocked packet.

9.3.5.4 Source Address of Register Message

To configure the source IP address of Register packets sent by DR, overriding the default source IP address, use **ip pim register-source** command. The configured address must be a reachable address to be used by the RP to send corresponding Register-Stop mes-

sage in response. It is normally the loopback interface address, but can also be other physical addresses. This address must be advertised by unicast routing protocols on the DR.

Command	Mode	Description
ip pim register-source {*A.B.C.D* | *INTERFACE*}	Global	Configures the source address of register message. A.B.C.D: IP address to be used as source INTERFACE: interface address to be used as source
no ip pim register-source		Disables the registration suppression time.

By default, the IP address of the outgoing interface of the DR leading to the RP is used as the IP source address of a register message.

9.3.5.5 Reachability for PIM Register Process

To enable the RP reachability verification for PIM Register processing at the DR, use the following command.

Command	Mode	Description
ip pim register-rp-reachability	Global	Enables the RP reachability verification function.
no ip pim register-rp-reachability		Disables the RP reachability verification function. (default)

i This command is disabled by default.

9.3.6 SPT Switchover

This command is used to enable and configure the bandwidth of the switchover from RPT to SPT for the certain group. If a source sends at a rate greater than or equal to traffic rate (the kbps value), a PIM join message is triggered toward the source to construct a source tree. Specifying a group list access list indicates the groups to which the threshold applies. If the traffic rate from the source drops below the threshold traffic rate, the leaf router will switch back to the shared tree and send a prune message toward the source.

Command	Mode	Description
ip pim spt-threshold	Global	Enables the ability for the last-hop PIM router to switch to SPT.
ip pim spt-threshold group-list {<1-99> | <1300-1999> | *ACCESS-LIST*}		Enables the ability for the last-hop PIM router to switch to SPT for multicast group addresses specified by the given access list.
no ip pim spt-threshold		Disables switching to SPT option.
no ip pim spt-threshold group-list {<1-99> | <1300-1999> | *ACCESS-LIST*}		

9.3.7 PIM Join/Prune Interoperability

To configure the TX interval of PIM/Join/Prune Message, use the following command.

Command	Mode	Description
ip pim message-interval <1-65535>	Global	Configures Join/Prune timer value. 1-65535: interval (unit: second)
no ip pim message-interval		Disables TX interval configuration.

9.3.8 Cisco Router Interoperability

9.3.8.1 Checksum of Full PIM Register Message

Although source of multicast is not connected to multicast group, multicast communication is possible. In the below picture, First-Hop router directly connected to source can receive packet from source without (S, G) entry about source. The First-Hop router encapsulates the packet in Register message and unicasts to RP of multicast group. RP decapsulates capsule of Register message and transmits it to members of multicast group.

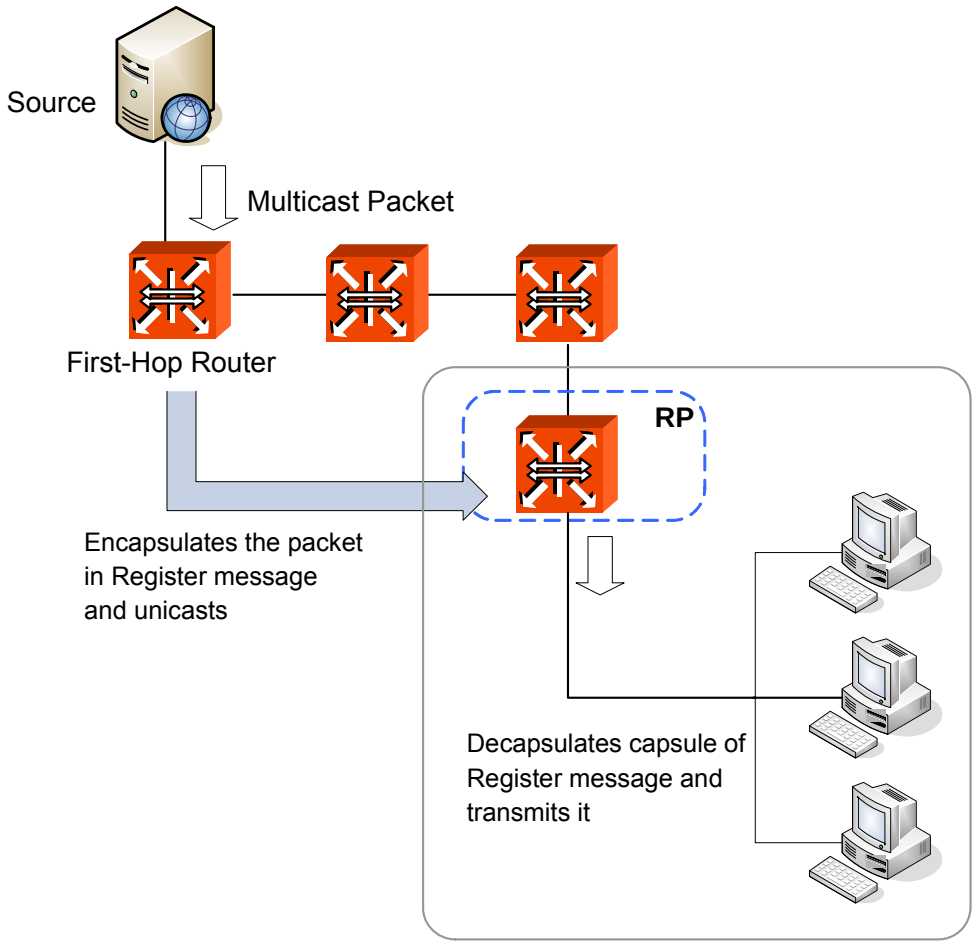


Fig. 9.7 In Case Multicast Source not Directly Connected to Multicast Group

When the Register message is transmitted, the range of Checksum in header conforms to header part as RFC standard, but whole packet is included in the range of checksum in case of Cisco router. For compatibility with Cisco router, you should configure the range of Checksum of Register message as whole packet.

To configure the range of Checksum of Register message as whole packet for compatibility with Cisco router, use the following command.

Command	Mode	Description
ip pim cisco-register-checksum	Global	Configures the option to calculate the Register checksum over the whole packet.
ip pim cisco-register-checksum group-list {<1-99> | <1300-1999> | *ACCESS-LIST*}		Configures the option to calculate the Register checksum over the whole packet on multicast group specified by the access list. 1-99: simple access-list 1300-1999: simple access list (extended range) ACCESS-LIST: IP named standard access list

To delete a configured Cisco-compatible checksum option, use the following command.

Command	Mode	Description
no ip pim cisco-register-checksum	Global	Deletes a configured value.

i This command is disabled by default. And Register Checksum is calculated only over the header by default.

9.3.8.2 Candidate RP Message with Cisco BSR

Cisco's BSR code does not conform to the latest BSR draft, it does not accept candidate RPs with a group prefix number of zero. To make the hiD 6615 S323 candidate RP work with a Cisco BSR, use the following command. This command is used to inter-operate with older Cisco IOS versions.

Command	Mode	Description
ip pim crp-cisco-prefix	Global	Configure the Candidate RP-Message to work with Cisco BSR
no ip pim crp-cisco-prefix		Return to the default setting

9.3.8.3 Excluding GenID Option

To exclude the GenID option from Hello packets on particular interface for inter-operation with older Cisco IOS versions, use the following command

Command	Mode	Description
ip pim exclude-genid	Interface	Excludes the GenID from hello packets.
no ip pim exclude-genid		Returns to the default setting.

9.3.9 PIM-SSM Group

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the following command. When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.

Command	Mode	Description
ip pim ssm range {<1-99> | *ACCESS-LIST*}	Global	Defines the SSM range of IP multicast address. 1-99: simple access list ACCESS-LIST: IP named standard access list
ip pim ssm default		Configures the SSM by default.
no ip pim ssm		Disables the command.

9.3.10 PIM Snooping

PIM Snooping is used to reduce unnecessary bandwidth by restricting data and multicast control packets which transmitted between each port. In networks where a Layer 2 switch interconnects several routers, the switch floods IP multicast packets on all multicast router ports by default, even if there are no multicast receivers downstream. If PIM Snooping is enabled, the switch restricts multicast packets for each IP multicast group to only those multicast router ports that have downstream receivers joined to that group. And the switch learns which multicast router ports need to receive the multicast traffic within a specific VLAN by listening to the PIM hello messages, PIM join and prune messages.

To configure PIM Snooping, use the following command.

Command	Mode	Description
ip pim snooping	Global	Enables PIM Snooping function on the switch.
ip pim snooping vlan *VLANS*		Enables PIM Snooping function on a specific interface.
no ip pim snooping		Disables the PIM Snooping command.
no ip pim snooping vlan *VLANS*		

To delete all L2 PIM snooping multicast groups of a specified port, multicast address or vlan, use the following command.

Command	Mode	Description
clear ip pim snooping groups [*A.B.C.D*]	Enable Global Bridge	Deletes all PIM snooping groups and source addresses of a specified multicast group address.
clear ip pim snooping groups [**port** *PORTS*]		Deletes all PIM snooping groups and source addresses of a specified port.
clear ip pim snooping groups [**vlan** *VLANS*]		Deletes all of the multicast router addresses and DR of a specified VLAN.

i By default, PIM Snooping is disabled. To operate PIM Snooping, IGMP Snooping should be enabled as well.

To display the PIM Snooping configuration, use the following command.

Command	Mode	Description
show ip pim snooping	Enable Global Bridge	Shows the PIM snooping configuration such as enable/disable status and the enabled VLANs.
show ip pim snooping vlan *VLANS*		Shows the multicast router address and DR of a specified VLAN.
show ip pim snooping groups [*A.B.C.D*]		Shows the PIM snooping group, source addresses of a specified VLAN, port or multicast group address. A.B.C.D : Multicast group address PORTS: Spedify the logical port number to use VLANS: VLAN ID (ex : NAME | X | X-Y)
show ip pim snooping groups port *PORTS*		
show ip pim snooping groups vlan [*VLANS*]		

9.3.11 Displaying PIM-SM Configuration

To display the information of PIM-SM configuration, use the following command.

Command	Mode	Description
show ip pim bsr-router	Enable Global Bridge	Shows Bootstrap router (v2).
show ip pim interface [**detail**]		Shows PIM interface information.
show ip pim local-members [*INTERFACE*]		Shows PIM local membership information.
show ip pim neighbor [**detail**]		Shows PIM neighbor information.
show ip pim mroute [*A.B.C.D*]		Shows PIM master router.
show ip pim nexthop		Shows PIM next hops.
show ip pim rp mapping		Shows PIM Rendezvous Point (RP) information.
show ip pim rp-hash *A.B.C.D*		Shows RP to be chosen based on group selected. A.B.C.D: group address

10 IP Routing Protocol

Routing functionalities such as RIP, OSPF, BGP and PIM-SM are only available for hiD 6615 S323. (Unavailable for hiD 6615 S223)

10.1 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different autonomous systems (AS). BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops and en-force policy decisions at the AS level.

Multiprotocol BGP (MBGP) extensions enable BGP to support IPv6. MBGP defines the attributes MP_REACH_NLRI and MP_UNREACH_NLRI, which are used to carry IP v6 reachability information. Network layer reachability information (NLRI) update messages carry IPv6 address prefixes of feasible routes.

BGP allows for policy-based routing. You can use routing policies to choose among multiple paths to a destination and to control the redistribution of routing information.

BGP uses the Transmission Control Protocol (TCP) as its transport protocol, using port 179 for establishing connections. Running over a reliable transport protocol eliminates the need for BGP to implement update fragmentation, retransmission, acknowledgment, and sequencing.

The routing protocol software supports BGP version 4. This version of BGP adds support for classless interdomain routing (CIDR), which eliminates the concept of network classes. Instead of assuming which bits of an address represent the network by looking at the first octet, CIDR allows you to explicitly specify the number of bits in the network address, thus providing a means to decrease the size of the routing tables. BGP version 4 also supports aggregation of routes, including the aggregation of AS paths

An Autonomous System (AS) is a set of routers that are under a single technical administration and normally use a single interior gateway protocol and a common set of metrics to propagate routing information within the set of routers. To other ASs, an AS appears to have a single, coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.

The two most important consequences are the need for interior routing protocols to reach one hop beyond the AS boundary, and for BGP sessions to be fully meshed within an AS. Since the next-hop contains the IP address of a router interface in the next autonomous system, and this IP address is used to perform routing, the interior routing protocol must be able to route to this address. This means that interior routing tables must include entries one hop beyond the AS boundary. When a BGP routing update is received from a neighboring AS, it must be relayed directly to all other BGP speakers in the AS. Do not expect to relay BGP paths from one router, through another, to a third, all within the same AS.

10.1.1 Basic Configuration

10.1.1.1 Configuration Type of BGP

When configuring BGP, you can select BGP configuration type between standard BGP and ZebOS BGP for the hiD 6615 S323.

The standard BGP is one of the general BGP configuration type, which includes the following restrictions.

- **Manual transmission of community information**
  You should send the community information or message to neighbors directly using the **neighbor** {*A.B.C.D* | *WORD*} **send-community** command.
- **No synchronization**
  Standard configuration type does not support a synchronization between IGP and eBGP. In this type, BGP network disables IGP synchronization in BGP by default.
- **No auto-summary**
  Standard configuration type does not support auto summary feature. By default, the system disables the automatic network number summarization.

i The ZebOS type requires no specific configuration for sending out BGP community and extended community attributes. ZebOS type is the default for the hiD 6615 S323.

To select configuration type of the BGP router, use the following command.

Command	Mode	Description
bgp config-type {**standard** | **zebos**}	Global	Sets the BGP configuration type between standard and ZebOS.
no bgp config-type		Deletes the recent BGP configuration type and returns to default.

10.1.1.2 Enabling BGP Routing

Step 1

To define an AS number and open *Router Configuration* mode, use the following command.

Command	Mode	Description
router bgp <1-65535>	Global	Assigns AS number to configure BGP routing and opens *Router Configuration* mode. 1-65535: AS number

Step 2

To specify a network to operate with BGP, use the following command.

Command	Mode	Description
network *A.B.C.D/M*	Router	Adds BGP network to operate. A.B.C.D/M: network address with netmask A.B.C.D: network address NETMASK: subnet mask
network *A.B.C.D* **mask** *NET-MASK*		

10.1.1.3 Disabling BGP Routing

Step 1

To delete a specified network to operate with BGP, use the following command.

Command	Mode	Description
no network *A.B.C.D/M*	Router	Deletes BGP network. A.B.C.D/M: network address with netmask A.B.C.D: network address NETMASK: subnet Mask
no network *A.B.C.D* **mask** *NET-MASK*		

Step 2

Go back to *Global Configuration* mode using the **exit** command.

Step 3

To disable BGP routing of the chosen AS, use the following command.

Command	Mode	Description
no router bgp <1-65535>	Global	Deletes assigned AS number to configure BGP routing, enter the AS number. 1-65535: AS number

10.1.2 Advanced Configuration

The hiD 6615 S323 is possibly configured for the additional configurations related BGP. The advanced configurations describe in the following sections, are as follows:

- Summary of Path
- Automatic Summarization of Path
- Multi-Exit Discriminator (MED)
- Choosing Best Path
- Graceful Restart

10.1.2.1 Summary of Path

Aggregation combines the characteristics of several different routes and advertises a single route. In the example of 2 routes information of 172.16.0.0/24 and 172.16.1.0/24, the **as-set** parameter creates an aggregate entry advertising the path for a single route of 172.16.0.0/23, consisting of all elements contained in all paths being summarized. Use this feature to reduce the size of path information by listing the AS number only once, even if it was included in multiple paths that were aggregated. And it's useful when aggregation of information results in incomplete path information.

Using the **summary-only** parameter transmits the IP prefix only, suppressing the more-specific routes to all neighbors. Using the **as-set** parameter transmits a single AS path information only, one of AS numbers of each path.

To summarize route's information for the transmission, use the following command.

Command	Mode	Description
aggregate-address *A.B.C.D/M* **as-set** [**summary-only**]	Router	Summarizes the information of routes and transmits it to the other routers. A.B.C.D/M: network address summary-only: transmits IP prefix only. as-set: transmits one AS-path information.
aggregate-address *A.B.C.D/M* **summary-only** [**as-set**]		

To delete the route's information of specific network address, use the following command.

Command	Mode	Description
no aggregate-address *A.B.C.D/M* **as-set** [**summary-only**]	Router	Disables the summarization function of routes.
no aggregate-address *A.B.C.D/M* **summary-only** [**as-set**]		

10.1.2.2 Automatic Summarization of Path

Automatic summarization is new feature to expend the route information up to the class of specified IP address on interface connected directly to BGP router. For example, A class is fundamentally had "/8" as the subnet mask in case IP address assigned 100.1.1.1 in A class. It can generate route information of 100.0.0.0/8.

To enable/disable automatic summarization of the route, use the following command.

Command	Mode	Description
auto-summary	Router	Enables automatic network summarization of a route.
no auto-summary		Disables automatic network summarization of a route.

Please note that, use this feature when you use the basic classes in network.

10.1.2.3 Multi-Exit Discriminator (MED)

During the best-path selection process, the switch compares weight, local preference and as-path in turn among the similar parameters of BGP routers. Then, the MED is considered when selecting the best path among many alternative paths.

The hiD 6615 S323, MED comparison is configured only among all paths from the autonomous system. You can configure the comparison of MEDs among all BGP routers within autonomous system. In addition, MED is used when comparing of routes from the neighboring routers placed within different AS.

To find the best route by comparing MED values, use the following command.

Command	Mode	Description
bgp always-compare-med	Router	Configures the router to consider the comparison of MEDs in choosing the best path from among paths.
no bgp always-compare-med		Chooses the best path regardless of the comparison of MEDs.

Meanwhile, when the best-path is selected among the neighbor routers within same Autonomous System, it doesn't compare MED values of them. However, in case the paths have same AS-path information, it does compare MED values. If there are two paths with different AS-path each other, the comparison of MED is unnecessary work. Other parameter's path information can be used to find the best path.

To compare MED values in order to choose the best path among lots of alternative paths included same AS-path value, use the following command.

Command	Mode	Description
bgp deterministic-med	Router	Configures the router to compare MEDs in choosing the best path when paths have same AS-path information.
no bgp deterministic-med		Configures the router not to compare MEDs even if the paths have same AS-path.

i During the best-path selection process, use the **bgp always-compare-med** command in case of comparing MED values regardless of AS-path. Otherwise, use the **bgp deterministic-med** command if it compares MED values of lots of paths contained same AS-path information.

10.1.2.4 Choosing Best Path

There are a lot of path parameters BGP protocol, which are IP address, AS, MED value and router ID. Even if two paths look same under the condition of IP address, they are actually different when other parameters are compared with each other.

To ignore AS-path for selecting the best path, use the following command.

Command	Mode	Description
bgp bestpath as-path ignore	Router	Ignores the information of AS-path as a factor in the algorithm for choosing the best route.
no bgp bestpath as-path ignore		Considers the information of AS-path as a factor in the algorithm for choosing the best route.

i If you would like to configure to select the best route by considering AS-path length of Confederation, you should configure the router first to ignore AS-path for choosing the best route using the **bgp bestpath as-path ignore** command before implementing the following command.

To consider AS-path length of Confederation during the best-path selection process, use the following command.

Command	Mode	Description
bgp bestpath compare-confed-aspath	Router	Considers the information of AS-path length of confederation as a factor in the algorithm for choosing the best route.
no bgp bestpath compare-confed-aspath		Ignores AS-path length of confederation as a factor in the algorithm for choosing the best route.

When comparing similar routes from more than 2 peers the BGP router does not consider router ID of the routes. It selects the first received route. The hiD 6615 S323 uses router ID in the selection process; similar routes are compared and the route with lowest router ID is selected as the best route. Router ID can be manually set by using the following command.

To select the best path by comparing router ID, use the following command. However, the default condition is that BGP receives routes with identical eBGP paths from eBGP peers.

Command	Mode	Description
bgp bestpath compare-routerid	Router	Selects the best path using the router ID for identical eBGP paths.
no bgp bestpath compare-routerid		Disables selecting the best path using the router ID.

The hiD 6615 S323 is basically configured not to compare MED values of the path information that exchanges between the Confederation Peers. But just in case, it can be configured to compare MED values of the path information that exchanges between Confederation Peers.

To compare MED values on the exchange of path information between Confederation Peers, use the following command.

Command	Mode	Description
bgp bestpath med confed [**missing-as-worst**]	Router	Configures the router to consider the MED in choosing a path from among the paths on the exchange of information between confederation peers.
bgp bestpath med missing-as-worst [**confed**]		

To ignore MED values of paths on the exchange of information between confederation peers, use the following command.

Command	Mode	Description
no bgp bestpath med confed [**missing-as-worst**]	Router	Ignores MEDs of paths on the exchange of their information between confederation peers.
no bgp bestpath med missing-as-worst [**confed**]		

If there are several equal paths, one of them has no MED value. Because this path is considered as “zero” without MED value, it will be chosen the best path. But the path would be the worst one if it has no MED value after **missing-as-worst** is set.

i After **missing-as-worst** parameter is configured in the system, the path will be recognized as the worst path without MED value.

10.1.2.5 Graceful Restart

Graceful restart allows a router undergoing a restart to inform its adjacent neighbors and peers of its condition. The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. With a graceful restart, the restarting router can still forward traffic during the restart period, and convergence in the network is not disrupted. The restart is not visible to the rest of the network, and the restarting router is not removed from the network topology.

The main benefits of graceful restart are uninterrupted packet forwarding and temporary suppression of all routing protocol updates. Graceful restart thus allows a router to exchange path information with the neighboring router.

To configure graceful restart specifically for BGP, use the following command.

Command	Mode	Description
bgp graceful-restart	Router	Sets to use graceful restart in BGP protocol.
no bgp graceful-restart		Disables the restart time value setting.

Therefore, 2 options of the time can be used to speed up routing convergence by its peer in case that BGP doesn’t come back after a restart.

- **Restart Time**
  It's the waiting time for the restarting of Neighboring router's BGP process. Restart time allows BGP process time to restart and implement the internal connection (The session). However, if it's not working properly, it is considered as the router stops operating.
- **Stalepath Time**
  After BGP process of Neighboring router is restarted, it holds the time until BGP up dates the path information. In case that the information of BGP routes is not updated until the stalepath time, the switch discards this BGP routes information.

To set restart time or stalepath time on Graceful Restarting algorithm, use the following command.

Command	Mode	Description
bgp graceful-restart restart-time <1-3600>	Router	Sets the restart time of Graceful Restart configuration in the unit of second. 1-3600: restart time (default: 120)
bgp graceful-restart stalepath-time <1-3600>		Sets the stalepath-time of Graceful Restart configuration in the unit of second. 1-3600: stalepath time (default: 30)

If you don't use Graceful Restart feature or want to return the default value for restart time or stalepath time, use the following command.

Command	Mode	Description
no bgp graceful-restart restart-time [<1-3600>]	Router	Restores the default value for restart time.
no bgp graceful-restart stalepath-time [<1-3600>]		Restores the default value for stalepath time.

10.1.3 IP Address Family

The hiD 6615 S323 recently supports both unicast and multicast as address-family. Use the following command in choosing either unicast or multicast to enter the *Address-Family Configuratio*n mode allowing configuration of address-family specific parameters.

Use the following command in order to enable address family routing process, which open you in *Address-Family Configuration* mode.

Command	Mode	Description
address-family ipv4 [**multicast** | **unicast**]	Router	Opens the *Address-Family Configuration* mode to configure sessions for IP v4 prefixes.
exit-address-family	Address-Family	Exits to *Router Configuration* mode.

10.1.4 BGP Neighbor

To assign IP address or peer group name for BGP Neighboring router within specified AS number, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *WORD*} **remote-as** <1-65535>	Router	Configures BGP neighboring router and specify AS number of BGP Neighbor. NEIGHBOR-IP: neighbor IP address WORD: peer group name or neighbor tag 1-65535: remote AS Number
no neighbor {*NEIGHBOR-IP* | *WORD*} **remote-as** <1-65535>		Deletes the configured BGP Neighbor within specified AS number.

10.1.4.1 Default Route

The hiD 6615 S323 can be configured that particular neighboring BGP routers or peer group is assigned by default route as 0.0.0.0. Then, neighboring router or member of peer group is able to receive the information of default route from the designated routers.

The following command allows neighboring BGP routers or Peer Group to transmit 0.0.0.0 as the default route.

To generate the default route to BGP neighbor or peer group, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *WORD*} **default-originate** [**route-map** *NAME*]	Router	Generates the default route to BGP Neighbor. NEIGHBOR-IP: neighbor IP address WORD: peer group name or neighbor tag 1-65535: remote AS number NAME: route map name
no neighbor {*NEIGHBOR-IP* | *WORD*} **default-originate** [**route-map** *NAME*]		Removes the default route for BGP Neighbor or peer group.

10.1.4.2 Peer Group

As the number of external BGP group increases, the ability to support a large number of BGP sessions may become a scaling issue. In principle all members of BGP routers within a single AS must connect to other neighboring routers. The preferred way to configure a large number of BGP neighbors is to configure a few groups consisting of multiple neighbors per group. Supporting fewer BGP groups generally scales better than supporting a large number of BGP groups. This becomes more evident in the case of dozens of BGP neighboring groups when compared with a few BGP groups with multiple peers in each group. If the routers belong to same group, they can be applied by same configuration. This group is called as Peer Group.

After peer relationships have been established, the BGP peers exchange update message to advertise network reachability information. You can arrange BGP routers into groups of peers.

To create a BGP Peer Group, use the following command.

Command	Mode	Description
neighbor *NAME* **peer-group**	Router	Create a BGP peer group. NAME: peer group name
no neighbor *NAME* **peer-group**		Delete the BGP peer group created before.

To specify neighbor to the created peer group, use the following command.

Command	Mode	Description
neighbor *NEIGHBOR-IP* **peer-group** *NAME*	Router	Includes BGP neighbor to specified peer group using IP address. NEIGHBOR-IP: neighbor IP address NAME: peer group name
no neighbor *NEIGHBOR-IP* **peer-group** *NAME*		Removes BGP neighbor from the specified Peer Group.

10.1.4.3 Route Map

You can apply the specific route map on neighboring router that the exchange route information between routers or blocking the IP address range is configured on route map.

To make BGP Neighbor router exchange the routing information using Route-map, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *GROUP*} **route-map** *NAME* {**in** | **out**}	Router	Applies a route map to incoming or outgoing routes on neighboring router or peer group and exchange the route information. NEIGHBOR-IP: neighbor IP address GROUP: peer group name NAME: route map name
no neighbor {*NEIGHBOR-IP* | *GROUP*} **route-map** *NAME* {**in** | **out**}		Removes the connection with configured route-map.

10.1.4.4 Force Shutdown

The hiD 6615 S323 supports the feature to force to shutdown any active session for the specified BGP router or peer group and to delete the routing data between them. It shutdowns all connections and deletes the received path information from neighboring router or peer group.

To disable the exchange information with a specified router or peer group, use the following command.

Command	Mode	Description
neighbor {*NEIGHBOR-IP* | *WORD*} **shutdown**	Router	Shutdowns any active session for the specified router or peer group and delete all related routing data. NEIGHBOR-IP: neighbor IP address WORD: peer group name or neighbor tag
no neighbor {*NEIGHBOR-IP-ADDRESS* | *WORD*} **shutdown**		Enables the sessions with a previously existing neighbor or peer group that had been disabled.

10.1.5 BGP Session Reset

When you manage BGP network, you can use the command to reset the session for all peers occasionally. Because the internal connections are re-established newly after resetting, the route information of the connected routers is restored by default.

You can reset the session in specified condition. The hiD 6615 S323 is available with several parameters to reset the BGP connections.

The advanced configurations describe in the following sections, are as follows:

- Session Reset of All Peers
- Session Reset of Peers within Particular AS
- Session Reset of Specific Route
- Session Reset of External Peer
- Session Reset of Peer Group

10.1.5.1 Session Reset of All Peers

To reset the sessions with all BGP peers, use the following command.

Command	Mode	Description
clear ip bgp *	Global	Resets all sessions with BGP peer groups.

When the route parameters restore to the default value by reset command, you can configure the specific parameters for its initialization. If you would like to reset/clear the outgoing advertised routes only, you should use **out** parameter. Otherwise, if you'd like to reset/clear the incoming advertised routes only, you should use **in** parameter.

Meanwhile, if **prefix-filter** is configured with **in** option, ORF (Outbound Route Filtering) and incoming route can be reset. **ipv4** option makes BGP peers have narrowed down to IP address family peers. By using **soft** option, you can configure the switch to update route information only when the session is still connected.

To reset the sessions of all peers and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp * in [**prefix-filter**]	Global	Resets the session of specific group under * condition. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does in-bound soft reconfiguration. *: the conditional option (peer group name or AS number or IP address)
clear ip bgp * ipv4 {**unicast** | **multicast**}**in** [**prefix-filter**]		
clear ip bgp out		Resets the session of specific group under * condition. *: the conditional option (peer group name or AS number or IP address) out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp * ipv4 {**unicast** | **multicast**} **out**		
clear ip bgp * soft [**in** | **out**]		Updates the route information only while the session is possible for specific group under * condition. Apply the route either incoming or outgoing routes. *: the conditional option (peer group name or AS number or IP address)
clear ip bgp * ipv4 {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.5.2 Session Reset of Peers within Particular AS

To reset the session with all neighbor router which are connected to a particular AC, use the following command.

Command	Mode	Description
clear ip bgp <1-65535>	Global	Resets the session with all members of neighbor routers which are configured a particular AC number.

i See Section 10.1.5.1 when you configure the detail parameters.

To reset the sessions of BGP neighboring routers which are belong to specific AS number and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp <1-65535> **in** [**prefix-filter**]	Global	Resets the session of BGP neighboring routers which are configured a particular AC number. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does in-bound soft reconfiguration. 1-65535: AS number
clear ip bgp <1-65535> **ipv4** {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp <1-65535> **out**		Resets the session of BGP neighboring routers which are configured a particular AC number. 1-65535: AS number out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp <1-65535> **ipv4** {**unicast** | **multicast**} **out**		

Command	Mode	Description
clear ip bgp <1-65535> **soft** [**in** | **out**]	Global	Updates the route information only while the session is possible of BGP neighboring routers which are configured a particular AC number. Apply the route either incoming or outgoing routes. 1-65535: AS number
clear ip bgp <1-65535> **ipv4** {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.5.3 Session Reset of Specific Route

To reset the sessions of BGP neighboring router with specified IP address, use the following command.

Command	Mode	Description
clear ip bgp *ROUTE-IP-ADDRESS*	Global	Resets the sessions of BGP neighboring router with specified IP address.

i See Section 10.1.5.1 when you configure the detail parameters.

To reset the sessions of BGP neighboring router with specified IP address and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp *A.B.C.D* **in** [**prefix-filter**]	Global	Resets the session of BGP neighboring router contained specified IP address. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. A.B.C.D: route IP address
clear ip bgp *A.B.C.D* **ipv4** {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp *A.B.C.D* **out**		Resets the session of BGP neighboring router with specified IP address. A.B.C.D: route IP address out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp *A.B.C.D* **ipv4** {**unicast** | **multicast**} **out**		
clear ip bgp *A.B.C.D* **soft** [**in** | **out**]		Updates the route information only while the session is possible of BGP neighboring router with specified IP address. Apply the route either incoming or outgoing routes. A.B.C.D: route IP address
clear ip bgp *A.B.C.D* **ipv4** {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.5.4 Session Reset of External Peer

You can reset the session of BGP router connected to external AS. To reset a BGP connection for all external peers, use the following command.

Command	Mode	Description
clear ip bgp external	Global	Resets the session of all external AS peers.

i See Section 10.1.5.1 when you configure the detail parameters.

To reset the sessions of BGP router connected to external AS and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp external in [**prefix-filter**]	Global	Resets the session of BGP router connected to external AS. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. external: clears all external peers.
clear ip bgp external ipv4 {**unicast** | **multicast**} **in** [**prefix-filter**]		
clear ip bgp external out		Resets the session of BGP router connected to external AS. external: clears all external peers. out: clears outgoing advertised routes. unicast | multicast : address family modifier
clear ip bgp external ipv4 {**unicast** | **multicast**} **out**		
clear ip bgp external soft [**in** | **out**]		Updates the route information only while the session is possible of BGP router connected to external AS. Apply the route either incoming or outgoing routes. external: clears all external peers.
clear ip bgp external ipv4 {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.5.5 Session Reset of Peer Group

To reset the session for all members of a peer group, use the following command.

Command	Mode	Description
clear ip bgp peer-group *GROUP*	Global	To reset the session for all configured routers of specified peer group. GROUP: peer group name

i See Section 10.1.5.1 when you configure the detail parameters.

To reset the sessions of BGP routers which are members of specified peer group and initialize the details of route configurations, use the following command.

Command	Mode	Description
clear ip bgp peer-group *GROUP* **in** [**prefix-filter**]	Global	Resets the session for all members of specified peer group. in: clears incoming advertised routes. prefix-filter: pushes out prefix-list ORF and does inbound soft reconfiguration. GROUP: peer group name
clear ip bgp peer-group *GROUP* **ipv4** {**unicast** | **multicast**} **in** [**prefix-filter**]		

Command	Mode	Description
clear ip bgp peer-group *GROUP* **out**	Global	Resets the session for all members of specified peer group. GROUP: peer group name out: clears outgoing advertised routes. unicast | multicast: address family modifier
clear ip bgp peer-group *GROUP* **ipv4** {**unicast** | **multicast**} **out**		
clear ip bgp peer-group *GROUP* **soft** [**in** | **out**]		Resets the route information only while the session is possible for all members of specified peer group. Apply the route either incoming or outgoing routes. GROUP: peer group name
clear ip bgp peer-group *GROUP* **ipv4** {**unicast** | **multicast**} **soft** [**in** | **out**]		

10.1.6 Displaying and Managing BGP

BGP network information or configurations provided can be used to determine resource utilization and enable BGP troubleshooting functions to solve network problems.

To see the configurations involved in BGP routing protocol, use the following command.

Command	Mode	Description
show ip bgp summary	Enable Global	Shows the summarized network status of BGP neighboring routers.
show ip bgp [**ipv4** {**unicast** | **multicast**}] **summary**		

To show detailed information on BGP neighbor router's session, use the following command.

Command	Mode	Description
show ip bgp neighbors	Enable Global	Shows general information on BGP neighbor connections of all neighboring routers.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors**		
show ip bgp neighbors *NEIGHBOR-IP*		Shows information of a specified neighbor router by its IP address. NEIGHBOR-IP: neighbor router' s IP address
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP*		
show ip bgp neighbors *NEIGHBOR-IP* **advertised-routes**		The **advertised-routes** option displays all the routes the router has advertised to the neighbor.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **advertised-routes**		
show ip bgp neighbors *NEIGHBOR-IP* **received prefix-filter**		Displays all received routes from neighbor router, both accepted and rejected.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **received prefix-filter**		

Command	Mode	Description
show ip bgp neighbors *NEIGHBOR-IP* **received-routes**	Enable Global	The **received-routes** option displays all received routes (both accepted and rejected) from the specified neighbor. To implement this feature, BGP soft reconfiguration is set.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **received-routes**		
show ip bgp neighbors *NEIGHBOR-IP* **routes**		The **routes** option displays the available routes only that are received and accepted.
show ip bgp ipv4 {**unicast** | **multicast**} **neighbors** *NEIGHBOR-IP* **routes**		

10.2 Open Shortest Path First (OSPF)

Open shortest path first (OSPF) is an interior gateway protocol developed by the OSPF working group of Internet Engineering Task Force (IETF). OSPF designed for IP network supports IP subnetting and marks on information from exterior network. Moreover, it supports packet authorization and transmits/receives routing information through IP multicast. It is most convenient to operate OSPF on layered network.

OSPF is the most compatible routing protocol in layer network environment. The first setting in OSPF network is planning network organized with router and configures border router faced with multiple section.

After that, sets up the basic configuration for OSPF router operation and assigns interface to Area. To make compatible OSPF router configuration for user environment, each router configuration must be accorded by verification.

This section provides configurations for OSPF routing protocol. Lists are as follows.

- Enabling OSPF
- ABR Type Configuration
- Compatibility Support
- OSPF Interface
- Non-Broadcast Network
- OSPF Area
- Default Metric
- Graceful Restart Support
- Opaque-LSA Support
- Default Route
- Finding Period
- External Routes to OSPF Network
- OSPF Distance
- Host Route
- Passive Interface
- Blocking Routing Information
- Summary Routing Information
- OSPF Monitoring and Management

Routing functionalities such as RIP, OSPF, BGP and PIM-SM are only available for hiD 6615 S323. (Unavailable for hiD 6615 S223)

10.2.1 Enabling OSPF

To use OSPF routing protocol, it must be activated as other routing protocols. After activation, configures network address and ID which is operated by OSPF.

The following command shows steps of activating OSPF.

Step1

Open *Router Configuration* mode from *Global Configuration* mode.

Command	Mode	Description
router ospf [<1-65535>]	Global	Opens *Router Configuration* mode with enabling OSPF.
no router ospf [<1-65535>]		Disables OSPF routing protocol.

In case that more than 2 OSPF processes are operated, a process number should be assigned. Normally, there is one OSPF which is operating in one router.

If OSPF routing protocol is disabled, all related configuration will be lost.

Step2

Configure a network ID of OSPF. Network ID decides IP v4 address of this network.

Command	Mode	Description
router-id *A.B.C.D*	Router	Assigns a router ID with enabling OSPF.
no router-id *A.B.C.D*		Deletes a configured router ID.

In case if using **router-id** command to apply new router ID on OSPF process, OSPF process must be restarted to apply. Use the **clear ip ospf process** command to restart OSPF process.

If there is changing router ID while OSPF process is operating, configuration must be processed from the first. In this case, the hiD 6615 S323 can change only router ID without changing related configurations.

Command	Mode	Description
ospf router-id *A.B.C.D*	Router	Changes only a router ID without changing related configurations.
no ospf router-id *A.B.C.D*		Deletes a changed router ID.

To transfer above configuration to other routers, Use the **clear ip ospf process** command to restart OSPF process.

To display configured **router-id**, use the following command.

Command	Mode	Description
show router-id	Enable Global Bridge	Displays configured router ID

Step 3

Use the **network** command to specify a network to operate with OSPF.

There are two ways to show network information configurations. Firstly, shows IP address with bitmask like “10.0.0.0/8”. Secondly, shows IP address with wildcard bit information like “10.0.0.0 0.0.0.255”. The variable option after **area** must be IP address or OSPF area ID.

To configure a network, use the following command.

Command	Mode	Description
network *A.B.C.D/M* **area** {<0-4294967295> | *A.B.C.D*}	Router	Specifies a network with OSPF area ID. 0-4294967295: OSPF area ID
network *A.B.C.D A.B.C.D* **area** {<0-4294967295> | *A.B.C.D*}		

10.2.2 ABR Type Configuration

The hiD 6615 S323 supports 4 types of OSPF ABR which are Cisco type ABR (RFC 3509), IBM type ABR (RFC 3509), IETF Draft type and RFC 2328 type.

To configure ABR type of OSPF, use the following command.

Command	Mode	Description
ospf abr-type {**cisco** | **ibm** | **shortcut** | **standard**}	Router	Selects an ABR type. cisco: cisco type ABR, RFC 3509 (default) ibm: IBM type ABR, RFC 3509 shortcut: IETF draft type standard: RFC 2328 type
no ospf abr-type {**cisco** | **ibm** | **shortcut** | **standard**}		Deletes a configured ABR type.

10.2.3 Compatibility Support

OSPF protocol in the hiD 6615 S323 uses RFC 2328 which is finding shorten path. However, Compatibility configuration enables the switch to be compatible with a variety of RFCs that deal with OSPF. Perform the following task to support many different features within the OSPF protocol.

Use the following command to configure compatibility with RFC 1583.

Command	Mode	Description
compatible rfc1583	Router	Supports compatibility with RFC 1583.
no compatible rfc1583		Disables configured compatibility.

10.2.4 OSPF Interface

OSPF configuration can be changed. Users are not required to alter all of these parameters, but some interface parameters must be consistent across all routers in an attached network.

10.2.4.1 Authentication Type

Authentication encodes communications among the routers. This function is for security of information in OSPF router.

To configure authentication of OSPF router for security, use the following command.

Command	Mode	Description
ip ospf authentication [**message-digest** | **null**]	Interface	Enables authentication on OSPF interface. message-digest: MD5 encoding null: no encoding A.B.C.D: IP address for authentication
ip ospf *A.B.C.D* **authentication** [**message-digest** | **null**]		

If there is no choice of authentication type, the code communication will be based on text.

To delete comfigured authentication, use the following command.

Command	Mode	Description
no ip ospf authentication [**message-digest** | **null**]	Interface	Deletes configured authentication.
no ip ospf *A.B.C.D* **authentication** [**message-digest** | **null**]		

10.2.4.2 Authentication Key

If authentication enables on OSPF router interface, the password is needed for authentication. The authentication key works as a password. The authentication key must be consistent across all routers in an attached network.

There are two ways of authentication by user selection, one is type based on text, and another is MD5 type.

The authentication key must be consistent across all routers in an attached network.

To configure an authentication key which is based on text encoding, use the following command.

Command	Mode	Description
ip ospf authentication-key *KEY*	Interface	Configures the authentication which is based on text encoding. KEY: maximum 16 alphanumeric characters
ip ospf authentication-key *KEY* {**first** | **second**} [**active**]		
ip ospf *A.B.C.D* **authentication-key** *KEY*		
ip ospf *A.B.C.D* **authentication-key** *LINE*		
ip ospf *A.B.C.D* **authentication-key** *KEY* {**first** | **second**} [**active**]		

To configure an authentication key which is based on MD5 encoding, use the following command.

Command	Mode	Description
ip ospf message-digest-key <1-255> **md5** *KEY* [**active**]	Interface	Configures the authentication which is based on md5 type. 1-255: key ID KEY: maximum 16 alphanumeric characters
ip ospf message-digest-key <1-255> **md5** [**active**]		
ip ospf *A.B.C.D* **message-digest-key** <1-255> **md5** [**active**]		
ip ospf *A.B.C.D* **message-digest-key** <1-255> **md5** *LINE* [**active**]		
ip ospf *A.B.C.D* **message-digest-key** <1-255> **md5** *KEY* [**active**]		

To delete a configured authentication key, use the following command.

Command	Mode	Description
no ip ospf authentication-key *KEY*	Interface	Deletes a configured authentication key.
no ip ospf authentication-key *KEY* {**first** | **second**}		
no ip ospf *A.B.C.D* **authentication-key** *KEY*		
no ip ospf *A.B.C.D* **authentication-key** *KEY* {**first** | **second**}		
no ip ospf message-digest-key <1-255>		
no ip ospf *A.B.C.D* **message-digest-key** <1-255>		

10.2.4.3 Interface Cost

OSPF protocol assigns suitable cost according to the bandwidth on the each interface to find the shortest route. Cost is used for packet routing, and routers are using the Cost to communicate.

To configure an interface cost for OSPF, use the following command.

Command	Mode	Description
ip ospf cost <1-65535>	Interface	Configures an interface cost for OSPF.
ip ospf *A.B.C.D* **cost** <1-65535>		

To delete a configured interface cost for OSPF, use the following command.

Command	Mode	Description
no ip ospf cost	Interface	Deletes a configured an interface cost for OSPF.
no ip ospf *A.B.C.D* **cost**		

10.2.4.4 Blocking Transmission of Route Information Database

OSPF routing communicates through the LAS. Each routing information is saved internal router as a datebase, but user can configure the specific interface to block the transmission of routing information saved in database to other router.

To block the transmission of routing information to other router, use the following command.

Command	Mode	Description
ip ospf database-filter all out	Interface	Blocks the transmission of routing information to other router.
ip ospf *A.B.C.D* **database-filter all out**		

To release a blocked interface, use the following command.

Command	Mode	Description
no ip ospf database-filter	Interface	Releases a blocked interface.
no ip ospf *A.B.C.D* **database-filter**		

10.2.4.5 Routing Protocol Interval

Routers on OSPF network exchange various packets, about that packet transmission, time interval can be configured in several ways

The following lists are sort of time interval which can be configured by user:

- **Hello Interval**
  OSPF router sends Hello packet to notify existence of itself. Hello interval is that packet transmission interval.
- **Retransmit Interval**
  When router transmits LSA, it is waiting for approval information come from receiver. In this time, if there is no answer from receiver for configured time, the router transmits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission.
- **Dead Interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit Delay**
  When a router transmits LSA, the traffic can be delayed by status of communications.

Transmit delay is considering of the configuration for LSA transmission time.

i The interval explained as above must be consistent across all routers in an attached network.

To configure a Hello interval, use the following command.

Command	Mode	Description
ip ospf hello-interval <1-65535>	Interface	Configures a Hello interval in the unit of second. 1-65535: interval value (default: 10)
ip ospf *A.B.C.D* **hello-interval** <1-65535>		
no ip ospf hello-interval		Sets a Hello interval to the default value.
no ip ospf *A.B.C.D* **hello-interval**		

To configure a retransmit interval, use the following command.

Command	Mode	Description
ip ospf retransmit-interval <1-65535>	Interface	Configures a retransmit interval in the unit of second. 1-65535: interval value (default: 5)
ip ospf *A.B.C.D* **retransmit-interval** <1-65535>		
no ip ospf retransmit-interval		Sets a retransmit interval to the default value.
no ip ospf *A.B.C.D* **retransmit-interval**		

To configure a dead interval, use the following command.

Command	Mode	Description
ip ospf dead-interval <1-65535>	Interface	Configures a dead interval in the unit of second. 1-65535: interval value (default: 40)
ip ospf *A.B.C.D* **dead-interval** <1-65535>		
no ip ospf dead-interval		Sets a dead interval to the default value.
no ip ospf *A.B.C.D* **dead-interval**		

To configure a transmit delay, use the following command.

Command	Mode	Description
ip ospf transmit-delay <1-65535>	Interface	Configures a transmit delay in the unit of second. 1-65535: interval value (default: 1)
ip ospf *A.B.C.D* **transmit-delay** <1-65535>		
no ip ospf transmit-delay		Sets a transmit delay to the default value.
no ip ospf *A.B.C.D* **transmit-delay**		

10.2.4.6 OSPF Maximum Transmission Unit (MTU)

Router verifies MTU when DD (Database Description) is exchanging among the routers on OSPF networks. Basically, OSPF network can not be organized if there are different sizes of MTUs between routers. Therefore MTU value must be consistent. Generally MTU value is 1500 bytes on Ethernet interface.

To configure MTU on OSPF interface, use the following command.

Command	Mode	Description
ip ospf mtu <576-65535>	Interface	Configures an MTU on OSPF interface.
no ip ospf mtu		Deletes a configured MTU on OSPF interface.

i Configuration as above makes MTU consistently on same OSPF network; actual MTU value on interface itself will not be changed.

On the other hands, if there are two routers which have different MTU, it can be participated with OSPF network through the configuration that skips the verification of MTU value when there is DD exchanging.

To configure the switch to skip the MTU verification in DD process, use the following command.

Command	Mode	Description
ip ospf mtu-ignore	Interface	Configures the switch to skip the MTU verification in DD process.
ip ospf *A.B.C.D* **mtu-ignore**		

To configure the switch not to skip the MTU verification in DD process, use the following command.

Command	Mode	Description
no ip ospf mtu-ignore	Interface	Configures the switch not to skip the MTU verification in DD process.
no ip ospf *A.B.C.D* **mtu-ignore**		

10.2.4.7 OSPF Priority

Routers have each role to exchange the information on OSPF network. DR (Designated Router) is one of essential role to get and transmit the route information in the same area.

The router having the highest priority becomes DR (Designated Router). If there are routers which have same priority, the highest router ID will be DR.

Normally, router has priority 1, but it can be changed to make DR through the configuration of priority.

To configure a priority of OSPF router, use the following command.

Command	Mode	Description
ip ospf priority <0-255>	Interface	Configures a priority of OSPF router.
ip ospf *A.B.C.D* **priority** <0-255>		

To delete a configured priority of OSPF router, use the following command.

Command	Mode	Description
no ip ospf priority	Interface	Deletes a configured priority of OSPF router.
no ip ospf *A.B.C.D* **priority**		

10.2.4.8 OSPF Network Type

There are 4 types of OSPF network. Broadcast network, NBMA (Non-broadcast-multiple-access) network, Point-to-multipoint network and Point-to-point network.

User can configure OSPF network as a Broadcast network or Non-broadcast network type. For example, if the network does not support multicasing it can be configured Non-broadcast type from Broadcast type, and NBMA network as a Frame relay can be broadcast network type.

NBMA type network need virtual circuit to connect routers. But Point-to-multipoint type uses virtual circuit on part of network to save the management expenses. It does not to need to configure Neighbor router to connect routers which are not directly connected. It also saves IP resources and no need to configure the process for destination router. It supports those benefits for stable network services.

Generally, the routers and Layer 3 switches are using Broadcast type network.

To select an OSPF network type, use the following command.

Command	Mode	Description
ip ospf network {**broadcast** | **non-broadcast** | **point-to-multi-point** | **point-to-point**}	Interface	Selects an OSPF network type.

10.2.5 Non-Broadcast Network

To operate NBMA type network, neighbor router configuration is needed. And IP address, Priority, Poll-interval configuration as well. Priority is information for designate router selection and it configured [0] as a default. Poll-interval is the waiting time to re-get the hello packet from dead Neighbor router. It configured 120 seconds as a default.

To configure a router communicated by non-broadcast type, use the following command.

Command	Mode	Description
neighbor *A.B.C.D* **cost** <1-65535>	Router	Configures a neighbor router of NBMA type.
neighbor *A.B.C.D* **priority** <0-255>		
neighbor *A.B.C.D* **priority** <0-255> **poll-interval** <1-65535>		
neighbor *A.B.C.D* **poll-interval** <1-65535>		
neighbor *A.B.C.D* **poll-interval** <1-65535> **priority** <0-255>		

To delete a configured router communicated by non-broadcast type, use the following command.

Command	Mode	Description
no neighbor *A.B.C.D* **cost** [<1-65535>]	Router	Deletes a configured neighbor router of NBMA type.
no neighbor *A.B.C.D* **priority** [<0-255>]		
no neighbor *A.B.C.D* **priority poll-interval** [<1-65535>]		
no neighbor *A.B.C.D* **poll-interval** [<1-65535>]		
no neighbor *A.B.C.D* **poll-interval priority** [<0-255>]		

10.2.6 OSPF Area

Router configuration on OSPF network includes Area configuration with each interface, network. Area has various and special features. It needs to be configured pertinently to make effective management on whole of OSPF network.

OSPF network defines several router types to manage the Area. ABR (Area Border Router) is one of the router types to transmit information between Areas.

ASBR (Autonomous System Border Router) is using OSPF on oneside and using other routing protocol except for OSPF on other interface or Area. ASBR exchanges area information between different routing protocols.

Area types are various. The most principle Area types are Stub Area and NSSA (Not So Stubby Area).

10.2.6.1 Area Authentication

OSPF routers in specific Area can configure authentication for security of routing information. Encoding uses password based on text or MD5. To set password on interface assigned Area, use the **ip ospf authentication-key** and **ip ospf message-digest-key** commands in interface mode, see Section 10.2.4.1 for more information.

To configure authentication information for encoding, use the following command.

Command	Mode	Description
area <0-4294967295> **authentication**	Router	Configures authentication information which is based on text encoding in the Area.
area <0-4294967295> **authentication message-digest**		Configures authentication information which is based on MD5 encoding in the Area.

To delete configured authentication information for encoding, use the following command.

Command	Mode	Description
no area <0-4294967295> **authentication**	Router	Deletes configured authentication information.

10.2.6.2 Default Cost of Area

The default cost of Area is configured only in ABR. ABR function is for delivering the summary default route to stub area or NSSA, in that cases the default cost of area must be required. However, ABR which does not have stub area or NSSA can not use the following command.

To configure a default cost of Area, use the following command.

Command	Mode	Description
area <0-4294967295> **default-cost** <1-16777215>	Router	Configures a default cost of Area.

To delete a configured default cost of Area, use the following command.

Command	Mode	Description
area <0-4294967295> **default-cost** <1-16777215>	Router	Deletes a configured default cost of Area.

This command is only for ABR which is delivering summary default route to stub or NSSA.

10.2.6.3 Blocking the Transmission of Routing Information Between Area

ABR transmits routing information between Areas. In case of not to transmit router information to other area, the hiD 6615 S323 can configure it as a blocking.

First of all, use the **access-list** or **prefix-list** command to assign LIST-NAME. And use the following command to block the routing information on LIST-NAME. This configuration only available in case of OSPF router is ABR.

To block routing information on LIST-NAME, use the following command.

Command	Mode	Description
area <0-4294967295> **filter-list access** *LIST-NAME* {**in** | **out**}	Router	Blocks routing information on LIST-NAME.
area <0-4294967295> **filter-list prefix** *LIST-NAME* {**in** | **out**}		

To delete configured blocking information, use the following command.

Command	Mode	Description
no area <0-4294967295> **filter-list access** *LIST-NAME* {**in** | **out**}	Router	Deletes configured blocking information.
no area <0-4294967295> **filter-list prefix** *LIST-NAME* {**in** | **out**}		

This command is only available for ABR.

10.2.6.4 Not So Stubby Area (NSSA)

NSSA (Not So Stubby Area) is stub Area which can transmit the routing information to Area by ASBR. On the other hand, Stub Area cannot transmit the routing information to area. To configure NSSA, use the following command.

Command	Mode	Description
area <0-4294967295> **nssa**	Router	Configures NSSA.

The following options are configurable for NSSA:

- **default-information-originate**
  This option is configuration for allowing default path of Type-7 in NSSA. It means routing path without routing information will use the interface which is allowed in default type-7 path. **metric** is for metric value, **metric-type** is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.
- **no-redistribution**
  This option is configuration in NSSA for restriction to retransmit the routing information which is from outside.
- **no-summary**
  This option is for restriction to exchange routing information between OSPF areas.
- **translator-role**
  NSSA-LSA (Link State Advertisement) has three types according to the way of process type. **always** changes all NSSA-LSA into Type-5 LSA. **candidate** changes NSSA-LSA into Type-5 LSA when it is translator. **never** does not change NSSA-LSA.

NSSA uses ASBR when it transmits Stub Area or other routing protocol Area into OSPF. In this case, if other routing protocol has default path, use **default-information-originate** command to configure the all of default path is using the assigned ASBR

To configure **NSSA** with various features, use command with options. **area** <0-4294967295> **NSSA** command has 4 options as **default-information-originate**, **no-redistribution**, **no-summary**, **translator-role** and it can be selected more than 2 options without order. **default-information-originate** has **metric** <0-16777214> and **metric-type** <1-2> as an option, **translator-role** must choose one of **candidate**, **never**, **always as an options**.

The following is explaining options of command:

- **default-information-originate** or
  default-information-originate metric <0-16777214> or
  default-information-originate metric-type <1-2>
- **no-redistribution**
- **no-summary**
- **translator-role** {**candidate** | **never** | **always**}

To configure NSSA with one option, use the following command.

Command	Mode	Description
area <0-4294967295> **nssa default-information-originate**	Router	Configures NSSA with one option.
area <0-4294967295> **nssa default-information-originate metric** <0-16777214>		
area <0-4294967295> **nssa default-information-originate metric-type** <1-2>		
area <0-4294967295> **nssa no-redistribution**		
area <0-4294967295> **nssa no-summary**		
Command	**Mode**	**Description**
area <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**}	Router	Configures NSSA with one option.

The following example shows how to configure NAAS with more than 2 options:

- **area** <0-4294967295> **nssa no-summary no-redistribution**
- **area** <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**} **default-information-originate metric-type** <1-2> **no-redistribution**

To delete configured NSSA, use the following command.

Command	Mode	Description
no area <0-4294967295> **nssa**	Router	Deletes configured NSSA.
no area <0-4294967295> **nssa default-information-originate**		
no area <0-4294967295> **nssa default-information-originate metric** <0-16777214>		
no area <0-4294967295> **nssa default-information-originate metric-type** <1-2>		
no area <0-4294967295> **nssa no-redistribution**		
no area <0-4294967295> **nssa no-summary**		
no area <0-4294967295> **nssa translator-role** {**candidate** | **never** | **always**}		

10.2.6.5 Area Range

In case of OSPF belongs to several Areas, Area routing information can be shown in one routing path. Like as above, various routing information of Area can be combined and summarized to transmit to outside.

To summarize and combine the routing information, use the following command.

Command	Mode	Description
area <0-4294967295> **range** *A.B.C.D/M*	Router	Configures to use summarized information for assigned path.
area <0-4294967295> **range** *A.B.C.D/M* {**advertise** | **not-advertise**}		

Use **advertise** option to transmit summarized routing information with using summarized information. And use the **not-advertise** option to block the transmission of summarized routing information to outside.

To release the configuration, use the following command.

Command	Mode	Description
no area <0-4294967295> **range** *A.B.C.D/M*	Router	Releases the configuration to use summarized information for assigned path
no area <0-4294967295> **range** *A.B.C.D/M* {**advertise** | **not-advertise**}		

10.2.6.6 Shortcut Area

Backbone Area is the default Area among the Areas of OSPF. All traffic should pass the Backbone Area and OSPF network must be planned for that, but there is some efficiency way which is not to pass the Backbone Area. That is Shortcut, and it must be configured for efficient traffic in every ABR type, see Section 10.2.2.

To configure the shortcut option, use the following command.

Command	Mode	Description
area <0-4294967295> **shortcut** {**default** | **disable** | **enable**}	Router	Configures the shortcut option.

To releases the configured shortcut option, use the following command.

Command	Mode	Description
no area <0-4294967295> **shortcut** {**default** | **disable** | **enable**}	Router	Releases the configured shortcut option.

10.2.6.7 Stub Area

Stub Area is that ABR is connected to Backbone Area. If it is assigned as Stub Area, ABR will notify the default path to Stub Area and other routing protocol information will not transmit to Stub Area.

To create Stub Area, use the following command.

Command	Mode	Description
area <0-4294967295> **stub** [**no-summary**]	Router	Creates a Stub Area.

If **no-summary** option adds to Stub Area, other Area OSPF routing information also can not come to Stub Area, However, it only goes to default route from ABR router. That is Totally Stubby Area.

To delete a created Stub Area, use the following command.

Command	Mode	Description
no area <0-4294967295> **stub** [**no-summary**]	Router	Deletes a created Stub Area.

10.2.6.8 Virtual Link

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully portioned, you can establish a virtual link. The virtual link must be configured in both routers.

OSPF network regards virtual link routers as Point-to-point router. Therefore, the Hello-interval, Retransmit-interval, Transmit-delay must be consistent across all routers in an attached network.

User can configure Authentication for security, Authentication key for password, and time period for Hello-interval, Retransmit-interval, Transmit-delay and Dead-interval to operate virtual link.

The following items describe 7 configurations for virtual link:

- **Authentication**
  This is configuration for security of routing information. **message-digest** uses MD5 to encode for authentication, **null** means not using any of authentication.
- **Authentication-key**
  Configures the authentication which is based on text encoding.
- **Message-digest-key**
  Configures the authentication which is based on md5 type.
- **Hello-interval**
  OSPF router sends Hello packet to notify existence of itself. Hello-interval is that packet transmission interval.
- **Retransmit-interval**
  When router transmits LSA, it is waiting for approval information come from receiver.

In this time, if there is no answer from receiver for configured time, the router transmits LSA again. Retransmit-interval is configuration of the time interval between transmission and retransmission

- **Dead-interval**
  If there is no hello packet for the configured time. The router perceives other router is stopped working. Dead-interval is configuration of the time interval which perceives other router is stopped operating.
- **Transmit-delay**
  When a router transmits LSA, the traffic can be delayed by status of communications. Transmit-delay is considering of the configuration for LSA transmission time.

Configuration for virtual link can be selected more than 2 options without order. The following is explaining options of command:

- **authentication** [**message-digest** | **null**]
- **authentication-key** *KEY*
- **message-digest-key** *KEY* **md5** *KEY*
- **hello-interval** <1-65535>
- **retransmit-interval** <1-65535>
- **dead-interval** <1-65535>
- **transmit-delay** <1-65535>

To configure a virtual link with one option, use the following command.

Command	Mode	Description
area <0-4294967295> **virtual-link** *A.B.C.D* **authentication** [**message-digest** | **null**]	Router	Configures a virtual link.
area <0-4294967295> **virtual-link** *A.B.C.D* **authentication-key** *KEY*		
area <0-4294967295> **virtual-link** *A.B.C.D* **message-digest-key** *KEY* **md5** *KEY*		
area <0-4294967295> **virtual-link** *A.B.C.D* **hello-interval** <1-65535>		
area <0-4294967295> **virtual-link** *A.B.C.D* **retransmit-interval** <1-65535>		
area <0-4294967295> **virtual-link** *A.B.C.D* **dead-interval** <1-65535>		
area <0-4294967295> **virtual-link** *A.B.C.D* **transmit-delay** <1-65535>		

The following example shows how to configure virtual link with more than 2 options:

- **area** <0-4294967295> **virtual-link** *A.B.C.D* **authentication-key** *KEY* **authentication** [**message-digest** | **null**]
- **area** <0-4294967295> **virtual-link** *A.B.C.D* **hello-interval** <1-65,535> **dead-interval** <1-65535>

To delete a configured virtual link, use the following command.

Command	Mode	Description
no area <0-4294967295> **virtual-link** *A.B.C.D* **authentication** [**message-digest** | **null**]	Router	Deletes a configured virtual link.
no area <0-4294967295> **virtual-link** *A.B.C.D* **authentication-key** *KEY*		
no area <0-4294967295> **virtual-link** *A.B.C.D* **message-digest-key** *KEY* **md5** *KEY*		
no area <0-4294967295> **virtual-link** *A.B.C.D* **hello-interval** <1-65535>		
no area <0-4294967295> **virtual-link** *A.B.C.D* **retransmit-interval** <1-65535>		
no area <0-4294967295> **virtual-link** *A.B.C.D* **dead-interval** <1-65535>		
no area <0-4294967295> **virtual-link** *A.B.C.D* **transmit-delay** <1-65535>		

10.2.7 Default Metric

OSPF finds metric based on interface bandwidth. For example, default metric of T1 link is 64, but default metric of 64K line is 1562. If there are plural lines in the bandwidth, you can view costs to use line by assigning metric to each line.

To classify costs to use line, use the following command.

Command	Mode	Description
auto-cost reference-bandwidth <1-4294967>	Router	Configures default metric in the unit of Mbps. (default: 100)

To delete the configuration, use the following command.

Command	Mode	Description
no auto-cost reference-bandwidth	Router	Deletes the configuration.

10.2.8 Graceful Restart Support

You need to restart OSPF protocol processor when there is network problem. In this case, it takes long time to restarts OSPF and there is no packet transmission. Other routers are also need to delete routing information and register it again. Graceful Restart improves those inconveniences. Although OSPF is restarting, Graceful Restart makes the transmission of a packet with routing information.

To configure the Graceful Restart, use the following command.

Command	Mode	Description
capability restart {**graceful** | **reliable-graceful** | **signaling**}	Router	Configures the Graceful Restart.
no capability restart		Releases the configuration.

The following items are additional options for the Graceful Restart:

- **grace-period**
  When OSPF restarts, process is keeping status in graceful for the time configured as **grace-period**. After the configured time, OSPF operates in normal.
- **helper**
  This is functions that helps other routers around the restarting router. It makes re starting router as a working and transmitting to other routers. **only-reload** is for the case of OSPF router is restarting, **only-upgrade** is for the OSPF router which is up-grading software, and **max-grace-period** works when **grace-period** from other routers has less value than it. Configuration for Helper can be selected more than 2 options without order.

To configure the additional options for Graceful Restart, use the following command.

Command	Mode	Description
ospf restart grace-period <1-1800>	Global	Configures the additional options for Graceful Restart.
ospf restart helper max-grace-period <1-1800>		
ospf restart helper max-grace-period <1-1800> **only-reload** [**only-upgrade**]		
ospf restart helper max-grace-period <1-1800> **only-upgrade** [**only-reload**]		
ospf restart helper only-reload [**only-upgrade**]		
ospf restart helper only-reload only-upgrade max-grace-period <1-1800>		
ospf restart helper only-reload max-grace-period <1-1800> [**only-upgrade**]		
ospf restart helper only-upgrade [**only-reload**]		
ospf restart helper only-upgrade only-reload max-grace-period <1-1800>		
ospf restart helper only-upgrade max-grace-period <1-1800> [**only-reload**]		

To release the configuration, use the following command.

Command	Mode	Description
no ospf restart grace-period <1-1800>	Global	Releases the configuration.
ospf restart helper never		
no ospf restart helper max-grace-period <1-1800>		

10.2.9 Opaque-LSA Support

Opaque-LSA is LSA Type-9, Type-10, Type-11. The hiD 6615 S323 enables Opaque-LSA as a default but it can be released by user.

To release the enabled Opaque-LSA management, use the following command.

Command	Mode	Description
no capability opaque	Router	Releases the enabled Opaque-LSA management.

To enable Opaque-LSA management, use the following command.

Command	Mode	Description
capability opaque	Router	Enables Opaque-LSA management.

10.2.10 Default Route

You can configure ASBR (Autonomous System Boundary Router) to transmit default route to OSPF network. Autonomous System Boundary router transmits route created externally to OSPF network. However, it does not create system default route.

To have autonomous System Boundary router create system default route, use the following command.

Command	Mode	Description
default-information originate	Router	Configures the default route.

The following items are detail options for the Default Route configuration.

- **metric**
  Configures Metric value of the default route.
- **metric-type**
  metric-type is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, **metric type 2** always uses external cost value only.
- **always**
  Transmits the default route to outside.
- **no-summary**
  Restricts to exchange routing information between OSPF area in NSSA.

- **route-map**
  Transmits specific routing information to assigned route which has MAP-NAME.

The detail options for default route configuration are classified in 4 as above, and those configurations can be selected more than 2 options without order.

The following is explaining options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **always**
- **route-map** *MAP-NAME*

To configure the default route with an option, use the following command.

Command	Mode	Description
default-information originate metric <0-16777214>	Router	Configures the default route with one option.
default-information originate metric-type <1-2>		
default-information originate always		
default-information originate route-map *MAP-NAME*		

The following example shows how to configure default route with more than 2 options:

- **default-information originate metric-type** <1-2> **always**
- **default-information originate route-map** *MAP-NAME* **metric** <0-16777214>

To delete the configuration, use the following command.

Command	Mode	Description
no default-information originate	Router	Deletes the configuration.
no default-information originate metric <0-16777214>		
no default-information originate metric-type <1-2>		
no default-information originate always		
no default-information originate route-map *MAP-NAME*		

10.2.11 Finding Period

OSFP start to find the shortest path as soon as got a notification of changing the network component. You can configure the period to find the path.

To configure the period of finding, use the following command.

Command	Mode	Description
timers spf *SPF-DELAY SPF-HOLD*	Router	Configures the period of finding in the unit of second. SPF-DELAY: 0-2147483647 (default: 5) SPF-HOLD: 0-2147483647 (default: 10)

To release the configuration, use the following command.

Command	Mode	Description
no timers spf	Router	Release the configuration.

10.2.12 External Routes to OSPF Network

If other routing protocol redistribute into OSPF network, these routes become OSPF external routes. Other routing protocols are RIP and BGP. And static route, connected route, kernel route are also external route. Those routing information can distribute into OSPF network.

There are 4 kinds of additional configuration about external routes to OSPF network. **metric** is configures Metric value of the default route, **metric-type** is for type of finding the path. **metric-type 1** uses internal path cost with external path cost as a cost, metric type 2 always uses external cost value. **route-map** is transmission of specific routing information to assigned route which has MAP-NAME, and, **tag** is using the assign tag number on the specific MAP-NAME.

Those 4 kinds of additional configuration can be selected more than 2 options without order, and it applies to consistent across all external routes in an attached network.

The following is explaining 4 options of command:

- **metric** <0-16777214>
- **metric-type** <1-2>
- **route-map** *MAP-NAME*
- **tag** <0-4294967295>

To configure the external route transmission, use the following command.

Command	Mode	Description
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric** <0-16777214>	Router	Configures the external route transmission.
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric-type** <1-2>		
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **route-map** *MAP-NAME*		
redistribute {**bgp** | **connected** | **kernel** | **rip** | **static**} **tag** <0-4294967295>		

The following example shows how to configure it with more than 2 options:

- **redistribute** {**bgp** | **connected** | **kernel** | **rip** | **static**} **metric** <0-16777214> **tag** <0-4294967295>
- **redistribute** {**bgp** | **connected** | **kernel** | **rip** | **static**} **tag** <0-4294967295> **metric-type** <1-2>

For efficient transmission of routing information, and to avoid non-matching between metric and OSPF routing protocol, use the **default matric** command to assign metric about redistribute route.

To configure the default metric, use the following command.

Command	Mode	Description
default-metric <0-16777214>	Router	Configures the default metric.

To delete the default metric, use the following command.

Command	Mode	Description
no default-metric [<0-16777214>]	Router	Deletes the default metric.

10.2.13 OSPF Distance

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer between 0 and 255. In general, the higher the value is, the lower the trust rating is. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

OSPF uses three different administrative distances: intra-area, inter-area, and external. Routes learned through other domain are external, routes to another area in OSPF domain are inter-area, and routes inside an area are intra-area. The default distance for each type of route is 110. In order to change any of the OSPF distance values, use the following commands.

The following is explaining 3 options of command.

- **external** <1-255>
- **inter-area** <1-255>
- **intra-area** <1-255>

To configure the distance with 1 option, use the following command.

Command	Mode	Description
distance ospf external <1-255>	Router	Configures the distance of OSPF route. (default: 110)
distance ospf inter-area <1-255>		
distance ospf intra-area <1-255>		

The following example shows how to configure the distance with more than 2 options:

- **distance ospf external** <1-255> **inter-area** <1-255>
- **distance ospf inter-area** <1-255> **intra-area** <1-255>

To make it as a default, use the following command.

Command	Mode	Description
no distance ospf	Router	Restores it as the default.

10.2.14 Host Route

OSPF regards routing information of specific host as stub link information. Routing information can be assigned to each host which is connected with one router.

To configure the routing information to each host, use the following command.

Command	Mode	Description
host *A.B.C.D* **area** *A.B.C.D*	Router	Configures the routing information to each host.
host *A.B.C.D* **area** *A.B.C.D* **cost** <0-65535>		

Command	Mode	Description
host *A.B.C.D* **area** <1-4294967295>	Router	Configures the routing information to each host.
host *A.B.C.D* **area** <1-4294967295> **cost** <0-65535>		

10.2.15 Passive Interface

The passive interface which is configured by OSPF network operate as stub area. Therefore passive interface can not exchange the OSPF routing information.

To configure the passive interface, use the following command.

Command	Mode	Description
passive-interface *INTERFACE* [*A.B.C.D*]	Router	Configures the passive interface.

To release the configured as passive interface, use the following command.

Command	Mode	Description
no passive-interface *INTERFACE* [*A.B.C.D*]	Router	Releases the configured as passive interface.

10.2.16 Blocking Routing Information

The hiD 6615 S323 can classify and restrict the routing information. To configure this function, sort the specific routing information in **access-list** first, and block the routing information in **access-list.**

To block the routing information in access-list, use the following command.

Command	Mode	Description
distribute-list *ACCESS-LIST* **out** {**bgp** | **connected** | **kernel** | **rip** | **static**}	Router	Blocks the routing information in access-list

To release the configuration, use the following command.

Command	Mode	Description
distribute-list *ACCESS-LIST* **out** {**bgp** | **connected** | **kernel** | **rip** | **static**}	Router	Releases the configuration.

10.2.17 Summary Routing Information

In case of external routing protocol transmits to OSPF network, more than 2 routing information can be summarized as one. For example, 192.168.1.0/24 and 192.168.2.0/24 can become 192.168.0.0/16 to transmit to OSPF network. This summary reduces the number of routing information and it improves a stability of OSPF protocol

And you can use **no-advertise** option command to block the transmission of summarized routing information to outside. Or assign the specific **tag** number to configure.

To configure the summary routing information, use the following command.

Command	Mode	Description
summary-address *A.B.C.D/M*	Router	Configures the summary routing information.
summary-address *A.B.C.D/M* **not-advertise**		Blocks the transmission of summarized routing information to outside
no summary-address *A.B.C.D/M* **tag** <0-4294967295>		Configures the summary routing information with a specific tag

10.2.18 OSPF Monitoring and Management

You can view all kinds of statistics and database recorded in IP routing table. These information can be used to enhance system utility and solve problem in case of trouble. You can check network connection and data routes through the transmission.

10.2.18.1 Displaying OSPF Protocol Information

You can verify several information about OSPF protocol. To display the information about OSPF protocol, use the following command.

Command	Mode	Description
show ip ospf	Enable Global	Shows the information about OSPF protocol.
show ip ospf <0-65535>		Shows the information about a specific process ID in OSPF protocol.

To display OSPF routing table to ABR and ASBR, use the following command.

Command	Mode	Description
show ip ospf border-routers	Enable Global	Shows OSPF routing table to ABR and ASBR.

To display the OSPF database, use the following command.

Command	Mode	Description
show ip ospf database {**self-originate** | **max-age**}	Enable Global	Shows the OSPF database.
show ip ospf database adv-router *A.B.C.D*		
show ip ospf database {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**}		
show ip ospf database {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} **self-originate**		
show ip ospf database {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} **adv-router** *A.B.C.D*		
show ip ospf database {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D*		
show ip ospf database {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D* **self-originate**		
show ip ospf database {**asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as**} *A.B.C.D* **adv-router** *A.B.C.D*		

To display the interface information of OSPF, use the following command.

Command	Mode	Description
show ip ospf interface [*INTERFACE*]	Enable Global	Shows the interface information of OSPF.

To display the information of neighbor route, use the following command.

Command	Mode	Description
show ip ospf neighbor	Enable Global	Shows the information of neighbor router.
show ip ospf neighbor *A.B.C.D* [**detail**]		
show ip ospf neighbor interface *A.B.C.D*		
show ip ospf neighbor detail [**all**]		
show ip ospf neighbor all		

To display the routing information which is registered in routing table, use the following command.

Command	Mode	Description
show ip ospf route	Enable Global	Shows the routing information which is registered in routing table.

To display the information of virtual link, use the following command.

Command	Mode	Description
show ip ospf virtual-links	Enable Global	Shows the information of virtual link.

10.2.18.2 Displaying Debugging Information

The hiD 6615 S323 uses debug command to find the reason of problem. Use the following command.

Command	Mode	Description
debug ospf all	Enable	Shows all the debugging information.
debug ospf events [**abr** | **asbr** | **lsa** | **nssa** | **os** | **router** | **vlink**]		Shows information about OSPF operation such as OSPF neighbor router, transmitted information, deciding destination router, calculating the shortest route, and so on.
debug ospf ifsm [**events** | **status** | **timers**]		Shows the debugging information of OSPF interface.
debug ospf lsa [**flooding** | **generate** | **refresh**]		Shows information transmitted by OSPF and calculating the shortest route.
debug ospf nfsm [**events** | **status** | **timers**]		Shows the debugging information of OSPF Neighbor router.
debug ospf nsm [**events** | **status** | **timers**]		Shows the debugging information between OSPF process and NSM (Network Services Module).
debug ospf packet {**hello** | **dd** | **ls-ack** | **ls-request** | **ls-update** | **all**} [**send** | **recv** [**detail**]]		Shows the debugging information of each packet.
debug ospf route [**ase** | **ia** | **install** | **spf**]		Shows the debugging information of OSPF routing.

To display the debugging information, use the following command.

Command	Mode	Description
show debugging ospf	Enable Global	Shows the debugging information of OSPF.

10.2.18.3 Limiting Number of Database

The hiD 6615 S323 can limit the Number of Database to process in OSPF. For example, if a router connected with many of routers, it carries overload to process the database. Therefore, Limiting the Number of Database reduces the overload on system.

To configure the limiting Number of Database, use the following command.

Command	Mode	Description
max-concurrent-dd <1-65535>	Router	Configures the limiting Number of Database.

To delete the configuration, use the following command.

Command	Mode	Description
no max-concurrent-dd <1-65535>	Router	Deletes the configuration.

10.2.18.4 Maximum Process of LSA

The hiD 6615 S323 can configures maximum number of LSA to process. LSA is classified as internal route LSA and external route LSA, maximum number of LSA can configure on each class.

And also, If process of LSA is over the configured number, you can configure it to stop the process or send the caution message. When the outer route of LSA is overflowed the assigned value, you can configure it to restart OSPF after the waiting time. If the waiting time is 0, OSPF keep the process before the administrator reboots the system.

To assign the maximum number of LSA to process in OSPF, use the following command.

Command	Mode	Description
overflow database <1-4294967294> [**hard** | **soft**]	Router	Assigns the number of LSA for internal route.
overflow database external <0-2147483647> <0-65535>		Assigns the number of LSA for external route.

When there is an overflow, **hard** configuration will stop the process, and **soft** configuration will send a caution message.

To release the configuration, use the following command.

Command	Mode	Description
no overflow database	Router	Releases the configuration for OSPF internal route.
no overflow database external [<0-2147483647>]		Releases the configuration for OSPF external route.
no overflow database external <0-2147483647> [<0-65535>]		

10.3 Routing Information Protocol (RIP)

Routing Information Protocol (RIP), as it is more commonly used than any other Routing Protocols, for use in small, homogeneous networks. It is a classical distance-vector routing protocol with using hop count. RIP is formally defined in documents in Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became both more numerous and greater in size, it became apparent to the Internet Engineeing Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388, RFC 1723 and RFC 2453, which described RIP v2 (the second version of RIP).

RIP v2 uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The hiD 6615 S323 sends routing information and updates it every 30 seconds. This process is termed advertised. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the non-updating router as being unusable. If there is still no update after 120 seconds, the router removes all routing table entries for the non-updating router.

The metric that RIP uses to rate the value of different routes is hop count. The hop count is the number of routers that should be traversed through the network to reach the destination. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This short range of metrics makes RIP an unsuitable routing protocol for large networks.

A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors. RIP sends updates to the interfaces in the specified networks.

If an interface's network is not specified, it will not be advertised in any RIP update. The hiD 6615 S323 supports RIP version 1 and 2.

Routing functionalities such as RIP, OSPF, BGP and PIM-SM are only available for hiD 6615 S323. (Unavailable for hiD 6615 S223)

10.3.1 Enabling RIP

To use RIP protocol, you should enable RIP.

Step 1

To open *Router Configuration* mode, use the following command on *Global Configuration* mode.

Command	Mode	Description
router rip	Global	Opens *Router Configuration* mode and operates RIP routing protocol.
no router rip		Restores all configurations involved in RIP to the default.

Step 2

Configure the network to operate as RIP.

Command	Mode	Description
network {*A.B.C.D/M* | *INTERFACE* }	Router	Establishes the network to operate as RIP. A.B.C.D/M: IP prefix (e.g. 35.0.0.0/8) INTERFACE: interface name
no network {*A.B.C.D/M* | *INTERFACE* }		Removes a specified network to operate as RIP.

The command **network** enables RIP interfaces between certain numbers of a special network address. For example, if the network for 10.0.0.0/24 is RIP enabled, this would result in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP.

By the way, it's not possible to exchange the RIP routing information if it hasn't been established RIP network using **network** command even though interface belongs to RIP network. RIP packets with RIP routing information is transmitted to port specified with the **network** command.

After RIP is enabled, you can configure RIP with the following items:

- RIP Neighbor Routers
- RIP Version
- Creating available Static Route only for RIP
- Redistributing Routing Information
- Metrics for Redistributed Routes
- Administrative Distance
- Originating Default Information
- Routing Information Filtering
- Maximum Number of RIP Routes
- RIP Network Timer
- Split Horizon
- Authentication Key
- Restarting RIP
- UDP Buffer Size of RIP
- Monitoring and Managing RIP

10.3.2 RIP Neighbor Router

Since RIP is broadcast protocol, routers should be connected each other to transmit the routing information of RIP to non-broadcast network.

To configure neighbor router to transmit RIP information, use the following command on *Router Configuration* mode.

Command	Mode	Description
neighbor *A.B.C.D*	Router	Configures a neighbor router to exchange routing information. A.B.C.D: neighbor address
no neighbor *A.B.C.D*		Deletes the neighbor router.

i You can block the routing information to specific interface by using the **passive-interface** command.

10.3.3 RIP Version

Basically, the hiD 6615 S323 supports RIP version 1 and 2. However, you can configure to receive either RIP v1 type packets only or RIP v2 type packets only.

To configure RIP version, use the following command.

Command	Mode	Description
version {**1** | **2**}	Router	Selects one type of RIP packets to transmit either RIP v1 or RIP v2 type packet
no version {**1** | **2**}		Restores the default of specified RIP version type

The preceding task controls default RIP version settings. You can override the routers RIP version by configuring a particular interface to behave differently.

To control which RIP version an interface sends, perform one of the following tasks after opening *Interface Configuration* mode.

Command	Mode	Description
ip rip send version 1	Interface	Sends RIP v1 type packet only to this interface.
ip rip send version 2		Sends RIP v2 type packet only to this interface.
ip rip send version 1 2		Sends RIP v1 and RIP v2 type packets both.

To delete the configuration that sends RIP version packet to interface, use the following command.

Command	Mode	Description
no ip rip send version 1	Interface	Deletes the configuration of RIP v1 type packet for helping them to be sent to the interface.
no ip rip send version 2		Deletes the configuration of RIP v2 type packet for helping them to be sent to the interface.
no ip rip send version 1 2		Deletes the configuration of both RIP v1 and v2 type packets for helping them to be sent to the interface.

Similarly, to control how packets received from an interface are processed, perform one of the following tasks.

Command	Mode	Description
ip rip receive version 1	Interface	Receives RIP v1 type packet only from the interface.
ip rip receive version 2		Receives RIP v2 type packet only from the interface.
ip rip receive version 1 2		Receives both RIP v1 and RIP v2 type packets from the interface.

To delete the configuration that receives RIP version packet from the interface, use the following command.

Command	Mode	Description
no ip rip receive version 1	Interface	Deletes the configuration of RIP v1 type packet for helping them be received from the interface.
no ip rip receive version 2		Deletes the configuration of RIP v2 type packet for helping them to be received from interface.
no ip rip receive version 1 2		Deletes the configuration of both RIP v1 and RIP v2 type packets for helping them to be received from the interface.

10.3.4 Creating available Static Route only for RIP

This feature is provided only by Siemens' **route** command creates static route available only for RIP. If you are not familiar with RIP protocol, you would better use **redistribute static** command.

Command	Mode	Description
route *A.B.C.D/M*	Router	Creates suitable static route within RIP environment only. A.B.C.D/M: IP prefix
no route *A.B.C.D/M*		Deletes this static route established by route command.

10.3.5 Redistributing Routing Information

The hiD 6615 S323 can redistribute the routing information from a source route entry into the RIP tables. For example, you can instruct the router to re-advertise connected, kernel, or static routes as well as other routes established by routing protocol. This capability applies to all the IP-based routing protocols.

To redistribute routing information from a source route entry into the RIP table, use the following command.

Command	Mode	Description
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**}	Router	Registers transmitted routing information in another router's RIP table. 1-16: metric value WORD: pointer to route-map entries
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16>		
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **route-map** *WORD*		
redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16> **route-map** *WORD*		

To delete the configuration for redistributing routing information in another router's RIP table, use the following command.

Command	Mode	Description
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**}	Router	Removes the configuration of transmitted routing information in another router's RIP table.
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16>		
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp**} **route-map** *WORD*		
no redistribute {**kernel** | **connected** | **static** | **ospf** | **bgp** } **metric** <0-16> **route-map** *WORD*		

As the needs of the case demand, you may also conditionally restrict the routing information between the two networks using **route-map** command.

To permit or deny the specific information, open the *Route-map Configuration* mode using the following command in *Global Configuration* mode.

Command	Mode	Description
route-map *TAG* {**deny** | **permit**} <1-65535>	Global	Creates the route map. TAG: route map tag 1-65535: sequence number

One or more **match** and **set** commands typically follow **route-map** command. If there are no **match** commands, then everything matches. If there are no set commands, nothing is done. Therefore, you need at least one **match** or **set** command.

Use the following command on *Route-map Configuration* mode to limit the routing information for transmitting to other routers' RIP table.

Command	Mode	Description
match interface *INTERFACE*	Route-map	Transmits the information to specified interface only. INTERFACE: interface name
match ip address {<1-199> | <1300-2699> | N*AME*}		Transmits the information matched with access-list. 1-199: IP access list number 1300-2699: IP access list number (expanded range) NAME: IP access list name
match ip address prefix-list *NAME*		Transmits the information matched with prefix-list. NAME: IP prefix list name
match ip next-hop {<1-199> | <1300-2699> | N*AME*}		Transmits information to only neighbor router in access-list. 1-199: IP access list number 1300-2699: IP access list number (expanded range) NAME: IP access list name
match ip next-hop prefix-list *NAME*		Transmits information to only neighbor router in prefix-list. NAME: IP prefix list name
Command	**Mode**	**Description**
match metric <0-4294967295>	Route-map	Transmits information matched with specified metric, enter the metric value.
set ip next-hop *A.B.C.D*		Configures Neighbor router's address. A.B.C.D: IP address of next hop
set metric <1-2147483647>		Sets the metric value for destination routing protocol. 1-2147483647: metric value

10.3.6 Metrics for Redistributed Routes

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the OSPF metric is a combination of five quantities. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable tampering with dynamic information, carelessly exchanging routing information between different routing protocols can create routing loops, which can seriously degrade network operation. To prevent this situation, we configure metrics

To set metrics for redistributed routes, use the following command.

Command	Mode	Description
default-metric <1-16>	Router	Configures the equal metric of all routes transmitted by routing protocol, enter the value. 1-16: default metric value
no default-metric [<1-16>]		Removes the equal metric of all routes transmitted by routing protocol.

i The metric of all protocol can be configured from 0 to 4294967295. It can be configured from 1 to 16 for RIP.

10.3.7 Administrative Distance

Administrative distance is a measure of the trustworthiness of the source of the routing information.

In large scaled network, Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

Remember that administrative distance has only local significance, and is not advertised in routing updates. Most routing protocols have metric structures and algorithms that are not compatible with other protocols. In a network with multiple routing protocols, the exchange of route information and the capability to select the best path across the multiple protocols are critical. Administrator should set the distance value based on whole routing networks.

To configure the administrative distance value, use the following command.

Command	Mode	Description
distance <1-255> [*A.B.C.D/M* [*ACCESS-LIST*]]	Router	Sets the administrative distance value for routes. 1-255: distance value A.B.C.D/M: IP source prefix ACCESS-LIST: access list name
no distance [<1-255>] [*A.B.C.D/M* [*ACCESS-LIST*]]		Deletes the administrative distance value.

10.3.8 Originating Default Information

You can set an autonomous system boundary router to generate and transmit a default route into an RIP routing domain. If you specifically set to generate a default routes into an RIP network, this router becomes an autonomous system (AS) boundary router. However, an AS boundary router does not generate a default route automatically into the RIP network.

To generate a default route into RIP by the AS boundary router, use the following command on *Router Configuration* mode.

Command	Mode	Description
default-information originate	Router	Generates a default route into RIP by the AS boundary router.
no default-information originate		Disables a default route feature.

10.3.9 Routing Information Filtering

You can limit the routing protocol information by performing the following tasks.

- Block the transmission of routing information to a particular interface. This is to prevent other systems on an interface from learning about routes dynamically.
- Provides a local mechanism for increasing the value of routing metrics.

10.3.9.1 Filtering Access List and Prefix List

The hiD 6615 S323 switch is able to permit and deny conditions that you can use to filter inbound or outbound routes by access-list or prefix-list. Use the **distribute-list** command to apply the access list to routes received from or forwarded to a neighbor.

User should configure the route information for a set of deny conditions based on matching each access list or prefix list. In addition, this configuration is able to be applied on the specific interface as well as the whole routes information of switch.

To block the route information based on matching access list or prefix list, use the following command.

Command	Mode	Description
distribute-list *ACCESS-LIST* {**in** | **out**} [*INTERFACE*]	Router	Apply a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route. INTERFACE: interface name ACCESS-LIST: access list name PREFIX-LIST: prefix list name
distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

To remove the filtering access list or prefix-list to incoming or outgoing RIP route

Command	Mode	Description
no distribute-list *ACCESS-LIST* {**in** | **out**} [*INTERFACE*]	Router	Removes the application of a specific access list or prefix list to incoming or outgoing RIP route updates on interface in order to block the route.
no distribute-list prefix *PREFIX-LIST* {**in** | **out**} [*INTERFACE*]		

10.3.9.2 Disabling the transmission to Interface

To prevent other routers on a local network from learning about routes dynamically, you can keep routing update messages from being sent through a router interface. This feature applies to all IP-based routing protocols except for BGP.

Disable the routing information to transmit on this interface of router, use the following command.

Command	Mode	Description
passive-interface *INTERFACE*	Router	Disables the transmission of multicast RIP messages on the interface. INTERFACE: interface name
no passive-interface *INTERFACE*		Re-enables the transmission of RIP multicast messages on the specified interface.

10.3.9.3 Offset List

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. You can limit the offset list with an access list.

To add the value of routing metrics, use the following command.

Command	Mode	Description
offset-list *ACCESS-LIST* {**in** | **out**} <0-16> [*INTERFACE*]	Router	Add an offset to incoming or outgoing metrics to routes learned via RIP. ACCESS-LIST: access list name 0-16: type number INTERFACE: interface name

Command	Mode	Description
no offset-list *ACCESS-LIST* {**in** | **out**} <0-16> [*INTERFACE*]	Router	Removes an offset list.

10.3.10 Maximum Number of RIP Routes

You can set the maximum number of RIP routes for using on RIP protocol. To set the maximum number of routes, use the following command.

Command	Mode	Description
maximum prefix <1-65535> [1-100]	Router	Sets the maximum number of routes of RIP. 1-65535: maximum number of RIP routes 1-100: percentage of maximum routes to generate a warning (default: 75)
no maximum prefix <1-65535> [1-100]		Removes the maximum number of routes of RIP which are set before.

10.3.11 RIP Network Timer

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better your internet needs. The default settings for the timers are as follows.

- **Update**
  The routing information is updated once every 30 seconds. This is the fundamental timing parameter of the routing protocol. Every update timer seconds, the RIP process is supposed to send the routing table to all neighboring RIP routers.
- **Timeout**
  The default is 180 seconds. It's the interval of time in seconds after which a route is declared invalid. However, this information will be still written in routing table until the neighbor routers are notified that this route is removed from the routing table.
- **Garbage**
  The invalid information of route is deleted on the routing table every 120 seconds. Once the information of route is classified as "invalid", it's eventually removed from the routing table after 120 seconds.

To adjust the timers, use the following command.

Command	Mode	Description
timers basic *UPDATE TIMEOUT GARBAGE*	Router	Adjusts RIP network timers.
no timers basic *UPDATE TIMEOUT GARBAGE*		Restores the default timers.

10.3.12 Split Horizon

Normally, routers that are connected to broadcast type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with non-broadcast networks, such as Frame Relay, situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon.

If the interface is configured with secondary IP address and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon mechanism, use the following command in *Interface Configuration* mode.

Command	Mode	Description
ip rip split-horizon [**poisoned**]	Interface	Enables the split horizon mechanism. poisoned: performs poisoned reverse.
no rip ip split-horizon [**poisoned**]		Disables the split horizon mechanism.

10.3.13 Authentication Key

RIP v1 does not support authentication. If you are sending and receiving RIP v2 packets, you can enable RIP authentication on an interface. The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, plain text authentication can be performed using string command.

The hiD 6615 S323 supports two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP v2 packet is plain text authentication.

Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP v2 packet. Use plain text authentication when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

To configure RIP authentication, use the following command.

Command	Mode	Description
ip rip authentication key-chain *NAME*	Interface	Enables authentication for RIP v2 packets and to specify the set of keys that can be used on an interface. NAME: name of key chain
ip rip authentication mode {**text** | **md5**}		Specifies the authentication mode. text: sends a simple text password to neighbors. If a neighbor does not have the same password, request and updates from this system are rejected. md5: sends an MD5 hash to neighbors. Neighbors must share the MD5 key to decrypt the message and encrypt the response.
Command	**Mode**	**Description**
ip rip authentication string *STRING*	Interface	Configures RIP authentication string which will be using on interface without Key chain. The string must be shorter than 16 characters. STRING: RIP authentication string

To disable RIP authentication, use the following command.

Command	Mode	Description
no ip rip authentication key-chain *NAME*	Interface	Disables authentication keys that can be used on an interface.
no ip rip authentication mode {**text** | **md5**}		Disables specified authentication mode.
no ip rip authentication string *STRING*		Removes RIP authentication string which will be using on interface without Key chain.

10.3.14 Restarting RIP

Occasionally, you should restart RIP system only when the switch is still operating while you manage and configure RIP. At this time, the switch reports the neighbors that RIP system is being restarting. It keeps previous route information until the restarting is complete in timer.

To restart RIP system only, use the following command.

Command	Mode	Description
rip restart grace-period <1-65535>	Global	Restarts RIP system and set the period.
no rip restart grace-period [<1-65535>]		Removes a configured period.

10.3.15 UDP Buffer Size of RIP

RIP protocol exchanges the routing information between routers using UDP packets. The hiD 6615 S323 can be configured theses UDP packets buffer size, use the following

command.

Command	Mode	Description
recv-buffer size <8196-2147483647>	Router	Sets the UDP Buffer size value for using RIP. 8196-2147483647: UDP buffer size value
no recv-buffer size <8196-2147483647>		Restore the default value of UDP buffer size.

10.3.16 Monitoring and Managing RIP

You can display specific router information such as the contents of IP routing tables, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also discover the routing path your router's packets are taking through the network.

To display RIP information, use the following command.

Command	Mode	Description
show ip rip	Enable Global	Shows RIP information being used in router.
show ip route rip		Shows a routing table information involved in RIP.
show ip protocols [**rip**]		Shows a current status of RIP protocol and its information.

To quickly diagnose problems, the **debug** command is useful for customers. To display information on RIP routing transactions or debugging information, use the following command.

Command	Mode	Description
debug rip events	Enable Global	Shows RIP event such as packet transmit and sending and changed RIP information.
debug rip packet [**recv** | **send**]		Shows more detailed information about RIP packet. The information includes address of packet transmission and port number.
debug rip packet [**recv** | **send**] **detail**		
show debugging rip		Shows all information configured for RIP debugging.

11 System Software Upgrade

For the system enhancement and stability, new system software may be released. Using this software, the hiD 6615 S223/323 can be upgraded without any hardware change. You can simply upgrade your system software with the provided upgrade functionality via the CLI.

11.1 General Upgrade

The hiD 6615 S223/323 supports the dual system software functionality, which you can select applicable system software stored in the system according to various reasons such as the system compatibility or stability.

To upgrade the system software of the switch, use the following command.

Command	Mode	Description
copy {**ftp** | **tftp**} **os download** {**os1** | **os2**}	Enable	Downloads the system software of the switch via FTP or TFTP. os1 | os2: the area where the system software is stored
copy {**ftp** | **tftp**} **os upload** {**os1** | **os2**}		Uploads the system software of the switch via FTP or TFTP.

To upgrade the system software, FTP or TFTP server must be set up first. Using the **copy** command, the system will download the new system software from the server.

To reflect the downloaded system software, the system must restart using the **reload** command. For more information, see Section 4.1.8.

The following is an example of upgrading the system software stored in **os1**.

```
SWITCH# copy ftp os download os1
 To exit : press Ctrl+D
-------------------------------------
IP address or name of remote host (FTP): 10.100.158.144
Download File Name : V5212G.3.18.x
User Name : admin
Password:
Hash mark printing on (1024 bytes/hash mark).
Downloading NOS ....
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################

(Omitted)

################################################################################
################################################################################
################################################################################
################################################################################
```

```
################################################################################
################################################################################
#################################################################
13661792 bytes download OK.
SWITCH# show flash

Flash Information(Bytes)

 Area                          total          used          free
 ------------------------------------------------------------------
 OS1(default)(running)     16777216      13661822       3115394     3.18 #1009
 OS2                       16777216      13661428       3115788     3.12 #1008
 CONFIG                     4194304        663552       3530752
 ------------------------------------------------------------------
 Total                     37748736      27986802       9761934
SWITCH# reload
Do you want to save the system configuration? [y/n]y
Do you want to reload the system? [y/n]y

Broadcast message from admin (ttyp0) (Fri Aug 18 15:15:41 2006 +0000):

The system is going down for reboot NOW!
```

11.2 Boot Mode Upgrade

In case that you cannot upgrade the system software with the general upgrade procedure, you can upgrade it with the boot mode upgrade procedure. Before the boot mode upgrade, please keep in mind the following restrictions.

- A terminal must be connected to the system via the console interface. To open the boot mode, you should press <**S**> key when the boot logo is shown up.
- The boot mode upgrade supports TFTP only. You must set up TFTP server before upgrading the system software in the boot mode.
- In the boot mode, the only interface you can use is MGMT interface. So the system must be connected to the network via the MGMT interface.
- All you configures in the boot mode is limited to the boot mode only!

To upgrade the system software in the boot mode, perform the following step-by-step instruction.

Step 1
To open the boot mode, press <**S**> key when the boot logo is shown up.

```
*********************************************************
*                                                       *
*                 Boot Loader Version 4.76              *
*                       Siemens AG                      *
*                                                       *
*********************************************************
Press 's' key to go to Boot Mode:  0
Boot>
```

Step 2
To enable the MGMT interface to communicate with TFTP server, you need to configure a proper IP address, subnet mask and gateway on the interface.

To configure an IP address, use the following command.

Command	Mode	Description
ip *A.B.C.D*	Boot	Configures an IP address.
ip		Shows a currently configured IP address.

To configure a subnet mask, use the following command.

Command	Mode	Description
netmask *A.B.C.D*	Boot	Configures a subnet mask. (e.g. 255.255.255.0)
netmask		Shows a currently configured subnet mask.

To configure a default gateway, use the following command.

Command	Mode	Description
gateway *A.B.C.D*	Boot	Configures a default gateway.
gateway		Shows a currently configured default gateway.

To display a configured IP address, subnet mask and gateway, use the following command.

Command	Mode	Description
show	Boot	Shows a currently configured IP address, subnet mask and gateway.

The configured IP address, subnet mask and gateway on the MGMT interface are limited to the boot mode only!

The following is an example of configuring an IP address, subnet mask and gateway on the MGMT interface in the boot mode.

```
Boot> ip 10.27.41.83
Boot> netmask 255.255.255.0
Boot> gateway 10.27.41.254
Boot> show
IP          = 10.27.41.83
GATEWAY     = 10.27.41.254
NETMASK     = 255.255.255.0
MAC         = 00:d0:cb:00:0d:83
MAC1        = ff:ff:ff:ff:ff:ff
Boot>
```

Step 3
Download the new system software via TFTP using the following command.

Command	Mode	Description
load {**os1** | **os2**} *A.B.C.D FILE-NAME*	Boot	Downloads the system software. os1 | os2: the area where the system software is stored A.B.C.D: TFTP server address FILENAME: system software file name

To verify the system software in the system, use the following command.

Command	Mode	Description
flashinfo	Boot	Shows the system software in the system.

To upgrade the system software in the boot mode, TFTP server must be set up first. Using the **load** command, the system will download the new system software from the server.

The following is an example of upgrading the system software stored in **os1** in the boot mode.

```
Boot> load os1 10.27.41.82 V5212G.3.18.x
TFTP from server 10.27.41.82; our IP address is 10.27.41.83
Filename 'V5212G.3.18.x'.
Load address: 0xffffe0
Loading: ##########################################################################
         ##########################################################################
         ##########################################################################
         ##########################################################################
         ##########################################################################

        (Omitted)

         ##########################################################################
         ##########################################################################
         ##########################################################################
         ##########################################################################
         ##########################################################################
         ####
done
Bytes transferred = 13661822 (d0767e hex)

Update flash: Are you sure (y/n)? y
 Erasing     : 0x01D00000 - 0x01D1FFFF
 Programming : 0x01D00000 - 0x01D1FFFF
 Verifying   : 0x01D00000 - 0x01D1FFFF
Boot> flashinfo
Flash Information(Bytes)
Area     OS size      Default-OS    Standby-OS     OS Version
-----------------------------------------------------------
os1       13661806        *             *         3.18 #1009
os2       13661412                                3.12 #1008

Boot>
```

Step 4
Reboot the system with the new system software using the following command.

Command	Mode	Description
reboot [**os1** | **os2**]	Boot	Reboots the system with specified system software. os1 | os2: the area where the system software is stored

If the new system software is a current standby OS, just exit the boot mode, then the interrupted system boot will be continued again with the new system software.

To exit the boot mode, use the following command.

Command	Mode	Description
exit	Boot	Exits the boot mode.

11.3 FTP Upgrade

The system software of the hi can be upgraded using FTP. This will allow network or system administrators to remotely upgrade the system with the familiar interface.

To upgrade the system software using FTP, perform the following step-by-step instruction:

Step 1
Connect to the hiD 6615 S223/323 with your FTP client software. To login the system, you can use the system user ID and password.

Note that you must use the command line-based interface FTP client software when upgrading the hiD 6615 S223/323. If you use the graphic-based interface FTP client software, the system cannot recognize the upgraded software.

Step 2
Set the file transfer mode to the binary mode using the following command.

Command	Mode	Description
bin	FTP	Sets the file transfer mode to the binary mode.

Step 3
Enable to print out the hash marks as transferring a file using the following command.

Command	Mode	Description
hash	FTP	Prints out the hash marks as transferring a file.

Step 3
Uploads the new system software using the following command.

Command	Mode	Description
put *FILENAME* {**os1** | **os2**}	FTP	Uploads the system software. FILENAME: system software file name os1 | os2: the area where the system software is stored

Step 4
Exit the FTP client using the following command.

Command	Mode	Description
exit	FTP	Exits the FTP client.

To reflect the downloaded system software, the system must restart using the **reload** command! For more information, see Section 4.1.8.1.

The following is an example of upgrading the system software of the hiD 6615 S223/323 using the FTP provided by Microsoft Windows XP in the remote place.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ftp 10.27.41.91
Connected to 10.27.41.91.
220 FTP Server 1.2.4 (FTPD)
User (10.27.41.91:(none)): admin
331 Password required for admin.
Password:
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put V5212G.3.18.x os1
200 PORT command successful.
150 Opening BINARY mode data connection for os1.
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################

(Omitted)

################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
########################################
226 Transfer complete.
ftp: 13661428 bytes sent in 223.26Seconds 61.19Kbytes/sec.
ftp> bye
221 Goodbye.

C:\>
```

12 Abbreviations

ACL	Access Control List
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CBS	Committed Burst Size
CE	Communauté Européenne
CIDR	Classless Inter Domain Routing
CIR	Committed Information Rate
CLI	Command Line Interface
CoS	Class of Service
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check/Code
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Service Code Point
EGP	Exterior Gateway Protocol
EMC	Electro-Magnetic Compatibility
EN	Europäische Norm (European Standard)
ERP	Ethernet Ring Protection
FDB	Filtering Data Base
FE	Fast Ethernet
FTP	File Transfer Protocol
GB	Gigabyte
GE	Gigabit Ethernet
hiD	Access Products in SURPASS Product Family
HW	Hardware
I^2C	Inter - Integrated Circuit interface
ID	Identifier
IEC	International Electro technical Commission
IEEE 802	Standards for Local and Metropolitan Area Networks
IEEE 802.1	Glossary, Network Management, MAC Bridges, and Internetworking
IEEE	Institute of Electrical and Electronic Engineers

IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IRL	Input Rate Limiter
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunications standardization sector
L2	Layer 2
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCT	Local Craft Terminal
LLC	Logical Link Control
LLDP	Link Layer Discover Protocol
LOF	Loss of Frame
LOL	Loss of Link
LOS	Loss of Signal
LPR	Loss of Power
MAC	Medium Access Control
NE	Network Element
OAM	Operation, Administration and Maintenance
OS	Operating System
OSPF	Open Shortest Path First
PC	Personal Computer
PPP	Point to Point Protocol
QoS	Quality of Service
RFC	Request for Comments
RIP	Routing Information Protocol
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Clock
SA	Source Address
SFP	Small Form Factor Pluggable
SNMP	Simple Network Management Protocol

STP	Spanning Tree Protocol
SW	Software
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial FTP
TMN	Telecommunication Management Network
TOS	Type of Service
UDP	User Datagram Protocol
UMN	User Manual
VID	VLAN ID
VLAN	Virtual Local Area Network
VoD	Video on Demand
VPI	Virtual Path Identifier
VPN	Virtual Private Network