

# iSG18GFP

**Intelligent 18 Port Compact Service Aware Ethernet Switch**  
**IEC 61850-3 and IEEE 1613 Compliant**

---



Version 4.5.06.01, Apr 2020

**iS5 COMMUNICATIONS**

**SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS**

© 2020 iS5 Communications Inc. All rights reserved.

## **COPYRIGHT NOTICE**

© 2020 iS5 Communications Inc. All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of iS5 Communications Inc. (iS5).

## **TRADEMARKS**

iS5Com is a registered trademark of iS5. All other trademarks belong to their respective owners.

## **REGULATORY COMPLIANCE STATEMENT**

Product(s) associated with this publication complies/comply with all applicable regulations. For more details, refer to the Technical Specifications.

## **WARRANTY**

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident.

Refer to the Technical Specifications for the actual warranty period(s) of the product(s) associated with this publication.

## **DISCLAIMER**

Information in this publication is intended to be accurate. iS5 shall not be responsible for its use or infringements on third-parties because of the use of this publication. There may occasionally be unintentional errors on this publication. iS5 reserves the right to revise the contents of this publication without notice.

## **CONTACT INFORMATION**

### **iS5 Communications Inc**

5895 Ambler Dr., Mississauga, Ontario, L4W 5B7

Tel: 1+ 905-670-0004 // Fax: 1+ 289-401-5206

Website: <http://www.is5com.com/>

### **Technical Support**

E-mail: [support@is5com.com](mailto:support@is5com.com)

### **Sales Contact**

E-mail: [sales@is5com.com](mailto:sales@is5com.com)

## Contents

<b>CHAPTER 1:</b>	<b>ABOUT THE DOCUMENT .....</b>	<b>7</b>
	1.1 iSG18GFP Overview.....	7
	1.2 Using this Document .....	7
	1.3 List of Abbreviations .....	8
<b>CHAPTER 2:</b>	<b>VLAN .....</b>	<b>9</b>
	2.1 VLANs of System Usage .....	9
	2.2 VLAN Range of NMS Usage .....	9
	2.3 VLAN Configuration Guidelines .....	10
	2.3.1 VLAN Default State .....	10
	2.3.2 Vlan Ports .....	10
	2.3.3 Enabling VLAN.....	10
	2.3.4 VLAN Command Hierarchy .....	11
	2.3.5 Configuration Example.....	12
<b>CHAPTER 3:</b>	<b>IP INTERFACES .....</b>	<b>14</b>
	3.1 GCE IP Interfaces .....	14
	3.1.1 Commands Hierarchy .....	14
	3.1.2 Commands Description.....	15
	3.1.3 Default State .....	15
	3.1.4 Configuration Examples.....	15
	3.1.5 Static and Dynamic Switch Default IP Address Assignment .....	17
	3.2 ACE IP Interfaces .....	18
	3.2.1 ACE IP Interface Commands Hierarchy .....	18
	3.2.2 ACE IP Interface Commands Description.....	19
	3.2.3 Example for Creating ACE IP Interface .....	19
<b>CHAPTER 4:</b>	<b>DIAGNOSTIC .....</b>	<b>21</b>
	4.1 System Environment .....	21
	4.1.1 Environment Command Hierarchy.....	21
	4.1.2 Environment Commands Description .....	21
	4.1.3 Example .....	22
	4.2 RMON .....	23
	4.2.1 Commands Hierarchy .....	23
	4.2.2 Commands Description.....	23
	4.2.3 Example .....	24
	4.3 System Logs Export .....	25
	4.3.1 Commands Hierarchy .....	25
	4.3.2 Commands Description.....	25
	4.4 Capturing Ethernet Service Traffic.....	26
	4.4.1 Commands Hierarchy .....	26
	4.4.2 Commands Description.....	27
	4.4.3 Example .....	27
	4.5 DDM .....	29
	4.5.1 Commands Hierarchy .....	29
	4.5.2 Commands Description.....	29
	4.5.3 Example .....	30
	4.6 Debugging .....	33
	4.6.1 Commands Hierarchy .....	33
	4.6.2 Commands Description.....	34
	4.7 Syslog .....	35
	4.7.1 The Priority indicator .....	35
	4.7.2 GCE Message Format .....	36

4.7.2.1	Console message format .....	36
4.7.3	ACE Message Format.....	37
4.7.3.1	ACE Message severity .....	37
4.7.3.2	Firewall TCP SCADA Protocols .....	37
4.7.3.3	Firewall Serial SCADA Protocols .....	38
4.7.3.4	DM-VPN logs .....	40
4.7.3.5	Cellular logs .....	41
4.7.4	Commands Hierarchy .....	43
4.7.5	Commands Description.....	44
4.7.6	Configuration Example.....	45
4.7.7	Output Example .....	46
<b>4.8</b>	<b>Alarm Relay .....</b>	<b>47</b>
4.8.1	Alarm Interface.....	47
4.8.1.1	Wiring Example .....	48
4.8.2	Dry Contact Interface .....	48
4.8.2.1	Wiring example.....	49
4.8.3	Supported Alarms .....	49
4.8.3.1	SFP port state .....	49
4.8.3.2	L2 VPN state.....	49
4.8.3.3	Temperature threshold .....	49
4.8.3.4	CPU threshold .....	50
4.8.3.5	System up/down .....	50
4.8.4	Default State .....	50
4.8.5	Commands Hierarchy .....	50
4.8.6	Commands Description.....	50
<b>4.9</b>	<b>Monitor Session .....</b>	<b>52</b>
4.9.1	Commands Hierarchy .....	52
4.9.2	Commands Description.....	52
4.9.3	Example .....	52
<b>4.10</b>	<b>ACE Watchdog .....</b>	<b>52</b>
<b>4.11</b>	<b>Commands Hierarchy.....</b>	<b>53</b>
4.11.1	Commands Description.....	53
<b>CHAPTER 5:</b>	<b>SNMP.....</b>	<b>54</b>
<b>5.1</b>	<b>Supported Traps .....</b>	<b>54</b>
<b>5.2</b>	<b>SNMP Command Hierarchy .....</b>	<b>54</b>
<b>5.3</b>	<b>SNMP Commands Description .....</b>	<b>55</b>
<b>5.4</b>	<b>Example .....</b>	<b>60</b>
<b>CHAPTER 6:</b>	<b>CLOCK AND TIME.....</b>	<b>61</b>
<b>6.1</b>	<b>Local Clock.....</b>	<b>61</b>
6.1.1	Commands Hierarchy .....	61
6.1.2	Commands Description.....	61
6.1.3	Example .....	62
<b>6.2</b>	<b>SNTP.....</b>	<b>62</b>
6.2.1	SNTP Command Hierarchy .....	62
6.2.2	SNTP Commands Description.....	63
6.2.3	Example .....	70
<b>CHAPTER 7:</b>	<b>SSH.....</b>	<b>71</b>
<b>7.1</b>	<b>SSH Command Hierarchy .....</b>	<b>71</b>
<b>7.2</b>	<b>SSH Commands Description .....</b>	<b>72</b>
<b>CHAPTER 8:</b>	<b>DHCP.....</b>	<b>74</b>
<b>8.1</b>	<b>DHCP Client and Snooping Commands Hierarchy .....</b>	<b>74</b>
<b>CHAPTER 9:</b>	<b>DHCP SERVER.....</b>	<b>75</b>
<b>9.1</b>	<b>DHCP Server Commands Hierarchy .....</b>	<b>75</b>
<b>9.2</b>	<b>DHCP Relay Commands Description.....</b>	<b>76</b>

	9.3	Example .....	77
CHAPTER 10:		DHCP RELAY .....	81
	10.1	DHCP Relay GCE Command Hierarchy .....	81
	10.2	DHCP Relay GCE Commands Description .....	82
	10.3	DHCP Relay ACE Command Hierarchy .....	84
	10.4	DHCP Relay ACE Commands Description .....	84
	10.5	Example, GCE DHCP Relay .....	85
	10.6	Example, ACE DHCP Relay .....	87
CHAPTER 11:		RADIUS .....	89
	11.1	RADIUS Command Hierarchy .....	89
	11.2	RADIUS Commands Description .....	90
	11.3	Example .....	92
CHAPTER 12:		TACACS .....	93
	12.1	Default Configurations .....	93
	12.2	TACACS Command Hierarchy .....	94
	12.3	TACACS Commands Descriptions .....	94
	12.4	TACACS Command Hierarchy .....	95
	12.5	TACACS Commands Description .....	96
	12.6	Configuration Example .....	98
CHAPTER 13:		802.1X .....	99
	13.1	x Commands Hierarchy .....	99
	13.2	802.1x Commands Description .....	100
	13.3	Examples .....	103
CHAPTER 14:		IGMP SNOOPING .....	104
	14.1	IGS Commands Hierarchy .....	104
	14.2	IGS Commands Description .....	105
	14.3	Example .....	108
CHAPTER 15:		ACLs .....	110
	15.1	ACL Flow validation at a port .....	110
	15.2	GCE ACL Commands Hierarchy .....	111
	15.3	GCE ACL Commands Description .....	112
	15.4	Configuration Examples .....	120
	15.5	Flow Example .....	122
	15.5.1	Test 1 .....	122
	15.5.2	Test 2 .....	122
	15.5.3	Test 3 .....	123
	15.5.4	Test 4 .....	124
	15.5.5	Test 5 .....	124
CHAPTER 16:		QOS .....	126
	16.1	QOS Commands Hierarchy .....	126
	16.2	QOS Commands Description .....	128
	16.3	Packet Queue Assignment .....	134
	16.3.1	Port Based Assignment of Priority .....	134
	16.3.2	ACL Map to COS .....	135
	16.3.3	Set VPT or DSCP .....	135
	16.3.3.1	Map VPT to COS .....	135
	16.3.3.2	Map DSCP to COS .....	136
	16.4	Setting a Scheduling Algorithm .....	138

	16.5	Traffic Filtering at Ingress .....	139
	16.6	Setting a Shaper per Egress Port.....	139
CHAPTER 17:		LINK AGGREGATION .....	140
	17.1	LAG Command Hierarchy .....	142
	17.2	LAG Commands Description .....	142
	17.3	Example .....	144
CHAPTER 18:		STP .....	147
	18.1	STP Description .....	147
	18.2	Bridge ID and Switch Priority .....	148
	18.3	Election of the Root Switch .....	149
	18.3.1	Default State .....	149
	18.4	STP Commands Hierarchy .....	149
	18.5	STP Commands Description.....	150
CHAPTER 19:		RSTP/MSTP .....	156
	19.1	RSTP Description.....	156
	19.1.1	Port States .....	156
	19.1.2	Port Roles .....	156
	19.2	Rapid Convergence .....	157
	19.3	Proposal Agreement Sequence.....	157
	19.4	Topology Change and Topology Change Detection .....	158
	19.4.1	Default Configurations .....	158
	19.5	Setting Spanning Tree Compatibility to STP .....	159
	19.6	Configuring Spanning Tree Path Cost.....	161
	19.7	Configuring Spanning Tree Port Priority.....	163
	19.7.1	Configuring Spanning Tree Link type .....	165
	19.7.2	Configuring Spanning Tree Portfast .....	166
	19.7.3	Configuring Spanning Tree Timers .....	167
CHAPTER 20:		LLDP.....	168
	20.1	LLDP Commands Hierarchy .....	169
	20.2	LLDP Commands Description .....	170
	20.3	Example 1 .....	180
	20.3.1	S1 configuration .....	180
	20.3.2	S2 configuration .....	181
	20.3.3	Show LLDP .....	182
	20.4	Example 2 .....	183
	20.4.1	Show LLDP .....	184
CHAPTER 21:		OAM CFM .....	185
	21.1	CFM Command Hierarchy .....	185
	21.2	CFM Commands Description.....	186
CHAPTER 22:		DISCRETE IO CHANNELS.....	194
	22.1	Discrete Channel interfaces.....	194
	22.1.1	Hardware .....	194
	22.2	Modbus/TCP .....	194
	22.3	Electric Data .....	195
	22.3.1	Discrete IO Channels Commands Hierarchy .....	195
	22.4	Discrete Interfaces Commands .....	195
	22.5	Example .....	196

## Figures

Figure 4-1: Configuration Screen.....	46
Figure 4-2: Alarm Interface .....	47
Figure 4-3: Wiring Example .....	48
Figure 4-4: Dry Contact Interface .....	48
Figure 4-5: Wiring of the 2 Alarm outputs.....	49
Figure 9-1: iSG18GFP Set as DHCP Server to two Different Clients .....	77
Figure 9-2: PC Client view .....	80
Figure 10-1: GCE DHCP-Relay Configuration .....	85
Figure 10-2: DHCP-Relay configuration .....	87
Figure 14-1: IGMP Setup and Configuration .....	108
Figure 15-1: Flow Example .....	122
Figure 17-1: Link Aggregation—Example.....	140
Figure 17-2: Link Aggregation Example .....	144
Figure 18-1: Spanning Tree Topology .....	147
Figure 18-2: Bridge ID .....	148
Figure 19-1: Proposal Agreement Handshake .....	157
Figure 19-2: Spanning Tre Topology for Configuring Port Priority .....	163
Figure 20-1: Configuration and Show Outputs of LLDP Signaling .....	180
Figure 22-1: Connection Terminals .....	194
Figure 22-2: DNP3 Gateway Configuration .....	196

## About the Document

---

### 1.1 iSG18GFP Overview

The iSG18GFP is an intelligent 18 port compact Service-Aware Ethernet switch, IEC 61850-3 and IEEE 1613 compliant which is designed with a unique strong packet processing application-aware engine to fit the most critical industrial application. The optional support of an integrated firewall on every port of the iSG18GFP provides a network-based distributed security. The switch also contains a VPN gateway with 2 operational modes: inter-site connectivity using IPsec tunnels and remote user access via SSH.

The iSG18GFP is a natural fit for installation at MV/LV transformer sites acting as secure access points for the distributed automation control of remote sites. This product is as a secure gateway for Ethernet, IP, and Serial services as an optimized platform for servicing these needs over the network core. The iSG18GFP provides maximum protection against cyber threats.

The iSG18GFP can be managed by a Windows utility called Industrial Device Management System (iDMS). The product is made of galvanized steel and has a wide operating temperature from -40°C to +85°C suitable for the harshest of environments without fans.

### 1.2 Using this Document

This document contains Section B of the iSG18GFP user manual. The section covers all features available in the basic product configuration.



## 1.3 List of Abbreviations

Table 1-1: Acronyms Used in this Document

Acronym	Explanation
<b>ACE</b>	Application Configuration Environment
<b>ACL</b>	Access Control List
<b>CFM</b>	Connectivity Fault Management
<b>DDM</b>	Digital Diagnostics Monitoring
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>ERPS</b>	Ethernet Ring Protection Switching
<b>FTP</b>	File Transfer Protocol
<b>GCE</b>	General Configuration Environment
<b>HTTP</b>	HyperText Transfer Protocol
<b>ICMP</b>	Internet Control Message Protocol
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>LACP</b>	Link Aggregation Control Protocol
<b>LAG</b>	Link Aggregation Group
<b>LAN</b>	Local Area Network
<b>MAC</b>	Media Access Control
<b>OAM</b>	Operations, Administration, and Maintenance
<b>OSPF</b>	Open Shortest Path First
<b>QoS</b>	Quality of Service
<b>RMON</b>	Remote Monitoring
<b>RSTP</b>	Rapid Spanning Tree Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SNTP</b>	Simple Network Time Protocol
<b>SSH</b>	Secure Shell
<b>STP</b>	Spanning Tree Protocol
<b>TACACS</b>	Terminal Access Controller Access Control System
<b>TCP</b>	Transport Control Protocol
<b>VLAN</b>	Virtual LAN
<b>WAN</b>	Wide Area Network
<b>WTB</b>	wait-to-block (timer)
<b>USB</b>	Universal Serial Bus

# VLAN

---

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

## Performance

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

## Formation of Virtual Workgroups

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

## Simplified Administration

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

## Reduced Cost

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

## Security

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

## 2.1 VLANs of System Usage

The VLAN range of 4000-4093 is reserved for system internal usage and is not to be used or manipulated by the user unless explicitly indicated in this manual.

## 2.2 VLAN Range of NMS Usage

The iSG18GFP iSIM NMS uses a configurable range of VLANs for the creation and management of services. The user should take notice to avoid manipulating NMS created VLANs.

## 2.3 VLAN Configuration Guidelines

- VLAN is enabled in the switch by default. The default VLAN 1 cannot be deleted in the switch, but the ports can be.
- Mapping of forwarding database identifier (FID) to VLANs is successful only when VLAN learning mode is hybrid. To configure a static unicast/multicast MAC address in the forwarding database, VLAN and member ports must have been configured for the specified VLAN.
- It is not possible to configure a port as trunk, if the port is an untagged member of a VLAN.
- Up to 1k VLANs may be configured simultaneously.

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




### 2.3.1 VLAN Default State

Command	Description
VLAN Module status	Enable
Default VLAN ID configured in the switch	1
MAC address table aging time	300 seconds
Acceptable frame types	All (Accepts untagged frames or priority-tagged frames or tagged frames received on the port)
Ingress filtering	Disabled

### 2.3.2 Vlan Ports

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

The untagged setting allows the port to transmit the frames without a VLAN tag. This setting is used to configure a port connected to an end user device.

-  If the port type is not explicitly specified as untagged, then all ports are configured to be of tagged port type allowing transmission of frames with the specified VLAN tag.
-  If PVID value has not been explicitly configured for a port, then PVID assumes a default value of 1
-  Adding port to a VLAN using the command "ports <type>.." will remove all ports from the VLAN and associate only the detailed ports to the VLAN. Adding port to a VLAN using the command "ports **add** <type>.." will add this port to the VLAN without affecting other port members of the VLAN.

### 2.3.3 Enabling VLAN

A VLAN can be activated in two ways:

- By adding a member port to a VLAN (refer to section Configuring Static)
- By using the VLAN active command.

## 2.3.4 VLAN Command Hierarchy

```

+ root

+ config terminal

+ [no] vlan <vlan id>
    - [no] ports <port type> <port IDs> [untagged <port type> <port IDs>]
    - ports add <port type> <port IDs> [untagged <port type> <port IDs>]
    - set unicast-mac learning { enable | disable | default}
    - vlan active
    - vlan unicast-mac learning limit <0-4294967295>

+ interface <type> <port id>
    - [no] switchport pvid <vlan ID>
    - port mac-VLAN
    - mac-address-table static [unicast | multicast] <MAC> Vlan <id> recv port <type>
      <port id> interface <type> <port id>
    - switchport unicast-mac learning { enable | disable }
    - switchport unicast-mac learning limit <0-4294967295>

+ interface vlan <vlan id>
    - [no] shutdown
    - ip address [dhcp | <ip-address> <subnet-mask>]

- Show vlan [brief | id <vlan-range> | summary]
- show vlan device info
- show vlan port config [port <type> <port id>]
- show running-config vlan [<vlan id>]
- show mac-address table static [unicast | multicast ]

```

## 2.3.5 Configuration Example

### Setting all ports of the iSG18GFP to VLAN 1 as untagged members

```
config terminal
vlan 1
ports fastethernet 0/1-8 untagged fastethernet 0/1-8
ports add gigabitethernet 0/1-2 untagged gigabitethernet 0/1-2
exit
interface fastethernet 0/1
no shutdown
switchport pvid 1
exit
interface fastethernet 0/2
no shutdown
switchport pvid 1
exit
interface fastethernet 0/3
no shutdown
switchport pvid 1
exit
interface fastethernet 0/4
no shutdown
switchport pvid 1
exit

interface fastethernet 0/5
no shutdown
switchport pvid 1
exit
interface fastethernet 0/6
no shutdown
switchport pvid 1
exit
interface fastethernet 0/7
no shutdown
switchport pvid 1
exit
interface fastethernet 0/8
no shutdown
switchport pvid 1
exit
```

```
interface gigabitethernet 0/1
no shutdown
switchport pvid 1
exit
interface gigabitethernet 0/2
no shutdown
switchport pvid 1
exit
end
```

## VLAN configuration example #1

```
iSG18GFP# config terminal

iSG18GFP(config)# vlan 55

iSG18GFP(config-vlan)# ports fastethernet 0/1-4,0/7 untagged fastethernet
0/2,0/7

iSG18GFP(config-vlan)# end
```

## VLAN configuration example #2

```
iSG18GFP# config terminal

iSG18GFP(config)# vlan 32

iSG18GFP(config-vlan)# vlan active

iSG18GFP(config-vlan)# ports fastethernet 0/1-8 untagged all

iSG18GFP(config-vlan)# end
```



Configuration example for static Unicast entry configuring a Static Unicast .4 Entry requires the VLAN to be configured and the member ports for that specified VLAN must also be configured.

```
iSG18GFP(config)# mac-address-table static unicast 22:22:22:22:22:22 VLAN 2
recv-port gigabitethernet 0/1 interface gigabitethernet 0/2
```

# IP Interfaces

The iSG18GFP supports multiple layer 3 interfaces to be set for the purposes of:


- Routing
- Management
- Serial services

An IP interface is always assigned to a VLAN. Depending on its purpose an interface will be set either at the Global Configuration Environment (GCE) or at the Application Configuration Environment (ACE).

## 3.1 GCE IP Interfaces

The GCE interfaces are usually used for:

- IP Management to the switch (SSH, Telnet ,HTTP, SNMP, FTP).
- Routing of access traffic using static entries or OSPF.
- Different Interfaces must be in different subnets.
- Each interface can be assigned, and must be assigned, to a single VLAN.
- A VLAN can only be assigned a single IP interface.
- Static routing of GCE IP interfaces is immediate and requires no special configuration.
- Dynamic routing of GCE IP interfaces is supported with OSPF.

 Total limit of 64 subnets is supported at the routing table. Customer static and dynamic entries in total should not exceed a total of 60 entries.

### 3.1.1 Commands Hierarchy

+ root

#### + config terminal

+ interface vlan <vlan id>

- [no] shutdown

- ip address [dhcp | <ip-address> <subnet-mask>] [no]

ip route <destination ip address> <destination subnet mask>

<next hop ip> <distance>

#### debug ip dhcp client all

- release dhcp vlan <>

- renew dhcp vlan <>

- show interfaces

- show ip interface [vlan <vlan id>] [loopback <loopback id>]


- show ip route [{<ip-address> <mask> | connected | ospf | rip | static | summary}]

- show debugging

#### show ip dhcp client stats

#### show ip dhcp server binding

- show running-config ip

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

### 3.1.2 Commands Description

Command	Description
Config terminal	
Interface vlan <>	
ip address	<i>This command sets the IP address for an interface. The no form of the command resets the IP address of the interface to its default value.</i>
<ip address>	<i>Sets the IP address for an interface. If the network in which Default : 172.18.212.150.</i>
<subnet mask>	<i>Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed.</i> Default : 255.255.255.0
[no] shutdown	<i>Disable / enable the interface.</i> <i>Prior to any configuration changes to the interface it must first be disabled.</i>
[no] ip route	<i>This command adds a static route. The Route defines the IP address or interface through which the destination can be reached. The no form of this command deletes a static route.</i>
<destination ip address>	A.B.C.D
<destination mask>	Format 255.255.255.255
<next hop ip address>	<i>Defines the IP address or IP alias of the next hop that can be used to reach that network.</i>
<distance>	(1-254)

### 3.1.3 Default State

```
iSG18GFP# show ip interface
```

```
vlan1 is up, line protocol is up Internet Address is 10.0.0.1/8
```

```
Broadcast Address 255.255.255.255 vlan4093 is up, line protocol is up Internet Address is 7.7.7.4/29
```

```
Broadcast Address 7.7.7.7
```



Interface VLAN 1 is available by default for In-band management.



Interface VLAN 4093 is used for internal purposes and should not be deleted /changed.

### 3.1.4 Configuration Examples

#### 1. Example for interface configuration

```
iSG18GFP# configure terminal
```



```
iSG18GFP(config)# interface vlan 10
iSG18GFP (config-if)#ip address 192.168.0.100 255.255.255.0
iSG18GFP (config-if)no shutdown
iSG18GFP (config-if)end
iSG18GFP# write startup-cfg
```

## 2. Static route configuration

```
iSG18GFP# configure terminal
iSG18GFP(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.10 1
iSG18GFP(config)#end
write startup-cfg
```

## 3. DHCP configuration

```
iSG18GFP# configure terminal
iSG18GFP(config)# interface vlan 1
iSG18GFP (config-if)# ip address address dhcp
iSG18GFP (config-if)# end
iSG18GFP# show ip interface
vlan1 is up, line protocol is up
Internet Address is 172.17.203.39/24
Broadcast Address 172.17.203.255
IP address allocation method is dynamic
IP address allocation protocol is dhcp
```

### 3.1.5 Static and Dynamic Switch Default IP Address Assignment

+ root

+ config terminal

+ default mode [dynamic | manual]

+ default ip address <ip-address> [subnet-mask<subnet mask>] [interface <interface-type><interface-id>]

+ default ip allocation protocol dhcp

show nvram

Command	Description
Config terminal	
default mode	
manual dynamic	<p><b>manual</b> - Assigns static IP address to the default interface. The IP address and IP mask configured by user are assigned to the default interface.</p> <p><b>dynamic</b> - Assigns dynamic IP address to the default interface. IP address provided by the server in the network is assigned to the default interface on switch reboot. The IP address is fetched through the dynamic IP address configuration protocols such as DHCP client.</p> <p>Default : manual</p>
Default ip address	
<ip address>	<p>Sets the IP address for the default interface / specified interface. If the network in which the switch is implemented contains a server such as DHCP server, dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches.</p> <p>This precaution avoids creation of IP address conflicts between the switches.</p> <p>Default : 10.0.0.1</p>
subnet-mask <subnet mask>	<p>Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed</p> <p>Default : 255.0.0.0</p>
<interface-type>	fastethernet   gigabitethernet
<interface-id>	ID : <slot number>/<port number> Slot number is fixed as 0.
default ip allocation protocol dhcp	<p>Allows the client device to obtain configuration parameters such as network address, from the DHCP server.</p> <p>Default : dhcp</p>

## 3.2 ACE IP Interfaces

Multiple IP interfaces are optional. The Application IP interfaces are supported on top of the layer 3 interfaces configured at the GCE and may be routed with them.

- The following services require assignment of an IP interface and possibly routes at the ACE.
  - Serial tunneling
  - Terminal server
  - Protocol gateway
  - L2-VPN
  - L3-DMVPN
  - IPSec
- Each IP interface must be associated with a user predefined VLAN (set at the GCE).
- Each interface must be associated with a “purpose”.
- One (and only one) of the interfaces must be set to purpose application-host.
- All other interfaces must be set to purpose general
- At each such purpose VLAN, the ACE port Gi 0/3 must be set as a tagged member.
- Each interface must be in a unique subnet.
- The IP interfaces are given an automatic name indicating the VLAN tag they are created with. The name format is: `ETH1.<vlan id>`

### 3.2.1 ACE IP Interface Commands Hierarchy

+ root

+ application connect

+ router

- interface {create | remove} address-prefix <IP address>/<netmask>  
vlan [vlan id] purpose {application-host | general}

- static {enable | dissable}

+ configure terminal

- ip route static <dest network> /<subnet> <Gateway>

- interface show

- route show

### 3.2.2 ACE IP Interface Commands Description

Command	Description
<b>Application connect</b>	<i>Enter the industrial application menu</i>
<b>Router</b>	<i>Enter the application router configuration mode</i>
<b>interface create   remove</b>	<i>Add or Remove an IP interface for the application engine. The configuration should include:</i> <ul style="list-style-type: none"> <li>• <i>Address-prefix : IP address in the format aa.bb.cc.dd/xx</i></li> <li>• <i>vlan : VLAN ID that the application engine will use for this IP interface</i></li> <li>• <i>The interface will be name eth1.&lt;vlan id&gt;</i></li> </ul>
<b>Static</b>	<i>Managing static route entries</i> <i>Enable</i> <i>Disable</i>
<b>Configure terminal</b>	
<b>ip route static</b>	<ul style="list-style-type: none"> <li>• <i>dest network: target network address in the format aa.bb.cc.dd/xx</i></li> <li>• <i>Gateway : IP address in the format aa.bb.cc.dd</i></li> </ul>
<b>Show</b>	<i>Show ACE IP interfaces</i>
<b>Route show</b>	<i>Show ACE static route entries</i>

### 3.2.3 Example for Creating ACE IP Interface

1. Create a VLAN to be used for interface. port gigabitethernet 0/3 is mandatory to be assigned as tagged.

```
iSG18GFP# config terminal vlan 100
```

```
ports add gigabitethernet 0/3 end
```

```
write startup-cfg
```

2. Create an IP interface and static route (default gateway).

```
iSG18GFP#application connect
```

```
[/] router interface create address-prefix 172.17.212.10/24 vlan 100 purpose
application-host
```

```
[/]router interface show
```

```
+-----+-----+-----+-----+-----+-----+
```

---

VLAN	Name	IP/Subnet	Purpose	Description
100	eth1.100	172.17.212.10/24	application host	

---

```
[router/] static
```

```
router/static> enable
```

```
router/static# configure terminal
```

```
router/static(config)# ip route 0.0.0.0/0 172.17.212.100
```

```
router/static(config)# write
```

```
router/static(config)# exit
```

```
router/static# exit
```

```
[/]router route show
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.17.212.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1.100
0.0.0.0	172.17.212.100	0.0.0.0	UG	0	0	0	eth1.100

```
Completed OK
```

# Diagnostic

## 4.1 System Environment

### 4.1.1 Environment Command Hierarchy

+ root

+ config terminal

- set switch maximum { RAM | CPU | flash } threshold <percentage>
- set switch temperature {min|max} threshold <celsius>
- + interface <type> <port id>
- [no] snmp trap link-status
- show system information
- show env {all | temperature| RAM | CPU | flash | power}
- show nvram

### 4.1.2 Environment Commands Description

Command	Description
Config terminal	
Interface <type> <port id>	
[no] snmp trap link-status	<p>This command enables trap generation on the interface. The no form of this command disables trap generation on the interface.</p> <p>The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow.</p>
set switch maximum	<p>This command sets the switch maximum threshold values of RAM, CPU, and Flash. When the current resource usage rises above the threshold limit, the SNMP trap message with maximum severity will be sent for the specified resource and the SNTF message will be displayed. This threshold value is represented in percentage and ranges between 1 and 100 percentage</p>
{RAM   CPU   flash}	<p>RAM : Indicates the maximum RAM usage of the switch in percentage to trigger a trap.</p> <p>CPU : Indicates the maximum CPU usage of the switch in percentage to trigger a trap.</p> <p>Flsh : Indicates the maximum flash usage of the switch in percentage to trigger a trap.</p>
threshold <percentage>	<p>Percentage : 1-100</p> <p>Default : 100</p>

Command	Description
set switch temperature	<p>This command sets the maximum and minimum temperature threshold values of the switch in Celsius.</p> <p>When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between -14 and 40 degree Celsius.</p>
{min max}	<p>Sets the minimum /maximum temperature threshold value for the switch to trigger a trap.</p> <p>Defaults : Minimum : 10 degree Celsius Maximum : 40 degree Celsius</p>
threshold <celsius>	

### 4.1.3 Example

Below is a show example of a typical output:

```
iSG18GFP# show env all
RAM Threshold           : 95%
Current RAM Usage       : 54%
CPU Threshold           : 95%
Current CPU Usage       : 0%
Current power supply     :
Max Temperature         : 76C
Current Temperature     : 41.500C
Current Flash Usage     : 32%
```

## 4.2 RMON

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network- fault diagnosis, planning, and performance-tuning information.

### 4.2.1 Commands Hierarchy

- + root
- + config
  - set rmon {enable | disable}
  - + interface <type> <id>
    - rmon collection stats <index (1-65535)> [owner <ownername (127)>]
    - show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [overview]]
    - show running-config rmon

### 4.2.2 Commands Description

Command	Description
Config	
Set rmon	<p>Enable: Enables the RMON feature in the system. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis</p> <p>Disable: Disables the RMON feature in the system. On disabling, the RMON's network monitoring is called off.</p> <p>Default :disabled</p>
Interface <type> <id>	
rmon collection stats	<p>This command enables history collection of interface statistics in the buckets for the specified time interval. The no form of the command disables the history collection on the interface</p> <p>&lt;index (1-65535)&gt; : Identifies an entry in the alarm table. The value ranges between 1 and 65535.</p> <p>Owner: Allows the user to enter the name of the owner of the RMON group of statistics.</p>



### 4.2.3 Example

```
iSG18GFP# show rmon statistics 1
```

RMON is enabled

Collection 1 on Fa0/1 is active, and owned by iS5C, Monitors ifEntry.1.1 which has

Received 5449624 octets, 73797 packets,  
73797 broadcast and 0 multicast packets,  
0 undersized and 0 oversized packets,  
0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions.


0 out FCS errors,

# of packets received of length (in octets):

64: 73291, 65-127: 228, 128-255: 0,  
256-511: 0, 512-1023: 0, 1024-1518: 506

## 4.3 System Logs Export

System logs can be exported to a flash USB drive ad-hoc or by time provisioning.

 In this version, the hardware configuration allows operation of a single USB device (cellular modem OR external USB interface). Therefore, if using an iSG18GFP unit with cellular modem, please make sure to select the correct configuration of active USB device for your purposes. To do so, address section S of this manual.

### 4.3.1 Commands Hierarchy

```
+ root

-logs-export [flash:<file_name> | sftp://user:password@aa.bb.cc.dd/<file_name>
| tftp://aa.bb.cc.dd/<file_name> ]

+ application connect

+ schedule

- add task-name copy-logs [day | hour | minute | month | year]

- remove task-name copy-logs

- show
```

### 4.3.2 Commands Description

Command	Description
Logs-export	Export the logs to a server or to a USB flash drive.  The USB must be fat32 formatted and must be mounted. To mound a USB drive insert it to the switch USB port and reboot the switch.
Application connect	Entering the ACE.
Schedule	manage scheduled task to copy system logs to the USB drive. To mound a USB drive insert it to the switch USB port and reboot the switch.
add task-name copy-logs	Add a scheduled task to copy system logs to the switch drive. Day: <1-31> Month: <1-12> year: <2013-3000> hour: <1-24> minute: <1-60>
remove task-name copy-logs	Remove a scheduled task to copy system logs to the USB drive.
Show	Display tasks.

## 4.4 Capturing Ethernet Service Traffic

The system supports sniffing and capturing of Ethernet traffic for selected service IP interfaces. This capability is important in order to diagnose network traffic of a service for debugging.

The capturing is available for traffic passing via the application ports gigabitethernet 0/3-4.

The capture command is implemented on the IP interfaces eth1.<vlan id>, eth2 and mGRE where :

- eth1.<vlan id> : ACE IP interface configured by the user. Port gigabitethernet 0/3 is a tagged member at vlan x.
- eth2: ACE IP interface set internally by the system. Port gigabitethernet 0/4 is a tagged member at the service vlan. It is relevant for firewall services only (MODBUS, IEC104, DNP3).
- mGRE – VPN tunnel name.

Captures can be displayed at the terminal (up to 200 packets) or saved to the local flash (cyclic, up to 10M total size of last packets). The capture log can be exported from the flash to a USB drive or a tftp/sftp server.

### 4.4.1 Commands Hierarchy

```
+ root
+ application connect
  + router
    - interface {create | remove} address-prefix <IP address>/<netmask>
      vlan [vlan id] purpose {application-host [general]}
    - interface show
  + capture
    - start -i eth1.<vlan id> [-C] [-s] [-y] [expression <>]
    - start -i eth2 {-C} [-s] [-y] [expression <>]
    - stop
    - delete
    - export remote-address <destination address,A.B.C.D>
    - show {captured-packets | status}
    - help
```

## 4.4.2 Commands Description

Command	Description
Application connect	Entering the ACE.
Capture	<p><b>Start:</b> initiate Ethernet traffic capture on a selected ACE IP interface.</p> <ul style="list-style-type: none"> <li>• <i>-i : mandatory prefix to be followed with the IP interface name.</i></li> <li>- eth1.&lt;vlan id&gt; : an ACE IP interface created by the user for a chosen vlan id.</li> <li>- eth2 : a system internal IP interface.</li> <li>- mGRE name.</li> <li>• <i>-c : optional. Stop the capture after a defined number of packets. &lt;1-200&gt;</i></li> <li>• <i>-n : Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.</i></li> </ul> <p><b>Stop :</b> stop Ethernet traffic capture.</p> <p><b>Delete :</b> delete capture files.</p> <p><b>Export remote-address:</b> export file to a tftp server.</p> <p><b>Show</b> captured-packets -C&lt;1-200&gt;: display the captured content up to a chosen length (1-200) lines.</p> <p><b>Show status :</b> display capture configuration.</p> <p><b>Help :</b> display help on settings options.</p>

## 4.4.3 Example

1. Set a vlan for the service traffic. Assign an access port and the ACE port gi 0/3.

Config terminal Vlan 20

```
ports add fastethernet 0/5 gigabitethernet 0/3 untagged fastethernet 0/5
exit
```

```
interface fastethernet 0/5
switchport pvid 20
```

2. Set an ip interface in the ACE for the vlan.

application connect

```
router interface create address-prefix 172.18.212.235/24 vlan 20
```

[/] router interface show

```

+-----+-----+-----+-----+-----+
| VLAN | Name | IP/Subnet | Purpose | Description |
+=====+=====+=====+=====+=====+
| 20 | eth1.20 | 172.18.212.235/24 | application host | |
+-----+-----+-----+-----+-----+

```

## 3. Start capture.

```
Capture start -i eth1.20
```

```
Capture show
```

```
[capture/] show status
```

```
capture is running
```

## 4. Stop the capture and display the output.

```
Capture stop
```

```
capture show captured-packets -c 10
```

```
16:55:07.370814 IP 172.18.212.240.netbios-ns > 172.18.212.232.netbios-ns: NBT  
UDP PACKET(137): QUERY; POSITIVE;
```

```
RESPONSE; UNICAST
```

```
16:55:07.616319 IP 172.18.212.240.17500 > 255.255.255.255.17500: UDP, length  
112
```

```
16:55:07.616628 IP 172.18.212.240.17500 > 172.18.212.255.17500: UDP, length  
112
```

```
16:55:07.926503 arp who-has 172.18.212.232 tell 172.18.212.64
```

```
16:55:08.122046 IP 172.18.212.240.netbios-ns > 172.18.212.232.netbios-ns: NBT  
UDP PACKET(137): QUERY; POSITIVE;
```

```
RESPONSE; UNICAST
```

```
6:55:08.258801 arp who-has 172.18.212.232 tell 172.18.212.40
```

```
16:55:08.602306 IP 172.18.212.40.17500 > 255.255.255.255.17500: UDP, length  
112
```

```
6:55:08.604927 IP 172.18.212.40.17500 > 255.255.255.255.17500: UDP, length 112
```

```
16:55:08.605016 IP 172.18.212.40.17500 > 172.18.212.255.17500: UDP, length 112
```

```
16:55:08.680664 CDPv2, ttl: 180s, Device-ID 'Switch'[[cdp]
```

## 4.5 DDM

The system supports DDM (digital diagnostics monitoring) information for Fiber SFP modules supporting this information.

The SFP ports are gigabitethernet 0/1 and 0/2. Depending if the SFP itself supports DDM, diagnostics is available at the CLI interface.

### 4.5.1 Commands Hierarchy

#### + root

- [show sfp-port detailed](#)
- [show sfp-port extended](#)
- [show sfp-port ddm](#) [gigabitethernet <id>]

### 4.5.2 Commands Description

Command	Description
Application	Entering the ACE.
Capture	<p><b>Start</b> : initiate Ethernet traffic capture on a selected ACE IP interface.</p> <ul style="list-style-type: none"> <li>• <i>-i : mandatory prefix to be followed with the IP interface name eth1.&lt;vlan id&gt; where "vlan id" is the vlan of the ip interface.</i></li> </ul> <p><b>Stop</b> : stop Ethernet traffic capture.</p> <p><b>Delete</b> : delete capture files.</p> <p><b>Export remote-address</b> : export file to a tftp server.</p> <p><b>Show captured-packets -C&lt;1-200&gt;</b>: display the captured content up to a chosen length (1-200) lines.</p> <p><b>Show status</b> : display capture configuration.</p> <p><b>Help</b> : display help on settings options.</p>

### 4.5.3 Example

**Below is a show output of a DDM supporting SFP**

```
iSG18GFP# show sfp-port ddm
_____ Diagnostic Data For gigabitethernet 0/1 ____
```

Diagnostics Rev 9.5 supported on SFP

```
_____ ALARM Bits_WARNING Bits _____
```

Tx Power Low : OK : OK

Tx Power High : OK : OK

Tx Bias Low : OK : OK

Tx Bias High : OK : OK

Vcc Low : OK : OK

Vcc High : OK : OK

Temperature Low : OK : OK

Temperature High : OK : OK

Rx Power Low : OK : OK

Rx Power High : OK : OK

```
_____ Diagnostic Data For gigabitethernet 0/2 ____
```

Diagnostics Rev 9.3 supported on SFP

```
_____ ALARM Bits_WARNING Bits _____
```

Tx Power Low : OK : OK

Tx Power High : OK : OK

Tx Bias Low : OK : OK

Tx Bias High : OK : OK

Vcc Low : OK : OK

Vcc High : OK : OK

Temperature Low : OK : OK

Temperature High : OK : OK

Rx Power Low : FAIL : FAIL

Rx Power High : OK : OK

```
iSG18GFP# show sfp-port detailed
```

Transceiver type : SFP

Cable Connector : LC

```
Vendor Name : DELTA
Encoding    : NRZ
Manufacture Date : 2010/12/23 - 0
Media : N/A
Serial Number : 105100100009
Tx Laser Wavelength : N/A
Part Number : LCP-155A4HDRZR
Revision Level : C
Link Length Support : 2000m for 62.5/125 mm fiber link
Transceiver type : SFP
Cable Connector : LC
Vendor Name : MICROSENS
Encoding    : NRZ
Manufacture Date : 2013/03/29 - 0
Media : N/A
Serial Number : 0028 0004
Tx Laser Wavelength : N/A
Part Number : MS100190DX
Revision Level : 0000
Link Length Support : 2000m for 50/125 mm fiber link
```

```
iSG18GFP# show sfp-port extended
```

```
_____ Extended Data For gigabitethernet 0/1 _____
```

```
Temperature      : 45. 0 C
Supply Voltage    : 3.2736 V
Tx Current Bias   : 17.0776 mA
Tx Output Power   : -16.216021Dbm 0.023900mW
Rx Input Power    : -20.000000Dbm 0.010000mW
```

```
_____ Status/Control Bits _____
```

```
Data Ready Bar   : OK
Rx_LOS           : OK
Tx Fault         : OK
Soft Rate Select : OK
Rate Select      : OK
RS(1)            : OK
Soft Tx Disable  : OK
Tx Disable       : OK
```

```
_____ Extended Data For gigabitethernet 0/2 _____
```

```
Temperature      : 41.50 C
Supply Voltage    : 3.2792 V
Tx Current Bias   : 2.0544 mA
```



Tx Output Power : -10.757207Dbm 0.084000mW

Rx Input Power : -40.000000Dbm 0.000000mW

\_\_\_\_\_ Status/Control Bits \_\_\_\_\_

Data Ready Bar : OK

Rx\_LOS : FAIL

Tx Fault : OK

Soft Rate Select : OK

Rate Select : OK

RS(1) : OK

Soft Tx Disable : OK

Tx Disable : OK

## 4.6 Debugging

Debug Logging allows related logs to be displayed at the terminal.

The debug logging is implemented per feature and is by default disabled on all.

### 4.6.1 Commands Hierarchy

```
+ root
- [no]debug aps ring {[all] [critical] [start-shut] [mgmt] [ctrl] [pkt-dump] [resource] [all-
fail] [buff]>}]
- [no]debug dot1x {all | errors | events | packets | state-machine | redundancy | registry}
- [no]debug ethernet-cfm {global | {[all] | {[critical] [init] [resource]
[failure][pkt][buffer] [ctrl] [func-entry] [func-exit]}}
- [no] debug interface [track] [enetpkt dump] [ippktdump] [arppktdump] [trcerror] [os]
[failall] [buffer] [all]
- [no]debug ip dhcp client { all | event | packets | errors | bind }

- [no]debug ip dhcp relay {all | errors}
- [no]debug ip igmp snooping {[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt][redundancy] | all }
- [no]debug ip ospf
-[no]debug ip vrrp { all | init | pkt | timers | events | failures }

- [no]debug lacp
- [no]debug lldp
- [no]debug radius
- [no]debug snmp
- [no]debug spanning-tree { global | all | [errors] [init-shut] [management] [bpdu]
[events]}
- [no]debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])
- [no]debug tacacs { all | info | errors | dumptx | dumprx }
- [no]debug vlan global
- show debugging
+ config terminal
- debug-logging console
- no debug-logging
- clear core-files
```

## 4.6.2 Commands Description

Command	Description
debug-logging { console  file  flash }	<p><b>Console</b> : Displays the debug logs in the console.</p> <p><b>File  flash</b> : Stores the debug logs in the file. This feature is planned for</p>
No logging	Send the debug logs to the console.
debug interface	<p>This command sets the debug traces for all interfaces. The no form of the command resets the configured debug traces.</p> <p><b>Track</b> : Generates debug messages for all track messages.</p> <p><b>Enetpkt dump</b> : Generates debug messages for ethernet packet dump messages.</p> <p><b>Ippkt dump</b> : Generates debug messages for IP protocol related packet dump messages</p> <p><b>Arppkt dump</b> : Generates debug messages for address resolution protocol related packet dump messages.</p> <p><b>Trcerror</b> : Generates debug messages for trace error messages.</p> <p><b>Os</b> : Generates debug messages for OS resources. For example, when there is a failure in mem pool creation / deletion, this trace level is used.</p> <p><b>Failall</b> : Generates debug messages for all failures including packet validation.</p> <p><b>Buffer</b> : Generates debug messages for buffer trace levels where packet buffer is used.i.e in cases wher packet is enqueued</p> <p><b>All</b> : Generates debug messages for all kinds of traces</p>
Clear core-files	Remove files pertaining to debug information gathered on prior

## 4.7 Syslog

Syslog is a protocol used for capturing log information for devices on a network. It provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is designed to transport the event messages.

One of the fundamental advantages of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

User enables syslog server and configures the syslog related parameters. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server.

Severity of logging can be set with its numeric value <0-7> or its name tag. When configuring a server, it should be set with priority tag, reflecting the level of the message and the facility.

Syslog messages are available for both GCE and ACE processes.

### 4.7.1 The Priority indicator

The Priority indicator is calculated as:  $\text{Priority} = 8 \times \text{facility\_coefficient} + \text{severity\_level}$ .

Facility Coefficient	Facility	Priority
0	kernel messages	$0 \times 8 + \text{level}$
1	user-level messages	$1 \times 8 + \text{level}$
2	mail system	$2 \times 8 + \text{level}$
3	system daemons	$3 \times 8 + \text{level}$
4	security/authorization messages	$4 \times 8 + \text{level}$
5	messages generated internally by syslog	$5 \times 8 + \text{level}$
6	line printer subsystem	$6 \times 8 + \text{level}$
7	network news subsystem	$7 \times 8 + \text{level}$
8	UUCP subsystem	$8 \times 8 + \text{level}$
9	clock daemon	$9 \times 8 + \text{level}$
10	security/authorization messages	$10 \times 8 + \text{level}$
11	FTP daemon	$11 \times 8 + \text{level}$
12	NTP subsystem	$12 \times 8 + \text{level}$
13	log audit	$13 \times 8 + \text{level}$
14	log alert	$14 \times 8 + \text{level}$
15	clock daemon (note 2)	$15 \times 8 + \text{level}$
16	Local0	$16 \times 8 + \text{level}$
17	Local1	$17 \times 8 + \text{level}$

Facility Coefficient	Facility	Priority
18	Local2	18x8 + level
19	Local3	19x8 + level
20	Local4	20x8 + level
21	Local5	21x8 + level
22	Local6	22x8 + level
23	Local7	23x8 + level

For example, Syslog message priority tag with facility local0 is as follows:

Level purpose	Numeric level	Priority (w. local0)
emergencies	0	16x8+0=128
alerts	1	129
critical	2	130
errors	3	131
warnings	4	132
notification	5	133
informational	6	134
debugging	7	135

## 4.7.2 GCE Message Format

The following will describe the iS5Com's structure of syslog messages generated by GCE processes.

### 4.7.2.1 Console message format

The message format when sent to the CLI console is,

```
{<PRI> [Time Stamp] [Host Name] [App]}{[MSG]}
```

Examples of messages received at the CLI

```
<134>May 8 15:46:00 iSG18GFP CFA Slot0/1 Link Status [UP]
<134>May 8 15:50:52 iSG18GFP CFA Slot0/1 Link Status [DOWN]
```

#### Server message format

The message format when sent to a SYSLOG server is,

```
{<PRI> [Host IP] [Time Stamp] [Host name] [App]} {[MSG]}
```

Examples of messages received at a server

```
May 11 13:34:48 iSG18GFP CFA Slot0/2 Link Status [UP] 172.19.212.237 Local0.Info
```

May 11 13:34:42 iSG18GFP CFA Slot0/2 Link Status [DOWN] 172.19.212.237  
Local0.Info

### 4.7.3 ACE Message Format

The following will describe the iS5Com's structure of syslog messages generated by ACE processes.

#### 4.7.3.1 ACE Message severity

Severity	S indicator	Description
0	S=E	Emergency: system is unusable
1	S=A	Alert: action must be taken immediately
2	S=C	Critical: critical conditions
3	S=E	Error: error conditions
4	S=W	Warning: warning conditions
5	S=N	Notice: normal but significant condition
6	S=I	Informational: informational messages
7	S=D	Debug: debug-level messages

#### 4.7.3.2 Firewall TCP SCADA Protocols

The following describes the iSG18GFP structure of syslog messages generated for firewall of IEC 104, DNP3 TCP, MODBUS TCP.

### Console message format

The message format when sent to the CLI console is:

```
{[APP-NAME] [PROCID][Severity] [MSGID] [Time Stamp]} {[MSG]} {STRUCTURED-DATA}
```

The message structured data includes following information fields,

```
|S=SEVERITY|SG=VLAN_ID|SRC=SRC_IP_ADDR:SRC_IP_PORT|DST=DEST_IP_ADDR:DEST_IP_PORT|  
LEN=DATA_MSG_LEN|TTL=TTL|PROTO=PRTOCOL_NAME|MSG=VIOLATION_DESCR|
```

Examples of messages received at the CLI. Use the command "firewall log show" at the ACE to retrieve following log entries.

1. Example for violation type "no rule configured"

```
RF_Syslog : module 3 (firewall) severity 3 message : firewall
```

```
- |ID=74|T=2014-05-12,11:52:43 -
```

```
|S=E|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=  
iec104|MSG=[0x100]
```

```
[45,0]:FW RULE - no rule configured| (164 bytes)
```

2. Example for violation type "protocol type mismatch"

```
F_Syslog : module 3 (firewall) severity 1 message : firewall -
```

```
|ID=80|T=2014-05-12,11:52:59
|S=A|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=
iec104|MSG=[0x101][45, 0]:FW PROTOCOL protocol type mismatch| (170 bytes)
```

## Server message format

The message format when sent to a SYSLOG server is,

```
{<PRI> [Host IP] [Time Stamp] [APP-NAME]} {MSG} {STRUCTURED-DATA}
```

The message structured data includes following information fields,

```
|S=SEVERITY|SG=VLAN_ID|SRC=SRC_IP_ADDR:SRC_IP_PORT|DST=DEST_IP_ADDR:DEST_IP_PORT|LEN=DATA_
MSG_LEN|TTL=TTL|PROTO=PRTOCOL_NAME|MSG=VIOLATION_DESCR|
```

Examples of messages received at server

1. Example for violation type “no rule configured”

```
May 12 11:52:54 SW iSG18GFP firewall - Local0.Error 172.18.212.183
- |ID=79|T=2014-05-12,11:52:54
|S=E|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=62|TTL=128|PROTO=iec104|MSG=[0x100][45,
0]:FW RULE - no rule configured|
```

2. Example for violation type “protocol type mismatch”

```
172.18.212.183 May 12 11:52:59 SW iSG18GFP firewall 05-12-2014 16:53:40 Local0.Alert -
|ID=80|T=2014-05-12,11:52:59 -
|S=A|SG=3500|SRC=172.18.212.50:52011|DST=172.18.212.46:2404|LEN=56|TTL=128|PROTO=iec104|MSG=[0x101]
[45,0]:FW PROTOCOL protocol type mismatch| (170 bytes)
```

### 4.7.3.3 Firewall Serial SCADA Protocols

The following describes the iS5Com structure of syslog messages generated for firewall of IEC 101, DNP3 RTU, MODBUS RTU.

```
IP=IP_ADDR|SLOT=SLOT_NUMBER|PORT=PORT_NUMBER|DIR=DATA_MSG_DIR|LEN=DATA_MSG_LEN|PR
O
TO=PROTOCOL_NAME|MSG=VIOLATION_DESCR|
```

## Syslog message fields description

Command	Description
VLAN_ID	The VLAN number
SRC_IP_ADDR	The pointed string source IP address.
SRC_IP_PORT	The source IP port number
DEST_IP_ADDR	The pointed string destination IP address.
DEST_IP_PORT	The destination IP port number
DATA_MSG_LEN	The total data message length
TTL	The ttl value of the IP header
PRTOCOL_NAME	The protocol name field. The following values are available:
VIOLATION_DESCR	The FW violation description string. The following format is used: [Major Protocol Id,Minor Protocol Id]:Violation description string: Major Protocol Id: Major protocol id value,

	<p>for ModBus - Function Code</p> <p>for IEC101/104 - Type Id</p> <p>for DNP3 - Function Code</p> <p>Minor Protocol Id: Minor protocol id value,</p> <p>for ModBus - Sub-Function Code</p> <p>for IEC101/104 - non used</p> <p>for DNP3 - non used</p> <p>Violation description string:</p> <p>The following values are available for general violations:</p> <p>"Flow is not allowed"</p> <p>"FW PROTOCOL no violation" "FW internal error (no drop)"</p> <p>"FW PROTOCOL SW problem"</p> <p>"FW PROTOCOL no free memory"</p> <p>"FW PROTOCOL illegal message length"</p> <p>"FW PROTOCOL illegal data length"</p> <p>"FW PROTOCOL illegal value",</p> <p>"FW PROTOCOL Timeout problem"</p> <p>"FW PROTOCOL message flow inconsistency"</p> <p>"FW PROTOCOL invalid creation"</p> <p>"FW PROTOCOL general flow error"</p> <p>"FW PROTOCOL illegal message"</p> <p>"FW PROTOCOL general session problem"</p> <p>"FW PROTOCOL illegal identifier"</p> <p>"FW PROTOCOL illegal address"</p> <p>"FW PROTOCOL protocol type mismatch"</p> <p>"FW RULE - illegal flow"</p> <p>"FW RULE - illegal message" "FW RULE - illegal identifier"</p> <p>"FW RULE - illegal address" "FW RULE - no rule configured"</p>
VIOLATION_DESCR (cont)	<p>The following values are available for MODBUS protocol violations:</p> <p>"Modbus validity: illegal function"</p> <p>"Modbus validity: illegal sub-function"</p> <p>"Modbus validity: illegal encapsulated interface"</p> <p>"Modbus validity: unknown device ID"</p> <p>"Modbus validity: illegal quantity "</p> <p>"Modbus validity: illegal FIFO byte counter"</p> <p>"Modbus validity: illegal FIFO counter"</p> <p>"Modbus validity: illegal record number"</p> <p>"Modbus validity: illegal reference type"</p> <p>"Modbus validity: illegal byte counter"</p> <p>"Modbus validity: illegal length of File sub-record"</p> <p>"Modbus validity: illegal write quantity",</p> <p>"Modbus validity: illegal read quantity"</p> <p>"Modbus validity: illegal File sub-record length"</p> <p>"Rule violation: not allowed function"</p> <p>"Rule violation: not allowed sub function"</p> <p>"Rule violation: out of allowed address range"</p> <p>"Rule violation: not allowed quantity"</p> <p>"Rule violation: out of allowed value range"</p> <p>"Rule violation: not allowed sub function"</p> <p>"Rule violation: not allowed file number"</p> <p>"Rule violation: not allowed record number"</p> <p>"Rule violation: out of allowed READ address range"</p> <p>"Rule violation: out of allowed WRITE address range"</p> <p>"Rule violation: not allowed READ quantity"</p> <p>"Rule violation: not allowed WRITE quantity"</p> <p>"Rule violation: out of the allowed address range"</p> <p>"Rule violation: out of the allowed FIFO address range"</p> <p>"Rule violation: out of the allowed encapsulated interface range"</p> <p>"Rule violation: out of the allowed device identifiers range"</p>



	"Rule violation: out of the allowed object identifiers range" "Rule violation: address and quantity are out of the allowed range" "Rule violation: illegal operation" "Rule violation: inconsistent TCP Unit Identifier" The following values are available for IEC104/IEC101 protocol violations: "Iec104 validity:Illegal TypeId field" "Iec104 validity:Illegal Cause field" "Iec104 validity:Illegal APCI header" "Iec104 validity: Illegal Control field 1 in APCI header" "Iec104 validity: Illegal Control field 2 in APCI header" "Iec104 validity: Illegal Control field 3 in APCI header" "Iec104 validity: Illegal Control field 4 in APCI header" "Iec104 rule validity: Illegal type id, no rule" The following values are available for DNP3 protocol violations: "DNP3 validity: Illegal Function Code field" "DNP3 validity: Illegal Group Id field" "DNP3 validity: Invalid Object" "DNP3 validity: Parsing Error" "DNP3 validity: unused"
SLOT_NUMBER	Serial Slot number on IS5Com equipment
PORT_NUMBER	Serial port number on IS5Com equipment
DATA_MSG_DIR	The field defines data message direction. The following values are available: "access", "network", "N/A"

#### 4.7.3.4 DM-VPN logs

### Syslog message fields description

Syslog message	Description
"NHRP Event:<NHS-UP NHS- DOWN>,i/f=<MGRE IF	Appears when NHS status changed in spoke, happen when registered to NHS (NHS-UP) or NHS became unreachable (NHS-DOWN).
"<MGRE IF NAME>,<ip/mask>,<NBMA NAME>: state change <UP DOWN> -> <UP DOWN>"	Appears when status of mgre interface changed.
"Handle interface UP, walk over upper layer device via <ppp0>,Operator:<Mobile Operator>"	Appears when cellular interface connected to mobile network
"Handle interface DOWN, walk over upper layer devices via %s"	Appears when cellular interface disconnected from mobile
"WTR expired for <ip/mask>,<MGRE IF NAME>"	Wait to restore timer expired. Relevant when protection group is configured between dm vpn interfaces
"WTR started for <MGRE IF NAME> <ip/mask>,<NBMA address> "	Relevant when protection group is configured between dm vpn
"WTR stopped for <MGRE IF NAME> <ip/mask>,<NBMA address> "	Relevant when protection group is configured between dm vpn
"Failed to create dm-vpn mGRE interface <MGRE IF	Unexpected error while creating mGRE interface.
"Failed to reload config with <Mobile operator>"	Unexpected error trying to change configuration.
"Failed to create ipsec tunnel <IPSEC tunnel name>"	Failed to create ipsec tunnel

Failed to remove dm-vpn mGRE interface <MGRE IF	Failed to remove dm-vpn mGRE interface
"Failed to remove ipsec-vpn tunnel <IPSEC tunnel name>"	Failed to remove ipsec-vpn tunnel

#### 4.7.3.5 Cellular logs

### Message fields description

Syslog message	Description
"admin status <UP DOWN>"	Cellular enabled/disabled
"Modem is busy or no ready SIM, retrying..."	Modem is not responsive or SIM cards are not present
"Cellular Admin UP cannot be applied, SIMs are disabled. Stop	SIMs are not configured.
"No ready SIMs"	A SIM is enabled, but not in READY state
"Only SIM in slot <1 2> is ready"	Only SIM in slot <1 2> is ready
"slot <1 2> is preferred"	slot <1 2> is selected as preferred
"<1 2> slot has better(or equal) RSSI (<RSSI>=<RSSI>).Threshold is <Threshold>"	
"Both slots are below required threshold <RSSI>,<RSSI>	Both slots are below required threshold
"<1 2> slot is above threshold as required <RSSI>=<RSSI>. Other slot	"<1 2> slot is above threshold as required
"disconnected... attempt moving to alternative provider will be performed"	Announced disconnection while other provider is configured
"disconnected... attempt to recover will be performed"	Announced disconnection while other provider is not configured
"failed to connect... attempt to recover will be performed"	Announced failure while trying to connect
"T2 expired - remove caveat on slot <1 2>"	Announce of T2 timer expiration
"T1 expired on slot <1 2>"	Announce of T1 timer expiration
"Wait to restore expired. Attempt to move to primary..."	Wait to restore expired. Attempt to move to primary SIM
"Wait to restore expired, but primary SIM is not present or	Wait to restore expired, but primary SIM is not present or disabled
"RSSI is <RSSI> - below required threshold	RSSI is <RSSI> - below required threshold
"RSSI is <RSSI> - below required threshold (<Threshold>), but primary SIM is not present or	RSSI is <RSSI> - below required threshold (<Threshold>), but primary SIM is not present or disabled
"Continuity check failed, attempt moving to alternative provider will be performed "	Announce cont. check failure when alternative provider is configured
"Continuity check failed, attempt to recover will be performed"	Announce cont. check failure when no alternative provider is
"unexpected failure, keep trying.... Retry within <SEC> sec"	Announce unexpected failure
"Clear caveat on slot <1 2>"	Announce clear caveat of specified slot
"Retry threshold exceeded <RETRIES>, reloading switch!"	Announce threshold exceeded of cellular failures while trying to
"<ppp0> connected to <Operator>,IP <address>, BAND=<WCDMA GSM>, Channel=<channel>"	Cellular connection information

Syslog message	Description
"Periodic echo check failed <NAME> LOSS=<%LOSS>(threshold=<%THRESHOLD>), RTT=<Round	Echo test failure
"change SIM slot to <1 2>"	SIM change
"SIM[<1 2>] state chg: <UNKNOWN DISABLED NOT_PRESENT PIN_LOC K PUK_LOCK READY CONNECTING FAILED CO	SIM state change
"Cellular experienced <NUM1> backpressure events in last <NUM2> seconds. Total since connected	This log is to help to fine tune the rate limit for cellular interface (Relevant when QOS is enabled)

## Output example at CLI

Use the command "show logging" to retrieve following log entries.

```
<134>May 13 13:31:41 iSG18GFP Cellular admin status enabled
<133>May 13 13:32:08 iSG18GFP Cellular SIM[1] state chg: UNKNOWN -> READY
<134>May 13 13:32:16 iSG18GFP Cellular sim in slot 2 is disabled
<133>May 13 13:32:16 iSG18GFP Cellular SIM[2] state chg: UNKNOWN -> DISABLED
<134>May 13 13:32:16 iSG18GFP Cellular Only SIM in slot 1 is ready
<133>May 13 13:32:20 iSG18GFP Cellular SIM[1] state chg: READY -> CONNECTING...
<134>May 13 13:32:23 iSG18GFP Mgmt Handle interface DOWN, walk over upper layer
devices via ppp0
<134>May 13 13:32:28 iSG18GFP Cellular ppp0 connected to cellcom,IP
109.253.86.77, B AND=WCDMA 850 MHz, Channel=4413
<133>May 13 13:32:28 iSG18GFP Cellular SIM[1] state chg: CONNECTING... ->
CONNECTED!
<134>May 13 13:32:28 iSG18GFP Mgmt Handle interface UP, walk over upper layer
device via ppp0,Operator:cellcom
```

## Alarm Relay LOGS

"Got '<SET|CLEAR>' event from <Manual Alarm Test|Manual D-out1 Test|Manual D-out2 Test|CPU usage|Temperature|System Power|L2VPN|GIGA Ethernet Port 9|GIGA Ethernet Port 10|Cellular|IPSec|Serial|All>:<STRING from the module> (<Alarm|D-OUT1|D-OUT2> output port)"

<STRING from the module>
System up
CPU overload, CPU usage is very High
CPU usage is now back to normal usage-rate
Temperature exceeded, Temperature is too High
Temperature level is now back to normal extent
phase1 dead
phase1 down
phase1 up

## Serial Services logs

<STRING from the module>
"connection with remote IP(<address>) for serial service id <SVC> is now resumed!!"
"no connection with remote IP(<address>) for serial service id <SVC>"
"no more missing data on Serial service id # <SVC>"
"Missing data on Serial service id # <SVC>"
"Serial Card on slot (<Slot>) is Active"
"Serial Card on slot (<Slot>) failure! Last seen <SEC>"
"Serial Station[<SLOT>,<PORT>]: Traffic is now resumed. Time=<TIME>, service-id <SVC>"
"Serial Point[<SLOT>,<PORT>,<SVC>]: No traffic since <TIME> (latest Rx=<NUM>)"

## Scheduled Reload logs

Syslog message
"Reload will happen every <SEC> seconds"
"Scheduled reload at <TIME> (within <SEC> seconds,daily=<TIME>"
"Next reload in <SEC> seconds"
"Scheduled reloading happens now!"

### 4.7.4 Commands Hierarchy

#### + config terminal

- debug-logging [console | file | flash]
- + [no] logging
- On
- buffered <1-200>
- console
- facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}
- severity <level 0-7> | emergencies | alerts | critical | errors | warnings | notification | informational | debugging
- logging-server <short(0-191)> {ipv4 <uaddr> | <host-name>} [ port <0-65535>] [{udp | tcp | beep}]
- [no] syslog localstorage
- syslog {filename-one | filename-two | filename-three } <string(32)>
- [no] logging-file <short(0-191)> <string(32)>
- clear logs
- show logging
- show logging-file
- show syslog file-name
- show syslog role

- show debug-logging
- show system information
- show syslog localstorage
- show running-config syslog

## 4.7.5 Commands Description

Command	Description
Config terminal	
logging	<ul style="list-style-type: none"> <li>• <b>buffered</b> - Limits Syslog messages displayed from an internal buffer.</li> <li>• This size ranges between 1 and 200 entries.</li> <li>• <b>console</b> - Limits messages logged to the console.</li> <li>• <b>facility</b> - The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7.</li> <li>• <b>severity</b> - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: <ul style="list-style-type: none"> <li>0   emergencies - System is unusable.</li> <li>1   alerts - Immediate action needed.</li> <li>2   critical - Critical conditions.</li> <li>3   errors - Error conditions.</li> <li>4   warnings - Warning conditions.</li> <li>5   notification - Normal but significant conditions.</li> <li>6   informational - Informational messages.</li> <li>7   debugging - Debugging messages.</li> </ul> </li> </ul> <p>Defaults :</p> <ul style="list-style-type: none"> <li>• console - enabled</li> <li>• severity - informational, when no option is selected while configuration</li> <li>• debugging, at system start-up</li> <li>• buffered - 50</li> <li>• facility - local0</li> </ul>

Command	Description
logging-server	<ul style="list-style-type: none"> <li>• <b>&lt;short(0-191)&gt;</b> - Sets the priority for the syslog messages.</li> <li>• 0-lowest priority, 191-highest priority.</li> <li>• <b>ipv4</b> &lt;uicast_addr&gt;- Sets the server address type as internet protocol version 4.</li> <li>• <b>Port</b> &lt;integer(0-65535)&gt; - Sets the port number through which it sends the syslog message. The value ranges between 0 and 65535.</li> <li>• <b>udp</b> - Sets the forward transport type as udp.</li> <li>• <b>tcp</b> - Sets the forward transport type as tcp.</li> <li>• <b>beep</b> - Sets the forward transport type as beep.</li> </ul>
syslog localstorage	enables the syslog file storage to log the status in the local storage path.
syslog filename-one	<ul style="list-style-type: none"> <li>• configures a first file to store the syslog messages locally.</li> <li>• <b>&lt;string(32)&gt;</b></li> </ul>
logging-file <short(0-191)>	adds an entry in the file table.
show logging	displays all logging status and configuration information.
show logging-file	displays the priority and file name of all three files configured in the syslog file table.
show syslog file-	displays all syslog local storage file names.
show syslog role	displays the syslog role.
show syslog localstorage	displays the syslog local storage.

## 4.7.6 Configuration Example

Set a server with priority 135 for facility local0 and severity debugging (priority=135)

```
iSG18GFP(config)# logging severity debugging
iSG18GFP(config)# logging console
iSG18GFP(config)# logging on
iSG18GFP(config)# logging facility local0
iSG18GFP(config)# logging-server 128 172.17.203.35 port 1234 udp
iSG18GFP(config)# logging-server 129 172.17.203.35 port 1234 udp
iSG18GFP(config)# logging-server 130 172.17.203.35 port 1234 udp
iSG18GFP(config)# logging-server 131 172.17.203.35 port 1234 udp
iSG18GFP(config)# logging-server 132 172.17.203.35 port 1234 udp
iSG18GFP(config)# logging-server 133 172.17.203.35 port 1234 udp
iSG18GFP(config)# logging-server 134 172.17.203.35 port 1234 udp
iSG18GFP(config)# logging-server 135 172.17.203.35 port 1234 udp
iSG18GFP(config)# end
```

The result of this configuration is that every action logged on the unit will be sent to the server. Below is shown how every cli command done on the local management is notified at the server

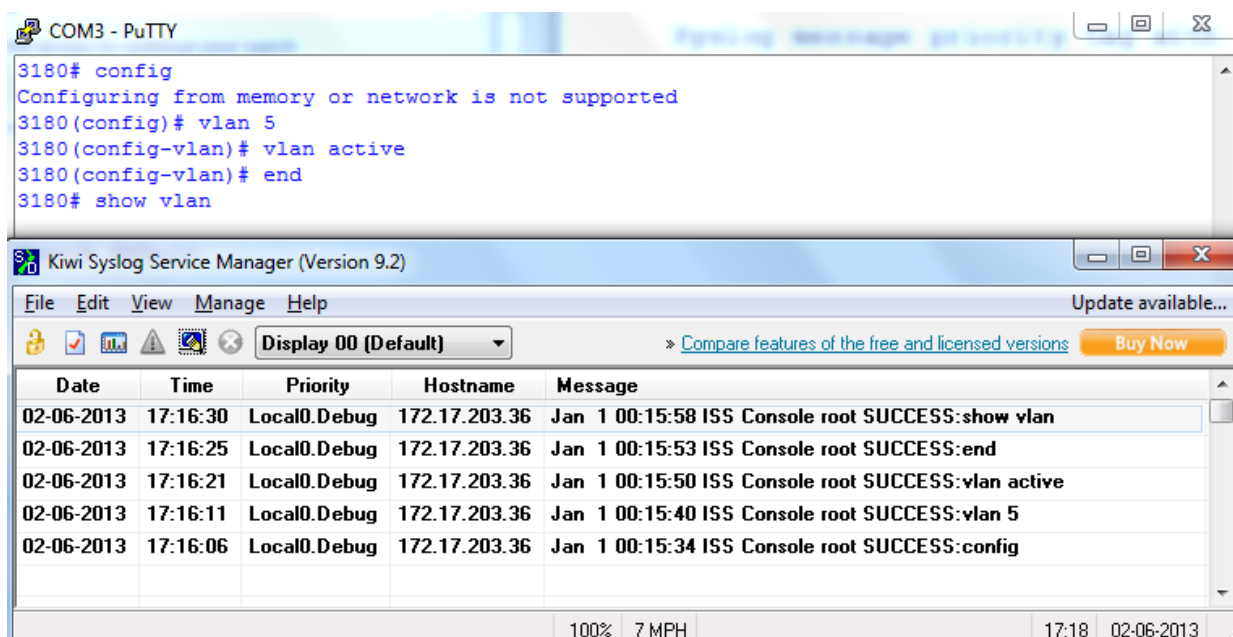


Figure 4-1: Configuration Screen

## 4.7.7 Output Example

A typical output of syslog at console interface

```
iSG18GFP# show logging
<134>May 11 09:52:21 iSG18GFP CFA vlan1 Link Status [DOWN]

<133>May 11 09:52:21 iSG18GFP CFA IP Address change in Default vlan interface.
<134>May 11 09:52:21 iSG18GFP CFA vlan1 Link Status [UP]
<129>May 8 10:38:25 iSG18GFP FM [FM - MSR] : Configuration restored successfully.
<129>May 8 10:52:15 iSG18GFP CLI Attempt to login as su via console Succeeded

<129>May 8 10:56:31 iSG18GFP CLI Attempt to login as su via telnet from
172.18.212.239 Succeeded

<134>May 8 15:45:25 iSG18GFP MSR Saved configuration to flash successfully!
<134>May 8 15:46:00 iSG18GFP CFA Slot0/1 Link Status [UP]
<134>May 8 15:50:52 iSG18GFP CFA Slot0/1 Link Status [DOWN]
<134>May 13 14:07:37 iSG18GFP CFA Slot0/7 Link Status [UP]

<134>May 13 14:07:46 iSG18GFP CFA Slot0/7 Link Status [DOWN]
<133>May 11 09:52:21 iSG18GFP CFA IP Address change in Default vlan interface.
<134>May 11 13:34:52 iSG18GFP Mgmt Got 'SET' event from GIGA Ethernet Port 9: SFP
port #9 is Down (no output port)
<134>May 11 13:34:52 iSG18GFP Mgmt Got 'SET' event from GIGA Ethernet Port 10:
SFP port #10 is Down (no output port)
```

```

<129>May 11 13:34:56 iSG18GFP FM [FM - MSR] : Configuration restored
successfully.

<129>May 11 11:38:12 iSG18GFP CFA Mac learning limit exceeded on Port Fa 0/1 SRC
MAC 54:53:ED:2B:19:86

<129>Jul 9 10:08:24 iSG18GFP FM [FM - SYS] : Temperature: 60 celsius crosses the
threshold limit. Min Temperature




```

## 4.8 Alarm Relay

The switch has a capability to manifest system and features alarms as a relay output.

Two interfaces are available for the alarm to be set at:

1. Dedicated 3 pole mechanical relay marked “ALARM” interface.
2. Optional 2 N/O relay contacts marked as “DRY CONTACT”.

-  The physical interface used for this feature can be utilized as well for the purpose of manifesting system alarms acting as “Alarm-Relay”.
-  The physical interface cannot be assigned simultaneously to both feature types.
-  For the use of discrete channels please make sure the interface is not occupied by the Alarm-Relay service.

### 4.8.1 Alarm Interface

The relay is a 3 pole interface holding a Normally Closed (NC) state between terminals 2 and 3, and a Normally Open state between terminals 2 and 1.

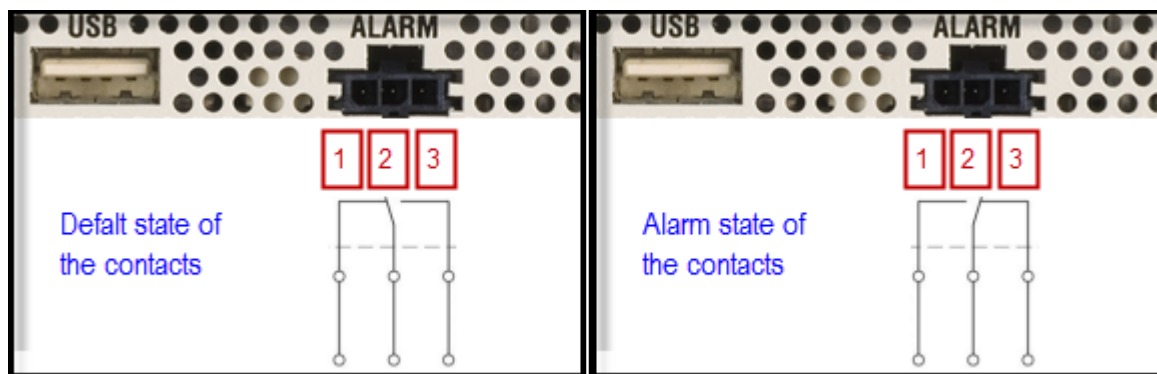


Figure 4-2: Alarm Interface

### Contact switching capabilities

DC voltage range: 9v-60v Max current : 1A



### 4.8.1.1 Wiring Example

Below connection diagram illustrates the wiring of the alarm output at its N/O contact. Poles 1 and 2 are normally open when no alarm trigger is available.

Once an alarm condition triggers the relay the contact will close as seen in this example.

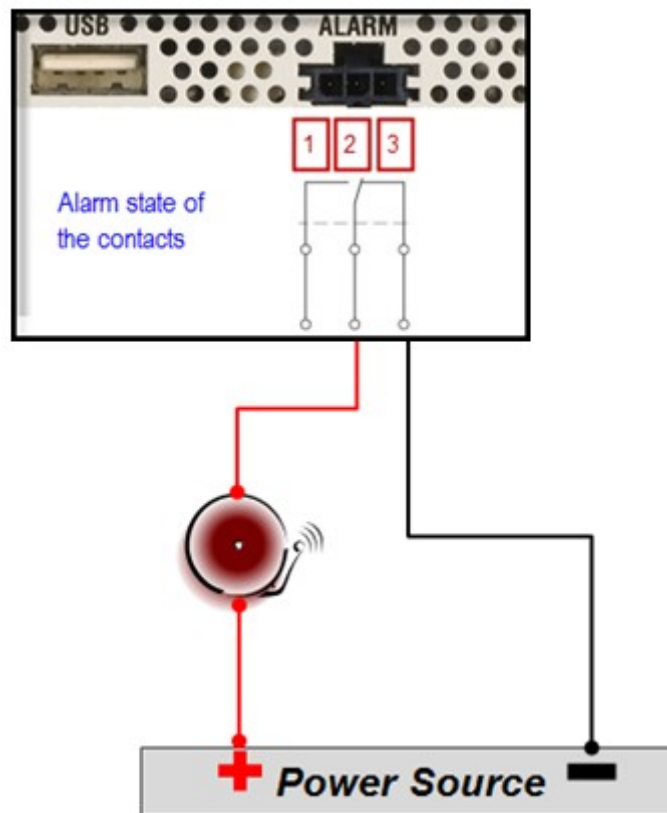


Figure 4-3: Wiring Example

### 4.8.2 Dry Contact Interface

1. Digital Output 1
2. Digital Output 2
3. Digital Output Common
4. Not Applicable
5. Not Applicable
6. Not Applicable

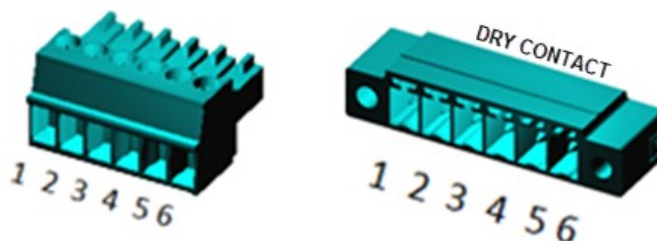


Figure 4-4: Dry Contact Interface

### 4.8.2.1 Wiring example

Below connection diagram illustrates the wiring of the 2 alarm outputs.

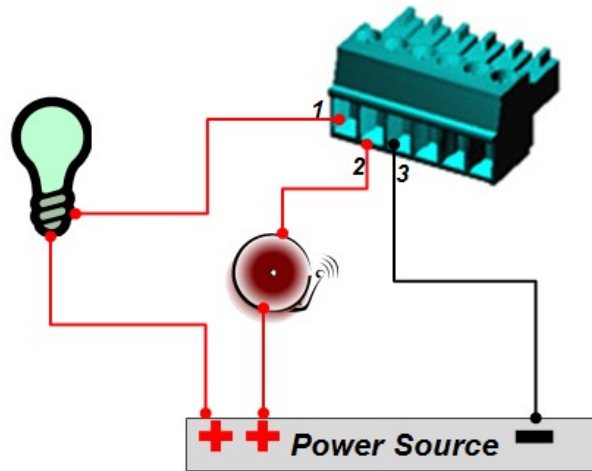


Figure 4-5: Wiring of the 2 Alarm outputs

## Contact switching capabilities

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

- AC: Max 250v, 37.5vA.
- DC: 9v-60v, 1A.

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

## 4.8.3 Supported Alarms

### 4.8.3.1 SFP port state

Two Gigabit SFP based ports are available at the unit.

These are titles Gi 0/1 and Gi 0/2 (in the IF table are 9 and 10).

A state of port down for these interfaces is supported as alarm trigger (relay state change) at the a chosen relay interface.

### 4.8.3.2 L2 VPN state

The state of a layer 2 VPN is monitored by the IPSec SA. A VPN failure is supported as alarm trigger (relay state change) at the chosen relay interface.

### 4.8.3.3 Temperature threshold

Alarm set if exceeds 76°C. Alarm clear when lower than 72°C.

#### 4.8.3.4 CPU threshold

Alarm set if exceed 95% for more than 60 sec. Alarm clears when lower than 90% for more than 60 sec.

#### 4.8.3.5 System up/down

Alarm set while system is in BOOT phase.

This specific alarm type can be associated only to the physical interface "alarm" and not to d-out1 or d-out2. Once this alarm is activated, no other alarm types can be assigned to the interface.

### 4.8.4 Default State

No alarms are associated to the relay interfaces at default machine state.

The relay contacts are at their default mechanical state and are not triggered.

### 4.8.5 Commands Hierarchy

```
+ root
+ application connect

+ Alarm-relay
- Add condition { sfp_eth9| sfp_eth10| temperature| cpu-usage| l2vpn| system-power
}
interface { alarm| d-out1| d-out2}
    - admin-status {enable| disable}
    - remove condition { sfp_eth9| sfp_eth10| temperature| cpu-usage| l2vpn| system-power
    }
    - read interface { alarm| d-out1| d-out2}
    - set interface { alarm| d-out1| d-out2} state { set| clear}
    - update condition { sfp_eth9| sfp_eth10| temperature| cpu-usage| l2vpn| system-power
    }
    interface { alarm| d-out1| d-out2}
show { admin-status| alarming_conditions| conditions| settings}
```

### 4.8.6 Commands Description

Command	Description
Config	
Application	Entering the ACE mode.
Alarm-relay	Entering the alarm relay mode.

Command	Description
Add   update	<p><b>Condition</b> : set the trigger condition for the alarm.</p> <ul style="list-style-type: none"> <li><i>temperature</i> - Alarm set if exceeds 76°C.</li> <li><i>cpu-usage</i> - Alarm set if exceed 95% for more than 60 sec.</li> <li><i>l2vpn</i> - failure at the l2 VPN will trigger a relay change.</li> <li><i>sfp_eth9</i> - status down for this port will trigger a relay change.</li> <li><i>sfp_eth10</i> - status down for this port will trigger a relay change.</li> <li><i>system-power</i> - Alarm set while in BOOT, and when the S/W performs reset.</li> </ul> <p><b>interface</b> : set the target relay interface for the condition.</p> <ul style="list-style-type: none"> <li><i>Alarm</i> - the "ALARM" relay interface.</li> <li><i>d-out1</i> - Out channel 1 at the DRY-CONTACT interface.</li> <li><i>d-out2</i> - Out channel 2 at the DRY-CONTACT interface.</li> </ul>
Admin-status	<p>Enable   disable of all relay interfaces condition to alarms.</p> <p>Default : disabled</p>
Remove condition	<p>Remove the assignment of trigger conditions.</p> <ul style="list-style-type: none"> <li><i>l2vp</i></li> </ul>
read interface	<p>Read the current relay state at the interface.</p> <ul style="list-style-type: none"> <li><i>Alarm</i> - the "ALARM" relay interface.</li> <li><i>d-out1</i> - Out channel 1 at the DRY-CONTACT interface.</li> <li><i>d-out2</i> - Out channel 2 at the DRY-CONTACT interface.</li> </ul>
set	<p><b>interface</b> : choose a target relay interface to set a static state to (not dependent on a trigger condition).</p> <ul style="list-style-type: none"> <li><i>Alarm</i> - the "ALARM" relay interface.</li> <li><i>d-out1</i> - Out channel 1 at the DRY-CONTACT interface.</li> <li><i>d-out2</i> - Out channel 2 at the DRY-CONTACT interface.</li> </ul> <p><b>State</b> : the static state to set the relay interface state to.</p>
show	<p>Show the current state.</p> <ul style="list-style-type: none"> <li><i>admin-status</i></li> <li><i>alarming_conditions</i></li> <li><i>conditions</i></li> <li><i>settings</i></li> </ul>

## 4.9 Monitor Session

### 4.9.1 Commands Hierarchy

```

+ root
+ config terminal
- monitor session <session name string> <(source | destination)>
  {interface <(port | port-channel)> <interface ID> | mac-acl <acl id> } [<(rx | tx | both)>]
set mirroring {enable | disable}
  - show monitor <(all | range <mirror session range>)>

```

### 4.9.2 Commands Description

Command	Description
Config	
Monitor	<p>Session name : string</p> <p><b>Source   destination:</b> designation of the interface.</p> <p><b>Interface :</b> source  destination interface to monitor</p> <p><b>rx   tx   both :</b> monitor of tx, rx or bote. Default</p>
set mirroring	Enable  disable the feature globally.

### 4.9.3 Example

```

iSG18GFP# config terminal
iSG18GFP(config)# monitor session 1 source interface fa 0/1 both
iSG18GFP(config)# monitor session 1 destination interface fa 0/2
iSG18GFP(config)# end

```

## 4.10 ACE Watchdog

The ACE process availability can be verified using internal connectivity check from the GCE. If the ACE is identified as unavailable, the action can be set to reboot the unit to recover it. Such an action may help in recovering ACE services as VPN and serial tunneling.

## 4.11 Commands Hierarchy

+ application connect

+  
watch  
dog

- set do-reboot <no(no| yes)> keepalive-interval <60 seconds(5-600)> number-of-retries <3,(1-10)>
- show

### 4.11.1 Commands Description

Command	Description
application connect	
set	<p>do-reboot - set action to reboot the unit if the connectivity check results in fail. default- no.</p> <p>keepalive-interval - set the time interval in seconds for the connectivity test. default -60.</p> <p>number-of-retries - set the number of retries for the connectivity test. default- 3.</p>

# SNMP

## 5.1 Supported Traps

The following traps are currently supported with version 1, 2c, 3.

- **Port up.**
- **Port down.**

## 5.2 SNMP Command Hierarchy

```
+root
+ config
- set switch-host-name { default | <string(15)> }
- enable snmpagent
- disable snmpagent
- [no] snmp community index <CommunityIndex> name <CommunityName> security
  <SecurityName> [context <Name >] [{volatile | nonvolatile}] [transporttag
  <TransportTagIdentifier | none>] [contextengineid <ContextEngineID>]
- [no] snmp user <UserName> [auth {md5 | sha} <passwd> [priv DES <passwd>]] [{volatile |
  nonvolatile}] [engineid <EngineID>]
- [no] snmp group {group name <string>}user {user name <string>}security-model
  {v1 | v2 | v3} [{volatile | nonvolatile}]
- [no] snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}
  [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView |
  none>] [{volatile | nonvolatile}] [context <string(32)> ]
- [no] snmp engineid <EngineIdentifier>
- [no] snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]
- [no] snmp targetaddr <Name> param <Name> <IPAddress> [timeout <1-1500>] [retries
  <1-3>] [taglist <TagIdentifier | none>] [{volatile | nonvolatile}] [port
  <1-65535>]
- [no] snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c | v3
  {auth | noauth | priv}} message-processing {v1 | v2c | v3} [{volatile |
  nonvolatile}] [filterprofile-name <profilename> ] [filter-storagetype
  {volatile | nonvolatile}]
- snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]
- show snmp group
- show snmp user
- show snmp group access
- show snmp viewtree
```

## 5.3 SNMP Commands Description

Command	Description
Config	
set switch-host-name	<p>Set the system host name and the snmp name. configurable 15 character string. Special characters are supported except the symbol!.</p> <p>Default - 'iSG18GFP'.</p>
enable snmpagent	<p>This command enables SNMP agent which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets and sends them to the manager.</p> <p><b>Default</b> : SNMP agent is enabled.</p>
disable snmpagent	This command disables SNMP agent
snmp community index	<p>This command configures the SNMP community details. The no form of this command removes the SNMP community details.</p> <p><b>&lt;CommunityIndex&gt;</b> - Creates a community index identifier which stores the index value of the row. This ID must be unique for every community name entry.  <i>default : NETMAN/PUBLIC</i></p> <p><b>name&lt;CommunityName&gt;</b> - Creates a community name which stores the community string. Alpha-numeric characters are allowed. Special characters are allowed except the ! Sign.  <i>Default : NETMAN/PUBLIC</i></p> <p><b>security&lt;SecurityName&gt;</b> - Stores the security model of the corresponding Snmp community name.  <i>default : none</i></p> <p><b>Context &lt;Name&gt;</b> - Indicates the name of the context in which the management information is accessed when using the community string specified by the corresponding instance of snmp community name.  <i>default : null</i></p> <p><b>volatile   non-volatile</b> - Sets the storage type as either volatile or non volatile.  <i>Default : Non Volatile</i></p> <p><b>Volatile</b> - Sets the storage type as temporary and erases the configuration setting on restarting the system.</p>



Command	Description
	<p><b>Non Volatile</b> - Sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed on restarting the system.</p> <p><b>&lt;TransportTagIdentifier&gt;</b> - Specifies a set of transport endpoints from which a command responder application can accept management request.  <i>default : null</i></p> <p>Contextengineid &lt;ContextEngineID&gt; - Indicates the location of the context through which the management information is accessed when using the community string specified by the corresponding instance of snmp community name.  <i>default : 80.00.08.1c.04.46.53</i></p>
snmp group	<p>This command configures SNMP group details.</p> <p><b>Group Name</b> - Creates a name for an SNMP group.</p> <p>Default: iso/initial Default: none/initial/templateMD5/templateSHA <b>User</b> - Sets an user for the configured group. <b>security-model</b> - Sets the security model for SNMP</p> <ul style="list-style-type: none"> <li>• V1 - Sets the SNMP version as Version 1.</li> <li>• V2c - Sets the SNMP version as Version 2.</li> <li>• V3 - Sets the SNMP version as Version 3.</li> </ul> <p>Default : v3</p> <p><b>volatile   non-volatile</b> - Sets the required storage type for the group entry  <i>default : non volatile</i></p> <p>volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.</p> <p>non-volatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.</p>
snmp access	<p>This command configures the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command.</p> <p>Group Name - Sets the name of the group for which access is to be provided.</p>

Command	Description
	<p>default :iso</p> <p>v1   v2c   v3-</p> <p><b>v1</b> - Sets the SNMP version as Version 1.</p> <p><b>v2c</b> - Sets the SNMP version as Version 2.</p> <p><b>v3</b> - Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word</p> <p><b>auth</b> - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.</p> <p><b>noauth</b> - Sets no-authentication</p> <p><b>priv</b> - Sets both authentication and privacy</p> <p><b>read</b> - Mentions the MIB view of the SNMP context to which read access is authorized by this entry</p> <p>default :iso</p> <p><b>write</b> - Mentions the MIB view of the SNMP context to which write access is authorized by this entry</p> <p>default :iso</p> <p><b>notify</b> - Mentions the MIB view of the SNMP context to which notification access is authorized by this entry</p> <p>default :iso</p> <p><b>volatile</b>   <b>non-volatile</b> - Sets the required storage type for the group entry</p> <p>default :volatile</p> <p><b>Volatile</b> - Sets the storage type as temporary. Erases the configuration setting on restarting the system.</p> <p><b>Non Volatile</b> - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.</p> <p><b>context</b> - Configures the name of the SNMP context. The maximum length of the string is 32.</p>
snmp engineid	<p>This command configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination. The no form of the command resets the engine ID to the default value.</p>
	<p>Default : 80.00.08.1c.04.46.53</p> <p>The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets.</p> <p>SNMP engine ID is an administratively unique identifier.</p> <p>Changing the value of the SNMP engine ID has significant effects. All user information will be updated automatically to reflect the change.</p>

Command	Description
snmp view	<p>This command configures the SNMP view. To configure an SNMP view (read/write/notify), a group must have already been created using the snmp group command and SNMP group access must be configured using the snmp access command.</p> <p>View Name - Specifies the view name for which the view details are to be configured.</p> <p>OID Tree - Specifies the sub tree value for the particular view. default :1</p> <p>mask - Specifies a mask value for the particular view. default :1</p> <p>view type : default : included</p> <p>Included - Allows access to the subtree</p> <p>excluded - Denies access to the subtree</p> <p>volatile - Sets the storage type as temporary.</p> <p>Erases the configuration setting on restarting the system.</p> <p>default : non volatile</p>
snmp targetaddr	<p>This command configures the SNMP target address.</p> <p>Target Address Name - Configures a unique identifier of the Target.</p> <p>Param- Configures the parameters when generating messages to be sent to transport address.</p> <p>IPAddress - Configures a IP target address to which the generated SNMP notifications are sent.</p> <p>IP6Address - Configures a IP6 target address to which the generated SNMP notifications are sent.</p>
	<p>Timeout - Sets the time in which the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message. The value ranges between 1 and 1500 seconds.</p> <p>Retries - Sets the maximum number of times the agent can retransmit the Inform Request Message. The value ranges between 1 and 3.</p> <p>taglist - Sets the tag identifier that selects the</p>
snmp targetparams	<p>This command configures the SNMP target parameters.</p> <p>&lt;ParamName&gt; - Sets a unique identifier of the parameter.</p> <p>User - Sets a user for which the target parameter is to be done.</p>

Command	Description
	<p>message-processing - Sets the message processing model default : v2c</p> <p>v1 - Sets the SNMP version as Version 1. v2c - Sets the SNMP version as Version 2. v3 - Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word volatile Sets the storage type as temporary. Erases the configuration setting on restarting the system</p> <p>Nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.</p> <p>filterprofile-name Configures the profile name filter-storage type Sets the required storage type for the filter profile</p> <p>Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system. Non Volatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.</p>
snmp user	<p>This command configures the SNMP user details.</p> <p>User Name - Configures an user name which is the User-based Security Model dependent security ID.</p> <p>Auth - Sets an authentication Algorithm. default : none. Options are: a)md5 - Sets the Message Digest 5 based authentication. b)sha - Sets the Security Hash Algorithm based authentication.</p> <p>&lt;Passwd&gt; - Sets the authentication password that will be used for the configured authentication algorithm.</p> <p>priv DES - Sets the DES encryption and also the password to be used for the encryption key.</p>
	<p>Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.</p> <p>Nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the saved configuration on restarting the system.</p>

Command	Description
snmp notify	<p>This command configures the SNMP notification details.</p> <p>&lt;NotifyName&gt; - Configures a unique identifier associated with the entry.</p> <p>Tag - Sets a notification tag, which selects the entries in the Target Address Table.</p>

## 5.4 Example

Following configuration allows snmp v2 user WR, belonging to group corporate access to the entire tree using a view called v2all.

Config

```
snmp community index iS5Com name iS5Com security none
snmp user WR
snmp group corporate user WR security-model v2c
snmp access corporate v2c read v2all write v2all notify v2all
snmp view v2all 1.3 included
```

### Allowing Traps

```
snmp targetaddr PC1 param paramlist1 172.18.212.36 taglist taglist1
snmp targetparams paramlist1 user none security-model v2c message-processing v2c
snmp notify iS5Com tag taglist1 type Trap
```

# Clock and Time

Local or server based time set and update are available. Clock configuration is available at both the ACE however the preferred method of configuration should be at the GCE.

## 6.1 Local Clock

### 6.1.1 Commands Hierarchy

```
+ root

  -clock set-rt hh:mm:ss <day(1-31)>{january|february|march|april|may|june|july|august|september|october|november|december} <year (2000 - 2035)>

- show clock

+ config terminal

+ clock

-   time source [internal-oscillator | ntp ]

-   utc-offset <offset>

-   accuracy <value(32-49)>

-   class <value(0-255)>

-   set time <time-nanoseconds>

+ application connect

+ date { [YYYY.]MM.DD-hh:mm[:ss] | hh:mm[:ss] }

- date
```

### 6.1.2 Commands Description

Command	Description
Config terminal	
Clock set	
time source	Select the clock source option. internal-oscillator
Show clock	Show the GCE clock
Application connect	
Date	Set  show the ACE clock

## 6.1.3 Example

### 1. Example for GCE time configuration

```
iSG18GFP# clock set 14:00:00 20 august 2012
```

```
iSG18GFP# show clock
```

```
Sun Feb 02 09:42:50 2
```

### 2. Example for ACE time configuration

```
[/] date 2014.02.02-10:01:30
```

```
Sun Feb 2 10:01:30 UTC 2014
```

```
Current RTC date/time is 2-2-2014, 10:01:30. [/] date
```

```
Sun Feb 2 10:01:34 UTC 2014
```

## 6.2 SNTP

The SNTP (Simple Network Time Protocol) is a simplified version or subnet of the NTP protocol. It is used to synchronize the time and date in iSG18GFP by contacting the SNTP Server. The administrator can choose whether to set the system clock manually or to enable SNTP. If SNTP is enabled, the SNTP implementation discovers the SNTP server and gets the time from the server. The SNTP implementation also has callouts to set the system time based on the time received from the SNTP server. It supports different time zones, where the user can set the required time zone.

### 6.2.1 SNTP Command Hierarchy

```
+root
+ config terminal
+ sntp
- set sntp client {enabled | disabled}
- set sntp client version { v1 | v2 | v3 | v4}
- set sntp client addressing-mode { unicast | broadcast | multicast | anycast }
- set sntp client port <portno(1025-65535)>
- set sntp client clock-format {ampm | hours}
- set sntp client time-zone <+/- UTC TimeDiff in Hrs:UTC TimeDiff in Min> Eg: +05:30
- set sntp client clock-summer-time <week-day-month, hh:mm> <week-day- month, hh:mm> Eg:
  set sntp client clock-summer-time First-Sun-Mar,05:10 Second-Sun-Nov,06:10
- set sntp client authentication-key <key-id> md5 <key>
- set sntp unicast-server auto-discovery {enabled | disabled}
- set sntp unicast-poll-interval <value (16-16284) seconds>
- set sntp unicast-max-poll-timeout <value (1-30) seconds>
- set sntp unicast-max-poll-retry <value (1-10) times>
```

- `set sntp unicast-server` {ipv4 <uicast\_addr> | domain-name <string(64)>} [{primary | secondary}] [version { 3 | 4 }] [port <integer(1025-36564)>]
- `set sntp broadcast-mode send-request` {enabled | disabled}
- `set sntp broadcast-poll-timeout` [<value (1-30) seconds>]
- `set sntp broadcast-delay-time` [<value (1000-15000) microseconds>]
- `set sntp multicast-mode send-request` {enabled | disabled}
- `set sntp multicast-poll-timeout` [<value (1-30) seconds>]
- `set sntp multicast-delay-time` [<value (1000-15000) microseconds>]
- `set sntp multicast-group-address` {ipv4 {<mcast\_addr> | default} | default}}
- `set sntp manycast-poll-interval` [<value (16-16284) seconds>]
- `set sntp manycast-poll-timeout` [<value (1-30) seconds>]
- `set sntp manycast-poll-retry-count` [<value (1-10)>]
- `set sntp manycast-server` { broadcast | multicast {ipv4 [<ipv4\_addr>] } }
- `show sntp clock`
- `show sntp status`
- `show sntp unicast-mode status`
- `show sntp broadcast-mode status`
- `show sntp multicast-mode status`
- `show sntp manycast-mode status`
- `debug sntp` (all | init-shut | mgmt | data-path | control | pkt-dump | resource | all-fail | buff)

## 6.2.2 SNTP Commands Description

Command	Description
<code>config terminal</code>	Enters the Configuration mode.
<code>sntp</code>	This command enters to SNTP configuration mode which allows the user to execute all commands that supports SNTP configuration mode.
<code>set sntp client</code>	<p>This command either enables or disables SNTP client module.</p> <p><b>Enabled:</b> Sends a request to the host for time synchronization.</p> <p><b>Disabled:</b> Does not send any request to the host for time synchronization. Defaults: Disabled.</p>



Command	Description
set sntp client version	<p>This command sets the operating version of the SNTP for the client.</p> <p><b>v1:</b> Sets the version of SNTP client as 1 <b>v2:</b> Sets the version of SNTP client as 2 <b>v3:</b> Sets the version of SNTP client as 3 <b>v4:</b> Sets the version of SNTP client as 4</p> <p>Defaults: v4</p>
set sntp client addressing mode	<p>This command sets the addressing mode of SNTP client.</p> <p><b>Unicast:</b> Sets the addressing mode of SNTP client as unicast which operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the roundtrip delay and local clock offset relative to the server.</p> <p><b>Broadcast:</b> Sets the addressing mode of SNTP client as broadcast which operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.</p> <p><b>Multicast:</b> Sets the addressing mode of SNTP client as multicast which operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates.</p> <p><b>Anycast:</b> Sets the addressing mode of SNTP client as anycast which operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 local broadcast address or multicast group address. One or more anycast servers reply with their individual unicast addresses.</p> <p>Defaults: unicast</p>
set sntp client port	<p>This command sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection. The value ranges between 1025 and 65535. The no form of this command deletes the listening port for SNTP client and sets the default value.</p> <p>Defaults: 123</p>
set sntp client clock-format	<p>This command sets the system clock as either AM PM format or HOURS format. SNTP clock format configuration in the switch:</p> <ul style="list-style-type: none"> <li>• Date - Hours, Minutes, Seconds, Date, Month and Year</li> <li>• Month - Jan, Feb, Mar...</li> <li>• Year - yyyy</li> </ul> <p><b>am-pm:</b> Sets the system clock in am/ pm format.</p> <p><b>hours:</b> Sets the system clock in 24 hours format.</p>

Command	Description
	Default: hours
set sntp client time zone	<p>This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.</p> <p><b>+/-:</b> Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone.</p> <p>Default: + 0: 0</p>
set sntp client clock-summer- time	<p>This command enables the DST (Daylight Saving Time). DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year. The no form of this command disables the Daylight Saving Time.</p> <p><b>week-day-month:</b> Week - First, Second, Third, Fourth or Last week of month. Day - Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday. Month: January, February, March, April, May, June, July, August, September, October, November or December.</p> <p><b>hh:mm:</b> Time in hours and minutes</p> <p>Default: Not set</p>
set sntp client authentication-key	<p>This command sets the authentication parameters for the key. Some SNMP servers requires authentication to be done before exchanging any data. This authentication key is used to authenticate the client to the SNMP server to which it tries to connect. The no form of this command disables authentication.</p> <p><b>&lt;key-id&gt;:</b> Sets a key identifier (integer value) to provide authentication for the server. The value ranges between 1 and 65535.</p> <p><b>md5:</b> Verifies data integrity. MD5 is intended for use with digital signature applications, which requires that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem.</p> <p><b>&lt;key&gt;:</b> Sets the authentication code as a key value.</p> <p>Default: Authentication key ID not set.</p>

Command	Description
set sntp unicast-server auto-discovery	<p>This command discovers the entire available SNTP client.</p> <p><b>Enabled:</b> Automatically discovers the entire available SNTP client even if the necessary configuration is not done.</p> <p><b>Disabled:</b> Does not discover any SNTP client.</p> <p>Defaults: Disabled</p>
set sntp unicast-poll-interval	<p>This command sets the SNTP client poll interval which is the maximum interval between successive messages in seconds. The value ranges between 16 and 16284 seconds.</p> <p>Default: 64</p>
set sntp unicast-max-poll-timeout	<p>This command configures SNTP client maximum poll interval timeout which is the maximum interval to wait for poll to complete. The value ranges between 1 and 30 in seconds.</p> <p>Default: 5</p>
set sntp unicast-max-poll-retry	<p>This command configures SNTP client maximum retry poll count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in times.</p> <p>Default: 3</p>
set sntp unicast-server	<p>This command configures SNTP unicast server. The no form of this command deletes the sntp unicast server attributes and sets to default value.</p> <p><b>ipv4 &lt;uicast_addr&gt;:</b> Sets the address type of the unicast server as Internet Protocol Version 4.</p> <p><b>Primary:</b> Sets the unicast server type as primary server.</p> <p><b>Secondary:</b> Sets the unicast server type as secondary server.</p> <p><b>version 3:</b> Sets the SNTP version as 3.</p> <p><b>version 4:</b> Sets the SNTP version as 4.</p> <p><b>Port &lt;integer(1025- 36564)&gt;:</b> Selects the port identifier numbers in the selected server. The port number ranges between 1025 and 36564.</p>

Command	Description
set sntp broadcast-mode send-request	<p>This command either enables or disables the sntp to send status request.</p> <p><b>Enabled:</b> Sends the SNTP request packet to broadcast server to calculate the actual delay.</p> <p><b>Disabled:</b> Does not send any SNTP request packet to broadcast server instead default value for the delay is taken.</p> <p>Default: disabled</p>
set sntp broadcast-poll- timeout	<p>This command configures SNTP client poll interval in broadcast mode which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 seconds.</p> <p>Default: 5</p>
set sntp broadcast-delay- time	<p>This command configures SNTP delay time in broadcast mode which is the time interval the SNTP client needs to wait for a response from the server. The value ranges between 1000 and 15000 in microseconds.</p> <p>Default: 8000</p>
set sntp multicast-mode send-request	<p>This command sets the status of sending the request to the multicast server to calculate the delay time.</p> <p><b>Enabled:</b> Sends the SNTP request to the multicast server to calculate the actual delay time.</p> <p><b>Disabled:</b> Does not send any SNTP request to the multicast server.</p> <p>Defaults: Disabled</p>
set sntp multicast-poll- timeout	<p>This command configures SNTP client poll interval in multicast mode which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 seconds.</p> <p>Default: 5</p>
set sntp multicast-delay- time	<p>This command configures SNTP delay time in which there is no response from the multicast server. The value ranges between 1000 and 15000 in microseconds.</p> <p>Default: 8000</p>
set sntp multicast-group- address	<p>This command configures a group address for the SNTP so that all SNTP client servers can be connected to this address.</p> <p>ipv4: Sets the Internet Protocol Version as version 4. &lt;mcast_addr&gt; - Sets the multicast group address. Default - Sets the multicast default address as a default value.</p>

Command	Description
set sntp manycast-poll-interval	This command configures SNTP client poll interval which is the maximum interval between successive messages. The poll interval value ranges between 16 and 16284 in seconds.  Default: 64
set sntp manycast-poll-timeout	This command configures SNTP client poll timeout which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 in seconds.  Default: 5
set sntp manycast-poll-retry-count	This command configures SNTP poll retries count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in seconds.  Default: 3
set sntp manycast-server	This command configures SNTP multicast or broadcast server address in anycast mode.  Broadcast: Configures SNTP broadcast server address in anycast mode  multicast: Configures SNTP multicast server address in anycast mode. ipv4 <ipv4_addr> - Sets the multicast server address in internet protocol v4.
show sntp clock	This command displays the current time.
show sntp status	This command displays SNTP status.
show sntp unicast mode status	This command displays the status of SNTP in unicast mode.
show sntp broadcast mode status	This command displays the status of SNTP in broadcast mode.
show sntp multicast mode status	This command displays the status of SNTP in multicast mode.
show sntp manycast mode status	This command displays the SNTP anycast mode status.

Command	Description
debug sntp	<p>This command enables SNTP trace. The no form of the command disables the SNTP trace.</p> <p><b>All:</b> Generates debug statements for all kinds of traces.</p> <p><b>init-shut:</b> Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of SNTP related entries.</p> <p><b>mgmt.:</b> Generates debug statements for management traces. This trace is generated during failure in configuration of any of the SNTP features.</p> <p><b>data-path:</b> Generates debug statements for data path traces. This trace is generated during failure in packet processing.</p> <p><b>Control:</b> Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of SNTP entries.</p> <p><b>pkt-dump:</b> Generates debug statements for packet dump traces. This trace is currently not used in SNTP module.</p> <p><b>Resource:</b> Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.</p> <p><b>all-fail:</b> Generates debug statements for all failure traces of the above mentioned traces.</p> <p><b>Buff:</b> Generates debug statements for SNTP buffer related traces. This trace is currently not used in SNTP module.</p> <p>Defaults: Debugging is Disabled.</p>

## 6.2.3 Example

### 1. The following is a configuration example.

```
iSG18GFP# show clock
```

```
Sat Jan 01 02:00:33 2000
```

```
config
```

```
clock time source ntp
```

```
sntp
```

```
set sntp client enabled
```

```
set sntp client version v2
```

```
set sntp client clock-summer-time Last-Sun-Mar,02:00 Last-Sun-Oct,02:00
```

```
set sntp unicast-poll-interval 16
```

```
set sntp client time-zone +01:00
```

```
set sntp unicast-server ipv4 96.47.67.105 primary
```

```
set sntp unicast-server ipv4 165.193.126.229 secondary
```

```
iSG18GFP(config-sntp)#
```

```
<134>Feb 6 12:26:52 ISS SNTP Old Time:Sat Jan 01 2000 00:01:35 (UTC +00:00
```

```
,New Time:Wed Feb 06 2013 12:26:52 (UTC +00:00 )
```

```
,ServerIpAddress:96.47.67.105
```

```
set sntp client time-zone +01:00
```

```
iSG18GFP(config-sntp)# <134>Feb 6 14:34:09 ISS SNTP Old Time:Wed Feb 06 2013  
12:34:02 (UTC +00:00 )
```

```
,New Time:Wed Feb 06 2013 14:34:09 (UTC +02:00 )
```

```
,ServerIpAddress:96.47.67.105
```

```
iSG18GFP# show clock
```

```
Wed Feb 06 14:35:58 2013
```

```
iSG18GFP#
```

### 2. To remove configuration, perform the following:

```
config
```

```
sntp
```

```
no sntp unicast-server ipv4 96.47.67.105
```

 It is mandatory to set the clock source to ntp as shown above

# SSH

SSH (Secure Shell) is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality and integrity.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.

The connection protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

The list of CLI commands for the configuration of SSH is as follows:

- ip ssh
- ssh
- debug ssh
- show ip ssh

## 7.1 SSH Command Hierarchy

```
+root

+config terminal

-[no] ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]
[aes128-          cbc] [aes256-cbc]) |
          auth ([hmac-md5] [hmac-sha1]) }

- ssh {enabled | disabled}

- [no] ssh server-address <IPv4> port <1-9999>

-[no] debug ssh (all | shut | mgmt | data | ctrl | dump | resource
| buffer | server)

- show ip ssh

- show ssh-configurations
```



## 7.2 SSH Commands Description


Command	Description
config terminal	Enters the Configuration mode.
[no] ip ssh	<p>This command configures the various parameters associated with SSH server. The no form of this command re-sets the various parameters associated with SSH server. The standard port used by SSH is 22.</p> <p>SSH server allows remote and secure configuration of the switch. The SSH server provides protocol version exchange, data integrity, cipher and key exchange algorithms negotiation between two communicating entities, key exchange mechanism, encryption and server authentication. The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication.</p> <p><b>Version compatibility:</b> Configures the version of the SSH. When set to true, it supports both SSH version-1 and version-2. When set to false, it supports only the SSH version-2.</p> <p><b>Cipher:</b> Configures the Cipher-List. This cipher-list takes values as bit mask. Setting a bit indicates that the corresponding cipher-list is used for encryption. <b>des-cbc</b> - This is a 1 bit cipherlist. It is based on a symmetric-key algorithm that uses a 56-bit key. <b>3des-cbc</b> - This is a 0 bit cipherlist. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.</p> <p><b>Auth:</b> Configures Public key authentication for incoming SSH sessions.</p> <p>Defaults: version compatibility-False  cipher - 3des-cbc  auth - hmac-sha1</p>
ssh	<p>This command either enables or disables the ssh subsystem. When set to enable, the switch is accessible through ssh from a remote locations. Setting ssh to disable, removes the ssh access to the switch.</p> <p><b>Enable:</b> Enables the ssh subsystem.</p> <p><b>Disable:</b> Disables the ssh subsystem.</p> <p>Defaults: enable</p>

Command	Description
ssh server-address	<p>Set a specific GCE interface to be used for the SSH server. Other GCE interface will no longer accept incoming SSH connections.</p> <p>The command requires the IPv4 of a locally available GCE interface and the port to listen on.</p> <p>Port &lt;1-9999&gt;.</p> <p>The 'no' command will return the SSH server to its default state, allowing management to any GCE interface.</p>
[no]debug ssh	<p>This command enables the trace levels for SSH. The no form of this command re-sets the SSH trace levels. Trace. System errors such as memory allocation failures are notified using LOG messages and TRACE messages.</p> <p>Interface errors and protocol errors are notified using TRACE messages. Setting all bits will enable all trace levels and resetting them will disable all trace levels.</p> <p><b>All:</b> Generates debug statements for all traces.</p> <p><b>Shut:</b> Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory.</p> <p><b>mgmt:</b> Generates debug statements for management plane functionality traces.</p> <p><b>data:</b> Generates debug statements for data path.</p> <p><b>ctrl:</b> Generates debug statements for Control Plane functionality traces.</p> <p><b>dump:</b> Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.</p> <p><b>Resource:</b> Generates debug statements for traces with respect to allocation and freeing of all resource except the buffers.</p> <p><b>Buffer:</b> Generates debug statements for traces with respect to allocation and freeing of buffer.</p> <p><b>Server:</b> Generates debug statements while creating/ opening/ closing SSH server sockets and any failures to wake up SSH server sockets. Also generates debug statements during enabling /disabling of SSH server.</p> <p>Defaults: Debugging is Disabled.</p>
show ip ssh	<p>This command displays the SSH server information such as version, cipher algorithm, authentication and trace level.</p>

# DHCP

The iSG18GFP supports the following Dynamic Host Configuration Protocol (DHCP) modes:

1. DHCP client: local interfaces can send requests to retrieve IP from DHCP server.
2. DHCP Server: the iSG18GFP can allocate IP addresses to connected DHCP clients. Multiple instances are supported using the GCE and ACE services.
3. DHCP Snooping: forwarding of connected clients requests.
4. DHCP Relay: forward the DHCP packets between client and server when they are not in the same subnets.

 DHCP snooping is disabled by default. To pass a clients request, make sure to enable dhcp snooping.

## 8.1 DHCP Client and Snooping Commands Hierarchy

+ root

+ config terminal

ip dhcp snooping [vlan <1-3999>] -

ip dhcp snooping verify mac-address -

+ interface {fastethernet| gigabitethernet} <id>

- [no] ip dhcp snooping trust

+ interface vlan <vlan id>

- [no] shutdown

- ip address dhcp

- debug ip dhcp client all

- show ip dhcp snooping

- release dhcp vlan <>

- renew dhcp vlan <>

- show interfaces

show running-config dhcp

# DHCP Server

The iSG18GFP supports DHCP Server functionality, allowing allocation of IP addresses to its local clients.

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

The server supports IP address allocation per specific conditions as client MAC or physical port, allowing assurance for specific IP out of the pool range to be assigned.

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

## 9.1 DHCP Server Commands Hierarchy

```
+ root
+ config terminal
- no service dhcp-relay
- service dhcp-server
+ [no] ip dhcp pool <index (1-2147483647)>
    - [no] network <network-IP> [ { <mask> | / <prefix-length (1-31)> } ] [end ip]
    - [no] ip dhcp server offer-reuse <timeout (1-120)>
    - lease { <days (0-365)> [<hours (0-23)> [<minutes (1-59)>]] |
infinite
        }
    - excluded-address <low-address> <high-address>
    - host hardware-type <1-2147483647> { [[client-identifier {mac} option
<id>] | [port-identifier [interface <type> <id>]] } ip
        {ip address}
    - option <1-2147483647> ip {ip address}
- show ip dhcp server information
- debug ip dhcp server all
    - show ip dhcp server binding
    - renew dhcp vlan <>
    - show ip dhcp server statistics
    - show running-config dhcp
```

## 9.2 DHCP Relay Commands Description

Command	Description
no service dhcp-relay	Disabling dhcp relay is mandatory in order to activate dhcp server
[no] service dhcp-server	Enable   disable dhcp server
Config terminal	
[no] ip dhcp pool	This command creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
[no] ip dhcp	<p>This command enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server.</p> <p>These parameters are used to control the allocation of IP address to a DHCP client.</p> <p>ping packets - Enables / disables ICMP echo mechanism. This mechanism allows the DHCP server to verify the availability of an IP address before assigning it to a DHCP client. DHCP server sends ping packets to the IP address that is intended to be assigned for the DHCP client. If the ping operation fails, DHCP server assumes that the address is not in use and assigns the address to the requesting DHCP client.</p> <p>server offerreuse - Configures the amount of time (in seconds), the DHCP server entity should wait for the DHCP REQUEST from the DHCP client before reusing the lease offer for other DHCP client.</p> <p>Binding - Deletes the specified IP address entry from the server binding table. This frees the IP address allocated to a DHCP client, so that the IP address can be allocated for another DHCP client.</p>
[no] network	This command creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
ip dhcp server offer-reuse	
Lease	This command configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
excluded-address	This command creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool. That is, the IP

Command	Description
	addresses in this range including start and end IP address of the excluded pool are not assigned to any DHCP client.
Host hardware-type	<p>This command configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.</p> <p>client-identifier: assign specific IP address from the pool range to be assigned to a specific MAC. The IP will be reserved for that MAC.</p> <p>port-identifier: assign specific IP address from the pool range to be assigned to a host connected at specific port. The IP will be reserved for that port, regardless of the host MAC. A single host (dhcp client) is allowed to be connected at a port for which this option is used for.</p>

## 9.3 Example

Following example will demonstrate allocation of IP addresses by a iSG18GFP set as dhcp server to two different clients.

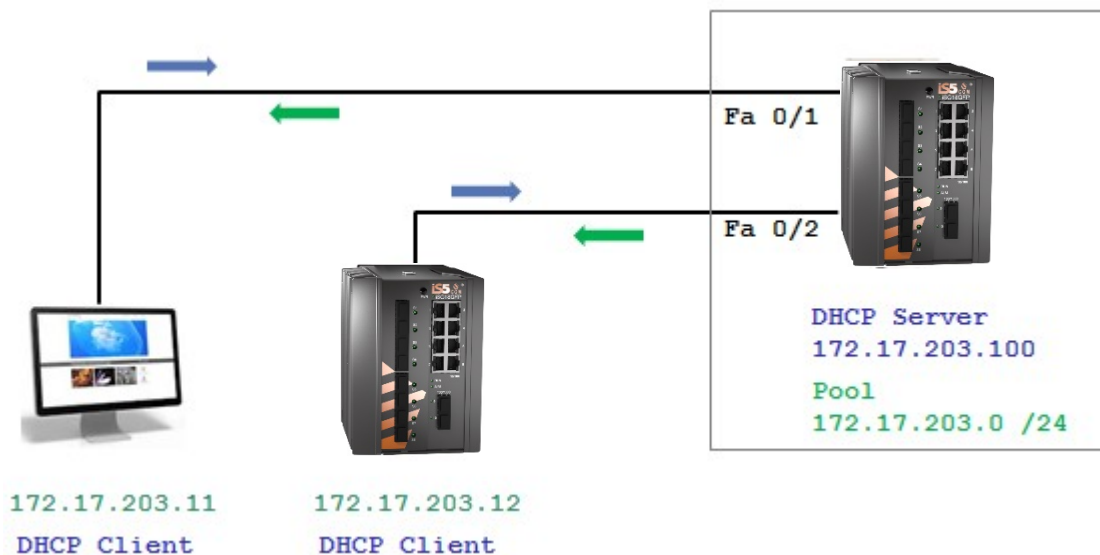


Figure 9-1: iSG18GFP Set as DHCP Server to two Different Clients

### DHCP Server

Step 1: set system host name (optional)

```
set host-name dhcp-server
```

Step 2: set GCE interface

```
config
```

```
interface vlan 1
ip address 172.17.203.100 255.255.255.0
no shutdown
exit
```

**Step 3: enable dhcp server**

```
no service dhcp-relay
service dhcp-server
```

**Step 4: set IP range pool as 172.17.203.0/24 with excluded range of 1-10.**

```
ip dhcp pool 1
network 172.17.203.0 255.255.255.0
excluded-address 172.17.203.1 172.17.203.10 exit
```

**Step 5: set a default router ip to be sent to the clients as default gateway.**

```
ip dhcp pool 1
default-router 172.17.203.100
end
write startup-config
```

**DHCP Client****Step 1: set system host name (optional)**

```
set host-name dhcp-client
```

**Step 2: set GCE interface**

```
config
interface vlan 1
ip address dhcp no shutdown
end
write startup-config
```

**DHCP Server show outputs**

```
dhcp-server# show ip dhcp server binding
Ip                Hw                Hw                Binding           Expire
Address           Type              Address            State             Time
-----
172.17.203.12 Ethernet  00:20:d2:fc:c1:f0 Assigned  Apr  7 06:34:51 2000
172.17.203.11 Ethernet  54:53:ed:2b:19:86 Assigned  Apr  7 06:49:57 2000

dhcp-server# show ip dhcp server pools
Pool Id           : 1
```

```

-----
Subnet                                     :
172.17.203.0
Subnet Mask                             : 255.255.255.0
Lease time                              : 3600 secs
Utilization threshold                   : 75%
Start Ip                                : 172.17.203.11
End Ip                                  : 172.17.203.254
Subnet Options
-----

```

```

Code      :      1, Value      : 255.255.255.0
Code      :      3, Value      : 172.17.203.100

```

```
dhcp-server# show ip dhcp server information
```

```

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

```

```
dhcp-server# show ip dhcp server statistics
```

```
Address pools : 1
```

Message	Received	
-----	-----	
DHCPDISCOVER	2	
DHCPREQUEST	5	
DHCPDECLINE	0	
DHCPRELEASE	0	
DHCPINFORM	0	
Message	Sent	
-----		----
DHCPOFFER		2
DHCPACK	5	
DHCPNAK	0	

```
dhcp-server#
```

### DHCP Client show outputs

```

dhcp-client# show ip interface
vlan1 is up, line protocol is up
Internet Address is 172.17.203.12/24
Broadcast Address 172.17.203.255
IP address allocation method is dynamic
IP address allocation protocol is dhcp

```



```

dhcp-client#
dhcp-client# show ip dhcp client stats
Dhcp Client Statistics
-----
Interface                               : vlan1
Client IP Address                       : 172.17.203.12
Client Lease Time : 3600
Client Remain Lease Time                : 2550
Message Statistics
-----
DHCP DISCOVER                          : 4
DHCP REQUEST                           : 3
DHCP DECLINE                           : 0
DHCP RELEASE                           : 0
DHCP INFORM                            : 0
DHCP OFFER                             : 1
DHCP ACKS IN REQ                       : 1
DHCP NACKS IN REQ                      : 0
DHCP ACKS IN RENEW                     : 2
DHCP NACKS IN RENEW                    : 0
DHCP ACKS IN REBIND                    : 0
DHCP NACKS IN REBIND                   : 0
DHCP ACKS IN REBOOT                    : 0
DHCP NACKS IN REBOOT                   : 0
DHCP COUNT ERROR IN HEADER             : 0
DHCP COUNT ERROR IN XID                 : 0
DHCP COUNT ERROR IN OPTIONS            : 0
dhcp-client#

```

#### PC Client view

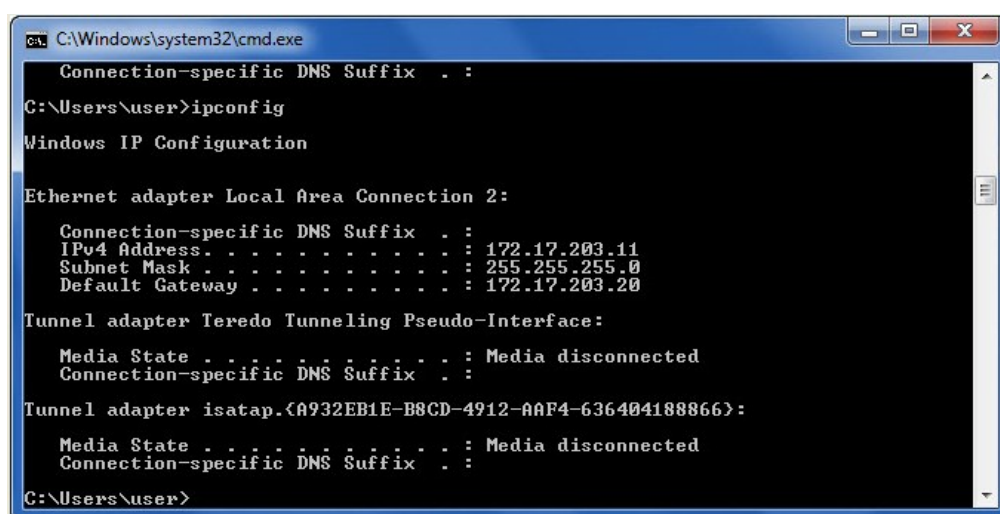


Figure 9-2: PC Client view


## DHCP Relay

DHCP relay agent is used to forward the DHCP packets between client and server when they are not in the same subnets. The relay receives packets from the client and inserts certain information like the network in which the packet is received and then forwards it to the server. The Server identifies the client's network from this information and allocates IP accordingly, then sends the reply to the relay. The Relay then strips the information inserted and broadcasts the packets into the client's network.

A maximum of 5 servers can be configured. If no servers are configured, then the DHCP packets will be broadcasted to entire network, except to the network from which packet is received.

DHCP-Relay is supported at both the GCE and ACE. The ACE should be used if segregation of DHCP relay services is required. The ACE and GCE DHCP services are each a separate service and thus the user is supported with multiple, segregated services.

 By default, DHCP-Relay is disabled.

 With IS5Com systems supporting DHCP Server (future feature) mode, the server must be disabled prior to enabling DHCP- Relay mode.

### 10.1 DHCP Relay GCE Command Hierarchy

```
+root
+config terminal
- no server dhcp-server
- [no] service dhcp-relay
- ip dhcp server <A.B.C.D>
- ip dhcp relay circuit-id option [router-index] [vlanid] [recv-port]
- ip dhcp relay information option
+ interface vlan <>
    - [no] shutdown
- ip address < A.B.C.D > <subnet>
- ip dhcp relay circuit-id <numeric circuit-id>
- ip dhcp relay information option
- ip dhcp relay remote-id <remote-id name>
- debug ip dhcp relay all
- show ip dhcp relay information [vlan <>]
- show ip interface
- show running-config dhcp
```

## 10.2 DHCP Relay GCE Commands Description

Command	Description
Config terminal	
no server dhcp-server	DHCP server is not available at the system and must be disabled to activate DHCP relay function
service dhcp-relay	<p>This command enables the DHCP relay agent in the switch. The no form of the command disables the DHCP relay agent.</p> <p>DHCP relay agent relays DHCP messages between DHCP client and DHCP server located in different subnets.</p>
ip dhcp server <A.B.C.D>	<p>This command adds the configured IP address to the IP address list created for the DHCP server. The switches or systems having these IP addresses represent the DHCP servers to which the DHCP relay agent can forward the packets that are received from DHCP clients.</p> <p>The no form of the command deletes the mentioned IP address from the IP address list.</p> <p>The DHCP relay agent broadcasts the received packets to entire network except the network from which the packets are received, if the DHCP server list is empty (that is IP address is configured as 0.0.0.0).</p>
ip dhcp relay circuit-id option	<p>This command defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option.</p> <p><b>router-index</b> - Adds information related to router interface indexes in the circuit ID sub-option.</p> <p><b>vlanid</b> - Adds information related to VLAN IDs in the circuit ID sub-option.</p> <p><b>recv-port</b> - Adds information related to physical interfaces or LAG ports in the circuit ID sub-option.</p>
ip dhcp relay information option	<p>This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option.</p> <p>The no form of the command disables the processing related to DHCP relay agent information option.</p> <p>The options contain a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves:</p> <ul style="list-style-type: none"> <li>• Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client.</li> <li>• Examining / removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client from the DHCP server.</li> </ul>

Command	Description
<pre>interface vlan &lt;id&gt; ip dhcp relay circuit-id</pre>	<p>This command configures circuit ID value for an interface.</p> <p>The no form of the command deletes the circuit ID configuration for the interface (that is, the circuit ID is configured as 0).</p> <p>The circuit ID uniquely identifies a circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed.</p> <p>The configured circuit ID is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The circuit ID is unique for the interfaces and ranges from 1 to 2147483647.</p>
<pre>ip dhcp relay information option</pre>	<p>This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option.</p> <p>The no form of the command disables the processing related to DHCP relay agent information option.</p> <p>The options contain a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves:</p> <ul style="list-style-type: none"> <li>• Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client.</li> <li>• Examining/removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client the DHCP server.</li> </ul>
<pre>ip dhcp relay remote-id</pre>	<p>This command configures remote ID value for an interface.</p> <p>The no form of the command deletes the remote ID configuration for the interface (that is, the remote ID is set with a string of length zero).</p> <p>The configured remote ID is used to inform the DHCP client about the remote circuit to which the DHCP packets should be forwarded from the interface. The remote ID is globally unique and an octet string of maximum size of 32. The remote ID should not be same as that of the default value.</p>

## 10.3 DHCP Relay ACE Command Hierarchy

- + application connect
- + router dhcp
  - add-interface {vlan <vlan-id>} [[interface-name <eth1.<vlan-id>]] {server-address <A.B.C.D>}
  - remove-interface {vlan <vlan-id>} [[interface-name <eth1.<vlan-id>]]
  - update option-82 {enable| disable}
  - enable
  - disable
- + show
  - allowed-interfaces
  - status

## 10.4 DHCP Relay ACE Commands Description

Command	Description
application connect	Access the ACE mode.
Add  remove interface	Add interface behind which the DHCP server is connected. Server-address: IPv4 address of the DHCP server. VLAN: identify the local ACE interface behind which the DHCP clients reside by its VLAN. Interface-name: identify the local ACE interface behind which the DHCP clients reside by its name. eth1<vlan-id>
update option-82	Enable  disable support of option 82.
Enable  disable	Enable/disable the DHCP relay.
Show	Show output of the DHCP configuration and state.
update option-82	Enable  disable support of option 82.
Enable  disable	Enable/disable the DHCP relay.
Show	Show output of the DHCP configuration and state.
ip dhcp relay information option	This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option.  The no form of the command disables the processing related to DHCP relay agent information option.  The options contains a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves: <ul style="list-style-type: none"> <li>• Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client.</li> <li>• Examining / removing of DHCP relay information</li> </ul>

Command	Description
	option from DHCP response messages forwarded to the DHCP client the DHCP server.
interface vlan <id>	
ip dhcp relay circuit-id	<p>This command configures circuit ID value for an interface.</p> <p>The no form of the command deletes the circuit ID configuration for the interface (that is, the circuit ID is configured as 0).</p> <p>The circuit ID uniquely identifies a circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed.</p> <p>The configured circuit ID is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The circuit ID is unique for the interfaces and ranges from 1 to 2147483647.</p>

## 10.5 Example, GCE DHCP Relay

Following setup will illustrate DHCP-Relay configuration

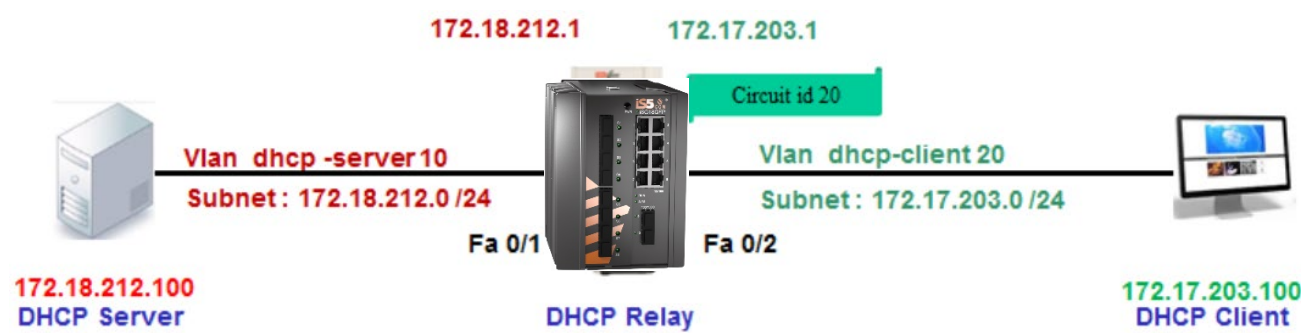


Figure 10-1: GCE DHCP-Relay Configuration

1. Configure vlan and ip interface towards the server .

```

config
vlan 10
ports fastethernet 0/1 untagged fastethernet 0/1 name dhcp-server
exit
interface fastethernet 0/1
switchport pvid 10
exit

interface vlan 10
ip address 172.18.212.1 255.255.255.0
no shutdown
exit

```

**2.Configure vlan and ip interface towards the client**

```
vlan 20
ports fastethernet 0/2 untagged fastethernet 0/2 name dhcp-client
exit
interface fastethernet 0/2
switchport pvid 20
exit
interface vlan 20
ip address 172.17.203.1 255.255.255.0
no shutdown
exit
```

**3.Enable dhcp-relay option**

```
no service dhcp-server
service dhcp-relay
ip dhcp relay information option
```

**4.Set the address of the dhcp server**

```
ip dhcp server 172.18.212.100
```

**5.set a circuit id to the client interface**

```
interface vlan 20
ip dhcp relay circuit-id 20
end
write startup-cfg
```

The configuration will result in following state

```
iSG18GFP# sh ip dhcp relay information
```

```
Dhcp Relay : Enabled
```

```
Dhcp Relay Servers only : Enabled
```

```
DHCP server 1 : 172.18.212.100
```

```
Dhcp Relay RAI option : Enabled
```

```
Default Circuit Id information : router-index
```

```
Debug Level : 0x1
```

```
No of Packets inserted RAI option : 0
```

```
No of Packets inserted circuit ID suboption : 0
```

```
No of Packets inserted remote ID suboption : 0
```

```
No of Packets inserted subnet mask suboption : 0
```

```
Mo of Packets dropped : 0
```

No of Packets which did not inserted RAI option : 0

```
Interface  vlan20
Circuit ID : 20
Remote  ID : XYZ

iSG18GFP#
```

## 10.6 Example, ACE DHCP Relay

Following setup will illustrate DHCP-Relay configuration.

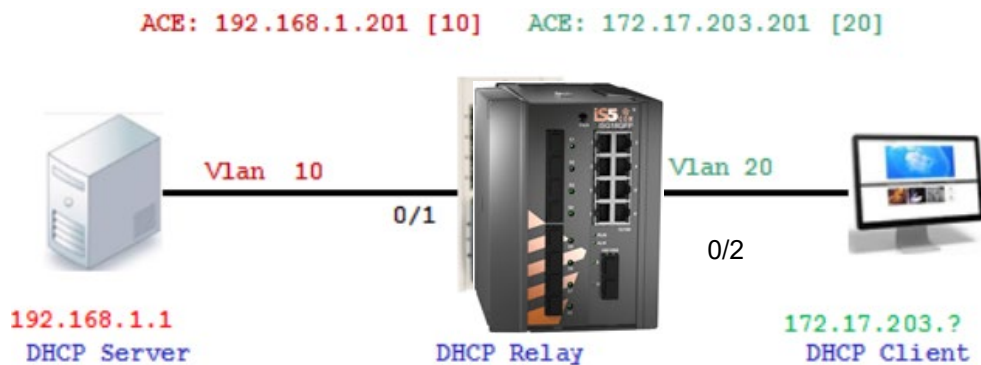


Figure 10-2: DHCP-Relay configuration

1. Configure vlan and ip interface towards the server

```
config
vlan 10
ports fastethernet 0/1 gigabitethernet 0/3 untagged fastethernet 0/1 name dhcp-server
exit
interface fastethernet 0/1
switchport pvid 10
exit
interface vlan 10
ip address 172.18.212.101 255.255.255.0 no shutdown
exit
```

2. Configure vlan and ip interface towards the client

```
vlan 20
ports fastethernet 0/2 gigabitethernet 0/3 untagged fastethernet 0/2 name dhcp-client
exit
interface fastethernet 0/2
switchport pvid 20
end
```



**3.Create ACE interfaces for the dhcp relay**

```
application connect
```

```
router interface create address-prefix 172.17.203.201/24 vlan 20 purpose application-host
```

```
router interface create address-prefix 192.168.1.201/24 vlan 10 purpose general
```

**4.Set the configuration of the dhcp**

```
router dhcp-relay add-interface server-address 192.168.1.1 vlan 20
```

```
router dhcp-relay enable
```

```
exit
```

```
write startup-cfg
```

**5.Verify configuration**

```
[/]router interface show
```

+-----+-----+-----+-----+-----+-----+-----+-----+							
Id	VLAN	Name	IP/Subnet	Mtu	Purpose	Admin status	Description
+-----+-----+-----+-----+-----+-----+-----+-----+							
10	eth1.10	192.168.1.201/24	1500	general	enable		
+-----+-----+-----+-----+-----+-----+-----+-----+							
20	eth1.20	172.17.203.201/24	1500	application host	enable		

```
+-----+-----+-----+-----+-----+-----+-----+-----+
[/]
```

```
[/]router dhcp-relay show allowed-interfaces
```

+-----+-----+-----+-----+			
If name	If IP	Server IP	
+-----+-----+-----+-----+			
eth1.10	192.168.1.201/24	192.168.1.1	
+-----+-----+-----+-----+			

Completed OK

```
[/]router dhcp-relay show status
```

+-----+-----+	
Admin Status	Option 82
+-----+-----+	
enable	enable
+-----+-----+	

Completed OK

```
[/]
```

---

# RADIUS

---

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a Client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on.

RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. It is used for several reasons:

- facilitating centralized user administration (Authentication, Authorization and Accounting).
- consistently providing some level of protection against an active attacker

The list of CLI commands for the configuration of RADIUS is as follows:

- radius-server host
- debug radius
- show radius server
- show radius statistics

## 11.1 RADIUS Command Hierarchy

```
+ root
+ config terminal
- login authentication radius [local]
-[no]radius-server host {ipv4-address | host-name} [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>] [key <secret- key-string>] [primary]
- show radius server
```

## 11.2 RADIUS Commands Description

Command	Description
config terminal	Enters the Configuration mode.
<pre> [no]radius-server host{ipv4- address   host-name} [auth- port &lt;integer(1-65535)&gt;] [acct- port &lt;integer(1-65535)&gt;] [timeout &lt;1-120&gt;] [retransmit &lt;1-254&gt;] [key &lt;secret- key- string&gt;] [primary] </pre>	<p>This command configures the RADIUS client with the parameters (host, timeout, key, retransmit). The no form of the command deletes RADIUS server configuration.</p> <p><b>ipv4-address:</b> Configures the IPv4 address of the RADIUS server host.</p> <p><b>host-name:</b> Configures the DNS (Domain Name System) name of the RADIUS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.</p>
	<p><b>auth-port &lt;integer(1-65535)&gt;:</b> Configures a specific UDP (User Datagram Protocol) destination port on this RADIUS server to be used solely for the authentication requests. The value of the auth port ranges between 1 and 65535.</p> <p><b>acct-port &lt;integer (1-65535)&gt;:</b> Configures a specific UDP destination port on this RADIUS to be solely used for accounting requests. The value of the auth port ranges between 1 and 65535.</p> <p><b>timeout &lt;1-120&gt;:</b> Configures the time period in seconds for which a client waits for a response from the server before re-transmitting the request. The value of the time out in ranges between 1 to 120 in seconds.</p> <p><b>retransmit &lt;1- 254&gt;:</b> Configures the maximum number of attempts the client undertakes to contact the server. The value number of retransmit attempts ranges between 1 and 254.</p> <p><b>key &lt;secret-keystring&gt;:</b> Configures the Per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The value of the maximum length of the secret key string is 46.</p> <ul style="list-style-type: none"> <li>• should be 1-46 characters length.</li> <li>• May include small letters.</li> </ul>

Command	Description
	<ul style="list-style-type: none"> <li>• May include capitol letter.</li> <li>• must include numbers.</li> <li>• May include special symbol.</li> <li>• allowed symbols: @#\$\$%^&amp;*()-+./&lt;\/`</li> </ul> <p><b>Primary:</b> Sets the RADIUS server as the primary server. Only one primary server will be replaced, when the command is executed with this option. Server can be configured as the primary server, any existing</p> <p>Defaults:    timeout - 3 seconds                     Retransmit - 3 attempts                     key- empty string</p>
show radius server	<p>This command displays RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port.</p> <p><b>&lt;ucast_addr&gt;:</b> Displays the related information of the specified unicast address of the RADIUS server host.</p> <p><b>&lt;string&gt;:</b> Displays the name of the RADIUS server host. This maximum value of the string is of size 32.</p>
show radius statistics	<p>This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.</p>

## 11.3 Example

### 1.configure server list and selected primary

```
iSG18GFP(config)# radius-server host 172.18.212.65 timeout <1-120> retransmit <1-254> key <key> primary
iSG18GFP(config)# radius-server host 172.18.212.45 timeout <1-120> retransmit <1-254> key <key>
```

### 2.set default login authentication method

```
iSG18GFP(config)# login authentication radius local
iSG18GFP(config)# end
iSG18GFP# write startup-cfg
```

### Output example

```
iSG18GFP# show radius server
Primary Server           : 172.18.212.65
```

#### Radius Server Host Information

```
-----
Index                : 1
Server address       : 172.18.212.65
Shared secret        :
Radius Server Status :
Enabled Response Time      : 10
Maximum Retransmission    : 3
Authentication Port       : 1812
Accounting Port          : 1813
-----
```

```
-----
Index                : 2
Server address       : 172.18.212.45
Shared secret        :
Radius Server Status : Enabled
Response Time        : 10
Maximum Retransmission    : 3
Authentication Port       : 1812
Accounting Port          : 1813
-----
```

# TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities. TACACS is used for several reasons:

- Facilitates centralized user administration.
- Uses TCP for transport to ensure reliable delivery.
- Supports inbound authentication, outbound authentication and change password request for the Authentication service.
- Provides some level of protection against an active attacker.

The list of CLI commands for the configuration of TACACS is as follows:

- `tacacs-server host`
- `tacacs use-server address`
- `tacacs-server retransmit`
- `debug tacacs`
- `show tacacs`

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or Network Access Server. TACACS+ allows a client to accept a username and password and sends a query to a TACACS+ authentication server, sometimes called TACACS+ daemon or simply TACACS+D.

The TACACS+ server is generally a program running on a host. The host determines whether to accept or deny the request and sends a response back. A Network Access Server (NAS) operates as a TACACS+ Client.

TACACS+ services (the user and group profiles with the authentication and the authorization information) are maintained in a central security database on a TACACS+ daemon running typically on a UNIX or Windows NT workstation. TACACS+ is commonly used for embedded network devices such as routers, modem servers, switches, etc.

## 12.1 Default Configurations

Feature	Default Setting
<code>tacacs-server timeout</code>	5 seconds
<code>login authentication</code>	Local

## 12.2 TACACS Command Hierarchy

```
+root

+ config terminal

    -[no] tacacs-server host {ipv4-
address} [timeout <5,(1-255)>] [key
<secret-key-string>]

- tacacs-server host {ipv4-address}                {port <40,(1-65535)>}
- tacacs-server retransmit <2,(1-100)>
    - [no] tacacs use-server address{ipv4-address }

    - [no] login authentication tacacs [local]

- show tacacs
- show system-information
- show running-config tacacs
```

## 12.3 TACACS Commands Descriptions

Command	Description
tacacs-server host	<p>This command configures the TACACS server with the parameters (host, timeout, key) and specifies the IP address of one or more TACACS and it specifies the names of the IP host or hosts maintaining a TACACS+ server. The no form of the command deletes server entry from the TACACS server table.</p> <p><b>&lt;ipv4-address&gt;:</b> Configures the IPv4 address of the host.</p> <p><b>Port &lt;tcp port (1- 65535 )&gt;:</b> Configures the TCP port number in which the multiple sessions are established. The value ranges between 1 and 65535.</p> <p><b>Timeout &lt;time out in seconds(1-255)&gt;:</b> Configures the time period (in seconds) till which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded. The value ranges from 1 to 255 seconds.</p> <p><b>Key &lt;secret key&gt;:</b> Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64.</p> <ul style="list-style-type: none"> <li>• <i>should be 1-64 characters length.</i></li> <li>• <i>May include small letters.</i></li> <li>• <i>May include capitol letter.</i></li> </ul>

## 12.4 TACACS Command Hierarchy

```
+root
+ config terminal
    -[no] tacacs-server host {ipv4-
address} [timeout <5,(1-255)>] [key
<secret-key-string>]
- tacacs-server host {ipv4-address}          {port <40,(1-65535)>}
- tacacs-server retransmit <2,(1-100)>
    - [no] tacacs use-server address {ipv4-address }
        - [no] login authentication tacacs [local]
- show tacacs
- show system-information
- show running-config tacacs
```



## 12.5 TACACS Commands Description

Command	Description
tacacs-server host	<p>This command configures the TACACS server with the parameters (host, timeout, key) and specifies the IP address of one or more TACACS and it specifies the names of the IP host or hosts maintaining a TACACS+ server. The no form of the command deletes server entry from the TACACS server table.</p> <p><b>&lt;ipv4-address&gt;:</b> Configures the IPv4 address of the host.</p> <p><b>Port &lt;tcp port (1- 65535 )&gt;:</b> Configures the TCP port number in which the multiple sessions are established. The value ranges between 1 and 65535.</p> <p><b>Timeout &lt;time out in seconds(1-255)&gt;:</b> Configures the time period (in seconds) till which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded. The value ranges from 1 to 255 seconds.</p> <p><b>Key &lt;secret key&gt;:</b> Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64.</p> <ul style="list-style-type: none"> <li>• Should be 1-64 characters length.</li> <li>• May include small letters.</li> <li>• May include capitol letter.</li> <li>• Must include numbers</li> <li>• May include special symbol.</li> <li>• Allowed symbols are @#\$\$%^&amp;*()-+./&lt;\'</li> </ul> <p>Defaults: port - 40, Timeout - 5 seconds</p>
tacacs use-server address	<p>This command configures the server IP address and an active server from the list of servers available in the TACACS server table. The no form of the command disables the configured client active server.</p> <p><b>&lt;ipv4-address&gt;:</b> Configures the IPv4 address of the host.</p>
tacacs-server retransmit	<p>Number of times the client searches the active server from the list of servers maintained in the TACACS client. The retransmit value ranges from 1 to 100 seconds.</p> <p>Defaults: 2 seconds</p>
debug tacacs	<p>This command sets the debug trace level for TACACS client module. The no form of the command disables the debug trace level for TACACS client module.</p> <p><b>All:</b> Generates debug messages for all possible traces (Dumprtx, Dumphrx, Error,</p>

Command	Description
	<p>Info).</p> <p><b>Info:</b> Generates debug statements for server information messages such as TACACS session timed out, server unreachability, Session ID exceeded and so on.</p> <p><b>Errors:</b> Generates debug statements for error debug messages such as failure caused during packet transmiSG18GFPion and reception.</p> <p><b>Dumptx:</b> Generates debug statements for handling traces. This trace is generated when there is an error condition in transmutation of packets.</p> <p><b>Dumprx:</b> Generates debug statements for handling traces. This trace is generated when there is an error condition in reception of packets.</p> <p>Defaults: Debugging is Disabled</p>
show tacacs	<p>This command displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.</p>

## 12.6 Configuration Example

### 1. Configure server list

```
iSG18GFP(config)# tacacs-server host 172.18.212.210 key secretkey
```

```
iSG18GFP(config)# tacacs-server host 172.18.212.49 timeout 5 key secretkey
```

### 2. Configure default server

```
iSG18GFP(config)# tacacs use-server address 172.18.212.210
```

### 3. Set default login authentication method

```
iSG18GFP(config)# login authentication tacacs local
```

```
iSG18GFP(config)# end
```

```
iSG18GFP# write startup-cfg
```

### 4. Remove tacacs configuration

```
config
```

```
no tacacs use-server
```

```
no tacacs-server host 172.18.212.210
```

```
login authentication local
```

### 5. Output example

```
iSG18GFP# show tacacs
```

```
Server : 1
```

```
Server address : 172.18.212.49
```

```
Address Type : IPV4
```

```
Single Connection : no
```

```
TCP port : 49
```

```
Timeout : 5
```

```
Secret Key :
```

```
Server : 2
```

```
Server address : 172.18.212.210
```

```
Address Type : IPV4
```

```
Single Connection : no
```

```
TCP port : 49
```

```
Timeout : 5
```

```
Secret Key :
```

```
Active Server address: 172.18.212.210
```

## 802.1x

802.1X defines a client-server based access control and authentication protocol. It provides a means of authenticating and authorizing devices attached to a port, thus preventing access to unauthorized clients. The authentication server authenticates each client connected to a switch port before allowing any services offered by the switch.

Until the client is authenticated, 802.1X access control allows only EAPOL (Extensible Authentication Protocol over LAN) traffic through the port on which the client is connected. When the port connecting the client (Port-Based authentication) is authenticated, normal traffic is allowed through the port. If MAC based authentication is enabled on the port, and if the Client MAC-address session is authenticated, then the traffic from the client is allowed.

### 13.1 x Commands Hierarchy

```
+ root

+ config terminal

- [no] aaa authentication dot1x default { group {radius | tacacsplus | tacacs+}
| local }

- [no] dot1x local-database <username> password <password> permission {allow | deny} [<auth-
timeout (value(1-7200))>] [interface <interface-type> <interface list>]

- [no] dot1x system-auth-control

- [no] shutdown dot1x

- [no] dot1x timeout {quiet-period <value (0-65535)> | {reauth-period | servertimeout | supp-
timeout | tx-period | start-period | held-period | auth- period} <value (1-65535)>}

+ interface <type> <id>

- [no] dot1x max-req <count(1-10)>

- [no] dot1x max-start <count(1-65535)>

- [no] dot1x reauthentication

- [no] dot1x port-control {auto|force-authorized|force-unauthorized}

- [no] dot1x auth-mode {port-based | mac-based}

- show dot1x [{ interface <interface-type> <interface-id> | statistics interface
<interface-type> <interface-id> | supplicant-statistics interface <interfacetype>
<interface-id>|local-database | mac-info [address <aa.aa.aa.aa.aa.aa>] |mac-
statistics [address <aa.aa.aa.aa.aa.aa>] | all ]}]
```

## 13.2 802.1x Commands Description

Command	Description
config terminal	Enters the Configuration mode.
aaa authentication dot1x default	<p>This command enables the dot1x local authentication or RADIUS server or TACACS PLUS server based remote authentication method for all ports. The actual authentication of the supplicant happens at the authentication server.</p> <p>The no form of the command disables dot1x in the switch.</p> <p><b>radius</b> - Configures Radius as the authentication server. Radius offers Authentication, Authorization and Accounting management for computers to access a network.</p> <p><b>tacacsplus</b> - Configures TACACS PLUS as the remote authentication server. Tacacs offers Authentication, Authorization and Accounting management for computers to access a network.</p> <p>This is mainly used for backward compatibility.</p> <p><b>tacacs+</b> - Configures TACACS+ as the authentication server. This feature has been included to adhere to the Industry Standard CLI syntax.</p> <p><b>local</b> - Configures Local authentication as the authentication mode. It provides authentication based on usernames and password using EAPMD5 authentication mechanism.</p>
dot1x local-database	<p>This command configures dot1x authentication server local database with user name and password. The no form of the command deletes an entry from the dot1x authentication server database.</p> <p><b>&lt;username&gt;</b> - Configures the User name for the new entry in the database.</p> <p><b>password&lt;password&gt;</b> - Configures the Password for the new entry in the database.</p> <p><b>permission-</b> Configures the permission for access for the user on a set of ports.</p> <p>The options are:</p> <p>Allow- Provides access to the user</p>
	<p>Deny- Denies access to the user.</p> <p><b>&lt;auth-timeout(value(1-7200))&gt;</b> - Configures the time in seconds after which the authentication allowed to the user expires.</p> <p>Maximum value is 7200 seconds. When the timeout value is 0, the authenticator uses the re-authentication period of the authenticator port.</p> <p><b>&lt;interface-type&gt;</b> - Configures the interface type for the specified type of interface.</p> <p>Default : Permission - allow interface-list - all</p>
dot1x system-auth-control	<p>This command enables dot1x in the switch. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames. The no form of this command disables dot1x in the switch.</p>

Command	Description
	Default - enabled
shutdown dot1x	This command shuts down dot1x feature. By shutting down the dot1x feature, the supplicant authenticator- authentication server architecture is dissolved. The data transport and authentication are directly governed by the authentication server/server. When shutdown, all resources acquired by dot1x module are released to the system. The no form of the command starts and enables dot1x  Default - enabled
dot1x timeout	This command sets the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, starts and stops timer. It provides handlers to respective expired timers.  Default - 60 seconds
Interface <type> <id> dot1x max-req	This command sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10.  The no form of the command sets the maximum number of EAP retries to the client to default value Default - 2
dot1x max-start	This command sets the maximum number of EAPOL retries to the authenticator. The no form of the command sets the maximum number of EAPOL retries to the authenticator to its default value. The value range is 1 to 65535.  Default - 3
dot1x reauthentication	This command enables periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually.  Default - Periodic re-authentication is disabled
dot1x port-control	This command configures the authenticator port control parameter. The dot1x exercises port based authentication to increase the security of the network. The different modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports.  The no form of the command sets the authenticator port control state to force authorized  <b>auto</b> - Configures the 802.1x authentication process in this port.  Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an <b>EAPOL-start</b> frame is received. The switch requests the identity of the

Command	Description
	<p>client and begins relaying authentication messages between the client and the authentication server. The switch can uniquely identify each client attempting to access the network by the client's MAC address.</p> <p><b>force-authorized</b> - Configures the port to allow all traffic through this port. Disables 802.1X authentication and causes the port.</p> <p>to transit to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client.</p> <p><b>forceunauthorized</b>- Configures the port to block all traffic through this port. Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.</p> <p>Default – force-authorized</p>
dot1x auth-mode	<p>This command configures the authentication mode of a port as either port-based (which is also known as multi-host) or mac-based (which is also known as single-host). Port based authentication has different modes of authentication. MAC based authentication allows secured mac addresses to pass through the port. Non secure mac addresses are dropped.</p> <p>The no form of the command configures the port authentication mode to its default values.</p> <p><b>port-based</b> - Configures the port's authentication mode to Port-based.</p> <p>The port authenticates the host to use the restricted resource. The port state is changed to authorize. The traffic flows through the port without any access restriction till any event that causes the port state to become unauthorized.</p> <p><b>mac-based</b> - Configures the port to MAC-based authentication. On receiving tagged/untagged data/control frames from the CFA Module, it checks if the source MAC is present in the Authenticator Session Table and is authorized.</p> <p>If it is present in the table and is authorized, the result is passed to CFA, which then forwards the frame to the appropriate destination module.</p> <p>If it is present in the table but not authorized, the CFA Module is intimated and the frame is dropped at the CFA Module.</p> <p>If neither of the above occurs, the Authenticator will initiate a new authentication session for that source MAC address and return the unauthorized status to the CFA Module, which then drops the frame</p> <p>Default - port based</p>

## 13.3 Examples

### 1.Port based authentication with RADIUS

```
configure terminal
dot1x system-auth-control
aaa authentication dot1x default group radius
radius-server host 172.18.212.142 timeout 20 retransmit 20 key 12345
interface fa 0/5
dot1x port-control auto
end
```

### 2.Port based authentication with local database

```
configure terminal
dot1x system-auth-control
dot1x local-database fsoft password admin123 permission allow
dot1x local-database fsoft1 password admin123 permission deny
interface fa 0/5
dot1x port-control auto
end
```

### 3.MAC based authentication with RADIUS

```
configure terminal
dot1x system-auth-control
aaa authentication dot1x default group radius
radius-server host 172.18.212.142 timeout 20 retransmit 20 key 12345
interface fa 0/5
dot1x port-control auto
dot1x auth-mode mac-based
end
```

### 4.MAC based authentication with local database

```
configure terminal
dot1x system-auth-control
dot1x local-database fsoftA password admin123 permission allow
dot1x local-database fsoftB password admin123 permission allow
dot1x local-database fsoftC password admin123 permission allow
onterface fa 0/5
dot1x port-control auto
dot1x auth-mode mac-based
end
```



# IGMP Snooping

Internet Group Multicast Protocol (IGMP) is a protocol used by a host to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGMP Snooping (IGS) is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. The multicast packet transfer happens only between the source and the destination computers. Broadcasting of packets is avoided. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

## 14.1 IGS Commands Hierarchy

```
+ root

+ config terminal

- [no] shutdown snooping

- [no] ip igmp snooping [vlan <vlanid>]

- [no] ip igmp snooping clear counters [vlan <vlanid>]

- [no] ip igmp snooping group-query-interval <(2,2 - 5) seconds>

- [no] ip igmp snooping mrouter-time-out <(125,60 - 600) seconds>

- [no] ip igmp snooping port-purge-interval <(260,130 - 1225) seconds>

- [no] ip igmp snooping query-forward {all-ports | non-router-ports}

- [no] ip igmp snooping report-forward {all-ports | router-ports | non-edge-ports}

- [no] ip igmp snooping retry-count <1 - 5>

- [no] ip igmp snooping send-query { enable | disable }

- [no] ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>

- [no] ip igmp snooping vlan <vlanid(1-4094)> immediate-leave

+ [no] vlan <vlan id>

    - [no] ip igmp snooping

        - ip igmp snooping fast-leave

        - ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>

        - ip igmp snooping mrouter-port <ifXtype> <iface_list> version {v1 | v2 | v3}

        - ip igmp snooping static-group <mcast_addr> ports <ifXtype><iface_list>

ip igmp snooping version {v1 | v2 | v3}
```

## 14.2 IGS Commands Description

Command	Description
config terminal	Enters the Configuration mode.
[no] shutdown snooping	Enable /disable snooping at the switch.  default: enabled (no shut)
[no] ip igmp snooping [vlan<vlanid(1- 4094)>]	This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode. The no form of the command deletes the IP access-list.  <b>default:</b> IGMP snooping is globally disabled, and in all VLANs.
[no] ip igmp snooping clear counters [vlan <vlanid>]	This command clears the IGMP snooping statistics maintained for VLAN(s).
[no] ip igmp snooping group-query- interval	This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database.  <b>default:</b> 2 seconds
ip igmp snooping mrouter-time-out	This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learnt router port. The router sends control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds.  <b>default:</b> 125 seconds
ip igmp snooping port-purge-interval	This command configures the IGMP snooping port purge time interval. When the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds.  <b>default:</b> 260 seconds
ip igmp snooping query-forward	This command configures the IGMP queries to be forwarded to all VLAN member ports or only to non-router ports. This configuration directs the queries to the selected ports to avoid flooding of the network. The queries are

Command	Description
	forwarded to multicast groups. If the VLAN module is enabled, IGMP snooping sends and receives the multicast packets through VLAN module.  Defaults: non-router-ports
ip igmp snooping report-forward	This command configures the IGMP reports to be forwarded to all ports, router ports of a VLAN or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network.  Defaults: router-ports
ip igmp snooping retry-count	This command sets the maximum number of group specific queries sent by the switch to check if there are any interested v2 receivers for the group when it receives a leave message in the proxy/ proxy-reporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number.  Defaults: 2
ip igmp snooping send-query	This command configures the IGMP general query transmission feature upon the topology change in the switch.
ip igmp snooping vlan <> mrouter	This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, if IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.
	Any IGMP message received on a switch is forwarded only on the router-ports and not on host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.
ip igmp snooping vlan<> immediate- leave	This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094.
Vlan <id>	
[no] ip igmp snooping	This command enables IGMP snooping in the switch/ a specific VLAN. When snooping is enabled in a switch or interface, it learns the hosts intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it

Command	Description
	forwards the packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all existing VLAN interfaces.
ip igmp snooping fast-leave	This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled.  When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received.
ip igmp snooping mrouter	This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, when IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.  Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.
ip igmp snooping mrouter-port	This command configures the router port purge time-out interval for a VLAN. The time interval after which the proxy assumes there are no v1/v2 routers present on the upstream port. While the older querier timer is running, the proxy replies to all queries with consolidated v1/v2 reports. When the timer expires, if the v2/v3 queriers are not present and the port is dynamically learnt, the port is purged. If the port is static, router port, the proxy replies to all queries with new version of v2/v3 consolidated reports.
ip igmp snooping version	This command configures the operating version of the IGMP snooping switch for a specific VLAN. The version can be set manually to execute condition specific commands.  <b>Default:</b> v3

## 14.3 Example

The following setup is an example for IGMP setup and configuration.

The server sends multicast traffic with group 225.0.0.70 and port 2222.

The client and server ports are members of VLAN 5. IGMP snooping is enabled on both these ports. Port 0/1 is set as mrouter port.

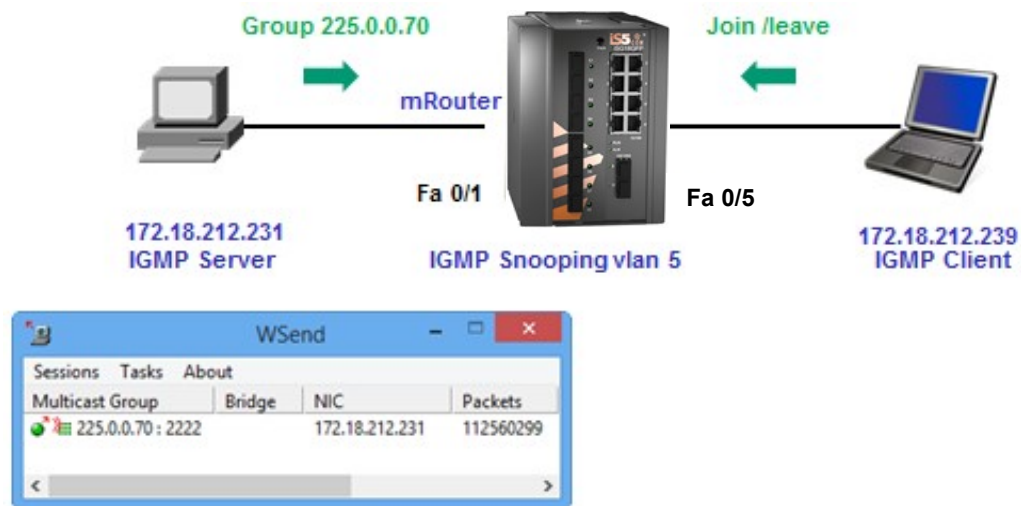


Figure 14-1: IGMP Setup and Configuration

## Switch Configuration

### 1.Create the service vlan

```
Config
```

```
Vlan 5
```

```
Port fastethernet 0/1,0/5 untagged fastethernet 0/1,0/5 Exit
```

```
Interface fastethernet 0/1
```

```
Switchport pvid 5
```

```
Exit
```

```
Interface fastethernet 0/5 Switchport pvid 5
```

```
Exit
```

### 2. Enable igmp snooping .2

```
ip igmp snooping
```

### 3.activate igmp snooping on vlan 5

```
ip igmp snooping vlan 5 mrouter fastethernet 0/1
```

```
vlan 5
```

```
ip igmp snooping mrouter fastethernet 0/1 end
```

```
write startup-cfg
```

#### 4. Output result after client "join" request

```
iSG18GFP# show ip igmp snooping forwarding-database
```

Vlan	MAC-Address	Ports
------	-------------	-------

-----

5	01:00:5e:00:00:46	Fa0/1, Fa0/5
---	-------------------	--------------

5	01:00:5e:7f:ff:fa	Fa0/1, Fa0/5
---	-------------------	--------------

Total Group Mac entries = 2

Output result after client "leave" request

```
iSG18GFP# show ip igmp snooping forwarding-database
```

Vlan	MAC-Address	Ports
------	-------------	-------

-----

5	01:00:5e:7f:ff:fa	Fa0/1, Fa0/5
---	-------------------	--------------

Total Group Mac entries = 1

# ACLs

ACLs (Access Control Lists) configured in the GCE environment filter network traffic by forwarding or blocking IP packets at the router's interfaces. The router evaluates each packet based on the criteria specified within the access lists. ACL criteria can be the source address, the destination address, the upper-layer protocol or other information as specified below.

ACLs can be used to restrict contents of routing updates or to provide traffic flow control. ACLs should be used to provide a basic level of security for accessing the network. For example, ACLs can allow one host to access a part of the network and prevent another host from accessing the same area.

## 15.1 ACL Flow validation at a port

Access lists are divided in to two main types: IP based and MAC based. Each ACL contains the following information:

- Action: allow or deny.
- Priority (1-255). Applies to extended ACLs only.
- Rule: the condition for the packet to be validated with. Only one rule can be defined per ACL.
- Sub action: optional for additional traffic manipulation.

At the port level, the ACL assignment is referred to as ACG (Access Group). The ACGs are also separated to IP and MAC, relating to the matching ACL types.

A packet arriving at incoming direction to a port will be evaluated using the steps below:

### IP based ACG entries


- a. The order of execution between multiple ACGs is derived from the ACL priority set at each individual ACL.
- b. Only the priority value determines the order of execution at the port, not the ACL number neither its name.
- c. At any and all ports to which IP ACGs are assigned, the operating system automatically creates the last rule of "permit ip any any". This rule allows all other IP traffic which was not addressed by user ACLs to enter the port.
- d. IP ICMP ACLs are subset of IP ACLs and follow the same priority based flow of execution between them.

### MAC based ACG entries


- a. The order of execution between multiple ACGs is derived from the ACL priority set at each individual ACL.
- b. The ACL number or its name, does not determine or affect the order of execution at the port.
- c. At any and all ports at which MAC ACGs are assigned, the operating system automatically creates the last rule of "permit mac any any". This rule allows all other MAC and Ether-Type traffic which was not addressed by user ACLs to enter the port.


To add a rule of blocking all traffic which is not explicitly permitted, use a MAC based ACL of "deny any any".

When implementing MAC based ACLs, consider permitting ARP traffic explicitly as dropping this traffic entirely may result in unintentional connections failure.

 The way to control the order of execution of ACGs at a port is to define a priority for each ACL. The lower the number (range 1-255), the higher the priority. The ACL with lower number (higher priority) would be executed before ACL with higher number (lower priority). For example, priority 1 would be executed before priority 255."

 IP ACGs are executed first at a port, then MAC ACGs.

 Only ACLs of IN direction are supported.

 IP ACLs of 'standard' type are not supported in current version

## 15.2 GCE ACL Commands Hierarchy

```
+ config terminal

+[no] ip access-list standard {<string(20)>} [[description <string(64)>]]

- permit {any|host <src-ip-address>|<src-ip-address><mask>}}{any|host <dest-ip-address>|<dest-ip-
address><mask>}} {priority <1-255>}[redirect {interface ifXtype
<ifnum>}}[sub-action {modify-vlan <short (1-4094)>}}]

- deny {any | host <src-ip-address> | <src-ip-address> <mask> } {any | host <dest-ip-address> | <dest-ip-
address> <mask>}} {priority <1-255>}

+[no] ip access-list extended {<string(20)> | [description < string(64)>]}

- {permit| deny} {ip | ospf | <protocol-type (1-255)> } {any | host <src-ip-address>
| <src-ip-address> <mask> } {any | host <dest-ip-address> | <dest-ip-
address>
<mask> } {priority <1-255>}

- {permit| deny} icmp {any | host <src-ip-address>|<src-ip-address> <mask> } {any | host <dest-ip-address> |
<dest-ip-address> <mask> } [<message-type (0-255)>] [<message-code (0-255)>] {priority <value (1-255)>}
[svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-
7)>] [{single-tag | double-tag}] [redirect {interface <ifXtype>
<ifnum>}} [sub- action {modify-vlan <short (1-4094)>}}]

- {permit| deny} tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number(1-
65535)> | lt <port-number(1-65535)> | eq <port-number(1-65535)>
| range <port-number(1-65535)><port-number(1-65535)>}}] {any | host <dest-
ip- address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-
65535)> | lt <port- number(1-65535)> | eq <port-number(1-65535)> | range
<port-number(1-65535)><port- number(1-65535)>}}] [{ack|rst}] [{tos{max-
reliability|max-throughput|min- delay|normal|<tos-value(0-7)>}} | dscp
<value (0-63)>}}] {priority <short (1- 255)>}[svlan-id <vlan-id (1-4094)>]
[svlan-priority <value (0-7)>] [cvlan-id <vlan- id (1-4094)>] [cvlan-
priority <value (0-7)>] [{single-tag | double-tag}] [redirect
{interface <ifXtype> <ifnum>}}] [sub-action {modify-vlan <short (1-4094)>}}]

- {permit | deny} udp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number(1-
65535)> | lt <port-number(1-65535)> | eq <port number(1- 65535)> | range <port-number (1-
65535)><port-number (1-65535)>}}] {any | host
<dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number
(1-65535)> | lt <port-number (1-65535)> | eq <port-number(1-65535)> |
range <port-number(1- 65535)> <port-number(1-65535)>}}] [{tos{max-
reliability|max-throughput|min- delay|normal|<tos-value(0-7)>}} | dscp
<value (0-63)>}}] {priority <1-255>} [svlan-id
<vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id
(1-4094)>] [ cvlan-priority <value (0-7)>] [ { single-tag | double-tag
} ] [redirect {interface
<ifXtype> <ifnum>}}] [sub-action {modify-vlan(1-4094)}}]

+[no] mac access-list extended {<string (20)> | [description <string(64)>]}

- {permit | deny}{any | host <src-mac-address>}{any | host <dest-mac-address>}
[{ aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-
6000 | etype- 8042 | lat | lavc-sca | mop-console | mop-dump | msdos |
mumps | netbios | vines- echo | vines-ip | xns-id | <short (0-65535)>}}]
[encaptype(1-65535)] [vlan <vlan-id (1-4094)>] {priority <1-255>}
[outerEtherType(1-65535)] [svlan-id
<vlan-id (1-
```



```

4094)>] [cvlan-priority <value (0-7)>] [svlan-priority <value (0-7)>]
[{single-tag
| double-tag}}] [redirect {interface <ifXtype>      <ifnum>}] [sub-action
{modify-vlan (1-4094)}}]
+ interface <port type> <port ID>

-[no] ip access-group <string (20)> in

-[no] mac access-group <string (20)> in

- show access-lists [[[ip | mac | user-defined ]] <access-list-number (1-65535)>]

- show running-config acl

```

## 15.3 GCE ACL Commands Description

Command	Description
config terminal	Enters the Configuration mode.
[no] ip access-list standard	<p>This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode. The <b>no</b> form of the command deletes the IP access-list.</p> <p>The ACL identifier is a name of up to 20 characters.</p> <p><b>Description:</b> Optional parameter, specifies a description of the ACL, up to 64 characters long.</p>

Command	Description
permit	<p>The standard permit command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.</p> <p><b>any   host &lt;src-ip-address&gt;   &lt;src-ip-address&gt;&lt;mask&gt;</b>: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address.</p> <p><b>any   host &lt;dest-ip-address&gt;   &lt;dest-ip-address&gt;&lt;mask&gt;</b>: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address.</p> <p><b>Redirect</b>: Redirects the action to the destination interface or set of interfaces:  <b>ifXtype</b> - Specifies the interface type,  <b>ifnum</b> - Specifies the interface number.</p> <p><b>sub-action</b>: Specifies the VLAN specific sub action to be performed on the packet:  none - Actions relating to the VLAN ID will not be considered, <b>modify-vlan</b> - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet. nested-vlan - Adds an outer VLAN tag to the packet with the VLAN ID as configured.</p> <p><b>priority</b>: lower value implies a higher priority. Default -1. Although this is a required parameter it is disregarded in standard ACL (auto priority 0).</p>
deny	<p>This command denies traffic if the conditions defined in the deny statement are matched.</p> <p><b>any   host &lt;src-ip-address&gt;   &lt;src-ip-address&gt;&lt;mask&gt;</b>: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address.</p> <p><b>any   host dest-ip-address   &lt;network-destip&gt;&lt;mask&gt;</b>: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address.</p> <p><b>priority</b>: lower value implies a higher priority. Default -1. Although this is a required parameter it is disregarded in standard ACL (auto priority 0).</p>

Command	Description
[no] ip access-list extended	<p>Extended access lists enable specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters), and additional parameters as specified below. The <b>no</b> form of the command deletes the IP access-list.</p> <p>The ACL identifier is a name of up to 20 characters.</p> <p><b>Description:</b> Optional parameter, specifies a description of the ACL, up to 64 characters long.</p>
permit  deny	<p>This command forwards (or drops for deny) all protocol specific traffic between specified source and destination. The protocol can be specified as <b>ip</b>, <b>ospf</b> or any number between 1 and 255</p> <p><b>any   host &lt;src-ip-address&gt;   host &lt;src-ip-address&gt;&lt;mask&gt;</b>: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP and the network mask to use with the source IP address.</p> <p><b>any   host &lt;dest-ip-address&gt;   host &lt;dest-ip-address&gt;&lt;mask&gt;</b>: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address.</p> <p><b>priority</b>: 0 to 255. Lower value implies a higher priority. Default -1.</p>
permit icmp, deny icmp	<p>This command specifies the ICMP packets to be forwarded (or dropped for deny command) based on the IP address and the associated parameters.</p> <p><b>any   host &lt;src-ip-address&gt;   host &lt;src-ip-address&gt;&lt;mask&gt;</b>: Source IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the source IP address.</p> <p><b>any   host &lt;dest-ip-address&gt;   host &lt;dest-ip-address&gt;&lt;mask&gt;</b>: Destination IP address can be: 'any', or the word 'host' followed by a dotted decimal IP address, or the network IP address and the network mask to use with the destination IP address.</p> <p><b>message-type</b>: ICMP Message type</p> <p><b>message-code</b>: ICMP Message code</p>

Command	Description
	<p><b>priority:</b> 0 to 255. Lower value implies a higher priority. Default -1.</p> <p><b>svlan-id</b> &lt;vlan-id (1-4094)&gt; - allows or denies packets with the specified server VLAN ID</p> <p><b>svlan-priority</b> &lt;value (0-7)&gt;: allow/deny packets for outer VLAN with specified priority.</p> <p><b>cvlan-id</b> &lt;vlan-id (1-4094)&gt; allows or denies packets with the specified client (nested) VLAN ID</p> <p><b>cvlan-priority</b> &lt;value (0-7)&gt;: allow/deny packets for inner VLAN with specified priority.</p> <p><b>single-tag   double-tag:</b> allows/denies single tagged or double tagged packets</p> <p><b>Redirect:</b> Redirects the action to the destination interface. ifXtype - Specifies the interface type. ifnum - Specifies the interface number.</p> <p><b>sub-action:</b> Specifies the VLAN specific sub action to be performed on the packet: none - Actions relating to the VLAN ID will not be considered. modify-vlan - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</p>
<p>permit tcp, deny tcp</p>	<p>the TCP RST bit will not be checked to decide the action)</p> <p>Tos: Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7. Default value is 0.</p> <p>Dscp: Differentiated services code point provides the quality of service control. The various options available are:</p> <ul style="list-style-type: none"> <li>• 0-63 - Differentiated services code point value.</li> </ul> <p>The parameters newly added in the existing commands for industry standard CLI are:</p> <ul style="list-style-type: none"> <li>• af11 - Matches packets with AF11 DSCP (001010)</li> <li>• af12 - Matches packets with AF12 DSCP (001100)</li> <li>• af13 - Matches packets with AF13 DSCP (001110)</li> <li>• af21 - Matches packets with AF21 DSCP (010010)</li> <li>• af22 - Matches packets with AF22 DSCP</li> </ul>

Command	Description
	<p>(010100)</p> <ul style="list-style-type: none"> <li>• af23 - Matches packets with AF23 DSCP (010110)</li> <li>• af31 - Matches packets with AF31 DSCP (011010)</li> <li>• af32 - Matches packets with AF32 DSCP (011100)</li> <li>• af33 - Matches packets with AF33 DSCP (011110)</li> <li>• af41 - Matches packets with AF41 DSCP (100010)</li> <li>• af42 - Matches packets with AF42 DSCP (100100)</li> <li>• af43 - Matches packets with AF43 DSCP (100110)</li> <li>• cs1 - Matches packets with CS1 (precedence 1) DSCP (001000)</li> <li>• cs2 - Matches packets with CS2 (precedence 2) DSCP (010000)</li> <li>• cs3 - Matches packets with CS3 (precedence 3) DSCP (011000)</li> <li>• cs4 - Matches packets with CS4 (precedence 4) DSCP (100000)</li> <li>• cs5 - Matches packets with CS5 (precedence 5) DSCP (101000)</li> <li>• cs6 - Matches packets with CS6 (precedence 6) DSCP (110000)</li> <li>• cs7 - Matches packets with CS7 (precedence 7) DSCP (111000)</li> <li>• default - Default DSCP (000000)</li> <li>• ef - Matches packets with EF DSCP (101110)</li> </ul>
<p>permit tcp, deny tcp (cont).</p>	<p><b>priority:</b> 0 to 255. Lower value implies a higher priority. Default -1</p> <p><b>svlan-id</b> &lt;vlan-id (1-4094)&gt; - allows or denies packets with the specified server VLAN ID</p> <p><b>svlan-priority</b> &lt;value (0-7)&gt;: allow/deny packets for outer VLAN with specified priority.</p> <p><b>cvlan-id</b> &lt;vlan-id (1-4094)&gt; allows or denies packets with the specified client (nested) VLAN ID</p> <p><b>cvlan-priority</b> &lt;value (0-7)&gt;: allow/deny packets for inner VLAN with specified priority.</p> <p><b>single-tag   double-tag:</b> allows/denies single tagged or double tagged packets</p> <p><b>Redirect:</b> Redirects the action to the destination interface. <b>ifXtype</b> - Specifies the interface type. <b>ifnum</b> - Specifies the</p>

Command	Description
	<p>interface number.</p> <p><b>sub-action:</b> Specifies the VLAN specific sub action to be performed on the packet: none - Actions relating to the VLAN ID will not be considered. <b>modify-vlan</b> - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</p>
<pre>permit udp, deny udp</pre>	<p>This command specifies the UDP datagrams to be forwarded (or blocked for the deny command) based on the associated parameters.</p> <p>any   host &lt;src-ip-address&gt;   host &lt;src-ip-address&gt;&lt;mask&gt;: see permit   deny tcp command.</p> <p><b>port-number:</b> see permit   deny tcp command.</p> <p>any   host&lt;dest-ip-address&gt;   &lt;dest-ip-address&gt;&lt;dest-mask&gt;: see permit   deny tcp command.</p> <p><b>Tos:</b> see permit   deny tcp command.</p> <p><b>Dscp:</b> see permit   deny tcp command.</p> <p><b>priority:</b> see permit   deny tcp command.</p> <p><b>svlan-id:</b> see permit   deny tcp command.</p> <p><b>svlan-priority:</b> see permit   deny tcp command.</p> <p><b>cvlan-id:</b> see permit   deny tcp command.</p> <p><b>cvlan-priority:</b> see permit   deny tcp command.</p> <p><b>single-tag   double-tag:</b> see permit   deny tcp command.</p> <p><b>Redirect:</b> see permit   deny tcp command.</p> <p><b>sub-action:</b> see permit   deny tcp command</p>
[no] mac access-list extended	<p>Creates Layer 2 MAC ACL and returns the MAC-Access list configuration mode to the user. The <b>no</b> form of the command deletes the MAC access-list.</p> <p>The ACL identifier is a name of up to 20 characters.</p> <p><b>Description:</b> Optional parameter, specifies a description of the ACL, up to 64 characters long.</p>

Command	Description
Permit   deny	<p>Main action to be set as permit or deny.</p> <p><b>any   host &lt;src-mac-address&gt;</b>: Source MAC address to be matched with the packet or 'any'.</p> <p><b>any   host &lt;dest-mac-address&gt;</b>: Destination MAC address to be matched with the packet.</p> <p><b>Redirect</b>: Redirects the action to the destination interface. <b>ifXtype</b> - Specifies the interface type. <b>ifnum</b> - Specifies the interface number.</p> <p><b>sub-action</b> - Specifies the VLAN specific sub action to be performed on the packet; none or <b>modify-vlan</b> : Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet.</p> <p><b>aarp   amber   dec-spanning   decnet-iv   diagnostic   dsm   etype-6000   etype-8042   lat   lavc-sca   mop-console   mop-dump   msdos   mumps   netbios   vines-echo   vines-ip   xns-id   &lt;short (0-65535)&gt;</b>:</p> <p><b>encaptype(1-65535)</b>:</p> <p><b>vlan &lt;vlan-id (1-4094)&gt;</b>: optional.</p> <p><b>priority &lt;1-255&gt;</b> : 0 to 255.Lower value implies a higher priority.</p> <p><b>outerEtherType(1-65535)</b> : Optional.</p> <p><b>svlan-id &lt;vlan-id (1-4094)&gt;</b> - allows or denies packets with the specified server VLAN ID</p> <p><b>svlan-priority &lt;value (0-7)&gt;</b>: allow/deny packets for outer VLAN with specified priority.</p> <p><b>cvlan-id &lt;vlan-id (1-4094)&gt;</b> allows or denies packets with the specified client (nested) VLAN ID</p> <p><b>cvlan-priority &lt;value (0-7)&gt;</b>: allow/deny packets for inner VLAN with specified priority.</p> <p><b>single-tag   double-tag</b>: allows/denies single tagged or double tagged packets</p>
interface <port type> <port ID>	Entering to the relevant interface to be configured.

Command	Description
[no] ip access-group <access-list-number (1-65535)> {in   out}	<p>This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.</p> <p><b>access-list-number:</b> IP access control list number</p> <p><b>in:</b> Inbound packets</p> <p><b>out:</b> Outbound packets</p>
-[no] mac access-group <access-list-number (1-65535)> in	<p>This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.</p> <p><b>access-list-number:</b> Access List Number</p> <p><b>in:</b> Inbound packets</p> <p><b>out:</b> Outbound packets</p>
show access-lists [{ip   mac   user-defined}] <access-list-number (1-65535)>]	<p>This command displays the access lists configuration.</p> <p><b>ip:</b> IP Access List</p> <p><b>mac:</b> MAC Access List</p> <p><b>user-defined:</b> user defined access list</p>



## 15.4 Configuration Examples

iSG18GFP# config terminal

**Example for IP ACL allowing specific IP traffic:**

```
iSG18GFP(config)# ip access-list extended 1001
iSG18GFP(config-1001)# permit ip any 172.18.212.0 255.255.255.0 priority 10
iSG18GFP(config-1001)# exit
iSG18GFP(config)# int fa 0/3
iSG18GFP(config-if)# ip access-group 1001 in
iSG18GFP(config-if)# end
```

**Example for IP ACL allowing specific IP traffic:**

```
iSG18GFP(config)# ip access-list extended 1001
iSG18GFP(config-1001)# permit ip host 10.10.10.10 host 11.11.11.11 priority 15
iSG18GFP(config-1001)# exit
iSG18GFP(config)# int fa 0/3
iSG18GFP(config-if)# ip access-group 1001 in
iSG18GFP(config-if)# end
```

**Example for IP ACL denying all IP traffic:**

```
iSG18GFP(config)# ip access-list extended 1002
iSG18GFP(config-1002)# deny ip any any priority 100
iSG18GFP(config-1002)# exit
iSG18GFP(config)# int fa 0/2
iSG18GFP(config-if)# ip access-group 1002 in
iSG18GFP(config-if)# end
```

**Example how to allow ICMP ACL:**

```
iSG18GFP(config)# ip access-list extended 1001
iSG18GFP(config-1001)# permit icmp any any priority 10
iSG18GFP(config-1001)# exit
iSG18GFP(config)# int fa 0/1
iSG18GFP(config-if)# ip access-group 1001 in
iSG18GFP(config-if)# end
```

**Example for MAC ACL:**

```
iSG18GFP(config)# mac access-list extended 1
iSG18GFP (config-1)#permit host 00:11:11:11:22:33 host 00:11:11:11:22:44 priority 10
iSG18GFP(config-1)# exit
iSG18GFP(config)# interface fastethernet 0/3
iSG18GFP(config-if)# mac access-group 1 in
iSG18GFP(config-if)# end
```

**Example for MAC ACL:**

```
iSG18GFP(config)# mac access-list extended 1
iSG18GFP(config-1)# permit any any priority 20
iSG18GFP(config-1)# exit
iSG18GFP(config)# interface fastethernet 0/3
iSG18GFP(config-if)# mac access-group 1 in
iSG18GFP(config-if)# end
```

**Example how to deny MAC Traffic ACL:**

```
iSG18GFP# config terminal
iSG18GFP(config)# mac access-list extended 25
iSG18GFP(config-ext-macl)# deny any any priority 250
iSG18GFP(config-ext-macl)# exit
iSG18GFP(config)# interface fastethernet 0/3
iSG18GFP(config-if)# mac access-group 25 in
iSG18GFP(config-if)# end
```

**Example TCP ACL:**

```
iSG18GFP# config terminal
iSG18GFP(config)# ip access-list extended tcp-502
iSG18GFP(config-tcp-502)# permit tcp any eq 502 any range 100 200 priority 10
iSG18GFP(config-tcp-502)# exit
iSG18GFP(config)# interface fastethernet 0/3
iSG18GFP(config-if)# ip access-group tcp-502 in
iSG18GFP(config-if)# end
```

**Example Redirect ACL:**

```
iSG18GFP# config terminal
iSG18GFP(config)# ip access list extended redirect_example
iSG18GFP(config-redirect_example)# permit ip host 1.1.1.1 host 2.2.2.2 priority
15 redirect interface fastethernet 0/4
iSG18GFP(config-redirect_example)# exit
iSG18GFP(config)# interface fastethernet 0/3
iSG18GFP(config-if)# ip access-group redirect_example in
iSG18GFP(config-if)# end
```

**Example how to allow ARP ACL:**

```
iSG18GFP# config terminal
iSG18GFP(config)# mac access-list extended 1
iSG18GFP(config-1)# permit any any 0x0806 priority 5
iSG18GFP(config-1)# exit
iSG18GFP(config)# interface fa 0/3
```

```
iSG18GFP(config-if)# mac access-group 1 in
iSG18GFP(config-if)# end
```

## 15.5 Flow Example

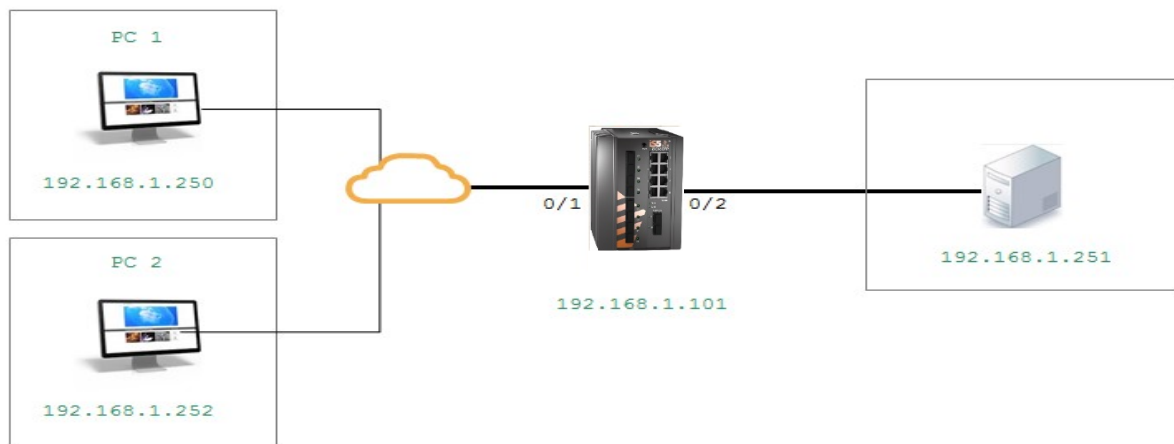


Figure 15-1: Flow Example

For the above setup, ACLs will be implemented at port fast 0/1 and traffic result will be reviewed.

### 15.5.1 Test 1

```
iSG18GFP(config)#
ip access-list extended 1010
permit ip host 192.168.1.250 host 192.168.1.101 priority 20
!
ip access-list extended 1020
deny ip any host 192.168.1.101 priority 10
!
interface fastethernet 0/1 ip access-group 1010 in
!
interface fastethernet 0/1 ip access-group 1020 in
```

#### Results

PC1 SSH management to the switch: blocked. PC1 ping to the switch: blocked.  
 PC1 ping to the server: allowed.  
 PC2 SSH management to the switch: blocked. PC2 ping to the switch: blocked.  
 PC2 ping to the server: allowed.

### 15.5.2 Test 2

```
iSG18GFP(config)#
ip access-list extended 1001 permit icmp any any priority 50
!
ip access-list extended 1010
```

```
permit ip host 192.168.1.250 host 192.168.1.101 priority 10
!
ip access-list extended 1020

deny ip any host 192.168.1.101 priority 20
!
interface fastethernet 0/1
ip access-group 1001 in
!
interface fastethernet 0/1 ip access-group 1010 in
!
interface fastethernet 0/1 ip access-group 1020 in
```

### Results

PC1 SSH management to the switch: allowed. PC1 ping to the switch: allowed.  
PC1 ping to the server: allowed.  
PC2 SSH management to the switch: blocked. PC2 ping to the switch: blocked.  
PC2 ping to the server: allowed.

## 15.5.3 Test 3

```
iSG18GFP(config)#
ip access-list extended 1001 permit icmp any any priority 5
!
ip access-list extended 1010
permit ip host 192.168.1.250 host 192.168.1.101 priority 30
!
ip access-list extended 1020
deny ip any host 192.168.1.101 priority 40
!
interface fastethernet 0/1 ip access-group 1001 in
!
interface fastethernet 0/1 ip access-group 1010 in
!
interface fastethernet 0/1 ip access-group 1020 in
```

### Results

PC1 SSH management to the switch: allowed. PC1 ping to the switch: allowed.  
PC1 ping to the server: allowed.  
PC2 SSH management to the switch: blocked. PC2 ping to the switch: allowed.  
PC2 ping to the server: allowed.

## 15.5.4 Test 4

```
iSG18GFP(config)#
ip access-list extended 1001 permit icmp any any priority 5
!

ip access-list extended 1010
permit ip host 192.168.1.250 host 192.168.1.101 priority 100
!
mac access-list extended 10 permit any any 2054 priority 1
!
mac access-list extended 100 deny any any priority 250
!

interface fastethernet 0/1 ip access-group 1001 in
!
interface fastethernet 0/1 ip access-group 1010 in
!
interface fastethernet 0/1 mac access-group 10 in
!
interface fastethernet 0/1
```

### Results

PC1 SSH management to the switch: allowed. PC1 ping to the switch: allowed.  
PC1 ping to the server: blocked.  
PC2 SSH management to the switch: blocked. PC2 ping to the switch: blocked  
PC2 ping to the server: allowed.

## 15.5.5 Test 5

```
iSG18GFP(config)#
ip access-list extended 1010
permit ip host 192.168.1.250 host 192.168.1.101 priority 100
!
mac access-list extended 10 permit any any 2054 priority 1
!
mac access-list extended 100 deny any any priority 20
!
interface fastethernet 0/1 ip access-group 1010 in
!
interface fastethernet 0/1 mac access-group 10 in
!
```

```
interface fastethernet 0/1
```

**Results**

PC1 SSH management to the switch: allowed. PC1 ping to the switch: allowed.

PC1 ping to the server: blocked.

PC2 SSH management to the switch: blocked. PC2 ping to the switch: blocked.

PC2 ping to the server: blocked.

# QOS

QoS (Quality of Service) defines the ability to provide different priorities to different applications, users or data flows or the ability to guarantee a certain level of performance to a data flow. QoS refers to resource reservation control mechanisms rather than the achieved service quality and specifies a guaranteed throughput level.

## 16.1 QOS Commands Hierarchy

```
+ config

- [no] shutdown qos

- qos {enable | disable}

- qos interface <iftype> <ifnum> def-user-priority <0-7>

- [no] priority-map <1-65535>

+ [no] class-map <1-65535>

- [no] set class <1-65535> [pre-color { green | yellow | red | none }] [regen-priority <0-7> group-name <string(31)> ]

+ [no] meter <1-65535>

- meter-type { simpleTokenBucket | avgRate | srTCM | trTCM | tswTCM | mefCoupled | mefDeCoupled } [color-mode { aware | blind }] [interval <short(1-10000)>] [cir <0-65535>] [cbs <0-65535>] [eir <0-65535>] [ebs <0-65535>] [next-meter 0-65535>]

+ [no] policy-map <1-65535>

- set policy [class <0-65535>] [interface <iftype> <ifnum>] defaultpriority-type { none | { vlanPri | ipTos } <0-63> }

- set meter <1-65535> [ conform-action { none | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | set-port <iftype> <ifnum> | setinner-vlan-pri <short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ exceed-action { drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | setinner-vlan-pri <short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] [ violateaction { drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | set-inner-vlan-pri <short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> } ] setconform-newclass <0-65535> ] [ set-exceed-newclass <0-65535> ] [ set-violate-newclass <0-65535> ]

- [no] queue-type <1-65535>

- set algo-type { tailDrop | headDrop | red | wred } [queue-limit <1-65535>] [queue-drop-algo {enable | disable }]

- [no] shape-template <1-65535> [cir <1-65535>] [cbs <0-65535>] [eir <0-65535>] [ebs <0-65535>]

- [no] scheduler <1-65535> interface <iftype> <ifnum> [sched-algo {strictpriority| rr | wrr | wfq | strict-rr | strict-wrr | strict-wfq | deficit-rr}] [shaper <0-65535>] [hierarchy-level <0-10>]

- [no] scheduler <1-65535> interface <iftype> <ifnum> [sched-algo {strictpriority| rr | wrr | wfq | strict-rr | strict-wrr
```

```
| strict-wfq | deficit-rr}}[shaper <0-65535>] [hierarchy-level < 0-10>]
- [no] queue < 1-65535> interface <iftyp> <ifnum>
    [qtype < 1-65535>][scheduler < 1-65535>] [weight <0-
    1000>] [priority <0-15>] [shaper <0-65535>]
- [no] queue-map { CLASS <1-65535> | regn-priority {vlanPri | ipTos} <0-63>} [interface <iftyp>
    <ifnum>] queue-id <1-65535>
- [no] sched-hierarchy interface <iftyp> <ifnum> hierarchy-level <1-10> sched-id <1-65535>
    {next-level-queue <0-65535> | next levelscheduler
    <0-65535>} [priority <0-15>] [weight <0-1000>]
+ [no] map [interface <iftyp> <ifnum>] [vlan <1-4094>] in-priority-type
    { vlanPri | ipTos } [in-priority <0-63>]regen-
    priority <0-63> [regen-inner-priority <0-7>]
+ match access-group { [mac-access-list <0-65535>] [ ip-access-list
    <0-65535>] | priority-map <0-65535> }

- show qos global info
- show priority-map [<priority-map-id(1-65535)>]
- show class-map [<class-map-id(1-65535)>]
- show class-to-priority-map <group-name(31)>
- show meter [<meter-id(1-65535)>]
- show policy-map [<meter-id(1-65535)>]
- show queue-template [<queue-template-id(1-65535)>]
- show shape-template [<shape-template-id(1-65535)>]
- show scheduler [interface <iftyp> <ifnum>]
- show queue [interface <iftyp> <ifnum>]
- show queue-map [interface <iftyp> <ifnum>]
- show sched-hierarchy [interface <iftyp> <ifnum>]
- show qos def-user-priority [interface <iftyp> <ifnum>]
- show qos meter-stats [<Meter-Id(1-65535)>]
- show qos queue-stats [interface <iftyp> <ifnum>]
```



## 16.2 QOS Commands Description

Command	Description
config terminal	Enters the Configuration mode.
shutdown qos	shuts down the QoS subsystem. The no form of the command starts the QoS subsystem.
qos	{enable   disable}  enables or disables the QoS subsystem.
priority-map	adds a Priority Map entry. The no form of the command deletes a Priority Map entry.  <b>Priority-map-Id</b> : Priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority. This value ranges between 1 and 65535
class-map	adds a Class Map entry. The no form of the command deletes a Class Map entry.  <b>class-map-id</b> : Index that enumerates the MultiField Classifier table entries. This value ranges between 1 and 65535.
meter	This command creates a Meter. The no form of the command deletes a Meter.  <b>meter-id</b> : Index that enumerates the Meter entries. This value ranges between 1 and 65535.
policy-map	creates a policy map. The no form of the command deletes a policy map.  <b>policy-map-id</b> : Index that enumerates the policy- map table entries. This value ranges between 1 and 65535.
queue-type	creates a Queue Template Type. The no form of the command deletes a Queue Template Type.  <b>Q-Template-Id</b> : Queue Template Table index. This value ranges between 1 and 65535.
shape-template	creates a Shape Template. The no form of the command deletes a Shape Template  <b>Shape-Template-Id</b> : Shape Template Table index.  <b>cir</b> : Committed information rate for packets through the queue.  <b>cbs</b> : Committed burst size for packets through the queue.  <b>eir</b> : Excess information rate for packets through the hierarchy.  <b>ebs</b> : Excess burst size for packets through the hierarchy
scheduler	creates a Scheduler and configures the Scheduler parameters. The no form of the command deletes a scheduler.  <b>Scheduler-Id</b> : Scheduler identifier that uniquely identifies

Command	Description
	<p>the scheduler in the system/egress interface</p> <p><b>Iftype</b> : Interface type</p> <p><b>Ifnum</b> : Interface number</p> <p><b>sched-algo</b> : Packet scheduling algorithm for the port. The algorithms are: strict-priority - strictPriority.</p> <p>-rr - roundRobin.</p> <p>-wrr - weightedRoundRobin.</p> <p>-wfg - weightedFairQueing.</p> <p>-strict-rr - strictRoundRobin.</p> <p>-strict-wrr - strictWeightedRoundRobin.</p> <p>-strict-wfg - strictWeightedFairQueing.</p> <p>-deficit-rr - deficitRoundRobin</p> <p><b>Shaper</b> : Shaper identifier that specifies the bandwidth requirements for the scheduler.</p> <p>hierarchy-level : Depth of the queue/scheduler hierarchy</p>
queue	<p>Creates a Queue and configures the Queue parameters. The no form of the command deletes a Queue.</p> <p><b>Queue</b> : Queue identifier that uniquely identifies the queue in the system/port.</p> <p><b>Iftype</b> : Interface type</p> <p><b>Ifnum</b> : Interface number</p> <p><b>Qtype</b> : Queue Type identifier.</p> <p><b>Scheduler</b> : Scheduler identifier that manages the specified queue.</p> <p><b>Weight</b> : User assigned weight to the CoS queue</p> <p><b>Priority</b> : User assigned priority for the CoS queue.</p> <p><b>Shaper</b> : Shaper identifier that specifies the bandwidth requirements for the queue.</p>
queue-map	<p>creates a Map for a Queue with Class or regenerated priority. The no form of the command deletes a Queue map entry.</p> <p><b>CLASS</b> : Input CLASS that needs to be mapped to an outbound queue.</p> <p><b>regn-priority</b> : Regenerated-priority type and regenerated-</p>

Command	Description
	<p>priority that needs to be mapped to an outbound queue. The types are</p> <ul style="list-style-type: none"> <li>vlanPri - VLAN Priority.</li> <li>ipTos - IP Type of Service.</li> </ul> <p><b>Iftype</b> : Interface type</p> <p><b>Ifnum</b> : Interface number</p> <p><b>queue-id</b> : Queue identifier that uniquely identifies a queue relative to an interface.</p>
sched-hierarchy	<p>This command creates a Scheduler Hierarchy. The no form of the command deletes a Scheduler Hierarchy</p> <p><b>hierarchy-level</b> : Depth of the queue/scheduler hierarchy</p> <p><b>sched-id</b> : Scheduler identifier.</p> <ul style="list-style-type: none"> <li>next-level-queue - Next-level queue to which the scheduler output needs to be sent.</li> <li>next-level-scheduler - Next-level scheduler to which the scheduler output needs to be sent.</li> </ul>
qos interface	<p>sets the default ingress user priority for the port.</p> <p><b>def-user-priority</b> : Default ingress user priority for the port.</p>
map	<p>This command adds a Priority Map Entry for mapping an incoming priority to a regenerated priority. The no form of the command sets default value to the Interface, VLAN, regenerated inner priority.</p> <p><b>in-priority-type</b> : Type of the incoming priority. The types are:</p> <ul style="list-style-type: none"> <li>vlanPri - VLAN Priority.</li> <li>ipTos - IP Type of Service.</li> <li>ipDscp - IP Differentiated Services Code Point.</li> </ul> <p><b>in-priority</b> : Incoming priority value determined for the received frame. This value ranges between 0 and 63.</p> <p><b>regen-priority</b> : Regenerated priority value determined for the received frame. This value ranges between 0 and 63.</p> <p><b>regen-innerpriority</b> : Regenerated inner-VLAN (CVLAN) priority value determined for the received frame. This value ranges between zero and seven.</p>

Command	Description
	<p>Defaults:</p> <p>Vlan - 0 in-priority-type - vlanPri in-priority - -1 regen-priority - 0</p>
match access-group	<p>This command sets Class Map parameters using L2and/or L3 ACL or Priority Map ID.</p> <p><b>mac-access-list</b> : Identifier of the MAC filter. This value ranges between 0 and 65535.</p> <p><b>ip-access-list</b> : Identifier of the IP filter. This value ranges between 0 and 65535.</p> <p><b>priority-map</b> : Priority Map identifier for mapping incoming priority against received packet. This value ranges between 0 and 65535.</p> <p>Defaults:</p> <p>mac-access-list - 0 ip-access-list- 0 priority-map- -1</p>
set class	<p>This command sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map entry with regenerated priority. The no form of the command deletes a CLASS to Priority Map Table entry.</p> <p><b>Class</b> : Traffic CLASS to which an incoming frame pattern is classified.</p> <p><b>pre-color</b> : Color of the packet prior to metering. This can be any one of the following:</p> <ul style="list-style-type: none"> <li>• None - Traffic is not pre-colored.</li> <li>• green - Traffic conforms to SLAs (Service Level Agreements).</li> <li>• yellow - Traffic exceeds the SLAs.</li> <li>• red - Traffic violates the SLAs.</li> </ul> <p><b>regen-priority</b> : Regenerated priority value determined for the input CLASS. This value ranges between zero and seven.</p> <p><b>group-name</b> : Unique identification of the group to which an input CLASS belongs.</p>
meter-type	<p>This command sets Meter parameters CIR, CBS, EIR, EBS, Interval, meter type and color awareness.</p> <p><b>simpleTokenBucket</b> - Two Parameter Token Bucket Meter</p> <p><b>avgRate</b> - Average Rate Meter.</p> <p><b>srTCM</b> - Single Rate Three Color Marker Metering as defined by RFC 2697.</p>

Command	Description
	<p><b>trTCM</b> - Two Rate Three Color Marker Metering as defined by RFC 2698 tswTCM</p> <p><b>color-mode</b> - Indicates the color mode of the Meter. The color modes are:</p> <p>*aware - The Meter considers the pre-color of the packet.</p> <p>*blind - The Meter ignores the pre-color of the packet.</p> <p><b>interval</b> - Time interval used with the token bucket. This value ranges between 1 and 10000.</p> <p><b>cir</b> - Committed information rate. This value ranges between 0 and 65535.</p> <p><b>cbs</b> - Committed burst size. This value ranges between 0 and 65535.</p> <p><b>eir</b> - Excess information rate. This value ranges between 0 and 65535.</p> <p><b>ebs</b> - Excess burst size. This value ranges between 0 and 65535.</p> <p><b>next-meter</b> - Meter entry identifier used for applying the second/next level of conformance on the incoming packet. This value ranges between 0 and 65535.</p>
set policy	<p>This command sets CLASS for policy. The no form of the command sets the default value for interface in this policy</p> <p><b>default-prioritytype</b> : Per-Hop Behaviour (PHB) type to be used for filling the default PHB for the policy-map entry. The types are:</p> <ul style="list-style-type: none"> <li>• none - No specific PHB type is set.</li> <li>• vlanPri - VLAN priority.</li> <li>• ipTos - IP Type of Service.</li> <li>• ipDscp - IP Differentiated Services Code Point.</li> </ul>
set meter	<p>This command sets Policy parameters such as Meter and Meter Actions. The no form of the command removes the Meter from the Policy and the Meter Actions.</p> <p><b>meter</b> - Meter table identifier which is the index for the Meter table.</p> <p><b>conform-action</b> - Action to be performed on the packet, when the packets are found to be In profile (conform). Options are:</p> <ul style="list-style-type: none"> <li>• none - No action is configured.</li> <li>• set-cos-transmit - Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit - Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-port - Sets the new port value.</li> <li>• set-inner-vlan-pri - Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-ip-prec-transmit - Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit - Sets the new DSCP value.</li> </ul> <p><b>exceed-action</b> - Action to be performed on the packet, when the packets are found to be In profile (exceed). Options are:</p>

Command	Description
	<ul style="list-style-type: none"> <li>• drop - Drops the packet.</li> <li>• set-cos-transmit - Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit - Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-inner-vlan-pri - Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-ip-prec-transmit - Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit - Sets the new DSCP value.</li> </ul> <p><b>violate-action</b> - Action to be performed on the packet, when the packets are found to be out of profile. Options are:</p> <ul style="list-style-type: none"> <li>• drop - Drops the packet.</li> <li>• set-cos-transmit - Sets the VLAN priority of the outgoing packet.</li> <li>• set-de-transmit - Sets the VLAN Drop Eligible indicator of the outgoing packet.</li> <li>• set-inner-vlan-pri - Sets the inner VLAN priority of the outgoing packet.</li> <li>• set-ip-prec-transmit - Sets the new IP TOS value.</li> <li>• set-ip-dscp-transmit - Sets the new DSCP value.</li> </ul> <p><b>set-conformnewclass</b> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.</p> <p><b>set-exceednewclass</b> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.</p> <p><b>set-violatenewclass</b> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.</p>
set algo-type	<p>This command sets Q Template entry parameters.</p> <p><b>algo-type</b> - Type of drop algorithm used by the queue template. Options are:</p> <ul style="list-style-type: none"> <li>• tailDrop - Beyond the maximum depth of the queue, all newly arriving packets will be dropped.</li> <li>• headDrop - Packets currently at the head of the queue are dropped to make room for the new packet to be enqueued at the tail of the queue, when the current depth of the queue is at the maximum depth of the queue.</li> <li>• red - On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.</li> <li>• wred - On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.</li> </ul> <p><b>queue-limit</b> - Queue size. This value ranges between 1 and 65535.</p> <p><b>queue-drop-algo</b> - Enable/disable Drop Algorithm for Congestion Management. Options are:</p> <ul style="list-style-type: none"> <li>• enable - Enables Drop Algorithm.</li> <li>• disable - Disables Drop Algorithm.</li> </ul>
random-detect dp	<p>This command sets Random Detect Table entry parameters. The no form of the command deletes the entry.</p> <p><b>dp</b> - Drop Precedence. Options are:</p>

Command	Description
	<ul style="list-style-type: none"> <li>• 0 - low drop precedence.</li> <li>• 1 - medium drop precedence.</li> <li>• 2 - high drop precedence.</li> </ul> <p><b>min-threshold</b> - Minimum average threshold for the random detect algorithm. Value ranges between 1 and 65535.</p> <p><b>max-threshold</b> - Maximum average threshold for the random detect algorithm. Value ranges between 1 and 65535.</p> <p><b>max-pkt-size</b> - Maximum allowed packet size. Value ranges between 1 and 65535.</p> <p><b>mark-probabilitydenominator</b> : Maximum probability of discarding a packet in units of percentage. Value ranges between 1 and 100.</p> <p><b>exponential-weight</b> - Exponential weight for determining the average queue size. This value ranges between 0 and 31.</p>

## 16.3 Packet Queue Assignment

Each port has 8 transmit queues. A single packet can be assigned for transmission in one of those queues.

Addressing a data packet to a desired QOS port queue can be done using the following measures.

- Port based assignment of priority- all packets coming into the port will be assigned with a specific common priority.
- ACL mapping- ACLs at a port will determine the assigned queue for packets meeting the condition.
- VPT/DSCP- setting VPT or DSCP values to packets based on ACL conditions. The VPT/DSCP values are mapped to queues.

These measures will reflect on the internal Forwarding Class (FC) and will result in a queue assignment as per following table.

Forwarding Class	QOS queue	Priority
Be	1	lowest
l2	2	
af	3	
l1	4	
h2	5	
ef	6	
h1	7	
nc	8	highest

### 16.3.1 Port Based Assignment of Priority

The following script will assign static priority to all ingress UNTAGGED traffic at ports 1 and 2. The ports have the same PVID assigned to them.

Packets originated from these ports will be egressed at the out port in accordance to their assigned priority.

```
Config
interface fastethernet 0/1 no shutdown
switchport pvid 100 switchport priority default 1
exit
interface fastethernet 0/2
no shutdown switchport pvid 100
switchport priority default 2
exit
```

## 16.3.2 ACL Map to COS

The following will demonstrate how to map incoming packets to a desired queue.

1.Create a mac based access list and assign to the a port as in type

```
Config
mac access-list extended 10 permit any any
exit
interface fastethernet 0/1
mac access-group 10 in
exit
```

2.Create a class map to assign a queue id to packets which comply with the acl. All packets ingressing at port 0/1 will thus be assigned to queue 7.

```
class-map 10
match access-group mac-access-list 10
set class 10
exit
queue-map class 10 queue-id 7
```

## 16.3.3 Set VPT or DSCP

### 16.3.3.1 Map VPT to COS

Addressing a packet to a desired queue can be done by its VLAN priority tag (VPT). The following table details the relation of VPT value to a queue assignment.

VPT	Fc	QOS queue	
0	Be	1	lowest
1	l2	2	
2	af	3	
3	l1	4	
4	h2	5	



VPT	Fc	QOS queue	
5	ef	6	
6	h1	7	
7	nc	8	highest

### 16.3.3.2 Map DSCP to COS

Addressing a packet to a desired queue can be done by its DSCP value. The following table details the relation of DSCP value to a queue assignment.

DSCP	Fc	QOS queue	
0-7	Be	1	lowest
8-15	l2	2	
16-23	af	3	
24-31	l1	4	
32-39	h2	5	
40-47	ef	6	
48-55	h1	7	
56-63	nc	8	highest

The following will demonstrate how to set the vpt or dscp values using ACL rules. The values of the DSCP/VPT will determine the target queue for the packet.

#### 1.Create ACLs

Config

```
ip access-list extended 1001
permit ip any 172.18.212.0 255.255.255.0
exit
ip access-list extended 1002 permit ip any any
exit
interface fastethernet 0/1 ipaccess-group 1001 in
ip access-group 1002 in
```

#### 2.Enable QOS

```
qos enable
```

#### 3.Create policer for ACL 1001 to determine dscp to 5

```
class-map 20
match access-group ip-access-list 1001
set class 200
exit
policy-map 20
```

```
set policy class 200 default-priority-type ipDscp 5
exit
```

#### 4.Create policer for ACL 1002 to determine vpt to 2

```
class-map 30
match access-group ip-access-list 1002 set class 300
exit
policy-map 30
set policy class 300 default-priority-type vlanPri 2 exit
write startup-cfg
```

```
iSG18GFP# show policy-map
```

```
QoS Policy Map Entries
```

```
-----
```

```
PolicyMapId   : 20
```

```
IfIndex       : 0
```

```
Class:        200
```

```
DefaultPHB    : IP DSCP 5
```

```
MeterId       : 0
```

```
ConNClass:    0
```

```
ExcNClass:    0
```

```
VioNClass:    0
```

```
ConfAct       : None. ExcAct   : None.
```

```
VioAct        : None.
```

```
QoS Policy Map Entries
```

```
-----
```

```
PolicyMapId 30
```

```
IfIndex      0
```

```
Class        : 300
```

```
DefaultPHB   : VlanPri 2
```

```
MeterId      : 0
```

```
ConNClass    : 0
```

```
ExcNClass    : 0
```

```
VioNClass    : 0
```

```
ConfAct      : None.
```

```
ExcAct       : None.
```

```
VioAct       : None.
```

```
iSG18GFP# show class-map
```

```
QoS Class Map Entries
```

```
-----
```

```
ClassMapId           : 20
```

```
L2FilterId           : None
L3FilterId           : 1001
PriorityMapId         : None
CLASS : 200
PolicyMapId          : 20
PreColor              : None
Status                : Active
QoS Class Map Entries
-----
ClassMapId           : 30
L2FilterId           : None
L3FilterId           : 1002
PriorityMapId         : None
CLASS                : 300
PolicyMapId          : 30
PreColor              : None
Status                : Active
```

## 16.4 Setting a Scheduling Algorithm

The following script will configure scheduler-1 for the outgoing interface Fa 0/4 as wrp. The queues with weights configured will be serviced with Weighted Round Robin.

```
Config
scheduler 1 interface Fa 0/4 sched-algo wrp
queue 1 interface Fa 0/4 weight 1
queue 2 interface Fa 0/4 weight 2
queue 3 interface Fa 0/4 weight 4
queue 4 interface Fa 0/4 weight 4
queue 5 interface Fa 0/4 weight 4
queue 6 interface Fa 0/4 weight 8
queue 7 interface Fa 0/4 weight 8
```

The following script configures scheduler-1 for the outgoing interface Fa 0/4 as strict. The Q with weight 0 will be serviced with strict priority.

The Qs with weights configured will be serviced with Weighted Round Robin.

```
Config
scheduler 1 interface Fa 0/4 sched-algo strict-wrp
queue 1 interface fastethernet 0/4 weight 0
queue 2 interface fastethernet 0/4 weight 2
queue 3 interface fastethernet 0/4 weight 2
queue 4 interface fastethernet 0/4 weight 2
queue 5 interface fastethernet 0/4 weight 4
queue 6 interface fastethernet 0/4 weight 4
```

```
queue 7 interface fastethernet 0/4 weight 4
```

## 16.5 Traffic Filtering at Ingress

In this example, ICMP packets from 12.0.0.100 are filtered at ingress to port 0/1.

```
iSG18GFP# configure terminal
iSG18GFP(config)# ip access-list extended 1001
iSG18GFP(config-ext-nacl)# deny icmp host 12.0.0.100
any iSG18GFP(config-ext-nacl)# exit
iSG18GFP(config)# interface gigabitethernet 0/1
iSG18GFP(config-if)# ip access-group 1001 in
iSG18GFP# show access-lists
```

## 16.6 Setting a Shaper per Egress Port

The following script will configure a “rate-limiter” shaper CIR/CBS based per output port. rate-limit output [CIR (Kbps )] [CBS(Kbytes )]

```
Config
interface Fa 0/4
rate-limit output 2000 15000
```

## Link Aggregation

Link Aggregation allows aggregation of point-to-point links operating at the same data rate. Link Aggregation is supported only on point-to-point links with MAC clients operating in full duplex mode.

A MAC client communicates with a set of ports through an Aggregator, which presents a standard IEEE 802.3 service interface to the MAC client. The Aggregator binds to one or more ports within a system.

LACP (Link Aggregation Control Protocol) is used for automatic communication of aggregation capabilities and automatic configuration of Link Aggregation between systems.

The list of ports that are aggregated to a particular aggregator is transparent to the higher modules (such as Spanning Tree).

Few of the main features of Link Aggregation are as follows:

- Load sharing
- Increased availability
- Increased bandwidth
- Linear incremental bandwidth
- Low risk of duplication or mis-ordering

Upon Link Aggregation, individual point-to-point ports/interfaces are aggregated into a group that is regarded as a single port/interface by the higher layers such as Spanning-tree. The total capacity of such an aggregated group is the sum of the capacities of the individual links composing the aggregate, thus providing higher bandwidth to the MAC client (such as Spanning Tree). As shown in Figure 2-1 multiple ports are aggregated together to form a single link.

iS5Com LA is responsible for taking frames from the aggregator and submitting them for transmission on the appropriate port. The physical port for transmission is chosen based on the selection policy in the chipset. LA is responsible for collecting the frames received on various ports of the aggregator.

The user can configure a specific distribution policy for the traffic flow based on the deployment scenario. This allows the switches to get the advantage of increased bandwidth for the traffic between the hosts and the server. Also, if one of the links in the aggregation group is made down, say, for maintenance purpose, and then it will not affect the traffic between the hosts and the server.

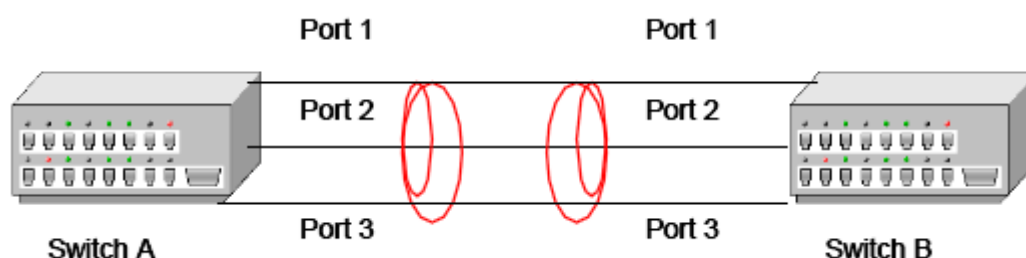



Figure 17-1: Link Aggregation—Example

The guidelines for the configuration of LA are as follows:

- Port-channel must be enabled in the system for Link aggregation configuration to take effect.
- If 802.1x is enabled on a port, then Link Aggregation can be enabled on that port only when the port is in the authorized state. Link Aggregation cannot be enabled on unauthorized ports.


 Up to eight interfaces of the same type and speed can be configured for the same group.

The Default Configurations of LA are as follows:

Feature	Default Setting
Port-channel	Disabled
Channel-groups	None
LACP System Priority	0x8000 or 32768
Load balancing	Source and Destination MAC address based
LACP Port Priority	128 on all interfaces
LACP Wait time	2
LACP timeout	Long: The long timeout value means that LACP PDU will be sent every 30 seconds and LACP timeout value (no packet is received from peer) is 90 seconds
MAC-selection	Dynamic: Port-channel MAC address is address of an active port

Configure the physical port in a port channel and specify the mode by which the port becomes part of the port-channel. The channel-group-number ranges from 1 to 64. Each port-channel can have up to eight compatibly configured Ethernet interfaces.

Whenever a port-channel is created, it is added as an untagged member port of the default VLAN 1. For other VLANs, it needs to be explicitly configured (or dynamically learnt through GVRP) as a member port. It does not inherit the VLAN membership of its member ports. When a port is aggregated into a bundle, that port will not be visible to higher Layer 2 applications like VLAN, STP, etc., only the port-channel port will be visible to them. Hence, when the port gets aggregated into a port channel port, then it will be removed from the membership of the specific VLAN. Similarly, when a port is disaggregated from a port-channel, it is added as a member port of the default VLAN 1.

 When the MTU of a port in a bundle differs from the Port Channel's MTU, then the port will not be up in the bundle. However, if we change the MTU of the port channel then it will be applied on all ports in the bundle. All port-channel member ports will become up in bundle in Switch A.

## 17.1 LAG Command Hierarchy

```

+ root

+ config terminal

    -[no] shutdown port-channel

    - set port-channel {enable | disable}

- channel-protocol lacp

- [no] lacp system-identifier <aa:aa:aa:aa:aa:aa>

- port-channel load-balance ([src-mac][dest-mac][src-dest-mac][src ip][destip][src-dest-ip][vlan-id][service-
instance][mac-src-vid][mac-dest vid][macsrc-dest-vid][l3-protocol][dest-l4-port][src-l4 port]][<port-channel
index(1-65535)>]

-[no] interface port-channel <LAG ID>

    -[no] description DESCRIPTION

    -[no] shutdown

    - interface <port type> <port ID>

        -[no] lacp port-priority (0-65535)

        -[no] channel-group <channel-group-number(1-65535)> mode on

-[no] default port <interface-type> <interface-id>

- port-channel max-ports <integer (2-8)>

    - port-channel load-balance <policy> <LAG ID>

- show etherchannel

- show etherchannel summary

- show etherchannel <> detail

- show interfaces etherchannel

- show lacp counters

- show lacp neighbor

```

## 17.2 LAG Commands Description

Command	Description
config terminal	Enters the Configuration mode.
[no] shutdown port-channel	This command shuts down LA feature in the switch and releases all resources allocated to the LA feature. The no form of the command starts and enables LA feature in the switch, and allocates required memory to the LA module. The LA feature is made available in the switch only if the LA is enabled in the switch. LA feature allows to aggregate individual point-to-point links into a port channel group, so that the capacity and

Command	Description
	<p>availability of the communications channel between devices are increased using the existing interface technology.</p> <p>Defaults: LA is started in the switch, but not enabled. That is LA operational status is disabled.</p>
set port-channel (enable   disable)	<p>This command configures the admin status of LA in the switch. The LA feature is made available in the switch only if the LA is enabled in the switch. LA feature allows you to aggregate individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology.</p> <p>Defaults: disable</p>
[no] interface port-channel <LAG ID>	This command creates logical interface that represents an aggregator which contains several ports aggregated together.
[no] description DESCRIPTION	Add description to port channel.
[no] shutdown	Enable/ Disable port channel.
interface <port type> <port ID>	Entering to the relevant interface to be configured.
[no] lacp port-priority (0- 65535)	<p>This command configures the LACP port priority. The no form of the command resets the LACP port priority to its default value. This port priority is used in combination with LACP port identifier during the identification of best ports in a port channel. The priority determines if the link is an active link or a standby link, when the number of ports in the aggregation exceeds the maximum number supported by the hardware. The links with lower priority becomes active links. This value ranges between 0 and 65535.</p> <p>Defaults: 128</p>
channel-group <channel-group- number (1-65535)> mode on	<p>This command adds the port as a member of the specified port channel that is already created in the switch. The no form of the command deletes the aggregation of the port from all port channels.</p> <p><b>channel-group-number (1-65535) :</b> Adds the port as a member of the specified port channel. This is a unique value that represents the specific port channel created. This value ranges from 1 to 65535.</p>
port-channel load-balance <policy> <LAG ID>	This command configures the load balancing policy for all port channels created in the switch. The no form of the command resets the load balancing policy to its default value. The policy sets the rule for distributing the Ethernet traffic



Command	Description
	<p>among the aggregated links to establish load balancing.</p> <p>The load-balance policy can be configured as:</p> <p><b>src-mac:</b> Load distribution is based on the source MAC address in the frame. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.</p> <p><b>dest-mac:</b> Load distribution is based on the destination MAC address in the frame. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.</p> <p><b>src-dest-mac:</b> Load distribution is based on the source and destination MAC addresses.</p> <p><b>src-ip:</b> Load distribution is based on the source IP address.</p> <p><b>dest-ip:</b> Load distribution is based on the destination IP address.</p> <p><b>src-dest-ip:</b> Load distribution is based on the source and destination IP addresses.</p> <p><b>vlan-id:</b> Load distribution is based on VLAN Identifier.</p>
show interfaces etherchannel	This command shows LAG detailed info.
show etherchannel	This command shows LAG feature status on the switch.

## 17.3 Example

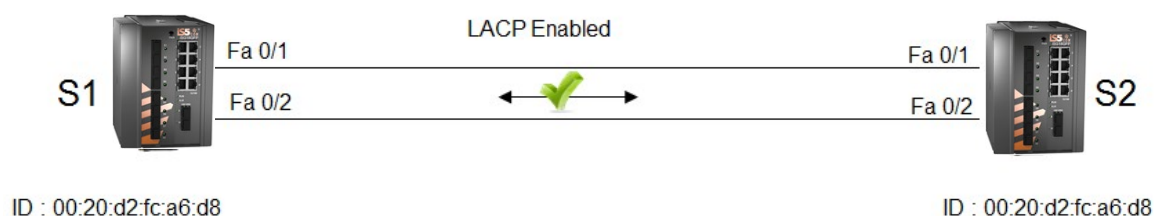


Figure 17-2: Link Aggregation Example

### 1. Configure port channel

```

config
set port-channel enable interface
port-channel 1 no shutdown
exit

```

## 2. Assign the Interfaces

```
interface fastethernet 0/1
channel-group 1 mode active
exit
interface fastethernet 0/2
channel-group 1 mode active
end
```

### Output of show commands, switch S1

#### show ether channel summary

```
S1# show etherchannel summary
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel Independent mode is disabled
Port-channel System Identifier is 00:20:d2:fc:6d:78
LACP System Priority: 32768

Flags:
D - down P - in port-channel
I - stand-alone H - Hot-standby (LACP only)
U - in-use d - default port

Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports

1 Po1(U) LACP Fa0/1(P),Fa0/2(P)
```

#### show lacp neighbor

```
l# show lacp neighbor
Flags:
A - Device is in Active mode
P - Device is in Passive mode
Channel group 1 neighbors
Port Fa0/1

Partner System ID : 00:20:d2:fc:a6:d8
Flags : A
LACP Partner Port Priority : 128
LACP Partner Oper Key : 1
LACP Partner Port State : 0xbc
Port Fa0/2

Partner System ID : 00:20:d2:fc:a6:d8
```

Flags : A

LACP Partner Port Priority : 128

LACP Partner Oper Key : 1

LACP Partner Port State : 0xbc

**show counters**

S1# show lacp counters

LACPDUs Marker Marker Response LACPDUs

Port Sent Recv Sent Recv Sent Recv Pkts Err

Channel group: 1

Fa0/1 75 76 0 0 0 0 0 0 Fa0/2 73 72 0 0 0 0 0 0

# STP

The following sections describe the configuration of the Spanning Tree Protocol (STP).

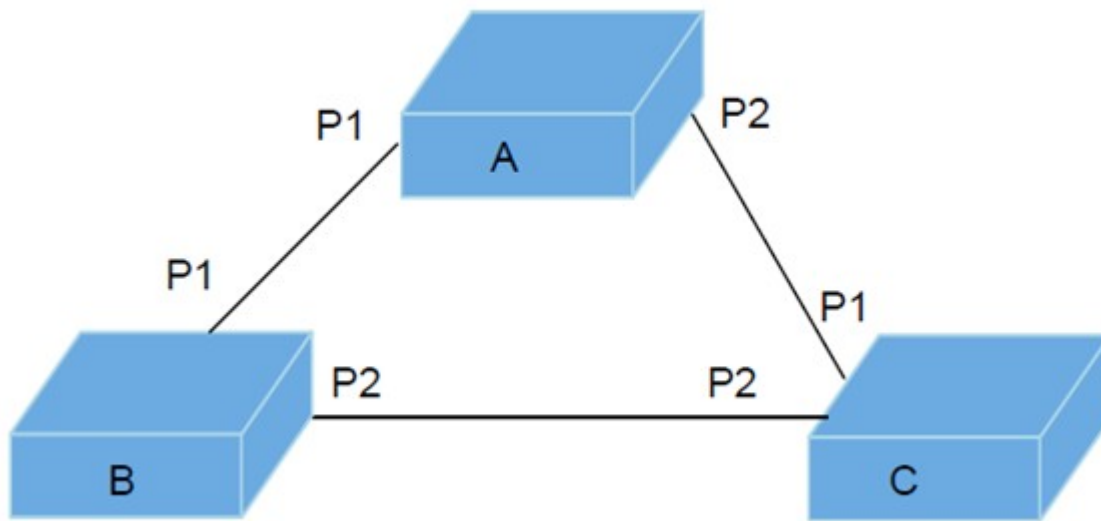


Figure 18-1: Spanning Tree Topology

## Switch A

MAC Address: 00:01:02:03:04:01

VLAN 1 - 10.0.0.1/255.0.0.0

## Switch B:

MAC Address: 00:02:02:03:04:01

VLAN 1 – 10.0.0.2 /255.0.0.0

## Switch C:

MAC Address: 00:03:02:03:04:01

VLAN 1 – 10.0.0.3/255.0.0.0

## 18.1 STP Description

STP runs on bridges and switches that are 802.1D-compliant. A bridge allows interconnection of end stations attached to separate LANs and allows them to communicate as if they were attached to a single LAN. The bridge operates below the MAC service boundary and is transparent to the protocols operating above this boundary. In complex networks, a loop may occur when there are two or more paths between two end points. This leads to the duplication of frames, which in turn leads to heavy traffic in the network. To avoid this, STP is used in the iSG18GFP software. STP forms a logical, loop-free topology from the physical topology and forwards the frames without duplication. To avoid prolonged stabilization time following a reconfiguration event in Spanning tree algorithm, iSG18GFP provides support for RSTP (Rapid Spanning Tree Protocol). The operation of RSTP provides for rapid recovery of connectivity following the failure of a Bridge/ Bridge Port or a LAN.

To isolate link fluctuations specific to a particular VLAN segment(s) and to provide for load balancing, iSG18GFP supports Multiple Spanning Trees. These can be configured on a per VLAN basis or multiple VLANs can be mapped to the same spanning tree. A switch can take the role of either a root or a designated switch. Spanning tree operation provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. It logically breaks such loops and prevents looping traffic from clogging the network.

STP calculates the best loop free path by assigning port roles to the port of switch as follows:

- Root: The port that offers the lowest cost path towards the Root bridge.
- Designated: A forwarding port elected for every switched LAN segment.
- Alternate: A blocked port providing an alternate path to the root bridge of the spanning tree.
- Backup: A blocked port that acts as a backup for the path provided by a Designated Port.

The stable, active spanning-tree topology of a switched network is determined by the following elements.

- Bridge ID (Switch Priority and MAC address)
- Path Cost to the Root Switch
- Port Identifier (Port priority and the Port Number)

When switches in a network come up, each switch assumes itself to be the Root Bridge and starts sending configuration messages through all its ports. BPDUs are used to communicate and compute the spanning tree topology. These BPDUs contain the following information:

- Unique Bridge ID of the switch that has been identified as the Root.
- The spanning-tree path cost to the Root.
- The Bridge ID of the sending switch.
- Message age.
- The identifier of the sending interface (port priority and port number).
- Values for the hello, forward-delay, and max-age protocol timers.

When a switch receives a superior configuration BPDU on a port, it stores the received information for that port. If the port is a root port, it forwards the updated message to all attached LANs for which this switch is the designated bridge. If the switch receives an inferior configuration BPDU to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for that LAN from which the inferior information was received, then it sends up-to-date information stored for that port, thus discarding inferior information and propagating superior information in the network. Each Layer 2 interface in the switch running spanning tree protocol can be in one of the following states.

- Blocking: The interface in this state discards the frames and does not learn the MAC addresses.
- Listening: This is the first state that a port can transition to after blocking. The interface enters this state when spanning tree decides that the interface must participate in frame forwarding.
- Learning: An interface enters this state from listening state. In this state, the interface gets ready to participate in frame forwarding and learns MAC addresses from the packet received.
- Forwarding: In this state, the interface receives and forwards frames received on that port or forwards frames switched from another port. This transition from blocking to forwarding takes 30 seconds.

## 18.2 Bridge ID and Switch Priority

Each switch has a unique bridge identifier (bridge ID), which determines the selection of the Root Switch. The bridge ID is an 8-byte field that is composed of two subfields as shown in Figure 2-2.

Bridge Identifier 8 bytes

Bridge Priority	MAC
-----------------	-----

Figure 18-2: Bridge ID

6 bytes MAC address 2 bytes Range-0-65535

Default:32768

## 18.3 Election of the Root Switch

All switches in the Layer 2 network participating in STP gather information on other switches in the network through an exchange of data messages called Bridge Protocol Data Units (BPDUs). The exchange of messages results in the following actions:

- Election of a unique Root Switch for each spanning tree instance.
- Election of a Designated switch for every switched LAN segment.
- Removal of loops in the switched network by blocking Layer 2 interfaces connected to redundant links.

The switch with the highest switch priority (the lowest numerical priority value) is elected as the Root Switch. If all switches are configured with the default priority (32768), then the switch with the lowest MAC address becomes the Root Switch. The switch priority value occupies the most significant bits of the bridge ID. The Root Switch is the logical center of the STP topology in a switched network. Redundant paths to the Root are put in STP blocking mode.

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

### 18.3.1 Default State

By default, the STP is enabled on all ports.

Application ports Gi 0/3 and Gi 0/4 are set as edge ports.

## 18.4 STP Commands Hierarchy

```
+root

+config terminal

- shutdown spanning-tree

-[no] spanning-tree

-[no] spanning-tree mode (mst | rst | rapid-pvst)

-[no] spanning-tree (forward-time | hello-time | max-age)

-[no] spanning-tree [mst <instance-id>] priority <value(0-61440)>

-[no] spanning-tree portfast {bpdufilter default | bpduguard default |
default}

-interface <port type> <port ID>

-[no] spanning-tree (cost <value(0-2000000000)> | disable | link-
type(point-topoint | shared) | portfast | port-priority
<value(0-240)> )

-[no] spanning-tree disable

-[no] spanning-tree auto-edge

- spanning-tree bpduguard {disable | enable}

- spanning-tree mst configuration
```

- [no] `name` <string>
- [no] `instance` <instance-id (1-64)> `vlan` <vlan-range>
- `show spanning-tree detail`
- `show spanning-tree interface` <interface-id>
- `show spanning-tree summary`

## 18.5 STP Commands Description

Command	Description
<code>config terminal</code>	Enters the Configuration mode.
<code>shutdown spanning-tree</code>	<p>This command shuts down spanning tree functionality in the switch. The switch does not execute any kind of STP to form a loop free topology in the Ethernet network and operates with the existing topology structure.</p> <p>Defaults: Spanning tree MSTP is started and enabled in the switch.</p>
<code>[no] spanning-tree</code>	<p>This command enables the spanning tree operation in the switch for the selected spanning tree mode. The no form of this command disables the spanning tree operation in the switch. The spanning tree operation is automatically enabled in the switch, once the spanning tree mode is changed.</p> <p>Defaults: Spanning tree MSTP is started and enabled in the switch.</p>
<code>[no]spanning-tree mode (mst   rst   rapid-pvst)</code>	<p>This command sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled and the existing spanning tree type is disabled in the switch.</p> <p><b>Mst:</b> Configures the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. The mode cannot be set as mst, if the base bridge mode is configured as transparent bridging.</p> <p><b>Rst:</b> Configures the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN.</p> <p>Defaults: mst</p>

Command	Description
<pre>[no] spanning- tree (forward- time   hello-time   max-age)</pre>	<p>This command sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology. The no form of this command resets the spanning tree timers to its default values. The spanning tree timers are reset to its default value, even if the spanning tree mode is changed.</p> <p><b>forward-time:</b> Configures the number of seconds, a port waits before changing from the blocking state to the forwarding state. This value ranges between 4 and 30 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0).</p> <p>Defaults: forward-time - 15 seconds</p> <p><b>hello-time:</b> Configures the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value should be either 1 or 2 seconds. This value is configured on per-port basis for MSTP and is configured globally for RSTP.</p> <p>Defaults: hello-time - 2 seconds</p> <p><b>max-age:</b> Configures the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval. This value ranges between 6 and 40 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0).</p> <p>Defaults: max-age - 20 seconds</p>
<pre>[no]spanning-tree[mst &lt;instance-id&gt;] priority &lt;value(0-61440)&gt;</pre>	<p>This command configures the priority value that is assigned to the switch. The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree mode is changed.</p> <p><b>Mst:</b> Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree mode is set as mst.</p> <p><b>Priority:</b> Configures the priority value for the switch and for the MSTI, in RSTP and MSTP respectively. This value ranges between 0 and 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.</p> <p>Defaults: priority = 32768</p>



Command	Description
no spanning-tree portfast	<p>This command configures the portfast of the non-trunk ports as bpdudfilter default or bpduguard default or default.</p> <p>Default- Enables PortFast by default on all access ports.</p> <p>bpdudfilter- Enables BPDU filtering on all PortFast ports.</p> <p>bpduguard default- Enables BPDU guard feature on all PortFast ports.</p>
Interface <port type> <port ID>	Entering to the relevant interface to be configured
[no]spanning-tree (cost <value(0-2000000000)> disable  link-type(point-to-point  shared)   portfast   port- priority <value(0-240)>)	<p>This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP/MSTP mode. The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree mode is changed.</p> <p><b>Cost:</b> Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 2000000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. This configuration is not supported for the spanning tree mode pvrst.</p> <p>Defaults: 200000 for all physical ports. 199999 for port channels</p> <p><b>Disable:</b> Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.</p> <p>Defaults: Spanning tree operation is enabled in the port.</p> <p><b>link-type:</b> Configures the link status of the LAN segment attached to the port. The options available are: 1. point-to-point - The port is treated as if it is connected to a point-to-point link. 2. shared - The port is treated as if it is using a shared media connection.</p> <p>Defaults: The port is considered to have a point-to-point link if: It is an aggregator and all of its members can be aggregated. The MAC entity is configured for full duplex operation, either manually or through auto negotiation process (that is, negotiation mode is set as Auto). Otherwise port is considered to have a shared media connection.</p>

Command	Description
	<p><b>Portfast:</b> Configures the portfast feature in the port. This feature specifies that the port is connected to only one hosts and hence can rapidly transit to forwarding. This feature can cause temporary bridging loops, if hubs, concentrators, switches, bridges and so on are connected to this port. This feature takes effect only when the interface is shutdown.</p> <p><b>port-priority:</b> Configures the priority value assigned to the port. This value is used during port role selection process.</p> <p>This value ranges between 0 and 240.</p> <p>This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on.</p> <p>This configuration is not supported for the spanning tree mode pvrst.</p>
[no] spanning-tree auto-edge	<p>This command enables automatic detection of Edge port parameter of an interface. The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree mode is changed. Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received.</p> <p>Defaults: Automatic detection of Edge port parameter of an interface is enabled.</p>
spanning-tree mst configuration	<p>This command enters into MSTP configuration mode, where instance specific and MST region configuration can be done.</p>
spanning-tree bpduguard {disable   enable}	<p>This command configures the status of BPDU guard. The BPDU guard feature disables the port and puts the port in error-disabled state on receiving BPDU, if the portfast feature is enabled on the port. This feature prevents the devices connected to the port from participating in STP operation. Once disabled, the port can be enabled only manually. feature in an interface.</p>
[no] name <string>	<p>This command configures the name for the MST region. The no form of this command resets the name to its default value. The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST.</p> <p>Defaults: Same as that of the base MAC address of the switch.</p>

Command	Description
[no] instance <instance-id (1-64)> vlan <vlan-range>	<p>This command creates an MST instance and maps it to VLANs. The no form of this command deletes the instance / un-maps specific VLANs from the MST instance.</p> <p><b>instance-id (1-64):</b> Configures the ID of MSTP instance to be created /deleted and mapped with / unmapped from VLAN. This value ranges between 1 to 64. The special value 4094 can be used in the switch that supports PBB-TE. Except vlan instance mapping, other commands for stp configurations will not be applicable in this mode. This special value represents PTETID that identifies VID used by ESPs.</p> <p><b>Vlan:</b> Configures a VLAN ID or list of VLAN IDs that should be mapped with / unmapped from the specified MST instance. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to represent the list of VLANs IDs from 4000 to 4010.</p> <p>Defaults: Instance 0 is created and mapped with all VLANs (1-4094).</p>
show spanning-tree active	<p>This command displays spanning tree related information available in the switch for the current STP enabled in the switch. The information contains priority, address and timer details for root and bridge, status of dynamic path cost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.</p>
show spanning-tree detail	<p>This command displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features.</p>

Command	Description
<code>show spanning-tree interface &lt;interface-id&gt;</code>	<p>This command displays the port related spanning tree information for the specified interface. The information contains port ID, port role, port state, port cost, port priority and link type. The generic command cannot be executed without any option in the PVRST mode.</p> <p><b>interface-id:</b> Displays the port related spanning tree information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p>
<code>show spanning-tree summary</code>	Displays a summary of port states or displays the total lines of the STP state section.

## RSTP/MSTP

### 19.1 RSTP Description

The Rapid Spanning Tree Protocol Module is based on the IEEE 802.1D rapid reconfiguration. The existing spanning tree protocol, in particular, takes significant time to re-configure and restore the service on link failure/restoration. RSTP avoids re-convergence delay by calculating an alternate root port and immediately switching over to the alternate port if the root port becomes unavailable.

#### 19.1.1 Port States

STP (802.1D) PortState	RSTP Port State	Is Port Included in active topology?	Is Port Learning MAC address?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

#### 19.1.2 Port Roles

Port Role	Description
Root	Provides the best path to the root. This is the port that receives the best BPDU on a bridge.
Designated	A port is designated if it can send the best BPDU on a segment to which it is connected. Bridges connected to a given segment listen to the BPDUs of other bridges and agree on the bridge sending the best BPDU as the designated bridge for that segment and the port as designated port.
Alternate	A port blocked since another port on the bridge receives superior information from another bridge. This port corresponds to the blocking state of 802.1D.
Back-up	A port blocked since another port receives superior information from the same bridge. This port also corresponds to the blocking state of 802.1D.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port is excluded from the active topology.

## 19.2 Rapid Convergence

Faster convergence compared to legacy spanning tree algorithm is the most important feature in RSTP. RSTP relies on two new variables for achieving this.

- **Edge Port:** Ports that are directly connected to end stations cannot create bridging loops and hence can rapidly transition to forwarding skipping the learning and listening states. When the link toggles on an edge-port then the topology-change is not triggered. Whenever a BPDU is received on an edge port, it loses its edge port status and becomes a normal spanning tree port. IS5Com RSTP uses portfast keyword for edge port configuration.
- **Link Types:** RSTP can achieve rapid transition on point-to-point links. The link type is automatically derived from the duplex mode of a port. A port operating in full-duplex will be assumed to be point-to-point, while a half-duplex port will be considered as a shared port by default. This automatic link type setting can be overridden by explicit configuration.

## 19.3 Proposal Agreement Sequence

In the spanning tree algorithm, a port selected as a designated port waits for 2 x Fwd-delay (2 x 15) seconds before transitioning to forwarding state. In RSTP, this port corresponds to a designated role and blocking state. Figure 19-1 illustrates the rapid transition of a port to forwarding state.

P0: Designated port

P1: New root port

P2: Alternate port

P3: Designated port

P4: Edge Port

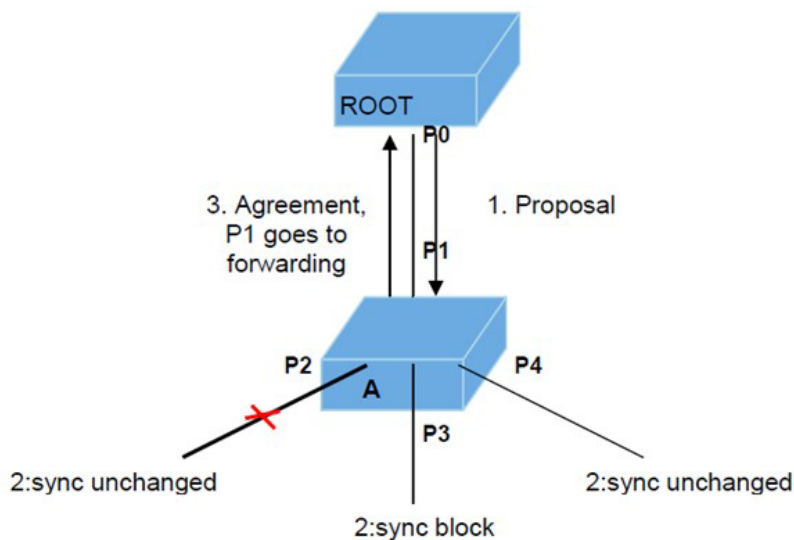


Figure 19-1: Proposal Agreement Handshake

If a new link is created between the Root and Switch A, then both the ports on this link are put in designated blocking state, until they receive a BPDU from their counterpart. When a designated port is in discarding or learning state (and only in this case), it sets the proposal bit on the BPDUs it sends out. This happens for port P0 of the root bridge, as shown in step 1 of Figure 3-1. Because switch A receives superior information, it immediately knows that P1 will be its new root port. Switch A then starts a sync operation to ensure that all of its ports are in-sync with this new information. A port is in- sync if it meets either of the following criteria:

- The port is in blocking state.
- The port is an edge port.

If there exists an alternate port P2, a designated forwarding port P3, and an edge port P4 on switch A. P2 and P4 already meet one of the listed criteria. To be in-sync (step 2 of the diagram above), switch A just needs to block port P3, assigning it the discarding state. If all ports are in-sync, switch A can unblock its newly selected root port P1 and reply to the Root by sending an agreement message (step 3). This message is a copy of the proposal BPDU, with the agreement bit set instead of the proposal bit. This ensures that port P0 knows exactly to which proposal, the agreement it receives corresponds.

When P0 receives that agreement, it can immediately transition to forwarding. Port P3 which was left in a designated discarding state after the sync, in the next Step, is exactly in the same state as port P0 was in Step 1. It then starts proposing to its neighbor, attempting to quickly transition to forwarding. This handshake mechanism propagates quickly towards the edge of the network, and quickly restores connectivity after a change in the topology.

## 19.4 Topology Change and Topology Change Detection

When an 802.1D Bridge detects a topology change, it first notifies the Root Bridge, using a reliable mechanism. Once the Root Bridge is aware of a change in the topology of the network, it sets the Topology Change (TC) flag on the BPDUs it sends out, which are then relayed to all bridges in the network. When a bridge receives a BPDU with the TC flag bit set, it reduces its bridging-table aging time to forward delay seconds, ensuring a relatively quick flushing of stale information.

In RSTP, only non-edge ports moving to the forwarding state cause a topology change. This means that a loss of connectivity is not considered as a topology change any more, contrarily to 802.1D (that is, a port moving to blocking does no longer generates a TC). When a RSTP bridge detects a topology change, the following happens:

- It starts the TC While timer with a value equal to twice the hello time for all its non-edge designated ports and its root port, if necessary.
- It flushes the MAC addresses associated with all Non-edge designated ports.
- As long as the TC While timer is running on a port, the BPDUs sent out of that port have the TC bit set. The BPDUs are also sent on the root port while the timer is active.

### 19.4.1 Default Configurations

Feature	Default Setting
Spanning Tree mode	MSTP
Spanning Tree Status	Enabled
Spanning tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds. Maximum-aging time: 20 seconds.
Switch Priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	200000 (For RSTP, the default value is 65535)

## 19.5 Setting Spanning Tree Compatibility to STP

When the switch comes up, spanning tree is enabled by default with MSTP operating in the switch.

### 1. Execute the following commands in the switch to set the spanning tree compatibility version for STP.

-Enter the Global Configuration mode.

```
iSG18GFP# configure terminal
```


-Set the priority for the spanning tree protocol.

```
iSG18GFP(config)# spanning-tree priority 4096
```

For priority, the range is 0 to 61440, in increments of 4096. The default is 32768. The lower the number, the more likely the switch will be chosen as the Root Switch. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

-Exit configuration mode.

```
iSG18GFP(config)#end
```

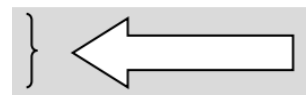
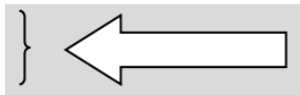
 Observation after configuring the Bridge priority for Switch C: Switch C has been detected as the Root and Port 1 of Switch B is the Alternate Port.

### 2. View the spanning tree information by executing the following show command.

```
iSG18GFP# show spanning-tree
```

#### In Switch A

```
Root Id Priority 4096
Address 00:03:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST000 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
-----
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Root Forwarding 200000 128 SharedLan
```





**In Switch B**

```
Root Id Priority 4096
Address 00:03:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST000 is executing the mstp compatible Mutiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:02:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
----
Gi0/1 Alternate Discarding 200000 128 SharedLan Gi0/2 Root Forwarding 200000 128
SharedLan
```

**In Switch C**

```
Root Id Priority 4096
Address 00:03:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST000 is executing the mstp compatible Mutiple Spanning Tree Protocol
Bridge Id Priority 4096
Address 00:03:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
----
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```



Execute the no spanning-tree priority from the Global Configuration mode command to set the Priority to its default value.

```
iSG18GFP(config)# no spanning-tree priority
```

## 19.6 Configuring Spanning Tree Path Cost

When a loop occurs in the network topology, spanning tree protocol may use path cost to determine the spanning-tree states of the ports. Path cost is obtained from the speed of the interface. A user can configure lower path cost for an interface, if the port needs to be selected first or the user can configure higher path cost if the port needs to be selected last for putting it to forwarding state.

Path cost is used to determine the topology only if the loop in the network cannot be resolved using only the Bridge IDs. If all ports have same path cost values, then the lowest numbered port is first put into forwarding state by spanning tree.

Refer Figure 2-1 for topology. All switches are configured for STP compatible using spanning-tree compatibility STP in Global Configuration mode. After the topology stabilizes and switch A is elected as Root and the ports of all switches except Port 2 of switch C are in forwarding state. Port 2 of Switch C is an alternate port and is in discarding state.

### 1. Execute the following commands in the switch C.

- Enter the Global Configuration mode.

```
iSG18GFP # configure terminal
```

- Specify the interface for which the path cost is to be configured.


```
iSG18GFP(config)# interface gigabitethernet 0/1
```

Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

- Configure the cost for the interface.

```
iSG18GFP(config-if)# spanning-tree cost 2000
```

For cost, the range is 1 to 200000000; the default value is derived from the media speed of the interface.

 **Observation after configuring the Path Cost for port 1 in Switch C:** Port 2 of Switch B is the Alternate Port and Port 2 of Switch C is a Designated Port.

- Exit configuration mode.

```
iSG18GFP(config-if)# end
```

### 2. View the spanning tree properties of an interface.

#### In Switch A

```
iSG18GFP# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
```

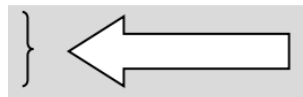
```
Name Role State Cost Prio Type
-----
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```

### In Switch B

```
iSG18GFP# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 200000
Port 1 [Gi0/1]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:02:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
-----
Gi0/1 Root Forwarding 200000 128 SharedLan
Gi0/2 Alternate Discarding 200000 128 SharedLan
```

### In Switch C

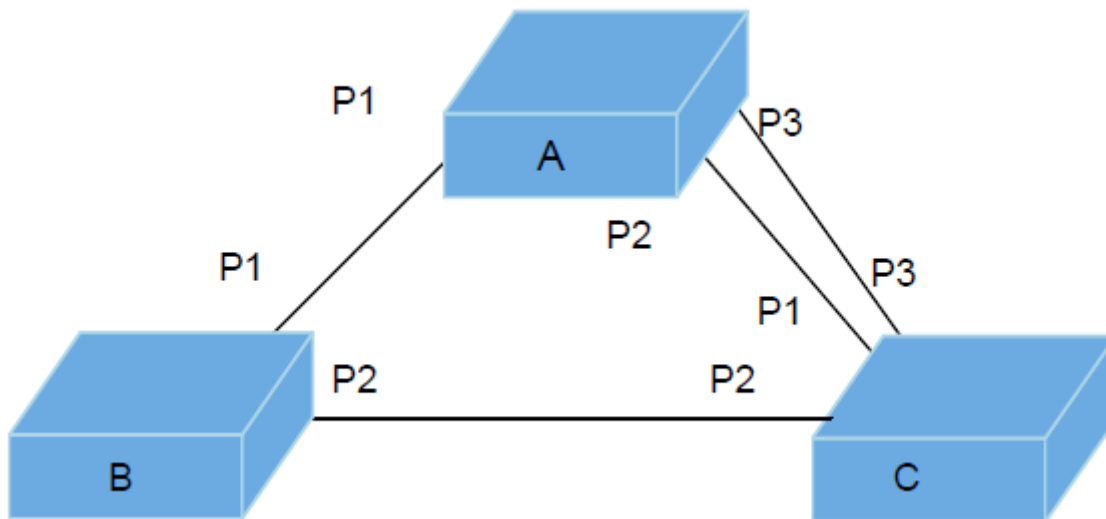
```
iSG18GFP# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 2000
Port 1 [Gi0/1]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:03:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
-----
Gi0/1 Root Forwarding 2000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```



Execute the no spanning-tree cost Interface Configuration mode command to set the default value of the Spanning Tree Path Cost.

```
iSG18GFP(config-if)# no spanning-tree cost
```

## 19.7 Configuring Spanning Tree Port Priority



Switch A :VLAN 1 – 10.0.0.1/255.0.0.0

Switch B :VLAN 1 – 10.0.0.2 /255.0.0.0

Switch C :VLAN 1 – 10.0.0.3/255.0.0.0

**Figure 19-2: Spanning Tree Topology for Configuring Port Priority**

When a loop occurs in a network topology, spanning tree may use the value of port-priority of the ports to decide the port that must be put in the forwarding state.

Port priority is used to determine the topology only if the loop in the network cannot be resolved using the Bridge IDs or path-cost.

If higher priority (lower numerical value) is assigned to a port, it goes to forwarding first and when lower priority (higher numerical value) is assigned to a port, it goes to forwarding last. If all ports have same priority values, spanning tree puts the lowest numbered interface to forwarding and blocks all other interfaces.

Refer Figure 3-1 for setup. All switches are configured for STP compatible using the spanning-tree compatibility stp Global Configuration mode command. After the topology stabilizes, switch A is elected as Root and all ports of all switches except Port 2 and 3 (alternate, discarding) of switch C are in forwarding.

### 1. Execute the following commands in the switch A.

-Enter the Global Configuration mode.

```
iSG18GFP# configure terminal
```

-Specify the interface for which the port priority is to be configured.


```
iSG18GFP(config)# interface gigabitethernet 0/3
```

Interfaces can be physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

-Configure the port priority for spanning tree.

```
iSG18GFP(config-if) # spanning-tree port-priority 32
```

For priority, the range is 0 to 240 in increments of 16. The default is 128. The lower the number, the higher the priority. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.

 Observation after configuring the Port Priority for Port 3 in Switch A: Ports 1, 2 of Switch B are the Alternate Ports and Port 3 is the root port.

- Exit configuration mode

```
iSG18GFP(config-if)# end
```

## 2. View the spanning tree properties of an interface

### In Switch A

```
iSG18GFP# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ----
Gi0/1 Designated Forwarding 200000 128 SharedLan
Gi0/2 Designated Forwarding 200000 128 SharedLan
```

### In Switch B

```
iSG18GFP# show spanning-tree
Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec
MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:02:02:03:04:01
Max age is 20 sec, forward delay is 15 sec Name Role State Cost Prio Type
---- ----
Gi0/1 Root Forwarding 200000 128 SharedLan
```

**In Switch C**

```
iSG18GFP# show spanning-tree Root Id Priority 32768
Address 00:01:02:03:04:01
Cost 200000
Port 2 [Gi0/2]
Max age 20 Sec, forward delay 15 Sec MST00
Spanning Tree Protocol Enabled.
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id Priority 32768
Address 00:03:02:03:04:01
Max age is 20 sec, forward delay is 15 sec
Name Role State Cost Prio Type
---- ----
Gi0/1 Alternate Discarding 200000 128 SharedLan
Gi0/2 Alternate Discarding 200000 128 SharedLan
```

Execute the no spanning-tree port-priority Interface configuration command to set the Spanning Tree Port Priority to its default value

```
iSG18GFP(config-if) # no spanning-tree port-priority
```

**19.7.1 Configuring Spanning Tree Link type**

If a port is configured as point-to-point link and its port role is designated, then IS5Com RSTP negotiates a rapid transition to forwarding with the other port by using proposal-handshake agreement mechanism to ensure that the topology is loop free. By default, if the interface is full-duplex, it is considered to have a point to point connection. If the interface is half duplex, then it is considered to have a shared connection. This default setting of link type can be overridden to enable rapid transition to forwarding.

**1. Execute the following commands in the switch.**

-Enter the Global Configuration mode.

```
iSG18GFP# configure terminal
```

-Specify the interface for which the link type is to be configured.

```
iSG18GFP(config)# interface gigabitethernet 0/1
```

Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

-Configure link type of interface as point-to-point.

```
iSG18GFP(config-if) # spanning-tree link-type point-to-point
```

-Exit configuration mode.

```
iSG18GFP(config-if) # end
```

**2. View the spanning tree properties of an interface.**

```
iSG18GFP# show spanning-tree detail
Spanning tree Protocol Enabled.
```

```
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol Bridge
Identifier has Priority 32768, Address 00:01:02:03:04:01
```

```
Configured Max age 20 sec, Forward delay 15 sec
Configured Hello Time 2 sec
We are root of the spanning tree
Current Root has priority 32768, address 00:01:02:03:04:01
cost of root path is 0
Number of Topology Changes 1, Time since topology Change 37 seconds ago
Transmit Hold-Count 3
Times : Max age 20 Sec,Forward delay 15 Sec
Port 1 [Gi0/1] of MST00 is Designated Forwarding
Gi0/1 is operating in the MSTP Mode
Port path cost 200000, Port priority 128,
Port Identifier 128.1. Port HelloTime 2,
Timers:Hello - 0,Forward Delay - 0,Topology Change - 2
Designated root has priority 32768, address 00:01:02:03:04:01
Designated Bridge has priority 32768, address 00:01:02:03:04:01
Designated Port Id is 128.1, Designated pathcost is 0
Operational Forward delay 15, Max age 20
Number of Transitions to forwarding State : 1
PortFast is disabled
Link type is point to Point
BPDUs : sent 35, received 53
Restricted Role is disabled.
Restricted TCN is disabled.
```



### 3. Execute the no spanning-tree link-type Interface Configuration mode command to set the default link type for an Interface.

```
iSG18GFP(config-if) # no spanning-tree link-type
```

## 19.7.2 Configuring Spanning Tree Portfast

All ports that are directly connected to end stations cannot create bridging loops and hence can rapidly transition to forwarding, skipping the learning and listening states.

A switch can be configured to automatically detect the presence of another switch connected to one of its port. If a switch receives configuration BPDUs from other switch, it can detect the presence of the other switch connected to one of its ports. On configuring a port as portfast, if the switch does not receive any BPDUs for a certain interval then Spanning Tree puts the port to forwarding state rapidly.

#### Execute the following commands in the switch

-Enter the Global Configuration mode.

```
iSG18GFP# configure terminal
```

-Specify the interface for which the auto edge configuration is to be done.

```
iSG18GFP(config)# interface gigabitethernet 0/1
```

Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number).

-Shutdown the interface

```
iSG18GFP(config-if)# shutdown
```

-Specify that the port has only hosts connected to it and hence can transition the port to forwarding rapidly.

```
iSG18GFP(config-if) # spanning-tree portfast
```

-Execute the no shutdown command to make the interface up.

```
iSG18GFP(config-if)# no shutdown
```

-Exit configuration mode.

```
iSG18GFP(config-if)# end
```

### 19.7.3 Configuring Spanning Tree Timers

The following table describes the timers.

Variable	Description
forward-time	Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state.
hello-time	Determines how often the switch broadcasts its hello message to other switches, when it is the Root of the spanning tree.
max-age	The maximum time allowed for the Spanning Tree Protocol information learnt from the network on any port to be retained before it is discarded.

Example for Configuring Spanning Tree Timers:

```
iSG18GFP# configure terminal
iSG18GFP(config)# spanning-tree forward-time 11
iSG18GFP(config)# end
```



# LLDP

---

Link Layer Discovery Protocol (LLDP) supports a set of attributes that are used for discovering the neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors.

The switch supports these mandatory basic management TLVs.

- Port description TLV
- System name TLV
- System description
- System capabilities TLV
- Management address TLV
- Port VLAN ID TLV ((IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV(IEEE 802.3 organizationally specific TLVs)

iS5Com LLDP is a portable software implementation of the Link Layer Discovery Protocol (LLDP). It provides complete management capabilities using SNMP and CLI. iS5Com LLDP conforms to IEEE 802.1AB-2005 standard. The LLDP allows systems on an Ethernet LAN to advertise their key capabilities and also to learn about the key capabilities of other systems on the same Ethernet LAN. This, in turn, promotes a unified network management view of the LAN topology and connectivity to aid network administration and trouble-shooting.

iS5Com LLDP provides the following features:

- Provides full conformance to the 802.1AB specification.
- Supports all mandatory TLVs (Chassis ID, Port ID and Time To Live).
- Supports optional TLVs - Port description, System name, System description, System capabilities and Management address.
- Supports organizationally specific optional TLVs - Port VLAN ID, Port and protocol VLAN ID, VLAN name, MAC or PHY configuration or status, Link Aggregation and Maximum frame size.
- Provides a generic set of APIs for easy integration into different platforms.
- Supports the basic MIB, as well as, the extension MIBs in Appendix F and Appendix G, defined in the 802.1AB specification and a proprietary MIB for management.
- Provides support for configuration and management byproviding generic APIs usable from different management schemes like SNMP, CLI.
- Provides support for notifications through Traps.
- Conforms to Flexible Software Architecture for Portability (FSAP2), thus ensuring portable code, which uses flexible buffer and timer management libraries.

## 20.1 LLDP Commands Hierarchy

```
+root

+config terminal

    -[no] shutdown lldp

    -set lldp {enable | disable}

    -[no] lldp transmit-interval <seconds (30,5-32768)>

    -[no] lldp holdtime-multiplier <value (4,2-10)>

    -[no] lldp reinitialization-delay <seconds (2,1-10)>

    -[no] lldp tx-delay <seconds (2,1-8192)>

    -[no] lldp notification-interval <seconds (5,5-3600)>

    - lldp chassis-id-subtype { chassis-comp <string(255)> | if-
alias | port- comp <string(255)> | mac-addr | nw-addr | if-name | local
<string(255)> }

    -clear lldp counters

    -clear lldp table

+interface <port type> <port ID>

    -[no] lldp {transmit | receive}

    -[no] lldp notification [remote-table-chg][mis-configuration]

    -[no] lldp tlv-select basic-tlv { [port-descr] [sys-
name] [sys- descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> }

        -lldp port-id-subtype { if-alias | port-comp
<string(255)> | mac- addr | if-name | local <string(255)> }

    -[no] lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id
{all|<vlan-id>}] [vlan-name {all | <vlan-id>}]}

        -[no] lldp tlv-select dot3tlv { [macphy-config] [link-
aggregation] [max-framesize] }

        -[no] debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump]
[resource] [all-fail] [buf] [neigh-add] [neigh-del] [neigh-updt] [neigh-drop]
[neighageout] [critical] [tlv {all | [chassis-id] [port-id] [ttl] [port-descr]
[sysname] [sys-descr] [sys-capab] [mgmt-addr] [port-vlan] [ppvlan] [vlan-name]
[proto-id] [mac-phy] [pwr-mdi] [lagg] [max-frame]}] [redundancy]}]

    -show lldp

    -show lldp interface [<interface-type> <interface-id>]

    -show lldp traffic [<ifttype> <ifnum>]

    - show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface- type> <interface-id>][detail]



    -show lldp local {[<interface-type> <interface-id>] | [mgmt-addr]}



    -show lldp errors

    -show lldp statistics
```

## 20.2 LLDP Commands Description

Command	Description
config terminal	Enters the Configuration mode.
[no] shutdown lldp	<p>This command shuts down all ports in the LLDP and releases all allocated memory. The no form of the command enables all ports by allocating the required resources in the LLDP.</p> <p>Default: LLDP is not shutdown in the system.</p>
set lldp {enable   disable}	<p>This command transmits or receives LLDP frames from the server to the LLDP module.</p> <p><b>Enable:</b> Transmits/receives the LLDP packets between LLDP module and the server.</p> <p><b>Disable:</b> Does not transmit/receive the LLDP packets between LLDP module and the server.</p>
[no] lldp transmit-interval <seconds (5-32768)>	<p>This command sets the transmission interval in which the server sends the LLDP frames to the LLDP module. The no form of the command sets the transmission interval to the default value. The value ranges between 5 and 32768 seconds.</p> <p>Default: 30 seconds</p>
[no] lldp holdtime-multiplier <value (2-10)>	<p>This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. The no form of the command sets the multiplier to the default value. The value ranges between 2 and 10 seconds. TLV (Time to Live) A value that tells the receiving agent, how long the information contained in the TLV Value field is valid.</p> <p>TTL = message transmission interval * hold time multiplier.</p> <p>For example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header.</p>
[no] lldp reinitialization-delay <seconds (1-10)>	<p>This command sets the re-initialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission. The no form of the command sets the re-initialization delay time to the default value. The value ranges between 1 and 10 seconds.</p> <p>Default: 2 seconds</p>

Command	Description
[no] lldp tx-delay <seconds(1- 8192)>	<p>This command sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. The no form of the command sets the transmit delay to the default value. The value ranges between 1 and 8192 seconds.</p> <p> <b>TxDelay</b> should be less than or equal to (0.25 * Message Tx Interval)</p> <p>Default: 2 seconds</p>
[no] lldp notification-interval <seconds(5-3600)>	<p>This command sets the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. The value ranges between 5 and 3600 seconds. The no form of the command sets the notification interval to the default value.</p> <p>Default: 5 seconds</p>
lldp chassis-id-subtype { chassis-comp <string(255)>   if- alias   port-comp <string(255)>   mac-addr   nw-addr   if-name   local <string(255)> }	<p>This command configures an ID for LLDP chassis subtype which is a unique address of any module.</p> <p> <b>Chassis id</b> value can be set only for the chassis-component and local system subtypes. For all other subtypes, it takes the value from the system automatically.</p> <p><b>chassis-comp:</b> Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component.</p> <p><b>if-alias:</b> Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.</p> <p><b>port-comp:</b> Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.</p> <p><b>mac-addr:</b> Represents a chassis identifier based on the value of a unicast source address, of a port on the chassis.</p> <p><b>nw-addr:</b> Represents a chassis identifier based on a network address, associated with a particular chassis. The encoded address is actually composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value.</p> <p><b>if-name:</b> Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.</p> <p><b>Local:</b> Represents a chassis identifier based on a locally defined value.</p> <p>Default: mac-addr</p>

Command	Description
clear lldp counters	<p>This command clears the inbuilt counter which has the total count of LLDP frames that are transmitted/received.</p> <p> This command does not clear the global statistics.</p>
clear lldp table	This command clears all LLDP information about the neighbors.
interface <port type> <port ID>	Entering to the relevant interface to be configured.
[no] lldp {transmit   receive}	<p>This command transmits or receives LLDP frames from the one of the ports of the server to the LLDP module. The no form of the command resets LLDP admin status on an interface.</p> <p><b>Transmit:</b> Enables transmission of LLDPDU from one of the ports of the server to the LLDP module.</p> <p><b>Receive:</b> Enables reception of LLDPDU from one of the ports of the server to the LLDP module.</p> <p>Default: Transmission and Reception are enabled.</p> <p> This command can be executed only if lldp is not shutdown.</p>
[no] lldp notification [remote- table-chg] [mis-configuration]	<p>This command controls the transmission of LLDP notifications. The no form of the command disables LLDP trap notification on an interface.</p> <p><b>remote-table-chg:</b> Sends trap notification to NMS whenever remote table change occurs.</p> <p><b>mis-configuration:</b> Sends trap notification to NMS whenever misconfiguration is identified.</p> <p>Default: mis-configuration</p>
[no] lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr] {all   ipv4 <ucast_addr>}	<p>This command enables the basic settings while transmitting the LLDP frames on a given port. The no form of the command disables the basic TLV transmission on a given port.</p> <p><b>port-descr:</b> Configures the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).</p> <p><b>sys-name:</b> Configures the system name of the TLV.</p> <p><b>sys-descr:</b> Configures the system description of the TLV.</p> <p><b>sys-capab:</b> Configures the system capabilities of the TLV.</p>

Command	Description
	<p><b>mgmt-addr all:</b> Enables the transmission of all available management address on the current interface. If no management address is present/configured in the system, switch mac- address will be taken for transmission.</p> <p><b>mgmt-addr ipv4 &lt;ip addr&gt;:</b> Enables the transmission of a particular ipv4 address on the current interface.</p> <p><b>Default :</b> no Tx Tlvs</p>
<pre>lldp port-id-subtype { if-alias   port-comp &lt;string(255)&gt;   mac- addr   if-name   local &lt;string(255)&gt; }</pre>	<p>This command configures an ID for LLDP port subtype.</p> <p><b>if-alias:</b> Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.</p> <p><b>port-comp:</b> Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.</p> <p><b>mac-addr:</b> Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis.</p> <p><b>if-name:</b> Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.</p> <p><b>Local:</b> Represents a chassis identifier based on a locally defined value.</p> <p>Default: if-alias</p>
<pre>[no] lldp tlv-select dot1tlv [port-vlan-id] [protocol- vlan- id {all   &lt;vlan-id&gt;}] [vlan-name {all   &lt;vlan-id&gt;}]}</pre>	<p>This command performs dot1 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings. The no form of the command disables the transmission of dot1 TLV types on a port.</p> <p><b>port-vlan-id:</b> Specifies the VLAN ID of the port that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port.</p> <p><b>protocol-vlan-id:</b> Specifies the protocol ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This group ID is associated with the specific port.</p> <p><b>vlan-name:</b> Specifies the administratively assigned string, which is used to identify the VLAN.</p>

Command	Description
<pre>[no] lldp tlv-select dot3tlv { [macphy-config] [link- aggregation] [max-framesize] }</pre>	<p>This command performs dot3 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings. The no form of the command disables the transmission of dot3 TLV types on a port.</p> <p><b>macphy-config:</b> Configures the physical MAC address of the TLV.</p> <p><b>link-aggregation:</b> Configures the link aggregation protocol statistics for each port on the device.</p> <p><b>max-framesize:</b> Configures the maximum frame size of the TLV.</p>
<pre>[no] debug lldp [{all   [init- shut] [mgmt] [data-path] [ctrl] [pkt-dump] [resource] [all- fail] [buf] [neigh-add] [neigh- del] [neigh-updt] [neigh-drop] [neighageout] [critical] [tlv {all   [chassis-id] [port- id] [ttl] [port-descr]</pre>	<p>This command specifies debug level for LLDP module. The no form of the command disables debug option for LLDP module.</p> <p><b>All:</b> Generates debug statements for all traces.</p>
<pre>[sys-descr] [sys-capab] [mgmt- addr] [port-vlan] [ppvlan] [vlan-name] [proto-id] [mac- phy] [pwr-mdi] [lagg] [max- frame]}} [redundancy]}}</pre>	<p><b>init-shut:</b> Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of LLDP related entries.</p> <p><b>Mgmt:</b> Generates debug statements for management traces. This trace is generated during failure in configuration of any of the LLDP features.</p> <p><b>data-path:</b> Generates debug statements for data path traces. This trace is generated during failure in packet processing.</p> <p><b>Ctrl:</b> Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of LLDP entries.</p> <p><b>pkt-dump</b> - Generates debug statements for packet dump traces. This trace is currently not used in LLDP module.</p> <p><b>Resource:</b> Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.</p> <p><b>all-fail:</b> Generates debug statements for all failure traces of the above mentioned traces</p> <p><b>buf:</b> Generates debug statements for LLDP buffer related traces. This trace is currently not used in LLDP neigh-add - Generates debug statements for add SEM.</p> <p><b>neigh-del:</b> Generates debug statements</p>

Command	Description
	<p>for delete SEM.</p> <p><b>neigh-updt:</b> Generates debug statements for update SEM.</p> <p><b>neigh-drop:</b> Generates debug statements for drop SEM.</p> <p><b>neigh-ageout:</b> Generates debug statements for ageout SEM.</p> <p><b>Critical:</b> Generates debug statements for critical SEM.</p> <p><b>tlv all:</b> Generates debug statements for all TLV traces.</p> <p><b>tlv chassis-id:</b> Generates debug statements for chassis-id TLV traces.</p> <p><b>tlv port-id:</b> Generates debug statements for port-id TLV trace.</p> <p><b>tlv ttl:</b> Generates debug statements for TTL TLV trace.</p> <p><b>tlv port-descr:</b> Generates debug statements for the port description TLV traces.</p> <p><b>tlv sys-name:</b> Generates debug statements for the system name TLV traces.</p> <p><b>tlv sys-descr:</b> Generates debug statements for system description TLV traces.</p> <p><b>tlv sys-capab:</b> Generates debug statements for system capabilities TLV traces.</p> <p><b>tlv mgmt-addr:</b> Generates debug statements for management address TLV traces.</p> <p><b>tlv port-vlan:</b> Generates debug statements for port-vlan TLV traces.</p> <p><b>tlv ppvlan:</b> Generates debug statements for port-protocol-vlan TLV traces.</p> <p><b>tlv vlan-name:</b> Generates debug statements for vlan-name TLV traces.</p> <p><b>tlv proto-id:</b> Generates debug statements for protocol-id TLV traces.</p> <p><b>tlv mac-phy:</b> Generates debug statements for MAC or PHY TLV traces.</p> <p><b>tlv pwr-mdi:</b> Generates debug statements for power-through-MDI TLV traces.</p>



Command	Description
	<p><b>tlv lag:</b> Generates debug statements for link aggregation TLV traces.</p> <p><b>tlv max-frame:</b> Generates debug statements for maximum frame size TLV traces.</p> <p><b>redundancy:</b> Generates the debug statements for the LLDP redundancy module.</p>
show lldp	This command displays LLDP global configuration details to initialize on an interface.
show lldp interface [<interface- type> <interface-id>]	<p>This command displays the information about interfaces where LLDP is enabled.</p> <p><b>interface-type:</b> Displays the information about the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet - A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan - Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> <p><b>interface-id:</b> Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port- channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i- lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p>

Command	Description
<pre>show lldp neighbors [chassis-id &lt;string(255)&gt; port-id &lt;string(255)&gt;] [&lt;interface-type&gt; &lt;interface-id&gt;] [detail]</pre>	<p>This command displays information about neighbors on an interface or all interfaces.</p> <p><b>chassis-id:</b> Configures the chassis identifier string.</p> <p><b>port-id:</b> Configures the port number that represents the concerned aggregation port.</p> <p><b>interface-type:</b> Displays information about neighbors for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet - A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan - Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> <p><b>interface-id:</b> Displays information about neighbors for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p> <p><b>Detail:</b> Displays the information obtained from all received TLVs.</p>

Command	Description
<pre>show lldp traffic [&lt;iftype&gt; &lt;ifnum&gt;]</pre>	<p>This command displays LLDP counters on all interfaces or on a specific interface. This includes the following:</p> <ul style="list-style-type: none"> <li>• Total Frames Out</li> <li>• Total Entries Aged</li> <li>• Total Frames In</li> <li>• Total Frames Received In Error</li> <li>• Total Frames Discarded</li> <li>• Total TLVS Unrecognized</li> <li>• Total TLVs Discarded</li> </ul> <p><b>Iftype:</b> Displays the LLDP counters for specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet - A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan - Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.</li> </ul> <p><b>Ifnum:</b> Displays the LLDP counters for specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents ilan and port-channel ID</p>

Command	Description
show lldp local {[<interface-type> <interface-id>]   [mgmt- addr]}	<p>This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.</p> <p><b>Interfacetype:</b> Displays the current switch information for the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> <li>• fastethernet - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</li> <li>• gigabitethernet - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</li> <li>• extreme-ethernet - A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</li> <li>• i-lan / internal-lan - Internal LAN created on a bridge per IEEE 802.1ap.</li> <li>• port-channel - Logical interface that represents an aggregator which contains several ports aggregated together</li> </ul> <p><b>interface-id:</b> Displays the current switch information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p> <p><b>mgmt-addr:</b> All management addresses configured in the system and Tx enabled ports.</p>
show lldp errors	This command displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
show lldp statistics	This command displays the LLDP remote table statistics information.

## 20.3 Example 1

The following setup demonstrates the configuration and show outputs of LLDP signaling.

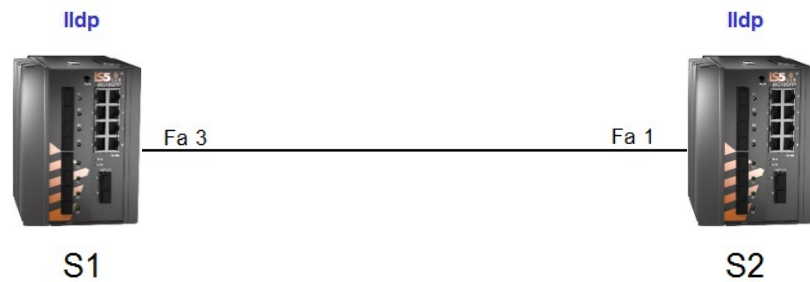


Figure 20-1: Configuration and Show Outputs of LLDP Signaling

### 20.3.1 S1 configuration

#### 1. Set system hostname (not mandatory).

```
set hostname S1
```

#### 2. Enable lldp.

(Timer values are examples only)

```
no shutdown lldp
set lldp enable
lldp transmit-interval 5
lldp notification-interval 5
```

#### 3. Set the chassis id option to be the system own mac address.

```
lldp chassis-id-subtype mac-addr
```

#### 4. Set lldp at the local interface fastethernet 0/3.

```
interface fastethernet 0/3
lldp transmit
lldp receive
lldp notification remote-table-chg
lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab mgmt-addr all
```

#### 5. set the port-id to be the port own local name

```
lldp port-id-subtype if-name
end
```

#### 6. Show local lldp state at the interface

```
S1# show lldp local fastethernet 0/3
```

```
Port Id SubType           : Interface Name
Port Id : Slot0/3
Port Description          : Ethernet Interface Port 03
Enabled Tx Tlvs           : Port Description, System Name,
```

```

System Description, System Capability,

Management Address, Port Vlan
Extended 802.1 TLV Info
-Port VLAN Id           : 1
-Vlan Name
Vlan Id      Vlan Name      TxStatus
-----
1 Disabled
-----

```

## 20.3.2 S2 configuration

### 1. Set system hostname (not mandatory).

```
set hostname S2
```

### 2. Enable lldp. (Timer values are examples only)

```
no shutdown lldp
set lldp enable
lldp transmit-interval 5
lldp notification-interval 5
```

### 3. Set the chassis id option to be the system management IP address.

```
lldp chassis-id-subtype nw-addr
```

### 4. Set lldp at the local interface fastethernet 0/1.

```
interface fastethernet 0/1
lldp transmit
lldp receive
lldp notification remote-table-chg
lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab mgmt-addr all
```

### 5. Set the port-id to be the port alias.

```
lldp port-id-subtype if-alias
alias S2P3
end
```

### 6. Show local lldp state at the interface.

```

S2# show lldp local fastethernet 0/1
Port Id SubType : Interface Alias
Port Id           : S2P3
Port Description   : Ethernet Interface Port 01
Enabled Tx Tlvs    : Port Description, System Name,

```

---

System Description, System Capability, Management Address

Extended 802.1 TLV Info

-Port VLAN Id: 1

-Vlan Name

Vlan Id	Vlan Name	TxStatus
-----	-----	-----
1	Disabled	

### 20.3.3 Show LLDP

#### 1. The following is the LLDP readings of switch 2 as received at switch 1.

S1# show lldp neighbors

Capability Codes :

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID	Local Intf	Hold-time	Capability	Port Id
-----	-----	-----	-----	-----
172.18.212.51	Fa0/3	20	B,R S2P3	

Total Entries Displayed : 1

S1#

#### 2. The following is the LLDP readings of switch 1 as received at switch 2.

S2# show lldp neighbors

Capability Codes :

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID	Local Intf	Hold-time	Capability	Port Id
-----	-----	-----	-----	-----
00:20:d2:fc:a6:d8	Fa0/1	20	B,R Slot0/3	

Total Entries Displayed : 1

## 20.4 Example 2

Based on same setup, following changes in lldp configuration are made at switch 1 in order to show the updated state seen at switch 2.

### S1 configuration

#### 1. Set the chassis id option to be a chosen text "S1."

```
lldp chassis-id-subtype local S1
```

#### 2. Add the interface 0/3 to vlan id 5 (vlan name is www).

```
vlan 5
ports fastethernet 0/3 name www
end
```

#### 3. Set lldp at the local interface fastethernet 0/3.

```
interface fastethernet 0/3
lldp transmit
lldp receive
lldp notification remote-table-chg
lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab mgmt-addr all
```

#### 4. Set the port-id to be the port alias

```
lldp port-id-subtype if-alias
alias S1P1
```

#### 5. Activate lldp for vlan id

```
lldp tlv-select dot1tlv port-vlan-id
lldp tlv-select dot1tlv vlan-name 5
end
```

#### 6. Show local lldp state at the interface

```
S1# show lldp local fastethernet 0/3
Port Id SubType          : Interface Alias
Port Id                  : S1P1
Port Description         : Ethernet Interface Port 03
Enabled Tx Tlvs          : Port Description, System Name,
                           System Description, System Capability,
                           Management Address, Port VlanExtended 802.1 TLV Info
-Port VLAN Id            : 1
Vlan Id      Vlan Name    TxStatus
-----
1            Disabled
5            www Enabled
```



## 20.4.1 Show LLDP

### 1. The following is the updated LLDP readings of switch 1 as received at switch 2.

```
S2# show lldp neighbors
```

```
Capability Codes :
```

```
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

Chassis	ID	Local Intf	Hold-time	Capability	Port Id
S1		Fa0/1	20	B,R	
S1P1					

Total Entries Displayed : 1

### 2. Detailed readings

```
S2# show lldp neighbors detail
```

```
Capability Codes :
```

```
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

```
Chassis Id SubType : Local
```

```
Chassis Id : S1
```

```
Port Id SubType : Interface Alias
```

```
Port Id : S1P1
```

```
Port Description : Ethernet Interface Port 03
```

```
System Name : Linux Router Ver 1.0
```

```
System Desc : Switch software version 3.2
```

```
Local Intf : Fa0/1
```

```
Time Remaining : 18 Seconds
```

```
System Capabilities Supported : B,R
```

```
System Capabilities Enabled : B,R
```

```
Management Addresses :
```

```
IfId SubType Address : OID
```

```
-----
```

```
49 IPv4 172.18.212.53 1 3 6 1 2 1 2 2 1 1
```

```
Extended 802.1 TLV Info
```

```
-Vlan Name
```

```
Vlan Id Vlan Name
```

```
-----
```

```
5 www
```

Total Entries Displayed : 1

# OAM CFM

The Connectivity Fault Management (CFM) provides the capabilities useful for detecting, verifying and isolating connectivity failures in Virtual Bridged Local Area Networks. These capabilities are used in network operated by multiple independent organizations, each with restricted access to each other's equipment. In general, a network administrator is informed about the failure in the connection based on the Continuity Check Messages reception or by the User. It initiates the Loop Back or Link Trace and quickly determines and isolate the fault condition.

IEEE 802.1ag (IEEE Standard for Local and Metropolitan Area Networks Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management) defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and LANs.

The following is the order in which the Ethernet Connectivity Fault Management elements must be configured:

- Domain at the same level as the MEP (Maintenance association End Point)
- Service within the domain (Maintenance Association)
- If a Service (Maintenance Association) is to be associated with more than one Vlan-id, then its Primary VLAN ID must be mapped to all associated VLAN
- Ids with the command `Ethernet cfm associate vlan-id`
- primary-vlan-id
- MA (Maintenance Association), MEP List with MEP ID of the MEP

## 21.1 CFM Command Hierarchy

```
+root

+ config terminal

+ ethernet cfm domain name <name> level <level-id> [format {}]

- service name <name> [format] [icc <code>] [{vlan <vlan-id>
| service-instance <instance>] [mip-
creationcriteria{}}] [sender-id permission
{}]]

- set mip-creation-criteria {none | default | explicit}

- set sender-id-permission {}

- ethernet cfm mep { domain <name> | level <0-7> } [inward] mpid <id> [{service
<name>| vlan <id> | service-instance <integer>}] [active]

- ethernet cfm mip {domain <domain-name> | level <level-id (0-7)>} vlan <vlan-id (1-4094)> [active]

- [no] ethernet cfm start

- [no] ethernet cfm enable

- [no] ethernet cfm cc {domain <name> | level <>} [vlan{<id> | vlan-list} | [interval {}] [role{}]]

- [no] ethernet cfm cc enable {domain <domain-name> | level <a,b,c-d>} [vlan <a,b,c-d>
| service-instance <integer>{<>}]

- [no] ethernet cfm associate vlan-id <a.b,c-d> primary-vlan-id <id>

- [no] mep crosscheck mpid <id> [{vlan <id> | service-instance <id>}]

- [no] ethernet cfm traceroute cache [

- [no] ethernet cfm mip ccm-database
```

- ```
-traceroute ethernet {mpid <id> | mac <>} {domain <name> | level <id>}
[service <name> | vlan <id>] | service-instance <id>] [interface <type>
<number>] [direction {}] [time-to-live <ttl>][timeout <msec>] [use-
mip-ccm-db]

-show ethernet cfm domain [brief]

-show ethernet cfm service [brief]

-show ethernet cfm maintenance-point local [mep | mip] [interface [<type> <number>] | [domain <name>] | [level
<id>]

-show ethernet cfm maintenance-points remote detail {mpid <id> | mac <> } [domain <name> | level <id> [{service <name>
| unaware | vlan <id> | service-instance <id>}]

-show ethernet cfm traceroute-cache
```

## 21.2 CFM Commands Description

| Command         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| config terminal | Enters the Configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ethernet cfm    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| domain          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| format          | <p>Sets the format of the CFM maintenance domain. The options are:</p> <ul style="list-style-type: none"> <li><b>dns-like-name</b> – Configures the domain name like string. Globally unique text string derived from a DNS name. this option of format should be chosen only along with Y.1731.</li> <li><b>mac-addr</b> – Configures the MAC address plus 2-octet (unsigned) integer.</li> <li><b>char-string</b> – Configures the RFC2579 display string. The character codes 0-31 (decimal) are not used.</li> </ul> |
| Name            | Creates a domain with a specified name. Character string has a maximum limit of 20 characters.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Level           | Sets a level for the created domain.at which the maintenance domain is defined. This integer value ranges between 0 and 7.                                                                                                                                                                                                                                                                                                                                                                                               |
| service         | This command configures the service (Maintenance Association) at the specified service-instance or VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| name            | Identifies the association. Maximum limit of the Character string is up to 20 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Command          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Format           | <p>Configures the format of the service. The options are:</p> <p><b>primary-vid</b> - Specifies Primary VLAN ID. 1 to 4096. The vlan must be created beforehand.</p> <p><b>char-string</b> - Specifies RFC2579 DisplayString, except that the character codes 0-31 (decimal) are not used. String with maximum size 39.</p> <p><b>unsigned-int16</b> - 0 to 65535.</p> <p><b>icc</b> - Specifies ITU-Carrier Code</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Icc              | <p>Configures the ITU-Carrier Code. String with maximum size 40.</p> <p>User can configure ICC only when Y.1731 is enabled.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Umc              | <p>Configures the Unique Maintenance Entity Group Identifier Code. User can configure UMC only when Y.1731 is enabled.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| vlan             | <p>Configures the primary VLAN ID which the Maintenance Association must be associated. This is a unique value that represents the specific VLAN created / to be created. Value ranges between 1 and 4094.</p> <p>when the service vlan command is executed:</p> <ul style="list-style-type: none"> <li>• Maintenance Association Name must be unique within a Maintenance Domain.</li> <li>• More than one VLAN can be associated with the Maintenance Association through the command ethernet cfm associate vlan-id primary-vlan-id.</li> <li>• Primary VLAN ID associated with a Maintenance association is not assigned to any other Maintenance Association at the same level. The same Maintenance Association Name can be used, if the Maintenance Association exists in different domain.</li> <li>• All MEPs related to the Maintenance Association must be removed before removing that Maintenance Association.</li> </ul> |
| Service instance | <p>Indicates a service-instance for the configuration. This value ranges between 256 and 16777214.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Command              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mip-creationcriteria | Indicates, whether the management entity is able to create MHF for this Maintenance Association. The options are: none   default   explicit   defer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| sender-id-permission | Sets the value to control the Sender ID TLV, to be transmitted in CFM PDUs by MHFs associated with this Maintenance Association. The options are: none   chassis   manage   chassis-mgt- address   defer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| mep                  | <p>This command configures the MEP (Maintenance End Point) for a service-instance. Sets an interface as a domain boundary (edge), defines it as a MEP (Maintenance End Point), sets direction for the MEP and sets the operational status of the MEP. The no form of the command removes the MEP configuration from the interface.</p> <p>An active keyword is provided to enable or disable the MEP, if it is already configured. By default, MEP is disabled. For Vlan unaware MEP, Vlan is not to be specified.</p> <p><b>domain</b> : Identifies the Maintenance Domain. The maximum length of the domain-name is 20.</p> <p><b>level</b> : Maintenance Domain level for the MEP. This integer value ranges between zero and seven.</p> <p><b>inward</b> : Specifies the direction. By default, outward is created, that is, down MEP.</p> <p><b>mpid</b> : MEP identifier. This integer value ranges between 1 and 8191.</p> <p><b>Service</b> : Indicates the service name. The maximum length of the service-name is 20.</p> <p><b>Vlan</b> : VLAN ID. This value ranges between 1 and 4094. Following restrictions apply:</p> <ul style="list-style-type: none"> <li>- On a particular interface, only one MEP can be configured at particular level, VLAN ID and direction.</li> <li>- MPID has to be unique in a Maintenance Association.</li> </ul> <p><b>Service instance</b>: Service instance identifier for which the MEP is defined. This is required only for the ISID aware MEP. This is applicable only for ports in PBB bridge mode. This value ranges between 256 and 16777214 (<math>2^{24}-1</math>).</p> <p><b>Active</b> : Operational status of the MEP. By default, MEP will not be active.</p> |

| Command | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mip     | <p>This command configures a Maintenance Intermediate Point (MIP) at the specified maintenance level and VLAN on an interface.</p> <p>An active keyword is provided to enable or disable the MIP, if it is already configured.</p> <p><b>domain:</b> Identifies the Maintenance Domain. The maximum length of the domain- name is 20.</p> <p><b>level:</b> Specifies the maintenance level at which the MIPs are defined. This integer value ranges between zero and seven.</p> <p><b>Service:</b> Indicates the service name. The maximum length of the service-name is 20.</p> <p><b>Vlan:</b> VLAN ID. This value ranges between 1 and 4094. Following restrictions apply:</p> <ul style="list-style-type: none"> <li>- There must not be any MP configured at an equal or higher MD Level at the same VLAN than the MIP to be configured.</li> <li>- Level with which MIP is to be created must be set corresponding to the</li> <li>- If the service (Maintenance Association) associated with the specified VLAN and level is configured in the system, with at least an up (inward) MEP then its MHF creation parameter must not be "none".</li> <li>- If the above MA exists and its MHF criteria is "defer", then its enclosing domain's MHF creation parameter must be either "default or explicit". It can be modified using the command set mip- creation- criteria.</li> <li>- If service (Maintenance Association) associated with the specified VLAN and level is not configured in the system, then the default MHF creation parameter must not be "none".</li> </ul> <p><b>Service instance:</b> Service instance for which the MIP is being defined. This value ranges between 256 and 16777214.</p> <p><b>Active:</b> Specifies the MIP's operational status. By default, MIP will be active.</p> |

| Command                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| set mip-creation-criteria | This command sets MIP creation criteria for a Maintenance Domain. MIP creation criteria is applicable only if Maintenance Domain's underlying Maintenance Association's MIP creation criteria is "defer".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| set sender-id-permission  | <p>This command sets Sender ID permission for a Maintenance Domain. Sender ID permission criteria is applicable only if Maintenance Domain's underlying Maintenance Association's SenderID permission is "defer".</p> <p>The following values are allowed:</p> <ol style="list-style-type: none"> <li>1. none</li> <li>2. chassis</li> <li>3. manage</li> <li>4. chassis-mgt-address</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ethernet cfm start        | This command starts an Ethernet connectivity fault Management (CFM), processing globally on the switch. The no form of the command shutdown an Ethernet CFM processing on the switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ethernet cfm enable       | This command enables a Connectivity Fault Management (CFM) processing globally on a device or on an interface. The no form of the command disables the CFM processing globally on a device or on an interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ethernet cfm cc           | <p>This command sets the parameters (that is, Interval and Role) for CCs (Continuity Check Messages).</p> <p>The level and vlan identifies the service (Maintenance Association) to which the configuration applies.</p> <p>This command is used to set the parameters for CC transmission for a Maintenance Association, that is, for a particular level and for a particular VLAN.</p> <p><b>domain:</b> Identifies the Maintenance Domain. The maximum length of the domain- name is 20.</p> <p><b>level:</b> Specifies the maintenance level at which the MIPs are defined. This integer value ranges between zero and seven.</p> <p><b>Service:</b> Indicates the service name. The maximum length of the service-name is 20.</p> <p><b>Vlan id:</b> VLAN ID. This value ranges between 1 and 4094.</p> <p><b>Vlan list:</b> Indicates a list of VLANs.</p> |

| Command                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <p><b>Service instance:</b> Indicates a service-instance for the configuration. This value ranges between 256 and 16777214.</p> <p><b>interval:</b> The time between CCM transmissions. Options are:</p> <ul style="list-style-type: none"> <li>• hundred-ms - 100 milliseconds</li> <li>• one-sec - one second</li> <li>• ten-sec - 10 seconds</li> <li>• one-min - one minute</li> <li>• ten-min - 10 minutes</li> </ul> <p><b>role:</b> ETH-CC role to be performed. Options are:</p> <ul style="list-style-type: none"> <li>• fault-management - ETH-CC is used for Fault Management.</li> <li>• performance-monitoring - ETH-CC is used for Performance Monitoring.</li> <li>• protection-switching - ETH-CC is used for Protection Switching.</li> </ul> <p>Default: fault management</p> |
| ethernet cfm cc enable         | <p>This command enables the transmission of Continuity Check Messages (CCMs). The level and vlan identifies the Maintenance End Points (MEPs) to which the configuration applies. The no form of the command disables the transmission of CCMs.</p> <p>For the transmission of CCMs by the Vlan unaware MEPs, vlan is not to be specified.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ethernet cfm associate vlan-id | <p>This command associates a VLAN ID or a list of VLAN IDs to a Primary VLAN. The no form of the command deletes the mapping of a VLAN ID or a list of VLAN IDs with a Primary VLAN.</p> <p><b>Vlan id:</b> Identifies the VLAN to which the Primary VLAN ID must be associated. This value ranges between 1 and 4094. vlan-id &lt;a,b,c-d&gt;.</p> <p><b>Primary-Vlan-id:</b> Identifies the Primary VLAN ID. The range of the integer value is from 1 to 4094. Restrictions:</p> <ul style="list-style-type: none"> <li>* VLAN ID and Primary VLAN ID cannot be the same.</li> <li>* One VLAN cannot be associated with more than one Primary VLAN.</li> </ul>                                                                                                                                |



| Command                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mep crosscheck mpid           | <p>This command statically defines an MEP (Maintenance End Point) in a Crosscheck List (MA-MEP List) within a Maintenance Association. The no form of the command deletes statically defined MEP from the Crosscheck List.</p> <p>Vlan/Service-Instance unaware MEP can be statically defined by not providing vlan/service-Instance.</p> <p><b>mpid:</b> Identifies MEP. The mep-id value ranges from 1 to 8191.</p> <p><b>Service:</b> Indicates the service name. The maximum length of the service-name is 20.</p> <p><b>Vlan:</b> Identifies the Primary VLAN ID of service (Maintenance Association) with which remote MEP must be associated.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> <li>- MEP Identifier must be unique within the service (Maintenance Association).</li> </ul> <p><b>Service instance:</b> Identifies a service-instance in a Provider backbone bridge mode. This value ranges between 256 and 16777214.</p> |
| ethernet cfm traceroute cache | <p>This command enables caching of Ethernet Connectivity Fault Management (CFM) data learned through traceroute (Linktrace Replies) messages. The no form of the command disables caching.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ethernet cfm mip ccm-database | <p>This command enables caching of Ethernet Connectivity Fault Management (CFM) data learned through the Continuity Check Messages (CCM). The no form of the command disables caching.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ethernet cfm loopback cache   | <p>This command enables loopback cache. The no form of the command disables loopback caching.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| traceroute Ethernet           | <p>This command initiates Linktrace message by providing MEP identifier of the destination MEP (Maintenance End Point) or the MAC Address of the MEP or MIP.</p> <p><b>Direction:</b> Specifies the direction of the MEP.</p> <p><b>inward</b> - MEP faces in up direction on the bridge port.</p> <p><b>outward</b> - MEP faces in down direction on the bridge port</p> <p>Time-to-live: 1-255</p> <p><b>timeout:</b> Deadline timeout (in milliseconds), before which the trace route reply must come. The value ranges from 10 to 10000 milliseconds.</p>                                                                                                                                                                                                                                                                                                                                                                                               |

| Command                                            | Description                                                                                                                                               |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| show ethernet cfm domain                           | This command displays the information about all CFM Maintenance Domains configured on a device.                                                           |
| show ethernet cfm service                          | This command displays the information about all CFM Maintenance Associations configured on a device.                                                      |
| show ethernet cfm maintenance-point                | This command displays the details of all maintenance points (Maintenance End Point (MEP) or Maintenance Intermediate Point (MIP)) configured on a device. |
| show ethernet cfm maintenance-points remote detail | This command displays the information about the remote maintenance points in continuity check database.                                                   |
| show ethernet cfm traceroute-cache                 | This command displays the contents of the traceroute cache.                                                                                               |

## Discrete IO Channels


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


The iSG18GFP switch allows the most effective feature of monitoring and controlling these channels over the IP network. The iSG18GFP switch basically acts as a Modbus gateway, expecting connections from Modbus TCP clients at port TCP 502.

### 22.1 Discrete Channel interfaces

The status of the digital inputs can be read via CLI and using Modbus TCP.

The digital output can be set using Modbus TCP. The state can be read via cli and Modbus TCP.

 The physical interface DO1 used for this feature can be utilized as well for the purpose of manifesting system alarms acting as “Alarm-Relay”. The physical interface cannot be assigned simultaneously to both feature types.

 For the use of discrete channels please make sure the interface is not occupied by the Alarm-Relay service.

Connection terminals are as shown in the figure below.

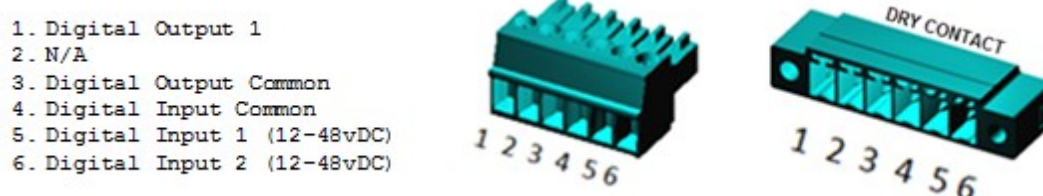


Figure 22-1: Connection Terminals

#### 22.1.1 Hardware


Contact iS5Com support to verify if your hardware supports this interface. (PCB 11 power only)

### 22.2 Modbus/TCP

The discrete channels are controllable via Modbus/TCP commands.

An ACE interface is required to accept incoming connections at TCP port 502.

| Channel         | Terminal | Default state             | Modbus address | Modbus Function Code             |
|-----------------|----------|---------------------------|----------------|----------------------------------|
| Discrete In #1  | 5, 4     | Low [0], no external PS   | 10001          | [2] read discrete input contacts |
| Discrete In #2  | 6, 4     | Low [0], no external PS   | 10002          | [2] read discrete input contacts |
| Discrete Out #1 | 1, 3     | Low [0], contact is open. | 0001           | [5] write single discrete output |
|                 |          |                           | 10011          | [1] read discrete output coil    |

 The state of the OUT channel is always set to 0 after system boot.

## 22.3 Electric Data

- At the digital Input points please connect a DC source in the nominal range 12- 48v at terminals 6,4 for channel 2; or 5,4 for channel 1. Maximum limits of 9-58vDC should not be exceeded.
- Maximum power to be implemented at the contacts :

AC: Max 250v , 37.5vA.

DC: 12v-60v ,30 watt.

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

### 22.3.1 Discrete IO Channels Commands Hierarchy

```
+ root
+ application connect
    + discrete-channels
        + admin-status <enable| disable>
+ mapping
- add modbus-gw {address-prefix <A.B.C.D/M>}
- remove modbus-gw {address-prefix <A.B.C.D/M>}
+ connection
    - show
    - clear
+ show
- discrete-values
- mb_gw
```

## 22.4 Discrete Interfaces Commands

| Command                    | Description                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Application connect</b> | Enter the industrial application menu.                                                                                                                                                                     |
| <b>discrete-channels</b>   | Enter the configuration mode for specific physical serial ports.                                                                                                                                           |
| <b>admin-status</b>        | Enable/disable listening to Modbus TCP connections.                                                                                                                                                        |
| <b>mapping</b>             | Assign an IP interface.                                                                                                                                                                                    |
| <b>add modbus-gw</b>       | IP address and subnet of the local ACE interface used to listen to incoming Modbus connections.                                                                                                            |
| <b>remove modbus-gw</b>    | IP address and subnet of the local ACE interface used to listen to incoming Modbus connections.                                                                                                            |
| <b>Connection show</b>     | Show connected Modbus clients.                                                                                                                                                                             |
| <b>Show</b>                | <ul style="list-style-type: none"> <li>• History - History Events.</li> <li>• Discrete-Values - The State Of The Discrete Channels.</li> <li>• Mb_Gw - The Properties And State Of The Gateway.</li> </ul> |

## 22.5 Example

Following setup demonstrates DNP3 gateway configuration.

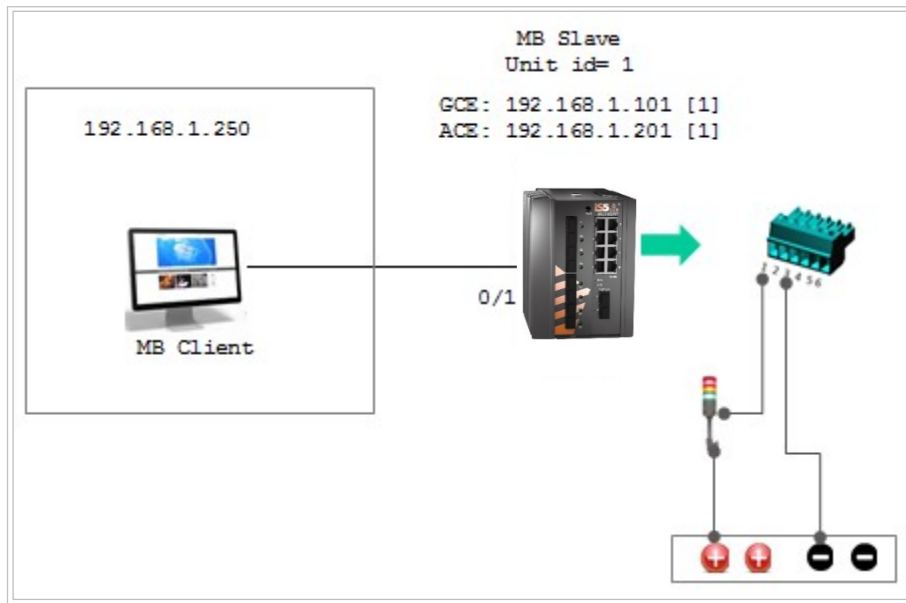


Figure 22-2: DNP3 Gateway Configuration

### 1. Set switch host name (optional).

```
set host-name Gateway
```

### 2. Set service vlan. Gigabitethernet 0/3 must be a tagged member.

```

config
vlan1
ports fastethernet 0/1 gigabitethernet 0/3 untagged fastethernet 0/1
exit
interface fastethernet 0/1
alias CLIENT
switchport pvid 1
exit

```

### 3. Assign management IP (optional).

```

interface vlan 1
ip address 192.168.1.101 255.255.255.0
no shut
end

```

### 4. Access the ACE mode.

```
application connect
```

### 5. Assign IP interface for the gateway.

```

router interface create address-prefix 192.168.1.201/24 vlan 1 purpose
application-host

```

**6. Assign the ACE interface to be used for the Modbus gateway.**

```
discrete-channels mapping add modbus-gw address-prefix 192.168.1.201/24
```

**7. Enable the feature.**

```
discrete-channels admin-status enable
```

```
exit
```

```
write startup-cfg
```

**8. Establish a Modbus connection from the client to the server.****9. Send a command from the client to the server, using function code 5 to address 0001 to activate the discrete output contact.**

```
[/]discrete-channels connection show
```

```
+-----+-----+-----+-----+
| Index | GW IP/Subnet | client ip addr | src port |
+=====+=====+=====+=====+
| 1 | 192.168.1.250/24 | 192.168.1.250 | 55218 |
+-----+-----+-----+-----+
```

```
[/]discrete-channels show discrete-values
```

```
+-----+-----+-----+
| Input#1 10001 | Input#2 10002 | Output#1 0001 |
+=====+=====+=====+
| 0 | 0 | 1 |
+-----+-----+-----+
```