

Aruba 2540 Management and Configuration Guide for ArubaOS- Switch 16.09

The Aruba logo consists of the word "aruba" in a lowercase, rounded, orange sans-serif font.

a Hewlett Packard
Enterprise company

Part Number: 5200-5896
Published: June 2019
Edition: 1

- TR-69
- Menu

There is a restriction on executing the following commands over CLI:

- boot
- recopy
- erase
- reload
- startup-default
- upgrade-software
- setup
- delete
- reboot
- restore
- menu
- write memory
- amp-server

LED Blink feature

Central connectivity loss is indicated by LEDs. If connectivity is broken and Aruba-Central is enabled, the USB/FDX and Locator LEDs will blink. The LEDs will stop blinking once the switch is connected back to Central.

Aruba Central Configuration manually

In factory default switches, ZTP with Central is turned ON. ZTP can be disabled in the following scenarios:

- Switches with edited configuration
- Switches where the administrator has explicitly turned off ZTP with Central

In any of the mentioned scenarios, an administrator can manually configure Aruba Central using the `aruba-central` command.

aruba-central

Syntax

```
aruba-central {enable | disable | support-mode {enable | disable}}
```

Description

Configure Aruba Central server support. When enabled, and when a server web address has been obtained using Aruba Activate, the system will connect to an Aruba Central server. The system will obtain configuration updates and most local configuration commands will be disabled. This mode is enabled by default.

Enter support mode to enable all configuration commands. Normally, when the system is connected to an Aruba Central server, the configuration is updated from that server and most local configuration commands are disabled. Support mode enables those commands for use in troubleshooting problems. Support mode is disabled by

default. When the system is not connected to Aruba Central server, the full command set is enabled for local configuration.

Restrictions

- Switch communication to Aruba Central is not supported via OOBM.
- Aruba-central is not supported in FIPS switches and it will be disabled by default.
- Aruba-central is not supported in Stack switches and it will be disabled by default.



CAUTION: To avoid broadcast storm or loops in your network while configuring ZTP, do not have redundant links after you complete ZTP and Airwave registration. Authorize the new switch and then push the Golden Configuration template from Airwave.

Example

Enable Aruba Central server support

```
switch(config)# aruba-central enable
```

Disable Aruba Central server support

```
switch(config)# aruba-central disable
```

Enter support mode to enable all CLI configuration commands

```
switch(config)# aruba-central support-mode enable
```

This mode will enable all CLI configuration commands, including those normally reserved by the Aruba Central service.
Use of this mode may invalidate the configuration provisioned through Aruba Central server.
Continue (y/n)?



NOTE: Starting with 16.09 release when switches are on-boarding to Central, SNMP access is read-only, and SNMP traps are supported.

Activating ArubaOS-Switch Firmware Integration

CLIs are available for Activate firmware updates which enables, update, checks and shows firmware upgrades.

Operating Notes

Switch will periodically check with Activate every seven days for the latest image version.

Download the image from the URL provided by Activate and upgrade the switch with the new image.

Restrictions

When a switch is managed by either AirWave or Aruba Central, the automatic firmware check is disabled.

Activate upgrade from the non-supported build is disabled upon upgrading to version 16.03.

Upon upgrade from version 16.02 to version 16.03 with activate provision enabled, activate software update will be enabled.

activate software-update enable

Syntax

```
activate software-update [enable | disable]
```

Description

Enables or disables the Activate software update.

Activate software-update is enabled by default.

Parameters

disable

Disables the Activate software update.

enable

Enables the Activate software update.

Example

Switch will check with activate for every seven days for latest image available and RMON logs will be generated:

```
I 10/25/16 14:04:27 05219 activate:  
A system software update is available to version WB.16.02.0012.
```

activate software-update check

Syntax

```
activate software-update check
```

Description

Check the Activate software update manually.

Example

```
switch(config)$# activate software-update check  
  
Configuration and Status - Activate Software Update  
  
Activate Server Address      : device.arubanetworks.com  
Activate Server Polling     : Enabled  
Installed Software Version  : WB.xx.xx  
Server Software Version     : Not available - server communication error.  
Server Software Image URL   : Not available - server communication error.  
switch(config)$
```



NOTE: This switch is not connected to Activate, hence communication error is shown in “Server Software Version” and “Server Software Image URL” field.

activate software-update update

Syntax

```
switch#(config) activate software-update update
```

Description

Updates the software for Activate.

Parameters

primary

Update primary software image using the Aruba Activate server.

secondary

Update secondary software image using the Aruba Activate server.

Example

```
switch# activate software-update update
```

This command will save the current configuration, update the selected software image, and reboot the system to the selected partition.

```
Continue (y/n)? y
```

```
000M
```

activate provision force

Syntax

```
activate provision force help
```

Description

Immediately provisions the system using Aruba Activate.

Usage

You can do a force ZTP provision using this command, thereby enabling the switch to be provisioned with Airwave/Central.

Example

```
switch(config)# activate provision force
switch(config)#
0008:04:35:03.63 ZTP mactivateCtrl:Hostname resolved with IP: 104.36.249.201:443
0008:04:35:03.78 ZTP mactivateCtrl:Proxy IP is not Configured
0008:04:35:03.86 ZTP mactivateCtrl:EndPoint Url :
    https://device.arubanetworks.com:443/hpe-provision
0008:04:35:03.98 ZTP mactivateCtrl:SOCKET IS OPEN!!!
0008:04:35:07.64 ZTP mactivateCtrl:Second POST msg is sent to Activate.
0008:04:35:09.15 ZTP mactivateCtrl:activate connection established
0008:04:35:09.23 ZTP mactivateCtrl:Custom CA  CUSTOM_CA installed

0008:04:35:09.30 ZTP mactivateCtrl:Central URL is
    https://internal.central.arubanetworks.com/ws

0008:04:35:09.41 ZTP mactivateCtrl:ZTP is disabled
```

show activate software-update

Syntax

```
show activate software-update
```

Description

Show the configuration and status of the Activate software update.

Example output

```
switch(config)$ show activate software-update

Configuration and Status - Activate Software Update

  Activate Server Address      : device.arubanetworks.com
  Activate Server Polling     : Enabled
  Installed Software Version   : WB.xx.xx
  Server Software Version     : Not available - server communication error.
  Server Software Image URL   : Not available - server communication error.
switch(config)$
```

Show activate provision

Syntax

```
show activate provision
```

Description

Show the configuration and status of the Activate Provision services.

Examples

```
switch(config)#show activate provision

Configuration and Status - Activate Provision service
  Activate server address      : device.arubanetworks.com
  Activate server polling     : Enabled
  Activation key               : ABC-XYZ-123
```

Default status when Activate server polling is not started

```
switch(config)#show activate provision

Configuration and Status - Activate Provision Service

  Activate Provision Service   : Enabled
  Activate Server Address     : device.arubanetworks.com
  Activation Key               : Not Available
  NTP/HTP Time Sync Status    : Not Updated
  Activate DNS Lookup         : NA
  Proxy Server DNS Lookup     : NA
  Activate Connection Status  : NA
  Error Reason                 : NA
```

Connected to Activate (post DNS resolution) and got Central URL

```
switch(config)#show activate provision

Configuration and Status - Activate Provision Service

  Activate Provision Service   : Enabled
  Activate Server Address     : device.arubanetworks.com
  Activation Key               : ZAELQSRB
  NTP/HTP Time Sync Status    : Time sync from NTP
  Activate DNS Lookup         : Success
  Proxy Server DNS Lookup     : NA
```



```
Activate Connection Status : Success
Error Reason                : NA
```

Disable the Activate polling, after getting the Central URL

```
switch(config)#show activate provision
```

Configuration and Status - Activate Provision Service

```
Activate Provision Service : Disabled
Activate Server Address    : device.arubanetworks.com
Activation Key             : ZAELQSRB
NTP/HTTP Time Sync Status : Time sync from NTP
Activate DNS Lookup       : Success
Proxy Server DNS Lookup   : NA
Activate Connection Status : Success
Error Reason              : NA
```

Unsuccessful Activate connection when device entry not present in Activate

```
switch(config)# show activate provision
```

Configuration and Status - Activate Provision Service

```
Activate Provision Service : Enabled
Activate Server Address    : device.arubanetworks.com
Activation Key             : Not Available
NTP/HTTP Time Sync Status : Time sync from NTP
Activate DNS Resolution    : Success
Proxy Server DNS Lookup   : NA
Activate Connection Lookup : Failure
Error Reason              : Failed response received.
Status code               : not-authenticated
```

Activate pushing AirWave parameters to switch

```
switch(config)#show activate provision
```

Configuration and Status - Activate Provision Service

```
Activate Provision Service : Enabled
Activate Server Address    : device.arubanetworks.com
Activation Key             : ZAELQSRB
NTP/HTTP Time Sync Status : Time sync from NTP
Activate DNS Lookup       : Success
Proxy Server DNS Lookup   : NA
Activate Connection Status : Success
Error Reason              : NA
```

Unsuccessful Activate connection due to unresolved Activate server address

```
switch(config)#show activate provision
```

Configuration and Status - Activate Provision Service

```
Activate Provision Service : Enabled
Activate Server Address    : device.arubanetworks.com
Activation Key             : Not Available
Time Sync Status          : Time sync from NTP pool
Activate DNS Lookup       : Failure
Proxy Server DNS Lookup   : NA
Activate Connection Status : NA
Error Reason              : NA
```



NOTE: DNS resolution is a field in the WebUI (under **Dependencies** section), it will show DNS resolution as *failure* .

Fields added in 16.07.	Status	Validation
Time sync status	<ul style="list-style-type: none"> Time sync from NTP Time sync from HTTP Time sync from other source Not updated NA 	<ul style="list-style-type: none"> Default - Not updated, time is not updated from NTP and HTTP. NA - In this case switch get the time through SNTP/ CLI/time server configuration before NTP/ HTTP.
Activate DNS Lookup.	<ul style="list-style-type: none"> Success Failure NA 	<ul style="list-style-type: none"> Default - NA Other outputs are based on device.arubanetworks.com DNS lookup.
Proxy Server DNS Lookup	<ul style="list-style-type: none"> Success Failure NA 	<ul style="list-style-type: none"> NA - If proxy is not configured. Other outputs are based on proxy lookup.
Activate Connection Status.	<ul style="list-style-type: none"> Success Failure NA 	Default - NA
Error Reason		Default - NA

Troubleshooting

You can troubleshoot switches by using the SSH connection and the device logs available in AirWave. For a list of all RMON message, refer to *Event Log Messages Guide* of your switch

You can enable the debug logging with the debug ztp command, see **debug ztp** .

Show aruba-central

Syntax

```
show aruba-central
```

Description

Shows Aruba Central server information.

Example

```
switch#show aruba-central
Configuration and Status - Aruba Central

Server URL           : https://internal.central.arubanetworks.com/ws
Connected            : Yes
Mode                  : Managed
```

```

Last Disconnect Time      : NA
Server DNS Lookup         : Success
Proxy Server DNS Lookup   : NA
Error Reason              : NA

```

Fields added in 16.07.	Status	Validation
Server DNS Lookup	<ul style="list-style-type: none"> • Success • Failure • NA 	By default status is NA. Other status is based on DNS resolution.
Proxy Server DNS Lookup	<ul style="list-style-type: none"> • Success • Failure • NA 	If proxy is not configured, status will be NA. Otherwise Status will be set based on proxy server DNS lookup.
Error Reason		Default-NA

Error reason for Aruba Central

Error Reason field is added in the switch firmware as part of Aruba Central Onboarding Feature from 16.07. Error reason log helps in debugging switch firmware for central connectivity failure.

	Preprocessor Directive	Mocana Error Enum	Error Reason
1	CLOUD_TCP_ERR	ERR_TCP	TCP error. Check the server reachability.
2	CLOUD_TCP_READ_ERR	ERR_TCP_READ_ERR OR	TCP read error. Malformed packet received or the SSL socket is closed.
3	CLOUD_TCP_READ_TIMEOUT_ERR	ERR_TCP_READ_TIM EOUT	TCP timeout. Server is taking longer time to respond. Check the server reachability.
4	CLOUD_TLS_ERR	ERR_SSL	TLS error. Verify if the device or system certificate is valid.
5	CLOUD_TLS_CERT_VAL_ERR	ERR_SSL_CERT_VAL IDATION_FAILED	Certificate validation failed. Verify if it is correctly installed, valid, and trusted.
6	CLOUD_TLS_MUTUAL_AUTH_FAIL_ERR	ERR_SSL_MUTUAL_A UTHENTICATION_FA ILED	TLS mutual authentication has failed.
7	CLOUD_TLS_MUTUAL_AUTH_NOT_REQ_ERR	ERR_SSL_MUTUAL_A UTHENTICATION_NO T_REQUESTED	Client authentication is not requested by server.

Table Continued

	Preprocessor Directive	Mocana Error Enum	Error Reason
8	CLOUD_TLS_MUTUAL_AUTH_REQ_IGNORE_ERR	ERR_SSL_MUTUAL_AUTHENTICATION_REQUEST_IGNORED	TLS mutual authentication request is ignored.
9	CLOUD_TLS_INVALID_SIG_ERR	ERR_SSL_INVALID_SIGNATURE	Unable to verify the signature on a certificate.
10	CLOUD_TLS_NO_DATA_RECV_ERR	ERR_SSL_NO_DATA_TO_RECEIVE	No data received from server. Check the server reachability.
11	CLOUD_CERT_ERR	ERR_CERT	System certificate is invalid.
12	CLOUD_CERT_EXPIRE_ERR	ERR_CERT_EXPIRED	System certificate expired. Contact Aruba support.
13	CLOUD_INVALID_TIME_ERR	ERR_CERT_START_TIME_VALID_IN_FUTURE	Wrong system time.
14	CLOUD_TLS_MULTIPLE_CONN	ERR_SSL_TOO_MANY_CONNECTIONS	Too many connections to server. Disconnect the device and connect back.
15	CLOUD_TLS_NO_CIPHER_MATCH	ERR_SSL_NO_CIPHER_MATCH	Cipher suites are not common between device and server.
16	CLOUD_TLS_UNKNOWN_CA	ERR_SSL_UNKNOWN_CERTIFICATE_AUTHORITY	Server certificate is not issued by a trusted CA.
17	CLOUD_TLS_NO_SELF_SIGNET_CERT	ERR_SSL_NO_SELF_SIGNED_CERTIFICATES	Server presented a self-signed certificate. This certificate is not supported for mutual authentication.
18	CLOUD_GENERIC_ERR		TLS generic error (code: -XYZ)
19	CLOUD_HTTP_101_PROT_MISSNG		Internal error: HTTP/1.1 protocol missing. Contact Aruba support.

Table Continued

	Preprocessor Directive	Mocana Error Enum	Error Reason
20	CLOUD_HTTP_UPGRADE_MISSNG_IN_RESP		Internal error: Missing Upgrade in HTTP response. Contact Aruba support.
21	CLOUD_HTTP_ACCEPT_KEY_MISSNG_IN_RESP		Internal error: Missing Sec-WebSocket-Accept in HTTP response. Contact Aruba support.
22	CLOUD_HTTP_MISMATCH_ACCEPT_KEY		Internal error: Mismatch Sec-WebSocket-Accept in HTTP response. Contact Aruba support.
23	CLOUD_URL_NOT_REACHABLE_VIA_PXY		Central server is not reachable through proxy.

debug ztp

Syntax

```
debug ztp
no debug ztp
```

Description

Enables or disables ZTP debug logging.

Parameters and options

ztp

Zero Touch Provisioning.

no

The `no debug ztp` command disables ZTP debug logging.

Error Reason log for Activate Provision

Error Reason field is added in the switch firmware as part of Aruba Central Onboarding Feature from 16.07. Error reason log helps in debugging switch firmware for central connectivity failure.

Following table shows the list of error reasons.

Preprocessor Directive	Error Reason
ACTIVATE_RESP_FAIL_CODE	Activate provision fails because of invalid response received from server with status code: %s.
ACTIVATE_CURL_FAIL_CODE	Device fails to reach Activate server with error: %s.

Table Continued

Preprocessor Directive	Error Reason
ACTIVATE_FAIL_PROV_NO_DEVICE_ENTRY	Device is not registered with Activate server.
ACTIVATE_NON_TPM_CODE_MISSING	EST provision with activate server fails because of invalid response received from Activate server.

Stacking support

The ZTP process for stacked switches with Central is similar to the one for a standalone switch, with the exception that only the commander in the stack checks in with Central. For switches supported on Central when stacking is ON, refer to the *Aruba Central Switch Configuration Guide*.

Fault finder switch events

Fault finder switch events supported by Aruba Central
EVENT_FF_BAD_DRIVER_NIC
EVENT_FF_BAD_XCVR_NIC
EVENT_FF_BAD_CABLE
EVENT_FF_CABLE_LEN_HOPS
EVENT_FF_LOOP_OVER_BAND
EVENT_FF_BCAST_STORM
EVENT_PPMGR_DMM_SET_FULL_WARN
EVENT_PPMGR_DMM_SET_AUTO_WARN
EVENT_FF_LINKFLAP

interface device-type network-device

Syntax

```
interface <PORT-LIST> device-type network-device
no interface <PORT-LIST> device-type network-device
```

Description

Configures the type of device and identifies a port connected with a network infrastructure device (such as switch, AP, router). The switch will not report the client entries on the port to Central.

The `no` form of this command removes the configuration of type of the device connected to the ports.

Command context

```
config
```

Parameters

PORT-LIST

Specifies the port number for the device.

Usage

```
no device-type { network-device }
```

Example

```
switch(config)# interface 2
device-type          Configures the type of device being connected to the port.

switch(config)# interface 2 device-type
network-device       Marks a port being connected with a network infra
                    device (switch / AP / router).

switch(config)# interface 2 device-type network-device

switch(config)# show running config
; JL074A Configuration Editor; Created on release #KB.16.04.0000x
; Ver #10:9b.7f.bf.bb.ff.7c.59.fc.7b.ff.ff.fc.ff.ff.3f.ef:81

hostname "Aruba-3810M-48G-PoEP-1-slot"
module 1 type j1074x
module 2 type j1074y
flexible-module A type JL078A
interface 2
    device-type network-device
    exit
interface 3
    device-type network-device
    exit
```

HTTP Proxy support with ZTP overview

The Aruba switch connects through Public Cloud or infrastructure to access Aruba Activate and Aruba Central. The switch can use a combination of the Public and Private networks to access Aruba AirWave, and Aruba ClearPass. In this case, the switch is visible as an Internet asset that can cause data breaching. Routing connections through the enterprise proxy servers prevents the data breaching.

The ArubaOS-Switch does not set up an HTTP/SSL connection with the public or private server directly. Instead, the switch sets up a TCP connection with the proxy server.

If the public server is available and reachable through the proxy server, then the switch connection to the destination server is successful. After establishing the connection, the proxy server behaves as a Network Address Translation (NAT) device, in which case, the proxy server forwards the received packets to the intended destinations.

Limitations:

- HTTPS proxy is not supported.
- Authenticating the HTTP proxy is not supported.
- HTTP proxy support is only for IPv4 endpoints.

Configuring ZTP:

When the switch is provisioned for Central or Controller, switch is managed once it is connected to the public network. In case the user wants to reach the public network through the proxy, then the IP address of the proxy server must be present in the switch before initiating the Activate or Central connectivity.

In ZTP mode, the proxy IP address can be received using the DHCP option. The ZTP mode works when the switch is booted with a default configuration. For the switch to connect to public servers through proxy, the proxy IP must be known through DHCP. The switch requests an IP address from the primary VLAN.

The proxy IP address is received through a vendor-specific DHCP option. The switch parses and uses the proxy IP address to connect in ZTP mode. Aruba switches reserve suboption -148 under DHCP vendor-specific option 43 for configuring proxy URL.

After the switch is out of ZTP mode, the proxy IP address if configured through CLI takes precedence. Otherwise, the Aruba OS switch may use the DHCP received proxy IP address for connectivity.

e Proxy Configuration

When configuring the proxy server, the following applications will be taking the proxy route to reach the destination. You can configure the proxy server as indicated in DHCP or `proxy server` command.

- Aruba AirWave
- Aruba Activate
- Firmware download through MNP
- Aruba ClearPass connectivity
- Aruba Central connectivity
- TR69 support

Support for Aruba AirWave

AirWave is used to manage the ArubaOS-Switches and its communication to the switch is over HTTPS. When AirWave is deployed with Aruba controller, an IPsec tunnel is created between the switch and the controller. All the communication between the switch and AirWave occurs through the tunnel. In this case, the proxy is bypassed implicitly.

AirWave establishes ICMP, SNMP, and SSH connections to the switch for switch management. Since AirWave does not have the visibility for the switch IP address, the ICMP, SNMP, and SSH connections will not be initiated to the switch. So reverse NAT functionality must be enabled for ensuring these packets reach the switch. If AirWave must work without proxy, then AirWave IP is bypassed explicitly.

Support for Aruba ClearPass

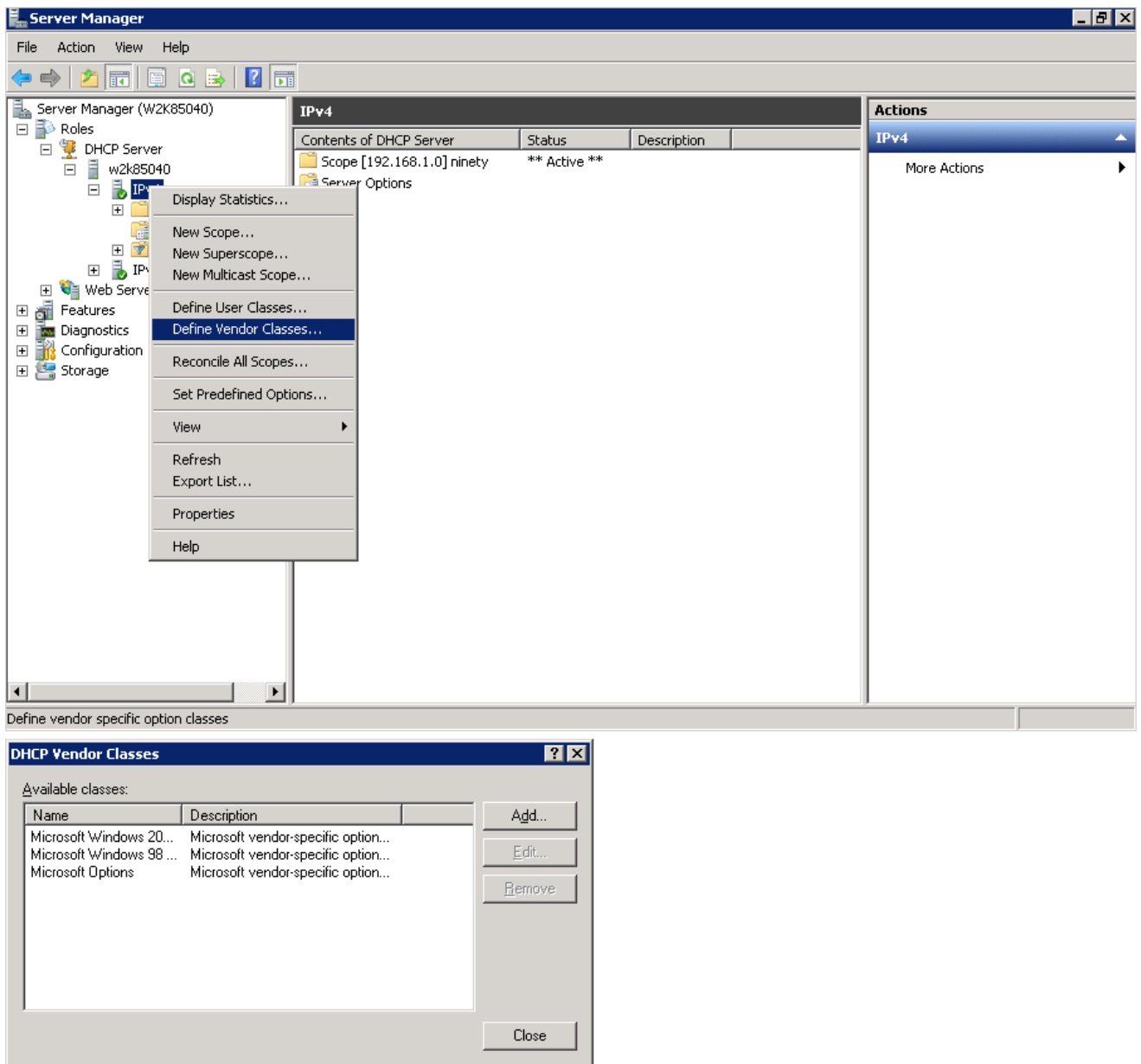
For downloading a user role from ClearPass, switch initiates HTTPS connection with ClearPass. If the proxy is configured, proxy server is used to reach ClearPass. When ClearPass is deployed with Aruba controller, ClearPass must be explicitly exempted from proxy. Add the ClearPass IP address in the exception list of the proxy as the communication happens through the IPsec tunnel or normally.

Proxy Configuration using windows DHCP server

In the ZTP provisioning, you can push the Proxy server and exception configurations through a Windows DHCP server using DHCP option 148.

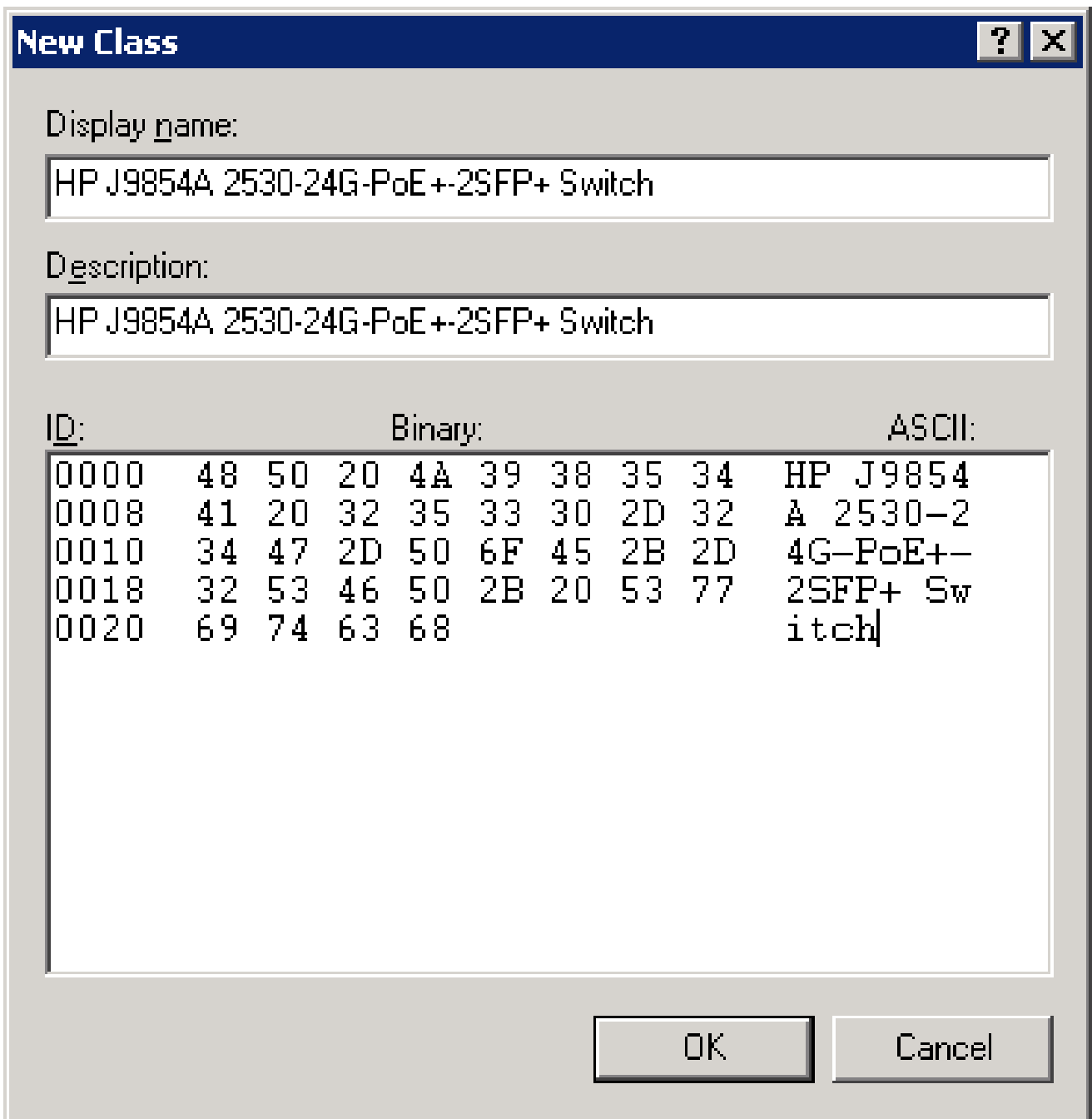
Procedure

1. Add a new **DHCP Server** role. Navigate to **Server Manager > Roles > DHCP sever > domain DHCP Server > IPv4**. In the master pane of the Server Manager window, click **IPv4** and select **Define Vendor classes**.

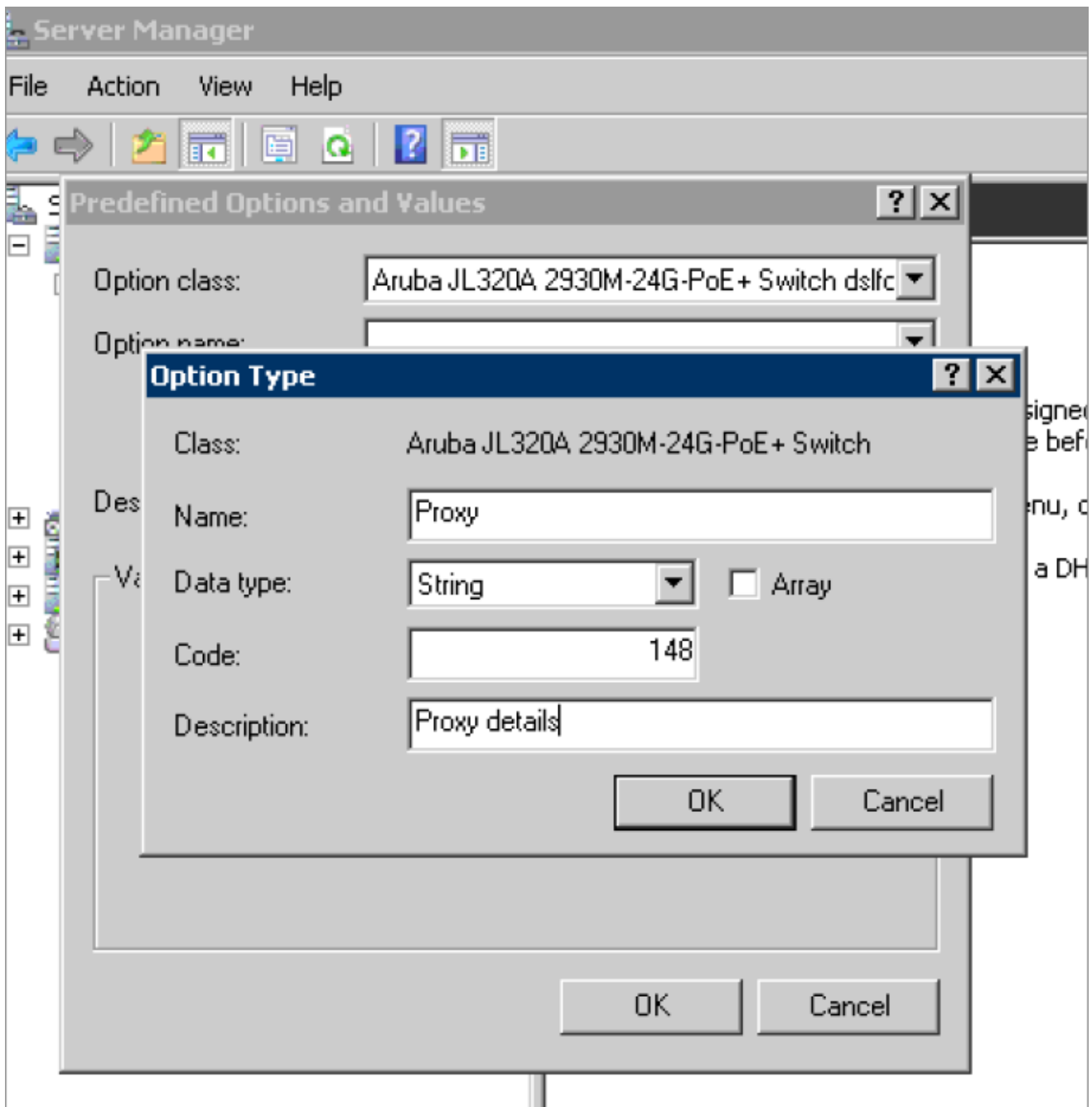


2. To get vendor-specific value of a switch, go to switch command prompt and enter `show dhcp client vendor-specific` command. Vendor class identifier for the switch (VCI) appears as follows:

```
Switch# show dhcp client vendor-specific
Vendor Class Id = J9854A 2530-24G-PoE+-2SFP+ Switch
Processing of Vendor Specific Configuration is enabled.
```
3. Add **Displayed name** and **Description** for the **New Vendor Class** in the ASCII field, add `J9854A 2530-24G-PoE+-2SFP+ Switch` value exactly obtained from the switch, otherwise the option may not work.



4. Right-click **IPv4** and select **Set Predefined Options**. Select option class as the newly defined vendor class, click **ADD** and enter the following information for Proxy details:
 - a. Name - Proxy
 - b. Data Type - String
 - c. Code - 148
 - d. Description - Proxy details.



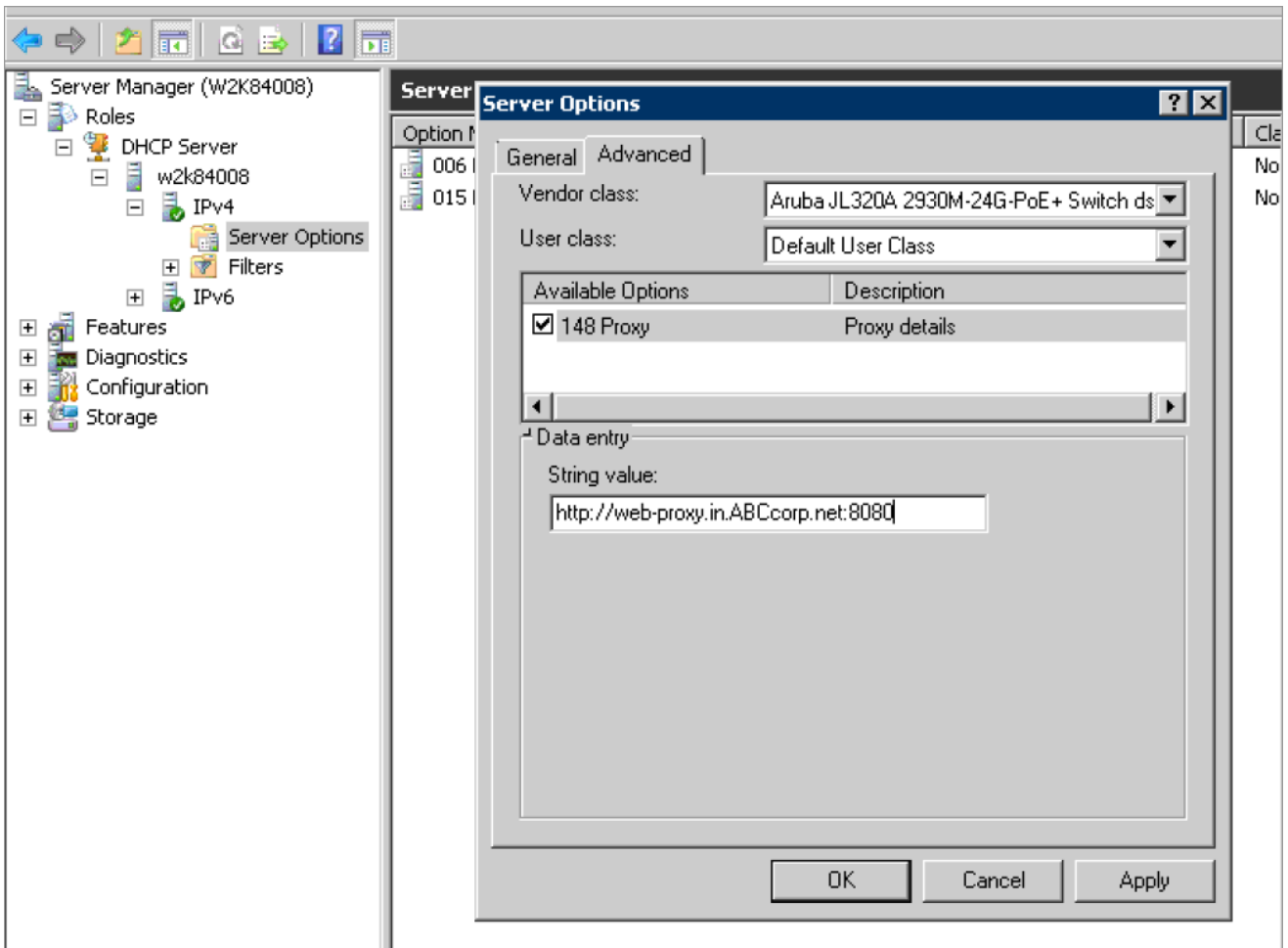
Now the new vendor class will have new suboption with code 148. Next is to add these vendor class and suboptions to the scope. To add proxy server details to scope, navigate to **Server Manager** and select **Server Options** in the **IPv4** window.

5. Right click server options and select **Configure options**. Go to **Advanced** tab, select the vendor class from the menu as the newly defined class. New suboptions that are added appears.

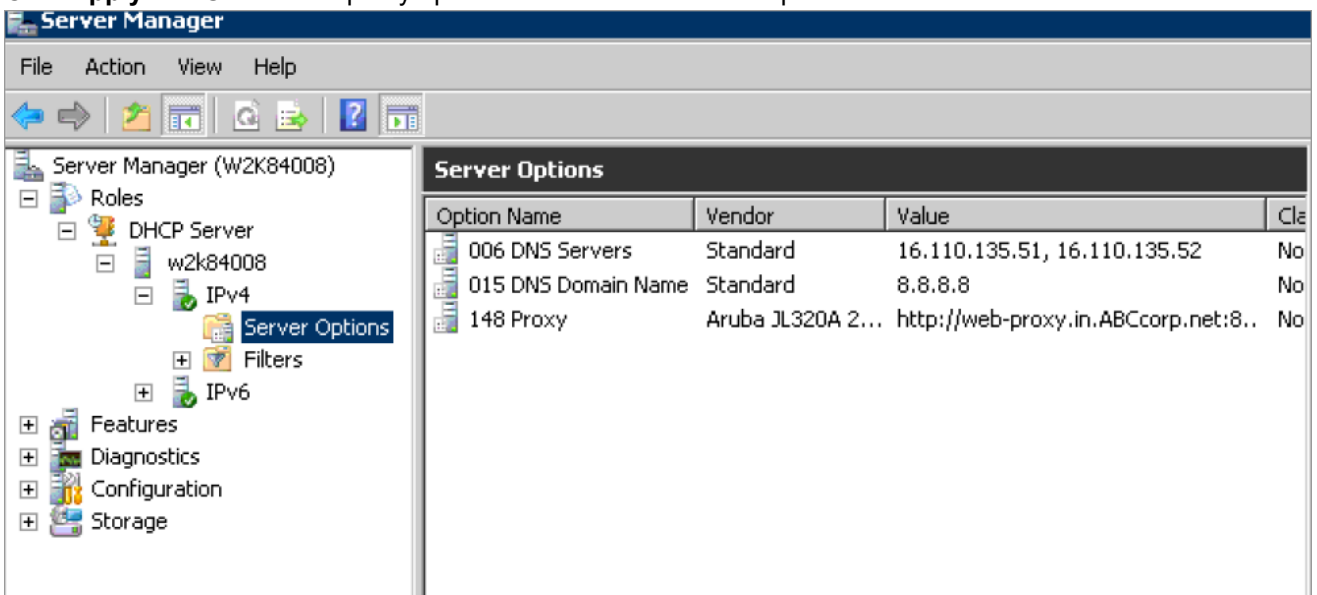
Check 148 and add Proxy details in string value field, in the format as mentioned:

<http://web-proxy.in.ABCcorp.net:8080> or <http://192.168.50.18:3128>

Check 144 and add configuration filename in string value field (optional).



- Click **Apply** and **OK** and the proxy option is added in the Server options.



- Now restart the DHCP service and download new DHCP attributes in the switch, you can check that the proxy details are correctly downloaded in the switch using the `show proxy config` command.

proxy server

Syntax

```
proxy server <http://<ip-addr/FQDN>:port number>
```

```
no proxy server
```

Description

Configures the URL/IP address to reach the proxy server. Provide the correct proxy port number along with the URL/IP address. Port number must be in the range of 1024 to 65535. HTTPS proxy server is not supported.

The `no` form of this command removes the proxy server.

Command context

```
config
```

Parameters

url:port number

Specifies the URL address with port number for the proxy server.

Parameters

ip-addr:port number

Specifies the IP address with port number for the proxy server.

Example

```
switch(config)# proxy server "http://web-proxy.au.abccorp.net:3128"  
switch(config)# proxy server "http://192.168.0.6:8080"
```

proxy exception ip | host

Syntax

```
proxy exception ip | host {ip-addr/mask-length | hostname}
```

```
no proxy exception ip | host {ip-addr/mask-length | hostname}
```

Description

Configures an IPv4 address/mask length and URL to the list of IP address and host, which can be reached without the HTTP proxy server.

The `no` form of this command removes the proxy exception for the specified entry (IPv4 address/host name).

Command context

```
config
```

Parameters

ip-addr/mask-length | hostname

Specifies IPv4 address/mask length and host name.

Example

```
switch(config)# proxy exception ip 192.168.0.10/12
switch(config)# proxy exception host "http://web-proxy.au.abdcorp.net:3128"
```

show proxy config

Syntax

```
show proxy config
```

Description

Shows the proxy configuration.

Command context

```
config
```

Examples

```
switch(config)# show proxy config

Http Proxy Configuration details

  Server URL           : http://web-proxy.au.abccorp.net:3128

Manually configured exceptions

  No      Exception
  -----
  1       192.168.0.10/12
  2       http://web-proxy.au.abdcorp.net:3128

Automatically added exceptions

  No      Exception
  -----
  1       2.0.0.9
```



NOTE: On configuring IPsec tunnel, Airwave IP is automatically added as an exception in the switch. The IPsec tunnel is configured directly over the network bypassing the HTTP proxy server.

LACP-MAD Passthrough commands

Configuration command

The following command defines whether LACP is enabled on a port, and whether it is in active or passive mode when enabled. When LACP is enabled and active, the port sends LACP packets and listens to them. When LACP is enabled and passive, the port sends LACP packets only if it is spoken to. When LACP is disabled, the port ignores LACP packets. If the command is issued without a mode parameter, 'active' is assumed. During dynamic link aggregation using LACP, ports with the same key are aggregated as a single trunk. MAD passthrough applies only to trunks and not to physical ports.

```
switch# no interface <port-list> lacp [mad-passthrough <enable|disable>|active|passive|key <key>]
```

show commands

LACP-MAD supports the following show commands:

- show LACP-MAD passthrough configuration on LACP trunks

```
switch# show lacp [counters [<port-list>] | local [<port-list>] |peer [<port-list>] | distributed | mad-passthrough [counters [<port-list>]]]
```

- show LACP-MAD passthrough counters on ports

```
switch# show lacp mad-passthrough counters [<port-list>]
```

clear command

Clear all LACP statistics including MAD passthrough counters. Resets LACP packets sent and received on all ports.

```
switch# clear lacp statistics
```

LACP-MAD overview

Link Aggregation Control Protocol-Multi-Active Detection (LACP-MAD) is a detection mechanism deployed by switches to recover from a breakup of the Virtual Switching Framework (VSF) stack due to link or other failure.

LACP-MAD is implemented by sending extended LACP data units (LACPDUs) with a type length value (TLV) that conveys the active ID of an VSF virtual device. The active ID is identical to the member ID of the master and is thus unique to the VSF virtual device. When LACP MAD detection is enabled, the members exchange their active IDs by sending extended LACPDUs.

- When the VSF virtual device operates normally, the active IDs in the extended LACPDUs sent by all members are the same, indicating that there is no multi-active collision.
- When there is a breakup in the VSF stack, the active IDs in the extended LACPDUs sent by the members in different VSF virtual devices are different, indicating that there are multi-active collisions.

LACP-MAD passthrough helps VSF-capable devices detect multi-access and take corrective action. These devices do not initiate transmission of LACP-MAD frames or participate in any MAD decision making process. These devices simply forward LACP-MAD TLVs received on one interface to the other interfaces on the trunk. LACP-MAD passthrough can be enabled for 24 LACP trunks. By default, LACP-MAD passthrough is disabled.

Overview

The switches support several methods for transferring files to and from a physically connected device or via the network, including TFTP and Xmodem. This appendix explains how to download new switch software, upload or download switch configuration files and software images, and upload command files for configuring ACLs.

Downloading switch software

Switch periodically provides switch software updates through the Switch Networking website. For more information, see the support and warranty booklet shipped with the switch, or visit <http://www.hpe.com/networking> and click on **software updates**.



NOTE: This manual uses the terms **switch software** and **software image** to refer to the downloadable software files the switch uses to operate its networking features. Other terms sometimes include **Operating System**, or **OS**.

General software download rules

- Switch software that you download via the menu interface always goes to primary flash.
- After a software download, you must reboot the switch to implement the new software. Until a reboot occurs, the switch continues to run on the software it was using before the download.



NOTE:

Downloading new switch software does not change the current switch configuration. The switch configuration is contained in separate files that can also be transferred. See **Transferring switch configurations** on page 316.

In most cases, if a power failure or other cause interrupts a flash image download, the switch reboots with the image previously stored in primary flash. In the unlikely event that the primary image is corrupted (which may occur if a download is interrupted by a power failure), the switch goes into boot ROM mode. In this case, use the boot ROM console to download a new image to primary flash.

Using TFTP to download software from a server

This procedure assumes that:

- A software version for the switch has been stored on a TFTP server accessible to the switch. (The software file is typically available from the Switch Networking website at <http://www.hpe.com/networking>.)
- The switch is properly connected to your network and has already been configured with a compatible IP address and subnet mask.
- The TFTP server is accessible to the switch via IP.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP server in which the software file has been stored.
- If VLANs are configured on the switch, determine the name of the VLAN in which the TFTP server is operating.
- Determine the name of the software file stored in the TFTP server for the switch (For example, E0820.swi).



NOTE: If your TFTP server is a UNIX workstation, ensure that the case (upper or lower) that you specify for the filename is the same case as the characters in the software filenames on the server.

Troubleshooting TFTP download failures

Cause

When using the menu interface, if a TFTP download fails, the Download OS (Operating System, or software) screen indicates the failure as seen in the following figure.

Figure 34: Example: of message for download failure

```

----- CONSOLE - MANAGER MODE -----
                          Download OS

Current Firmware revision : K.11.00

Method [TFTP] : TFTP
TFTP Server : 10.29.227.105

Remote File Name : os

                          Received 0 bytes of OS download.
+-----+
|                                     |
+-----+

Connection to 10.29.227.105 failed

Press any key to continue

```

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- Incorrect VLAN.
- Incorrect name specified for the **Remote File Name** parameter, or the specified file cannot be found on the TFTP server. This can also occur if the TFTP server is a UNIX machine and the case (upper or lower) for the filename on the server does not match the case for the filename entered for the **Remote File Name** parameter in the **Download OS** (Operating System, or software) screen.
- One or more of the switch's IP configuration parameters are incorrect.
- For a UNIX TFTP server, the file permissions for the software file do not allow the file to be copied.
- Another console session (through either a direct connection to a terminal device or through Telnet) was already running when you started the session in which the download was attempted.

To find more information on the cause of a download failure:

- Examine the messages in the switch's Event Log by executing the `show log tftp` command from the CLI.
- For descriptions of individual Event Log messages, see the latest version of the event log message reference guide for your switch, available on the Switch website. (See "Getting Documentation From the Web".)



NOTE: If an error occurs in which normal switch operation cannot be restored, the switch automatically reboots itself, and an appropriate message is displayed after the reboot.

Downloading from a server to flash using TFTP (CLI)

Syntax:

```
copy tftp flash <ip-address> <remote-file> [<primary | secondary>]
```

Automatically downloads a switch software file to primary or secondary flash. If you do not specify the flash destination, the TFTP download defaults to primary flash.

Example:

To download a switch software file named k0800.swi from a TFTP server with the IP address of 10.28.227.103 to primary flash:

Procedure

1. Execute `copy` as shown below:

The command to download an OS (switch software)

```
switch# copy tftp flash 10.28.227.103 k0800.swi
The primary OS Image will be deleted, continue [y/n]? y 1
01431K 2
```

- ¹This message means that the image you want to upload will replace the image currently in primary flash.
- ²Dynamic counter continually displays the number of bytes transferred.

When the switch finishes downloading the software file from the server, it displays this progress message:

```
Validating and Writing System Software to FLASH ...
```

2. When the download finishes, you must reboot the switch to implement the newly downloaded software image. To do so, use one of the following commands:

Syntax:

```
boot system flash {<primary | secondary>}
```

Boots from the selected flash.

Syntax:

```
reload
```

Boots from the flash image and startup-config file. A switch covered in this guide (with multiple configuration files), also uses the current startup-config file.

For more information on these commands, see "Rebooting the Switch" in the basic operation guide for your switch.

3. To confirm that the software downloaded correctly, execute `show system` and check the **Firmware revision** line.

For information on primary and secondary flash memory and the boot commands, see "Using Primary and Secondary Flash Image Options" in the basic operation guide for your switch.



NOTE: If you use `auto-tftp` to download a new image in a redundant management system, the active management module downloads the new image to both the active and standby modules. Rebooting after the `auto-tftp` process completes reboots the entire system.

Using SCP and SFTP

For some situations you may want to use a secure method to issue commands or copy files to the switch. By opening a secure, encrypted SSH session and enabling `ip ssh file transfer`, you can then use a third-party software application to take advantage of SCP and SFTP. SCP and SFTP provide a secure alternative to TFTP for transferring information that may be sensitive (like switch configuration files) to and from the switch. Essentially, you are creating a secure SSH tunnel as a way to transfer files with SFTP and SCP channels.

Once you have configured your switch to enable secure file transfers with SCP and SFTP, files can be copied to or from the switch in a secure (encrypted) environment and TFTP is no longer necessary.

To use these commands, you must install on the administrator workstation a third-party application software client that supports the SFTP and/or SCP functions. Some examples of software that supports SFTP and SCP are PuTTY, Open SSH, WinSCP, and SSH Secure Shell. Most of these are freeware and may be downloaded without cost or licensing from the internet. There are differences in the way these clients work, so be sure you also download the documentation.

As described earlier in this chapter you can use a TFTP client on the administrator workstation to update software images. This is a plain-text mechanism that connects to a standalone TFTP server or another switch acting as a TFTP server to obtain the software image files. Using SCP and SFTP allows you to maintain your switches with greater security. You can also roll out new software images with automated scripts that make it easier to upgrade multiple switches simultaneously and securely.

SFTP is unrelated to FTP, although there are some functional similarities. Once you set up an SFTP session through an SSH tunnel, some of the commands are the same as FTP commands. Certain commands are not allowed by the SFTP server on the switch, such as those that create files or folders. If you try to issue commands such as `create` or `remove` using SFTP, the switch server returns an error message.

You can use SFTP just as you would TFTP to transfer files to and from the switch, but with SFTP, your file transfers are encrypted and require authentication, so they are more secure than they would be using TFTP. SFTP works only with SSH version 2 (SSH v2).



NOTE: SFTP over SSH version 1 (SSH v1) is not supported. A request from either the client or the switch (or both) using SSH v1 generates an error message. The actual text of the error message differs, depending on the client software in use. Some examples are:

```
Protocol major versions differ: 2 vs. 1
Connection closed

Protocol major versions differ: 1 vs. 2
Connection closed

Received disconnect from <ip-addr> : /usr/local/libexec/
sftp-server: command not supported
Connection closed
```

SCP is an implementation of the BSD `r`cp (Berkeley UNIX remote copy) command tunneled through an SSH connection.

SCP is used to copy files to and from the switch when security is required. SCP works with both SSH v1 and SSH v2. Be aware that the most third-party software application clients that support SCP use SSHv1.

The general process for using SCP and SFTP involves three steps:

Procedure

1. Open an SSH tunnel between your computer and the switch if you have not already done so.
(This step assumes that you have already set up SSH on the switch.)
2. Execute `ip ssh filetransfer` to enable secure file transfer.
3. Use a third-party client application for SCP and SFTP commands.

Enabling SCP and SFTP

For more information about secure copy and SFTP, see [Using SCP and SFTP](#) on page 308.

Procedure

1. Open an SSH session as you normally would to establish a secure encrypted tunnel between your computer and the switch.

For more detailed directions on how to open an SSH session, see "Configuring secure shell (SSH)" in the access security guide for your switch. Please note that this is a one-time procedure for new switches or connections. If you have already done it once you should not need to do it a second time.

2. To enable secure file transfer on the switch (once you have an SSH session established between the switch and your computer), open a terminal window and enter the following command:

```
switch(config)# ip ssh filetransfer
```

For information on disabling TFTP and auto-TFTP, see [Disabling TFTP and auto-TFTP for enhanced security](#) on page 309.

Disabling TFTP and auto-TFTP for enhanced security

Using the `ip ssh filetransfer` command to enable SFTP automatically disables TFTP and auto-TFTP (if either or both are enabled), as shown below.

Switch configuration with SFTP enabled

```
switch(config)# ip ssh filetransfer
Tftp and auto-tftp have been disabled. 1
switch(config)# sho run
```

Running configuration:

```
; J9091A Configuration Editor; Created on release #xx.15.xx

hostname "Switch"
module 1 type J8702A
module 2 type J702A
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24,B1-B24
  ip address 10.28.234.176 255.255.240.0
```

```
exit
ip ssh filetransfer 2
no tftp-enable
password manager
password operator
```

¹ Enabling SFTP automatically disables TFTP and auto-tftp and displays this message.

² Viewing the configuration shows that SFTP is enabled and TFTP is disabled.

If you enable SFTP and then later disable it, TFTP and auto-TFTP remain disabled unless they are explicitly re-enabled.

Operating rules are:

- The TFTP feature is enabled by default, and can be enabled or disabled through the CLI or an SNMP application. Auto-TFTP is disabled by default and must be configured through the CLI.
- While SFTP is enabled, TFTP and auto-TFTP cannot be enabled from the CLI. Attempting to enable either non-secure TFTP option while SFTP is enabled produces one of the following messages in the CLI:

```
SFTP must be disabled before enabling tftp.
```

```
SFTP must be disabled before enabling auto-tftp.
```

Similarly, while SFTP is enabled, TFTP cannot be enabled using an SNMP management application. Attempting to do so generates an "inconsistent value" message. (An SNMP management application cannot be used to enable or disable auto-TFTP.)

- To enable SFTP by using an SNMP management application, you must first disable TFTP and, if configured, auto-TFTP on the switch. You can use either an SNMP application or the CLI to disable TFTP, but you must use the CLI to disable auto-TFTP.

Enabling SSH V2 (required for SFTP)

```
switch(config)# ip ssh version 2
```



NOTE: As a matter of policy, administrators should **not** enable the SSH V1-only or the SSH V1-or-V2 advertisement modes. SSHv1 is supported on only some legacy switches (such as the Switch Series 2500).

Confirming that SSH is enabled

```
switch(config)# show ip ssh
```

Once you have confirmed that you have enabled an SSH session (with the `show ip ssh` command), enter `ip ssh filetransfer` so that SCP and/or SFTP can run. You can then open your third-party software client application to begin using the SCP or SFTP commands to safely transfer files or issue commands to the switch.



NOTE:

Any attempts to use SCP or SFTP without using `ip ssh filetransfer` cause the SCP or SFTP session to fail. Depending on the client software in use, you will receive an error message on the originating console, for Example:

```
IP file transfer not enabled on the switch
```

Disabling secure file transfer

```
switch(config)# no ip ssh filetransfer
```

Authentication

Switch memory allows up to ten public keys. This means the authentication and encryption keys you use for your third-party client SCP/SFTP software can differ from the keys you use for the SSH session, even though both SCP and SFTP use a secure SSH tunnel.



NOTE:

SSH authentication is mutually exclusive with RADIUS servers.

Some clients, such as PSCP (PuTTY SCP), automatically compare switch host keys for you. Other clients require you to manually copy and paste keys to the `$HOME/.ssh/known_hosts` file. Whatever SCP/SFTP software tool you use, after installing the client software you must verify that the switch host keys are available to the client.

Because the third-party software utilities you may use for SCP/SFTP vary, you should refer to the documentation provided with the utility you select before performing this process.

SCP/SFTP operating notes

- Any attempts to use SCP or SFTP without using `ip ssh filetransfer` will cause the SCP or SFTP session to fail. Depending on the client software in use, you will receive an error message on the originating console, for Example:

```
IP file transfer not enabled on the switch
```

- There is a delay when SFTP is copying an image onto the switch, and although the command prompt returns in a couple of seconds, the switch may take approximately a minute and half writing the image to flash. You can keep entering the `show flash` command to see when the copy is complete and the flash is updated. You can also check the log for an entry similar to the following:

```
I 01/09/13 16:17:07 00150 update: Primary Image updated.
```

```
I 01/09/13 16:13:22 00636 ssh: sftp session from 15.22.22.03
```

- When an SFTP client connects, the switch provides a file system displaying all of its available files and folders. No file or directory creation is permitted by the user. Files may be only uploaded or downloaded, according to the permissions mask. All of the necessary files the switch needs are already in place on the switch. You do not need to (nor can you) create new files.
- The switch supports one SFTP session or one SCP session at a time.
- All files have read-write permission. Several SFTP commands, such as `create` or `remove`, are not allowed and return an error message. The switch displays the following files:

```
/
+---cfg
|  running-config
|  startup-config
+---log
|  crash-data
|  crash-data-a
|  crash-data-b
|  crash-data-c
|  crash-data-d
|  crash-data-e      "      "
|  crash-data-f ""
|  crash-data-g
|  crash-data-h      "      "
|  crash-data-I ""
|  crash-data-J ""
|  crash-data-K ""
|  crash-data-L "      "
|  crash-log
```

```

| crash-log-a
| crash-log-b
| crash-log-c
| crash-log-d
| crash-log-e""
| crash-log-f""
| crash-log-g
| crash-log-h" "
| crash-log-I" "
| crash-log-J" "
| crash-log-K" "
| crash-log-L" "
| event log
+---os
| primary
| secondary
\---ssh
+---mgr_keys
| authorized_keys
\---oper_keys
| authorized_keys
\---core
| port_1-24.cor core-dump for ports 1-24 (stackable switches only)
| port_25-48.cor core-dump for ports 25-48 (stackable switches only)

```

Once you have configured your switch for secure file transfers with SCP and SFTP, files can be copied to or from the switch in a secure (encrypted) environment and TFTP is no longer necessary.

Troubleshooting SSH, SFTP, and SCP operations

Cause

You can verify secure file transfer operations by checking the switch's event log, or by viewing the error messages sent by the switch that most SCP and SFTP clients print out on their console.



NOTE: Messages that are sent by the switch to the client depend on the client software in use to display them on the user console.

Broken SSH connection

If an ssh connection is broken at the wrong moment (for instance, the link goes away or spanning tree brings down the link), a fatal exception occurs on the switch. If this happens, the switch gracefully exits the session and produces an Event Log message indicating the cause of failure. The following three examples show the error messages that may appear in the log, depending on the type of session that is running (SSH, SCP, or SFTP):

```

ssh: read error Bad file number, session aborted I 01/01/90
00:06:11 00636 ssh: sftp session from ::ffff:10.0.12.35 W
01/01/90 00:06:26 00641 ssh:

sftp read error Bad file number, session aborted I 01/01/90
00:09:54 00637 ssh: scp session from ::ffff:10.0.12.35 W 01/
01/90

ssh: scp read error Bad file number, session aborted

```



NOTE:

The `Bad file number` is from the system error value and may differ depending on the cause of the failure. In the third Example:, the device file to read was closed as the device read was about to occur.

Attempt to start a session during a flash write

If you attempt to start an SCP (or SFTP) session while a flash write is in progress, the switch does not allow the SCP or SFTP session to start. Depending on the client software in use, the following error message may appear on the client console:

```
Received disconnect from 10.0.12.31: 2: Flash access in
progress
lost connection
```

Failure to exit from a previous session

This next Example: shows the error message that may appear on the client console if a new SCP (or SFTP) session is started from a client before the previous client session has been closed (the switch requires approximately ten seconds to timeout the previous session):

```
Received disconnect from 10.0.12.31: 2: Wait for previous
session to complete
lost connection
```

Attempt to start a second session

The switch supports only one SFTP session or one SCP session at a time. If a second session is initiated (For example, an SFTP session is running and then an SCP session is attempted), the following error message may appear on the client console:

```
Received disconnect from 10.0.12.31: 2: Other SCP/SFTP
session running
lost connection
```

Using Xmodem to download switch software from a PC or UNIX workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (For information on connecting a PC as a terminal and running the switch console interface, see the installation and getting started guide you received with the switch.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the **Send File** option in the **Transfer** drop-down menu.)

Downloading to primary or secondary flash using Xmodem and a terminal emulator (CLI)

Syntax:

```
copy xmodem flash [<primary | secondary>]
```

Downloads a software file to primary or secondary flash. If you do not specify the flash destination, the Xmodem download defaults to primary flash.

Example:

To download a switch software file named `E0822.swi` from a PC (running a terminal emulator program such as HyperTerminal) to primary flash:

Procedure

1. Execute the following command in the CLI:

```
switch# copy xmodem flash
Press 'Enter and start XMODEM on your host...
```

2. Execute the terminal emulator commands to begin the Xmodem transfer. For example, using HyperTerminal:
 - a. Click on **Transfer**, then **Send File**.
 - b. Type the file path and name in the Filename field.
 - c. In the Protocol field, select **Xmodem**.
 - d. Click on the **[Send]** button.

The download can take several minutes, depending on the baud rate used in the transfer.

3. When the download finishes, you must reboot the switch to implement the newly downloaded software. To do so, use one of the following commands:

Syntax:

```
boot system flash {<primary | secondary>}
```

Reboots from the selected flash

Syntax:

```
reload
```

Reboots from the flash image currently in use

For more information on these commands, see "Rebooting the Switches" in the basic operation guide for your switch.

4. To confirm that the software downloaded correctly:

```
switch# show system
```

Check the **Firmware revision** line. It should show the software version that you downloaded in the preceding steps.

If you need information on primary/secondary flash memory and the boot commands, see "Using Primary and Secondary Flash Image Options" in the basic operation guide for your switch.

Switch-to-switch download

You can use TFTP to transfer a software image between two switches of the same series. The CLI enables all combinations of flash location options.

Downloading the OS from another switch (CLI)

Where two switches in your network belong to the same series, you can download a software image between them by initiating a `copy tftp` command from the destination switch. The options for this CLI feature include:

- Copy from primary flash in the source to either primary or secondary in the destination.
- Copy from either primary or secondary flash in the source to either primary or secondary flash in the destination.

Downloading from primary only (CLI)

Syntax:

```
copy tftp flash <ip-addr> flash [primary | secondary]
```

When executed in the destination switch, downloads the software flash in the source switch's primary flash to either the primary or secondary flash in the destination switch.

If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.

To download a software file from primary flash in a switch with an IP address of 10.29.227.103 to the primary flash in the destination switch, you would execute the following command in the destination switch's CLI:

Switch-to-switch, from primary in source to either flash in destination

```
switch# copy tftp flash 10.29.227.13 flash
Device will be rebooted, do you want to continue [y/n]? y
00107K 1
```

¹Running Total of Bytes Downloaded

Downloading from either flash in the source switch to either flash in the destination switch (CLI)

Syntax:

```
copy tftp flash <ip-addr> {</os/primary> | </os/secondary>} [primary | secondary]
```

This command (executed in the destination switch) gives you the most options for downloading between switches. If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.

To download a software file from secondary flash in a switch with an IP address of 10.28.227.103 to the secondary flash in a destination switch, you would execute the following command in the destination switch's CLI:

Switch-to-switch, from either flash in source to either flash in destination

```
switch# copy tftp flash 10.29.227.13 flash /os/secondary secondary
Device will be rebooted, do you want to continue [y/n]? y
00184K
```

Using AirWave to update switch software

AirWave can be used to update switch products. For further information, refer to the **ZTP with Airwave network Management** chapter in this manual.

Copying software images



NOTE:

For details on how switch memory operates, including primary and secondary flash, see “Switch Memory and Configuration” in the basic operation guide for your switch.

TFTP: Copying a software image to a remote host (CLI)

Syntax:

```
copy flash tftp <ip-addr> <filename>
```

Copies the primary flash image to a TFTP server.

Example:

To copy the primary flash to a TFTP server having an IP address of 10.28.227.105:

```
switch# copy flash tftp 10.28.227.105 k0800.swi
```

where `k0800.swi` is the filename given to the flash image being copied.

Xmodem: Copying a software image from the switch to a serially connected PC or UNIX workstation (CLI)

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation.

Syntax:

```
copy flash xmodem {[<pc> | unix>]}
```

Uses Xmodem to copy a designated configuration file from the switch to a PC or UNIX workstation.

Example:

To copy the primary flash image to a serially connected PC:

Procedure

1. Execute the following command:

```
switch# copy xmodem flash  
Press 'Enter' and start XMODEM on your host...
```

2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.

Transferring switch configurations

Using the CLI commands described in the section beginning with **TFTP: Copying a configuration file to a remote host (CLI)** on page 317, you can copy switch configurations to and from a switch, or copy a software image to configure or replace an ACL in the switch configuration.

**NOTE:**

For greater security, you can perform all TFTP operations using SFTP, as described in the section **Using SCP and SFTP** on page 308.

You can also use the `include-credentials` command to save passwords, secret keys, and other security credentials in the running config file. For more information, see the section on "Saving Security Credentials in a Config File" in the access security guide for your switch.

TFTP: Copying a configuration file to a remote host (CLI)

Syntax:

```
copy {<startup-config | running-config>} tftp < ip-addr > < remote-file > [pc | unix]
```

```
copy config <filename> tftp <ip-addr> <remote-file> [pc | unix]
```

This command can copy a designated config file in the switch to a TFTP server. For more information, see "Multiple Configuration Files" in the basic operation guide for your switch.

Example:

To upload the current startup configuration to a file named `sw8200` in the `configs` directory on drive `"d"` in a TFTP server having an IP address of 10.28.227.105:

```
switch# copy startup-config tftp 10.28.227.105
d:\configs\sw8200
```

TFTP: Copying a configuration file from a remote host (CLI)

Syntax:

```
copy tftp {<startup-config | running-config> < ip-address > < remote-file >} [pc | unix]
```

```
copy tftp config <filename> <ip-address> <remote-file> [pc | unix]
```

This command can copy a configuration from a remote host to a designated config file in the switch. For more information, see "Multiple Configuration Files" in the basic operation guide for your switch.

For more information on flash image use, see "Using Primary and Secondary Flash Image Options" in the basic operation guide for your switch.

Example:

To download a configuration file named `sw8200` in the `configs` directory on drive `"d"` in a remote host having an IP address of 10.28.227.105:

```
switch# copy tftp startup-config 10.28.227.105
d:\configs\sw8200
```

TFTP: Copying a customized command file to a switch (CLI)

Using the `copy tftp` command with the `show-tech` option provides the ability to copy a customized command file to the switch. When the `show tech custom` command is executed, the commands in the custom file are executed instead of the hard-coded list of commands. If no custom file is found, the current hard-coded list is executed. This list contains commands to display data, such as the image stamp, running configuration, boot history, port settings, and so on.

Syntax:

```
copy tftp show-tech <ipv4 or ipv6 address> <filename>
```

Copies a customized command file to the switch (see [Using the copy tftp show-tech command to upload a customized command file](#) on page 318).

Using the copy tftp show-tech command to upload a customized command file

```
switch(config)# copy tftp show-tech 10.10.10.3 commandfile1
```

Syntax:

```
show tech custom
```

Executes the commands found in a custom file instead of the hard-coded list.

**NOTE:**

Exit the global config mode (if needed) before executing `show tech` commands.

You can include `show tech` commands in the custom file, with the exception of `show tech custom`. For example, you can include the command `show tech all`.

If no custom file is found, a message displays stating "No SHOW-TECH file found." (No custom file was uploaded with the `copy tftp show-tech` command.)

The show tech custom command

```
switch# show tech custom  
No SHOW-TECH file found.
```

Xmodem: Copying a configuration file to a serially connected PC or UNIX workstation (CLI)

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation. You will need to:

- Determine a filename to use
- Know the directory path you will use to store the configuration file.

Syntax:

```
copy {<startup-config | running-config>} xmodem {<pc | unix>}
```

```
copy config <filename> xmodem {<pc | unix>}
```

Uses Xmodem to copy a designated configuration file from the switch to a PC or UNIX workstation. For more information, see "Multiple Configuration Files" in the basic operation guide for your switch.

Example:

To copy a configuration file to a PC serially connected to the switch:

1. Determine the file name and directory location on the PC.
2. Execute the following command:

```
switch# copy startup-config xmodem pc
Press 'Enter' and start XMODEM on your host...
```

3. After you see the above prompt, press **[Enter]**.
4. Execute the terminal emulator commands to begin the file transfer.

Xmodem: Copying a configuration file from a serially connected PC or UNIX workstation (CLI)

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation on which is stored the configuration file you want to copy. To complete the copying, you need to know the name of the file to copy and the drive and directory location of the file.

Syntax:

```
copy xmodem startup-config {<pc | unix>}
```

```
copy xmodem config <filename> < {pc | unix}>
```

Copies a configuration file from a serially connected PC or UNIX workstation to a designated configuration file on the switch.

For more information, see "Multiple Configuration Files" in the basic operation guide for your switch.

Example:

To copy a configuration file from a PC serially connected to the switch:

Procedure

1. Execute the following command:

```
switch# copy xmodem startup-config pc
Device will be rebooted, do you want to continue [y/n]? y
Press 'Enter' and start XMODEM on your host...
```

2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.
4. When the download finishes, you must reboot the switch to implement the newly downloaded software. To do so, use one of the following commands:

Syntax:

```
boot system flash [primary | secondary]
```

```
boot system flash [config < filename >]
```

Switches boot from the designated configuration file. For more information, see "Multiple Configuration Files" in the basic operation guide for your switch.

Syntax:

```
reload
```

Reboots from the flash image currently in use.

(For more on these commands, see "Rebooting the Switch" in the basic operation guide for your switch.)

Overview

The switches have several built-in tools for monitoring, analyzing, and troubleshooting switch and network operation:

- **Status:** Includes options for displaying general switch information, management address data, port status, port and trunk group statistics, MAC addresses detected on each port or VLAN, and STP, IGMP, and VLAN data.
- **Counters:** Display details of traffic volume on individual ports.
- **Event Log:** Lists switch operating events ([Using the Event Log for troubleshooting switch problems](#) on page 364).
- **Alert Log:** Lists network occurrences detected by the switch—in the System > Logging screen of the WebAgent.
- **Configurable trap receivers:** Uses SNMP to enable management stations on your network to receive SNMP traps from the switch.
- **Port monitoring (mirroring):** Copy all traffic from the specified ports to a designated monitoring port.



NOTE: Link test and ping test—analysis tools in troubleshooting situations—are described in [Troubleshooting](#) on page 334. See [Diagnostic tools](#) on page 402.

Accessing port and trunk group statistics

Use the CLI to view port counter summary reports, and to view detailed traffic summary for specific ports.

Trunk bandwidth utilization

- Trunk interface counters display the accumulated statistics over the trunk members' ports since the time they are added into trunk.
- Bandwidth utilization for trunks is calculated by averaging the value of the sum of bandwidth utilization for each trunk member in the last 5 minute interval .

`show interfaces`

Syntax

```
show interfaces [brief | config | <PORT-LIST>]
```

Description

Shows interface information for ports or trunk groups in brief or configuration detail.

Command context

```
operator or manager
```


Parameters

brief

Shows the current operating status for all ports or trunk groups on the switch in brief detail.

config

Shows the configuration data for all ports or trunk groups on the switch.

<PORT-LIST>

Specifies the list of ports for which status information will be shown.

<TRUNK-GROUP>

Specifies the trunk group for which status information will be shown. The status information shown consists of total transmit and receive counters and weighted average rate for the trunk group specified. The weighted average rate is calculated in 5 minute intervals.

Usage

Both external and internal ports are supported on the same module. Internal ports have an "I" suffix in the output of the show command to indicate that they are internal ports.

- "10GbE-INT" – Internal 10G data-plane ports (1i-2i, 4i-5i)
- "1GbE-INT" – Internal 1G control-plane port (3i)
- Port 3i always shows as link-down.

Examples

Show brief information and status of all interfaces.

```
switch# show interfaces brief
```

```
Status and Counters - Port Status
```

Port	Type	Intrusion Alert	Enabled	Status	Mode	MDI Mode	Flow Ctrl	Bcast Limit
B1	100/1000T	No	Yes	Down	Auto-10-100	Auto	off	0
B2	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B3	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B4	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B5	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B6	100/1000T	No	Yes	Down	1000FDx	Auto	off	0

Show the configuration of the interfaces currently available.

```
switch# show interfaces config
```

```
Port Settings
```

Port	Type	Enabled	Mode	Flow Ctrl	MDI
B1	100/1000T	Yes	Auto-10-100	Disable	Auto
B2	100/1000T	Yes	Auto	Disable	Auto
B3	100/1000T	Yes	Auto	Disable	Auto
B4	100/1000T	Yes	Auto	Disable	Auto
B5	100/1000T	Yes	Auto	Disable	Auto
B6	100/1000T	Yes	Auto	Disable	Auto

Show brief information and status of interfaces for ports D1i, D2i, and D3i.

```
switch# show interfaces brief d1i-d3i
```

```
Status and Counters - Port Status
Port      Type      | Intrusion
          | Alert      Enabled Status Mode      MDI Flow Bcast
          |           |           |           |           | Mode Ctrl Limit
-----+-----
D1i      10GbE-INT | No        Yes    Up    10GigFD  NA  off  0
D2i      10GbE-INT | No        Yes    Up    10GigFD  NA  off  0
D3i      1GbE-INT  | No        Yes    Down  1000FDx  NA  off  0
```

Show the brief information and status of interfaces for ports B1 through internal port B3i.

```
switch# show interfaces brief b1-b3i
```

```
Status and Counters - Port Status
Port      Type      | Intrusion
          | Alert      Enabled Status Mode      MDI Flow Bcast
          |           |           |           |           | Mode Ctrl Limit
-----+-----
B1        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B2        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B3        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B4        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B5        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B6        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B7        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B8        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B9        100/1000T | No        Yes    Down  1000FDx  Auto off  0
B10       100/1000T | No        Yes    Down  1000FDx  Auto off  0
B11       100/1000T | No        Yes    Down  1000FDx  Auto off  0
B12       100/1000T | No        Yes    Down  1000FDx  Auto off  0
B1i       10GbE-INT | No        Yes    Up    10GigFD  NA  off  0
B2i       10GbE-INT | No        Yes    Up    10GigFD  NA  off  0
B3i       1GbE-INT  | No        Yes    Up    1000FDx  NA  off  0
```

Show detailed interface information for port trunk 1.

```
switch# show interface trk1
```

```
Status and Counters - Port Counters for port Trk1
Name      : Trk1
MAC Address      : 3464a9-b1b8bf
Link Status     : Up
Totals (Since boot or last clear) :
  Bytes Rx      : 777,713,956      Bytes Tx      : 596,853,141
  Unicast Rx    : 1,154,693      Unicast Tx    : 0
  Bcast/Mcast Rx : 48,563      Bcast/Mcast Tx : 607,474,910
Errors (Since boot or last clear) :
  FCS Rx       : 0      Drops Tx      : 0
  Alignment Rx : 0      Collisions Tx : 0
  Runts Rx     : 0      Late Colln    : 0
  Giants Rx    : 0      Excessive Colln : 0
  Total Rx Errors : 0      Deferred Tx   : 0
Others (Since boot or last clear) :
  Discard Rx   : 0      Out Queue Len : 0
  Unknown Protos : 0
Rates (5 minute weighted average) :
  Total Rx(Kbps) : 76,800      Total Tx(Kbps) : 76,800
  Unicast Rx (Pkts/sec) : 21      Unicast Tx (Pkts/sec) : 0
  B/Mcast Rx (Pkts/sec) : 114,878      B/Mcast Tx (Pkts/sec) : 114,900
  Utilization Rx : 00.76 %
Utilization Tx  : 00.76 %
```

show interfaces trunk-utilization

Syntax

```
show interfaces trunk-utilization
```

Description

Shows the bandwidth utilization calculations for all trunk members.

Command context

operator or manager

Example

Show bandwidth utilization for trunks.

```
Switch(config)# show interfaces trunk-utilization
```

```
Status and Counters - Port Utilization
```

Port	Rx			Tx		
	Kbits/sec	Pkts/sec	Util	Kbits/sec	Pkts/sec	Util
Trk1	0	0	0	0	0	0
Trk2	0	0	0	0	0	0
Trk10	0	0	0	0	0	0

Statistic interactions of interface counters

Table 25: Statistic interactions

Interface counters are cleared using the command `clear statistics`. When certain actions are taken to ports and trunks, the outcome of the `clear` command differs.

Action taken	Trigger	Interaction with interface counter
Adding Port into trunk	CLI/SNMP	<ul style="list-style-type: none">Interface counters for this port will be cleared across all sessions.Average rate counters are not cleared.
Removing Port from trunk	CLI/SNMP	<ul style="list-style-type: none">Interface counters for this port will be cleared across all sessions.Average rate counters are not cleared.
Trunk port coming Up	CLI enable	<ul style="list-style-type: none">No change in counters.Interface counters for this port are not cleared.Average rate counters are not cleared. Counters will start from 0 when the trunk port comes up.

Table Continued

Action taken	Trigger	Interaction with interface counter
Trunk port coming Up	Cable connect	<ul style="list-style-type: none"> No change in counters. Interface counters for this port are not cleared. Average rate counters are not cleared. Counters will start from 0 when the trunk port comes up.
Trunk port going Down	CLI disable	<ul style="list-style-type: none"> Interface counters for this port are not cleared. Average rate counters are cleared.
Trunk port going Down	Cable disconnect	<ul style="list-style-type: none"> Interface counters for this port are not cleared. Average rate counters are cleared.
Trunk port going Down	Module crash/ module reload	<ul style="list-style-type: none"> Interface counters for this port are not cleared. Average rate counters are cleared.
Trunk port going Down	Save power - off	<ul style="list-style-type: none"> Interface counters for this port are not cleared. Average rate counters are cleared.
Trunk port going Down	Stacking member reboot/ crash/shutdown.	<ul style="list-style-type: none"> Interface counters for this port are not cleared. Average rate counters of this port is not cleared. Utilization for the port is cleared. Utilization for the trunk group is updated accordingly
Trunk port going Down	Module remove/ member remove.	<ul style="list-style-type: none"> Statistics for removed trunk port can not be accessed as the port is removed. Interface counters for the trunk group is updated. Utilization for the trunk group is updated.
Clear statistics on physical port which is part of trunk	CLI	<ul style="list-style-type: none"> Not allowed. The error message <code>Module not present for port or invalid port: <PORT-NUM></code> displays when the command <code>clear statistics</code> is executed on a port which part of a trunk.
Clear statistics on trunk.	CLI	<ul style="list-style-type: none"> Interface counters for physical ports which are part of trunk will be cleared. Average rate counters are not cleared.

Reset port counters

When troubleshooting network issues, you can clear all counters and statistics without rebooting the switch using the `clear statistics global` command or using the menu.

SNMP displays the counter and statistics totals accumulated since the last reboot, and it is not affected by the `clear statistics global` command or the `clear statistics <PORT-LIST>` command. Clearing statistics initiates an SNMP trap.



IMPORTANT: Once cleared, statistics cannot be reintroduced.

clear statistics

Syntax

```
clear statistics [<PORT-LIST>|global]
```

Description

This command clears all counters and statistics for all interfaces except SNMP.

Parameters and options

<PORT-LIST>

Clears the counters and statistics for specific ports.

global

Clears all counters and statistics for all interfaces except SNMP.

MAC address tables

MAC address views and searches

You can view and search MAC addresses using the CLI or the menu.

show mac-address

Syntax

```
show mac-address [vlan <VLAN-ID>] [<PORT-LIST>] [<MAC-ADDR>]
```

Description

Lists all MAC addresses on the switch and their corresponding port numbers. You can also choose to list specific addresses and ports, or addresses and ports on a VLAN. The switches operate with a multiple forwarding database architecture.

List all learned MAC addresses on the switch and corresponding port numbers

```
switch# show mac-address
```

List all learned MAC addresses on one or more ports and corresponding port numbers

```
switch# show mac-address a1-a4,a6
```

List all learned MAC addresses on a VLAN and corresponding port numbers

```
switch# show mac-address vlan 100
```

List the port on which the switch learned a specific MAC address

To find the port on which the switch learns a MAC address of 080009-21ae84:

```
Select VLAN : DEFAULT VLAN
```

Using the menu to view and search MAC addresses

To determine which switch port on a selected VLAN the switch uses to communicate with a specific device on the network:

Procedure

1. From the Main Menu, select **1. Status and Counters ...**, and then select **5. VLAN Address Table**.
2. Use the arrow keys to scroll to the VLAN you want, and then press **Enter** on the keyboard to select it.

```
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Address Table

  MAC Address  Located on Port
-----
0030c1-7f49c0  A3
0030c1-7fec40  A1
0030c1-b29ac0  A3
0060b0-17de5b  A3
0060b0-880a80  A2
0060b0-df1a00  A3
0060b0-df2a00  A3
0060b0-e9a200  A3
009027-e74f90  A3
080009-21ae84  A3
080009-62c411  A3
080009-6563e2  A3

Actions-> Back   Search   Next page   Prev page   Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

The switch then displays the MAC address table for that VLAN ([Figure 35: Example of the address table on page 326.](#))

Figure 35: Example of the address table

```
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Address Table

  MAC Address  Located on Port
-----
0030c1-7fcc6d  2
005004-17df9c  1
0060b0-889e00  1
```

Located MAC address and corresponding port number

3. To page through the listing, use **Next page** and **Prev page**.

Finding the port connection for a specific device on a VLAN

This feature uses a device's MAC address that you enter to identify the port used by that device.

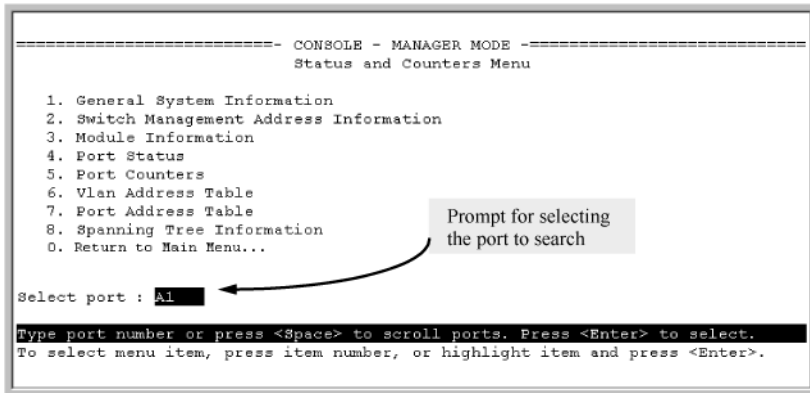
Procedure

1. Proceeding from **Figure 35: Example of the address table** on page 326, press **[S]** (for **Search**), to display the following prompt:

```
Enter MAC address: _
```

2. Enter the MAC address you want to locate and press **[Enter]**.
3. The address and port number are highlighted if found (**Figure 36: Example of menu indicating located MAC address** on page 327.) If the switch does not find the MAC address on the currently selected VLAN, it leaves the MAC address listing empty.

Figure 36: Example of menu indicating located MAC address



```
----- CONSOLE - MANAGER MODE -----  
                Status and Counters Menu  
  
1. General System Information  
2. Switch Management Address Information  
3. Module Information  
4. Port Status  
5. Port Counters  
6. Vlan Address Table  
7. Port Address Table  
8. Spanning Tree Information  
0. Return to Main Menu...  
  
Select port : A1  
Type port number or press <Space> to scroll ports. Press <Enter> to select.  
To select menu item, press item number, or highlight item and press <Enter>
```

4. Press **[P]** (for **Prev page**) to return to the full address table listing.

Viewing and searching port-level MAC addresses

This feature displays and searches for MAC addresses on the specified port instead of for all ports on the switch.

Procedure

1. From the Main Menu, select:
 1. Status and Counters ...
 7. Port Address Table
2. Use the Space bar to select the port you want to list or search for MAC addresses, then press **[Enter]** to list the MAC addresses detected on that port.

Determining whether a specific device is connected to the selected port

Proceeding from Step 2, above:

Procedure

1. Press **[S]** (for **Search**), to display the following prompt:

```
Enter MAC address: _
```

2. Enter the MAC address you want to locate and press **[Enter]**.

The address is highlighted if found. If the switch does not find the address, it leaves the MAC address listing empty.

3. Press **[P]** (for **Prev page**) to return to the previous per-port listing.

MSTP data

show spanning-tree

Syntax

```
show spanning-tree
```

Description

Displays the global and regional spanning-tree status for the switch, and displays the per-port spanning-tree operation at the regional level.

Values for the following parameters appear only for ports connected to active devices: Designated Bridge, Hello Time, PtP, and Edge.

show spanning-tree command output

Figure 37: show spanning-tree command output

```
Switch(config)# show spanning-tree
```

Multiple Spanning Tree (MST) Information

```

STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1,66

Switch MAC Address : 0004ea-5e2000
Switch Priority    : 32768
Max Age          : 20
Max Hops         : 20
Forward Delay     : 15

Topology Change Count : 0
Time Since Last Change : 2 hours

CST Root MAC Address : 00022d-47367f
CST Root Priority     : 0
CST Root Path Cost   : 4000000
CST Root Port        : A1

IST Regional Root MAC Address : 00883-028300
IST Regional Root Priority     : 32768
IST Regional Root Path Cost    : 200000
IST Remaining Hops             : 19

Protected Ports : A4
Filtered Ports  : A7-A10

```

Switch's Spanning Tree Configuration and Identity of VLANs Configured in the Switch for the IST Instance

Identifies the overall spanning-tree root for the network.

Lists the switch's MSTP root data for connectivity with other regions and STP or RSTP devices.

Identifies the spanning-tree root for the IST Instance for the region.

Internal Spanning Tree Data (IST Instance) for the region in which the Switch Operates

Identifies the ports with BPDU protection and BPDU filtering enabled.

Yes means the switch is operating the port as if it is connected to switch, bridge, or end node (but *not* a hub).

Port	Type	Cost	Prio	State	Designated	Hello	PTP	Edge
			rity		Bridge	Time		
A1	100/1000T	Auto	128	Forwarding	000883-028300	9	Yes	No
A2	100/1000T	Auto	128	Blocked	0001e7-948300	9	Yes	No
A3	100/1000T	Auto	128	Forwarding	000883-02a700	2	Yes	No
A4	100/1000T	Auto	128	Disabled				
A5	100/1000T	Auto	128	Disabled				
.				
.				

For **Edge, No** (**admin-edge-port** operation disabled) indicates the port is configured for connecting to a LAN segment that includes a bridge or switch. **Yes** indicates the port is configured for a host (end node) link. Refer to the **admin-edge-port** description under "Configuring MSTP Per-Port Parameters" on page 3-24.

IP IGMP status

show ip igmp

Syntax

```
show ip igmp <VLAN-ID> [config] [group <IP-ADDR>|groups] [statistics]
```

Description

Global command that lists IGMP status for all VLANs configured in the switch, including:

- VLAN ID (VID) and name
- Querier address
- Active group addresses per VLAN
- Number of report and query packets per group
- Querier access port per VLAN

Parameters and options

config

Displays the IGMP configuration information, including VLAN ID, VLAN name, status, forwarding, and Querier information.

vlan-id

Per-VLAN command listing above, IGMP status for specified VLAN (VID).

group <IP-ADDR>

Lists the ports currently participating in the specified group, with port type, Access type, Age Timer data and Leave Timer data.

groups

Displays VLAN-ID, group address, uptime, expiration time, multicast filter type, and the last reporter for IGMP groups.

statistics

Displays IGMP operational information, such as VLAN IDs and names, and filtered and flooding statistics.

Output from show ip igmp config command

```
Switch(config)# show ip igmp config

IGMP Service

VLAN ID  VLAN Name      IGMP   Forward with  Querier Querier
-----  -
1         DEFAULT_VLAN  No     No            Yes     125
2         VLAN2         Yes    No            Yes     125
12        New_Vlan      No     No            Yes     125
```

IGMP statistical information

```
switch(vlan-2)# show ip igmp statistics
```

IGMP Service Statistics

```
Total VLANs with IGMP enabled      : 1
Current count of multicast groups joined : 1
```

IGMP Joined Groups Statistics

VLAN ID	VLAN Name	Filtered	Flood
2	VLAN2	2	1

VLAN information

show vlan

Syntax

```
show vlan <VLAN-ID>
```

Description

Lists the maximum number of VLANs to support, existing VLANs, VLAN status (static or dynamic), and primary VLAN.

Parameters

<VLAN-ID>

Lists the following for the specified VLAN:

- Name, VID, and status (static/dynamic)
- Per-port mode (tagged, untagged, forbid, no/auto)
- "Unknown VLAN" setting (Learn, Block, Disable)
- Port status (up/down)

List data on specific VLANs

The next three figures show how you can list data for the following VLANs:

Ports	VLAN	VID
A1-A12	DEFAULT_VLAN	1

Table Continued

A1, A2	VLAN-33	33
A3, A4	VLAN-44	44

Figure 38: Listing the VLAN ID (vid) and status for specific ports

```
Switch# show vlan ports A1-A2
Status and Counters = VLAN Information - for ports A1,A2

802.1Q VLAN ID Name          Status
-----
1          DEFAULT_VLAN        Static
33         VLAN-33             Static
```

Because ports A1 and A2 are not members of VLAN-44, it does not appear in this listing.

Figure 39: Example of VLAN listing for the entire switch

```
Switch# show vlan
Status and Counters - VLAN Information

VLAN support : Yes
Maximum VLANs to support : 9
Primary VLAN: DEFAULT_VLAN

802.1Q VLAN ID Name          Status
-----
1          DEFAULT_VLAN        Static
33         VLAN-33             Static
44         VLAN-44             Static
```

Figure 40: Port listing for an individual VLAN

```
Switch(config)# show vlan 1
Status and Counters - VLAN Information - VLAN 1

VLAN ID : 1
Name : DEFAULT_VLAN
Status : Static
Voice : Yes
Jumbo : No

Port Information Mode      Unknown VLAN Status
-----
A1          Untagged Learn        Up
A2          Tagged Learn           Up
A3          Untagged Learn        Up
A4          Untagged Learn        Down
A5          Untagged Learn        Up
A6          Untagged Learn        Up
A7          Untagged Learn        Up
```

Viewing all mirroring session configured on the switch

Syntax

```
show monitor
```

If a monitored source for a mirror session is configured on the switch, the following information is displayed. Otherwise, the output displays: Mirroring is currently disabled. Mirror port configured on the switch is shown:

```
switch(config) # show monitor
Network Monitoring Port
Mirror Port: 16
Monitoring sources
-----
 2
 5
```

Using the Menu to configure local mirroring

Menu and WebAgent limits

You can use the Menu and WebAgent to quickly configure or reconfigure local mirroring and allow one of the following two mirroring source options:

- Any combination of source ports, trunks, and a mesh.
- One static, source VLAN interface.

High-level overview of the mirror configuration process

Determine the mirroring session and destination

For a local mirroring session

Determine the port number for the exit port (such as A5, B10, and so forth).

Troubleshooting traffic mirroring

Cause

If mirrored traffic does not reach the configured remote destination (endpoint) switch or remote exit port, check the following configurations:

- The configured remote exit port must not be a member of a trunk or mesh.
- If the destination for mirrored traffic is on a different VLAN than the source, routing must be correctly configured along the path from the source to the destination.



CAUTION: A mirroring exit port should be connected only to a network analyzer, IDS, or other network edge device that has no connection to other network resources. Configuring a mirroring exit port connection to a network can result in serious network performance problems, and is strongly discouraged.

Overview

This chapter addresses performance-related network problems that can be caused by topology, switch configuration, and the effects of other devices or their configurations on switch operation. (For switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, see the installation guide you received with the switch.)



NOTE: Switch software updates are periodically placed on the Switch Networking website. It is recommended that you check this website for software updates that may have fixed a problem you are experiencing.

For information on support and warranty provisions, see the Support and Warranty booklet shipped with the switch.

Troubleshooting approaches

Cause

Use these approaches to diagnose switch problems:

- Check the HPE website for software updates that may have solved your problem: <http://www.hpe.com/networking>
- Check the switch LEDs for indications of proper switch operation:
 - Each switch port has a Link LED that should light whenever an active network device is connected to the port.
 - Problems with the switch hardware and software are indicated by flashing the Fault and other switch LEDs. For a description of the LED behavior and information on using the LEDs for troubleshooting, see the installation guide shipped with the switch.
- Check the network topology/installation. For topology information, see the installation guide shipped with the switch.
- Check cables for damage, correct type, and proper connections. You should also use a cable tester to check your cables for compliance to the relevant IEEE 802.3 specification. For correct cable types and connector pin-outs, see the installation guide shipped with the switch.
- Use the Port Utilization Graph and Alert Log in the WebAgent included in the switch to help isolate problems. These tools are available through the WebAgent:
 - Port Utilization Graph
 - Alert log
 - Port Status and Port Counters screens
 - Diagnostic tools (Link test, Ping test, configuration file browser)
- For help in isolating problems, use the easy-to-access switch console built into the switch or Telnet to the switch console. For operating information on the Menu and CLI interfaces included in the console, see chapters 3 and 4. These tools are available through the switch console:

- Status and Counters screens
- Event Log
- Diagnostics tools (Link test, Ping test, configuration file browser, and advanced user commands)

Browser or Telnet access problems

Cannot access the WebAgent

- Access may be disabled by the Web Agent Enabled parameter in the switch console. Check the setting on this parameter by selecting:

2. Switch Configuration

1. System Information

- The switch may not have the correct IP address, subnet mask, or gateway. Verify by connecting a console to the switch's Console port and selecting:

2. Switch Configuration

5. IP Configuration

Note: If DHCP/Bootp is used to configure the switch, the IP addressing can be verified by selecting:

1. Status and Counters...

2. Switch Management Address Information

Also check the DHCP/Bootp server configuration to verify correct IP addressing.

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, see the documentation for the DHCP application that you are using.
- If one or more IP-authorized managers are configured, the switch allows inbound telnet access only to a device having an authorized IP address. For more information on IP Authorized managers, see the access security guide for your switch.
- Java™ applets may not be running on the web browser. They are required for the switch WebAgent to operate correctly. Refer to the online Help on your web browser for how to run the Java applets.

Cannot Telnet into the switch console from a station on the network

- Off-subnet management stations can lose Telnet access if you enable routing without first configuring a static (default) route. That is, the switch uses the IP default gateway only while operating as a Layer 2 device. While routing is enabled on the switch, the IP default gateway is not used. You can avoid this problem by using the ip route command to configure a static (default) route before enabling routing. For more information, see "IP Routing Features" in the multicast and routing guide for your switch.

- Telnet access may be disabled by the `Inbound Telnet Enabled` parameter in the System Information screen of the menu interface:

2. Switch Configuration

1. System Information

- The switch may not have the correct IP address, subnet mask, or gateway. Verify by connecting a console to the switch's Console port and selecting:

2. Switch Configuration

5. IP Configuration

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, see the documentation for the DHCP application that you are using.
- If one or more IP-authorized managers are configured, the switch allows inbound telnet access only to a device having an authorized IP address. For more information on IP Authorized managers, see the access security guide for your switch.

Unusual network activity

Network activity that fails to meet accepted norms may indicate a hardware problem with one or more of the network components, possibly including the switch. Such problems can also be caused by a network loop or simply too much traffic for the network as it is currently designed and implemented. Unusual network activity is usually indicated by the LEDs on the front of the switch or measured with the switchconsole interface or with a network management tool. For information on using LEDs to identify unusual network activity, see the installation guide you received with the switch.

A topology loop can also cause excessive network activity. The Event Log "FFI" messages can be indicative of this type of problem.

General problems

The network runs slow; processes fail; users cannot access servers or other devices

Broadcast storms may be occurring in the network. These may be caused by redundant links between nodes.

- If you are configuring a port trunk, finish configuring the ports in the trunk before connecting the related cables. Otherwise you may inadvertently create a number of redundant links (that is, topology loops) that will cause broadcast storms.
- Turn on STP to block redundant links
- Check for FFI messages in the Event Log

Duplicate IP addresses

This is indicated by this Event Log message:

```
ip: Invalid ARP source: IP address on IP address
```

where both instances of *IP address* are the same address, indicating that the switch's IP address has been duplicated somewhere on the network.

Duplicate IP addresses in a DHCP network

If you use a DHCP server to assign IP addresses in your network, and you find a device with a valid IP address that does not appear to communicate properly with the server or other devices, a duplicate IP address may have been issued by the server. This can occur if a client has not released a DHCP-assigned IP address after the intended expiration time and the server "leases" the address to another device. This can also happen, for example, if the server is first configured to issue IP addresses with an unlimited duration, and then is subsequently configured to issue IP addresses that will expire after a limited duration. One solution is to configure "reservations" in the DHCP server for specific IP addresses to be assigned to devices having specific MAC addresses. For more information, see the documentation for the DHCP server.

One indication of a duplicate IP address in a DHCP network is this Event Log message:

```
ip: Invalid ARP source: <IP-address>  
on <IP-address>
```


where both instances of *IP-address* are the same address, indicating that the IP address has been duplicated somewhere on the network.

The switch has been configured for DHCP/Bootp operation, but has not received a DHCP or Bootp reply

When the switch is first configured for DHCP/Bootp operation, or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration.

After verifying that the server has become accessible to the switch, reboot the switch to re-start the process.

802.1Q Prioritization problems

Ports configured for non-default prioritization (level 1 to 7) are not performing the specified action

If the ports were placed in a trunk group after being configured for non-default prioritization, the priority setting was automatically reset to zero (the default). Ports in a trunk group operate only at the default priority setting.

Addressing ACL problems

ACLs are properly configured and assigned to VLANs, but the switch is not using the ACLs to filter IP layer 3 packets

ACL filtering on the switches applies only to routed packets and packets having a destination IP address (DA) on the switch itself.

Also, the switch applies assigned ACLs only at the point where traffic enters or leaves the switch on a VLAN. Ensure that you have correctly applied your ACLs ("in" and/or "out") to the appropriate VLANs.

The switch does not allow management access from a device on the same VLAN

The implicit `deny any` function that the switch automatically applies as the last entry in any ACL always blocks packets having the same DA as the switch's IP address on the same VLAN. That is, bridged packets with the switch itself as the destination are blocked as a security measure.

To preempt this action, edit the ACL to include an ACE that permits access to the switch's DA on that VLAN from the management device.

Error (Invalid input) when entering an IP address

When using the "host" option in the Command syntax, ensure that you are not including a mask in either dotted decimal or CIDR format. Using the "host" option implies a specific host device and therefore does not permit any mask entry.

Correctly and incorrectly specifying a single host

```
switch(config)# access-list 6 permit host 10.28.100.100 1
switch(config)# access-list 6 permit host 10.28.100.100 255.255.255.2552
Invalid input: 255.255.255.255

switch(config)# access-list 6 permit host 10.28.100.100/32 3
Invalid input: 10.28.100.100/32
```

- ¹Correct.
- ²Incorrect. No mask needed to specify a single host.
- ³Incorrect. No mask needed to specify a single host.

Apparent failure to log all "deny" matches

Where the `log` statement is included in multiple ACEs configured with a "deny" option, a large volume of "deny" matches generating logging messages in a short period of time can impact switch performance. If it appears that the switch is not consistently logging all "deny" matches, try reducing the number of logging actions by removing the `log` statement from some ACEs configured with the "deny" action.

The switch does not allow any routed access from a specific host, group of hosts, or subnet

The implicit `deny any` function that the switch automatically applies as the last entry in any ACL may be blocking all access by devices not specifically permitted by an entry in an ACL affecting those sources. If you are using the ACL to block specific hosts, a group of hosts, or a subnet, but want to allow any access not specifically permitted, insert `permit any` as the last explicit entry in the ACL.

The switch is not performing routing functions on a VLAN

Two possible causes of this problem are:

- Routing is not enabled.
- An ACL may be blocking access to the VLAN (on a switch covered in this guide). Ensure that the switch's IP address on the VLAN is not blocked by one of the ACE entries in an ACL applied to that VLAN. A common mistake is to either not explicitly permit the switch's IP address as a DA or to use a wildcard ACL mask in a `deny` statement that happens to include the switch's IP address. For an Example: of this problem, see section "General ACL Operating Notes" in the "Access Control Lists (ACLs)" of the latest access security guide for your switch.

Routing through a gateway on the switch fails

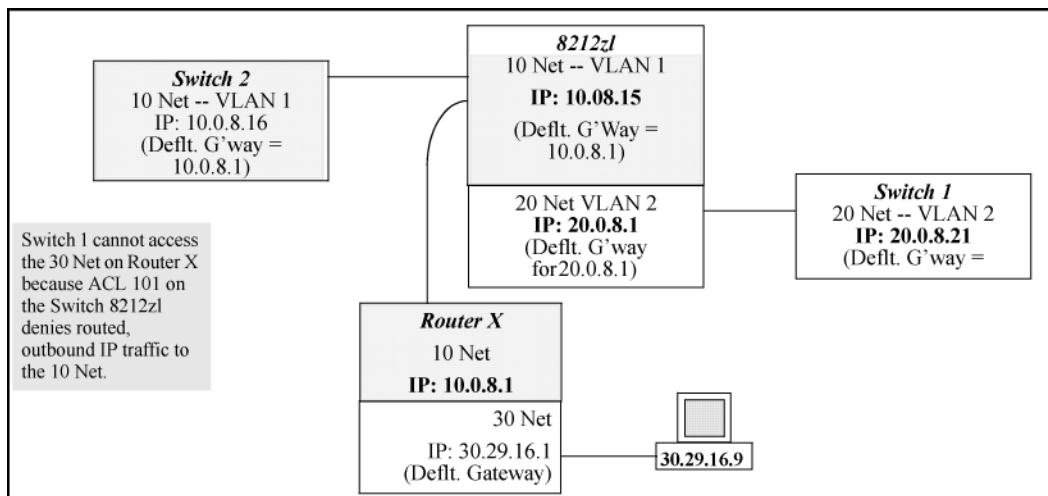
Configuring a "deny" ACE that includes a gateway address can block traffic attempting to use the gateway as a next-hop.

Remote gateway case

Configuring ACL "101" (example below) and applying it outbound on VLAN 1 in the figure below includes the router gateway (10.0.8.1) needed by devices on other networks. This can prevent the switch from sending ARP and other messages to the gateway router to support traffic from authorized remote networks.

In **Figure 41: Inadvertently blocking a gateway** on page 339, this ACE (see data in bold below) denies access to the 10 Net's 10.0.8.1 router gateway needed by the 20 Net (Subnet mask is 255.255.255.0). **See: example**

Figure 41: *Inadvertently blocking a gateway*



To avoid inadvertently blocking the remote gateway for authorized traffic from another network (such as the 20 Net in this Example):

Procedure

1. Configure an ACE that specifically permits authorized traffic from the remote network.
2. Configure narrowly defined ACEs to block unwanted IP traffic that would otherwise use the gateway; such ACEs might deny traffic for a particular application, particular hosts, or an entire subnet.
3. Configure a "permit any" ACE to specifically allow any IP traffic to move through the gateway.

ACE blocking an entire subnet

```
switch(config)# access-list config

ip access-list extended "101"
  deny ip 0.0.0.0 255.255.255.255 10.0.8.30 0.0.0.255
  permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```

Local gateway case

If you use the switch as a gateway for traffic you want routed between subnets, use these general steps to avoid blocking the gateway for authorized applications:

Procedure

1. Configure gateway security first for routing with specific permit and deny statements.
2. Permit authorized traffic.
3. Deny any unauthorized traffic that you have not already denied in step 1.

IGMP-related problems

IP multicast (IGMP) traffic that is directed by IGMP does not reach IGMP hosts or a multicast router connected to a port

IGMP must be enabled on the switch and the affected port must be configured for "Auto" or "Forward" operation.

IP multicast traffic floods out all ports; IGMP does not appear to filter traffic

The IGMP feature does not operate if the switch or VLAN does not have an IP address configured manually or obtained through DHCP/Bootp. To verify whether an IP address is configured for the switch or VLAN, do one of the following:

- **Try using the WebAgent:** If you can access the WebAgent, then an IP address is configured.
- **Try to telnet to the switch console:** If you can Telnet to the switch, an IP address is configured.
- **Use the switch console interface:** From the Main Menu, check the Management Address Information screen by clicking on:
 1. Status and Counters
 2. Switch Management Address Information

LACP-related problems

Unable to enable LACP on a port with the `interface <port-number> lacp` command

In this case, the switch displays the following message:

```
Operation is not allowed for a trunked port.
```

You cannot enable LACP on a port while it is configured as a static Trunk port. To enable LACP on a static-trunked port:

Procedure

1. Use the `no trunk <port-number>` command to disable the static trunk assignment.
2. Execute `interface <port-number> lacp` .



CAUTION: Removing a port from a trunk without first disabling the port can create a traffic loop that can slow down or halt your network. Before removing a port from a trunk, Hewlett Packard Enterprise recommends that you either disable the port or disconnect it from the LAN.

Port-based access control (802.1X)-related problems



NOTE:

To list the 802.1X port-access Event Log messages stored on the switch, use `show log 802`.

See also [Radius-related problems](#) on page 343.

The switch does not receive a response to RADIUS authentication requests

In this case, the switch attempts authentication using the secondary method configured for the type of access you are using (console, Telnet, or SSH).

There can be several reasons for not receiving a response to an authentication request. Do the following:

- Use `ping` to ensure that the switch has access to the configured RADIUS servers.
- Verify that the switch is using the correct encryption key (RADIUS secret key) for each server.
- Verify that the switch has the correct IP address for each RADIUS server.
- Ensure that the `radius-server timeout` period is long enough for network conditions.

The switch does not authenticate a client even though the RADIUS server is properly configured and providing a response to the authentication request

If the RADIUS server configuration for authenticating the client includes a VLAN assignment, ensure that the VLAN exists as a static VLAN on the switch. See "How 802.1X Authentication Affects VLAN Operation" in the access security guide for your switch.

During RADIUS-authenticated client sessions, access to a VLAN on the port used for the client sessions is lost

If the affected VLAN is configured as untagged on the port, it may be temporarily blocked on that port during an 802.1X session. This is because the switch has temporarily assigned another VLAN as untagged on the port to support the client access, as specified in the response from the RADIUS server. See "How 802.1X Authentication Affects VLAN Operation" in the access security guide for your switch.

The switch appears to be properly configured as a supplicant, but cannot gain access to the intended authenticator port on the switch to which it is connected

If `aaa authentication port-access` is configured for Local, ensure that you have entered the local **login** (operator-level) username and password of the authenticator switch into the `identity` and `secret` parameters of the supplicant configuration. If instead, you enter the enable (manager-level) username and password, access will be denied.

The supplicant statistics listing shows multiple ports with the same authenticator MAC address

The link to the authenticator may have been moved from one port to another without the supplicant statistics having been cleared from the first port. See "Note on Supplicant Statistics" in the chapter on Port-Based and User-Based Access Control in the access security guide for your switch.

The `show port-access authenticator <port-list>` command shows one or more ports remain open after they have been configured with `control unauthorized`

802.1X is not active on the switch. After you execute `aaa port-access authenticator active`, all ports configured with `control unauthorized` should be listed as Closed.

Authenticator ports remain "open" until activated

```
switch(config)# show port-access authenticator e 9
Port Access Authenticator Status
  Port-access authenticator activated no : No
      Access Authenticator Authenticator
Port Status Control  State Backend  State
-----
  9      Open  1    FU           Force Auth  Idle

switch(config)# show port-access authenticator active
switch(config)# show port-access authenticator e 9
Port Access Authenticator Status
```

```

Port-access authenticator activated no : Yes
Access Authenticator Authenticator
Port Status Control State Backend State
-----
9 Closed FU Force Unauth Idle

```

¹Port A9 shows an “Open” status even though Access Control is set to Unauthorized (Force Auth). This is because the port-access authenticator has not yet been activated.

RADIUS server fails to respond to a request for service, even though the server's IP address is correctly configured in the switch

Use `show radius` to verify that the encryption key (RADIUS secret key) the switch is using is correct for the server being contacted. If the switch has only a global key configured, it either must match the server key or you must configure a server-specific key. If the switch already has a server-specific key assigned to the server's IP address, it overrides the global key and must match the server key.

Displaying encryption keys

```

switch(config)# show radius
Status and Counters - General RADIUS Information
Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key : My-Global-Key
Dynamic Authorization UDP Port : 3799

Server IP Addr      Auth Acct DM/ Time
Port Port CoA Window Encryption Key
-----
10.33.18.119      1812 1813
                               119-only-key

```

Also, ensure that the switch port used to access the RADIUS server is not blocked by an 802.1X configuration on that port. For example, `show port-access authenticator <port-list>` gives you the status for the specified ports. Also, ensure that other factors, such as port security or any 802.1X configuration on the RADIUS server are not blocking the link.

The authorized MAC address on a port that is configured for both 802.1X and port security either changes or is re-acquired after execution of `aaa port-access authenticator <port-list> initialize`

If the port is force-authorized with `aaa port-access authenticator <port-list> control authorized` command and port security is enabled on the port, then executing `initialize` causes the port to clear the learned address and learn a new address from the first packet it receives after you execute `initialize`.

A trunked port configured for 802.1X is blocked

If you are using RADIUS authentication and the RADIUS server specifies a VLAN for the port, the switch allows authentication, but blocks the port. To eliminate this problem, either remove the port from the trunk or reconfigure the RADIUS server to avoid specifying a VLAN.

QoS-related problems

Loss of communication when using VLAN-tagged traffic

If you cannot communicate with a device in a tagged VLAN environment, ensure that the device either supports VLAN tagged traffic or is connected to a VLAN port that is configured as `Untagged`.

Radius-related problems

The switch does not receive a response to RADIUS authentication requests

In this case, the switch attempts authentication using the secondary method configured for the type of access you are using (console, Telnet, or SSH).

There can be several reasons for not receiving a response to an authentication request. Do the following:

- Use `ping` to ensure that the switch has access to the configured RADIUS server.
- Verify that the switch is using the correct encryption key for the designated server.
- Verify that the switch has the correct IP address for the RADIUS server.
- Ensure that the `radius-server timeout` period is long enough for network conditions.
- Verify that the switch is using the same UDP port number as the server.



NOTE: Because of an inconsistency between the Windows XP 802.1x supplicant timeout value and the switch default timeout value, which is 5, when adding a backup RADIUS server, set the switch `radius-server timeout` value to 4. Otherwise, the switch may not failover properly to the backup RADIUS server.

RADIUS server fails to respond to a request for service, even though the server's IP address is correctly configured in the switch

Use `show radius` to verify that the encryption key the switch is using is correct for the server being contacted. If the switch has only a global key configured, it either must match the server key or you must configure a server-specific key. If the switch already has a server-specific key assigned to the server's IP address, it overrides the global key and must match the server key.

Global and unique encryption keys

```
switch(config)# show radius
Status and Counters - General RADIUS Information
  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key : My-Global-Key 1
  Dynamic Authorization UDP Port : 3799

  Server IP Addr      Auth Port  Acct Port  DM/CoA  Time Window  Encryption Key
  -----
  10.33.18.119       1812     1813      -----  -----  -----
                                     119-only-key 2
```

- 1
Global RADIUS Encryption Key
- 2

MSTP and fast-uplink problems



CAUTION:

If you enable MSTP, Hewlett Packard Enterprise recommends that you leave the remainder of the MSTP parameter settings at their default values until you have had an opportunity to evaluate MSTP performance in your network. Because incorrect MSTP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how MSTP operates. To learn the details of MSTP operation, see the IEEE802.1s standard.

Broadcast storms appearing in the network

This can occur when there are physical loops (redundant links) in the topology. Where this exists, you should enable MSTP on all bridging devices in the topology to detect the loop.

STP blocks a link in a VLAN even though there are no redundant links in that VLAN

In 802.1Q-compliant switches, MSTP blocks redundant physical links even if they are in separate VLANs. A solution is to use only one, multiple-VLAN (tagged) link between the devices. Also, if ports are available, you can improve the bandwidth in this situation by using a port trunk. See "Spanning Tree Operation with VLANs" in "Static Virtual LANs (VLANs)" in the advanced traffic management guide for your switch.

Fast-uplink troubleshooting

Some of the problems that can result from incorrect use of fast-uplink MSTP include temporary loops and generation of duplicate packets.

Problem sources can include:

- Fast-uplink is configured on a switch that is the MSTP root device.
- Either the `Hello Time` or the `Max Age` setting (or both) is too long on one or more switches. Return the `Hello Time` and `Max Age` settings to their default values (2 seconds and 20 seconds, respectively, on a switch).
- A "downlink" port is connected to a switch that is further away (in hop count) from the root device than the switch port on which fast-uplink MSTP is configured.
- Two edge switches are directly linked to each other with a fast-uplink (`Mode = Uplink`) connection.
- Fast uplink is configured on both ends of a link.
- A switch serving as a backup MSTP root switch has ports configured for fast-uplink MSTP and has become the root device because of a failure in the original root device.

SSH-related problems

Switch access refused to a client

Even though you have placed the client's public key in a text file and copied the file (using the `copy tftp pub-key-file` command) into the switch, the switch refuses to allow the client to have access. If the source SSH client is an SSHv2 application, the public key may be in the PEM format, which the switch (SSHv1) does not interpret. Check the SSH client application for a utility that can convert the PEM-formatted key into an ASCII-formatted key.

Executing IP SSH does not enable SSH on the switch

The switch does not have a host key. Verify by executing `show ip host-public-key`. If you see the message

```
ssh cannot be enabled until a host key is configured (use 'crypto' command).
```

you need to generate an SSH key pair for the switch. To do so, execute `crypto key generate` (see "Generating the switch's public and private key pair" in the SSH chapter of the access security guide for your switch.)

Switch does not detect a client's public key that does appear in the switch's public key file (show ip client-public-key)

The client's public key entry in the public key file may be preceded by another entry that does not terminate with a new line (CR). In this case, the switch interprets the next sequential key entry as simply a comment attached to the preceding key entry. Where a public key file has more than one entry, ensure that all entries terminate with a new line (CR). While this is optional for the last entry in the file, not adding a new line to the last entry creates an error potential if you either add another key to the file at a later time or change the order of the keys in the file.

An attempt to copy a client public-key file into the switch has failed and the switch lists one of the following messages

```
Download failed: overlength key in key file.
```

```
Download failed: too many keys in key file.
```

```
Download failed: one or more keys is not a valid RSA public key.
```

The public key file you are trying to download has one of the following problems:

- A key in the file is too long. The maximum key length is 1024 characters, including spaces. This could also mean that two or more keys are merged together instead of being separated by a <CR> <LF>.
- There are more than ten public keys in the key file.
- One or more keys in the file is corrupted or is not a valid rsa public key.

Client ceases to respond ("hangs") during connection phase

The switch does not support data compression in an SSH session. Clients often have compression turned on by default, but then disable it during the negotiation phase. A client that does not recognize the compression-request FAILURE response may fail when attempting to connect. Ensure that compression is turned **off** before attempting a connection to prevent this problem.

TACACS-related problems

All users are locked out of access to the switch

If the switch is functioning properly, but no username/password pairs result in console or Telnet access to the switch, the problem may be caused by how the TACACS+ server and/or the switch are configured. Use one of the following methods to recover:

- Access the TACACS+ server application and adjust or remove the configuration parameters controlling access to the switch.
- If the above method does not work, try eliminating configuration changes in the switch that have not been saved to flash (boot-up configuration) by causing the switch to reboot from the boot-up configuration (which includes only the configuration changes made prior to the last `write memory` command.) If you did not use

`write memory` to save the authentication configuration to flash, pressing the `Reset` button reboots the switch with the boot-up configuration.

- Disconnect the switch from network access to any TACACS+ servers and then log in to the switch using either Telnet or direct console port access. Because the switch cannot access a TACACS+ server, it defaults to local authentication. You can then use the switch's local Operator or Manager username/password pair to log on.
- As a last resort, use the `Clear/Reset` button combination to reset the switch to its factory default boot-up configuration. Taking this step means you will have to reconfigure the switch to return it to operation in your network.

No communication between the switch and the TACACS+ server application

If the switch can access the server device (that is, it can `ping` the server), a configuration error may be the problem. Some possibilities include:

- The server IP address configured with the switch's `tacacs-serverhost` command may not be correct. (Use the switch's `show tacacs-server` command to list the TACACS+ server IP address.)
- The encryption key configured in the server does not match the encryption key configured in the switch (by using the `tacacs-server key` command). Verify the key in the server and compare it to the key configured in the switch. (Use `show tacacs-server` to list the global key. Use `show config` or `show config running` to list any server-specific keys.)
- The accessible TACACS+ servers are not configured to provide service to the switch.

Access is denied even though the username/password pair is correct

Some reasons for denial include the following parameters controlled by your TACACS+ server application:

- The account has expired.
- The access attempt is through a port that is not allowed for the account.
- The time quota for the account has been exhausted.
- The time credit for the account has expired.
- The access attempt is outside of the time frame allowed for the account.
- The allowed number of concurrent logins for the account has been exceeded.

For more help, see the documentation provided with your TACACS+ server application.

Unknown users allowed to login to the switch

Your TACACS+ application may be configured to allow access to unknown users by assigning them the privileges included in a *default user* profile. See the documentation provided with your TACACS+ server application.

System allows fewer login attempts than specified in the switch configuration

Your TACACS+ server application may be configured to allow fewer login attempts than you have configured in the switch with the `aaa authentication num-attempts` command.

TimeP, SNTP, or Gateway problems

The switch cannot find the time server or the configured gateway

TimeP, SNTP, and Gateway access are through the primary VLAN, which in the default configuration is the DEFAULT_VLAN. If the primary VLAN has been moved to another VLAN, it may be disabled or does not have ports assigned to it.

VLAN-related problems

Monitor port

When using the monitor port in a multiple-VLAN environment, the switch handles broadcast, multicast, and unicast traffic output from the monitor port as follows:

- If the monitor port is configured for tagged VLAN operation on the same VLAN as the traffic from monitored ports, the traffic output from the monitor port carries the same VLAN tag.
- If the monitor port is configured for untagged VLAN operation on the same VLAN as the traffic from the monitored ports, the traffic output from the monitor port is untagged.
- If the monitor port is not a member of the same VLAN as the traffic from the monitored ports, traffic from the monitored ports does not go out the monitor port.

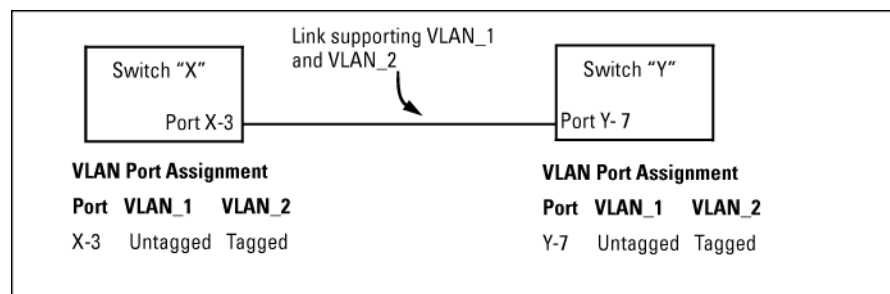
None of the devices assigned to one or more VLANs on an 802.1Q-compliant switch are being recognized

If multiple VLANs are being used on ports connecting 802.1Q-compliant devices, inconsistent VLAN IDs may have been assigned to one or more VLANs. For a given VLAN, the same VLAN ID must be used on all connected 802.1Q-compliant devices.

Link configured for multiple VLANs does not support traffic for one or more VLANs

One or more VLANs may not be properly configured as "Tagged" or "Untagged." A VLAN assigned to a port connecting two 802.1Q-compliant devices must be configured the same on both ports. For example, VLAN_1 and VLAN_2 use the same link between switch "X" and switch "Y," as shown in **Figure 42: Example: of correct VLAN port assignments on a link** on page 347.

Figure 42: Example: of correct VLAN port assignments on a link



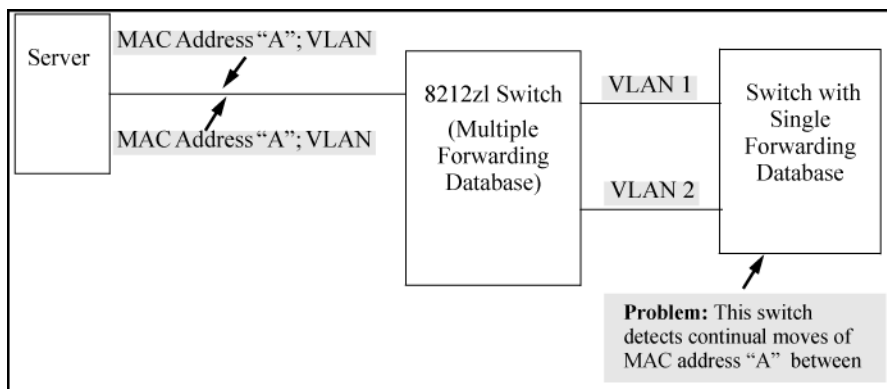
- If VLAN_1 (VID=1) is configured as "Untagged" on port 3 on switch "X," it must also be configured as "Untagged" on port 7 on switch "Y." Make sure that the VLAN ID (VID) is the same on both switches.
- Similarly, if VLAN_2 (VID=2) is configured as "Tagged" on the link port on switch "A," it must also be configured as "Tagged" on the link port on switch "B." Make sure that the VLAN ID (VID) is the same on both switches.

Duplicate MAC addresses across VLANs

The switches operate with multiple forwarding databases. Thus, duplicate MAC addresses occurring on different VLANs can appear where a device having one MAC address is a member of more than one 802.1Q VLAN, and the switch port to which the device is linked is using VLANs (instead of MSTP or trunking) to establish redundant links to another switch. If the other device sends traffic over multiple VLANs, its MAC address consistently appears in multiple VLANs on the switch port to which it is linked.

Be aware that attempting to create redundant paths through the use of VLANs causes problems with some switches. One symptom is that a duplicate MAC address appears in the Port Address Table of one port and then later appears on another port. While the switches have multiple forwarding databases and thus do not have this problem, some switches with a single forwarding database for all VLANs may produce the impression that a connected device is moving among ports because packets with the same MAC address but different VLANs are received on different ports. You can avoid this problem by creating redundant paths using port trunks or spanning tree.

Figure 43: Example: of duplicate MAC address



Disabled overlapping subnet configuration

Previous software versions allowed configuration of VLAN IP addresses in overlapping subnets which can cause incorrect routing of packets and result in IP communication failure. As of software version WB.15.09, overlapping subnet configurations are no longer allowed. An overlapping subnet is determined by the configuration order. The subnet that is configured first is valid, but any subsequent IP addresses that overlap are not allowed.

When the switch is booted into software version WB.15.09 or later, and the configuration file includes overlapping subnets, the following occurs:

- The event log provides an error message in the format:

```
ip: VLANx : IP initialization failed for vlan x.
```

For a multinetted VLAN (multiple IP addresses assigned to the VLAN), only the IP addresses that are overlapping subnets are removed. The other IP addresses on the VLAN are retained and function correctly. The error message can be somewhat misleading; the IP addresses on the VLAN that are not overlapping are initialized correctly.

- The output of the `show ip` command correctly indicates that the overlapping IP address does not exist on the VLANs that have error messages in the event log.

- The output of the `show running-config` command incorrectly indicates that the overlapping IP address is configured. In **Figure 44: An IP address that is not actually configured on the VLAN** on page 349, the IP address shown in VLAN6 is not actually configured on the VLAN; it has been removed.

Figure 44: An IP address that is not actually configured on the VLAN

```
switch(config)# show running-config

.
.
.
vlan 5
  name "VLAN5"
  ip address 11.22.33.1 255.0.0.0
  exit
vlan 6
  name "VLAN6"
  ip address 11.23.34.1 255.255.255.0
  exit
```

The information is retained in the config file to allow you to boot up the switch and have it function as it did when it was configured with earlier software that allows overlapping subnets. If you attempt to remove the overlapping subnet from the VLAN, the switch displays an error message similar to:

```
The IP address <ip-address> is not configured on this VLAN
```

This occurs because the overlapping IP address has been removed and is not visible to the switch. To resolve this:

- Enter the `show ip` command to determine which addresses are visible to the switch.
- Remove the erroneous IP addresses from the config file by entering the `no ip address` command to remove all the IP addresses from the specific VLAN. Be sure to document the other valid IP addresses on that VLAN so they can be restored after removing the erroneous IP addresses from the config file.

If you go back to a software version prior to WB.15.09 before removing the overlapping IP address, the prior software version enables the overlapping IP subnet.

Fan failure

Whenever a fan failure occurs, the Fan/Fault LEDs blink amber and a log entry is recorded. During a fan failure, all operational fans are automatically set to the maximum operating speed until the fan failure has been resolved. At that time, the fan speed is reset to the minimum operating speed.

Mitigating flapping transceivers

In traditional switches, the state of a link is driven directly by the reported state of the port, which is required for rapid detection of link faults. However, the consequence of this is that a marginal transceiver, optical, or wire cabling, one that "flaps" up and down several times per second, can cause STP and other protocols to react poorly, resulting in a network outage. The link-flap option expands the functionality of the existing fault finder function to include a "link-flap" event and a new action of "warn-and-disable." Together, these additions allow the errant condition to be detected, and the port in question can be optionally disabled.

Syntax:

```
fault-finder <link-flap> sensitivity {<low | medium | high>} > action {<warn | warn-and-disable>}
```

Default settings: Sensitivity = Medium; Action = Warn

Sensitivity thresholds are static. In a 10-second window, if more than the threshold number of link state transitions (up or down) are detected, the event is triggered. The 10-second window is statically determined, that is, the counters are reset every 10 seconds, as opposed to being a sliding window. The counters are polled twice per second (every 500 milliseconds), and the event is triggered if the sensitivity threshold is crossed at that time.

The sensitivity thresholds are:

High	3 transitions in 10 seconds
Medium	6 transitions in 10 seconds
Low	10 transitions in 10 seconds

Configuring the link-flap event and corresponding action applies to all ports and port types (it is a global setting per FFI event type). Note that normal link transition protocols may prevent link state changes from occurring fast enough to trigger the event for some port types, configurations, and sensitivity settings.

When the link-flap threshold is met for a port configured for warn (For example, `fault-finder link-flap sensitivity medium action warn`), the following message is seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
```

When the link-flap threshold is met for a port configured for warn-and-disable (For example, `fault-finder linkflap sensitivity medium action warn-and-disable`), the following messages are seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
```

```
02673 FFI: port <number>-Port disabled by Fault-finder.
```

```
02674 FFI: port <number>-Administrator action required to re-enable.
```

The warn-and-disable action is available for all fault-finder events on an individual basis. It may be used, For example, to disable a port when excessive broadcasts are received. Because the fault-generated disabling of a port requires operator intervention to re-enable the port, such configuration should be used with care. For example, link-flap-initiated disablement is not desired on ports that are at the client edge of the network, because link state changes there are frequent and expected.

Hewlett Packard Enterprise does not recommend automatic disabling of a port at the core or distribution layers when excessive broadcasts are detected, because of the potential to disable large parts of the network that may be uninvolved and for the opportunity to create a denial-of-service attack.

Fault-finder link-flap

Syntax

In the config context:

```
no fault-finder link-flap [ethernet] PORT-LIST action warn | warn-and-disable SECONDS sensitivity low | medium | high
```

Description

Configures the link-flap on a port. The default value is `warn`.

Parameters

link-flap

Configure link-flap control.

warn

Log the event only.

warn-and-disable

Log the event and disable the port.

seconds

Re-enable the port after waiting for the specified number of seconds. The default value is 0, which indicates that the port will not be automatically enabled.

sensitivity

Indicate the sensitivity of the link-flap control threshold within a 10-second interval.

- Low indicates 10 link-flaps.
- Medium indicates 6 link-flaps.
- High indicates 3 link-flaps.

Parameters**action**

Configure the action taken when a fault is detected.

ethernet *PORT-LIST*

Enable link-flap control on a list of ports.

warn

Warn about faults found.

warn-and-disable

Warn and disable faulty component.

seconds

Configure the number of seconds for which the port remains disabled. A value of 0 means that the port will remain disabled until manually re-enabled.

sensitivity

Configure the fault sensitivity level.

low

Low sensitivity.

medium

Medium sensitivity

high

High sensitivity.

Subcommand Syntax

```
no fault-finder link-flap ethernet PORT-LIST
```

Description

To remove the current configuration of link-flap on a port

Usage

Enable a linkFault-Finder check and set parameters for it. These commands may be repeated to enable additional checks. The default sensitivity is medium and the default action is warn.

```
no fault-finder all | fault sensitivity low | medium | high action warn | warn-and-disable
```

```
no fault-finder link-flap sensitivity low | medium | high action warn | warn-and-disable
```

```
no fault-finder link-flap PORT-LIST action warn | warn-and-disable SECONDS sensitivity low | medium | high
```

Configure ports for link-flap detection with high sensitivity

Configure ports A1 to A5 for link-flap detection with sensitivity of high (3 flaps over 10s) and to log and disable port for 65535s if the link-flap threshold is exceeded.

```
switch(config)# fault-finder link-flap ethernet A1-A5 action warn-and-disable 65535  
sensitivity high
```

Configure ports for link-flap detection with medium sensitivity

Configure ports A8 for link-flap detection with sensitivity of medium (6 flaps over 10s) and to log and disable port if the link-flap threshold is exceeded. User will need to re-enable the port if disabled.

```
switch(config)# fault-finder link-flap ethernet A8 action warn-and-disable 0 sensitivity medium
```

Configure ports for link-flap detection with low sensitivity

Configure ports A22 for link-flap detection with sensitivity of low (10 flaps over 10s) and to log if the link-flap threshold is exceeded

```
switch(config)# fault-finder link-flap ethernet A22 action warn sensitivity low
```

Disable link-flap detection

Disable link-flap detection for port A5

```
switch(config)# no fault-finder link-flap ethernet A5
```

Show fault-finder link-flap

Syntax

```
show fault-finder link-flap ethernet PORT-LIST
```

Description

Display the link-flap control configuration.

Show fault-finder link-flap

```
switch# show fault-finder link-flap A1
```


Port	Link Flap	Port Status	Sensitivity	Action	Disable Timer	Disable Time Left
A1	Yes	Down	Low	warn-and-disable	65535	45303

switch# show fault-finder link-flap

Port	Link Flap	Port Status	Sensitivity	Action	Disable Timer	Disable Time Left
A1	Yes	Down	Low	warn-and-disable	65535	45303
A5	No	Up	None	None	-	-
A22	Yes	Down	Low	warn-and-disable	-	-
A23	Yes	Down	High	warn-and-disable	100	-



NOTE: This example displays only the list of ports configured via the above per-port config commands, does not include the global configuration ports.

Restrictions

- Per port configuration for options – link-flap only. Global settings for other options.
- No support for menu interface.
- No support for Web UI.
- No support for trunks.

Viewing transceiver information

This feature provides the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. The following table indicates the support level for specific transceivers:

Product #	Description	Support ¹
J8436A	10GbE X2-SC SR Optic	V
J8437A	10GbE X2-SC LR Optic	V
J8440B	10GbE X2-CX4 Xcver	NA
J8440C	10GbE X2-CX4 Xcver	NA
J4858A	Gigabit-SX-LC Mini-GBIC	V
J4858B	Gigabit-SX-LC Mini-GBIC	V
J4858C	Gigabit-SX-LC Mini-GBIC	V (some)

Table Continued

Product #	Description	Support ¹
J9054B	100-FX SFP-LC Transceiver	N
J8177C	Gigabit 1000Base-T Mini-GBIC	NA
J9150A	10GbE SFP+ SR Transceiver	D
J9151A	10GbE SFP+ LR Transceiver	D
J9152A	10GbE SFP+ LRM Transceiver	D
J9153A	10GbE SFP+ ER Transceiver	D
J9144A	10GbE X2-SC LRM Transceiver	D
J8438A	10Gbe X2-SC ER Transceiver	D
JH233A	40G QSFP+ MPO eSR4 Transceiver	V
JH232A	40G QSFP+ LC LR4 SM Transceiver	V
JL308A	40G QSFP+BIDI	V
JH231A	40G QSFP+ MPO SR4 Transceiver	V

¹ Support indicators:

- V - Validated to respond to DOM requests
- N - No support of DOM
- D - Documented by the component suppliers as supporting DOM
- NA - Not applicable to the transceiver (copper transceiver)



NOTE: Not all transceivers support Digital Optical Monitoring. If DOM appears in the Diagnostic Support field of the `show interfaces transceiver detail` command, or the `hpicfTransceiverMIB hpicfXcvrDiagnostics` MIB object, DOM is supported for that transceiver.

Viewing information about transceivers (CLI)

Syntax:

```
show interfaces transceiver [port-list] [detail]
```

Displays information about the transceivers. If a port is specified, displays information for the transceiver in that port.

[detail]	Displays detailed transceiver information.
----------	--

MIB support

The `hpicfTransceiver` MIB is available for displaying transceiver information.

Viewing transceiver information

The transceiver information displayed depends on the `show` command executed.

The output for `show interfaces transceiver [port-list]` is shown below. You can specify multiple ports, separated by commas, and the information for each transceiver will display.

Output for a specified transceiver

```
switch(config)# show interfaces transceiver 21
```

```
Transceiver Technical information:
```

Port	Type	Product Number	Serial Number	Part Number
21	1000SX	J4858C	MY050VM9WB	1990-3657

If there is no transceiver in the port specified in the command, the output displays as shown below.

Output when no transceiver is present in specified interface

```
switch(config)# show interfaces transceiver 22
```

```
No Transceiver found on interface 22
```

When no ports are specified, information for all transceivers found is displayed.

Output when no ports are specified

```
switch(config)# show interfaces transceiver
```

```
Transceiver Technical information:
```

Port	Type	Product Number	Serial Number	Part Number
21	1000SX	J4858C	MY050VM9WB	1990-3657
22	1000SX	J4858B	P834DIP2	

You can specify `all` for `port-list` as shown below.

Output when “all” is specified

```
switch(config)# show interfaces transceiver all
```

```
No Transceiver found on interface 1
```

```
No Transceiver found on interface 2
```

```
.  
.  
.
```

```
No Transceiver found on interface 24
```

```
Transceiver Technical information:
```

Port	Type	Product Number	Serial Number	Part Number
21	1000SX	J4858C	MY050VM9WB	1990-3657
22	1000SX	J4858B	P834DIP2	

Information displayed with the detail parameter

When the `show interfaces transceiver [port-list] detail` command is executed, the following information displays.

Table 26: *General transceiver information*

Parameter	Description
Interface Index	The switch interface number
Transceiver-type	Pluggable transceiver type
Transceiver model	Pluggable transceiver model
Connector-type	Type of connector of the transceiver
Wavelength	For an optical transceiver: the central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, the values will be separated by a comma.
Transfer Distance	Link-length supported by the transceiver in meters. The corresponding transfer medium is shown in brackets following the transfer distance value, For example, 50um multimode fiber. If the transceiver supports multiple transfer media, the values are separated by a comma.

Table Continued

Parameter	Description
Diagnostic Support	Shows whether the transceiver supports diagnostics: None Supported DOM Supported VCT Supported
Serial Number	Serial number of the transceiver

The information in the next three tables is only displayed when the transceiver supports DOM.

Table 27: *DOM information*

Parameter	Description
Temperature	Transceiver temperature (in degrees Centigrade)
Voltage	Supply voltage in transceiver (Volts)
Bias	Laser bias current (mA)
RX power	Rx power (mW and dBm))
TX power	Tx power (mW and dBm)

The alarm information for GBIC/SFP transceivers is shown in this table.

Table 28: *Alarm and error information (GBIC/SFP transceivers only)*

Alarm	Description
RX loss of signal	Incoming (RX) signal is lost
RX power high	Incoming (RX) power level is high
RX power low	Incoming (RX) power level is low
TX fault	Transmit (TX) fault
TX bias high	TX bias current is high
TX bias low	TX bias current is low

Table Continued

Alarm	Description
TX power high	TX power is high
TX power low	TX power is low
Temp high	Temperature is high
Temp low	Temperature is low
Voltage High	Voltage is high
Voltage Low	Voltage is low

The alarm information for XENPAK transceivers is shown in this table.

Table 29: Alarm and error information (XENPAK transceivers)

Alarm	Description
WIS local fault	WAN Interface Sublayer local fault
Receive optical power fault	Receive optical power fault
PMA/PMD receiver local fault	Physical Medium Attachment/Physical Medium Dependent receiver local fault
PCS receiver local fault	Physical Coding Sublayer receiver local fault
PHY XS receive local fault	PHY Extended Sublayer receive local fault
RX power high	RX power is high
RX power low	RX power is low
Laser bias current fault	Laser bias current fault
Laser temperature fault	Laser temperature fault
Laser output power fault	Laser output power fault
TX fault	TX fault
PMA/PMD transmitter local fault	PMA/PMD transmitter local fault
PCS Transmit local fault	PCS transmit local fault

Table Continued

Alarm	Description
PHY XS transmit local fault	PHY SX transmit local fault
TX bias high	TX bias current is high
TX bias low	TX bias current is low
TX power high	TX power is high
TX power low	TX power is low
Temp high	Temperature is high
Temp low	Temperature is low

An Example: of the output for the show interfaces transceiver [port-list] detail for a 1000SX transceiver is shown below.

Detailed information for a 1000SX Mini-GBIC transceiver

```
switch(config)# show interfaces transceiver 21 detail
```

```
Transceiver in 21
Interface index      : 21
Type                 : 1000SX
Model                : J4858C
Connector type       : LC
Wavelength           : 850nm
Transfer distance    : 300m (50um), 150m (62.5um),
Diagnostic support   : DOM
Serial number        : MY050VM9WB
```

```
Status
Temperature          : 50.111C
Voltage              : 3.1234V
TX Bias              : 6mA
TX Power             : 0.2650mW, -5.768dBm
RX Power             : 0.3892mW, -4.098dBm
```

```
Time stamp           : Mon Mar 7 14:22:13 2011
```

An Example: of the output for a 10GbE-LR transceiver is shown below.

Detailed information for a 10GbE-LR transceiver

```
switch(config)# show interfaces transceiver 23 detail
```

```
Transceiver in 23
Interface Index      : 24
Type                 : 10GbE-LR
Model                : J8437A
Connector type       : SC
Wavelength           : Channel #0: 1310nm, #1:0nm, #2:0nm, #3:0nm
Transfer distance    : 10000m (SM)
Diagnostic support    : DOM
```

```
Serial number      : ED456SS987
```

Status

```
Temperature      : 32.754C  
TX Bias         : 42.700mA  
TX Power        : 0.5192mW, -2.847dBm  
RX Power        : 0.0040mW, -23.979dBm
```

Recent Alarms:

```
Rx power low alarm  
Rx power low warning
```

Recent errors:

```
Receive optical power fault  
PMA/PMD receiver local fault  
PMA/PMD transmitter local fault  
PCS receive local fault  
PHY XS transmit local fault
```

```
Time stamp : Mon Mar 7 16:26:06 2013
```

Viewing transceiver information for copper transceivers with VCT support

This feature provides the ability to view diagnostic monitoring information for copper transceivers with Virtual Cable Test (VCT) support. The cable quality of the copper cables connected between transceivers can be ascertained using the transceiver cable diagnostics. Results of the diagnostics are displayed with the appropriate CLI show commands and with SNMP using the hpicfTransceiver MIB.

The J8177C 1000Base-T Mini-GBIC is supported.

Testing the Cable

Enter the `test cable-diagnostics` command in any context to begin cable diagnostics for the transceiver. The diagnostic attempts to identify cable faults. The tests may take a few seconds to complete for each interface. There is the potential of link loss during the diagnostic.

Syntax:

```
test cable-diagnostics [port-list]
```

Invokes cable diagnostics and displays the results.

Output from test cable-diagnostics command

```
Switch # test cable-diagnostics a23-a24
```

The 'test cable-diagnostics' command will cause a loss of link and will take a few seconds per interface to complete.

```
Continue (Y/N)? y
```

MDI Port	Cable Pair	Distance Status	Pair to Fault	Pair Skew	MDI Polarity	Mode
A23	1-2	OK	0 m	6 ns	Normal	MDIX
	3-6	OK	0 m	0 ns	Normal	
	4-5	OK	0 m	6 ns	Normal	MDIX
	7-8	OK	0 m	6 ns	Normal	
A24	1-2	Short	2 m			
	3-6	Impedance	3 m			

4-5	Impedance	3 m
7-8	Open	1 m

Copper cable diagnostic test results

```
switch# show interfaces transceiver a23 detail
```

```
Transceiver in A23
Interface Index   : 23
Type              : 1000T-sfp
Model             : J8177C
Connector Type    : RJ45
Wavelength        : n/a
Transfer Distance : 100m (copper),
Diagnostic Support : VCT
Serial Number     : US051HF099

Link Status       : Up
Speed             : 1000
Duplex            : Full
```

Port	MDI Pair	Cable Status	Distance to Fault	Pair Skew	Pair Polarity	MDI Mode
A23	1-2	OK	0 m	6 ns	Normal	MDIX
	3-6	OK	0 m	0 ns	Normal	
	4-5	OK	0 m	6 ns	Normal	MDIX
	7-8	OK	0 m	6 ns	Normal	

```
Test Last Run   : Fri Apr 22 20:33:23 2011
```

General transceiver information

Parameter	Description
Interface Index	The switch interface number
Transceiver-type	Pluggable transceiver type
Transceiver model	Pluggable transceiver model
Connector-type	Type of connector of the transceiver
Wavelength	For an optical transceiver: the central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, the values will be separated by a comma. An electrical transceiver value is displayed as N/A.
Transfer Distance	Link-length supported by the transceiver in meters. The corresponding transfer medium is shown in brackets following the transfer distance value, For example, 50um multimode fiber. If the transceiver supports multiple transfer media, the values are separated by a comma.

Table Continued

Parameter	Description
Diagnostic Support	Shows whether the transceiver supports diagnostics: None Supported DOM Supported VCT Supported
Serial Number	Serial number of the transceiver
Link Status	Link up or down
Speed	Speed of transceiver in Mbps
Duplex	Type of duplexing
Cable Status	Values are OK, Open, Short, or Impedance
Distance to Fault	The distance in meters to a cable fault (accuracy is +/- 2 meters); displays 0 (zero) if there is no fault
Pair Skew	Difference in propagation between the fastest and slowest wire pairs
Pair Polarity	Signals on a wire pair are polarized, with one wire carrying the positive signal and one carrying the negative signal.
MDI Mode	The MDI crossover status of the two wire pairs (1&2, 3&6, 4&5, 7&8), will be either MDI or MDIX

Viewing transceiver information

This feature provides the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. The following table indicates the support level for specific transceivers:

Product #	Description	Support ¹
J8436A	10GbE X2-SC SR Optic	V
J8437A	10GbE X2-SC LR Optic	V
J8440B	10GbE X2-CX4 Xcver	NA

Table Continued

Product #	Description	Support ¹
J8440C	10GbE X2-CX4 Xcver	NA
J4858A	Gigabit-SX-LC Mini-GBIC	V
J4858B	Gigabit-SX-LC Mini-GBIC	V
J4858C	Gigabit-SX-LC Mini-GBIC	V (some)
J9054B	100-FX SFP-LC Transceiver	N
J8177C	Gigabit 1000Base-T Mini-GBIC	NA
J9150A	10GbE SFP+ SR Transceiver	D
J9151A	10GbE SFP+ LR Transceiver	D
J9152A	10GbE SFP+ LRM Transceiver	D
J9153A	10GbE SFP+ ER Transceiver	D
J9144A	10GbE X2-SC LRM Transceiver	D
J8438A	10Gbe X2-SC ER Transceiver	D

¹ Support indicators:

- V - Validated to respond to DOM requests
- N - No support of DOM
- D - Documented by the component suppliers as supporting DOM
- NA - Not applicable to the transceiver (copper transceiver)



NOTE: Not all transceivers support Digital Optical Monitoring. If DOM appears in the Diagnostic Support field of the `show interfaces transceiver detail` command, or the `hpicfTransceiverMIB hpicfXcverDiagnostics` MIB object, DOM is supported for that transceiver.

Using the Event Log for troubleshooting switch problems

The Event Log records operating events in single- or double-line entries and serves as a tool to isolate and troubleshoot problems.

Once the log has received 2000 entries, it discards the oldest message each time a new message is received. The Event Log window contains 14 log entry lines. You can scroll through it to view any part of the log.

Once the log has received 2000 entries, it discards the oldest message each time a new message is received. The Event Log window contains 14 log-entry lines. You can scroll through it to view any part of the log.



NOTE:

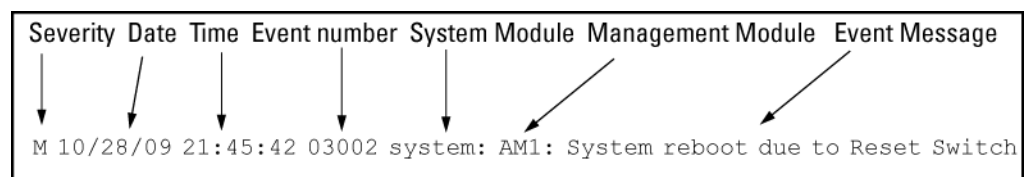
The Event Log is **erased** if power to the switch is interrupted or if you enter the `boot system` command. The contents of the Event Log are **not** erased if you:

- Reboot the switch by choosing the **Reboot Switch** option from the menu interface.
- Enter the `reload` command from the CLI.

Event Log entries

As shown in **Figure 45: Format of an event log entry** on page 364, each Event Log entry is composed of six or seven fields, depending on whether numbering is turned on or not:

Figure 45: *Format of an event log entry*



Item	Description
Severity	One of the following codes (from highest to lowest severity): M —(major) indicates that a fatal switch error has occurred. E —(error) indicates that an error condition occurred on the switch. W —(warning) indicates that a switch service has behaved unexpectedly. I —(information) provides information on normal switch operation. D —(debug) is reserved for internal diagnostic information.
Date	The date in the format mm/dd/yy when an entry is recorded in the log.
Time	The time in the format hh:mm:ss when an entry is recorded in the log.
Event number	The number assigned to an event. You can turn event numbering on and off with the <code>no log-number</code> command.

Table Continued

Item	Description
System module	The internal module (such as "ports:" for port manager) that generated a log entry. If VLANs are configured, a VLAN name also appears for an event that is specific to an individual VLAN.
Event message	A brief description of the operating event.

Table 30: *Event Log system modules*

System module	Description	Documented in Switch hardware/ software guide
802.1x	<p>802.1X authentication: Provides access control on a per-client or per-port basis:</p> <ul style="list-style-type: none"> • Client-level security that allows LAN access to 802.1X clients (up to 32 per port) with valid user credentials • Port-level security that allows LAN access only on ports on which a single 802.1X-capable client (supplicant) has entered valid RADIUS user credentials 	<i>Access Security Guide</i>
acl	<p>ACLs: Filter layer-3 IP traffic to or from a host to block unwanted IP traffic and block or limit other protocol traffic such as TCP, UDP, IGMP, and ICMP. ACEs specify the filter criteria and an action (permit or deny) to take on a packet if it meets the criteria.</p>	<i>Advanced Traffic Management Guide</i>
addrmgr	<p>Address Table Manager: Manages MAC addresses that the switch has learned and are stored in the switch's address table.</p>	<i>Management and Configuration Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
arp-protect	Dynamic ARP Protection: Protects the network from ARP cache poisoning. Only valid ARP requests and responses are relayed or used to update the local ARP cache. ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields are discarded.	<i>Access Security Guide</i>
auth	Authorization: A connected client must receive authorization through web, AMC, RADIUS-based, TACACS+-based, or 802.1X authentication before it can send traffic to the switch.	<i>Access Security Guide</i>
cdp	Cisco Discovery Protocol: Supports reading CDP packets received from neighbor devices, enabling a switch to learn about adjacent CDP devices. HPE does not support the transmission of CDP packets to neighbor devices.	<i>Management and Configuration Guide</i>
chassis	Hardware operation, including modules and ports, power supply, fans, transceivers, CPU interrupt errors, switch temperature, and so on. Chassis messages include events on Power Over Ethernet (POE) operation.	<i>Installation and Getting Started Guide</i> <i>Management and Configuration Guide</i>
connfilt	Connection-rate filtering: Used on the network edge to protect the network from attack by worm-like malicious code by detecting hosts that are generating IP traffic that exhibits this behavior and (optionally) either throttling or dropping all IP traffic from the offending hosts. Connection-rate filtering messages include events on virus throttling. Virus throttling uses connection-rate filtering to stop the propagation of malicious agents.	<i>Access Security Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
console	Console interface used to monitor switch and port status, reconfigure the switch, and read the event log through an in-band Telnet or out-of-band connection.	<i>Installation and Getting Started Guide</i>
cos	Class of Service (CoS): Provides priority handling of packets traversing the switch, based on the IEEE 802.1p priority carried by each packet. CoS messages also include QoS events. The QoS feature classifies and prioritizes traffic throughout a network, establishing an end-to-end traffic priority policy to manage available bandwidth and improve throughput of important data.	<i>Advanced Traffic Management Guide</i>
dca	Dynamic Configuration Arbiter (DCA) determines the client-specific parameters that are assigned in an authentication session.	<i>Access Security Guide</i>
dhcp	Dynamic Host Configuration Protocol (DHCP) server configuration: Switch is automatically configured from a DHCP (Bootp) server, including IP address, subnet mask, default gateway, Timep Server address, and TFTP server address.	<i>Management and Configuration Guide</i>
dhcp v6c	DHCP for IPv6 prefix assignment	<i>IPv6 Configuration Guide</i>
dhcpr	DHCP relay: Forwards client-originated DHCP packets to a DHCP network server.	<i>Advanced Traffic Management Guide</i>
download	Download operation for copying a software version or files to the switch.	<i>Management and Configuration Guide</i>
dhcp-snoop	DHCP snooping: Protects your network from common DHCP attacks, such as address spoofing and repeated address requests.	<i>Access Security Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
dma	Direct Access Memory (DMA): Transmits and receives packets between the CPU and the switch.	—
fault	Fault Detection facility, including response policy and the sensitivity level at which a network problem should generate an alert.	<i>Management and Configuration Guide</i>
fdr-log	FDR collects information that is “interesting” at the time of the crash, as well as when the switch is misbehaving, but has not crashed. Runtime logs are written to FDR memory while the switch is running, and crashtime logs are collected and stored in the FDR buffer during a switch crash.	<i>Management and Configuration Guide</i>
ffi	Find, Fix, and Inform: Event or alert log messages indicating a possible topology loop that causes excessive network activity and results in the network running slow. FFI messages include events on transceiver connections with other network devices.	<i>Installation and Getting Started Guide</i> <i>Management and Configuration Guide</i>
garp	Generic Attribute Registration Protocol (GARP), defined in the IEEE 802.1D-1998 standard.	<i>Advanced Traffic Management Guide</i>
gvrp	GARP VLAN Registration Protocol (GVRP): Manages dynamic 802.1Q VLAN operations, in which the switch creates temporary VLAN membership on a port to provide a link to another port in the same VLAN on another device.	<i>Advanced Traffic Management Guide</i>
hpesp	Management module that maintains communication between switch ports.	<i>Installation and Getting Started Guide</i>
idm	Identity-driven Management: Optional management application used to monitor and control access to switch.	<i>Advanced Traffic Management Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
igmp	Internet Group Management Protocol: Reduces unnecessary bandwidth usage for multicast traffic transmitted from multimedia applications on a per-port basis.	<i>Multicast and Routing Guide</i>
inst-mon	Instrumentation Monitor: Identifies attacks on the switch by generating alerts for detected anomalies.	<i>Access Security Guide</i>
ip	IP addressing: Configures the switch with an IP address and subnet mask to communicate on the network and support remote management access; configures multiple IP addresses on a VLAN; enables IP routing on the switch.	<i>Management and Configuration Guide</i> <i>Multicast and Routing Guide</i>
ipaddrmgr	IP Address Manager: Programs IP routing information in switch hardware.	<i>Multicast and Routing Guide</i>
iplock	IP Lockdown: Prevents IP source address spoofing on a per-port and per-VLAN basis by forwarding only the IP packets in VLAN traffic that contain a known source IP address and MAC address binding for the port.	<i>Access Security Guide</i>
ipx	Novell Netware protocol filtering: On the basis of protocol type, the switch can forward or drop traffic to a specific set of destination ports on the switch.	<i>Access Security Guide</i>
kms	Key Management System: Configures and maintains security information (keys) for all routing protocols, including a timing mechanism for activating and deactivating an individual protocol.	<i>Access Security Guide</i>
lACP	LACP trunks: The switch can either automatically establish an 802.3ad-compliant trunk group or provide a manually configured, static LACP trunk.	<i>Management and Configuration Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
ldbal	Load balancing in LACP port trunks or 802.1s Multiple Spanning Tree protocol (MSTP) that uses VLANs in a network to improve network resource utilization and maintain a loop-free environment. Load-balancing messages also include switch meshing events. The switch meshing feature provides redundant links, improved bandwidth use, and support for different port types and speeds.	<i>Management and Configuration Guide</i> <i>Advanced Traffic Management Guide</i>
lldp	Link-Layer Discovery Protocol: Supports transmitting LLDP packets to neighbor devices and reading LLDP packets received from neighbor devices, enabling a switch to advertise itself to adjacent devices and to learn about adjacent LLDP devices.	<i>Management and Configuration Guide</i>
loop_protect	Loop protection: Detects the formation of loops when an unmanaged device on the network drops spanning tree packets and provides protection by transmitting loop protocol packets out ports on which loop protection has been enabled.	<i>Advanced Traffic Management Guide</i>
macauth	Web and MAC authentication: Port-based security employed on the network edge to protect private networks and the switch itself from unauthorized access using one of the following interfaces: <ul style="list-style-type: none"> • Web page login to authenticate users for access to the network • RADIUS server that uses a device's MAC address for authentication 	<i>Access Security Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
maclock	<p>MAC lockdown and MAC lockout</p> <ul style="list-style-type: none"> MAC lockdown prevents station movement and MAC address "hijacking" by requiring a MAC address to be used only on an assigned port on the switch. MAC Lockdown also restricts the client device to a specific VLAN. MAC lockout blocks a specific MAC address so that the switch drops all traffic to or from the specified address. 	<i>Access Security Guide</i>
mgr	Windows-based network management solutions for managing and monitoring performance of the switches.	<i>Management and Configuration Guide</i>
mld	Multicast Listener Discovery (MLD): IPv6 protocol used by a router to discover the presence of multicast listeners. MLD can also optimize IPv6 multicast traffic flow with the snooping feature.	<i>Multicast and Routing Guide</i>
mtm	Multicast Traffic Manager (MTM): Controls and coordinates L3 multicast traffic for upper layer protocols.	<i>Multicast and Routing Guide</i>
netinet	Network Internet: Monitors the creation of a route or an Address Resolution Protocol (ARP) entry and sends a log message in case of failure.	<i>Advanced Traffic Management Guide</i>
pagp	Ports Aggregation Protocol (PAgP): Obsolete. Replaced by LACP (802.3ad).	—

Table Continued

System module	Description	Documented in Switch hardware/ software guide
ports	<p>Port status and port configuration features, including mode (speed and duplex), flow control, broadcast limit, jumbo packets, and security settings.</p> <p>Port messages include events on POE operation and transceiver connections with other network devices.</p>	<p><i>Installation and Getting Started Guide</i></p> <p><i>Management and Configuration Guide</i></p> <p><i>Access Security Guide</i></p>
radius	RADIUS (Remote Authentication Dial-In User Service) authentication and accounting: A network server is used to authenticate user-connection requests on the switch and collect accounting information to track network resource usage.	<i>Access Security Guide</i>
ratelim	Rate-limiting: Enables a port to limit the amount of bandwidth a user or device may utilize for inbound traffic on the switch.	<i>Management and Configuration Guide</i>
sflow	Flow sampling: sFlow is an industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.	<i>Management and Configuration Guide</i>
snmp	Simple Network Management Protocol: Allows you to manage the switch from a network management station, including support for security features, event reporting, flow sampling, and standard MIBs.	<i>Management and Configuration Guide</i>
sntp	Simple Network Time Protocol: Synchronizes and ensures a uniform time among interoperating devices.	<i>Management and Configuration Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
ssh	Secure Shell version 2 (SSHv2): Provides remote access to management functions on a switch via encrypted paths between the switch and management station clients capable of SSH operation. SSH messages also include events from the Secure File Transfer Protocol (SFTP) feature. SFTP provides a secure alternative to TFTP for transferring sensitive information, such as switch configuration files, to and from the switch in an SSH session.	<i>Access Security Guide</i>
ssl	Secure Socket Layer Version 3 (SSLv3), including Transport Layer Security (TLSv1) support: Provides remote web access to a switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation.	<i>Access Security Guide</i>
stack	Stack management: Uses a single IP address and standard network cabling to manage a group (up to 16) of switches in the same IP subnet (broadcast domain), resulting in a reduced number of IP addresses and simplified management of small workgroups for scaling your network to handle increased bandwidth demand.	<i>Advanced Traffic Management Guide</i>
stp	Multiple-instance spanning tree protocol/MSTP (802.1s): Ensures that only one active path exists between any two nodes in a group of VLANs in the network. MSTP operation is designed to avoid loops and broadcast storms of duplicate messages that can bring down the network.	<i>Advanced Traffic Management Guide</i>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
system	<p>Switch management, including system configuration, switch bootup, activation of boot ROM image, memory buffers, traffic and security filters.</p> <p>System messages also include events from management interfaces (menu and CLI) used to reconfigure the switch and monitor switch status and performance.</p>	<p><i>Basic Operation Guide</i></p> <p><i>Access Security Guide</i></p>
tacacs	<p>TACACS+ authentication: A central server is used to control access to the switches (and other TACACS-aware devices) in the network through a switch's console port (local access) or Telnet (remote access).</p>	<p><i>Access Security Guide</i></p>
tcp	<p>Transmission Control Protocol: A transport protocol that runs on IP and is used to set up connections.</p>	<p><i>Advanced Traffic Management Guide</i></p>
telnet	<p>Session established on the switch from a remote device through the Telnet virtual terminal protocol.</p>	<p><i>Basic Operation Guide</i></p>
tftp	<p>Trivial File Transfer Protocol: Supports the download of files to the switch from a TFTP network server.</p>	<p><i>Basic Operation Guide</i></p>
timep	<p>Time Protocol: Synchronizes and ensures a uniform time among interoperating devices.</p>	<p><i>Management and Configuration Guide</i></p>
udld	<p>Uni-directional Link Detection: Monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices.</p>	<p><i>Access Security Guide</i></p>

Table Continued

System module	Description	Documented in Switch hardware/ software guide
udpf	UDP broadcast forwarding: Supports the forwarding of client requests sent as limited IP broadcasts addressed to a UDP application port on a network server.	<i>Multicast and Routing Guide</i>
update	Updates (TFTP or serial) to HPE switch software and updates to running-config and start-up config files	<i>Basic Operation Guide</i>
vlan	<p>Static 802.1Q VLAN operations, including port-and protocol-based configurations that group users by logical function instead of physical location</p> <ul style="list-style-type: none"> • A port-based VLAN creates a layer-2 broadcast domain comprising member ports that bridge IPv4 traffic among themselves. • A protocol-based VLAN creates a layer-3 broadcast domain for traffic of a particular routing protocol, and comprises member ports that bridge traffic of the specified protocol type among themselves. <p>VLAN messages include events from management interfaces (menu and CLI) used to reconfigure the switch and monitor switch status and performance.</p>	<i>Advanced Traffic Management Guide</i>
xmodem	Xmodem: Binary transfer feature that supports the download of software files from a PC or UNIX workstation.	<i>Basic Operation Guide</i>

Using the CLI

Syntax:

```
show logging [-a, -b, -r, -s, -t, -m, -e, -p, -w, -i, -d, command, filter] [< option-str >]
```

By default, the `show logging` command displays the log messages recorded since the last reboot in chronological order:

-a	Displays all recorded log messages, including those before the last reboot.
-b	Displays log events as the time since the last reboot instead of in a date/time format.
-r	Displays all recorded log messages, with the most recent entries listed first (reverse order).
-s	Displays the active management module (AM) and standby management module (SM) log events.
-t	Displays the log events with a granularity of 10 milliseconds.
-m	Displays only major log events.
-e	Displays only error event class.
-p	Displays only performance log events.
-w	Displays only warning log events.
-i	Displays only informational log events.
-d	Displays only debug log events.
command	Displays only command logs.
filter	Displays only log filter configuration and status information.
<option-str>	Displays all Event Log entries that contain the specified text. Use an <option-str> value with -a or -r to further filter show logging command output.

Example:

To display all Event Log messages that have "system" in the message text or module name, enter the following command:

```
switch# show logging -a system
```

To display all Event Log messages recorded since the last reboot that have the word "system" in the message text or module name, enter:

```
switch# show logging system
```

Clearing Event Log entries

Syntax:

```
clear logging [command]
```

Removes all entries from the event log display output.

Use the `clear logging` command to hide, but not erase, Event Log entries displayed in `show logging` command output. Only new entries generated after you enter the command will be displayed.

To redisplay all hidden entries, including Event Log entries recorded prior to the last reboot, enter the `show logging -a` command.

The `command` option removes all entries from the command log.

Turning event numbering on

Syntax:

```
no log-numbers
```

Turns event numbering on and off

Using log throttling to reduce duplicate Event Log and SNMP messages

A recurring event can generate a series of duplicate Event Log messages and SNMP traps in a relatively short time. As a result, the Event Log and any configured SNMP trap receivers may be flooded with excessive, exactly identical messages. To help reduce this problem, the switch uses **log throttle periods** to regulate (throttle) duplicate messages for recurring events, and maintains a counter to record how many times it detects duplicates of a particular event since the last system reboot.

When the first instance of a particular event or condition generates a message, the switch initiates a log throttle period that applies to all recurrences of that event. If the logged event recurs during the log throttle period, the switch increments the counter initiated by the first instance of the event, but does not generate a new message.

If the logged event repeats again after the log throttle period expires, the switch generates a duplicate of the first message, increments the counter, and starts a new log throttle period during which any additional instances of the event are counted, but not logged. Thus, for a particular recurring event, the switch displays only one message in the Event Log for each log throttle period in which the event reoccurs. Also, each logged instance of the event message includes counter data showing how many times the event has occurred since the last reboot. The switch manages messages to SNMP trap receivers in the same way.

Log throttle periods

The length of the log throttle period differs according to an event's severity level:

Severity level	Log throttle period
I (Information)	6000 Seconds
W (Warning)	600 Seconds
D (Debug)	60 Seconds
M (Major)	6 Seconds

Example:

Suppose that you configure VLAN 100 on the switch to support PIM operation, but do not configure an IP address. If PIM attempts to use VLAN 100, the switch generates the first instance of the following Event Log message and counter.



NOTE:

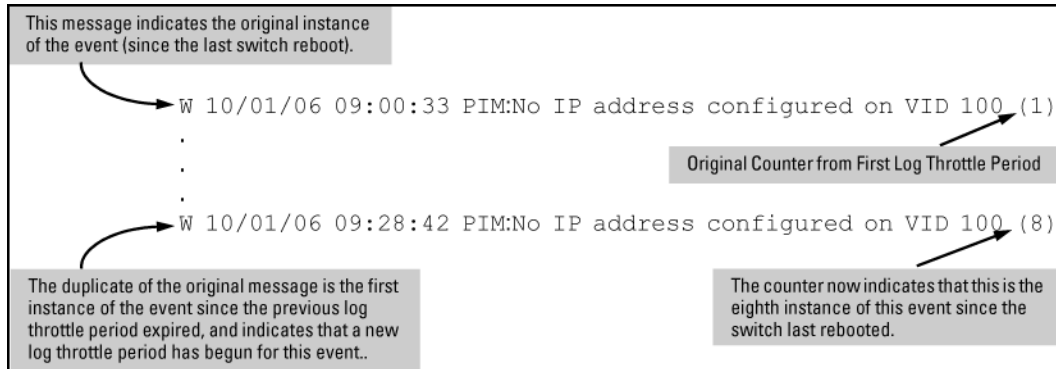
In **The first instance of an event message and counter** on page 378 the counter (1) indicates that this is the first instance of this event since the switch last rebooted.

The first instance of an event message and counter

```
W 10/01/12 09:00:33 PIM:No IP address configured on VID 100 (1)
```

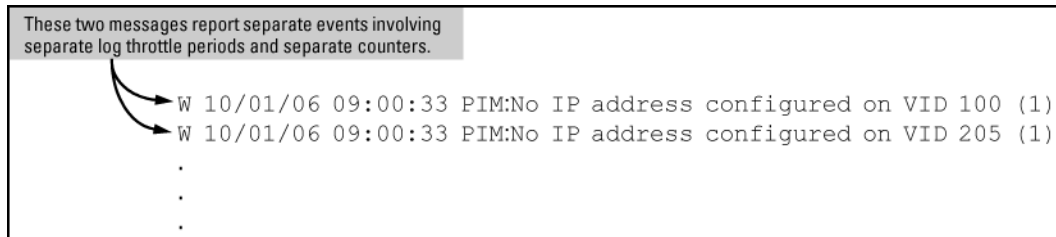
If PIM operation causes the same event to occur six more times during the initial log throttle period, there are no further entries in the Event Log. However, if the event occurs again after the log throttle period has expired, the switch repeats the message (with an updated counter) and starts a new log throttle period.

Figure 46: Duplicate messages over multiple log throttling periods



Note that if the same type of event occurs under different circumstances, the switch handles these as unrelated events for the purpose of Event Log messages. For example, if PIM operation simultaneously detects that VLANs 100 and 205 are configured without IP addresses, you see log messages similar to the following:

Figure 47: Example: of log messages generated by unrelated events of the same type



Example: of event counter operation

Suppose the switch detects the following after a reboot:

- Three duplicate instances of the PIM "Send error" during the first log throttle period for this event
- Five more instances of the same Send error during the second log throttle period for this event
- Four instances of the same Send error during the third log throttle period for this event

In this case, the duplicate message appears three times in the Event Log (once for each log throttle period for the event being described), and the duplicate message counter increments as shown in the following table. (The same operation applies for messages sent to any configured SNMP trap receivers.)

Table 31: How the duplicate message counter increments

Instances during 1st log throttle period	Instances during 2nd log throttle period	Instances during 3rd log throttle period	Duplicate message counter ¹
3			1
	5		4
		4	9

¹ This value always comprises the first instance of the duplicate message in the current log throttle period plus all previous occurrences of the duplicate message occurring since the switch last rebooted.

Reporting information about changes to the running configuration

Syslog can be used for sending notifications to a remote syslog server about changes made to the running configuration. The notifications in the syslog messages are sent in ASCII format and contain this information:

- Notice-Type: Describes the syslog notification as a “running config change”.
- Event-ID: Identifier for the running config change event that occurred on the switch.
- Config-Method: The source for the running config change.
- Device-Name: The managed device.
- User-Name: User who made the running config change.
- Remote-IP-Address: IP address of a remote host from which the user is connected.

Syntax:

```
no logging notify <running-config-change> [transmission-interval <0-4294967295>
```

Enables sending the running configuration change notifications to the syslog server.

The `no` form of the command disables sending the running configuration changes to the syslog server.

Default: Disabled

<code><running-config-change ></code>	Mandatory option for the notify parameter. Specifies the type of notification to send.
<code>transmission-interval <0-4294967295></code>	Specifies the time interval (in seconds) between the transmission of two consecutive notifications. Running config changes occurring within the specified interval will not generate syslog notifications.

A value of zero means there is no limit; a notification is sent for every running config change.

Default: Zero

Sending running config changes to the syslog server

```
switch(config)# logging notify running-config-change  
transmission-interval 10
```

Debug/syslog operation

While the Event Log records switch-level progress, status, and warning messages on the switch, the debug/system logging (**syslog**) feature provides a way to record Event Log and debug messages on a remote device. For example, you can send messages about routing misconfigurations and other network protocol details to an external device, and later use them to debug network-level problems.

Debug/syslog messaging

The debug/syslog feature allows you to specify the types of Event Log and debug messages that you want to send to an external device. You can perform the following operations:

- Use the `debug` command to configure messaging reports for the following event types:
 - ACL "deny" matches
 - Dynamic ARP protection events
 - DHCP snooping events
 - DIPLD events
 - Events recorded in the switch's Event Log
 - IP routing events (IPv4 and IPv6)
 - LACP events
 - LLDP events
 - SNMP events
 - SSH events
- Use the `logging` command to select a subset of Event Log messages to send to an external device for debugging purposes according to:
 - Severity level
 - System module

Hostname in syslog messages

The syslog now messages the sender identified by hostname.

The hostname field identifies the switch that originally sends the syslog message. Configurable through the CLI and SNMP, the format of the hostname field supports the following formats:

- `ip-address`: The IP address of the sending interface will be used as the message origin identifier. This is the default format for the origin identifier. The IP address of the sending interface (in dotted decimal notation) is the default format.
- `hostname`: The hostname of the sending switch will be used as the message origin identifier.
- `none`: No origin identifier will be embedded in the syslog message. Nil value is used as defined by “-“.

This configuration is system-wide, not per syslog server. There is no support for fully-qualified domain name.

Logging origin-id

Use the `logging origin-id` command to specify the content for the hostname field.

Syntax:

```
logging origin-id [ip-address|hostname|none]
```

```
no logging origin-id [ip-address|hostname|none]
```

To reset the hostname field content back to default (IP-address), use the `no` form of the command.

filter

Creates a filter to restrict which events are logged.

IP-ADDR

Adds an IPv4 address to the list of receiving syslog servers.

IPV6-ADDR

Adds an IPv6 address to the list of receiving syslog servers.

origin-id

Sends the Syslog messages with the specified origin-id.

notify

Notifies the specified type sent to the syslog server(s).

priority-descr

A text string associated with the values of facility, severity, and system-module.

severity

Event messages of the specified severity or higher sent to the syslog server.

system-module

Event messages of the specified system module (subsystem) sent to the syslog server.

hostname

Sets the hostname of the device as the origin-id.

none

Disables origin-id in the syslog message.

Add an IP address to the list of receiving syslog servers.

Use of `no` without an IP address specified will remove all IP addresses from the list of syslog receivers. If an IP address is specified, that receiver will be removed. Both link-local with zone ID and global IPv6 addresses are supported.

- Specify syslog server facility with the option `<facility>`. The command `no logging <facility>` sets the facility back to defaults.
- Specify filtering rules.
- Specify severity for event messages to be filtered to the syslog server with the option `<severity>`. The command `no logging <severity>` sets the severity back to default.

- Event messages of specified system module will be sent to the syslog server. Using `no` sends messages from all system modules. Messages are first filtered by selected severity.
- Specify syslog server transport layer with options `[udp] | [tcp] | [tls]`.
- Specify syslog server port number with options `[udp PORT-NUM] | [tcp PORT-NUM] | [tls PORT-NUM]`.
- Specify notification types to be sent to the syslog server.
- Use the option `transmission-interval` to control the egress rate limit for transmitting notifications, 0 value means there is no rate limit. The values are in seconds. Only one syslog message is allowed for transmission within specified time interval.
- Specify the origin information for the syslog messages with the option `origin-id`.



NOTE: When the syslog server receives messages from the switch, the IPv6 address of the switch is partly displayed.

Example:

Configured Host Ipv6 Address: 2001::1

Expected Syslog message:

```
Syslog message: USER.INFO: Oct 11 02:40:02 2001::1 00025 ip:
ST1CMDR: VLAN60: ip address 30.1.1.1/24 configured on vlan 60
```

Actual Truncated syslog message:

```
Syslog message: USER.INFO: Oct 11 02:40:02 2001:: 00025 ip: ST1CMDR:
VLAN60: ip address 30.1.1.1/24 configured on vlan 60
```

Use the command in the following example to set the `origin-id` to the hostname.

Setting the origin-id to the hostname

```
switch(config)# logging origin-id hostname
```

The following syslog message will occur:

```
<14> Jan 1 00:15:35 2910a1-24G 00076 ports: port 2 is now on-line
```

Use the command in the following example to set the `origin-id` to none (nilvalue).

Setting the origin-id to none (nilvalue)

```
switch(config)# logging origin-id none
```

The following syslog message will occur:

```
<14> Jan 1 00:15:35 - 00076 ports: port 2 is now on-line
```

Use any of the commands in the following example to set the `origin-id` to ip-address (default).

Setting the origin-id to ip-address (default)

```
switch(config)# logging origin-id ip-address
```

```
switch(config)# no logging origin-id hostname
```

```
switch(config)# no logging origin-id none
```

The following syslog message will occur:

```
<14> Jan 1 00:15:35 169.254.230.236 00076 ports: port 2 is now on-line
```

Viewing the identification of the syslog message sender

Use the commands `show debug` or `show running-config` to display the identification of the syslog message sender. The default option for `origin-id` is `ip-address`. The command `show running-config` will not display the configured option when `origin-id` is set to the default value of `ip address`.

When `hostname` or `none` is configured using `logging origin-id`, the same displays as part of the `show running-config` command.

Syntax:

```
show debug
```

Default option is `ip-address`.

The following shows the output of the `show debug` command when configured without `login origin-id`.

Output of the show debug command when configured without login origin-id

```
Debug Logging
  Origin identifier: Outgoing Interface IP
  Destination:      None
```

```
Enabled debug types:
  None are enabled.
```

The command `logging origin-id hostname` will produce the syslog message shown in the following example.

Syslog message for logging origin-id hostname

```
Debug Logging
  Origin identifier: Hostname
  Destination:      None
```

```
Enabled debug types:
  None are enabled.
```

The command `logging origin-id none` will produce the syslog message shown in the following example.

Syslog message for logging origin-id none

```
Debug Logging
  Origin identifier: none
  Destination:      None
```

```
Enabled debug types:
  None are enabled.
```

Syntax:

```
show running-config
```

The following example shows the output of the `show running-config` command.

Output of the show running-config command

The command logging **origin-id hostname** will display the following:
logging origin-id hostname

The command logging origin-id none will display as the following:
logging origin-id none

SNMP MIB

SNMP support will be provided through the following MIB objects.

HpicfSyslogOriginId = textual-convention

Description

This textual convention enumerates the origin identifier of syslog message.

Syntax: integer

ip-address
hostname
none

Status

current

hpicfSyslogOriginId OBJECT-TYPE

Description

Specifies the content of a Hostname field in the header of a syslog message.

Syntax:

HpicfSyslogOriginId

Max-access

read-write

Status

current

Default

ip-address

Debug/syslog destination devices

To use debug/syslog messaging, you must configure an external device as the logging destination by using the logging and debug destination commands. For more information, see [Debug destinations](#) on page 394 and [Configuring a syslog server](#) on page 396.

A debug/syslog destination device can be a syslog server and/or a console session. You can configure debug and logging messages to be sent to:

- Up to six syslog servers
- A CLI session through a direct RS-232 console connection, or a Telnet or SSH session

Debug/syslog configuration commands

Event notification logging	—	Automatically sends switch-level event messages to the switch's Event Log. Debug and syslog do not affect this operation, but add the capability of directing Event Log messaging to an external device.
logging command	<syslog-ip-addr>	Enables syslog messaging to be sent to the specified IP address. IPv4 and IPv6 are supported.
	facility	(Optional) The logging facility command specifies the destination (facility) subsystem used on a syslog server for debug reports.
	priority-desc	A text string associated with the values of facility, severity, and system-module.
	neighbor-adjacency [detail]	Enables or disables OSPFv3 (IPv6) adjacency logging. Must be executed in OSPFv3 context. The detail option displays all the adjacency state transitions and adjacency-related errors.
	severity	Sends Event Log messages of equal or greater severity than the specified value to configured debug destinations. (The default setting is to send Event Log messages from all severity levels.)

Table Continued

	system-module	<p>Sends Event Log messages from the specified system module to configured debug destinations. The severity filter is also applied to the system-module messages you select.</p> <p>The default setting is to send Event Log messages from all system modules. To restore the default setting, enter the <code>no logging system-module <system-module></code> or <code>logging system-module all-pass</code> commands.</p>
debug Command	acl	Sends ACL syslog logging to configured debug destinations. When there is a match with a "deny" statement, directs the resulting message to the configured debug destinations.
	all	Sends debug logging to configured debug destinations for all ACL, Event Log, IP-OSPF, and IP-RIP options.
	cdp	Displays CDP information.
	destination	<p><code>logging</code>: Disables or re-enables syslog logging on one or more syslog servers configured with the <code>logging syslog-ip-addr</code> command.</p> <p><code>session</code>: Assigns or re-assigns destination status to the terminal device that was most recently used to request debug output.</p> <p><code>buffer</code>: Enables syslog logging to send the debug message types specified by the <code>debug <debug-type></code> command to a buffer in switch memory.</p>
	event	Sends standard Event Log messages to configured debug destinations. (The same messages are also sent to the switch's Event Log, regardless of whether you enable this option.)

Table Continued

	ip	<p>fib: Displays IP Forwarding Information Base messages and events.forwarding: Sends IPv4 forwarding messages to the debug destinations.ospf: Sends OSPF event logging to the debug destinations.ospfv3: Enables debug messages for OSPFv3.packet: Sends IPv4 packet messages to the debug destinations. pim [packet [filter {source < ip-addr > vlan < vid >}]]: Enables or disables tracing of PIM messages.Note: When PIM debugging is enabled, the following message displays:</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p>PIM Debugging can be extremely CPU intensive when run on a device with an existing high CPU load or on a switch with more than 10 PIM-enabled VLANs. In high load situations, the switch may suffer from protocol starvation, high latency, or even reload. When debugging a switch with more than 10 PIM-enabled VLANs, the "vlan" option in "debug ip pim packet" should be utilized. Debugging should only be used temporarily while troubleshooting problems. Customers are advised to exercise caution when running this command in a highstress production network.</p> </div> <p>pbr: Logs a message when a PBR policy is applied, when the action in a class goes active or when it goes inactive.rip: Sends RIP event logging to the debug destinations.</p>
--	----	---

Table Continued

	ipv6	dhcpv6-client: Sends DHCPv6 client debug messages to the configured debug destination.dhcpv6-relay: Sends DHCPv6 relay debug messages to the configured debug destination.forwarding: Sends IPv6 forwarding messages to the debug destination(s)nd: Sends IPv6 debug messages for IPv6 neighbor discovery to the configured debug destinations.
	lACP	event: Sends messages related to change events.packet: Sends messages when BPDUs are exchanged.
	lldp	Sends LLDP debug messages to the debug destinations.
	security	Sends security messages to the debug destination.
	services	Displays debug messages on the services module.
	snmp	Sends snmp messages to the debug destination.

Using the Debug/Syslog feature, you can perform the following operations:

- Configure the switch to send Event Log messages to one or more Syslog servers. In addition, you can configure the messages to be sent to the User log facility (default) or to another log facility on configured Syslog servers.
- Configure the switch to send Event Log messages to the current management- access session (serial-connect CLI, Telnet CLI, or SSH).
- Disable all Syslog debug logging while retaining the Syslog addresses from the switch configuration. This allows you to configure Syslog messaging and then disable and re-enable it as needed.
- Display the current debug configuration. If Syslog logging is currently active, the list of configured Syslog servers is displayed.
- Display the current Syslog server list when Syslog logging is disabled.

Configuring debug/syslog operation

Procedure

1. To use a syslog server as the destination device for debug messaging, follow these steps:

- a. Enter the `logging <syslog-ip-addr>` command at the global configuration level to configure the syslog server IP address and enable syslog logging. Optionally, you may also specify the destination subsystem to be used on the syslog server by entering the `logging facility` command. If no other syslog server IP addresses are configured, entering the `logging` command enables both debug messaging to a syslog server and the event debug message type. As a result, the switch automatically sends Event Log messages to the syslog server, regardless of other debug types that may be configured.
- b. Re-enter the `logging` command in Step 1a to configure additional syslog servers. You can configure up to a total of six servers. (When multiple server IP addresses are configured, the switch sends the debug message types that you configure in **Step 3** to all IP addresses.)

2. To use a CLI session on a destination device for debug messaging:

- a. Set up a serial, Telnet, or SSH connection to access the switch's CLI.
- b. Enter the `debug destination session` command at the manager level.

3. Enable the types of debug messages to be sent to configured syslog servers, the current session device, or both by entering the `debug <debug-type>` command and selecting the desired options.

Repeat this step if necessary to enable multiple debug message types.

By default, Event Log messages are sent to configured debug destination devices. To block Event Log messages from being sent, enter the `no debug event` command.

4. If necessary, enable a subset of Event Log messages to be sent to configured syslog servers by specifying a severity level, a system module, or both using the following commands:

```
switch(config)# logging severity <debug | major | error | warning | info>
switch(config)# logging system-module <system-module>
```

To display a list of valid values for each command, enter `logging severity` or `logging system-module` followed by `?` or pressing the Tab key.

The severity levels in order from the highest to lowest severity are major, error, warning, info, and debug. For a list of valid values for the `logging system-module <system-module>` command, see **Event Log system modules**.

5. If you configure system-module, severity-level values, or both to filter Event Log messages, when you finish troubleshooting, you may want to reset these values to their default settings so that the switch sends all Event Log messages to configured debug destinations (syslog servers, CLI session, or both).

To remove a configured setting and restore the default values that send all Event Log messages, enter one or both of the following commands:

```
switch(config)# no logging severity <debug | major | error | warning | info>
switch(config)# no logging system-module <system-module>
```



CAUTION: If you configure a severity-level, system-module, logging destination, or logging facility value and save the settings to the startup configuration (For example, by entering the `write memory` command), the debug settings are saved after a system reboot (power cycle or reboot) and re-activated on the switch. As a result, after switch startup, one of the following situations may occur:

- Only a partial set of Event Log messages may be sent to configured debug destinations.
 - Messages may be sent to a previously configured syslog server used in an earlier debugging session.
-

Viewing a debug/syslog configuration

Use the `show debug` command to display the currently configured settings for:

- Debug message types and Event Log message filters (severity level and system module) sent to debug destinations
- Debug destinations (syslog servers or CLI session) and syslog server facility to be used

Syntax:

```
show debug
```

Displays the currently configured debug logging destinations and message types selected for debugging purposes. (If no syslog server address is configured with the `logging <syslog-ip-addr>` command, no `show debug` command output is displayed.)

Output of the show debug command

```
switch(config)# show debug

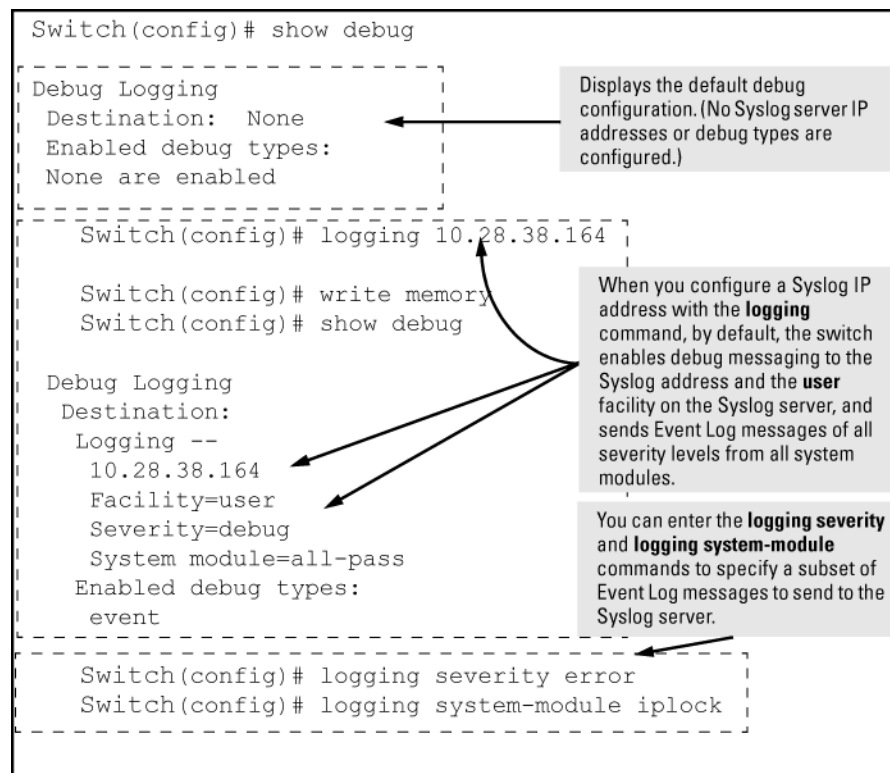
Debug Logging
Destination:
Logging --
 10.28.38.164
Facility=kern
Severity=warning
System module=all-pass
Enabled debug types:
event
```

Example:

In the following Example:, no syslog servers are configured on the switch (default setting). When you configure a syslog server, debug logging is enabled to send Event Log messages to the server. To limit the Event Log

messages sent to the syslog server, specify a set of messages by entering the `logging severity` and `logging system-module` commands.

Figure 48: Syslog configuration to receive event log messages from specified system module and severity levels



As shown at the top of **Figure 48: Syslog configuration to receive event log messages from specified system module and severity levels** on page 391, if you enter the `show debug` command when no syslog server IP address is configured, the configuration settings for syslog server facility, Event Log severity level, and system module are not displayed. However, after you configure a syslog server address and enable syslog logging, all debug and logging settings are displayed with the `show debug` command.

If you do not want Event Log messages sent to syslog servers, you can block the messages from being sent by entering the `no debug event` command. (There is no effect on the normal logging of messages in the switch's Event Log.)

Example:

The next Example: shows how to configure:

- Debug logging of ACL and IP-OSPF packet messages on a syslog server at 18.38.64.164 (with user as the default logging facility).
- Display of these messages in the CLI session of your terminal device's management access to the switch.
- Blocking Event Log messages from being sent from the switch to the syslog server and a CLI session.

To configure syslog operation in these ways with the debug/syslog feature disabled on the switch, enter the commands shown in **Figure 49: Debug/syslog configuration for multiple debug types and multiple destinations** on page 392.

Figure 49: Debug/syslog configuration for multiple debug types and multiple destinations

```
Switch# config
Switch(config)# logging 10.38.64.164
Switch(config)# show debug
Debug Logging
Destination:
Logging --
 10.38.64.164
 Facility=user
 Severity=debug
 System module=all-pass
Enabled debug types:
 event
Switch(config)# no debug event
Switch(config)# debug acl
Switch(config)# debug ip ospf packet
Switch(config)# debug destination session
Switch(config)# show debug
Debug Logging
Destination:
Logging --
 10.38.64.164
 Facility=user
 Severity=debug
 System module=all-pass
Session
Enabled debug types:
 acl log
 ip ospf packet
```

Configure a Syslog server IP address. (No other Syslog servers are configured on the switch.) The server address serves as an active debug destination for any configured debug types.)

Display the new debug configuration. (Default debug settings - facility, severity, system module, and debug types- are displayed.)

Remove the unwanted event message logging to debug destinations.

Configure the debug messages types that you want to send to the Syslog server and CLI session.

Configure the CLI session as a debug destination.

Display the final debug and Syslog server configuration.

Debug command

At the manager level, use the `debug` command to perform two main functions:

- Specify the types of event messages to be sent to an external destination.
- Specify the destinations to which selected message types are sent.

By default, no debug destination is enabled and only Event Log messages are enabled to be sent.



NOTE:

To configure a syslog server, use the `logging <syslog-ip-addr>` command. For more information, see **Configuring a syslog server** on page 396.

Debug messages

Syntax:

```
no debug <debug-type>
```





acl	<p>When a match occurs on an ACL "deny" ACE (with <code>log</code> configured), the switch sends an ACL message to configured debug destinations. For information on ACLs, see the "Access Control Lists (ACLs)" in the latest version of the following guides:</p> <ul style="list-style-type: none"> IPv4 ACLs: access security guide IPv6 ACLs: IPv6 configuration guide <hr/> <p> NOTE: ACE matches (hits) for permit and deny entries can be tracked using the <code>show statistics <aclv4 aclv6></code> command.</p> <hr/> <p>(Default: Disabled—ACL messages for traffic that matches "deny" entries are not sent.)</p>
all	Configures the switch to send all debug message types to configured debug destinations.(Default: Disabled—No debug messages are sent.)
cdp	Sends CDP information to configured debug destinations.
destination	<p><code>logging</code>—Disables or re-enables syslog logging on one or more syslog servers configured with the <code>logging <syslog-ip-addr></code> command. <code>session</code>—Assigns or re-assigns destination status to the terminal device that was most recently used to request debug output. <code>buffer</code>—Enables syslog logging to send the debug message types specified by the <code>debug <debug-type></code> command to a buffer in switch memory.For more information on these options, see Debug destinations on page 394.</p>
event	<p>Configures the switch to send Event Log messages to configured debug destinations.</p> <hr/> <p> NOTE: This value does not affect the reception of event notification messages in the Event Log on the switch.</p> <hr/> <p>Event Log messages are automatically enabled to be sent to debug destinations in these conditions:</p> <ul style="list-style-type: none"> If no syslog server address is configured and you enter the <code>logging <syslog-ip-addr></code> command to configure a destination address. If at least one syslog server address is configured in the startup configuration, and the switch is rebooted or reset. <p>Event log messages are the default type of debug message sent to configured debug destinations.</p>
ip [fib forwarding packet rip]	Sends IP messages to configured destinations.
	ip [fib [events]]
	For the configured debug destinations: <code>events</code> —Sends IP forwarding information base events.

Table Continued


	<code>ip [packet]</code>	Enables the specified PIM message type.
	<code>ip [rip [database event trigger]]</code>	<code>rip {<database event trigger>}</code> —Enables the specified RIP message type for the configured destination(s). <code>database</code> —Displays database changes. <code>event</code> —Displays RIP events. <code>trigger</code> —Displays trigger messages.
	<code>ipv6 [dhcpv6-client nd packet]</code>	 <p>NOTE: See the "IPv6 Diagnostic and Troubleshooting" in the IPv6 configuration guide for your switch for more detailed IPv6 debug options.</p> <p>When no debug options are included, displays debug messages for all IPv6 debug options. <code>dhcpv6-client [events packet]</code>—Displays DHCPv6 client event and packet data. <code>nd</code>—Displays debug messages for IPv6 neighbor discovery. <code>packet</code>—Displays IPv6 packet messages.</p>
	<code>lldp</code>	Enables all LLDP message types for the configured destinations.
	<code>security [arp-protect dhcp-snooping dynamic-ip-lockdown port-access port-security radius-server ssh tacacs-server user-profile-mib]</code>	<p><code>arp-protect</code>— Sends dynamic ARP protection debug messages to configured debug destinations. <code>dhcp-snooping</code>—Sends DHCP snooping debug messages to configured debug destinations. <code>agent</code>—Displays DHCP snooping agent messages. <code>event</code>—Displays DHCP snooping event messages. <code>packet</code>—Displays DHCP snooping packet messages.</p> <p><code>dynamic-ip-lockdown</code>—Sends dynamic IP lockdown debug messages to the debug destination. <code>port-access</code>—Sends port-access debug messages to the debug destination. <code>radius-server</code>—Sends RADIUS debug messages to the debug destination. <code>ssh</code>—Sends SSH debug messages at the specified level to the debug destination. The levels are fatal, error, info, verbose, debug, debug2, and debug3. <code>tacacs-server</code>—Sends TACACS debug messages to the debug destination. <code>user-profile-mib</code>—Sends user profile MIB debug messages to the debug destination.</p>
	<code>services <slot-id-range></code>	Displays debug messages on the services module. Enter an alphabetic module ID or range of module IDs for the <code><slot-id-range></code> parameter.
	<code>snmp <pdu></code>	Displays the SNMP debug messages. <code>pdu</code> —Displays SNMP pdu debug messages.

Debug destinations

Use the `debug destination` command to enable (and disable) syslog messaging on a syslog server or to a CLI session for specified types of debug and Event Log messages.

Syntax:

```
no debug destination {<logging | session | buffer>}
```

logging	<p>Enables syslog logging to configured syslog servers so that the debug message types specified by the <code>debug <debug-type></code> command (see Debug messages on page 392) are sent. (Default: Logging disabled) To configure a syslog server IP address, see Configuring a syslog server on page 396.</p> <hr/> <p> NOTE: Debug messages from the switches covered in this guide have a debug severity level. Because the default configuration of some syslog servers ignores syslog messages with the debug severity level, ensure that the syslog servers you want to use to receive debug messages are configured to accept the debug level. For more information, see Operating notes for debug and Syslog on page 401.</p> <hr/>
session	<p>Enables transmission of event notification messages to the CLI session that most recently executed this command. The session can be on any one terminal emulation device with serial, Telnet, or SSH access to the CLI at the Manager level prompt (<code>switch#_</code>). If more than one terminal device has a console session with the CLI, you can redirect the destination from the current device to another device. Do so by executing <code>debug destination session</code> in the CLI on the terminal device on which you now want to display event messages. Event message types received on the selected CLI session are configured with the <code>debug <debug-type></code> command.</p>
buffer	<p>Enables syslog logging to send the debug message types specified by the <code>debug <debug-type></code> command to a buffer in switch memory. To view the debug messages stored in the switch buffer, enter the <code>show debug buffer</code> command.</p>

Logging command

At the global configuration level, the `logging` command allows you to enable debug logging on specified syslog servers and select a subset of Event Log messages to send for debugging purposes according to:

- Severity level
- System module

By specifying both a severity level and system module, you can use both configured settings to filter the Event Log messages you want to use to troubleshoot switch or network error conditions.



CAUTION:

After you configure a syslog server and a severity level and/or system module to filter the Event Log messages that are sent, if you save these settings to the startup configuration file by entering the `write memory` command, these debug and logging settings are automatically re-activated after a switch reboot or power recycle. The debug settings and destinations configured in your previous troubleshooting session will then be applied to the current session, which may not be desirable.

After a reboot, messages remain in the Event Log and are not deleted. However, after a power recycle, all Event Log messages are deleted.

If you configure a severity level, system module, or both to temporarily filter Event Log messages, be sure to reset the values to their default settings by entering the `no` form of the following commands to ensure that Event Log messages of all severity levels and from all system modules are sent to configured syslog servers:

```
switch(config)# no logging severity <debug | major | error | warning | info>
switch(config)# no logging system-module <system-module>
```

Configuring a syslog server

Syslog is a client-server logging tool that allows a client switch to send event notification messages to a networked device operating with syslog server software. Messages sent to a syslog server can be stored to a file for later debugging analysis.

To use the syslog feature, you must install and configure a syslog server application on a networked host accessible to the switch. For instructions, see the documentation for the syslog server application.

To configure a syslog service, use the `logging <syslog-ip-addr>` command as shown below.

When you configure a syslog server, Event Log messages are automatically enabled to be sent to the server. To reconfigure this setting, use the following commands:

- `debug`
Specifies additional debug message types (see [Debug messages](#) on page 392).
- `logging`
Configures the system module or severity level used to filter the Event Log messages sent to configured syslog servers. (See [Configuring the severity level for Event Log messages sent to a syslog server](#) on page 400 and [Configuring the system module used to select the Event Log messages sent to a syslog server](#) on page 400.)

To display the currently configured syslog servers as well as the types of debug messages and the severity-level and system-module filters used to specify the Event Log messages that are sent, enter the `show debug` command (See [Debug/syslog configuration commands](#) on page 385).

Syntax:

```
no logging <syslog-ip-addr>
```

Enables or disables syslog messaging to the specified IP address. You can configure up to six addresses. If you configure an address when none are already configured, this command enables destination logging (syslog) and the Event debug type. Therefore, at a minimum, the switch begins sending Event Log messages to configured syslog servers. The ACL, IP-OSPF, and/or IP-RIP message types are also sent to the syslog servers if they are currently enabled as debug types. (See [Debug messages](#) on page 392.)

<code>no logging</code>	Removes all currently configured syslog logging destinations from the running configuration. Using this form of the command to delete the only remaining syslog server address disables debug destination logging on the switch, but the default Event debug type does not change.
<code>no logging <syslog-ip-address></code>	Removes only the specified syslog logging destination from the running configuration. Removing all configured syslog destinations with the <code>no logging</code> command (or a specified syslog server destination with the <code>no logging <syslog-ip-address></code> command) does not delete the syslog server IP addresses stored in the startup configuration.

Deleting syslog addresses in the startup configuration

Enter a `no logging` command followed by the `write memory` command.

Verifying the deletion of a syslog server address

Display the startup configuration by entering the `show config` command.

Blocking the messages sent to configured syslog servers from the currently configured debug message type

Enter the `no debug <debug-type>` command. (See [Debug messages](#) on page 392.)

Disabling syslog logging on the switch without deleting configured server addresses

Enter the `no debug destination logging` command. Note that, unlike the case in which no syslog servers are configured, if one or more syslog servers are already configured and syslog messaging is disabled, configuring a new server address does not re-enable syslog messaging. To re-enable syslog messaging, you must enter the `debug destination logging` command.

Sending logging messages using TCP

Syntax:

```
no logging <ip-addr> [udp 1024-49151 | tcp 1024-49151]
```

Allows the configuration of the UDP or TCP transport protocol for the transmission of logging messages to a syslog server.

Specifying a destination port with UDP or TCP is optional.

Default ports: UDP port is 514

TCP port is 1470

Default Transport Protocol: UDP

Because TCP is a connection-oriented protocol, a connection must be present before the logging information is sent. This helps ensure that the logging message will reach the syslog server. Each configured syslog server needs its own connection. You can configure the destination port that is used for the transmission of the logging messages.

Configuring TCP for logging message transmission using the default port

```
switch(config)# logging 192.123.4.5 tcp
```

(Default TCP port 1470 is used.)

Configuring TCP for logging message transmission using a specified port

```
switch(config)# logging 192.123.4.5 9514
```

(TCP port 9514 is used.)

Configuring UDP for logging message transmission using the default port

```
switch(config)# logging 192.123.4.5 udp
```

(Default UDP port 514 is used.)

Configuring UDP for logging message transmission using a specified port

```
switch(config)# logging 192.123.4.5 9512
```

(UDP port 9512 is used.)

Syntax:

```
no logging facility <facility-name>
```

The logging facility specifies the destination subsystem used in a configured syslog server. (All configured syslog servers must use the same subsystem.) Hewlett Packard Enterprise recommends the default (user) subsystem unless your application specifically requires another subsystem. Options include:

user	(default) Random user-level messages
kern	Kernel messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslog
lpr	Line-printer subsystem
news	Netnews subsystem
uucp	uucp subsystem
cron	cron/at subsystem
sys9	cron/at subsystem

Table Continued

sys10 - sys14	Reserved for system use
local10 - local17	Reserved for system use

Use the `no` form of the command to remove the configured facility and reconfigure the default (user) value.

Adding a description for a Syslog server

You can associate a user-friendly description with each of the IP addresses (IPv4 only) configured for syslog using the CLI or SNMP.



NOTE:

The Hewlett Packard Enterprise MIB `hpicfSyslog.mib` allows the configuration and monitoring of syslog for SNMP (RFC 3164 supported).



CAUTION:

Entering the `no logging` command removes ALL the syslog server addresses without a verification prompt.

The CLI command is:

Syntax:

```
logging <ip-addr> [control-descr ZZZZTRISHZZZZ <text_string>]
no logging <ip-addr> [control-descr]
```

An optional user-friendly description that can be associated with a server IP address. If no description is entered, this is blank. If `<text_string>` contains white space, use quotes around the string. IPv4 addresses only.

Use the `no` form of the command to remove the description. Limit: 255 characters



NOTE:

To remove the description using SNMP, set the description to an empty string.

The logging command with a control description

```
switch(config)# logging 10.10.10.2 control-descr syslog_one
```

Adding a priority description

This description can be added with the CLI or SNMP. The CLI command is:

Syntax:

```
logging priority-descr <text_string>
no logging priority-descr
```

Provides a user-friendly description for the combined filter values of `severity` and `system` module. If no description is entered, this is blank.

If `text_string` contains white space, use quotes around the string.

Use the `no` form of the command to remove the description.

Limit: 255 characters

The logging command with a priority description

```
switch(config)# logging priority-descr severe-pri
```



NOTE:

A notification is sent to the SNMP agent if there are any changes to the syslog parameters, either through the CLI or with SNMP.

Configuring the severity level for Event Log messages sent to a syslog server

Event Log messages are entered with one of the following severity levels (from highest to lowest):

Major	A fatal error condition has occurred on the switch.
Error	An error condition has occurred on the switch.
Warning	A switch service has behaved unexpectedly.
Information	Information on a normal switch event.
Debug	Reserved for switch internal diagnostic information.

Using the `logging severity` command, you can select a set of Event Log messages according to their severity level and send them to a syslog server. Messages of the selected and higher severity will be sent. To configure a syslog server, see [Configuring a syslog server](#) on page 396.

Syntax:

```
no logging severity {< major | error | warning | info | debug >}
```

Configures the switch to send all Event Log messages with a severity level equal to or higher than the specified value to all configured Syslog servers.

Default: `debug` (Reports messages of all severity levels.)

Use the `no` form of the command to remove the configured severity level and reconfigure the default value, which sends Event Log messages of all severity levels to syslog servers.



NOTE: The severity setting does not affect event notification messages that the switch normally sends to the Event Log. All messages remain recorded in the Event Log.

Configuring the system module used to select the Event Log messages sent to a syslog server

Event Log messages contain the name of the system module that reported the event. Using the `logging system-module` command, you can select a set of Event Log messages according to the originating system module and send them to a syslog server.

Syntax:

```
no logging system-module <system-module>
```


Configures the switch to send all Event Log messages being logged from the specified system module to configured syslog servers. (To configure a syslog server, see **Configuring a syslog server**.)

See **Event Log system modules** for the correct value to enter for each system module.

Default: `all-pass` (Reports all Event Log messages.)

Use the `no` form of the command to remove the configured system module value and reconfigure the default value, which sends Event Log messages from all system modules to syslog servers.

You can select messages from only one system module to be sent to a syslog server; you cannot configure messages from multiple system modules to be sent. If you re-enter the command with a different system module name, the currently configured value is replaced with the new one.



NOTE: This setting has no effect on event notification messages that the switch normally sends to the Event Log.

Enabling local command logging

Use this command to enable local command logging. This satisfies the NDcPP certification requirement that:

- All administrative actions (commands) are logged locally.
- Local command log storage can be enabled and disabled.
- The identity of the user causing an event is logged.
- When the command log is exhausted by 80% and wraparound occurs, the event is logged and a trap is generated.
- Log messages have a maximum of 240 characters (the RMON event maximum string length) and are stored in the command log buffer.
- Log messages greater than the maximum length are truncated and are not stored in the command log buffer.

Syntax:

```
no logging command
```

Operating notes for debug and Syslog

- Rebooting the switch or pressing the `Reset` button resets the debug configuration.

Debug option	Effect of a reboot or reset
logging (debug destination)	If syslog server IP addresses are stored in the startup-config file, they are saved across a reboot and the logging destination option remains enabled. Otherwise, the logging destination is disabled.
session (debug destination)	Disabled.
ACL (debug type)	Disabled.
All (debug type)	Disabled.

Table Continued

Debug option	Effect of a reboot or reset
event (debug type)	<p>If a syslog server IP address is configured in the startup-config file, the sending of Event Log messages is reset to <code>enabled</code>, regardless of the last active setting.</p> <p>If no syslog server is configured, the sending of Event Log messages is <code>disabled</code>.</p>
IP (debug type)	Disabled.

- Debug commands do not affect normal message output to the Event Log.

Using the `debug event` command, you can specify that Event Log messages are sent to the debug destinations you configure (CLI session, syslog servers, or both) in addition to the Event Log.

- Ensure that your syslog servers accept debug messages.

All syslog messages resulting from a debug operation have a "debug" severity level. If you configure the switch to send debug messages to a syslog server, ensure that the server's syslog application is configured to accept the "debug" severity level. (The default configuration for some syslog applications ignores the "debug" severity level.)

- Duplicate IP addresses are not stored in the list of syslog servers.
- If the default severity value is in effect, all messages that have severities greater than the default value are passed to syslog. For example, if the default severity is "debug," all messages that have severities greater than debug are passed to syslog.
- There is a limit of six syslog servers. All syslog servers are sent the same messages using the same filter parameters. An error is generated for an attempt to add more than six syslog servers.

Diagnostic tools

Port auto-negotiation

When a link LED does not light (indicating loss of link between two devices), the most common reason is a failure of port auto-negotiation between the connecting ports. If a link LED fails to light when you connect the switch to a port on another device, do the following:

Procedure

1. Ensure that the switch port and the port on the attached end-node are both set to `Auto` mode.
2. If the attached end-node does not have an `Auto` mode setting, you must manually configure the switch port to the same setting as the end-node port.

Ping and link tests

The ping test and the link test are point-to-point tests between your switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the switch is communicating properly with another device.

**NOTE:**

To respond to a ping test or a link test, the device you are trying to reach must be IEEE 802.3-compliant.

Ping test

A test of the path between the switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests). To use the `ping` (or `tracert`) command with host names or fully qualified domain names, see **DNS resolver** on page 420.

Link test

A test of the connection between the switch and a designated network device on the same LAN (or VLAN, if configured). During the link test, IEEE 802.2 test packets are sent to the designated network device in the same VLAN or broadcast domain. The remote device must be able to respond with an 802.2 Test Response Packet.

Executing ping or link tests (WebAgent)

To start a ping or link test in the WebAgent:

1. In the navigation pane, click **Troubleshooting**.
2. Click **Ping/Link Test**.
3. Click **Start**.
4. To halt a link or ping test before it concludes, click **Stop**.

For an Example: of the text screens, see **Figure 50: Ping test and link test screen on the WebAgent** on page 403.

Figure 50: *Ping test and link test screen on the WebAgent*

The screenshot displays two configuration windows from the WebAgent. The top window is titled "Ping Test" and contains a "Ping Status" section with three input fields: "Destination IP Address" (empty), "Number of Packets" (set to 5), and "Time Out in Seconds" (set to 1). The bottom window is titled "Link Test" and contains a "Link Status" section with four input fields: "Destination MAC Address" (empty), "VLAN" (a dropdown menu), "Number of Packets" (set to 5), and "Time Out in Seconds" (set to 1). Both windows have "Start", "Stop", and help icons in the top right corner.

Destination IP Address is the network address of the target, or destination, device to which you want to test a connection with the switch. An IP address is in the X.X.X.X format where X is a decimal number between 0 and 255.

Number of Packets to Send is the number of times you want the switch to attempt to test a connection.

Timeout in Seconds is the number of seconds to allow per attempt to test a connection before determining that the current attempt has failed.

Testing the path between the switch and another device on an IP network

The ping test uses ICMP echo requests and ICMP echo replies to determine if another device is alive. It also measures the amount of time it takes to receive a reply from the specified destination. The `ping` command has several extended commands that allow advanced checking of destination availability.

Syntax:

```
ping {<ip-address | hostname>} [repetitions <1-10000>] [timeout <1-60>] [source <
{ip-address | <vlan-id> | loopback <0-7>>}] [data-size <0-65471>] [data-fill
<0-1024>] [ip-option {<record-route | loose-source-route | strict-source-route |
include-timestamp | include-timestamp-and-address | include timestamp-from> >}]
[<tos <0-255>]
```

```
ping6 {<ipv6-address | hostname>} [repetitions <1-10000>] [timeout <1-60>] [source
< {ip-address | vlan-id | loopback <0-7>>}] [data-size <0-65471>] [data-fill
<0-1024>]
```

Sends ICMP echo requests to determine if another device is alive.

<code>{< ip-address hostname >}</code>	Target IP address or hostname of the destination node being pinged
<code>repetitions <1-10000></code>	Number of ping packets sent to the destination address. Default: 1
<code>timeout <1-60></code>	Timeout interval in seconds; the ECHO REPLY must be received before this time interval expires for the ping to be successful. Default: 5
<code>source {< ip-addr vid loopback <0-7>>}</code>	Source IP address, VLAN ID, or loopback address used for the ping. The source IP address must be owned by the router. If a VLAN is specified, the IP address associated with the specified VLAN is used.
<code>data-size <0-65471></code>	Size of packet sent. Default: 0 (zero)
<code>data-fill <0-1024></code>	The data pattern in the packet. Default: Zero length string

Table Continued

ip-option	<p>Specify an IP option, such as loose or strict source routing, or an include-timestamp option: include-timestamp: Adds the timestamp option to the IP header. The timestamp displays the amount of travel time to and from a host.</p> <p>Default: 9 include-timestamp-and-address: Records the intermediate router's timestamp and IP address.</p> <p>Default: 4 include-timestamp-from: Records the timestamp of the specified router addresses. loose-source-route <IP-addr> : The loose-source-route option prompts for the IP address of each source IP on the path. It allows you to specify the IP addresses that you want the ping packet to go through; the packet may go through other IP addresses as well. record-route <1-9> : Displays the IP addresses of the interfaces that the ping packet goes through on its way to the destination and on the way back.</p> <p>When specified without loose or strict recording, the source route is not recorded. The source route is automatically recorded when loose or strict source routing is enabled.</p> <p>Default: 9 strict-source-route <IP-addr> : Restricts the ping packet to only those IP addresses that have been specified and no other addresses.</p>
tos <0-255>	<p>Specifies the type of service to be entered in the header packet.</p> <p>Default: 0 (zero)</p>

Ping tests

```
switch# ping 10.10.10.10
10.10.10.10 is alive, time = 15 ms

switch# ping 10.10.10.10 repetitions 3
10.10.10.10 is alive, iteration 1, time = 15 ms
10.10.10.10 is alive, iteration 1, time = 15 ms
10.10.10.10 is alive, iteration 1, time = 15 ms

switch# ping 10.10.10.10 timeout 2
10.10.10.10 is alive, time = 10 ms

switch# ping 10.11.12.13
The destination address is unreachable.
```

Halting a ping test

To halt a ping test before it concludes, press **[Ctrl] [C]**.



NOTE:

To use the `ping` (or `tracert`) command with host names or fully qualified domain names, see **DNS resolver** on page 420.

Issuing single or multiple link tests

Single or multiple link tests can have varying repetitions and timeout periods. The defaults are:

- Repetitions: 1 (1 to 999)
- Timeout: 5 seconds (1 to 256 seconds)

Syntax:

```
link <mac-address> [repetitions <1-999>] [timeout <1-256>] [vlan < vlan-id >]
```

Example:

Figure 51: Link tests

Basic Link Test	Switch# link 0030c1-7fcc40 Link-test passed.
Link Test with Repetitions	Switch# link 0030c1-7fcc40 repetitions 3 802.2 TEST packets sent: 3, responses received: 3
Link Test with Repetitions and Timeout	Switch# link 0030c1-7fcc40 repetitions 3 timeout 1 802.2 TEST packets sent: 3, responses received: 3
Link Test Over a Specific VLAN	Switch# link 0030c1-7fcc40 repetitions 3 timeout 1 vlan 1 802.2 TEST packets sent: 3, responses received: 3
Link Test Over a Specific VLAN; Test Fail	Switch# link 0030c1-7fcc40 repetitions 3 timeout 1 vlan 222 802.2 TEST packets sent: 3, responses received: 0

Tracing the route from the switch to a host address

The `traceroute` command enables you to trace the route from the switch to a host address.

This command outputs information for each (router) hop between the switch and the destination address. Note that every time you execute `traceroute`, it uses the same default settings unless you specify otherwise for that instance of the command.

Syntax:

```
traceroute {< ip-address | hostname >} [maxttl <1-255>] [minttl <1-255>] [probes <1-5>] [source {<ip-address | source-vlan <vid> | loopback <0-7>}] [dstport <1-34000>] [srcport <1-34000>] [ip-option {<record-route | loose-source-route | strict-source-route | include-timestamp | include-timestamp-and-address | include-timestamp-from>}] [< timeout 1-120 >]
```

Lists the IP address or hostname of each hop in the route, plus the time in microseconds for the `traceroute` packet reply to the switch for each hop.

<code>{< ip-address hostname >}</code>	The IP address or hostname of the device to which to send the traceroute.
[minttl < 1-255 >]	<p>For the current instance of <code>traceroute</code>, changes the minimum number of hops allowed for each probe packet sent along the route.</p> <ul style="list-style-type: none"> • If <code>minttl</code> is greater than the actual number of hops, the output includes only the hops at and above the <code>minttl</code> threshold. (The hops below the threshold are not listed.) • If <code>minttl</code> matches the actual number of hops, only that hop is shown in the output. • If <code>minttl</code> is less than the actual number of hops, all hops are listed. <p>For any instance of <code>traceroute</code>, if you want a <code>minttl</code> value other than the default, you must specify that value.(Default: 1)</p>
[maxttl < 1-255 >]	<p>For the current instance of <code>traceroute</code>, changes the maximum number of hops allowed for each probe packet sent along the route.If the destination address is further from the switch than <code>maxttl</code> allows, <code>traceroute</code> lists the IP addresses for all hops it detects up to the <code>maxttl</code> limit.For any instance of <code>traceroute</code>, if you want a <code>maxttl</code> value other than the default, you must specify that value.(Default: 30)</p>
[probes < 1-5 >]	<p>For the current instance of <code>traceroute</code>, changes the number of queries the switch sends for each hop in the route.For any instance of <code>traceroute</code>, if you want a <code>probes</code> value other than the default, you must specify that value.(Default: 3)</p>
[source {< ip- addr vid loopback <0-7> >}]	The source IPv4 address, VLAN ID, or Loopback address.
[dstport < 1-34000 >]	Destination port.

Table Continued

[srcport < 1-34000 >]	Source port.
[ip-option]	Specify an IP option, such as loose or strict source routing, or an include-timestamp option: [include-timestamp]: Adds the timestamp option to the IP header. The timestamp displays the amount of travel time to and from a host. Default: 9 [include-timestamp-and-address]: Records the intermediate router's timestamp and IP address. Default: 4 [loose-source-route <IP-addr>]: Prompts for the IP address of each source IP on the path. It allows you to specify the IP addresses that you want the ping packet to go through; the packet may go through other IP addresses as well. Default: 9 [record-route <1-9>]: Displays the IP addresses of the interfaces that the ping packet goes through on its way to the destination and on the way back. When specified without loose or strict recording, the source route is not recorded. The source route is automatically recorded when loose or strict source routing is enabled. Default: 9 [strict-source-route <IP-addr>]: Restricts the ping packet to only those IP addresses that have been specified and no other addresses. Default: 9 [timeout <1-120>]: For the current instance of <code>traceroute</code> , changes the timeout period the switch waits for each probe of a hop in the route. For any instance of <code>traceroute</code> , if you want a timeout value other than the default, you must specify that value. (Default: 5 seconds)



NOTE: For information about `traceroute6`, see the IPv6 configuration guide for your switch.

Halting an ongoing traceroute search

Press the **[Ctrl] [C]** keys.

A low `maxttl` causes traceroute to halt before reaching the destination address

Executing `traceroute` with its default values for a destination IP address that is four hops away produces a result similar to this:

Figure 52: A completed traceroute enquiry

```
Switch# traceroute 125.25.24.35
traceroute to 125.25.24.35 ,
  1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.255.120.2      0 ms    0 ms    0 ms
 2 10.71.217.2      7 ms    3 ms    0 ms
 3 10.243.170.1     0 ms    1 ms    0 ms
 4 125.25.24.35    3 ms    3 ms    0 ms
```

Intermediate router hops with the time taken for the switch to receive an acknowledgement of each probe reaching each router.

Destination IP Address

Continuing from the previous Example: (**Figure 52: A completed traceroute enquiry** on page 408), executing `traceroute` with an insufficient `maxttl` for the actual hop count produces an output similar to this:

Figure 53: *Incomplete traceroute because of low maxttl setting*

```

Traceroute does not reach destination IP address because of low maxttl setting.
Switch# traceroute 125.25.24.35 (maxttl 3)
traceroute to 125.25.24.35 ,
          1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.255.120.2          0 ms          0 ms          0 ms
 2 10.71.217.2           0 ms          0 ms          0 ms
 3 10.243.170.1         0 ms *         0 ms

```

The asterisk indicates there was a timeout on the second probe to the third hop.

If a network condition prevents traceroute from reaching the destination

Common reasons for `traceroute` failing to reach a destination include:

- Timeouts (indicated by one asterisk per probe, per hop)
- Unreachable hosts
- Unreachable networks
- Interference from firewalls
- Hosts configured to avoid responding

Executing `traceroute` where the route becomes blocked or otherwise fails results in an output marked by timeouts for all probes beyond the last detected hop. For example, with a maximum hop count of 7 (`maxttl = 7`), where the route becomes blocked or otherwise fails, the output appears similar to this:

Figure 54: *Traceroute failing to reach the destination address*

```

At hop 3, the first and third probes timed out but the second probe reached the router.
All further probes within the maxttl timed-out without finding a router or the destination IP address.
Switch# traceroute 125.25.24.35 maxttl 7
traceroute to 107.64.197.100 ,
          1 hop min, 7 hops max, 5 sec. timeout, 3 probes
 1 10.255.120.2          0 ms          0 ms          0 ms
 2 10.71.217.2           0 ms          0 ms          0 ms
 3 * 10.243.170.1         0 ms *
 4 * * * *
 5 * * * *
 6 * * * *
 7 * * * *

```

An asterisk indicates a timeout without finding the next hop.

Viewing switch configuration and operation

In some troubleshooting scenarios, you may need to view the switch configuration to diagnose a problem. The complete switch configuration is contained in a file that you can browse from the CLI using the commands described in this section.

Viewing the startup or running configuration file

Syntax:

```
write terminal
```

Displays the running configuration.

<code>show config</code>	Displays the startup configuration.
<code>show running-config</code>	Displays the running-config file.

For more information and examples of how to use these commands, see “Switch Memory and Configuration” in the basic operation guide.

Viewing the configuration file (WebAgent)

To display the running configuration using the WebAgent:

1. In the navigation pane, click **Troubleshooting**.
2. Click **Configuration Report**.
3. Use the right-side scroll bar to scroll through the configuration listing.

Viewing a summary of switch operational data

Syntax:

```
show tech
```

By default, the `show tech` command displays a single output of switch operating and running-configuration data from several internal switch sources, including:

- Image stamp (software version data)
- Running configuration
- Event Log listing
- Boot history
- Port settings
- Status and counters — port status
- IP routes
- Status and counters — VLAN information
- GVRP support
- Load balancing (trunk and LACP)

The show tech command on page 410 shows sample output from the `show tech` command.

The show tech command

```
switch# show tech
show system
Status and Counters - General System Information
System Name       : Switch
System Contact   :
System Location   :
```

```
MAC Age Time (sec) : 300

Time Zone          : 0
Daylight Time Rule : None

Software revision  : XX.14.xx      Base MAC Addr  : 001871-c42f00
ROM Version        : XX.12.12     Serial Number  : SG641SU00L

Up Time           : 23 hours      Memory - Total :
CPU Util (%)      : 10             Free          :

IP Mgmt - Pkts Rx : 759           Packet - Total : 6750
          Pkts Tx : 2             Buffers Free  : 5086
                                   Lowest           : 4961
                                   Missed           : 0

show flash
Image      Size(Bytes)  Date  Version
-----
-----
```

To specify the data displayed by the `show tech` command, use the `copy show tech` command.

Saving show tech command output to a text file

When you enter the `show tech` command, a summary of switch operational data is sent to your terminal emulator. You can use your terminal emulator's text capture features to save the `show tech` data to a text file for viewing, printing, or sending to an associate to diagnose a problem.

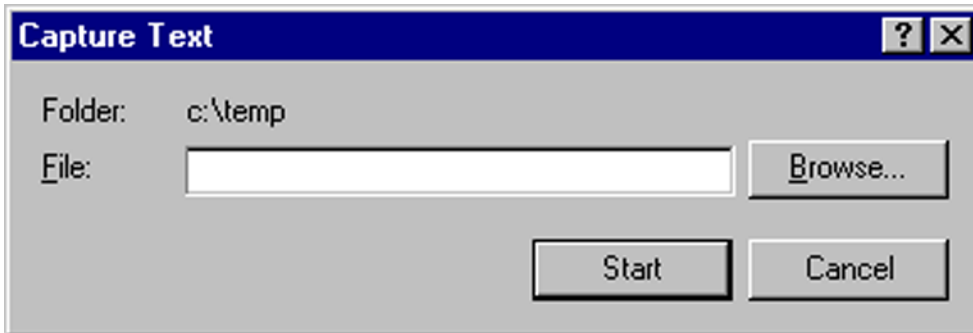
For example, if your terminal emulator is the Hyperterminal application available with Microsoft® Windows® software, you can copy the `show tech` output to a file and then use either Microsoft Word or Notepad to display the data. (In this case, Microsoft Word provides the data in an easier-to-read format.)

The following example uses the Microsoft Windows terminal emulator. If you are using a different terminal emulator application, see the documentation provided with the application.

Procedure

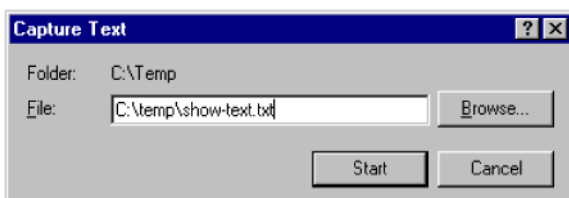
1. In Hyperterminal, click on **Transfer|Capture Text...**

Figure 55: Capture text window of the Hyperterminal application



2. In the **File** field, enter the path and file name in which you want to store the `show tech` output.

Figure 56: Entering a path and filename for saving `show tech` output



3. Click **[Start]** to create and open the text file.
4. From the global configuration context, enter the `show tech` command:

```
switch# show tech
```

The `show tech` command output is copied into the text file and displayed on the terminal emulator screen. When the command output stops and displays `-- MORE --`, press the Space bar to display and copy more information. The CLI prompt appears when the command output finishes.

5. Click on **Transfer|Capture Text|Stop** in HyperTerminal to stop copying data and save the text file.
If you do not stop HyperTerminal from copying command output into the text file, additional unwanted data can be copied from the HyperTerminal screen.
6. To access the file, open it in Microsoft Word, Notepad, or a similar text editor.

Customizing `show tech` command output

Use the `copy show tech` command to customize the detailed switch information displayed with the `show tech` command to suit your troubleshooting needs.

To customize the information displayed with the `show tech` command:

Procedure

1. Determine the information that you want to gather to troubleshoot a problem in switch operation.
2. Enter the `copy show tech` command to specify the data files that contain the information you want to view.

Syntax:

```
copy <source> show-tech
```

Specifies the operational and configuration data from one or more source files to be displayed by the `show tech` command. Enter the command once for each data file that you want to include in the display.

Default: Displays data from all source files, where `<source>` can be any one of the following values:

<pre>command-output "<command>"</pre>	<p>Includes the output of a specified command in <code>show-tech</code> command output.</p> <p>Enter the command name between double-quotation marks, For example, <code>copy "show system" show-tech</code>.</p>
<pre>crash-data [slot-id master]</pre>	<p>Includes the crash data from all management and interface modules in <code>show tech</code> command output.</p> <p>To limit the amount of crash data displayed, specify an installed module or management modules, where:</p> <ul style="list-style-type: none"> • <code>slot-id</code>: Includes the crash data from an installed module. Valid slot IDs are the letters <code>a</code> through <code>h</code>. • <code>master</code>: Includes the crash data from both management modules.
<pre>crash-log [slot-id master]</pre>	<p>Includes the crash logs from all management and interface modules in <code>show tech</code> command output.</p> <p>To limit the amount of crash-log data displayed, specify an installed module or management modules, where:</p> <p><code>slot-id</code>: Includes the crash log from an installed module. Valid slot IDs are the letters <code>a</code> through <code>h</code>.</p> <p><code>master</code>: Includes the crash log from both management modules.</p>
<pre>event-log</pre>	<p>Copies the contents of the Event Log to <code>show tech</code> command output.</p>
<pre>running-config</pre>	<p>Includes the contents of the running configuration file in <code>show tech</code> command output</p>
<pre>startup-config</pre>	<p>Includes the contents of the startup configuration file in <code>show tech</code> command output.</p>

Table Continued

<pre>tftp config {<startup-config running-config} <ip-addr> <remote- file> {<pc unix>}</pre>	<p>Downloads the contents of a configuration file from a remote host to show tech command output, where:</p> <p><i><ip-addr></i> : Specifies the IP address of the remote host device.</p> <p><i><remote-file></i>: Specifies the pathname on the remote host for the configuration file whose contents you want to include in the command output.</p> <p>pc unix: Specifies whether the remote host is a DOS-based PC or UNIX workstation.</p>
<pre>xmodem config {<startup-config config < filename > command-file < acl-filename.txt >} {<pc unix>}</pre>	<p>Copies the contents of a configuration file or ACL command file from a serially connected PC or UNIX workstation to show tech command output, where:</p> <p>startup-config: Specifies the name of the startup configuration file on the connected device.</p> <p>config <filename> : Specifies the pathname of a configuration file on the connected device.</p> <p>command-file <acl-filename.txt> : Specifies the pathname of an ACL command file on the connected device.</p> <p>pc unix: Specifies whether the connected device is a DOS-based PC or UNIX workstation.</p>

Viewing more information on switch operation

Use the following commands to display additional information on switch operation for troubleshooting purposes.

Syntax:

```
show boot-history
```

Displays the crash information saved for each management module on the switch.

```
show history
```

Displays the current command history. This command output is used for reference or when you want to repeat a command (See [Displaying the information you need to diagnose problems](#) on page 417).

```
show system-information
```

Displays globally configured parameters and information on switch operation.

```
show version
```

Displays the software version currently running on the switch and the flash image from which the switch booted (primary or secondary). For more information, see "Displaying Management Information" in the "Redundancy (Switch 8212zl)".

```
show interfaces
```

Displays information on the activity on all switch ports (see "Viewing Port Status and Configuring Port Parameters" in the "Port Status and Configuration").

```
show interfaces-display
```

Displays the same information as the `show interfaces` command and dynamically updates the output every three seconds. Press **Ctrl + C** to stop the dynamic updates of system information. Use the Arrow keys to view information that is off the screen.

Searching for text using pattern matching with show command

Selected portions of the output are displayed, depending on the parameters chosen.

Syntax:

```
show {< command option > | < include | exclude | begin >} <regular expression>
```

Uses matching pattern searches to display selected portions of the output from a `show` command. There is no limit to the number of characters that can be matched. Only regular expressions are permitted; symbols such as the asterisk cannot be substituted to perform more general matching.

<code>include</code>	Only the lines that contain the matching pattern are displayed in the output.
<code>exclude</code>	Only the lines that contain the matching pattern are not displayed in the output.
<code>begin</code>	The display of the output begins with the line that contains the matching pattern.



NOTE: Pattern matching is case-sensitive.

Following are examples of what portions of the running config file display depending on the option chosen.

Pattern matching with include option

```
switch(config)# show run | include ipv6 1
  ipv6 enable
  ipv6 enable
ipv6 access-list "EH-01"
switch(config)#
```

¹Displays only lines that contain "ipv6".

Pattern matching with exclude option

```
switch(config)# show run | exclude ipv6 1

Running configuration:

; J9299A Configuration Editor; Created on release #WB.15.XX

hostname "Switch"
snmp-server community "notpublic" Unrestricted
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24,B1-B20
```

```

ip address dhcp-bootp
no untagged B21-B24
exit
vlan 20
name "VLAN20"
untagged B21-B24
no ip address
exit
policy qos "michael"
exit
sequence 10 deny tcp 2001:db8:255::/48 2001:db8:125::/48
exit
no autorun
password manager

```

¹Displays all lines that do not contain "ipv6".

Pattern matching with begin option

```

switch(config)# show run | begin ipv6 1
ip address dhcp-bootp
no untagged 21-24
exit
vlan 20
name "VLAN20"
untagged 21-24
ip address dhcp-bootp
no ip address
exit
policy qos "michael"
exit
ip address dhcp-bootp
sequence 10 deny tcp 2001:db8:255::/48 2001:db8:125::/48
exit
no autorun
password manager

```

¹Displays the running config beginning at the first line that contains "ipv6".

The following is an Example: of the `show arp` command output, and then the output displayed when the `include` option has the IP address of 15.255.128.1 as the regular expression.

The show arp command and pattern matching with the include option

```

switch(config)# show arp

IP ARP table

  IP Address      MAC Address      Type      Port
  -----
  15.255.128.1    00000c-07ac00   dynamic   B1
  15.255.131.19   00a0c9-b1503d   dynamic
  15.255.133.150  000bcd-3cbeec   dynamic   B1

switch(config)# show arp | include 15.255.128.1
15.255.128.1    00000c-07ac00   dynamic   B1

```


Displaying the information you need to diagnose problems

Use the following commands in a troubleshooting session to more accurately display the information you need to diagnose a problem.

Syntax:

```
alias
```

Creates a shortcut alias name for commonly used commands and command options.

Syntax:

```
kill
```

Terminates a currently running, remote troubleshooting session. Use the `show ip ssh` command to list the current management sessions.

Syntax:

```
no page
```

Toggles the paging mode for `show` commands between continuous listing and per-page listing.

Syntax:

```
repeat
```

Repeatedly executes one or more commands so that you can see the results of multiple commands displayed over a period of time. To halt the command execution, press any key on the keyboard.

Syntax:

```
setup
```

Displays the Switch Setup screen from the menu interface.

Restoring the factory-default configuration

As part of your troubleshooting process, it may become necessary to return the switch configuration to the factory default settings. This process:

- Momentarily interrupts the switch operation
- Clears any passwords
- Clears the console Event Log
- Resets the network counters to zero
- Performs a complete self test
- Reboots the switch into its factory default configuration, including deleting an IP address

There are two methods for resetting to the factory-default configuration:

- CLI
- `Clear/Reset` button combination



NOTE: Hewlett Packard Enterprise recommends that you save your configuration to a TFTP server before resetting the switch to its factory-default configuration. You can also save your configuration via Xmodem to a directly connected PC.

Resetting to the factory-default configuration

Using the CLI

This command operates at any level **except** the Operator level.

Syntax:

```
erase startup-configuration
```

Deletes the startup-config file in flash so that the switch will reboot with its factory-default configuration.



NOTE:

The `erase startup-config` command does not clear passwords unless `include-credentials` has been set, at which time this command does erase username/password information and any other credentials stored in the config file. For more information, see the section on "Saving Security Credentials in a Config File" in the access security guide for your switch.

Using Clear/Reset

Procedure

1. Using pointed objects, simultaneously press both the `Reset` and `Clear` buttons on the front of the switch.
2. Continue to press the `Clear` button while releasing the `Reset` button.
3. When the Self Test LED begins to flash, release the `Clear` button.

The switch then completes its self test and begins operating with the configuration restored to the factory default settings.

Restoring a flash image

The switch can lose its operating system if either the primary or secondary flash image location is empty or contains a corrupted OS file and an operator uses the `erase flash` command to erase a good OS image file from the opposite flash location.

Recovering from an empty or corrupted flash state

Use the switch's console serial port to connect to a workstation or laptop computer that has the following:

- A terminal emulator program with Xmodem capability, such as the HyperTerminal program included in Windows PC software.
- A copy of a good OS image file for the switch



NOTE: The following procedure requires the use of Xmodem and copies an OS image into primary flash only.

This procedure assumes you are using HyperTerminal as your terminal emulator. If you use a different terminal emulator, you may need to adapt this procedure to the operation of your particular emulator.

1. Start the terminal emulator program.

Ensure that the terminal program is configured as follows:

- Baud rate: 9600
- No parity
- 8 Bits
- 1 stop bit
- No flow control

2. Use the `Reset` button to reset the switch.

The following prompt should then appear in the terminal emulator:

```
Enter h or ? for help.
```

```
=>
```

3. Because the OS file is large, you can increase the speed of the download by changing the switch console and terminal emulator baud rates to a high speed. For Example:

a. Change the switch baud rate to 115,200 Bps.

```
=> sp 115200
```

b. Change the terminal emulator baud rate to match the switch speed:

- I. In HyperTerminal, select **Call|Disconnect**.
- II. Select **File|Properties**.
- III. Click on **Configure**.
- IV. Change the baud rate to **115200**.
- V. Click on **[OK]**, then in the next window, click on **[OK]** again.
- VI. Select **Call|Connect**.
- VII. Press **[Enter]** one or more times to display the => prompt.

4. Start the Console Download utility by entering `do` at the => prompt and pressing **[Enter]**:

```
=> do
```

5. You then see this prompt:

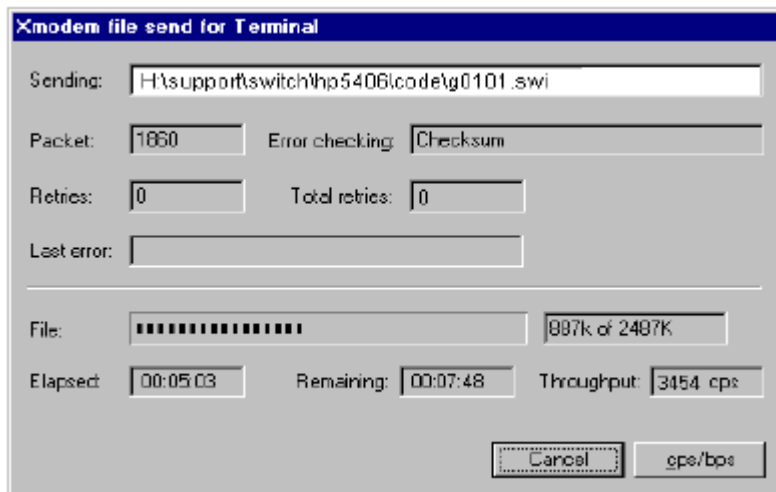
```
You have invoked the console download utility.  
Do you wish to continue? (Y/N)>_
```

6. At the above prompt:

- a. Enter **y** (for Yes)
- b. Select **Transfer|File** in HyperTerminal.
- c. Enter the appropriate filename and path for the OS image.
- d. Select the **Xmodem** protocol (and not the 1k Xmodem protocol).
- e. Click on **[Send]**.

If you are using HyperTerminal, you will see a screen similar to the following to indicate that the download is in progress:

Figure 57: Example: of Xmodem download in progress



When the download completes, the switch reboots from primary flash using the OS image you downloaded in the preceding steps, plus the most recent startup-config file.

DNS resolver

The domain name system (DNS) resolver is designed for use in local network domains, where it enables the use of a host name or fully qualified domain name with DNS-compatible switch CLI commands.

DNS operation supports both IPv4 and IPv6 DNS resolution and multiple, prioritized DNS servers. (For information on IPv6 DNS resolution, see the latest IPv6 configuration guide for your switch.)

Basic operation

- When the switch is configured with only the IP address of a DNS server available to the switch, a DNS-compatible command, executed with a fully qualified domain name, can reach a device found in any domain accessible through the configured DNS server.
- When the switch is configured with both of the following:

- The IP address of a DNS server available to the switch
- The domain suffix of a domain available to the configured DNS server then:
- A DNS-compatible command that includes the host name of a device in the same domain as the configured domain suffix can reach that device.
- A DNS-compatible command that includes a fully qualified domain name can reach a device in any domain that is available to the configured DNS server.

Example:

Suppose the switch is configured with the domain suffix `mygroup.Switch.net` and the IP address for an accessible DNS server. If an operator wants to use the switch to ping a target host in this domain by using the DNS name "leader" (assigned by a DNS server to an IP address used in that domain), the operator can use either of the following commands:

Figure 58: Example: of using either a host name or a fully qualified domain name

```
Switch# ping leader
10.28.229.220 is alive, time = 1 ms

Switch# ping leader.mygroup.Switch.net
10.28.229.220 is alive, time = 1 ms
```

In the proceeding Example:, if the DNS server's IP address is configured on the switch, but a domain suffix is either not configured or is configured for a different domain than the target host, the fully qualified domain name **must** be used.

Note that if the target host is in a domain **other than** the domain configured on the switch:

- The host's domain must be reachable from the switch. This requires that the DNS server for the switch must be able to communicate with the DNS servers in the path to the domain in which the target host operates.
- The fully qualified domain name must be used, and the domain suffix must correspond to the domain in which the target host operates, regardless of the domain suffix configured in the switch.

Example:

Suppose the switch is configured with the domain suffix `mygroup.Switch.net` and the IP address for an accessible DNS server in this same domain. This time, the operator wants to use the switch to trace the route to a host named "remote-01" in a different domain named `common.group.net`. Assuming this second domain is accessible to the DNS server already configured on the switch, a `traceroute` command using the target's fully qualified DNS name should succeed.

Figure 59: Example: using the fully qualified domain name for an accessible target in another domain

```
Switch# traceroute remote-01.common.group.net
[traceroute to 10.22.240.73]
  1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.28.229.3          0 ms    0 ms    0 ms
 2 10.71.217.1         0 ms    0 ms    0 ms
 3 10.0.198.2          1 ms    0 ms    0 ms
[4 10.22.240.73       0 ms    0 ms    0 ms]
```

Configuring and using DNS resolution with DNS-compatible commands

The DNS-compatible commands include `ping` and `traceroute`.)

Procedure

1. Determine the following:
 - a. The IP address for a DNS server operating in a domain in your network.
 - b. The priority (1 to 3) of the selected server, relative to other DNS servers in the domain.
 - c. The domain name for an accessible domain in which there are hosts you want to reach with a DNS-compatible command. (This is the domain suffix in the fully qualified domain name for a given host operating in the selected domain. See **Basic operation** on page 420.) Note that if a domain suffix is not configured, fully qualified domain names can be used to resolve DNS-compatible commands.
 - d. The host names assigned to target IP addresses in the DNS server for the specified domain.
2. Use the data from the first three bullets in step1 to configure the DNS entry on the switch.
3. Use a DNS-compatible command with the host name to reach the target devices.

Configuring a DNS entry

The switch allows up to two DNS server entries (IP addresses for DNS servers). One domain suffix can also be configured to support resolution of DNS names in that domain by using a host name only. Including the domain suffix enables the use of DNS-compatible commands with a target's host name instead of the target's fully qualified domain name.

Syntax:

```
no ip dns server-address priority <1-3> <ip-addr>
```

Configures the access priority and IP address of a DNS server accessible to the switch. These settings specify:

- The relative priority of the DNS server when multiple servers are configured
- The IP address of the DNS server

These settings must be configured before a DNS-compatible command can be executed with host name criteria.

The switch supports two prioritized DNS server entries. Configuring another IP address for a priority that has already been assigned to an IP address is not allowed.

To replace one IP address at a given priority level with another address having the same priority, you must first use the `no` form of the command to remove the unwanted address. Also, only one instance of a given server address is allowed in the server list. Attempting to enter a duplicate of an existing entry at a different priority level is not allowed .

To change the priority of an existing server address, use the `no` form of the command to remove the entry, then re-enter the address with the new priority.

The `no` form of the command replaces the configured IP address with the null setting. (Default: null)

Syntax:

```
no ip dns domain-name <domain-name-suffix>
```

This optional DNS command configures the domain suffix that is automatically appended to the host name entered with a DNS-compatible command. When the domain suffix and the IP address for a DNS server that can access that domain are both configured on the switch, you can execute a DNS-compatible command using only the host name of the desired target. (For an Example:, see **Example: of using either a host name or a fully qualified domain name**.) In either of the following two instances, you must manually provide the domain identification by using a fully qualified DNS name with a DNS-compatible command:

- If the DNS server IP address is configured on the switch, but the domain suffix is not configured (null).
- The domain suffix configured on the switch is not the domain in which the target host exists.

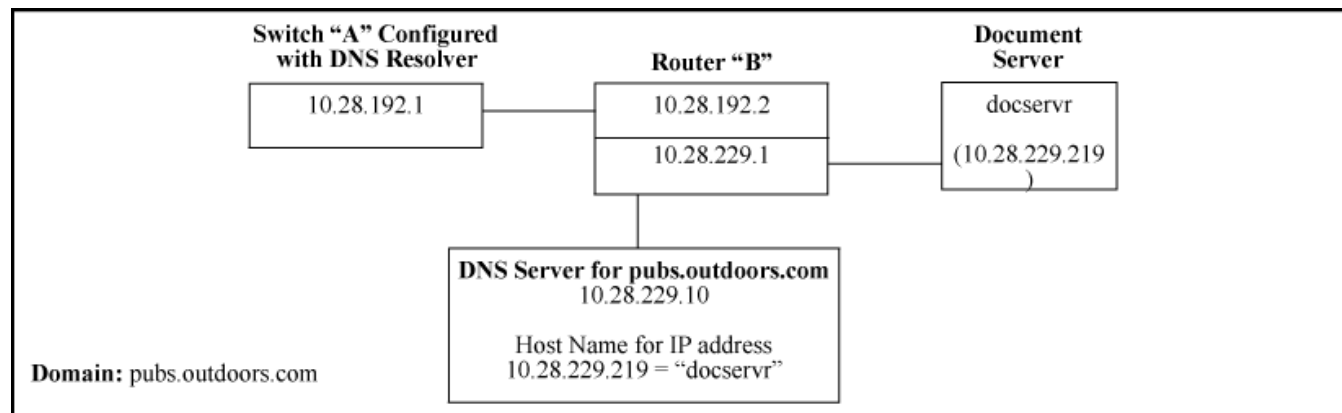
The switch supports one domain suffix entry and three DNS server IP address entries. (See the preceding command description.)

The `no` form of the command replaces the configured domain suffix with the null setting. (Default: null)

Using DNS names with ping and traceroute: Example:

In the network illustrated in **Figure 60: Example: network domain** on page 423, the switch at 10.28.192.1 is configured to use DNS names for DNS-compatible commands in the **pubs.outdoors.com** domain. The DNS server has been configured to assign the host name **docservr** to the IP address used by the document server (10.28.229.219).

Figure 60: Example: network domain



Configuring switch "A" with the domain name and the IP address of a DNS server for the domain enables the switch to use host names assigned to IP addresses in the domain to perform `ping` and `traceroute` actions on the devices in the domain. To summarize:

Entity	Identity
DNS server IP address	10.28.229.10
Domain name (and domain suffix for hosts in the domain)	pubs.outdoors.com
Host name assigned to 10.28.229.219 by the DNS server	docservr

Table Continued

Entity	Identity
Fully qualified domain name for the IP address used by the document server (10.28.229.219)	docservr.pubs.outdoors.com
Switch IP address	10.28.192.1
Document server IP address	10.28.229.219

With the above already configured, the following commands enable a DNS-compatible command with the host name `docserver` to reach the document server at 10.28.229.219.

Configuring switch "A" in Example: network domain to support DNS resolution

```
switch(config)# ip dns server-address 10.28.229.10
switch(config)# ip dns domain-name pubs.outdoors.com
```

Ping and traceroute execution for the network in Example: network domain

```
switch(config)# ping docservr
10.28.229.219 is alive, time = 1 ms

switch# traceroute docservr
traceroute to 10.28.229.219
      1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.28.192.2 1          1 ms      0 ms      0 ms
 2 10.28.229.219 2          0 ms      0 ms      0 ms
```


- ¹First-Hop Router ("B")
- ²Traceroute Target

As mentioned under the following example, if the DNS entry configured in the switch does not include the domain suffix for the desired target, you must use the target host's fully qualified domain name with DNS-compatible commands. For example, using the document server in [Figure 60: Example: network domain](#) on page 423 as a target:

Figure 61: Example: of ping and traceroute execution when only the DNS server IP address is configured

```
Switch# ping [docservr.pubs.outdoors.com]
10.28.229.219 is alive, time = 1 ms

Switch# traceroute [docservr.pubs.outdoors.com]
traceroute to 10.28.229.219
      1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.28.192.2 1          1 ms      0 ms      0 ms
 2 10.28.229.219 2          0 ms      0 ms      0 ms
```



Viewing the current DNS configuration

The `show ip` command displays the current domain suffix and the IP address of the highest priority DNS server configured on the switch, along with other IP configuration information. If the switch configuration currently includes a non-default (non-null) DNS entry, it will also appear in the `show run` command output.

Figure 62: Example: of viewing the current DNS configuration

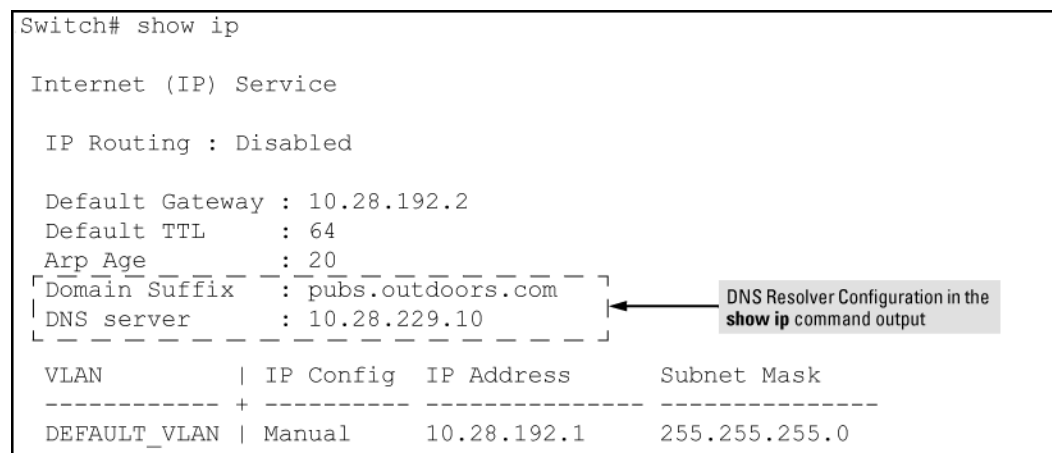
```
Switch# show ip

Internet (IP) Service

  IP Routing : Disabled

  Default Gateway : 10.28.192.2
  Default TTL     : 64
  Arp Age        : 20
  Domain Suffix  : pubs.outdoors.com
  DNS server     : 10.28.229.10

-----+-----
VLAN      | IP Config | IP Address | Subnet Mask
-----+-----
DEFAULT_VLAN | Manual   | 10.28.192.1 | 255.255.255.0
```



Operating notes

- Configuring another IP address for a priority that has already been assigned to an IP address is not allowed. To replace one IP address at a given priority level with another address having the same priority, you must first use the `no` form of the command to remove the unwanted address. Also, only one instance of a given server address is allowed in the server list. Attempting to enter a duplicate of an existing entry at a different priority level is not allowed. To change the priority of an existing server address, use the `no` form of the command to remove the entry, then re-enter the address with the new priority.
- To change the position of an address already configured with priority `x`, you must first use `no ip dns server-address priority x <ip-addr>` to remove the address from the configuration, then use `ip dns server-address priority <ip-addr>` to reconfigure the address with the new priority. Also, if the priority to which you want to move an address is already used in the configuration for another address, you must first use the `no` form of the command to remove the current address from the target priority.
- The DNS servers and domain configured on the switch must be accessible to the switch, but it is not necessary for any intermediate devices between the switch and the DNS server to be configured to support DNS operation.
- When multiple DNS servers are configured on the switch, they can reside in the same domain or different domains.
- A DNS configuration must include the IP address for a DNS server that is able to resolve host names for the desired domain. If a DNS server has limited knowledge of other domains, its ability to resolve DNS-compatible command requests is also limited.
- If the DNS configuration includes a DNS server IP address but does not also include a domain suffix, then any DNS-compatible commands should include the target host's fully qualified domain name.
- Switch-Initiated DNS packets go out through the VLAN having the best route to the DNS server, even if a Management VLAN has been configured.
- The DNS server address must be manually input. It is not automatically determined via DHCP.

Locating a switch (Locator LED)

To locate where a particular switch is physically installed, use the `chassislocate` command to activate the blue Locator LED on the switch's front panel.

Syntax:

```
chassislocate [blink | on | off]
```

Locates a switch by using the blue Locate LED on the front panel.

<code>blink <1-1440></code>	Blinks the chassis Locate LED for a specified number of minutes (Default: 30 minutes).
<code>on <1-1440></code>	Turns the chassis Locate LED on for a specified number of minutes (Default: 30 minutes).
<code>off</code>	Turns the chassis Locate LED off.

Locating a switch with the `chassislocate` command

```
switch(config)# chassislocate
  blink <1-1440>      Blink the chassis locate led (default 30 minutes).
  off                 Turn the chassis locate led off.
  on <1-1440>        Turn the chassis locate led on (default 30 minutes).
switch(config)# chassislocate
```

For redundant management systems, if the active management module failover, the Locator LED does not remain lit.

Show Aruba Switch Memory

Syntax

```
show system memory
```

Description

Displays system RAM and flash memory size.

Command context

manager and operator

Usage

You can execute this command in various command contexts. The following example explains the command usage.

Examples

To view the system memory status, execute the `show system memory` command.

```
Switch# show system memory
RAM and Flash - System Memory Information
```

```
System Name          : Switch
VSF-Member :1
  Product SKU        : J9851A
  Flash Size         : 1 GB
  RAM Size           : 4 GB
VSF-Member :2
  Product SKU        : J9851A
  Flash Size         : 1 GB
  RAM Size           : 4 GB
```

To view the system memory status within the STACK context, execute the `show system memory` command.

```
Switch (STACK)# show system memory
RAM and Flash - System Memory Information
System Name          : Switch
Member :1
  Product SKU        : JL072A
  Flash Size         : 1 GB
  RAM Size           : 4 GB
Member :2
  Product SKU        : JL076A
  Flash Size         : 1 GB
  RAM Size           : 4 GB
Member :3
  Product SKU        : JL074A
  Flash Size         : 1 GB
  RAM Size           : 4 GB
Member :4
  Product SKU        : JL076A
  Flash Size         : 1 GB
  RAM Size           : 4 GB
Member :5
  Product SKU        : JL075A
  Flash Size         : 1 GB
  RAM Size           : 4 GB
```

To view the system memory status within the Standalone context, execute the `show system memory` command.

```
Switch(Standalone)# show system memory
RAM and Flash - System Memory Information
System Name          : Switch
Product SKU          : J9779A
Flash Size           : 128 MB
RAM Size             : 256 MB
```

Overview of MAC Address Management

The switch assigns MAC addresses in these areas:

- For management functions, one Base MAC address is assigned to the default VLAN (VID = 1). (All VLANs on the switches covered in this guide use the same MAC address.)
- For internal switch operations: One MAC address per port (see [Viewing the port and VLAN MAC addresses](#) on page 429).

MAC addresses are assigned at the factory. The switch automatically implements these addresses for VLANs and ports as they are added to the switch.



NOTE: The switch's base MAC address is also printed on a label affixed to the switch.

Determining MAC addresses

Use the CLI to view the switch's port MAC addresses in hexadecimal format.



NOTE: The switch's base MAC address is used for the default VLAN (VID =1) that is always available on the switch. This is true for dynamic VLANs as well; the base MAC address is the same across all VLANs.

Viewing the MAC addresses of connected devices

Syntax:

```
show mac-address [port-list | mac-addr | vlan <vid>]
```

Lists the MAC addresses of the devices the switch has detected, along with the number of the specific port on which each MAC address was detected.

<code>[<i>port-list</i>]</code>	Lists the MAC addresses of the devices the switch has detected, on the specified ports.
<code>[<i>mac-addr</i>]</code>	Lists the port on which the switch detects the specified MAC address. Returns the following message if the specified MAC address is not detected on any port in the switch: MAC address < <i>mac-addr</i> > not found.
<code>[vlan <<i>vid</i>>]</code>	Lists the MAC addresses of the devices the switch has detected on ports belonging to the specified VLAN, along with the number of the specific port on which each MAC address was detected.

Viewing the switch's MAC address assignments for VLANs configured on the switch

The Management Address Information screen lists the MAC addresses for:

- Base switch (default VLAN; VID=1)
- Any additional VLANs configured on the switch.

Also, the Base MAC address appears on a label on the back of the switch.



NOTE: The Base MAC address is used by the first (default) VLAN in the switch. This is usually the VLAN named "DEFAULT_VLAN" unless the name has been changed (by using the VLAN Names screen). On the switches covered in this guide, the VID (VLAN identification number) for the default VLAN is always "1," **and cannot be changed**.

Viewing the port and VLAN MAC addresses

The MAC address assigned to each switch port is used internally by such features as Flow Control and the spanning-tree protocol. Using the `walkmib` command to determine the MAC address assignments for individual ports can sometimes be useful when diagnosing switch operation.



NOTE: This procedure displays the MAC addresses for all ports and existing VLANs in the switch, regardless of which VLAN you select.

Procedure

1. If the switch is at the CLI Operator level, use the `enable` command to enter the Manager level of the CLI.
2. Enter the following command to display the MAC address for each port on the switch:

```
switch# walkmib ifPhysAddress
```

(The above command is not case-sensitive.)

Example:

A switch with the following module configuration shows MAC address assignments similar to those shown in the example below:

- A 4-port module in slot A, a 24-port module in slot C, and no modules in slots B and D
- Two non-default VLANs configured

Figure 63: Example: of Port MAC address assignments on a switch

Switch# walkmib ifphysaddress	
ifPhysAddress.1 = 00 12 79 88 b1 ff	ifPhysAddress.1 - 4: Ports A1 - A4 in Slot A (Addresses 5 - 24 in slot A are unused.)
ifPhysAddress.2 = 00 12 79 88 b1 fe	
ifPhysAddress.3 = 00 12 79 88 b1 fd	
ifPhysAddress.4 = 00 12 79 88 b1 fc	
ifPhysAddress.49 = 00 12 79 88 b1 cf	ifPhysAddress.49 - 72: Ports C1 - C24 in Slot C (In this example, there is no module in slot B.)
ifPhysAddress.50 = 00 12 79 88 b1 ce	
ifPhysAddress.51 = 00 12 79 88 b1 cd	
ifPhysAddress.52 = 00 12 79 88 b1 cc	
ifPhysAddress.53 = 00 12 79 88 b1 cb	
ifPhysAddress.54 = 00 12 79 88 b1 ca	
ifPhysAddress.55 = 00 12 79 88 b1 c9	
ifPhysAddress.56 = 00 12 79 88 b1 c8	
ifPhysAddress.57 = 00 12 79 88 b1 c7	
ifPhysAddress.58 = 00 12 79 88 b1 c6	
ifPhysAddress.59 = 00 12 79 88 b1 c5	
ifPhysAddress.60 = 00 12 79 88 b1 c4	
ifPhysAddress.61 = 00 12 79 88 b1 c3	
ifPhysAddress.62 = 00 12 79 88 b1 c2	
ifPhysAddress.63 = 00 12 79 88 b1 c1	
ifPhysAddress.64 = 00 12 79 88 b1 c0	
ifPhysAddress.65 = 00 12 79 88 b1 bf	
ifPhysAddress.66 = 00 12 79 88 b1 be	
ifPhysAddress.67 = 00 12 79 88 b1 bd	
ifPhysAddress.68 = 00 12 79 88 b1 bc	
ifPhysAddress.69 = 00 12 79 88 b1 bb	
ifPhysAddress.70 = 00 12 79 88 b1 ba	
ifPhysAddress.71 = 00 12 79 88 b1 b9	
ifPhysAddress.72 = 00 12 79 88 b1 b8	
ifPhysAddress.362 = 00 12 79 88 a1 00	ifPhysAddress.362 Base MAC Address (MAC Address for default VLAN; VID = 1)
ifPhysAddress.461 = 00 12 79 88 a1 00	ifPhysAddress.461 and 488 Physical addresses for non-default VLANs configured on the switch. On the switches covered by this manual, all VLANs use the same MAC address as the Default VLAN. Refer to "Multiple VLAN Considerations" in the "Static LANs (VLANs)" chapter of the <i>Advanced Traffic Management Guide</i> for your switch.
ifPhysAddress.488 = 00 12 79 88 a1 00	
ifPhysAddress.4456 =	Virtual

Overview

To simplify the deployment of mobility and IoT devices, Aruba switches have a mechanism to automatically detect devices based on their LLDP signatures and apply configuration to the port to which they are connected. This reduces the time needed to add, move, or change devices on the network and also eliminates potential misconfigurations on the port.

Device Profiles allow an administrator to create configuration containers for different classes of devices and associate them with certain device types. The configuration containers are stored as part of the config, but do not come into effect until a device with the right LLDP signature is connected to a port on that switch. Device profiles allow network administrators to apply port settings automatically, eliminating configuration mistakes as well as reducing the time taken to connect wired devices.

Organization-specific TLVs and subtypes that come as part of LLDP messages are used to detect and apply profiles to devices. A maximum of 16 devices can be detected and defined using Device Profiles. The following sections talk about the operational steps that need to be followed to add Mobility and IoT devices as well as features such as Rogue AP detection that can be used for mobile-first deployments with Aruba APs.

Auto configuring Aruba APs

The auto device detection and configuration detects a directly connected Aruba AP dynamically and applies predefined configurations to ports on which the Aruba AP is detected.

You can create port configuration profiles, associate them to a device type, and enable or disable a device type. One of the device types supported is `aruba-ap` and it is used to identify all the Aruba APs.

When a configured device type is connected on a port, the system automatically applies the corresponding port profile. Connected devices are identified using LLDP. When the LLDP information on the port ages out, the device profile is removed.

By default, the device profile feature is disabled. When you enable the device profile support for a device type, if no other device profile is mapped to the device type, the default device profile `default-ap-profile` is associated with the device type. You can modify the AP default device profile configuration but you cannot delete it. The `default-ap-profile` command supports only the AP device type.



NOTE: Only APs which are connected directly will be detected.

Associating a device with a profile

To associate an Aruba access point (AP) device-type to a user-defined profile, use the context `Switch(device-aruba-ap) #`. All Aruba access points use the identifier **aruba-ap**.

The `no` form of the command removes the device type association and disables the feature for the device type.

The feature is disabled by default.

device-profile name

Syntax

```
device-profile name <PROFILE-NAME> [untagged-vlan <VLAN-ID> |  
tagged-vlan <VLAN-LIST> | cos <COS-VALUE> |  
ingress-bandwidth <Percentage> |  
egress-bandwidth <Percentage> |
```

```
{poe-priority {critical | high | low} |
speed-duplex {auto |auto-10 | auto-100 | ...} |
poe-max-power <Watts> |
allow-jumbo-frames | allow-tunneled-node]
```

```
no device-profile name <PROFILE-NAME> [untagged-vlan <VLAN-ID> |
tagged-vlan <VLAN-LIST> | cos <COS-VALUE> |
ingress-bandwidth <Percentage> |
egress-bandwidth <Percentage> |
{poe-priority {critical | high | low} |
speed-duplex {auto |auto-10 | auto-100 | ...} |
poe-max-power <Watts> |
allow-jumbo-frames | allow-tunneled-node]
```

Description

This command is used to create a user-defined profile. A profile is a named collection of port settings applied as a group. You can modify the default profile, `default-ap-profile`, but you cannot delete it. You can create four additional profiles.

The `no` form of the command removes the user-defined profiles.

The `default-ap-profile` has the following values:

- `untagged-vlan`: 1
- `tagged-vlan`: None
- `ingress-bandwidth`: 100
- `egress-bandwidth`: 100
- `cos`: 0
- `speed-duplex`: `auto`
- `poe-max-power`: `class/LLDP`
- `poe-priority`: `critical`

You can modify these parameters. For example, you can execute `no untagged-vlan` to create a device profile with tagged only ports.

Parameters

`name`

Specifies the name of the profile to be configured. The profile names can be at most 32 characters long.

`cos`

The Class of Service (CoS) priority for traffic from the device.

`untagged-vlan`

The port is an untagged member of specified VLAN.

`tagged-vlan`

The port is a tagged member of the specified VLANs.

`allow-tunneled node`

Configuration to allow Tunneled Node when device profile is applied on port.

`ingress-bandwidth`

The ingress maximum bandwidth for the device port.

egress-bandwidth

The egress maximum bandwidth for the device port.

poe-priority

The PoE priority for the device port.

speed-duplex

The speed and duplex for the device port.

poe-max-power

The maximum PoE power for the device port. The value is set based on PD Class detection and/or LLDP negotiation. `poe-max-power` will have class appropriate value depending on the class of your AP. (Example: class4 = 25.5W, class 3=13W, class2=6.49W, class1=3.84W, class0=13W)

Restrictions

- You can modify the configuration parameters of the default profile, `default-ap-profile`, but you cannot delete it or change its name.
- The profile configuration is only applicable to access points.

device-profile type

From within the configure context:

Syntax

```
device-profile type <DEVICE> [associate <PROFILE-NAME> | enable | disable ]
```

Description

This command specifies an approved device type in order to configure and attach a profile to it. The profile's configuration is applied to any port where a device of this type is connected.

Approved device types

aruba-ap

Aruba access point device.

arubaos-switch

ArubaOS switch

Parameters

From within the **device-aruba-ap** context

associate <PROFILE-NAME>

Associated the specified device type by profile name.

enable

Enables the automatic profile association.

disable

Disables the automatic profile association.

Usage

```
no device-profile type <DEVICE> [associate <PROFILE-NAME> |enable | disable]
```



NOTE: The device types supported are `aruba-ap` and `arubaos-switch`.

device-profile type device-name

Syntax

```
device-profile type [aruba-ap | aruba-switch | scs-wan-cpe |  
device-name <DEVICE-NAME> associate <PROFILE-NAME> | enable | disable]
```

```
no device-profile type [aruba-ap | aruba-switch | scs-wan-cpe |  
device-name <DEVICE-NAME> associate <PROFILE-NAME> | enable | disable]
```

Description

Associates the device profile with the type of device by identity.

The `no` form of this command removes the device profile from the device type.

Command context

config

Parameters

associate <PROFILE-NAME>

Selects the profile name associated with the device-type.

enable

Selects the profile of the device being enabled.

disable

Selects the profile of the device being disabled.

Usage

- The command `device-profile type aruba-ap enable` enables profile for Aruba-AP.
- Device Name is defined the same as Device Identity.

show device-profile

Syntax

Within the configure context:

```
show device-profile
```

Description

Show device profile configuration and status.

config

Show the device profile configuration details for a single, or all, profiles.

status

Show currently applied device profiles.

Usage

```
show device-profile config <PROFILE-NAME>
```

```
show device-profile status
```

show device-profile config

```
Switch# Show device-profile config
Device Profile Configuration

Configuration for device-profile : default-ap-profile
untagged-vlan      : 1
tagged-vlan        : None
ingress-bandwidth  : 100%
egress-bandwidth   : 100%
cos                : None
speed-duplex       : auto
poe-max-power      : Class/LLDP
poe-priority       : critical
allow-jumbo-frames : Disabled
allow-tunneled-node: Enabled
```

show device-profile config profile1

```
Switch(device-profile)# show device-p config test

Device Profile Configuration

Configuration for device-profile : profile1
untagged-vlan      : 1
tagged-vlan        : None
ingress-bandwidth  : 100%
egress-bandwidth   : 100%
cos                : None
speed-duplex       : auto
poe-max-power      : Class/LLDP
poe-priority       : critical
allow-jumbo-frames : Disabled
allow-tunneled-node: Enabled
```

show command device-profile status

Syntax

```
show device-profile [config | status]
```

Description

Displays the device-profile configuration or device-profile status.

Parameters

config

Show device profile configuration details for a single profile or all profiles.

status

Show currently applied device profiles status.

show device-profile status

```
Switch# show device-profile status
```

Device	Profile	Status	
Port	Device Type	Applied Device Profile	
----	-----	-----	
5	aruba-ap	profile1	
10	aruba-ap	profile1	

show device-profile config

Syntax

```
show device-profile config
```

Description

Shows the device profile configuration.

Command context

```
config
```

Examples

Use the command `show device-profile config` to display the device profile configuration.

```
switch(config)# show device-profile config
```

```
Device Profile Configuration
```

```
Configuration for device-profile : default-ap-profile
```

```
untagged-vlan      : 1
tagged-vlan        : None
ingress-bandwidth  : 100%
egress-bandwidth   : 100%
cos                : None
speed-duplex       : auto
poe-max-power      : Class/LLDP
poe-priority       : critical
allow-jumbo-frames : Disabled
allow-tunneled-node: Enabled
```

```
Configuration for device-profile : test
```

```
untagged-vlan      : 1
tagged-vlan        : None
ingress-bandwidth  : 100%
egress-bandwidth   : 100%
cos                : None
speed-duplex       : auto
poe-max-power      : Class/LLDP
poe-priority       : critical
allow-jumbo-frames : Disabled
allow-tunneled-node: Enabled
```

```
Configuration for device-profile : default-aos-profile
```

```
untagged-vlan      : 1
tagged-vlan        : None
ingress-bandwidth  : 100%
egress-bandwidth   : 100%
```

```
cos : None
speed-duplex : auto
poe-max-power : Class/LLDP
poe-priority : critical
allow-jumbo-frames : Disabled
allow-tunneled-node: Enabled
```

Configuration for device-profile : default-scs-profile

```
untagged-vlan : 1
tagged-vlan : None
ingress-bandwidth : 100%
egress-bandwidth : 100%
cos : None
speed-duplex : auto
poe-max-power : Class/LLDP
poe-priority : critical
allow-jumbo-frames : Disabled
allow-tunneled-node: Enabled
```

Configuration for device-profile : default-device-profile

```
untagged-vlan : 1
tagged-vlan : None
ingress-bandwidth : 100%
egress-bandwidth : 100%
cos : None
speed-duplex : auto
poe-max-power : Class/LLDP
poe-priority : critical
allow-jumbo-frames : Disabled
allow-tunneled-node: Enabled
```

Device Profile Association

```
Device Type : aruba-ap
Profile Name : default-ap-profile
Device Status : Disabled

Device Type : aruba-switch
Profile Name : default-aos-profile
Device Status : Disabled

Device Type : scs-wan-cpe
Profile Name : default-scs-profile
Device Status : Disabled
```

show device-profile status

Syntax

```
show device-profile status
```

Description

Shows the profile status of the device.

Command context

```
config
```

Example

Use the show device-profile status command to view status.

```
switch(config)# show device-profile status
Port      Device-type      Applied device profile
-----
A1        <device-name>    abc
```

Default AP Profile

Creates a user-defined profile.

The profile name is a valid character string with the maximum permissible length of 32. The default profile is named `default-ap-profile` and cannot be modified.

The default configuration parameters may be modified using the command `device-<PROFILE NAME> default-ap-profile` . Up to four different profiles may be configured.

The `no` command removes the user-defined profiles.

allow-jumbo-frames

Syntax

```
allow-jumbo-frames
```

Description

Configure jumbo frame support for the device port. Jumbo frames are not enabled by default.

Auto configuring IoT Devices

Wired IoT devices can also be automatically configured using device profiles. Since the market for IoT devices is vast, with several hundred manufacturers and thousands of devices, instead of hardcoding the LLDP signatures, Aruba switches provide a way for an administrator to create a device type for the IoT devices in their deployment. By associating the custom device type that they create with a device profile, users can leverage the power profiles not only for Aruba devices but also for other manufacturers. The requirement for automatic detection of IoT devices is that they should support LLDP.

Creating a device identity and associating a device type

Procedure

1. Create a device identity using the command:

```
switch# device-identity name <DEVICE-NAME>
```

2. Specify the OUI used in LLDP's organization using specific TLV, (type =127). OUI should be in XXXXXX format. The default OUI "000000" indicates that device-identity will not use LLDP to identify device:

```
switch(config)# device-identity name <DEVICE-NAME> lldp oui <MAC_OUI>
sub-type <SUBTYPE>
```

To add new device on switch:

```
switch(config)# device-identity name abc lldp oui a1b2c3 sub 2
```

To remove device from switch:

```
switch(config)# no device-identity name abc
```

3. Show device identity configuration:

```
switch(config)# show device-identity lldp
```

```
Device Identity Configuration
```

Index	Device name	Oui	Subtype
1	abc	a1b2c3	2



NOTE: The maximum devices that can be configured using `device-identity` are 16. The maximum devices that can be associated using `device-profile` are 19. The maximum profiles that can be created using `device-profile` are 17.

show device-identity

Syntax

```
show device-identity
```

Description

Specify name of the device to be discovered.

Command context

```
config
```

Usage

```
device-identity name <device_name> lldp oui <mac_oui> subtype <subtype>
```

```
no device-identity name <device_name> lldp oui <mac_oui> subtype <subtype>
```

Example

```
device-identity name avayaPhone lldp oui 00096e sub-type 1
```

```
switch(device-profile)# show device-identity
```

```
Device Identity Configuration
```

Index	Device name	Protocol
1	avayaPhone	LLDP

```
switch(device-profile)# show device-identity lldp
```

```
Device Identity Configuration
```

Index	Device name	Oui	Subtype
1	avayaPhone	00096e	1

device-profile type-device associate

From within the configure context:

Syntax

```
device-profile type-device <DEVICE_NAME> [associate <PROFILE-NAME> | enable | disable ]
```

Description

Specify device name defined in device-identity in order to configure and attach a profile to it. Device identity uses discovery protocol like LLDP to identify device. LLDP makes use of OUI and sub type of organizational specific TLV type 127 to detect device.

Approved device types

aruba-ap

Aruba access point device.

arubaos-switch

ArubaOS switch

Parameters

<DEVICE_NAME>

Defines in device-identity.

associate <PROFILE-NAME>

Associated the specified device type by profile name.

enable

Enables the automatic profile association.

disable

Disables the automatic profile association.

Usage

Use the following command to configure a device:

```
device-identity name <DEVICE_NAME> lldp oui <OUI> subtype <SUBTYPE>.
```

Example

```
device-p device-type avayaPhone associate avaya
```



NOTE: The device types supported are `aruba-ap` and `arubaos-switch`.

show device-profile config

Syntax

```
show device-profile config
```

Description

Shows the device profile configuration.

Command context

```
config
```

Examples

Use the command `show device-profile config` to display the device profile configuration.

```
switch(device-profile)# show device-p con avaya
```


Device Profile Configuration

```
Configuration for device-profile : avaya
untagged-vlan      : 1
tagged-vlan        : None
ingress-bandwidth  : 100%
egress-bandwidth   : 100%
cos                : None
speed-duplex       : auto
poe-max-power      : Class/LLDP
poe-priority       : critical
allow-jumbo-frames : Disabled
allow-tunneled-node : Enabled
```

show device-profile status

Syntax

```
show device-profile [config | status]
```

Description

Displays the device-profile configuration or device-profile status.

Parameters

config

Show device profile configuration details for a single profile or all profiles.

status

Show currently applied device profiles status.

show device-profile status

```
Switch# show device-profile status
```

```
Device Profile Status
```

Port	Device-type	Applied device profile
A2	avayaPhone	avaya

Support for Aruba device types

The following Aruba device types are supported:

- Aruba-AP
- ArubaOS-Switch
- Any device that can be defined using LLDP OUI and subtype in the switch

Isolating Rogue APs

One of the important features to turn on in a mobile-first deployment is the ability of the switches to detect and quarantine rogue access points. Administrators would like to prevent unauthorized access to their networks and a rogue AP can open up the network to unwanted users and traffic.

The Rogue AP Isolation feature detects and blocks any unauthorized APs in the network. You can either log or block the rogue device. If the action requested is to log the rogue device, the MAC address of the rogue device is

logged in the system logs (RMON). If the action is to block the rogue device, the traffic to and from the MAC address of the rogue device is blocked. The MAC is also logged in the system log.

When an Aruba AP detects a rogue AP on the network, it sends out the MAC address of the AP as well as the MAC of the clients connected to the AP to the switch using the ArubaOS-Switch proprietary LLDP TLV protocol. The switch then adds a rule in its hardware table to block all the traffic originating from the rogue AP's MAC address.

The `rogue-ap-isolation` command configures the rogue AP isolation for the switch and gives the option to enable or disable the rogue AP isolation feature. The `rogue-ap-isolation action` command gives you the ability to block the traffic to or from the rogue device or log the MAC of the rogue device. When the action is set to block, the rogue MAC is logged as well. By default, the action is set to block.

The `rogue-ap-isolation whitelist` command lets you add devices detected as possible rogue APs to the whitelist. A maximum of 128 MAC addresses are supported for the whitelist.

The `clear rogue-aps` command clears the detected rogue AP device MAC address.

Using the Rogue AP Isolation feature

Procedure

1. Check the feature state:

```
switch# show rogue-ap-isolation

Rogue AP Isolation

Rogue AP Status : Disabled
Rogue AP Action : Block

Rogue MAC Address Neighbour MAC Address
-----
```

2. Enable the feature:

```
switch# rogue-ap-isolation enable
switch# show rogue-ap-isolation

Rogue AP Isolation

Rogue AP Status : Enabled
Rogue AP Action : Block

Rogue MAC Address Neighbour MAC Address
-----
```

3. Change the action type from block to log:

```
switch# rogue-ap-isolation action log
switch# show rogue-ap-isolation

Rogue AP Isolation

Rogue AP Status : Enabled
Rogue AP Action : Log

Rogue MAC Address Neighbour MAC Address
-----
```

4. List the current whitelist entries:

```
switch# show rogue-ap-isolation whitelist
Rogue AP Whitelist Configuration
Rogue AP MAC
-----
```

5. Add a new whitelist entry:

```
switch# rogue-ap-isolation whitelist 005056-00326a
switch# show rogue-ap-isolation whitelist
Rogue AP Whitelist Configuration
Rogue AP MAC
-----
00:50:56:00:32:6a
```

rogue-ap-isolation

syntax

```
rogue-ap-isolation {enable | disable}
```

Description

Configures the rogue AP isolation for the switch.

Parameters

enable

Enables the rogue AP isolation.

disable

Disables the rogue AP isolation.

rogue-ap-isolation action

syntax

```
rogue-ap-isolation action {log | block}
```

Description

Configures the action to take for the rogue AP packets. This function is disabled by default.

Parameters

action

Configure the action to take for rogue AP packets. By default, the rogue AP packets are blocked.

Parameters

log

Logs traffic to or from any rogue access points.

block

Blocks and logs traffic to or from any rogue access points.

rogue-ap-isolation whitelist

syntax

```
no rogue-ap-isolation whitelist <MAC-ADDRESS>
```

Description

Configures the rogue AP Whitelist MAC addresses for the switch. Use this command to add to the whitelist the MAC addresses of approved access points or MAC addresses of clients connected to the rogue access points. These approved access points will not be added to the rogue AP list even if they are reported as rogue devices.

Parameters

MAC-ADDRESS

Specifies the MAC address of the device to be moved from the rogue AP list to the whitelist.

Parameters

no

Removes the MAC address individually by specifying the MAC.

Restrictions

You can add a maximum of 128 MAC addresses to the whitelist.

clear rogue-ap-isolation

syntax

```
clear rogue-ap-isolation { <MAC-ADDRESS> | all }
```

Description

Removes the MAC addresses from the rogue AP list.

Parameters

MAC-ADDRESS

Specifies the MAC address of the device to be moved from the rogue AP list.

all

Clears all MAC addresses from the rogue AP list.

Restrictions

The MAC addresses cleared using this option will be added back to the rogue list under the following cases:

1. The LLDP administrator status of the port on which the AP that reported the MAC is disabled and enabled back.
2. The data that is in the rogue AP TLV sent from the AP that informed the rogue MAC has changed.
3. To permanently ignore a MAC from being detected as rogue, add it to the whitelist.

Feature Interactions

L3 MAC

The Rogue AP isolation feature will not block a MAC configured as an IP receive MAC address on a VLAN interface. This event will be logged in RMON if such MACs are detected as rogue.

Conversely, any MAC already blocked by Rogue AP isolation will not be allowed to be configured as an IP receive MAC address of a VLAN interface.

For example:

```
switch# vlan 1 ip-recv-mac-address 247703-3effbb
Cannot add an entry for the MAC address 247703-3effbb because it is already
blocked by rogue-ap-isolation.
```

Limitations

- You can add a maximum of 128 MAC addresses to the whitelist.
- When a MAC is already authorized by any of the port security features such as LMA, WMA, or 802.1X, the MAC is logged but you cannot block it using the `rogue-ap-isolation` feature. A RMON event is logged to notify the user.
- When a MAC is already configured as an IP received MAC of a VLAN interface, the MAC is logged but you cannot block it by using the `rogue-ap-isolation` feature. A RMON event is logged to notify the user.
- When a MAC is already locked out via `lockout-mac` or locked down using the `static-mac` configuration, the MAC is logged but you cannot block it using the `rogue-ap-isolation` feature. A RMON event is logged to notify the user.
- The number of rogue MACs supported on a switch is a function of the value of `max-vlans` at boot time. Since the resources are shared with the `lockout-mac` feature, the scale is dependent on how many lockout addresses have been configured on the switch using the `lockout-mac` feature. The following table lists the scale when there are no lockout addresses configured on the switch:

Max VLAN	Supported MACs
0 < VLAN <= 8	200
8 < VLAN <= 16	100
16 < VLAN <= 256	64
256 < VLAN <= 1024	16
1024 < VLAN <= 2048	8
2048 < VLAN <= 4094	4

The switch will create an RMON log entry and the rogue MAC will be ignored when the limit is reached.



NOTE: If the `max-vlans` value is changed to a different value, the scale of rogue MACs supported will not change until the next reboot.

Troubleshooting

Switch does not detect the rogue AP TLVs

Symptom

The switch does not detect the rogue AP TLVs that could be sent from the neighboring device.

Cause

The LLDP administrator status of a port is moved from `txOnly` to `tx_rx` or `rx_only` within 120 seconds of the previous state change to `txOnly`.

Action

1. Wait for 120 seconds before moving from the state `txOnly` to the state `tx_rx` or `rx_only`.
2. Move the administrator status to `disable` and then back to `tx_rx` or `rx_only`.

Show commands

Use the following show commands to view the various configurations and status.

Command	Description
<code>show rogue-ap-isolation</code>	Shows the following information: <ul style="list-style-type: none">• The status of the feature: enabled or disabled.• The current action type for the rogue MACs detected.• The list of MAC addresses detected as rogue and the MAC address of the AP that reported them.
<code>show rogue-ap-isolation whitelist</code>	Shows the rogue AP whitelist configuration.

Requirements

Only APs directly connected to the switch will be detected.

Limitations

- Only one device type is supported, `aruba-ap`, and it is used to identify all the Aruba APs.
- You can modify the configuration parameters of the default profile, `default-ap-profile`, but you cannot delete it or change its name.
- If the port was part of any protocol VLANs prior to the device profile application, those VLANs will not be removed while applying the device profile.
- Enabling jumbo frame support in a profile affects other ports with different profiles. When a profile has jumbo frames enabled and is applied to any port, all other ports that are members of any VLAN listed in the profile will also have jumbo frame support.

Feature Interactions

Profile Manager and 802.1X

Profile Manager interoperates with RADIUS when it is working in the client mode. When a port is blocked due to 802.1X authentication failure, the LLDP packets cannot come in on that port. Therefore, the Aruba AP cannot be detected and the device profile cannot be applied. When the port gets authenticated, the LLDP packets comes in, the AP is detected, and the device profile is applied.

You must ensure that the RADIUS server will not supply additional configuration such as VLAN or CoS during the 802.1X authentication as they will conflict with the configuration applied by the Profile Manager. If the RADIUS server supplies any such configurations to a port, the device profile will not be applied on such ports.

Profile Manager and LMA/WMA/MAC-AUTH

If either LMA, WMA, or MAC-AUTH is enabled on an interface, all the MAC addresses reaching the port must be authenticated. If LMA, WMA, or MAC-AUTH is configured on an interface, the user can have more granular control and does not need the device profile configuration. Therefore, the device profile will not be applied on such interface.

Profile manager and Private VLANs

When the device profile is applied, a check is performed to verify if the VLAN addition violates any PVLAN requirements. The following PVLAN related checks are done before applying the VLANs configured in the device profile to an interface:

- A port can be a member of only one VLAN from a given PVLAN instance.
- A promiscuous port cannot be a member of a secondary VLAN.

MAC lockout and lockdown

The Rogue AP isolation feature uses the MAC lockout feature to block MACs in hardware. Therefore, any MAC blocked with the Rogue AP isolation feature cannot be added with the `lockout-mac` or `static-mac` command if the action type is set to `block`.

For example:

```
switch# lockout-mac 247703-7a8950
Cannot add the entry for the MAC address 247703-7a8950 because it is already
blocked by rogue-ap-isolation.
```

```
switch# static-mac 247703-7a8950 vlan 1 interface 1
Cannot add the entry for the MAC address 247703-7a8950 because it is already
blocked by rogue-ap-isolation.
```

Similarly, any MAC that was added with the `lockout-mac` or `static-mac` command and that is being detected as rogue will be logged, but not blocked in hardware as it already is set to `block`. If the MAC is removed from `lockout-mac` or `static-mac` but is still in the rogue device list, it will be blocked back in hardware if the action type is `block`.

LMA/WMA/802.1X/Port-Security

Any configuration using LMA, WMA, 802.1X, or Port-Security will not be blocked if the Rogue AP isolation feature is enabled. All these features act only when a packet with the said MAC is received on a port.

If `rogue-ap-isolation` blocks a MAC before it is configured to be authorized, packets from such MACs will be dropped until one of the following happens:

- Rogue action is changed to LOG.
- Rogue-AP isolation feature is disabled.
- The MAC is not detected as rogue anymore.
- LLDP is disabled on the port (or globally).

Once a MAC has been authorized by one of these features, it will not be blocked by Rogue AP isolation. A RMON will be logged to indicate the failure to block.

The Rogue AP module will retry to block any such MACs periodically. In the event of the MAC no longer being authorized, Rogue AP isolation will block the MAC again. No RMON is logged to indicate this event.

Troubleshooting

Dynamic configuration not displayed when using “show running-config”

Symptom

The `show running-config` command does not display the dynamic configuration applied through the device profile.

Cause

The `show running-config` command shows only the permanent user configuration and parameters configured through device profile.

Action

Use the specific `show device-profile` command to display the parameters dynamically configured through the device profile.

The `show run` command displays non-numerical value for untagged-vlan

Symptom

The `show run` command displays one of the following values for `untagged-vlan`:

- `no untagged-vlan`
- `untagged-vlan : None`

Cause

The `no device-profile` or the `no rogue-ap-isolation whitelist` command is executed to configure `untagged-vlan` to 0.

Action

No action is required.

Show commands

Use the following show commands to view the various configurations and status.

Command	Description
<code>show device-profile</code>	Shows the device profile configuration and status.
<code>show device-profile config</code>	Shows the device profile configuration details for a single profile or all profiles.
<code>show device-profile status</code>	Shows currently applied device profiles.
<code>show run</code>	Shows the running configuration.

Overview

The Job Scheduler feature enables the user to schedule commands or jobs on the switch for one time or multiple times. This is similar in concept to the UNIX 'cron' utility. The user can schedule any CLI command that the user would otherwise enter interactively. This includes commands to enable or disable ports, LEDs, and Power-Over-Ethernet. Jobs can also be scheduled to be triggered by certain pre-defined events such as switch reboot. The only major restriction on commands scheduled is that, it should not prompt/ask for any user inputs.

Commands

Job at | delay | enable | disable

Set schedule jobs using the options and set the count for the number of times the job is repeated.

Syntax

```
job JOB_NAME at | delay | enable | disable
```

Description

Schedule a command to run automatically. Jobs can be scheduled to run once, multiple times on a recurring basis, or after certain events such as reboots. All commands run with manager privilege in configuration context.

The no form of the command deletes a scheduled job.

By default, jobs will be repeated an infinite number of times.

Restrictions

Jobs scheduled at any event will not be counted.

Jobs that are scheduled at the event "reboot" will not work in some multi management switches.

Range

- <1-1000>: is the value range for the `count` option.
- ([[DD:]HH:]MM): is the format used for the specific delay.

Parameters

count

Specify the number of times the job should run.

delay

Specify the delay before running the job.

enable

Enable a job that is disabled or expired.

disable

Disable a job. By default, a job is enabled.

Usage

```
job <JOB NAME> at <([DD:]HH:]MM on <WEEKDAY-LIST>> config-save <COMMAND> count <1-1000>
```

```
job <JOB NAME> at <[HH:]MM on [MM/]DD> config-save <COMMAND> count <1-1000>
```

```
job <JOB NAME> at <EVENT> config-save <COMMAND>
```

```
job <JOB NAME> delay <([DD:]HH:]MM> config-save <COMMAND> count <1-1000>
```

```
job <JOB NAME> enable | disable
```

```
no job <JOB NAME>
```

Show job

Syntax

```
show job
```

Description

Show the jobs scheduled.

Show job

```
switch# show job
```

```
Job Scheduler Status and Configuration
```

```
Scheduler Status : Waiting for the system time to be set
```

Name	Event or Time	Repeat Count	Save Cfg	Command
Burrrrrrrrrrrrr...	reboot	--	Yes	chassislocate blink
baz	reboot	--	No	show time
foo	17:00 SxTWTxS	--	No	savepower led
a1	12:00	2	Yes	sh time
a2	Every 2:14:30 days	75	Yes	vlan 3
a3	Every 00:00:25 days	1	No	vlan 4



NOTE: Caution

The scheduler does not run until the system time is set.

Show job <Name>

Syntax

```
show job JOB NAME
```

Description

Show the job by name.

Show job <JOB NAME>

```
switch# show job a1
```

Job Information

```
Job Name      : a1
Runs At       : 01:24
Config Save   : No
Repeat Count  : --
Job Status    : Enabled
Run Count     : 1
Error Count   : 0
Command       : show time
Job Status    : Enabled
```

Output from Last Run

```
-----
Tue Dec 15 01:24:00 2015
```

```
switch# show job a2
```

Job Information

```
Job Name      : a2
Runs At       : Every 2:14:30 days
Config Save   : Yes
Repeat Count  : 75
Run Count     : 0
Error Count   : 0
Command       : vlan 3
Job Status    : Disabled
```

```
switch# show job foo
```

Job Information

```
Job Name      : foo
Runs At       : 17:00 SxTWTxS
Config Save   : Yes
Repeat Count  : --
Run Count     : 0
Error Count   : 0
Command       : savepower led
Job Status    : Enabled
```

Overview

The traditional way of restoring a configuration from a backup configuration file required a switch reboot for the new configurations to be effective. There were network outages and a planned downtime for even minor changes. The switch configuration can now be restored from a backup configuration without reboot. It also provides hash of the current running configuration, which can be used for auditing.

The backup configuration can be created using the new command `cfg-backup`. An existing method of copying a configuration file from a remote location (for example, TFTP server) can also be used to backup a configuration or copied from flash.

More information

[show hash](#) on page 473

[cfg-backup](#) on page 457

[cfg-restore config_bkp](#) on page 466

Benefits of configuration restore without reboot

- Restores a new or modified configuration without reboot, with minimal network outage. Any NMS can use this method for configuration rebase workflows. Only configurations that were exported from the switch can be imported or restored on the switch.
- Restores the configuration without reboot from a backup configuration when the running configuration has functional issues, like misconfigurations from remote management stations.

Recommended scenarios

- Use the configuration restore feature for incremental configuration updates.
- Use the `force` option with `cfg-restore`, for commands which require reboot.
- Use the `verbose` option to get detailed progress on the configuration restore process.

More information

[Force configuration restore](#) on page 461

[cfg-restore verbose](#) on page 465

Use cases

- A user can switch to a new configuration without rebooting the switch.
- If a user loses connectivity after applying the new configuration, a job scheduler executes the job after a specific time frame. This restores the current configuration to the switch, without rebooting it.

More information

[Switching to a new configuration](#) on page 454

[Rolling back to a stable configuration using job scheduler](#) on page 455

Switching to a new configuration

Procedure

1. Back up the configuration using `cfg-backup running-config config <config_name>` command. In the following example, the configuration name used is “stable”.

```
cfg-backup running-config config stable
```

2. Check the backup configuration using `show config files` command.

```
switch(config)# show config files
```

```
Configuration files:
```

id	act	pri	sec	name
1	*	*	*	config
2				stable
3				
4				
5				

3. Change the running configuration as required, and backup the new configuration as “newfile”.

```
cfg-backup running-config config newfile
```

```
switch(config)# show config files
```

```
Configuration files:
```

id	act	pri	sec	name
1	*	*	*	config
2				stable
3				newfile
4				
5				

4. Check the difference between the “newfile” (running configuration) and “stable” (backed up configuration) using `cfg-restore flash stable diff` command. Based on the difference, apply the backed-up configuration using `cfg-restore flash stable` command.
5. Check the status of the configuration restore using `show cfg-restore status` command.

```
switch(config)# show cfg-restore status
```

```
Status : Success
Config File Name : stable
Source : Flash
Time Taken : 3 Seconds
Last Run : Tue Nov 28 18:24:09 2017

Recovery Mode : Enabled
Failure Reason : -

Number of Add Commands : 14
Number of Remove Commands : 0

Time Taken for Each Phase :
  Calculating diff : 1 Seconds
```

```
Adding commands      : 2 Seconds
Removing commands    : 0 Seconds
```

Rolling back to a stable configuration using job scheduler

Procedure

1. Configure the job using `alias` with the required configuration.

```
alias <name> <command-list>
job <name> delay [[DD:]HH:]MM <command>
```

To schedule a job execution with `cfg-restore` operation once after 15 minutes (00:00:15):

```
alias "cfg_rollback" "cfg-restore flash stable"
job "cfg_stable" delay 00:00:15 "cfg_rollback" count 1
```

2. Back up the current stable configuration using the command `cfg-backup running-config config <config_name>`.

```
cfg-backup running-config config stable
```

3. Check the backup configuration using the command `show config files`.

```
switch(config)# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*	*	config
2				stable
3				
4				
5				

4. Edit the configuration as needed. If the user is still connected to the switch, the configuration is stable and the job which reloads the older configuration can be cancelled using the command `no job cfg_stable`.

```
switch(config)# no job cfg_stable
```

5. If the user loses connectivity after applying the new configuration, the job scheduler executes the job after the 15-minute timer expires, and "stable" configuration is restored. Use the following commands to check the output:

- `switch(config)# show job cfg_stable`
- `switch(config)# show cfg-restore status`

```
switch(config)# show job cfg_stable
```

Job Information

```
Job Name      : cfg_stable
Runs At       : Every 00:00:15 days:hours:minutes
Config Save   : No
Repeat Count  : 1
Job Status    : Enabled
Running Status : Active
```

```

Run Count      : 0
Error Count    : 0
Skip Count     : 0
Command       : cfg_rollback

switch(config)# show cfg-restore status
Status        : Success
Config File Name : stable
Source        : Flash
Time Taken    : 9 Seconds
Last Run      : Tue Nov 28 20:50:00 2017

Recovery Mode  : Enabled
Failure Reason : -

Number of Add Commands : 27
Number of Remove Commands : 0

Time Taken for Each Phase :
Calculating diff : 4 Seconds
Adding commands  : 1 Seconds
Removing commands : 0 Seconds

```



NOTE: If the configuration involves any sensitive information, backup and restore the configuration by enabling the `include-credentials` command.

Commands used in switch configuration restore without reboot

cfg-backup

Backs up the selected configuration to the flash file.

show config files details

Shows a detailed list of configuration files available in the flash.

cfg-restore

Restores the given configuration as the running configuration without reboot.

show cfg-restore status

Shows the status of latest restore performed.

show cfg-restore latest-diff

Views the list of configuration changes that are removed, modified, or added to the running configuration.

show hash

Shows the SHA ID of a startup or running configuration.

Configuration backup

The configuration backup creates a backup of the running or startup configuration of ArubaOS-Switch on-demand to the flash storage on the switch. The maximum number of backup files supported has increased from three to five.



NOTE: When you downgrade configuration backup files from five to three, and if the current number of files is either a four or five, an error message Configuration file <name> stored in config index 5 is not supported in lower image versions is displayed.

cfg-backup

Syntax

```
cfg-backup {running-config | startup-config} config <FILE-NAME>
```

Description

Backs up the selected configuration to the flash file mentioned. When the firmware is downgraded to lower versions, the details of only three configuration files appear in the `show config files` command.

Command context

```
config
```

Parameters

running-config

Copies the running configuration to switch flash file.

startup-config

Copies the startup configuration to switch flash file.

flash

Name of the configuration file in flash.

Usage

```
copy {startup-config | running-config} {sftp | tftp} <server address> <FILE-NAME>
```

The existing `copy` command copies the startup and running configuration to the TFTP or SFTP server.

Examples

```
switch(config)# cfg-backup
  running-config      Backup the running configuration to the flash file
                      mentioned.
  startup-config      Backup the startup configuration to the flash file
                      mentioned.

switch(config)# cfg-backup {running-config | startup-config}
  config              Backup the named configuration file.

switch(config)# cfg-backup {running-config | startup-config} config
  ASCII-STR          Enter an ASCII string.
```

show config files

Syntax

```
show config files
```

Description

Shows a list of configuration files available in the flash.

Command context

```
config
```

Examples

```
switch# show config files  
Configuration files:
```

id	act	pri	sec	name
1	*	*	*	config
2				add
3				modify
4				golden_config
5				poe2

To show the details of saved configuration files:

```
switch(config)# show config files  
details          Show details of saved configuration files.
```

```
switch(config)#show config files details
```

Backup Configuration files:

```
File Name       : config  
File ID         : 1  
File Size      : 35902 Bytes  
Last Modified  : Mon Jan 01 1990 00:09:28  
Version        : WC.16.xx
```

```
File Name       : add  
File ID         : 2  
File Size      : 35902 Bytes  
Last Modified  : Mon Oct 23 2017 03:42:38  
Version        : WC.16.xx
```

```
File Name       : modify  
File ID         : 3  
File Size      : 35902 Bytes  
Last Modified  : Mon Oct 23 2017 03:42:38  
Version        : WC.16.xx
```

To view the contents of a configuration file in the flash:

```
switch# show config add
```

```
; JL255A Configuration Editor; Created on release #WC.16.05.0000x  
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba  
hostname "switch"  
module 1 type jl255a  
snmp-server community "public" unrestricted  
vlan 1  
    name "DEFAULT_VLAN"  
    no untagged 3-10  
    untagged 1-2,11-28  
    ip address dhcp-bootp  
    exit  
vlan 100  
    name "VLAN100"  
    untagged 3-5  
    no ip address  
    exit  
vlan 200  
name "VLAN200"  
    untagged 6-10
```

```
no ip address
exit
```

Configuration restore without reboot

The `cfg-restore` without reboot command restores the configuration without reboot from a backup configuration to the running configuration of the switch.

The details about the difference between a running and a backup configuration can be displayed using `cfg-restore {flash | tftp | sftp} <FILE-NAME> diff` command.

More information

[Configuration backup](#) on page 456

[Viewing the differences between a running configuration and a backup configuration](#) on page 471

cfg-restore

Syntax

```
cfg-restore {flash | tftp <IP-ADDRESS> | sftp <IP-ADDRESS>} <FILE-NAME> [diff | force | non-blocking | recovery-mode | verbose]
```

Description

Restores the given configuration as the running configuration without reboot. If the configuration is not suitable to successfully restore without reboot, the command will return a failure message with details.



NOTE: The restored configuration commands will be executed on a running configuration, so the name of the current active configuration does not change after configuration restore, except for the `force` option.

Command context

config

Parameters

flash

Copies file from flash.

tftp

Copies file from TFTP server.

sftp

Copies file from SFTP server.

<IP-ADDRESS>

IP address of the TFTP server.

<FILE-NAME>

Name of the backup configuration file to restore into the running configuration.

diff

Provides the list of changes that will be applied on the running configuration.

force

Forces a reboot if configuration in restored configuration requires a reboot. Applies the configuration with reboot if the configuration has reboot required commands or system-wide change commands. After a forced reboot, the name of the configuration changes.

non-blocking

Configuration restoration in non-blocking mode, where actual process happens in the background.

recovery-mode

Enables or disables recovery-mode. Recovery-mode is enabled by default and this retains the current running configuration if configuration restoration fails.

verbose

Provides the details of configuration restore status and the list of commands to be added or deleted.

Usage

- `cfg-restore flash <FILE-NAME> [non-blocking | diff | force | recovery-mode{enable | disable}]] | [verbose [force | [recovery-mode{enable | disable}]] | [diff | force]`
- `cfg-restore tftp {<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME-STR> <FILE-NAME> [non-blocking | diff | force | recovery-mode{enable | disable}]] | [verbose [force | [recovery-mode{enable | disable}]] | [diff | force]`
- `cfg-restore sftp {<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME-STR> | user <name> {<IP-ADDRESS|IPV6-ADDRESS|HOSTNAME-STR>} | <USERNAME@>{<HOST-NAME> | <IPV4-ADDR> | <IPV6-ADDR>}} [port <1-65535>] <FILE-NAME> [non-blocking | diff | force | recovery-mode{enable | disable}]] | [verbose [force | [recovery-mode{enable | disable}]] | [diff | force]`

Examples

```
switch# cfg-restore
flash          Copy file from flash.
sftp           Copy file from SFTP Server.
tftp          Copy file from TFTP Server.

switch# cfg-restore flash
FILE-NAME      Name of the backup configuration file to restore into the running
               configuration.

switch# cfg-restore flash config_file
diff           Provide the list of changes that will be applied on the
               running configuration.

force          Apply the configuration with reboot if the
               configuration has reboot required commands or
               system-wide change commands present.

non-blocking   Config restoration in non-blocking mode.
recovery-mode  To enable/disable recovery-mode.
verbose        Provide the details of config restore status and the list of commands to be added
               or deleted.

switch# cfg-restore tftp
HOSTNAME-STR   Specify hostname of TFTP Server.
IP-ADDR        IP Address of the TFTP Server.
IPV6-ADDR      IPV6 Address of the TFTP Server.

switch# cfg-restore tftp 10.100.0.12
FILE-NAME      Name of the backup configuration file to restore into the running
               configuration.

switch# cfg-restore tftp 10.100.0.12 config_file
diff           Provide the list of changes that will be applied on the
               running configuration.

force          Apply the configuration with reboot if the
               configuration has reboot required commands or
```

```

non-blocking      system-wide change commands present.
recovery-mode    Config restoration in non-blocking mode.
verbose          To enable/disable recovery-mode.
                 Provide the details of config restore status and the list of commands to be added
                 or deleted.

switch(config)# cfg-restore flash add non-blocking
diff             Provide the list of changes that will be applied on
                 the running configuration.

force            Apply the configuration with reboot if the configuration has reboot required commands or
                 system-wide change commands present.

recovery-mode    To enable/disable recovery-mode.

```

Force configuration restore

The `cfg-restore` command fails if a reboot is required. The Configuration restoration is not allowed as the configuration has reboot required commands error is displayed, along with lines requiring a reboot. The force option in the `cfg-restore` command allows a user to force a reboot. The command is: `cfg-restore {flash | tftp | sftp} <FILE-NAME> force.`

Before reboot, `config` is the active configuration. After the device reboots, the backup file becomes the new active configuration.

```

id | act pri sec | name
---+-----+
 1 | *   *   *   | config
 2 |     *   *   | def
 3 |     *   *   | golden_config
 4 |     *   *   |
 5 |     *   *   |

```

```

switch(config)# cfg-restore flash golden_config
Current running-configuration will be replaced with 'golden_config'.
Continue (y/n)? y
Configuration restore is in progress, configuration changes are temporarily
disabled.
Configuration restoration is not allowed as the configuration has reboot required commands.

```

```

switch(config)# show cfg-restore status
Status                : Failed
Config File Name      : golden_config
Source                : Flash
Time Taken            : 5 Seconds
Last Run              : Mon Oct 30 23:03:19 2017

Recovery Mode         : Enabled
Failure Reason        : Reboot required commands present.
Command : console terminal none

```

```

Number of Add Commands : 0
Number of Remove Commands : 1

```

```

Time Taken for Each Phase :
  Calculating diff       : 3 Seconds
  Adding commands        : 0 Seconds
  Removing commands      : 0 Seconds

```

```

switch# cfg-restore flash golden_config force
Device may be rebooted if the configuration file has reboot required or
system-wide change commands. Do you want to continue (y/n)?
Current running-configuration will be replaced with 'golden_config'.
Continue (y/n)?
Configuration restore is in progress, configuration changes are temporarily
disabled.

```

```

Successfully applied configuration 'golden_config' to running configuration.

```

```

Rebooting switch...

```

In the preceding output, Command : console terminal none shows that `cfg-restore` failed because a reboot is required.

After the switch reboots and comes up, the `golden_config` becomes the active configuration.



NOTE: In case of a switch reboot, the switch comes up with the configuration associated with the primary or secondary.

```
id | act pri sec | name
-----
 1 |      *  *  | config
 2 |      *  *  | def
 3 | *      *  | golden_config
 4 |      *  *  |
 5 |      *  *  |

switch# show cfg-restore status
Status                : Success
Config File Name      : default
Source                : Flash
Time Taken             : 1 Seconds
Last Run              : Mon Oct 23 07:17:03 2017

Recovery Mode         : Enabled
Failure Reason        : -

Number of Add Commands : 0
Number of Remove Commands : 5

Time Taken for Each Phase :

    Calculating diff      : 1 Seconds
    Adding commands       : 0 Seconds
    Removing commands      : 0 Seconds
```



NOTE: Time taken for adding and deleting commands is zero, as the switch reboots. It is similar to downloading a startup-configuration to the device.

cfg-restore non-blocking

Syntax

```
cfg-restore {flash | tftp | sftp} <FILE-NAME> non-blocking
```

Description

Performs restore in non-blocking mode.

Command context

```
config
```

Example

```
switch(config)# cfg-restore flash add non-blocking
Current running-configuration will be replaced with 'add'.
Continue (y/n)? y
Configuration restore is in progress, configuration changes are
temporarily disabled.
switch(config)#
```

```

switch(config)# show cfg-restore status
Status                : Success
Config File Name      : add
Source                : Flash
Time Taken            : 2 Seconds
Last Run              : Sun Oct 22 22:09:02 2017

Recovery Mode        : Enabled
Failure Reason       : -

Number of Add Commands : 7
Number of Remove Commands : 10

Time Taken for Each Phase :
  Calculating diff      : 1 Seconds
  Adding commands       : 0 Seconds
  Removing commands     : 0 Seconds

```

cfg-restore recovery-mode

Syntax

```
cfg-restore {flash | tftp | sftp} <FILE-NAME> recovery-mode {enable | disable}
```

Description

Restores the current running configuration, if a restore to the backup configuration fails. By default, recovery-mode is enabled.

Command context

```
config
```

Usage

To disable recovery mode, use `cfg-restore {flash | tftp | sftp} <FILE-NAME> recovery-mode disable`.

Example

With the following running configuration, a restore to the backup file `modify` fails, but this configuration will be retained as recovery mode is enabled.

```

switch(config)# show running-config

Running configuration:

; JL255A Configuration Editor;
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba
hostname "switch"
module 1 type jl255a
snmp-server community "public" unrestricted
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-28
  ip address dhcp-bootp
  exit
vlan 10
  name "VLAN10"
  no ip address
  exit

```

```
switch(config)# show config modify
; JL255A Configuration Editor;
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba
hostname "switch"
module 1 type jl255a
ip default-gateway 172.20.0.1
snmp-server community "public" unrestricted
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-28
    ip address dhcp-bootp
    exit
vlan 100
    name "VLAN100"
    no ip address
    exit
```

```
switch(config)# cfg-restore flash modify
Current running-configuration will be replaced with 'modify'.
Continue (y/n)? y
Configuration restore is in progress, configuration changes are
temporarily disabled.
```

```
Configuration restore to config 'modify' failed, restored source
configuration to running configuration.
```

```
switch(config)# show running-config
```

```
Running configuration:
```

```
; JL255A Configuration Editor;
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba
hostname "switch"
module 1 type jl255a
snmp-server community "public" unrestricted
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-28
    ip address dhcp-bootp
    exit
vlan 10
    name "VLAN10"
    no ip address
    exit
```

```
switch(config)# cfg-restore flash modify recovery-mode disable
Current running-configuration will be replaced with 'modify'.
Continue (y/n)? y
Configuration restore is in progress, configuration changes are
temporarily disabled.
```

```
Partially applied configuration 'modify' to running configuration.
```

```
switch(config)# show running-config
```

```
Running configuration:
```

```
; JL255A Configuration Editor;
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba
hostname "switch"
module 1 type jl255a
snmp-server community "public" unrestricted
vlan 1
    name "DEFAULT_VLAN"
```



```
untagged 1-28
ip address dhcp-bootp
exit
vlan 100
name "VLAN100"
no ip address
exit
```

cfg-restore verbose

Syntax

```
cfg-restore {flash | tftp | sftp} <FILE-NAME> verbose
```

Description

Provides the details of configuration restore status and the list of commands to be added or deleted along with `cfg-restore`.

Command context

```
config
```

Examples

```
switch(config)# cfg-restore flash config verbose
Current running-configuration will be replaced with 'config'.
Continue (y/n)? y
```

Configuration restore is in progress, configuration changes are temporarily disabled.

Configuration Restore Information:

```
Status                : Success
Config File Name      : config
Source                : Flash
Time Taken             : 6 Seconds
Last Run               : Tue Nov  7 03:43:07 2017
```

```
Recovery Mode         : Enabled
Failure Reason        : -
```

```
Number of Add Commands : 0
Number of Remove Commands : 12
```

```
Time Taken for Each Phase :
  Calculating diff       : 2 Seconds
  Adding commands        : 0 Seconds
  Removing commands      : 0 Seconds
```

Configuration delete list:

```
vlan 2
name "VLAN2"
no ip address
exit
vlan 3
name "VLAN3"
no ip address
exit
vlan 4
name "VLAN4"
no ip address
```

```
exit
vlan 5
  name "VLAN5"
  no ip address
exit
```

Successfully applied configuration 'config' to running configuration.

cfg-restore config_bkp

Syntax

```
cfg-restore {tftp <ip-address> | sftp <ip-address>} config_bkp
```

Description

Downloads and restores a configuration from the TFTP or SFTP server, without rebooting the switch.



NOTE: The commands from the restored configuration will be executed on the running configuration. The name of the current active configuration will not change after a configuration restore.

Command context

```
config
```

Example

```
switch(config)# cfg-restore tftp
HOSTNAME-STR      Specify hostname of TFTP Server.
IP-ADDR           IP Address of the TFTP Server.
IPV6-ADDR         IPV6 Address of the TFTP Server.

switch(config)# cfg-restore sftp
HOSTNAME-STR      Specify hostname of the SFTP server.
IP-ADDR           IP Address of the SFTP Server.
IPV6-ADDR         IPV6 Address of the SFTP Server.
user              Specify username on the remote system information
USER@IP-STR       Specify username along with remote system
                  information

switch(config)# cfg-restore tftp 10.100.0.12 pvos/tftp_2930_config_file
Current running-configuration will be replaced with 'tftp_2930_config_file'.
Continue (y/n)? y
Configuration restore is in progress, configuration changes are temporarily disabled.

Successfully applied configuration 'tftp_2930_config_file' to running configuration.

switch(config)# sh cfg-restore status
Status            : Success
Config File Name  : tftp_2930_config_file
Source            : TFTP
Time Taken        : 4 Seconds
Last Run          : Wed Nov  8 21:11:10 2017

Recovery Mode     : Enabled
Failure Reason    : -

Number of Add Commands : 4
Number of Remove Commands : 7

Time Taken for Each Phase :
  Calculating diff      : 1 Seconds
  Adding commands       : 0 Seconds
```

```

Removing commands      : 0 Seconds

switch(config)# show config files

Configuration files:

id | act pri sec | name
---+-----+-----
 1 | *   *   *   | config
 2 |           |
 3 |           |
 4 |           |
 5 |           |

```

Configuration restore with force option

Prerequisites

Back up the configuration using traditional `copy config` or `cfg-backup` commands.

Procedure

1. Execute the `show config files` command. By default, the `config` file provides all the associations.

```

switch(config)# show config files

Configuration files:

id | act pri sec | name
---+-----+-----
 1 | *   *   *   | config
 2 |           | file1
 3 |           | file2
 4 |           |
 5 |           |

```

2. Use `cfg-restore flash file1 force` command to see the configuration of file1.

```
switch(config)# cfg-restore flash file1 force
```

As the `file1` configuration requires a reboot, a system reboot occurs. When the switch comes up, `file1` is the new active configuration.

```

switch(config)# sh config files

Configuration files:

id | act pri sec | name
---+-----+-----
 1 |           *   * | config
 2 | *           | file1
 3 |           | file2
 4 |           |
 5 |           |

```



NOTE: During a configuration restore with reboot, the association changes. To make the configuration as a default configuration for subsequent system reboots, use `startup-default [<primary|secondary>] config FILENAME` command.

For `startup-default config file1`:

```
switch(config)# show config files
```

```
Configuration files:
```

```
id | act pri sec | name
---+-----+---
1 |          | config
2 | * * *      | file1
3 |          | file2
4 |          |
5 |          |
```

System reboot commands

Following commands require a system reboot:

- `secure-mode standard`
- `secure-mode enhanced`
- `mesh id [0-9]`
- `mesh [a-z | A-Z | 0-9]`
- `max-vlans <257-4094>`
- `no allow-v2-modules`
- `qinq (mixedvlan | svlan)`
- `qos queue-config`
- `terminal type (vt100 | ansi)`
- `console (flow-control | terminal)`
- `vsf member [0-9]`
- `vsf remove`
- `access-list grouping`
- `console baud-rate (speed-sense | 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200)`

Systemwide change commands

Following commands change the system configuration:

- `module [0-9 | a-z | A-Z]`
- `module [0-9 | a-z | A-Z] type <type>`
- `igmp lookup-mode ip`
- `flexible-module [a-z | A-Z] type <type>`
- `stacking member [0-9] flexible-module [a-z | A-Z] type <type>`

Configuration restore without force option

If the two configuration files backed up are file1 and file2:

Prerequisites

Backup the configuration using either the traditional `copy config` or the `cfg-backup` commands.

Procedure

1. Execute the `show config files` command. By default, the `config` file provides all the associations.

```
switch(config)# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*	*	config
2				file1
3				file2
4				
5				

2. Use `cfg-restore flash file1` command to see the configuration of file1.

```
switch(config)# cfg-restore flash file1
```

Even after executing the previous command, associations will remain the same, but the running configuration is replaced by `file1` configuration.



NOTE: In a configuration restore without reboot, the association remains the same. The default `config` file is updated based on the configuration of the restored file.

show cfg-restore status

Syntax

```
show cfg-restore status
```

Description

Shows the status of latest restore performed. The running configuration is updated based on the configuration of the restored file.

Command context

```
config
```

Usage

```
show cfg-restore {status | latest-diff}
```

This command provides information on:

- how a restore is performed
- whether a flash file was used from SFTP or TFTP server
- the total time taken to restore
- the time when last restore was initiated
- whether a recovery-mode was enabled
- the number of add and delete commands

- reboot commands present (if any), and
- the split time taken for each phase

Examples

```
switch(config)# show cfg-restore
latest-diff           Shows the difference between running and back-up
                      configuration.
status               Show configuration restoration status.

switch(config)# show cfg-restore status
Status               : [Failed| In progress | Success | Not Started]
Config File name    : def
Source              : [-|Tftp|sftp|Flash|REST]
Time taken          : [-|20 Seconds.]
Last Run            : [-|Tue March 07 22:12:16 2017.]

Recovery Mode       : Enabled
Failure Reason      : -

Number of Add Commands : 0
Number of Remove Commands : 3

Time Taken for Each Phase :
  Calculating diff      : 1 Seconds
  Adding commands       : 0 Seconds
  Removing commands     : 0 Seconds
```

If the configuration restoration fails, the line number and the failed commands are displayed:

```
switch(config)# show cfg-restore status
Status               : Failed
Config File name    : def
Source              : Flash
Time taken          : 20 Seconds
Last Run            : Sun Oct 22 20:22:54 2017

Recovery Mode       : Enabled
Failure Reason      : Add commands have been failed

Number of Add Commands : 0
Number of Remove Commands : 3

Time Taken for Each Phase :
  Calculating diff      : 1 Seconds
  Adding commands       : 0 Seconds
  Removing commands     : 0 Seconds

Failed to remove commands:
  Line: 12 vlan 10
  Line: 15 no ipv6 nd snooping mac-check
Failed to add commands:
  Line: 10 icmp 10.100.0.12 source-inter vlan 1
  Line: 20 udp-echo 10.100.0.12 source vlan 1
```



NOTE: The number of add and delete commands is calculated excluding the `exit` commands in the configuration file.

Viewing the differences between a running configuration and a backup configuration

Prerequisites

Use the `cfg-restore {flash | tftp | sftp} <FILE-NAME> diff` command to view the list of configuration changes that are removed, modified, or added to the running configuration.

Procedure

1. Execute the `show running-config` command to show the running configuration of the switch.

```
switch(config)# show running-config

Running configuration:

; JL255A Configuration Editor;
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba
hostname "switch"
module 1 type jl255a
snmp-server community "public" unrestricted
vlan 1
    name "DEFAULT_VLAN"
    no untagged 11-13,15-18
    untagged 1-10,14,19-28
    ip address dhcp-bootp
    exit
vlan 100
    name "VLAN100"
    untagged 11-13
    no ip address
    exit
vlan 300
    name "VLAN300"
    untagged 15-18
    no ip address
    exit
```

2. Execute the `show config golden_config` command to show the backup configuration of the switch.

```
switch(config)# show config golden_config
; JL255A Configuration Editor;
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba
hostname "switch"
module 1 type jl255a
; JL255A Configuration Editor;
; Ver #12:08.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:ba
hostname "switch"
module 1 type jl255a
```

3. Execute the `cfg-restore flash golden_config diff` command to view the differences that will be applied.

```
switch# cfg-restore flash golden_config diff

Configuration delete list:

vlan 1
    no untagged 11-13,15-18
    untagged 3-10
```

```

exit
vlan 100
  untagged 11-13
  exit
vlan 300
  name "VLAN300"

  untagged 15-18
  no ip address
  exit

```

Configuration add list:

```

vlan 1
  no untagged 3-10
  untagged 11-13,15-18
  exit
vlan 100
  untagged 3-5
  exit
vlan 200
  name "VLAN200"
  untagged 6-10
  no ip address
  exit

```



NOTE: If the running and the backup configuration is the same, no difference will be displayed.

```
switch(config)# cfg-restore flash modify diff
```

```
Current config and backup config is identical.
```

4. Execute the `show cfg restore latest-diff` command to display the difference between the running and the backup configuration.

```

switch(config)# show cfg-restore
latest-diff      Shows the difference between running and back-up
                  configuration.
status           Show configuration restoration status.

```

```
switch(config)# show cfg-restore latest-diff
```

Configuration delete list:

```

ip default-gateway 172.20.0.1
vlan 100
  name "VLAN100"
  no ip address
  exit

```

Configuration add list:

```

vlan 10
  name "VLAN10"
  no ip address
  exit

```

```
switch(config)#
```


Show commands to show the SHA of a configuration

The `show` commands provide SHA details of the running and startup configurations.

show hash

Syntax

```
show {config | running-config} hash {recalculate}
```

Description

Shows SHA ID of startup or running configuration.

Command context

config

Examples

```
switch# show config
config
files          List saved configuration files.
hash           Display the hash calculated for the startup
               configuration.
interface      Show the startup configuration for interfaces.
oobm           Show the startup configuration for OOBM.
```

To display the hash calculated for the startup configuration:

```
switch(config)# show config hash
The hash must be calculated.  This may take several minutes.

Continue (y/n)? y

Calculating hash...
Startup Configuration hash:

4f66 8b77 6b66 e5fb 0c12 f7fb 8ea6 b548 af2e 2e03

This hash is only valid for comparison to a baseline hash if
the configuration has not been explicitly changed (such as
with a CLI command) or implicitly changed (such as by the
removal of a hardware module).

switch(config)# show config hash
recalculate      Calculate hash (if needed) without prompting.

switch(config)# show config hash recalculate
Startup Configuration hash:

4f66 8b77 6b66 e5fb 0c12 f7fb 8ea6 b548 af2e 2e03

This hash is only valid for comparison to a baseline hash if
the configuration has not been explicitly changed (such as
with a CLI command) or implicitly changed (such as by the
removal of a hardware module).
```

To display the hash calculated for the running configuration:

```
switch(config)# show running-config hash
The hash must be calculated. This may take several minutes.

Continue (y/n)? y

Calculating hash...
Running configuration hash:

6d88 0880 98af e8a8 b564 15cd 368e 4269 9d61 4bfa

This hash is only valid for comparison to a baseline hash if
the configuration has not been explicitly changed (such as
with a CLI command) or implicitly changed (such as by the
removal of a hardware module).
```

Scenarios that block the configuration restoration process

The configuration restoration process is blocked in the following scenarios:

- If the restored configuration file requires a reboot.
- If the restored configuration changes the entire configuration (for example, module add or remove).

More information

[cfg-restore](#) on page 459

Limitations

Switch configuration restore without reboot feature does not support the following scenarios:

- Removing a physically present member through `cfg-restore` command
- Flex-module provisioning or removal on standalone or a stack
- Module provisioning or removal on standalone or a stack
- Adding a VLAN when the VLAN limit is already reached by having dynamic VLANs. Due to timing issues, ports or dynamic VLANs take some time to become offline or be removed, even after applying a removal command. In such a case, restore commands fail as normal CLI commands.
- The maximum number of backup configuration files has been increased from three to five. When the firmware is downgraded to lower versions, the `show config files` command displays the details to only three configuration files.
- Restore is allowed based on the available system resource factors.

Blocking of configuration from other sessions

All `write` operations are not allowed from other sessions (CLI/WebUI/SNMP/REST, and so on) during a configuration restoration process. Only `read` operation is allowed. Attempts to use `write` operation results in the Configuration restore is in progress, configuration changes are temporarily disabled error. The following `show` commands are blocked during a configuration restoration process:

- `show-tech`
- `show config`

- show running-config
- show startup-config

Troubleshooting and support

Switch configuration restore without reboot feature provides CLI support to:

- display the number of commands with line number that failed to restore.
- display the delta between running configuration and the configuration to be restored.

More information

[Viewing the differences between a running configuration and a backup configuration on page 471](#)
[show cfg-restore status on page 469](#)

debug cfg-restore

Syntax

```
debug cfg-restore
```

Description

Debug logs display the commands executed by `cfg-restore`.

Command context

config and manager

Example

```
switch(config)# debug cfg-restore
switch(config)# debug destination buffer
switch(config)# show debug buffer
0000:01:39:51.58 CFG mCfgRestoreMgr:cfg-restore to config file "backup_conif"
    started.
0000:01:39:56.45 CFG mCfgRestoreMgr:cfg-restore diff calculated, number of
    commands to add =0 number of commands to delete = 3.
0000:01:39:56.45 CFG mCfgRestoreMgr:cfg-restore iteration count = 1.
0000:01:39:56.51 CFG mCfgRestoreMgr:Command executed = no vlan 2 tagged 9,
    Status = Success.
0000:01:39:56.51 CFG mCfgRestoreMgr:Command deleted = vlan 2 tagged 9.
0000:01:39:56.58 CFG mCfgRestoreMgr:Command executed = no vlan 3 tagged 9,
    Status = Success.
0000:01:39:56.58 CFG mCfgRestoreMgr:Command deleted = vlan 3 tagged 9.
0000:01:39:56.64 CFG mCfgRestoreMgr:Command executed = no vlan 4 tagged 9,
    Status = Success.
0000:01:39:56.65 CFG mCfgRestoreMgr:Command deleted = vlan 4 tagged 9.
0000:01:39:56.65 CFG mCfgRestoreMgr:cfg-restore iteration count = 2.
0000:01:39:59.38 CFG mCfgRestoreMgr:Successfully applied configuration
    'backup_conif' to running configuration.
** Total debug messages = 22
```

Virtual Technician is a set of tools aimed at aiding network switch administrators in diagnosing and caring for their networks. VT provides tools for switch diagnoses when faced with unforeseen issues.

To improve the Virtual Technician features of our devices have added the following tools:

- Cisco Discovery Protocol
- Enabling Debug tracing for MOCANA code
- User diagnostic crash via front panel security button
- User diagnostic crash via the serial console

Cisco Discovery Protocol (CDP)

Show cdp traffic

Syntax

```
show cdp traffic
```

Description

Displays the number of Cisco Discovery Protocol (CDP) packets transmitted, received and dropped.

CDP frame Statistics

Port No	Transmitted Frames	Received Frames	Discarded Frames	Error Frames
A1	46	26	6	7
A2	30	35	7	9
A3	120	420	670	670

Clear cdp counters

Syntax

```
clear cdp counters
```

Description

Allows a user to clear CDP statistics.

Clear cdp counters

Port No	Transmitted Frames	Received Frames	Discarded Frames	Error Frames
A1	46	26	6	7

A2	30	35	7	9
A3	120	420	670	670

show cdp neighbors detail

Syntax

```
show cdp neighbors detail
```

Description

Shows CDP neighbors on specified port only.

```
show cdp neighbor detail
```

```
CDP neighbors information
```

```

Port : 1/13
Device ID : 0.0.0.0
Address Type : IP
Address      : 0.0.0.0
Platform    :
Capability   : Switch
Device Port  : 00 1b 4f 49 e7 76
Version     :

```

```

-----
Port : 2/25
Device ID : 94 18 82 55 50 20
Address Type : IP
Address      : 172.31.99.143
Platform    : Aruba JL356A 2540-24G-PoE+-4SFP+ Switch, revision YC.16....
Capability   : Switch
Device Port  : 3
Version     : Aruba JL356A 2540-24G-PoE+-4SFP+ Switch, revision YC.16....

```

Enable/Disable debug tracing for MOCANA code

Debug security

Syntax

```
debug security ssl
```

Description

Enables the debug tracing for MOCANA code.

Use the no parameter to disable debug tracing.

ssl

Display all SSL messages.

User diagnostic crash via Front Panel Security (FPS) button

Allows the switch's front panel **Clear** button to manually initiate a diagnostic reset. In the case of an application hang, this feature allows you to perform reliable diagnostics by debugging via the front panel **Clear** button. Diagnostic reset is controlled via Front Panel Security (FPS) options.

Front panel security password-clear

From the configure context:

Syntax

```
no front-panel-security password-clear <RESET-ON-CLEAR> | factory-reset | password-recovery | diagnostic-reset <CLEAR-BUTTON | SERIAL-CONSOLE>
```

Description

Enable the ability to clear the password(s) and/or configuration via the front panel buttons.

no disables the password clear option.

Parameters

- If `password-clear` is disabled, the password(s) cannot be reset using the clear button on the front panel of the device.
- If `factory-reset` is disabled, the configuration/password(s) can not be reset using the clear and reset button combination at boot time.
- When `password-recovery` is enabled (and the front panel buttons disabled), a lost password can be recovered by contacting customer support.
- When `password-recovery` is disabled, there is no way to access a device after losing a password with the front panel buttons disabled.
- If `diagnostic-reset` is disabled, the user cannot perform a diagnostic switch reset on those rare events where the switch becomes unresponsive to user input because of unknown reason(s).
- If `diagnostic-reset` is enabled, the user can perform a diagnostic hard reset which will capture valuable diagnostic data and reset the switch.

Parameters

factory-reset

Enable/Disable factory-reset ability.

password-clear

Enable/Disable password clear.

password-recovery

Enable/Disable password recovery.

diagnostic-reset

Enable/Disable diagnostic reset.

Front-panel-security diagnostic-reset

From the configure context:

Syntax

```
front-panel-security diagnostic-reset <CLEAR-BUTTON | SERIAL-CONSOLE>
```

Description

Enables the diagnostic reset so that the switch can capture diagnostic data.

- To initiate diagnostic reset via the clear button, press the clear button for at least 30 seconds but not more than 40 seconds.
- To initiate diagnostic switch reset via the serial console, enter the diagnostic reset sequence on the serial console.

Parameters

Clear button

Enables the diagnostics by choosing the clear button option.

Serial console

Enables the diagnostics by choosing the serial console option.

no front-panel-security diagnostic-reset

From the configure context:

Syntax

```
no front-panel-security diagnostic-reset
```

Description

Disables the diagnostic reset feature so that the user is prevented from capturing diagnostic data and performing a diagnostic reset on the switch. Both the sub-options `reset-via-serial-console` and `reset-via-clear-button` will be disabled. This is necessary if the switch becomes unresponsive (hangs) for unknown reasons.

No front-panel-security diagnostic-reset

```
no front-panel-security diagnostic-reset
```

Clear Password	- Enabled
Reset-on-clear	- Disabled
Factory Reset	- Enabled
Password Recovery	- Enabled
Diagnostic Reset	- Disabled



CAUTION:

Disabling the diagnostic reset prevents the switch from capturing diagnostic data on those rare events where the switch becomes unresponsive to user input because of unknown reasons. Ensure that you are familiar with the front panel security options before proceeding.

Front-panel-security diagnostic-reset clear-button

From the configure context:

Syntax

```
front-panel-security diagnostic-reset clear-button
```

Description

This command will enable diagnostic-reset via clear button. The user will be allowed to perform diagnostic reset by depressing the clear button for 30 seconds and not more than 40 seconds.

Front-panel-security diagnostic-rest clear-button

```
front-panel-security diagnostic-rest clear-button
```

```
Diagnostic Reset      - Enabled
clear-button         - Enabled
serial-console       -Disabled
```



CAUTION:

Disabling the diagnostic reset prevents the switch from capturing diagnostic data on those rare events where the switch becomes unresponsive to user input because of unknown reasons. Ensure that you are familiar with the front panel security options before proceeding.

no front-panel-security diagnostic-reset clear-button

From the configure context:

Syntax

```
no front-panel-security diagnostic-reset clear-button
```

Description

Disables the diagnostic-reset via clear button.



CAUTION:

Disabling the diagnostic reset prevents the switch from capturing diagnostic data on those rare events where the switch becomes unresponsive to user input because of unknown reasons. Ensure that you are familiar with the front panel security options before proceeding.

Show front-panel-security

Syntax

```
show front-panel-security
```

Parameters



Show front-panel-security

```
Clear Password      - Enabled
Reset -on-clear     - Disabled
Factory Reset       - Enabled
Password Recovery   - Enabled
Diagnostic Reset     - Enabled
```




NOTE: By default, user initiated diagnostic reset is enabled.

Diagnostic table

To accomplish this	Do this	Result
Soft Reset (Standalone switch)	Press and release the Reset button	The switch operating system is cleared gracefully (such as data transfer completion, temporary error conditions are cleared), then reboots and runs self tests.
Hard Reset (Standalone switch)	Press and hold the Reset button for more than 5 seconds (until all LEDs turn on), then release.	The switch reboots, similar to a power cycle. A hard reset is used, for example, when the switch CPU is in an unknown state or not responding.
Delete console and management access passwords	Press Clear for at least one second, but not longer than 5 seconds.	The switch deletes all access password.
Restore the factory default configuration	<ol style="list-style-type: none"> 1. Press Clear and Reset simultaneously. 2. While continuing to press Clear, release Reset. 3. When the Test LED begins blinking (after approximately 25 seconds), release Clear. 	The switch removes all configuration changes, restores the factory default configuration, and runs self test.
Diagnostic reset	<ol style="list-style-type: none"> 1. Press Clear to 30–40 seconds. 2. When the test LED begins blinking (approximately after 30 seconds), release Clear. <div style="margin-top: 10px;">  <p>NOTE: Releasing the Clear button when TEST LED is not blinking (approximately after 40 seconds) will not honor the diagnostic reset request.</p> </div>	This initiates diagnostic reset, collects diagnostic information, and reboots the switch.
<div style="margin-top: 10px;">  <p>NOTE: These buttons are provided for the user's convenience. If switch security is a concern, ensure that the switch is installed in a secure location, such as a locked writing closet. To disable the buttons, use the <code>front-panel-security</code> command.</p> </div>		

FPS Error Log

Event	Message
RMON_BOOT_CRASH_RECORD1	<p>Diagnostic reset sequence detected on serial console; user has initiated diagnostic reset.</p> <p>On detection on local serial</p>
RMON_BOOT_CRASH_RECORD1	<p>SMM: Diagnostic reset sequence detected on serial console; user has initiated diagnostic reset.</p> <p>On detection on SMM serial console and signaled to AMM</p>
RMON_BOOT_CRASH_RECORD1	<p>STKM: Diagnostic reset sequence detected on serial console; user has initiated diagnostic reset.</p> <p>On detection on non-commander serial console and signaled to commander</p>
RMON_BOOT_CRASH_RECORD1	<p>User has initiated diagnostic reset via the serial console.</p> <p>Sw_panic() message</p>
RMON_BOOT_CRASH_RECORD1	<p>SMM: User has initiated diagnostic reset via the serial console.</p> <p>Sw_panic() message when triggered via SMM</p>
RMON_BOOT_CRASH_RECORD1	<p>STKM: User has initiated diagnostic reset via the serial console.</p> <p>Sw_panic() message when triggered via non-commander</p>

Table Continued

Event	Message
Console print	<p>STKM: HA Sync in progress; user initiated diagnostic request via the serial console rejected. Retry after sometime.</p> <p>Printed on the device console. When standby is in sync state, we don't want to crash the commander. So we report to the user to retry later</p>
Console print	<p>STKM: Member is booting; user initiated diagnostic request via the serial console rejected. Retry after sometime.</p> <p>Printed on the device console. When the member is till booting, it doesn't have the commander member number, thus we can't issue UIDC on the commander. So we report to the user to retry later.</p>

User initiated diagnostic crash via the serial console

Remotely triggers a diagnostic reset of the switch via a serial console. This reset reboots the switch and collects diagnostic data for debugging an application hang, a system hang or any other rare occurrence. Diagnostic reset is controlled via FPS options.

The serial sequence to initiate the User Initiated Diagnostic Reset via Serial console is Ctrl+S, Ctrl+T, Ctrl+Q, Ctrl+T, Ctrl+S.

Front-panel-security diagnostic-reset serial-console

In the configure context:

Syntax

```
front-panel-security diagnostic-reset serial-console
```

Enables the diagnostic-reset via serial console. Allows the user to perform diagnostic reset by keying-in diagnostic reset sequence.

Front-panel-security diagnostic-reset serial-console

```
front-panel-security diagnostic-reset serial-console
```

```
Diagnostic Reset      - Enabled
clear-button         - Disabled
serial-console       - Enabled
```

no front-panel-security diagnostic-reset serial-console

In the configure context:

Syntax

```
no front-panel-security diagnostic-reset serial-console
```

Description

Disables the diagnostic-reset via serial console.

No front-panel-security diagnostic-reset serial-console

```
no front-panel-security diagnostic-reset serial-console
```

Diagnostic Reset - Disabled



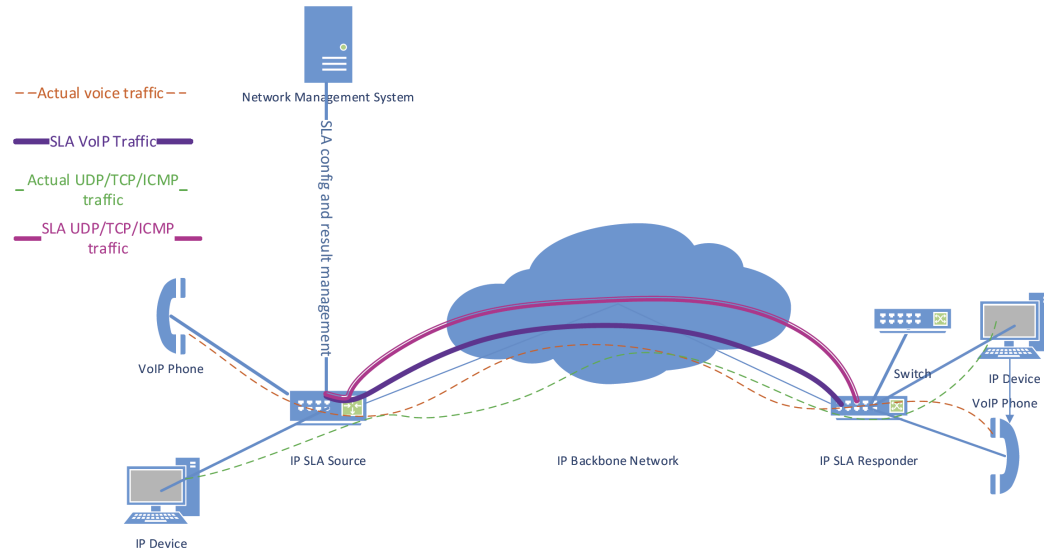
CAUTION: Disabling the diagnostic reset prevents the switch from capturing diagnostic data on those rare events where the switch becomes unresponsive to user input because of unknown reasons. Ensure that you are familiar with the front panel security options before proceeding.

Serial console error messages

Error	Message
RMON_BOOT_CRASH_RECORD1	Diagnostic reset sequence detected on serial console; user has initiated diagnostic reset.
RMON_BOOT_CRASH_RECORD1	SMM: Diagnostic reset sequence detected on serial console; user has initiated diagnostic reset.
RMON_BOOT_CRASH_RECORD1	STKM: Diagnostic reset sequence detected on serial console; user has initiated diagnostic reset.
RMON_BOOT_CRASH_RECORD1	User has initiated diagnostic reset via the serial console.
RMON_BOOT_CRASH_RECORD1	SMM: User has initiated diagnostic reset via the serial console.
RMON_BOOT_CRASH_RECORD1	STKM: User has initiated diagnostic reset via the serial console.
Console print	STKM: HA Sync in progress; user initiated diagnostic request via the serial console rejected. Retry after sometime.
Console print	STKM: Member is booting; user initiated diagnostic request via the serial console rejected. Retry after sometime.

Overview

IP Service Level Agreement (IP SLA) is a feature that helps administrators collect information about network performance in real time. With increasing pressure on maintaining agreed-upon Service Level Agreements on Enterprises and ISPs alike, IP SLA serves as a useful tool.



Any IP SLA test involves a source node and a destination node. For all discussions in this document, the source is always an ArubaOS-switch with IP SLA support. As shown in the diagram above, a destination can, in most cases, be any IP-enabled device. For some SLA types that expect a nonstandard response to a test packet, an “SLA responder” must be configured. An “SLA responder” is nothing but an ArubaOS-switch with IP SLA configurations on it that enable it to respond to the test packet.

The IP SLA feature provides:

- Application-aware monitoring that simulates actual protocol packets.
- Predictable measures that aid in ease of deployment and help with assessment of existing network performance.
- Accurate measures of delay and packet loss for time-sensitive applications.
- End-to-end measurements to represent actual user experience.

We support the following SLA types:

- UDP Echo, including connectivity testing of transport layer (UDP) services, Round-Trip-Time (RTT) measurement, one-way delay, and packet loss details.
- ICMP Echo, including connectivity testing, RTT measurement, and packet loss details.
- TCP Connect, including connectivity testing of transport layer (TCP) services, and handshake time measurement.
- DHCP, which measures the round-trip time taken to discover a DHCP Server and obtain a leased IP address from it.

- DNS, which measures the time taken for a DNS resolution. This measures the difference between the time taken to send a request to the DNS server and the time the IP SLA source receives a reply.
- User Datagram Protocol (UDP) Jitter, which measures RTT, one way jitter and one way delays.
- UDP Jitter for VoIP, which measures RTT, one way jitter, one way delays, ICPIF (Impairment Calculated Planning Impairment Factor) and MOS (Mean Opinion Score).

Limitations for IPSLA support on Aruba switches:

- IP SLA is not enabled for IPv6.
- DHCP SLA supports DHCPv4 only.
- IP SLA tests cannot be initiated over OOBM interfaces.
- History results for the configured IP SLAs will not be available after a switchover or a reboot.
- Maximum number of IP SLAs that can be configured varies based on the type of SLA test.
- When there are multiple IP SLAs configured with destination as hostname, the DNS resolution happens serially. There can be a delay in sending the test probe (which will be sent only after successful DNS resolution).
- For TCP Connect SLA type, the four-tuple (source IP/port, destination IP/port) must be unique.
- System clocks between the source and the responder must be synchronized with NTP if One Way Delay parameters have to be calculated for UDP Echo tests.
- Timeout for probes is 3 seconds for all SLA types and is not configurable.
- Transient spikes in RTT occur during the tests (in the source and the responder) if processor usage is high. Consider average result values over a period of time rather than point-in-time results. This is not applicable for UDP Jitter nor Jitter for VoIP.

Entity	Limit
Maximum number of SLAs enabled.	50
Maximum history bucket size per SLA. ¹	50
Number of responders that can be configured.	10

¹ Not applicable for UDP Jitter and Jitter for VoIP.

The following are operational restrictions with respect to IP SLA jitter implementation:

- Feature is supported only on v3-based platforms.
- No history results are stored.
- IPSLA Jitter and Jitter for VoIP initiator and responder is only supported on 5400R with v3 modules (noncompatibility mode), 3810, and 2930F switches.
- The maximum number of Jitter responder sessions (UDP Jitter + Jitter For VoIP) supported is 10. The maximum number of Jitter initiator sessions (UDP Jitter + Jitter For VoIP) supported is 5.

- IMC (Intelligent Management Center) supports below IP SLA:
 - DHCP
- Measurement of RTT and jitter values is in milliseconds.
- IPv6 SLA for UDP jitter and VoIP is not supported.
- UDP jitter and UDP jitter for VoIP tests are not supported over Tunnel, Trunk, and OOBM interfaces.
- UDP jitter and UDP jitter for VoIP results are not carried forward across failover or a device reboot.
- History bucket size cannot be configured for UDP jitter and VoIP tests. Results are aggregated for the last 25 probes.
- System clocks between the source and the responder must be synchronized with NTP if One Way Delay parameters have to be calculated for UDP Jitter & UDP Jitter for VoIP tests.
- The UDP jitter and UDP jitter for VoIP feature on ArubaOS-Switch has the following limited interoperability with Comware 7 SLA v2 version:
 - One Way packet drops (SD packet loss and DS packet loss) on the Comware Jitter initiator is not reported when interoperating with Aruba Jitter Responder.
- IP SLA responder or initiator implementation is not interoperable with Cisco's IP SLA feature.

How IP SLA works

1. The source originates a test packet to the destination.
2. The destination responds to the test packet, at times embedding the needed information in the response packet.
3. Upon receiving the response, the source calculates the test results based on the timestamp, other packet parameters, and so on.
4. The source stores the results and updates the history records for the SLA.
5. The source reschedules the SLA for the next run.



NOTE: For one-way delay calculations, the IP SLA sender and IP SLA responder must be NTP Time Synchronized.

Configuration commands

no ip-sla <ID>

Syntax

```
no ip-sla <ID>
```

Description

Configure the IP Service Level Agreement (SLA) parameters. The value of ID can range from 1-255.

Parameters

clear

Clear history records, message statistics, and threshold counters of particular SLA entry.

dhcp

Configure DHCP as the IP SLA test mechanism.

disable

Disable the IP SLA.

dns

Configure DNS as the IP SLA test mechanism.

enable

Enable the IP SLA.

history-size

Configure the number of history records to be stored for the IP SLA.

icmp-echo

Configure ICMP echo as the IP SLA test mechanism.

monitor

Configure monitoring parameters and respective threshold-action values.

schedule

Configure the start time, stop time, lifetime, and frequency of run for the IP SLA.

tcp-connect

Configure TCP connect as the IP SLA test mechanism.

tos

Configure the Type of Service value to be set in the test packet for the IP SLA.

udp-echo

Configure UDP echo as the IP SLA test mechanism.

On platforms that support Jitter and VOIP, the following options are also provided:

udp-jitter

Configure UDP jitter as the IP SLA test mechanism.

udp-jitter-voip

Configure UDP jitter for VoIP as the IP SLA test mechanism.

ip-sla <ID> clear**Syntax**

```
ip-sla <ID> clear
```

Description

Clear history records, message statistics, and threshold counters of a particular SLA entry.

Parameters**records**

Clear history records, message statistics, and threshold counters of particular SLA entry.

no ip-sla <ID> history-size

Syntax

```
no ip-sla <ID> history-size
```

Description

Configure the number of history records to be stored for the IP SLA. The maximum supported size is 50 and the default value for history-size is 25.

no ip-sla <ID> icmp-echo

Syntax

```
no ip-sla <ID> icmp-echo [<IP-ADDR> | <HOST-NAME>] [source <IP-ADDR> | source-interface vlan <VLAN-ID>] [payload-size <SIZE>]
```

Description

Configure ICMP echo as the IP SLA test mechanism. Requires destination address/hostname and source address/vlan id for the IP SLA of ICMP-Echo SLA type.

payload-size

: Value can range from 1-1440. By default, payload-size is not set.

no ip-sla <ID> udp-echo

Syntax

```
no ip-sla <ID> udp-echo [destination [<IP-ADDR> | <HOST-NAME>] <PORT-NUM>] [source <IP-ADDR> | <VLAN-ID>] [payload-size <SIZE>]
```

Description

Configure UDP echo as the IP SLA test mechanism. Requires destination address/hostname and source address/VLAN ID for the IP SLA of UDP-Echo SLA type.

- **PORT-NUM:** Value can range from 1024–65535.
- **payload-size:** Value can range from 1-1440. By default, payload-size is not set.

no ip-sla <ID> tcp-connect

Syntax

```
no ip-sla <ID> tcp-connect [destination [<IP-ADDR> | <HOST-NAME>] <PORT-NUM>] [source [<IP-ADDR> | <VLAN-ID>] <PORT-NUM>]
```

Description

Configure TCP connect as the IP SLA test mechanism. Requires destination address/hostname and source address/VLAN ID for the IP SLA of TCP connect SLA type. The value of PORT-NUM can range from 1024-65535.

ip-sla <ID> monitor threshold-config

Syntax

```
ip-sla <ID> monitor threshold-config [rtt | srcTodstTime | dstToSrcTime]
threshold-type [immediate | consecutive <COUNT>] threshold-value <UPPER-LIMIT>
<LOWER-LIMIT> action-type [trap | log | trap-log | none]

no ip-sla <ID> monitor threshold-config [rtt | srcTodstTime | dstToSrcTime]
threshold-type [immediate | consecutive <COUNT>] threshold-value <UPPER-LIMIT>
<LOWER-LIMIT> action-type [trap | log | trap-log | none]
```

Description

Set upper and lower threshold parameters.

Parameters

- **threshold-type immediate:** Take action immediately when the monitored parameters cross the threshold upper limit (subsequent notifications for upper thresholds are not generated until the parameter values go lower than the configured lower threshold value).
- **threshold-type consecutive:** Take action after threshold is hit consecutively for number of times.
- **action-type:** Describes action to be taken when the upper threshold is crossed.
- **trap:** Send snmp-trap when configured threshold is hit.
- **log:** Only log the event when configured threshold is hit.
- **trap-log:** Send snmp-trap and log the event when configured threshold is hit.
- **none:** Take no action.



NOTE: The command option threshold-config can be individually set for rtt, srcTodstTime, and dstToSrcTime.

no ip-sla <ID> monitor packet-loss

Syntax

```
no ip-sla <ID> monitor packet-loss threshold-type [immediate | consecutive
<COUNT>] action-type [trap | log | trap-log | none]
```

Description

Configure threshold-action values when packet loss happens.

- **threshold-type immediate:** Take action immediately when the monitored parameters cross the threshold upper limit (subsequent notifications for upper thresholds are not generated until the parameter values go lower than the configured lower threshold value).
- **threshold-type consecutive:** Take action after threshold is hit consecutively for number of times.
- **action-type:** Describes action to be taken when the upper threshold is crossed.
- **trap:** Send snmp-trap when configured threshold is hit.
- **log:** Only log the event when configured threshold is hit.
- **trap-log:** Send snmp-trap and log the event when configured threshold is hit.
- **none:** Take no action.

no ip-sla <ID> monitor test-completion

Syntax

```
no ip-sla <ID> monitor test-completion action-type [trap | log | trap-log | none]
```

Description

Configure action to be taken when test gets completed.

- **trap:** Send snmp-trap when configured threshold is hit.
- **log:** Only log the event when configured threshold is hit.
- **trap-log:** Send snmp-trap and log the event when configured threshold is hit.
- **none:** Take no action.

no ip-sla <ID> schedule

Syntax

```
no ip-sla <ID> schedule [[now | startTime <START-TIME>] [forever | stopTime <STOP-TIME> | repetitions <NUM>] [frequency <FREQUENCY>]
```

Description

Configure the start time, stop time, lifetime, and frequency of run for the IP SLA. The default value for the frequency of operation is 60 seconds.

no ip-sla <ID> tos

Syntax

```
no ip-sla <ID> tos <VALUE>
```

Description

Configure the Type of Service value to be set in the test packet for the IP SLA.

Valid values: 0–255

no ip-sla responder

Syntax

```
no ip-sla responder
```

Description

Configure SLA responder to respond to probe packets.

- **IP address:** local interface IP address
- **port:** takes L4 port numbers.
- **SLA types supported:** udp-echo, tcp-connect, UDP Jitter & Jitter For VoIP.

no ip-sla <ID> udp-jitter

Syntax

```
no ip-sla <ID> udp-jitter destination [<IP-ADDR> | <HOST-NAME>] <PORT-NUM> source [<IP-ADDR> | <VLAN-ID>] [payload-size <SIZE> num-of-packets <NUM> packet-interval <PKT-INTERVAL>]
```

Description

Configures the UDP Jitter test.

- **Payload-size:** Payload size of the test packet. Value can range from 68-8100. Default value is 68.
- **Num-of-packets:** Number of packets sent in one probe. Default is 10. Allowed range: 10-1000.
- **Packet-interval:** Inter packet gap in milliseconds. Time between consecutive packets within a probe. Default is 20ms. Allowed range: 10-60000

no ip-sla <ID> udp-jitter-voip

Syntax

```
no ip-sla <ID> udp-jitter-voip destination [<IP-ADDR> | <HOST-NAME>] <PORT-NUM>  
source [<IP-ADDR> | <VLAN-ID>] [codec-type <CODEC-TYPE> advantage-factor <ADV-  
FACTOR>]
```

Description

Configures the UDP Jitter for VoIP test.

- **Codec-type:** Codec to be used to encode the test VoIP packets. Available codecs: g711a, g711u, g729a. Default is g711a.
- **Advantage-factor:** Advantage factor to be configured for the test. Default is 0. Allowed range: 0-20.

Show commands

show ip-sla <ID>

Syntax

```
show ip-sla <ID>
```

Description

Show IP SLA configurations.

Parameters

history

Show the IP SLA results history.

message-statistics

Show the IP SLA message statistics.

results

Show the IP SLA results for UDP Jitter and UDP Jitter VoIP.

aggregated-results

Show the IP SLA aggregated results for UDP Jitter and UDP Jitter VOIP.

show ip-sla <ID>

```
SLA ID: 1  
Status: [Enabled | Admin-disabled | Scheduled | Expired | Running]  
SLA Type: [ICMP-echo | tcp-connect | UDP-echo | DHCP | DNS | udp-jitter | voip]
```

```

Destination Hostname: www.arubanetworks.com
Destination Address : 20.0.0.2
Source Address      : 20.0.0.1
History Bucket Size : 5
TOS: 32
Schedule:
  Frequency (seconds) : 60
  Life                 : [Forever | 144 seconds]
  Start Time          : Tue Oct 27 22:12:16 2015
  Next Scheduled Run Time : Tue Oct 27 22:43:16 2015

Threshold-Monitor is : Enabled
Threshold Config: RTT
Threshold Type : immediate
Upper Threshold : 500 ms
Lower Threshold : 100 ms
Action Type : Trap and Log

Threshold Config: packet-loss
Threshold Type : consecutive (5)
Action Type : Trap

Threshold Config: test-completion
Action Type: None

```

show ip-sla <ID> history

Syntax

```
show ip-sla <ID> history
```

Description

Show the IP SLA results history.

show ip-sla <ID> history

```

SLA ID : 1

SLA Type : UDP-Echo

Minimum RTT (ms)      : 1
Maximum RTT (ms)     : 4294967282
Average RTT (ms)     : 3
Total RTT (ms)       : 315
RTT2 (sum of RTT squared): 63681

Start Time           Status  RTT      Description
-----
Mon Jan 1 00:51:28 1990 Failed -      DMA tail drop detected.
Mon Jan 1 00:51:30 1990 Failed -      SLA disabled before probe response arrived.

```

show ip-sla <ID> message-statistics

Syntax

```
show ip-sla <ID> message-statistics
```

Description

Show the IP SLA message statistics.

show ip-sla <ID> message-statistics

```
SLA ID : 1
Status : Running
SLA Type : UDP-Echo
Destination Address : 10.0.0.2
Source Address : 10.0.0.1
Destination Port : 2000
History Bucket Size : 25
Payload Size : 500
TOS : 0
Messages:
Destination Address Unreachable : 0
Probes Skipped Awaiting DNS Resolution : 0
DNS Resolution Failed : 0
No Route to Target : 0
Internal Error : 0
Local Interface is Down : 0
No Response from Target : 0
Successful Probes Sent : 3
Probe Response received : 3
Possibly Tail Dropped : 0
```

show ip-sla <ID> results

Syntax

```
show ip-sla <ID> results
```

Description

Shows the results for the last IPSLA UDP Jitter or UDP Jitter for VoIP test. Note this command is not valid for any other SLA type.

Switch (config)# sh ip-sla 1 results

```
Test Results for SLA ID: 1
Probe Id           : 10
SLA Type           : UDP-Jitter
Destination IP Address : 10.2.2.2
Destination Port    : 4444
Source IP Address   : 10.2.2.2
Source Port        : 5555

Number of Packets Sent           : 10
Number of Packets Received       : 10
Minimum Round Trip Time         : 15
Maximum Round Trip Time         : 32
Average Round Trip Time         : 17
Square-Sum of Round Trip Time   : 3235
Last Succeeded Probe Time       : 2008-05-29 13:56:17.6

Extended Results:
  Packet Loss in Test           : 0%

UDP-Jitter Results:
  RTT Number                    : 10
  Min Positive SD                : 4           Min Positive DS       : 1
  Max Positive SD                : 21          Max Positive DS       : 28
```

```

Positive SD Number      : 5           Positive DS Number      : 4
Positive SD Sum         : 52          Positive DS Sum         : 38
Positive SD Average     : 10          Positive DS Average     : 10
Positive SD Square Sum  : 754         Positive DS Square Sum  : 460
Min Negative SD         : 1           Min Negative DS         : 6
Max Negative SD         : 13          Max Negative DS         : 22
Negative SD Number      : 4           Negative DS Number      : 5
Negative SD Sum         : 38          Negative DS Sum         : 52
Negative SD Average     : 10          Negative DS Average     : 10
Negative SD Square Sum  : 460         Negative DS Square Sum  : 754

```

One-way Results:

```

Max SD Delay           : 15           Max DS Delay           : 16
Min SD Delay           : 7           Min DS Delay           : 7
Number of SD Delays    : 10          Number of DS Delay     s : 10
Sum of SD Delays       : 78          Sum of DS Delays       : 85
Square Sum of SD Delays : 666         Square Sum of DS Delays : 787

```

For UDP Jitter for VoIP SLA, the following parameters are additionally shown:

Voice Scores:

```

ICPIF                                     : 4
MOS                                         : 4.38

```

show ip-sla <ID> aggregated-results

Syntax

```
show ip-sla <ID> aggregated-results
```

Description

Shows the aggregated results for the last 25 probes conducted for an IPSLA UDP Jitter or UDP Jitter For VoIP SLA test. Note this command is not valid for any other SLA type.

Switch (config)# show ip-sla 1 aggregated-results

```

Test results for SLA ID: 1
SLA Type           : UDP-Jitter
Destination IP Address : 10.2.2.2
Destination Port      : 4444
Source IP Address    : 10.2.2.2
Source Port          : 5555
First Probe Start Time : 2008-05-29 13:56:17.6

```

```

Number of Packets Sent           : 10
Number of Packets Received       : 10
Minimum Round Trip Time          : 15
Maximum Round Trip Time          : 32
Average Round Trip Time          : 17
Square-Sum of Round Trip Time    : 3235

```

Aggregated Results for the Last 25 Probes

Extended Results:

```

Packet Loss in Test           : 0%
Probe Failure Reason          :

```

UDP-Jitter Results:

```

RTT Number           : 10
Min Positive SD      : 4           Min Positive DS      : 1
Max Positive SD      : 21          Max Positive DS      : 28

```

Positive SD Number	: 5	Positive DS Number	: 4
Positive SD Sum	: 52	Positive DS Sum	: 38
Positive SD Average	: 10	Positive DS Average	: 10
Positive SD Square Sum	: 754	Positive DS Square Sum	: 460
Min Negative SD	: 1	Min Negative DS	: 6
Max Negative SD	: 13	Max Negative DS	: 22
Negative SD Number	: 4	Negative DS Number	: 5
Negative SD Sum	: 38	Negative DS Sum	: 52
Negative SD Average	: 10	Negative DS Average	: 10
Negative SD Square Sum	: 460	Negative DS Square Sum	: 754

One-way Results:

Max SD Delay	: 15	Max DS Delay	: 16
Min SD Delay	: 7	Min DS Delay	: 7
Number of SD Delays	: 10	Number of DS Delay s	: 10
Sum of SD Delays	: 78	Sum of DS Delays	: 85
Square Sum of SD Delays	: 666	Square Sum of DS Delays	: 787

For UDP Jitter for VoIP SLA, the following parameters are additionally shown:

Voice Scores:

Max MOS Value	: 4.38	Min MOS Value	: 4.38
Max ICPIF Value	: 0	Min ICPIF Value	: 0

show ip-sla responder

Syntax

```
show ip-sla responder
```

Description

Show the IP SLA responder details.

show ip-sla responder

```
SLA type           : UDP-echo
Listening Address: 1.1.1.1
Listening Port     : 5555
```

show ip-sla responder statistics

Syntax

```
show ip-sla responder statistics
```

Description

Show the IP SLA responder statistics details.

Parameters

udp-jitter

Show the IP SLA responder statistics for UDP Jitter SLA type.

udp-jitter-voip

Show the IP SLA responder statistics for UDP Jitter VoIP SLA type.

show ip-sla responder statistics

```
IP SLA Responder : Active
Number of packets received : 31
Number of error packets received : 0
Number of packets sent : 0

Recent Sources :
 10.12.80.100 [07:23:49.085 UTC Sun Oct 25 2015] UDP
 10.12.80.100 [07:22:49.003 UTC Sun Oct 25 2015] TCP
 10.12.80.100 [07:20:48.717 UTC Sun Oct 25 2015] TCP
 10.12.80.100 [07:18:48.787 UTC Sun Oct 25 2015] TCP
 10.12.80.100 [07:17:48.871 UTC Sun Oct 25 2015] TCP
```

show tech ip-sla

Syntax

```
show tech ip-sla
```

Description

Display output of a predefined command sequence used by technical support.

show tech ip-sla

```
switch# sh tech ip-sla

ipslaShowTech

===== IP SLA show tech BEGIN =====

GLOBALS:
Hash Handle:                1e7bab20
Struct Mem Handle for hash: 1e7ba2a8
Struct Mem Handle for SLA ID LL: 1e7c9430
Struct Mem Handle for FD List: 1e7bd690
FastLog Handle:             dfabf5c
IPSLA Ctrl task ID:         1068091456
IPSLA Sender ID:           1068092544
IPSLA Listener ID:         1068091840
Number of enabled SLA's:    1
SLA ID List Handle:         1ec1ffd4
FD ID List Handle:          0
Ring Full Counter:          0

Details for SLA ID: 1

SLA ID: 1
Status: Running

SLA mechanism: ICMP-Echo

Destination address: 192.168.1.2
Source address: 192.168.1.1
History bucket size: 25
Payload size: 0
TOS: 0
```

Schedule:

Frequency (seconds) : 60
Life : Forever
Start Time : Mon Jun 13 10:42:52 2016
Next Scheduled Run Time : Mon Jun 13 10:46:52 2016

Threshold-Monitor is : Enabled

Threshold Config : RTT
Threshold Type : Immediate
Upper Threshold : 10
Lower Threshold : 2
Action Type : Log

SLA ID: 1
Status: Running

SLA mechanism: ICMP-Echo

Destination address: 192.168.1.2
Source address: 192.168.1.1
History bucket size: 25
Payload size: 0
TOS: 0

Messages:

Destination address unreachable : 0
Probes skipped awaiting DNS resolution : 0
DNS resolution failed : 0
No route to target : 0
Internal error : 0
Local interface is down : 0
No response from target : 0
Successful probes sent : 9
Probe response received : 9
Possibly tail dropped : 0

Count of Threshold hits:

RTT : 0
packetLoss : 0

SLA ID: 1

Minimum RTT (ms) : 1
Maximum RTT (ms) : 1
Average RTT (ms) : 1
Total RTT (ms) : 9
RTT2 (sum of RTT squared): 9

Start Time	Status	RTT	Description
-----	-----	---	-----
Tue Jun 14 10:43:12 2016	Passed	1	
Mon Jun 13 10:39:05 2016	Passed	1	
Mon Jun 13 10:40:05 2016	Passed	1	
Mon Jun 13 10:41:05 2016	Passed	1	
Mon Jun 13 10:42:05 2016	Passed	1	
Mon Jun 13 10:42:52 2016	Passed	1	
Mon Jun 13 10:43:52 2016	Passed	1	
Mon Jun 13 10:44:52 2016	Passed	1	
Mon Jun 13 10:45:52 2016	Passed	1	

ICMP ID hash walk:

```
===== IP SLA show tech END =====  
  
===== IP SLA Server show tech BEGIN =====  
Responder not active  
IP SLA Responder: Inactive  
  
===== IP SLA Server show tech END =====  
  
=== The command has completed successfully. ===
```

clear ip-sla responder statistics

Syntax

```
clear ip-sla responder statistics <SLA-TYPE> <LOCAL-IP-ADDR> <LOCAL-PORT-NUM>  
source <SOURCE-IP-ADDR>
```

Description

Clear IP SLA responder statistics for either UDP jitter or VoIP UDP jitter.

Command context

config

Parameters

<SLA-TYPE>

Specifies the SLA type.

udp-jitter

Selects standard UDP jitter.

udp-jitter-voip

Selects UDP VOIP jitter.

<LOCAL-IP-ADDR>

Specifies the local interface IP address

<LOCAL-PORT-NUM>

Specifies the local interface port number. Range: 1024 to 65535.

<SOURCE-IP-ADDR>

Specifies the Source IP address.

Examples

Clear IP SLA responder statistics for UDP jitter:

```
switch(config)# clear ip-sla responder statistics udp-jitter 1.1.1.1 1100 source 1.1.1.2
```

Interoperability

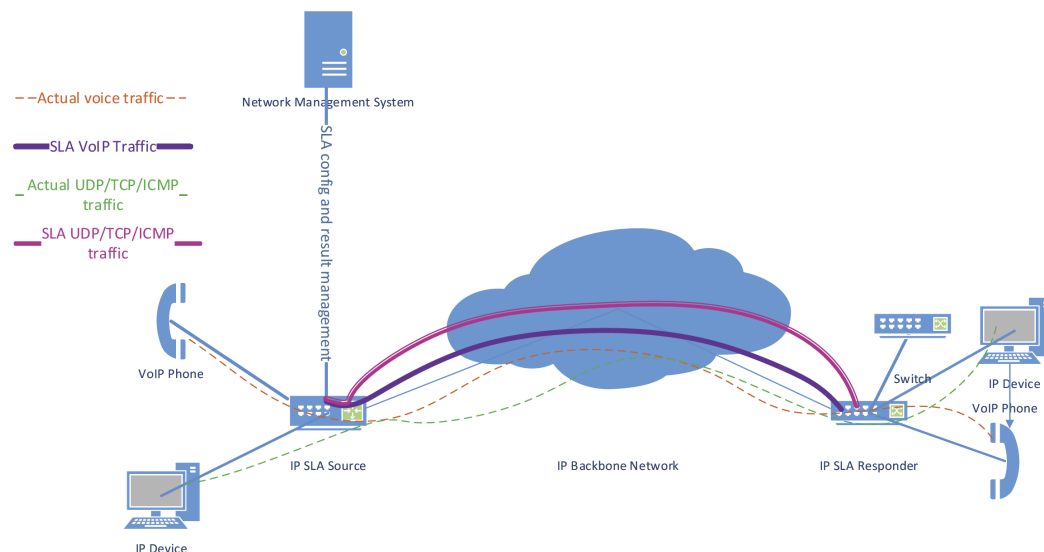


NOTE: Packet loss is expected when H3C TCP-CONNECT source, with a frequency less than or equal to 10 ms, interoperates with TCP-CONNECT responder.

IP SLA UDP Jitter and Jitter for VoIP

Overview

The UDP Jitter and Jitter for VoIP SLA types enable the user to assess the suitability of the network for voice & video related traffic. These SLA's basically calculate parameters like RTT, one way delay, one way positive and negative Jitter etc.



The above diagram shows a typical deployment, where voice & video traffic are exchanged between branch offices of an enterprise over the backbone network. Assessment of the network readiness is always helpful for hosting such services. Parameters like RTT, Jitter and one way delay are a good indicator of network health which assist a network administrator to diagnose latency related issues in the network. VoIP traffic is generally sensitive to delays in the network.

Jitter stands for inter-packet delay variance. If the inter-packet delay increases between successive probe packets, jitter is said to be positive. If the inter-packet delay decreases, jitter is said to be negative. Positive jitter values are undesirable for a network as they indicate increased latencies. A value of 0 jitter is desirable.

Significance of jitter

Consider a media player which plays video streams from a server. Assume that packets take 1 second in flight to reach the media player. This means the moment a user requests a video from the server, the very first packet will arrive after one second and successive packets will be sent immediately (ideally). In real world scenarios, intermediate node latencies, different return paths for different packets and network congestion can contribute to varying delays. To counter such effects, packets are buffered at the media player. The amount of packet buffering needed can be derived from the jitter values.



NOTE: The above analogy is applicable for other voice & video services and can be a good measure to assess the possibility for hosting a service on a network.

Solution components

IP SLA responder

This device receives IP SLA probe packets from a configured initiator, timestamps the frame at a pre-defined location in the packet upon receipt and sends the same frame back to the initiator.

IP SLA initiator

This device initiates IP SLA probe packets to multiple destinations each with a certain user configurable packet content and periodicity.

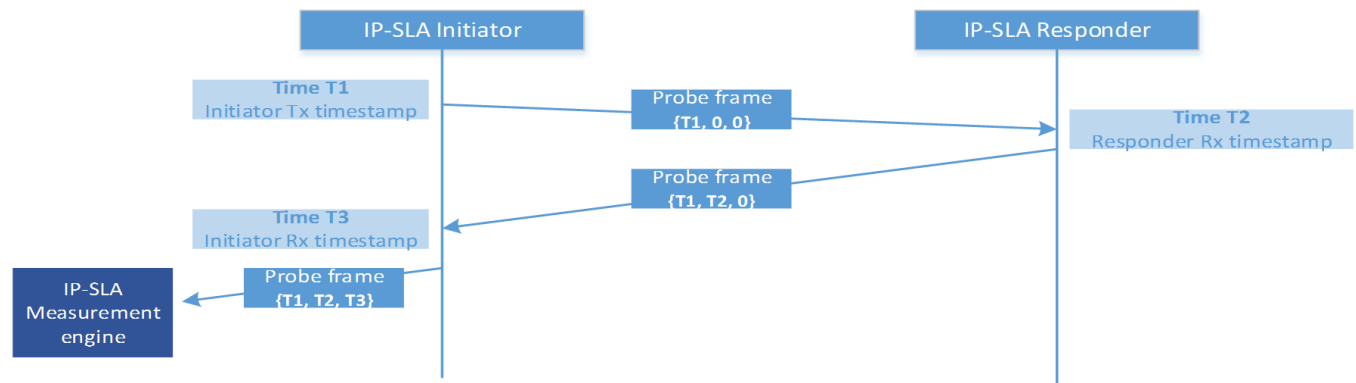
The initiator timestamps the frame at a pre-defined location before sending the frame out to the configured destinations and re-timestamps the frame at a different location once it receives the same back from the responder.

IP SLA measurement engine

This is an application running on the initiator. It processes response frames received from the IP SLA responder and computes one-way delay, jitter and RTT based on the timestamps present in the packet.

This application aggregates this computed information across multiple probe samples and stores this for consumption by an NMS via SNMP or via the device CLI.

It also supports asynchronous user configurable threshold breach notification to an NMS (via SNMP Traps).



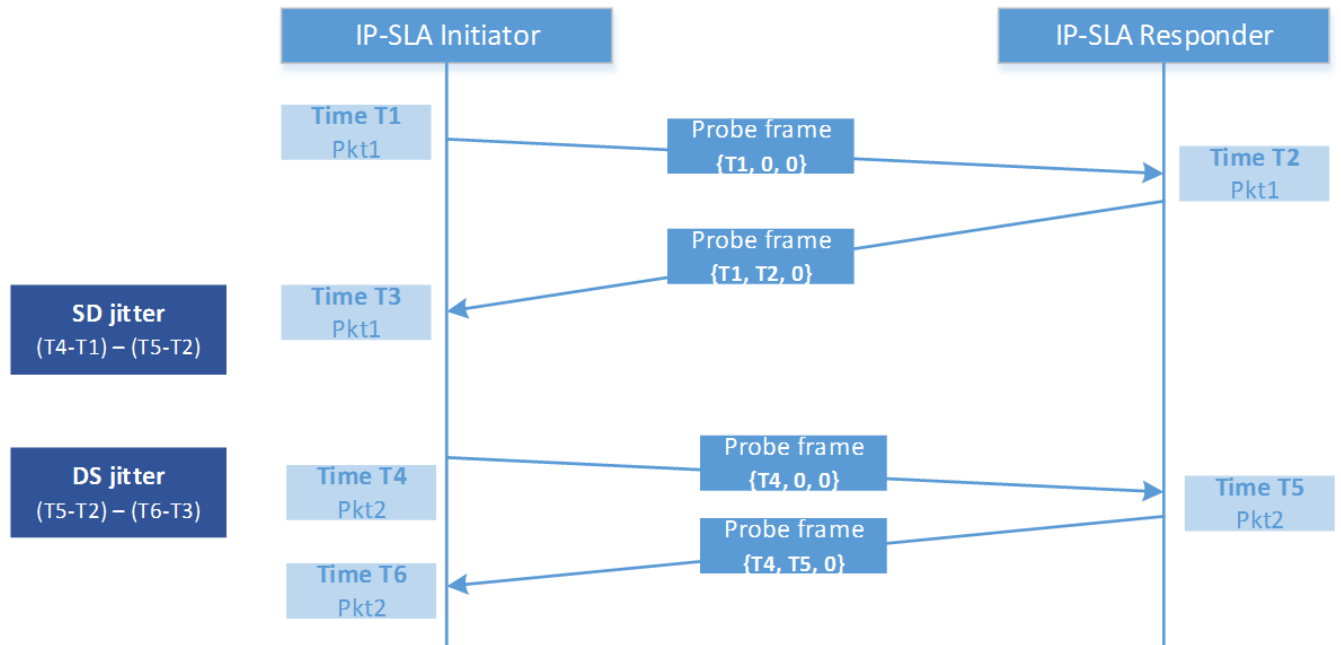
SLA Measurements

The following metrics are measured as part of this IP SLA jitter functionality.

One way jitter

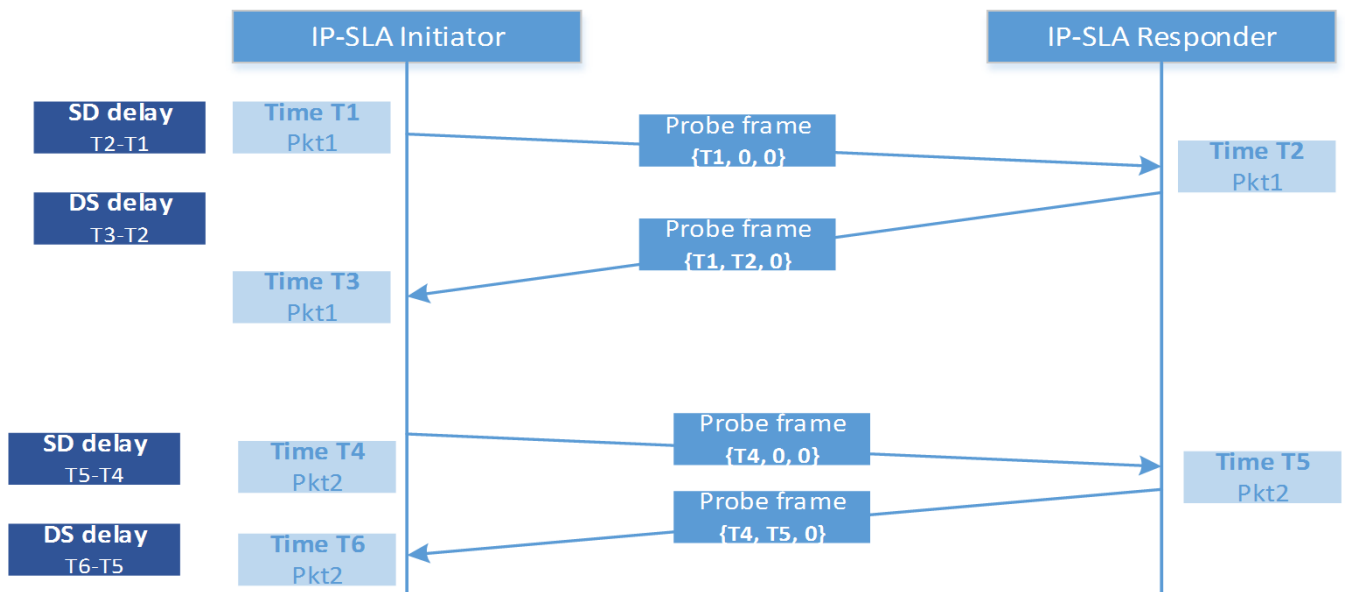
One way jitter is defined as the time difference between inter-packets transmit time and inter-packets arrival time in a given direction. This is measured in both the Initiator to Responder direction (referred to as SD jitter) as well as the Responder to initiator direction (referred to as DS jitter).

Ideally, the jitter in both directions should be 0. A positive value of jitter is bad for VOIP and higher values of jitter will mean poor conversation quality. This is explained in the illustration below:



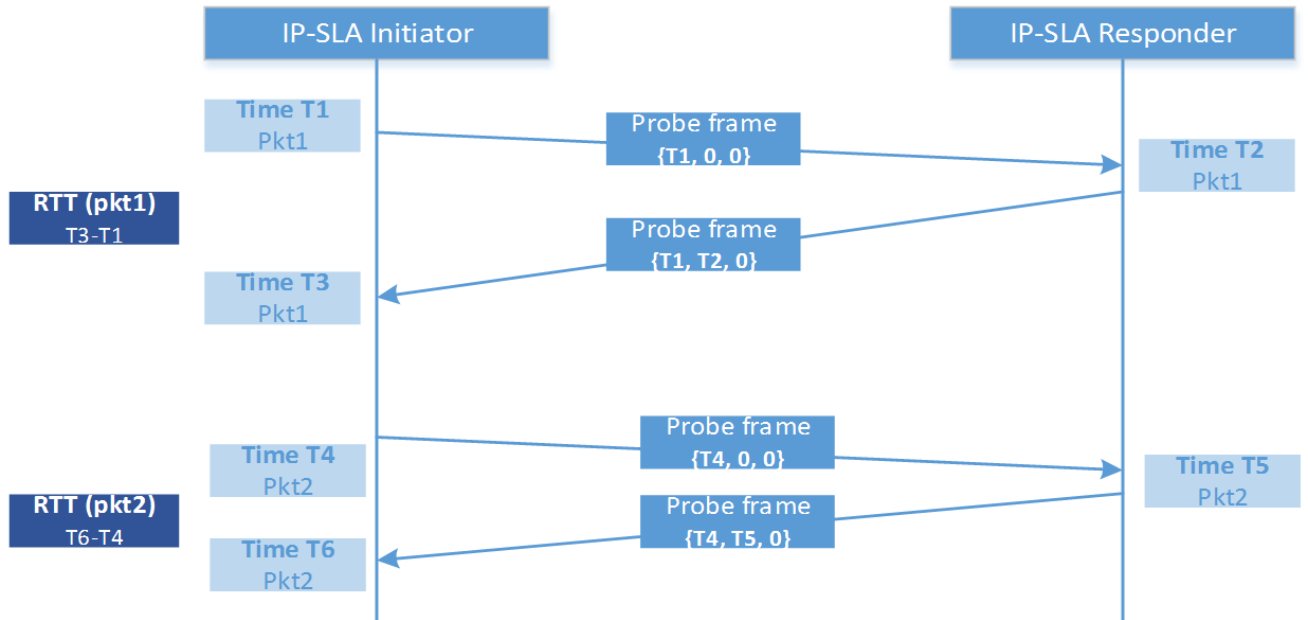
One way delay

One way delay is defined as the time difference between the Initiator transmitting the frame and the Responder receiving the frame. This requires the Initiator and the Responder to be time synchronized with the same clock server. This is explained in the illustration below:



Round trip time

RTT is measured at the initiator on a per packet basis and is as illustrated below:



Overview

The tunneled node feature encapsulates incoming packets from end-hosts in Generic Routing Encapsulation (GRE) and forwards them to a Mobility Controller for additional processing. The Mobility Controller strips the GRE header and processes the packet for authentication and stateful firewall, which enables centralized security policy, authentication, and access control.

The tunneled node feature is enabled on a per-port basis. Any traffic coming from nontunneled node interfaces is forwarded without being tunneled to a Mobility Controller. For Tunneled Node server configurations, see [Dynamic Segmentation](#).

With 16.08, User-Based Tunneling supports IPv6 along with IPv4. Both User-Based Tunneling extend-VLAN and no-VLAN support IPv6. For differences on extend-VLAN and no-VLAN, see [Differences between User-Based Tunneling extend-VLAN and no-VLAN](#).



NOTE: IPv6 addresses are supported only when User-Based Tunneling is operating in role-based mode. For information on User-Based Tunneling, see [User-Based Tunneling](#).

Operating notes

- Tunneled node profile can be created using CLI and SNMP.
- The tunneled node profile supports configuring of:
 - Primary controller (both IPv4 and IPv6).
 - Backup controller (both IPv4 and IPv6).
 - Heartbeat keepalive timeout – range 1-40 seconds.
- Only one tunneled node profile can be created.
- The tunneled-node profile can be applied to a physical port only via CLI and SNMP.
- The maximum number of physical ports to which the profile may be applied is:
 - Aruba 5400R Switch Series (non-VSF): 256
 - Aruba 5400R Switch Series (VSF): 512
- High availability (HA) will be supported for the tunneled node related configuration.
- A tunnel, associated with a port, is “up” when the following conditions are met. A tunnel is “down” when either of the conditions are not met.
 - Either the primary or backup controller is reachable.
 - A boot strap message response is received from the controller.
- Heartbeat between the switch and controller fails when the controller does not respond after five attempts. All tunnels are brought down with a heartbeat failure.
- A tunnel “up or down” status is logged for each tunnel node port in the event log.
- The `show tech` command dumps all user-mode and test-mode command outputs.
- To reach the Aruba controller, the VLAN must have a manual IP configured.

- With the exception of the 802.1x BPDUs, the switch consumes all other BPDUs.
- The controller cluster cannot have mix of IPv4 and IPv6 nodes.
- IPv6 addresses are not allowed for both Primary and Backup controllers when in Port-Based Tunnels.

Protocol Application Programming Interface (PAPI)

The PAPI Enhanced Security configuration provides protection to Aruba devices, AirWave, and ALE against malicious users sending fake messages that results in security challenges.

Starting from ArubaOS-Switch version 16.02, a minor security enhancement has been made to Protocol Application Programming Interface (PAPI) messages. Protocol Application Programming Interface endpoint authenticates the sender by performing a check of the incoming messages using MD5 (hash). All PAPI endpoints — APs, Controllers, Mobility Access Switches, Airwave, and ALE — must use the same secret key. The switch software currently uses a fixed key to calculate the MD5 digest and cooperate with the controller for PAPI enhanced security.



NOTE:

To use this functionality, the PAPI security profile must be configured on the controller. For more information on the Aruba controller, see the [Aruba Networks Controller Configuration Manual](#).

Configuration command

tunneled-node-server

Syntax

```
tunneled-node-server [controller-ip <IP-ADDR|IPv6-ADDR> | backup-controller-ip
<IP-ADDR|IPv6-ADDR> | [keepalive <TIMEOUT>] | enable | mode role-based {reserved-vlan <VLAN-ID>}]

no tunneled-node-server [controller-ip <IP-ADDR|IPv6-ADDR> | backup-controller-ip
<IP-ADDR|IPv6-ADDR> | [keepalive <TIMEOUT>] | enable | mode role-based {reserved-vlan <VLAN-ID>}]
```

Description

Configure tunneled node server information.

The no form of the command removes the tunneled node server configuration.

Parameters

controller-IP

Configure the controller IP address for the tunneled node. Both IPv4 and IPv6 are supported.

backup-controller-IP

Configure the backup controller IP address for the tunneled node. Both IPv4 and IPv6 are supported.

keepalive

Configure the keepalive timeout for the tunneled node in seconds [1-40]. The default is 8 seconds.

enable

Enter the manager command context.

mode role-based

Specifies the tunneled node server mode as role based.

mode role-based reserved-vlan

Specifies the VLAN used as tunneled node server reserved VLAN.

Examples

```
switch(config)# tunneled-node-server controller-ip 15.255.133.148
switch(config)# tunneled-node-server backup-controller-ip 15.255.133.148
switch(config)# tunneled-node-server keepalive 40
```

interface tunneled-node-server

Syntax

```
interface <PORT> tunneled-node-server
no interface <PORT> tunneled-node-server
```

Description

Enable tunneled node on a port.

The `no` command disables the tunneled node on the port.

controller-ip

From within the **tunneled-node-profile** context:

Syntax

```
no controller-ip <IP-ADDR|IPv6-ADDR>
```

Description

Configure the Controller IP address for the tunneled node.

controller-ip

Configure the Controller IP address for the tunneled node.

keepalive

From within the **tunneled-node** context:

Syntax

```
no keepalive <TIMEOUT>
```

Description

Configure the keepalive timeout for the tunneled node in seconds.

Keepalive timeout seconds [1-40].

Default: 8 seconds.

Parameters

keepalive

Configure the keepalive timeout for the tunneled node in seconds.

backup-controller-ip

From within the **tunneled-node-profile** context:

Syntax

```
no backup-controller-ip <IP-ADDR|IPv6-ADDR>
```

Description

Configure the backup controller IP address for the tunneled node.

Parameter

backup-controller-ip

Configure the backup controller IP address for the tunneled node.

fallback-local-switching

From within the **interface** context:

Syntax

```
fallback-local-switching
```

Description

To switch traffic locally upon losing connectivity to the controller, you must configure the fallback option before connectivity fails. When the tunneled node is applied to a port and the tunnel cannot be established with the controller, the fallback-local-switching option allows port traffic to be switched locally. When the option fallback-local-switching is not specified, the port traffic is dropped when the tunnel reestablishment fails.

VLAN show commands

VLAN show commands display information about configured VLANs.

show tunneled-node-server

Syntax

```
show tunneled-node-server [state | statistics]
```

Description

Display switch operation information.

Parameters

state

Display the tunneled node port state.

statistics

Display the tunneled node statistics.

show tunneled-node-server state

```
Tunneled node Port State
Active Controller IP Address :
Port      State
-----
2         Port down
```

show tunneled-node-server statistics

```
Tunneled node Statistics

Port : 2

Control Plane Statistics
Bootstrap packets sent      : 0
Bootstrap packets received  : 0
Bootstrap packets invalid   : 0

Tunnel Statistics
Rx Packets                  : 0
Tx Packets                  : 0
Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0

Aggregate Statistics
Heartbeat packets sent      : 0
Heartbeat packets received  : 0
Heartbeat packets invalid   : 0
Fragmented Packets Dropped (Rx) : 0
Packets to Non-Existent Tunnel : 0
MTU Violation Drop          : 0
```

clear statistics tunneled-node-server

Syntax

```
clear statistics tunneled-node-server
```

Description

Clear statistics from the tunneled node server.

Interaction table

Features enabled with tunneled node:

Feature
Mirrors (MAC, VLAN, port)
PVST/RPVST/STP
DLDP
UDLD
LLDP/CDP
GVRP/MVRP
LACP

Table Continued

Feature

Uplink Failure Detection

sFlow

Loop protect

Smartlink

Global QoS (VLAN, port, rate limit)

MAC lockout/lockdown

ACL/Classifiers (ingress/egress)

IGMP/MLD

GMB

Broadcast-limit

Energy Efficient Ethernet

Flow Control

PoE

- poe-allocate-by
- poe-lldp-detect

Rogue MAC detection

LLDP auto provisioning

Restrictions

- Once a tunneled node profile is applied to a port, the controller IP (primary and backup) cannot be changed.
- IP address cannot be assigned to VLANs that contain ports with Port-Based Tunneling configured.
- No support for fragmentation and reassembly for encapsulated frames that result in an MTU violation. Such frames will be dropped.
- Packets from ports configured with Port-Based Tunnels will not be bridged with locally switched ports.

Features that are blocked when Port-Based Tunnels are configured and the scope of the block (either globally, on a port basis or on a VLAN basis):

Feature	Blocked globally/per port/ VLAN with Port-Based Tunneling
IP multicast routing	Global
Openflow	Global
Q-in-Q	Global
Distributed Trunking	Global
Mesh	Global
VXLAN	Global
IP address: manual and dhcp	VLAN
802.1x, mac auth, webauth, LMA, port security	Port
DIPLD (IPv4/IPv6)	Port
DSNOOP (IPv4/IPv6)	VLAN
ARP protect	VLAN
RA guard	Port
Virus throttling	Port
BYOD	VLAN
Trunk	Profile cannot be applied to a trunk
PBR policies	VLAN
VSF on a Port-Based Tunnel configured port	Port
Source port/Multicast filters	Port
DHCP client/Server/Relay	VLAN

PAPI security

Protocol Application Programming Interface (PAPI)

The PAPI Enhanced Security configuration provides protection to Aruba devices, AirWave, and ALE against malicious users sending fake messages that results in security challenges.

Starting from ArubaOS-Switch version 16.02, a minor security enhancement has been made to Protocol Application Programming Interface (PAPI) messages. Protocol Application Programming Interface endpoint authenticates the sender by performing a check of the incoming messages using MD5 (hash). All PAPI endpoints — APs, Controllers, Mobility Access Switches, AirWave, and ALE — must use the same secret key. The switch software currently uses a fixed key to calculate the MD5 digest and cooperate with the controller for PAPI enhanced security.



NOTE: To use this functionality, the PAPI security profile must be configured on the controller. For more information on the Aruba controller, see the [Aruba Networks Controller Configuration Manual](#).

PAPI configurable secret key

To support enhanced PAPI security, a command is available to configure a MD5 secret key.

papi-security

Syntax

```
switch(config)# papi-security
```

Description

Configure MD5 key for enhanced PAPI security.

Parameters

enhanced-security

The enhanced-security CLI must be enabled in Aruba controller for the connection to be truly secured.

<KEY-STR>

Configure MD5 key for enhanced PAPI security using a key-string parameter.

<KEY-VALUE>

Configure MD5 key for enhanced papi security using a key-value parameter.

Restrictions

- To view the status of the PAPI security, using the `show run` command with the option `include credentials` enabled, the PAPI security key will show in the output as an encrypted form.
- Key length has to be between 10-64.
- By default the enhanced-security is disabled.
- When enhanced-security mode is disabled, any AP can obtain the current shared secret key.
- When enhanced-security mode is enabled, an AP is not updated with the new shared secret key unless the AP knows the previous key and the AP is updated with the new key within one hour of the key creation.
- Key length has to be between 10-64 or the following message will appear:

```
Minimum key-value length allowed is 10 characters and maximum allowed is 64 characters.
```

Usage

```
switch(config)# papi-security key-value <KEY-VALUE>  
switch(config)# no papi-security <KEY-VALUE>
```

papi-security key-value

```
switch(config)# papi-security key-value TestKey12345678
switch(config)# no papi-security key-value

switch(config)# papi-security key-value Test
Minimum key-value length allowed is 10 characters and maximum allowed is 64 characters.
```

show run with encrypted key

```
switch(config)# show run
Running configuration:
;J9576A Configuration Editor
;Ver #0e:01.f0.92.34.5f.3c.6b.fb.ff.fd.ff.ff.3f.ef:78
;encrypt-cred +NXT3w7ky2IXNXad1Jb1S/1ZRi/o73Qq28XXcLkSCZq9PU30Kl+KMLMva8rQri5g

hostname "Switch"
module 1 type j9576y
module 2 type j9576x
encrypt-credentials
papi-security encrypted-key <"encrypted-key">
snmp-server community "public" unrestricted
snmpv3 engineid "00:00:00:0b:00:00:50:65:f3:b4:a6:c0"
oobm
ip address dhcp-bootp
exit

vlan 1
name "DEFAULT_VLAN"
untagged 1-52
ip address dhcp-bootp
exit

activate provision disable
```

show run with include key

```
show run
Running configuration:
; J9576A Configuration Editor
; Ver#0e:01.f0.92.34.5f.3c.6b.fb.ff.fd.ff.ff.3f.ef:78

hostname "Switch"
module 1 type j9576y
module 2 type j9576x
include-credentials
papi-security key-value <"key">
snmp-server community "public" unrestricted
snmpv3 engineid "00:00:00:0b:00:00:50:65:f3:b4:a6:c0"
oobm
ip address dhcp-bootp
exit

vlan 1
name "DEFAULT_VLAN"
untagged 1-52
ip address dhcp-bootp
exit

activate provision disable
```

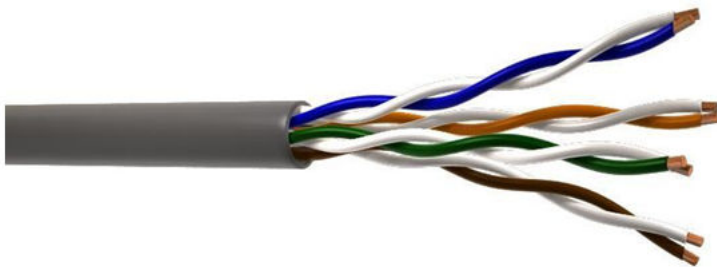

The Time Domain Reflectometry (TDR) or Cable Diagnostics is a port feature supported on some switches running ArubaOS-Switch software. TDR is used to detect cable faults on 100BASE-TX and 1000BASE-T ports.

Virtual cable testing

The Virtual Cable Test (VCT) uses the same command as TDR. It is applicable only for GigT transceivers like copper transceiver (J8177C–ProCurve Gigabit 1000Base-T Mini-GBIC). The VCT test results include distance to the fault, but not the cable length.

Cable diagnostics tests

The TDR (Time-domain reflectometer) cable diagnostic test allows an operator to test Ethernet cables for faults without physically disconnecting from the switch. It helps in troubleshooting connectivity or monitor performance on one or more switch ports.



Cable diagnostic test is categorized as four states. Each of the four twisted pairs is displayed in a standard Ethernet cable:

- 1. OK:** The twisted pair is intact and operating normally for the full length of the cable.
If displayed for all four pairs, the cable must operate normally with no connectivity or any performance issues.
- 2. Short:** There is a short between two wires in the same pair.
A pair that is shorted (example: blue and white) cannot transmit normally, and may cause impaired connectivity or performance for the cable.
- 3. Inter-short:** There is short between two or more wires in different pairs.
If multiple pairs are shorted together (example: brown and green), then there is a significant performance degradation or a total loss of connectivity.
- 4. Open:** There is a gap in one or more pairs resulting in a loss of continuity, or no cable is connected to the port.
It may indicate a damaged or cut cable. A port that has no cable connected is display **Open** for all pairs.

To start a cable diagnostic test, use the following command (in this example, port 1 and 2 are tested):

```
switch# test cable-diagnostics 1-2
```

This command will cause a loss of link on all tested ports and will take several seconds per port to complete. Use the 'show cable-diagnostics' command to view the results.

Continue (y/n)? y

After the test is complete, use the following command to view the test results:

```
switch# show cable-diagnostics
```

Cable Diagnostic Status - Copper Ports

Port	MDI Pair	Cable Status	Cable Length or Distance to Fault
1	1-2	OK	2m
	3-6	OK	4m
	4-5	OK	2m
	7-8	OK	2m
2	1-2	Open	0m
	3-6	Open	0m
	4-5	Open	0m
	7-8	Open	0m



NOTE:

- Running a cable diagnostic test will result in a brief interruption in connectivity on all tested ports.
- Displayed cable lengths and distances to detected faults are approximate (error margin is $\pm 10\%$ of cable length).

Syntax

```
test cable-diagnostics <PORT-LIST>
```

Description

Use the command to test for cable faults.

Parameter

PORT-LIST

Specify copper port as an input port number.

Test cable-diagnostics C21

```
test cable-diagnostics C21
```

The 'test cable-diagnostics' command will cause a loss of link and will take a few seconds per interface to complete. Continue [Y/N]? y

MDI Port	MDI Pair	Cable Status	Distance to Fault	Pair Skew	Pair Polarity	MDI Mode
C21	1-2	Open	0 m	0 ns		
	3-6	Open	0 m	0 ns		
	4-5	Open	0 m	0 ns		
	7-8	Open	1 m	0 ns		

Test cable-diagnostics 1/1-1/10

```
switch# test cable-diagnostics 1/1-1/10
```

This command will cause a loss of link on all tested ports and will take

several seconds per port to complete. Use the 'show cable-diagnostics' command to view the results.

Continue (y/n)? Y

```
switch# show cable-diagnostics 1/1-1/10
```

Cable Diagnostic Status - Copper Ports

Port	MDI Pair	Cable Status	Cable Length or Distance to Fault
1/1	1-2	OK	5m
	3-6	OK	5m
	4-5	OK	7m
	7-8	OK	7m
1/2	1-2	OK	7m
	3-6	OK	7m
	4-5	OK	7m
	7-8	OK	7m
1/3	1-2	OK	5m
	3-6	OK	7m
	4-5	OK	5m
	7-8	OK	7m
1/4	1-2	OK	7m
	3-6	OK	7m
	4-5	OK	7m
	7-8	OK	5m
1/5	1-2	OK	4m
	3-6	OK	5m
	4-5	OK	5m
	7-8	OK	4m
1/6	1-2	OK	4m
	3-6	OK	4m
	4-5	OK	4m
	7-8	OK	4m
1/7	1-2	OK	5m
	3-6	OK	4m
	4-5	OK	5m
	7-8	OK	4m
1/8	1-2	OK	4m
	3-6	OK	5m
	4-5	OK	4m
	7-8	OK	4m
1/9	1-2	OK	5m
	3-6	OK	5m
	4-5	OK	5m
	7-8	OK	5m
1/10	1-2	OK	7m
	3-6	OK	5m
	4-5	OK	5m
	7-8	OK	5m

Good cable tests

```
switch# test cable-diagnostics 51
```

This command will cause a loss of link on all tested ports and will take several seconds per port to complete. Use the 'show cable-diagnostics' command to view the results.

Continue (y/n)? Y

```
switch# show cable-diagnostics 51
```

```
Cable Diagnostic Status - Transceiver Ports
```

Port	MDI Pair	Cable Status	Distance to Fault	Pair Skew	Pair Polarity	MDI Mode
51	1-2	OK	0 m	8 ns	Normal	MDI
	3-6	OK	0 m	8 ns	Normal	
	4-5	OK	0 m	8 ns	Normal	MDIX
	7-8	OK	0 m	0 ns	Normal	

```
switch# test cable-diagnostics 52
```

This command will cause a loss of link on all tested ports and will take several seconds per port to complete. Use the 'show cable-diagnostics' command to view the results.

```
Continue (y/n)? Y
```

```
switch# show cable-diagnostics 52
```

```
Cable Diagnostic Status - Transceiver Ports
```

Port	MDI Pair	Cable Status	Distance to Fault	Pair Skew	Pair Polarity	MDI Mode
52	1-2	OK	0 m	0 ns	Normal	MDI
	3-6	OK	0 m	0 ns	Normal	
	4-5	OK	0 m	0 ns	Normal	MDIX
	7-8	OK	0 m	0 ns	Normal	

Faulty cable test

```
switch# test cable-diagnostics 51
```

This command will cause a loss of link on all tested ports and will take several seconds per port to complete. Use the 'show cable-diagnostics' command to view the results.

```
Continue (y/n)? y
```

```
switch# show cable-diagnostics 51
```

```
Cable Diagnostic Status - Transceiver Ports
```

Port	MDI Pair	Cable Status	Distance to Fault	Pair Skew	Pair Polarity	MDI Mode
51	1-2	OK	0 m	0 ns		
	3-6	Short	1 m	0 ns		
	4-5	Short	1 m	0 ns		
	7-8	OK	0 m	0 ns		

```
switch# test cable-diagnostics 52
```

This command will cause a loss of link on all tested ports and will take several seconds per port to complete. Use the 'show cable-diagnostics' command to view the results.

```
Continue (y/n)? Y
```

```
switch# show cable-diagnostics 52
```

Cable Diagnostic Status - Transceiver Ports

Port	MDI Pair	Cable Status	Distance to Fault	Pair Skew	Pair Polarity	MDI Mode
52	1-2	Open	0 m	0 ns		
	3-6	Open	0 m	0 ns		
	4-5	Open	1 m	0 ns		
	7-8	Open	0 m	0 ns		

Error message

Error Message	Cause
The transceiver on port 1/A1 does not support cable diagnostics.	<ul style="list-style-type: none">usage of invalid(fiber-SFP+) portThe selected range includes an entry for an invalid port.

show cable-diagnostics

Syntax

```
show cable-diagnostics <PORT-LIST>
```

Description

Use the command to generate results of completed tests on single or multiple ports. For incomplete tests, a warning is displayed.

Parameter

PORT

Specify one copper port as an input port number.

clear cable-diagnostics

Syntax

```
clear cable-diagnostics
```

Description

Use the command to clear the result buffer.

Example

```
switch(config)# clear cable-diagnostics
```

Limitations

TDR has the following limitations:

- TDR length accuracy is ± 5 m
- Does not work on Smart Rate Interfaces with 10GBASE-T and NGBASE-T (2.5G, 5G copper) ports available on:
 - v3 blades

- J9991A — Aruba 20-port 10/100/1000BASE-T PoE+ / 4-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 z12 Module
- J9995A — Aruba 8-port 1/2.5/5/10GBASE-T PoE+ MACsec v3 z12 Module
- 3810M (JL076A — Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch)
- Not supported on v2 z1 modules
- Valid only on 100BASE-TX and 1000BASE-T ports

An end client that gets IP address from a DHCP address will be included by default in RADIUS accounting packets. Visibility of statically assigned IP addresses in RADIUS accounting is available with a command that enables and disables static IP visibility for an authenticated client.

ip client-tracker

Syntax

```
ip client-tracker [trusted | untrusted]
no ip client-tracker [trusted | untrusted]
```

Description

Enables the visibility of statically and dynamically assigned IPv4 and IPv6 addresses for both authenticated and unauthenticated clients.

The `no` form of this command disables the visibility of statically and dynamically assigned IPv4 and IPv6 addresses for both authenticated and unauthenticated client.

Command context

```
config
```

Parameters

trusted

Enables or disables the visibility of statically and dynamically assigned IPv4 and IPv6 addresses for authenticated clients. The `trusted` option makes the feature track clients only on authentication enabled ports (edge ports), excluding uplink ports which are not enabled for authentication with the server.

untrusted

Enables or disables the visibility of statically and dynamically assigned IPv4 and IPv6 addresses for unauthenticated clients.

Usage

- Switch sends ARP probes when IP client tracker feature is enabled. This interval is determined by setting `arp-age timeout`. By default `arp-age timeout` is 20 minutes however the default timeout can be changed by using the command `ip arp-age <timeout value in minutes>`.
 - The periodic ARP probe aids in detecting any change of IP addresses on end clients.
 - Non-chatty clients that do not send packets within regular intervals get deauthenticated due to inactivity after the logoff period. IP client tracker can be used to keep these clients in the network. The customer must always configure the `ip arp-age` value to less than the configured logoff period, to avoid being deauthenticated due to inactivity.

- When the `ip client-tracker` command is executed more than once, it takes the last command's behavior. For example when the command `ip client-tracker trusted` is run after the command `ip client-tracker`, the behavior will follow the last command, `ip client-tracker trusted`.
 - When the administrator tries to execute the `no` command that has not been configured (does not exist in running configuration), an error will appear.

Example

Show port-access client with multiple addresses.

```
switch# show port-access clients
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
1	005056bd3ff7	005056-bd3ff7	3ffe:501:ffff:100::5e		MAC	1

Example

Show the port-access IPv4 client.

```
Switch-Stack(config)# show port-access clients
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
1/3	000002b85001	000002-b85001	10.1.1.30		MAC	10

Example

Show the port-access IPv6 client.

```
switch(config)# show port-access clients 22
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
22	0000005daa34	000000-5daa34	n/a		MAC	20

Example

Show the port-access client detail.

```
switch(config)# show port-access clients 22 detailed
```

Port Access Client Status Detail

```
Client Base Details :
Port                : 22
Client Status      : authenticated
Client Name        : 0000005daa34
MAC Address        : 000000-5daa34
IP                  : n/a
Authentication Type : mac-based
Session Time       : 64 seconds
Session Timeout    : 0 seconds

Access Policy Details :
COS Map            : Not Defined
Untagged VLAN     : 20
In Limit Kbps     : Not Set
Out Limit Kbps    : Not Set
```



```
Tagged VLANs      : No Tagged VLANs
Port Mode        : 1000FDx
RADIUS ACL List  : No Radius ACL List
IPV6 Address     : 2000::10
```



NOTE: If neither `trusted` nor `untrusted` option is configured, the feature is enabled for both `trusted` (authentication enabled) and `untrusted` (authentication disabled) ports. Since uplink ports are always authentication disabled, `ip client-tracker` command without any options starts tracking these ports which result in tracking routed clients as well.

ip client-tracker probe-delay

Syntax

```
ip client-tracker probe-delay <INTERVAL>
no ip client-tracker probe-delay <INTERVAL>
```

Description

Enables the delay in the client tracking for static IP visibility. By default, `ip client-tracker probe-delay` is disabled.

The `no` form of this command disables the delay in the client tracking for static IP visibility.

Command context

```
config
```

Parameter

<INTERVAL>

Specifies the delay time of static IP tracking probes from 15 to 300 seconds.

Default value is 15 seconds.

Examples

Configures the delay in the client tracking.

```
switch# ip client-tracker probe-delay
switch# show run
ip client-tracker
ip client-tracker probe-delay 15
exit
```

Configures the delay in the client tracking for 250 seconds.

```
switch# ip client-tracker probe-delay 250
switch# show run
ip client-tracker
ip client-tracker probe-delay 250
exit
```

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

For additional websites, see [Support and other resources](#).

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<http://www.hpe.com/info/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<http://www.hpe.com/support/hpesc>

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:
 - Hewlett Packard Enterprise Support Center**
www.hpe.com/support/hpesc
 - Hewlett Packard Enterprise Support Center: Software downloads**
www.hpe.com/support/downloads
 - Software Depot**
www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:
www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials



IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Introduction

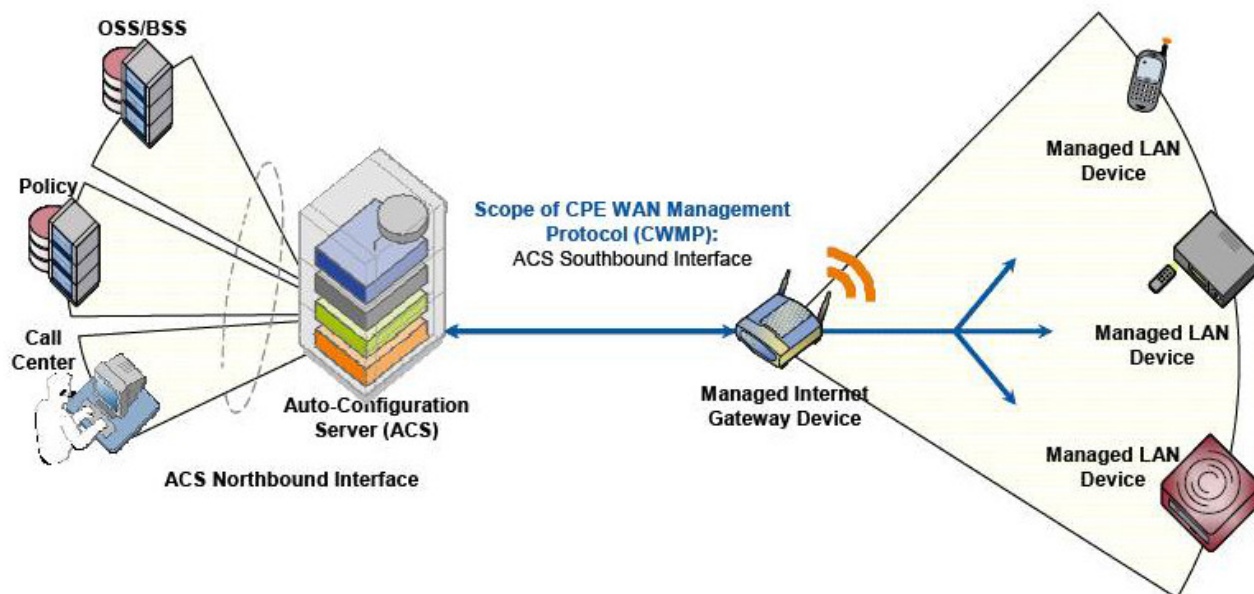
TR-069 is a technical specification created by the **Broadband Forum**. The TR-069 protocol specifies client and server requirements to manage devices across the Internet by using a client server architecture to provide communication between the CPE (Customer Premises Equipment) and the ACS (Auto Configuration Server). A protocol helps to manage complex networks where many devices such as modems, routers, gateways, VoIP phones and mobile tablets compete for resources. TR-069 defines the CPE WAN Management Protocol (CWMP) protocol necessary to remotely manage end-user devices. ACS provides automatic configuration for these devices.



NOTE: CWMP is automatically enabled. To conserve resources, reconfigure this setting using the `cwmp disable` command.

TR-069 defines an auto-configuration architecture which provides the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics
- Bidirectional SOAP/HTTP based protocol



Advantages of TR-069

- TR-069 can manage devices with dynamic IP addresses.
TR-069 use Organization Unique ID (OUI) and serial number rather than IP to identify a device.
- TR-069 can manage devices in a private network.
The HPE ACS BIMS (an iMC module) uses HTTP to communicate with the device, and the session is initiated by the device, so BIMS can pass through NAT to manage the device.
- TR-069 is secure.
TR-069 can use HTTPS to communicate with or transfer files to/from the device; it is more secure than TFTP, FTP or Telnet.
- TR-069 is suitable for WAN management across internet.
- TR-069 is suitable for zero-touch configuration.
The zero-configuration mechanism is defined in the TR-069 specification.
- TR-069 is suitable for large-scale device management.
TR-069 support distributed architecture. The ACS can be distributed to multiple servers, each ACS can manage part of devices.

Zero-touch configuration process

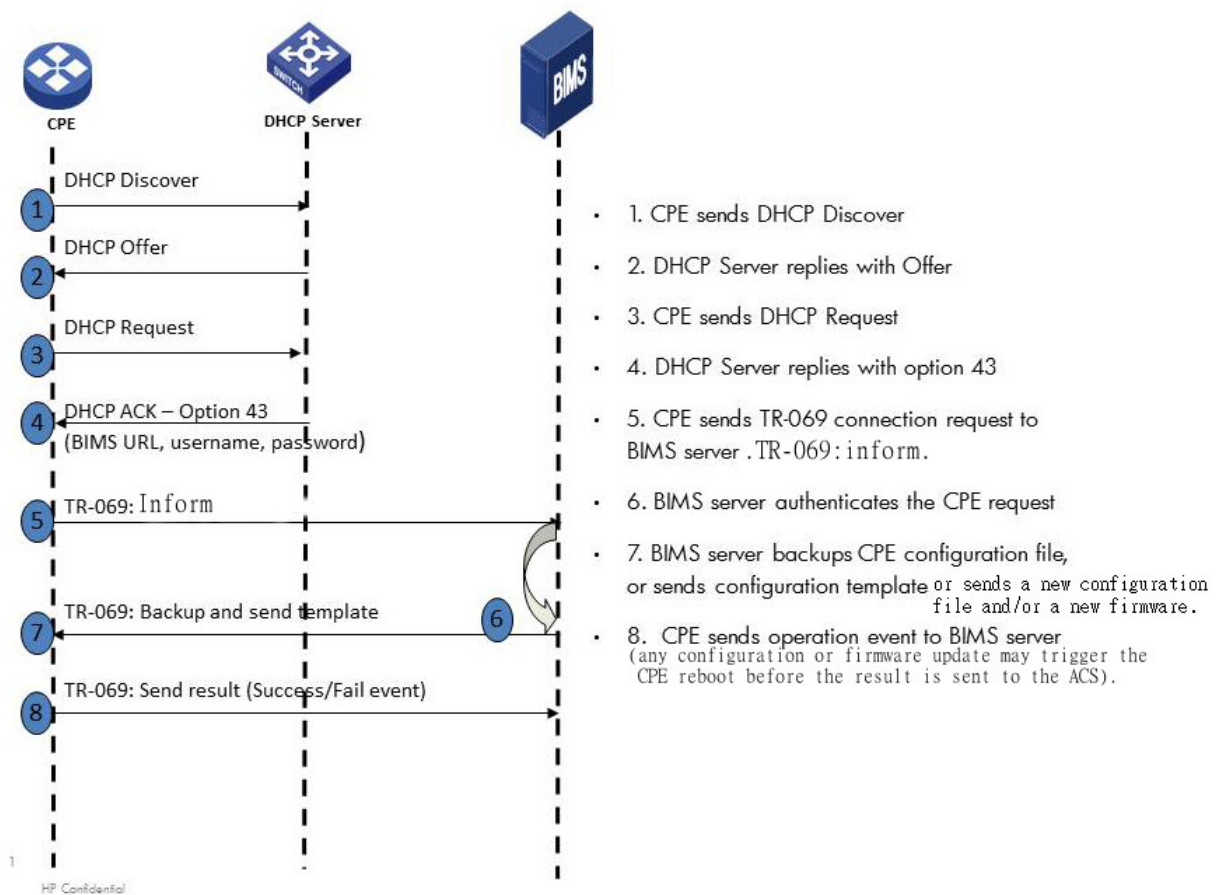
Auto configuration or “zero-touch” deployment is a recurring customer requirement, especially for remote-office deployments. New devices introduced inside a private network require management tools be co-located to configure them or update firmware, or require manual intervention to do configuration. TR-069 allows managing

devices that reside in a private network via HTTP(S), enabling a new set of deployment and management models today, not possible using SNMP.

The client side, when configured, will contact the server at a predefined URL, using HTTP or HTTPS as protocol. After authentication, the ACS is able to perform the following basic operations:

- Update CPE Configuration.
- Update CPE TR-069 parameters.
- Update CPE firmware.
- Reboot CPE (backup, startup, and running configurations)
- Run CPE ping diagnostics.
- Reset CPE to factory default.
- Get periodic Status (several parameters can be retrieved depending on what is supported).

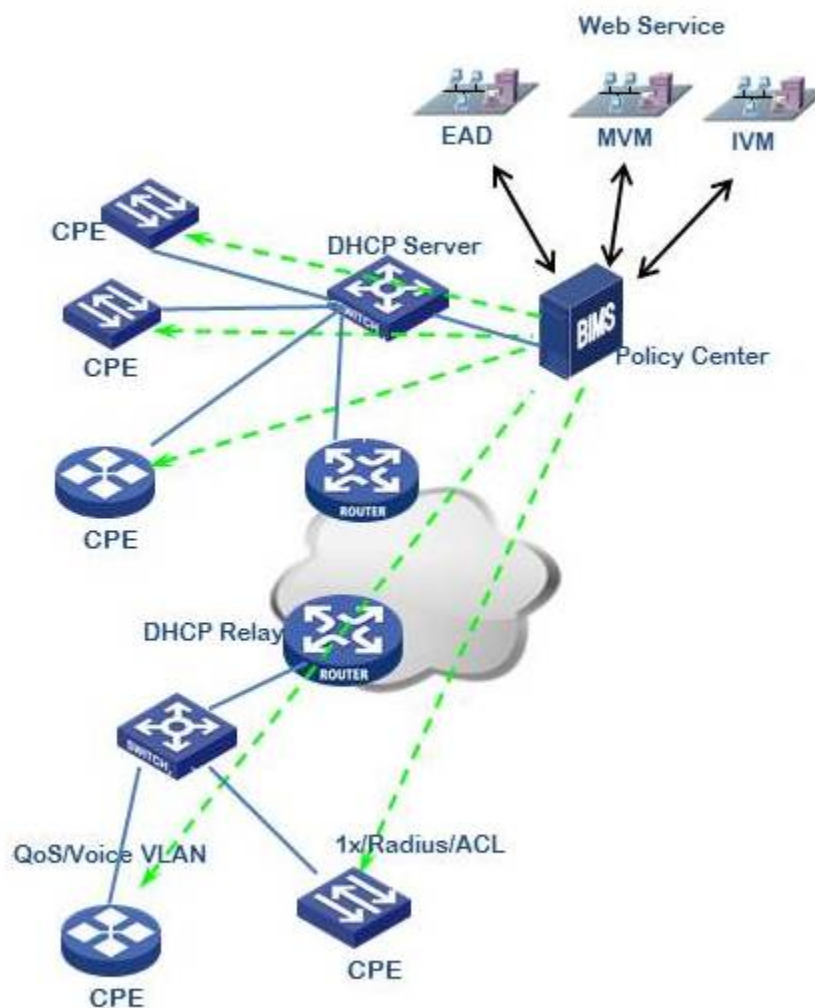
Since TR-069 uses HTTP, it can be used across a WAN. If the CPE can reach the URL, it can be managed. TR-069 is mostly a push protocol where the client periodically sends information without server requests. This allows for greater scalability over traditional SNMP based tools, which are also bounded to work within the LAN, while TR-069 can offer management to remote offices.



Zero-touch configuration for Campus networks

In this example, the following steps to configure CPEs for a Campus Network environment.

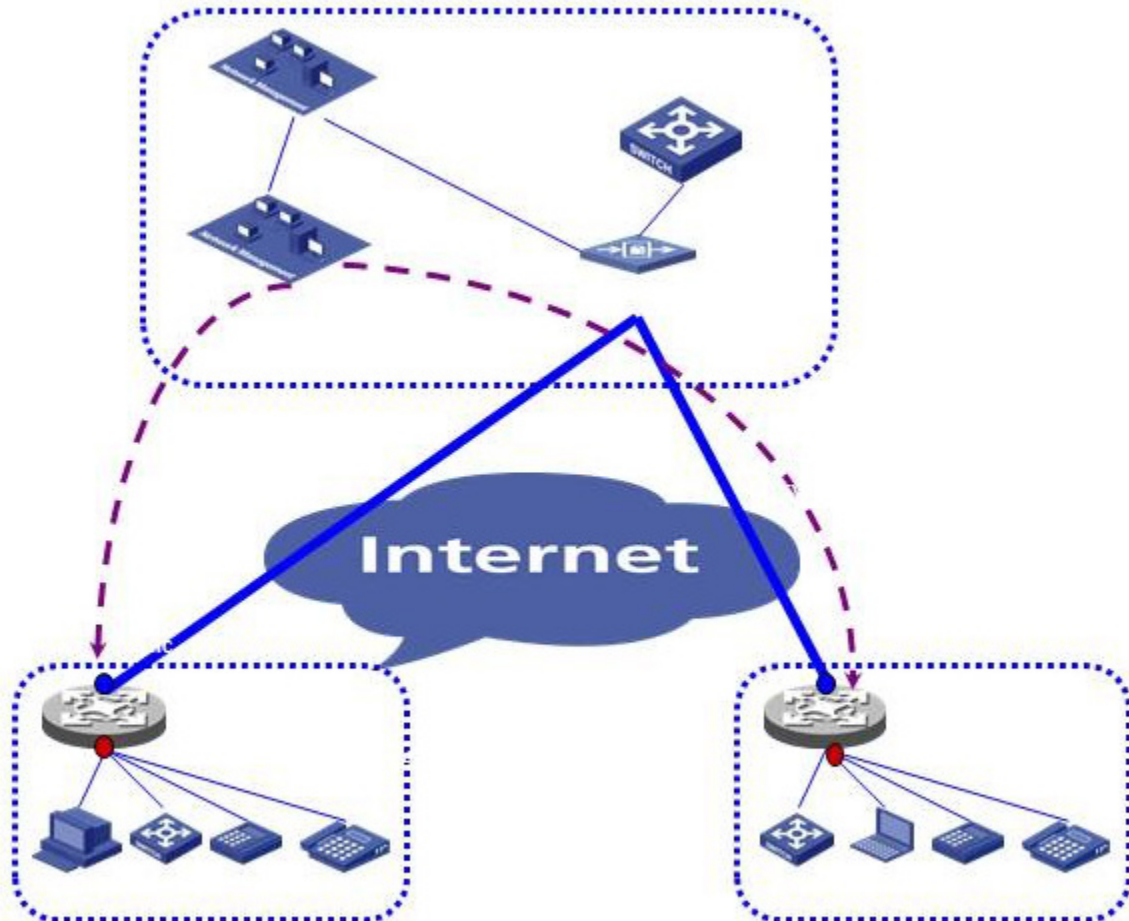
1. Pre-configuration for all CPEs in BIMS.
2. CPEs get BIMS parameters from DHCP server.
3. CPEs initiate a connection to BIMS, then BIMS deploys the pre-configuration to CPEs.



Zero-touch configuration for Branch networks

In this example, the following steps to configure CPEs for a Branch network environment.

1. Create the basic configuration for your spoke device manually, using the username/password from ISP and BIMS URL.
2. The IPsec VPN configuration is generated by IVM and deployed by BIMS.
3. The IPsec VPN tunnel is automatically created.
4. The device in the branch private network can DHCP relay to HQ to continue the zero touch configuration.



Zero-touch configuration setup and execution

1. DHCP configuration
2. BIMS configuration
3. Execution

CLI commands

Configuration setup

Within the configure mode:

Syntax:

```
cwmp
```

acs

Configure Auto Configuration Server (ACS) access.

cpe

Configure Customer Premises Equipment (CPE) access.

disable

Disable the CPE WAN Management Protocol.



NOTE:

CWMP is automatically enabled. To conserve resources, reconfigure this setting using the `cwmp disable` command.

enable

Enable the CPE WAN Management Protocol.

Syntax:

```
no cwmp
```

acs

Configure Auto Configuration Server (ACS) access.

cpe

Configure Customer Premises Equipment (CPE) access.

enable

Enable the CPE WAN Management Protocol.

ACS password configuration

Syntax:

```
cwmp acs
```

password

Configure the password used for authentication when the switch connects to the ACS.

url

Configure the URL of the ACS.

username

Configure the username used for authentication when the switch connects to the ACS.

When encrypt-credentials is off

Syntax:

```
cwmp acs password
```

plaintext

Configure the password used for authentication when the switch connects to the ACS.

When encrypt-credentials is on

Syntax:

```
cwmp acs password
```

encrypted-key

An encrypted password generated with the `encrypt-credentials` command.

plaintext

Configure the password used for authentication when the switch connects to the ACS.

Encrypt-credential on

```
cwmp acs password encrypted-key
```

ASCII-STR

Enter an ASCII string (maximum length: 384 characters).

Plaintext password

```
cwmp acs password plaintext
```

PASSWORD-STR

A plaintext password used for ACS authentication (maximum length: 256 characters).

ACS URL configuration

Syntax:

```
cwmp acs url
```

URL-STR

The URL of the ACS (maximum length: 256 characters).

ACS username configuration

Syntax:

```
cwmp acs username
```

USERNAME-STR

A username for ACS authentication (maximum length: 256 characters).

CPE configuration

Syntax:

```
cwmp cpe
```

password

Configure the password used for authentication when the ACS connects to the switch.

username

Configure the username used for authentication when the ACS connects to the switch.

CPE password configuration

When encrypt-credentials is on

Syntax:

```
cwmp cpe password
```

encrypted-key

An encrypted password generated with the 'encrypt-credentials' command.

plaintext

Configure the password used for authentication when the ACS connects to the switch.

Syntax:

```
cwmp cpe password encrypted-key
```

ASCII-STR

Enter an ASCII string (maximum length: 384 characters).

When encrypt-credentials is off

Syntax:

```
cwmp cpe [password]
```

plaintext

Configure the password used for authentication when the ACS connects to the switch

Syntax:

```
cwmp cpe
```

PASSWORD-STR

A plaintext password used for ACS authentication (maximum length: 256 characters).

CPE username configuration

Syntax:

```
cwmp cpe [username]
```

USERNAME-STR

A username for ACS authentication (maximum length: 256 characters).

Enable/disable CWMP

Syntax:

```
cwmp [enable|disable]
```

Show commands

CWMP configuration and status query

Syntax:

```
show cwmp
```

configuration

Show current CWMP configuration.

status

Show current CWMP status.

When CWMP is enabled

Syntax:

```
show cwmp configuration
```

CWMP configuration

```
CWMP Configuration
CWMP Status           : Enabled
ACS URL               : http://16.93.62.32:9090
ACS Username          : bims
Inform Enable Status  : Enabled
Inform Interval       : 60
Inform Time           : 2014-04-08T06:00:00
Reconnection Timeout  : 30
```

CWMP status

```
CWMP Status
CWMP Status           : Enabled
ACS URL               : http://16.93.62.32:9090
ACS URL Origin        : Config
ACS Username          : bims
Connection Status     : Disconnected
Data Transfer Status  : None
Last ACS Connection Time : Wed Apr 9 16:56:00 2014
Time to Next Connection : 00:00:36
```

When CWMP is disabled

Syntax:

```
show cwmp status
```

CWMP status

```
CWMP Status
CWMP Status          : Disabled
```

CWMP configuration

```
show cwmp configuration
CWMP Configuration
CWMP Status          : Disabled
```

Event logging

The TR-069 client offers some tools to diagnose problems:

- System logging
- Status/control commands

System logging

The CPE implements the following system log notification codes and sample messages:

- **RMON_TR69_INFORM_COMPLETE**
 - INFORM to http://15.29.20.50:9090/ from (IP address not set yet) completed with error.
 - INFORM to http://15.29.20.50:9090/ from 10.0.10.212 completed with error.
 - INFORM to http://15.29.20.50:9090/ from 10.0.10.212 completed successfully.
- **RMON_TR69_AUTH_FAILED**
 - Authentication on ACS http://15.29.20.50:9090/ failed.
- **RMON_TR69_CONN_FAILED**
 - Connection attempts with ACS http://15.29.20.50:9090/ from 10.0.10.212 failed.

To avoid flooding the system log on frequent attempts to connect with the ACS, the following criteria are used with both successful and failed attempts:

1. The very first event is always logged.
2. Any change from success to failure or vice versa is always logged.
3. Repeat success or failure events are logged only once every five minutes.

The HTTP file transfer component supports these system log notification codes and sample messages:

- **RMON_HTTP_XFER_COMPLETE**
 - I 11/19/13 08:06:13 04185 http: Download of http://10.0.11.240:9876/path to DestinationFile completed successfully.
 - I 11/19/13 08:06:13 04185 http: Upload of SourceFile to http://10.0.11.240:9876/path completed successfully.
- **RMON_HTTP_CONN_FAILED**
 - W 11/19/13 08:06:13 04186 http: Connection to http://10.0.11.240:9876/path failed.
- **RMON_HTTP_TIMED_OUT**
 - W 11/19/13 08:06:13 04192 http: Download of http://10.0.11.240:9876/path to DestinationFile timed out.
 - W 02/20/14 00:32:17 04192 http: Upload of SourceFile to http://10.0.11.240:9876/path timed out.
- **RMON_HTTP_NO_SPACE**
 - W 11/19/13 08:06:13 04189 http: Upload of SourceFile to http://10.0.11.240:9876/path canceled because of insufficient memory.
- **RMON_HTTP_REQ_FAILED**
 - W 11/19/13 08:06:13 04190 http: Upload of SourceFile to http://10.0.11.240:9876/path failed (errno 13).
 - W 11/19/13 08:06:13 04190 http: Upload of SourceFile to http://10.0.11.240:9876/path failed (errno 1).
 - W 11/19/13 08:06:13 04190 http: Download of http://10.0.11.240:9876/path to DestinationFile failed (errno 13).
 - W 11/19/13 08:06:13 04190 http: Download of http://10.0.11.240:9876/path to DestinationFile failed (errno 1).
 - W 11/19/13 08:06:13 04190 http: Download of http://10.0.11.240:9876/path to DestinationFile failed (errno 17).
- **RMON_HTTP_WRONG_FILE**
 - W 11/19/13 08:06:13 04191 http: Download canceled because file http://10.0.11.240:9876/path is malformed or incompatible.
 - W 11/19/13 08:06:13 04191 http: Download canceled because file http://10.0.11.240:9876/path is malformed or incompatible.
- **RMON_HTTP_FILE_NOT_FOUND**
 - W 11/19/13 08:06:13 04200 http: Upload of SourceFile to http://10.0.11.240:9876/path canceled because of inexistent file.

Status/control commands

The following commands help assess the general state of TR-069 and control the source of the ACS configuration record:

Table 32: Status/control commands

Command	Result
show cwmp status	CWMP is Enabled ACS URL : https://16.93.62.32:9443 ACS URL is set by : Config ACS Username : bims Connection status : Disconnected Data transfer status : None Time of last successful connection : Thu Feb 20 01:16:59 2014 Interval upon to next connection : Null
show cwmp configuration	CWMP is Enabled ACS URL : https://16.93.62.32:9443 ACS Username : bims Inform Enable Status : Disabled Inform Interval : 3559 Inform Time : Reconnection times : 30
no dhcp tr69-acurl	Prevents using any ACS information from DHCP

The configuration backup and restore without reboot supports the following features:

Interface Access (Telnet, Console/Serial, web)	Port Shutdown with Broadcast Storm
Access Control Lists (ACLs)	Source-Port Filters
AAA Authentication	TACACS+ Authentication
CoS (Class of Service)	Time Protocols (TimeP, SNTP)
Network Management Applications (SNMP)	Uni-directional Link Detection (UDLD)
Port Configuration	Virus Throttling (Connection-Rate Filtering)
Port Security	Web-based Authentication
Port-Based Access Control (802.1X)	Backplane stacking
Quality of Service (QoS)	Job Scheduler
Spanning Tree (STP, RSTP, MSTP, RPVST+)	Authorized IP Managers
VLANs	Authorized Manager List (Web, SSH, TFTP)
802.1Q VLAN Tagging	Auto MDIX Configuration
802.1X Port-Based Priority	DHCP Configuration
802.1X Multiple Authenticated Clients Per Port	Flow Control (802.3x)
IGMP	Friendly Port Names
LACP/Trunk	Guaranteed Minimum Bandwidth (GMB)
MAC Lockdown	IP Addressing
MAC-based Authentication	IP Routing
MAC Lockout	Jumbo Packets
LMA	LLDP
Multicast Filtering	LLDP-MED
Power over Ethernet (PoE and PoE+)	Loop Protection
Protocol Filters	MAC Address Management
RADIUS Authentication and Accounting	Management VLAN
RADIUS-Based Configuration	Passwords and Password Clear Protection/include-credentials

Table Continued

Encrypted-password	QoS: Strict-Priority Queuing
Port Monitoring	QoS: Turn on/off VLAN Precedence
Port Status	QoS: Egress Queue Rate-limiting
Rate-Limiting	CDP
Syslog	System Parameters (hostname, Banner)
System Information	Front-panel-security
Telnet Access	DLDP
Traffic/Security Filters	OOBM
VLAN Mirroring (1 static VLAN)/Port mirroring	Switch interconnect
Voice VLAN	Airwave Controller IP configuration
Web Authentication RADIUS Support	Aruba Central integration
Web UI	Captive portal commands
Log IP address of an ACL match	Consolidated Client View
access-list logtimer	IPsec for Zero Touch Provisioning
UFD: Uplink Failure Detection	Local User roles
Wake-on-LAN for a Specific VLAN	Port QoS Trust Mode
WebUI Inactivity Timer	Per-port Tunneled node
Control Plane Protection	Zero-touch provisioning - DHCP, Activate
Egress ACLs	ClearPass support
Device profile - switch auto configuration	HTTP redirection/Captive portal
Device profile: Auto configuration with Aruba AP detection	Device profile: LLDP Authentication Bypass with AP detection
Tunneled Node enhancement: fallback to switching	RADIUS Port Speed VSA
Rogue AP isolation	Dynamic ARP Protection
DHCP Option 82	Dynamic IP Lockdown
DHCP snooping	Eavesdrop Protection
Distributed Trunking	GVRP
RMON 1,2,3,9	Private VLANs
SavePower Features	IP SLA
sFlow	sys-debug acl
VxLAN	MAC Based VLANs (MBV)
Smartlink	RBAC: Role Based Access Control
Fault Finder extended to cover Flapping Transceiver Mitigation	RADIUS Service Tracking
Fault Finder (Per Port Enable)	sys-debug destination
SNMP Trap Throttling	Protocol VLANs

Acronym	Definition
ACL	Access Control List
AMP	AirWave Management Platform
AP	Access Point
BYOD	Bring Your Own Device
BPS	Backplane Stacking
CoA	Change of Authorization
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DoS	Denial-of-Service
EWA	Enhanced Web Authentication
IP	Internet Protocol
HA	High Availability
HMAC-SHA1	Hash-based Message Authentication Code used with the SHA-1 cryptographic hash function.
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
ID	Identifier
IP	Internet Protocol

Table Continued

Acronym	Definition
L3	The third, or routing, layer of the open systems interconnection (OSI) model. The network layer routes data to different LANs and Wide Area Networks (WANs) based on network addresses.
LAN	Local Area Network
MAC	Media Access Control
MAFR	MAC Authentication Failure Redirect
MAS	Management Interface Specification
NMS	Network Management System
PVOS	ArubaOS-Switch Operating System
RADIUS	Remote Authentication Dial In User Service
SNMP	Simple Network Management Protocol
VLAN	Virtual Local Area Network
VSA	Vendor Specific Attribute
VSF	Virtual Switching Framework
ZTP	Zero Touch Provisioning