HP Networking and Cisco CLI Reference Guide

Table of Contents

HP Networking and Cisco CLI Reference Guide

Introduction

This CLI Reference Guide is designed to help HP partners and customers who:

- Manage multi-vendor networks that include HP and Cisco switches
- Have experience deploying Cisco switches and are now deploying HP switches

This CLI Reference Guide compares many of the common commands in three switch operating systems: HP ProVision, Comware 5, and Cisco operating systems.

The HP ProVision operating system runs on HP 3500, 5400zl, 6200yl, 6600, and 8200zl Switch Series. (Other HP switches use an operating system that is very similar to the ProVision operating system.) Comware 5 runs on H3C and 3Com switches, which are now part of the HP Networking portfolio.

The commands included in this guide were tested on the following:

- HP 3500yl-24G switches running ProVision K.14.41 software
- 3Com 3CRS48G-24P-91 switches running Comware 5.20 release 2202P15
- Cisco WS-C3560-24PS switches running Cisco IOS Release 12.2(46)SE

Additional HP ProVision ASIC, H3C or 3Com, and Cisco switches and routers were used to provide systems connectivity and operational support as necessary. Likewise, various computers and voice over IP (VoIP) phones were used to help test functionality and provide output for commands, such as **show** or **display** commands.

Although HP Networking conducted extensive testing to create this guide, it is impossible to test every conceivable configuration and scenario. This document, therefore, cannot be assumed to be complete as it applies to every environment or each manufacturer's complete product platforms and software versions. For complete and detailed use of all commands and their options, refer to each manufacturer's documentation accordingly.

Using This Guide

This CLI Reference Guide provides CLI command comparisons in two different formats:

- Side-by-side comparison—The basic commands required to execute a given function in each of the operating systems are listed in a table. In this side-by-side comparison, each platform's commands do not always start at the top of the column. Instead, commands that have similar functions are aligned side-by-side so that you can easily "translate" the commands on one platform with similar commands on another platform.

- Detailed comparison—Beneath the side-by-side comparison, a more in-depth comparison is provided, displaying the output of the command and options.

Occasionally, there are few, if any, similarities among the commands required to execute a function or feature in each operating system. In these instances, each column has the commands necessary to implement the specific function or feature, and the side-by-side comparison does not apply.

Comware 5 Differences

If you are familiar with either the HP ProVision CLI or the Cisco CLI, you will notice that the Comware 5 CLI is organized slightly differently. Comware 5 was designed for networks provisioned by Internet Service Providers (ISPs). Many features and functions—such as security and quality of service (QoS)—are multi-tiered to support the different needs for multiple entities accessing the same switch.

Navigation Differences Among CLIs

Basic CLI navigation on all three platforms is very similar, with one notable difference:

- With ProVision, you can use the **Tab** key for command completion; you can also use the **Tab** key or the **?** key to find more command options
- With Comware 5, you can use the **Tab** key for command completion, but you use the **?** key to find more command options
- With Cisco, you use the **Tab** key for command completion, but you use the **?** key to find more command options

Configuration Differences Among CLIs

Most commands for port-to-VLAN assignments, interface IP addressing, and interface-specific routing protocol configuration are executed differently on the three platforms:

- On ProVision, you configure the aforementioned components in a VLAN context.
- On Comware 5, you configure the aforementioned components in an interface context.
- On Cisco, you configure the aforementioned components in an interface context.

Terminology Differences

Among the three operating systems, there are some differences in the terms used to describe features. The table on the following page lists three such terms that could be confusing. For example, in the ProVision operating system, aggregated interfaces are called *trunks*. In the Comware 5 operating system, the term is *bridge aggregation*, while on Cisco it is *EtherChannel*.

The confusion can arise because the term *trunk* is used differently in Cisco and Comware 5. In these operating systems, trunk refers to an interface that is configured to support 802.1Q (VLAN). That is, an interface that is configured to support multiple VLANs is called a trunk in Cisco and Comware 5. In the ProVision operating system, on the other hand, an interface that supports multiple VLANs is *tagged*.

Interface use	ProVision	Comware 5	Cisco
Non-802.1Q interfaces (such as computers or printers)	Untagged	Access	Access
802.1Q interfaces (such as switch-to-switch, switch-to-server, and switch-to-VoIP phones)	Tagged	Trunk	Trunk
Aggregated interfaces	Trunk	bridge aggregation	etherchannel

Comparing Frequently Used Commands

The table below lists frequently used commands for each operating system.

*	ProVision	*	Comware 5	*	Cisco
U	enable	U	system-view	U	enable
U/P	show flash	U	Dir	U/P	show flash
U/P	show version	U/S	display version	U/P	show version
P	show run	U/S	display current-configuration	P	show run
P	show config	U/S	display saved-configuration	P	show start
U/P	show history	U/S	display history	U/P	show history
U/P	show logging	U/S	display info-center	U/P	show logging
U/P	show ip route	U/S	display ip routing-table	U/P	show ip route
U/P	show ip	U/S	display ip interface brief	U/P	show ip interface brief
U/P	show interface brief	U/S	display brief interfaces	U/P	show interfaces status
P	erase start	U	reset saved	P	erase start
P	show config <filename>	U	more <filename>	P	more flash:/<filename>
P	reload	U	Reboot	P	reload
P	write memory	U/S	Save	P	write memory
P	show tech	U/S	display diagnostic-information	U/P	show tech-support
U/P/C	show	U/S	Display	U/P	show
U/P/C	no	U/S	Undo	P	no
C	end	S	Return	C	end
U/P/C	exit	U/S	Quit	U/P/C	exit
P/C	erase	U/S	Delete	P	erase
P/C	copy	U	copy/tftp	P	copy
C	hostname	S	Sysname	C	hostname
C	logging	S	info-center	C	logging
C	router rip	S	Rip	C	router rip
C	router ospf	S	Ospf	C	router ospf
C	ip route	S	ip route-static	C	ip route
C	access-list	S	Acl	C	access-list
C	redistribute	S	import-route	C	redistribute

* Context Legend	ProVision	Comware 5	Cisco
U = User Exec / User View	ProVision>	<Comware5>	Cisco>
P = Privileged Exec	ProVision#		Cisco#
S = System View		[Comware5]	
C = Configuration	ProVision(config)#		Cisco(config)#

Chapter 1 Basic Switch Management

This chapter compares commands for:

- Management access
- Configuration access
- Console access
- Switch reload
- USB interface (ProVision only)
- System and environment
- Remote management sessions (viewing and terminating)
- Tech support output
- Filtering output of **show running-config** and **display current-configuration** commands
- Motd
- Source interface for management communications

a) Management Access

ProVision	Comware 5	Cisco

`ProVision> enable`	`<Comware5> system-view`
	`System View: return to User View with Ctrl+Z.`
		`Cisco> enable`

`ProVision#`	`[Comware5]`	`Cisco#`

ProVision

```
ProVision> enable

ProVision#
```

Comware 5

```
<Comware5> system-view
System View: return to User View with Ctrl+Z.

[Comware5]
```

Cisco

```
Cisco> enable

Cisco#
```

b) Configuration Access

ProVision	Comware 5	Cisco
ProVision# configure	***No command, see note below***	Cisco# configure terminal Enter configuration commands, one per line. End with CNTL/Z.
ProVision(config)#		Cisco(config)#

ProVision

```
ProVision# configure ?
 terminal              Optional keyword of the configure command.
 <cr>

ProVision# configure

ProVision(config)#
```

Comware 5

Comware 5 does not have a specific configuration mode, when at "System View" context, configuration commands are entered directly at that prompt.

When configuring interfaces, protocols, etc, the prompt will change to indicate that sub-level.

Cisco

```
Cisco# configure ?
  confirm            Confirm replacement of running-config with a new config
                     file
  memory             Configure from NV memory
  network            Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  replace            Replace the running-config with a new config file
  revert             Parameters for reverting the configuration
  terminal           Configure from the terminal
  <cr>

Cisco_#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Cisco(config)#
```

c) Console Access—Baud Rate

ProVision	Comware 5	Cisco
ProVision(config)# console baud-rate ?	[Comware5]user-interface aux 0 [Comware5-ui-aux0]speed ?	Cisco(config-line)#line console 0 Cisco(config-line)#speed ?

ProVision

```
ProVision(config)# console baud-rate ?
 speed-sense
 1200
 2400
 4800
 9600
 19200
 38400
 57600
 115200

ProVision(config)# console baud-rate speed-sense  (default)

ProVision(config)# console baud-rate 9600
```

Comware 5

```
[Comware5]user-interface aux 0

[Comware5-ui-aux0]speed ?
  300     Only async serial user terminal interface can be configured
  600     Only async serial user terminal interface can be configured
  1200    Only async serial user terminal interface can be configured
  2400    Only async serial user terminal interface can be configured
  4800    Only async serial user terminal interface can be configured
  9600    Only async serial user terminal interface can be configured
  19200   Only async serial user terminal interface can be configured
  38400   Only async serial user terminal interface can be configured
  57600   Only async serial user terminal interface can be configured
  115200  Only async serial user terminal interface can be configured

[Comware5-ui-aux0]speed 19200 ?
  <cr>

[Comware5-ui-aux0]speed 19200  (default)
```

Cisco

```
Cisco(config)#line console 0

Cisco(config-line)#speed ?
  <0-4294967295>  Transmit and receive speeds

Cisco(config-line)#speed 9600  (default)
```

c) Console Access—Timeout

ProVision	Comware 5	Cisco

`ProVision(config)# console inactivity-timer ?`	`[Comware5]user-interface aux 0`
	`[Comware5-ui-aux0]idle-timeout 10`
		`Cisco(config)#line console 0`
		`Cisco(config-line)#exec-timeout ?`

ProVision

```
ProVision(config)# console inactivity-timer ?
 0
 1
 5
 10
 15
 20
 30
 60
 120

ProVision(config)# console inactivity-timer 0   (default)

ProVision(config)# console inactivity-timer 120
```

Comware 5

```
[Comware5]user-interface aux 0

[Comware5-ui-aux0]idle-timeout ?
  INTEGER<0-35791>  Specify the idle timeout in minutes for login user.

[Comware5-ui-aux0]idle-timeout 10  (default)
```

Cisco

```
Cisco(config)#line console 0

Cisco(config-line)#exec-timeout ?
  <0-35791>  Timeout in minutes

Cisco(config-line)#exec-timeout 5 ?
  <0-2147483>  Timeout in seconds

Cisco(config-line)#exec-timeout 10 0  (default)

Cisco(config)#line vty 0 4

Cisco(config-line)#exec-timeout 5 0
```

d) Reload

ProVision	Comware 5	Cisco
`ProVision# reload ?`	`<Comware5>reboot`	`Cisco#reload ?`
`ProVision# no reload`		

ProVision

```
ProVision# reload ?
 after                  Warm reboot in a specified amount of time.
 at                     Warm reboot at a specified time; If the mm/dd/yy
                        is left blank, the current day is assumed.
 <cr>

ProVision# no reload
```

Comware 5

```
[Comware5]quit
<Comware5>reboot ?
  slot  Specify the slot number
  <cr>
```

Cisco

```
 Cisco#reload ?
  /noverify  Don't verify file signature before reload.
  /verify    Verify file signature before reload.
  LINE       Reason for reload
  at         Reload at a specific time/date
  cancel     Cancel pending reload
  in         Reload after a time interval
  <cr>
```

e) USB Interface

ProVision	Comware 5	Cisco
`ProVision# dir`	***not an available feature***	***not an available feature***

ProVision

```
ProVision# dir
Listing Directory /ufa0:
-rwxrwxrwx    1     9533682 Mar 11 14:55 K_14_09.SWI
-rwxrwxrwx    1         978 Oct 25 20:37 ProVision_Config.cfg
-rwxrwxrwx    1     9798890 Aug 27 12:40 K_14_41.SWI

ProVision# show usb-port
 USB port status: enabled
 USB port power status: power on      (USB device detected in port)
```

Comware 5

not an available feature

Cisco

not an available feature

f) System and Environment

ProVision	Comware 5	Cisco
ProVision# show modules	<Comware5>display device manuinfo	Cisco#show inventory
ProVision# show system fans	<Comware5>display fan	Cisco#show env fan
ProVision# show system power-supply	<Comware5>display power	Cisco#show env power
ProVision# show system temperature	<Comware5>display environment	Cisco#show env temperature

ProVision

```
ProVision# show modules
 Status and Counters - Module Information
  Chassis: 3500yl-24G J8692A         Serial Number:   xxxxxxxxx
  Slot  Module Description                       Serial Number
  ----- ---------------------------------------- -------------

ProVision# show system fans
Fan Information
  Num   | State        | Failures
-------+-------------+----------
Sys-1  | Fan OK       |   0
0 / 1 Fans in Failure State
0 / 1 Fans have been in Failure State

ProVision# show system power-supply
Power Supply Status:
 PS# |   State      |   AC/DC  + V    | Wattage
 ----+-------------+-----------------+---------
   1 | Powered      |  -- ----         |    0
   1 /  1 supply bays delivering power.

ProVision# show system temperature
System Air Temperatures
  #    |Current Temp | Max Temp | Min Temp | Threshold | OverTemp
-------+-------------+----------+----------+-----------+----------
Sys-1  |     25C     |    28C   |    21C   |     55C   |    NO
```

Comware 5

```
<Comware5>display device ?
  frame     Frame number
  manuinfo  Manufacture information
  shelf     Shelf number
  slot      Specify the slot number
  verbose   Display detail information
  <cr>

<Comware5>display device manuinfo ?
  <cr>

<Comware5>display device manuinfo
slot 1
DEVICE_NAME          : 3CRS48G-24P-91
DEVICE_SERIAL_NUMBER : xxxxxxxxx
MAC_ADDRESS          : 0022-57BC-D900
MANUFACTURING_DATE   : 2009-02-25
```

```
VENDOR_NAME           : 3COM


<Comware5>display device verbose ?
  <cr>

<Comware5>display device verbose
 Slot 1
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      28      REV.C  NULL    002     604        IVL    MAIN       Normal
slot 1 info:
Status       : Normal
Type         : MAIN
Software Ver : 5.20 Release 2202P15
PCB Ver      : REV.C
FPGA Ver     : NULL
BootRom Ver  : 604
CPLD Ver     : 002
Chip         : 0
    Learning Mode: IVL


<Comware5>display fan ?
  slot  Display slot ID
  <cr>

<Comware5>display fan
 Slot 1
      FAN    1
      State    : Normal


<Comware5>display power ?
  slot  Display slot ID
  <cr>

<Comware5>display power
 Slot 1
      Power    1
      State    : Normal
      Type     : AC


<Comware5>display environment ?
  <cr>

<Comware5>display environment
 System Temperature information (degree centigrade):
----------------------------------------------------
 SlotNo    Temperature       Lower limit      Upper limit
 1         36                0                55
```

Cisco

```
Cisco#show inventory
NAME: "1", DESCR: "WS-C3560-24PS"
PID: WS-C3560-24PS-E   , VID: V06, SN: xxxxxxxxx

Cisco#show env fan
FAN is OK

Cisco#show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
 1  Built-in                                         Good

Cisco#show env temperature
TEMPERATURE is OK
```

g) Remote Management Sessions—Viewing

ProVision	Comware 5	Cisco
`ProVision# show telnet`	`<Comware5> display users`	`Cisco# show users`

ProVision

```
ProVision# show telnet
 Telnet Activity
 Source IP Selection: 10.0.100.24
 --------------------------------------------------------
   Session  :      1
   Privilege: Manager
   From     : Console
   To       :
   --------------------------------------------------------
   Session  : **   2
   Privilege: Manager
   From     : 10.99.1.162
   To       :
   --------------------------------------------------------
   Session  :      3
   Privilege: Manager
   From     : 10.99.1.161
   To       :
```

Comware 5

```
<Comware5> display users ?
  all   The information of all user terminal interfaces
  <cr>

<Comware5> display users
The user application information of the user interface(s):
  Idx UI       Delay    Type Userlevel
F 0   AUX 0    00:00:00      3
  14  VTY 0    00:00:08 TEL  3

Following are more details.
AUX 0   :
        User name: admin
VTY 0   :
        User name: admin
        Location: 10.99.1.161
 +    : Current operation user.
 F    : Current operation user work in async mode.


<Comware5> dis users all
The user application information of all user interfaces:
  Idx UI       Delay    Type Userlevel
F 0   AUX 0    00:00:00      3
  1   AUX 1
  2   AUX 2
  3   AUX 3
  4   AUX 4
  5   AUX 5
  6   AUX 6
  7   AUX 7
  8   AUX 8
+ 14  VTY 0    00:00:28 TEL  3
  15  VTY 1
  16  VTY 2
  17  VTY 3
  18  VTY 4

Following are more details.
AUX 0   :
        User name: admin
VTY 0   :
        User name: admin
        Location: 10.99.1.161
 +    : User-interface is active.
 F    : User-interface is active and work in async mode.
```

Cisco

```
Cisco# show users
    Line       User       Host(s)              Idle       Location
   0 con 0     manager    idle                 03:29:53
   1 vty 0     swmanager   idle                     1w2d 10.0.1.11
*  2 vty 1     swmanager   idle                 00:00:00 10.99.1.162
   3 vty 2     swmanager   idle                 00:10:20 10.0.100.24
  Interface      User        Mode                     Idle     Peer Address
```

g) Remote Management Sessions—Terminating

ProVision	Comware 5	Cisco
`ProVision# kill 3`	`<Comware5> free user-interface vty  0`	`Cisco# clear line 3`

ProVision

```
ProVision# kill 3

ProVision# show telnet
 Telnet Activity
 Source IP Selection: 10.0.100.24
 --------------------------------------------------------
 Session  :     1
 Privilege: Manager
 From     : Console
 To       :
 --------------------------------------------------------
 Session  : **  2
 Privilege: Manager
 From     : 10.99.1.162
 To       :
```

Comware 5

```
<Comware5>free ?
  ftp               Free FTP user
  user-interface    User terminal interface
  web-users         Web management users

<Comware5>free user-interface ?
  INTEGER<0-18>  Specify one user terminal interface
  aux            Aux user terminal interface
  vty            Virtual user terminal interface

<Comware5>free user-interface vty ?
  INTEGER<0-4>  Specify one user terminal interface

<Comware5>free user-interface vty 0
Are you sure to free user-interface vty0? [Y/N]:y
 [OK]

<Comware5>dis users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
F 0   AUX 0   00:00:00      3

Following are more details.
AUX 0    :
        User name: admin
 +    : Current operation user.
 F    : Current operation user work in async mode.
```

Cisco

```
Cisco#clear line 3
[confirm]
 [OK]

Cisco#show users
    Line       User       Host(s)              Idle       Location
   0 con 0     manager    idle                 03:30:07
   1 vty 0     swmanager   idle                     1w2d 10.0.1.11
*  2 vty 1     swmanager   idle                 00:00:00 10.99.1.162
  Interface      User        Mode                     Idle     Peer Address
```

h) Tech Support Information Output Listing

ProVision	Comware 5	Cisco
`ProVision# show tech ?`	`<Comware5>display diagnostic-information`	`Cisco#show tech-support ?`

ProVision

```
ProVision# show tech ?
 all                     Display output of a predefined command sequence used by
                         technical support.
 buffers                 Display output of a predefined command sequence used by
                         technical support.
 custom                  Display output of a predefined command sequence used by
                         technical support.
 instrumentation         Display output of a predefined command sequence used by
                         technical support.
 mesh                    Display output of a predefined command sequence used by
                         technical support.
 route                   Display output of a predefined command sequence used by
                         technical support.
 statistics              Display output of a predefined command sequence used by
                         technical support.
 transceivers            Display output of a predefined command sequence used by
                         technical support.
 vrrp                    Display output of a predefined command sequence used by
                         technical support.
 <cr>
```

Comware 5

```
<Comware5>display diagnostic-information ?
  <cr>

<Comware5>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:
```

Cisco

```
Cisco#show tech-support ?
  cef           CEF related information
  ipc           IPC related information
  ipmulticast   IP multicast related information
  ospf          OSPF related information
  page          Page through output
  password      Include passwords
  |             Output modifiers
  <cr>
```

i) Filtering Output show running-config and display current-configuration

ProVision	Comware 5	Cisco
	`<Comware5>display current-configuration | ?`	`Cisco#show running-config | ?`
`ProVision# show running-config | include <text-to-find>`	`<Comware5>display current-configuration | include <text-to-find>`	`Cisco#show running-config | include <text-to-find>`

ProVision

```
ProVision# show run | include <text-to-find>
```

Comware 5

```
<Comware5>display current-configuration | ?
  begin    Begin with the line that matches
  exclude  Match the character strings excluding the regular expression
  include  Match the character strings including with the regular expression

<Comware5>display current-configuration | include ?
  TEXT  Regular expression

<Comware5>display current-configuration | include <text-to-find>
```

Cisco

```
Cisco#show running-config | ?
  append    Append redirected output to URL (URLs supporting append operation
            only)
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output to URL
  tee       Copy output to URL


Cisco#show running-config | include <text-to-find>
```

j) Motd

ProVision	Comware 5	Cisco
ProVision(config)# banner motd # Enter TEXT message. End with the character'#'	[Comware5]header motd # Please input banner content, and quit with the character '#'.	Cisco(config)#banner motd # Enter TEXT message. End with the character '#'.

ProVision

```
ProVision(config)# banner motd #
Enter TEXT message.  End with the character'#'


 This is a secure lab network, do not connect to any production systems.

     Authorized users only!
#
```

Comware 5

```
[Comware5]header motd #
Please input banner content, and quit with the character '#'.


This is a secure lab network, do not connect to any production systems.

    Authorized users only!
#
```

Cisco

```
Cisco(config)#banner motd #
Enter TEXT message.  End with the character '#'.


This is a secure lab network, do not connect to any production systems.

    Authorized users only!
#
```

k) Source Interface for Management Communications

ProVision	Comware 5	Cisco
ProVision(config)# ip source-interface ?		Cisco(config)#ip <service> source-interface ?
ProVision(config)# ip source-interface syslog vlan 100	[Comware5]info-center loghost source Vlan-interface 100	Cisco(config)#logging source-interface vlan 100
ProVision(config)# ip source-interface radius 10.0.100.24	[Comware5]radius nas-ip 10.0.100.48	Cisco(config)#ip radius source-interface vlan 100
ProVision(config)# ip source-interface tacacs 10.0.100.24	[Comware5]hwtacacs nas-ip 10.0.100.48	Cisco(config)#ip tacacs source-interface vlan 100
	[Comware5]ftp client source interface Vlan-interface 100	Cisco(config)#ip ftp source-interface vlan 100
ProVision(config)# ip source-interface syslog vlan 100	[Comware5]tftp client source interface Vlan-interface 100	Cisco(config)#ip tftp source-interface vlan 100
ProVision(config)# ip source-interface sntp vlan 100	[Comware5]ntp source-interface Vlan-interface 100	Cisco(config)#ntp source vlan 100
ProVision(config)# ip source-interface telnet vlan 100	[Comware5]telnet client source interface Vlan-interface 100	Cisco(config)#ip telnet source-interface vlan 100
	[Comware5]ssh client source interface Vlan-interface 100	Cisco(config)#ip ssh source-interface vlan 100
ProVision(config)# snmp-server trap-source 10.0.100.24	[Comware5]snmp-agent trap source Vlan-interface 100	Cisco(config)#snmp-server source-interface traps vlan 100

ProVision

```
ProVision(config)# ip source-interface ?
 radius                RADIUS protocol.
 sntp                  SNTP protocol.
 syslog                SYSLOG protocol.
 tacacs                TACACS+ protocol.
 telnet                TELNET protocol.
 tftp                  TFTP protocol.
 all                   All listed above protocols.


ProVision(config)# ip source-interface all ?
 IP-ADDR               Specify the IP address.
 loopback              Specify the loopback interface.
 vlan                  Specify the VLAN interface.


ProVision(config)# ip source-interface all vlan 100


ProVision(config)# snmp-server trap-source 10.0.100.24
 <cr>
ProVision(config)# snmp-server trap-source 10.0.100.24


ProVision# show ip source-interface ?
 detail                Show detailed information.
 radius                Specify the name of protocol.
 sntp                  Specify the name of protocol.
 status                Show status information.
 syslog                Specify the name of protocol.
 tacacs                Specify the name of protocol.
 telnet                Specify the name of protocol.
 tftp                  Specify the name of protocol.
 <cr>
```

```
ProVision# show ip source-interface

 Source-IP Configuration Information

  Protocol | Admin Selection Policy  IP Interface   IP Address
  -------- + ----------------------- -------------- ---------------
  Tacacs   | Configured IP Interface vlan 100
  Radius   | Configured IP Interface vlan 100
  Syslog   | Configured IP Interface vlan 100
  Telnet   | Configured IP Interface vlan 100
  Tftp     | Configured IP Interface vlan 100
  Sntp     | Configured IP Interface vlan 100
```

Comware 5

```
[Comware5]info-center loghost ?
  X.X.X.X  Logging host ip address
  source   Set the source address of packets sent to loghost

[Comware5]info-center loghost source ?
  Vlan-interface  VLAN interface

[Comware5]info-center loghost source Vlan-interface 100 ?
  <cr>

[Comware5]info-center loghost source Vlan-interface 100


[Comware5]radius nas-ip 10.0.100.48

[Comware5]hwtacacs nas-ip 10.0.100.48

[Comware5]ftp client source interface Vlan-interface 100

[Comware5]tftp client source interface Vlan-interface 100

[Comware5]ntp source-interface Vlan-interface 100

[Comware5]telnet client source interface Vlan-interface 100

[Comware5]ssh client source interface Vlan-interface 100

[Comware5]snmp-agent trap source Vlan-interface 100
```

Cisco

```
Cisco(config)#ip ftp ?
  passive           Connect using passive mode
  password          Specify password for FTP connections
  source-interface  Specify interface for source address in FTP connections
  username          Specify username for FTP connections

Cisco(config)#ip ftp source-interface ?
  Async              Async interface
  Auto-Template      Auto-Template interface
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Filter             Filter interface
  Filtergroup        Filter Group interface
  GigabitEthernet    GigabitEthernet IEEE 802.3z
  GroupVI            Group Virtual interface
  Lex                Lex interface
  Loopback           Loopback interface
  Null               Null interface
  Port-channel       Ethernet Channel of interfaces
  Portgroup          Portgroup interface
  Pos-channel        POS Channel of interfaces
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing
  Vlan               Catalyst Vlans
  fcpa               Fiber Channel

Cisco(config)#ip ftp source-interface vlan 100 ?
  <cr>

Cisco(config)#ip ftp source-interface vlan 100

(the following additional commands are similar the above ftp example)

Cisco(config)#ip tftp source-interface vlan 100

Cisco(config)#ip rcmd source-interface vlan 100

Cisco(config)#ip telnet source-interface vlan 100

Cisco(config)#ip ftp source-interface vlan 100

Cisco(config)#ip radius source-interface vlan 100

Cisco(config)#ip tacacs source-interface vlan 100

Cisco(config)#logging source-interface vlan 100

Cisco(config)#ntp source vlan 100

Cisco(config)#ip ssh source-interface vlan 100

Cisco(config)#snmp-server source-interface traps vlan 100
```

Chapter 2 Switch User ID and Password

This chapter focuses on:

- Configuring local user ID (UID) and password options
- Recovering from a lost password
- Protecting the local password

a) Local User ID and Password

ProVision	Comware 5	Cisco
		`Cisco(config)#enable password 0 <password>`
		`Cisco(config)#enable secret 0 <password>`
	`[Comware5]super password level 3 simple password`	
	`[Comware5]super password level 3 cipher password`	

`ProVision(config)# password manager user-name <name> plaintext <password>`	`[Comware5]local-user <name>`
	`[Comware5-luser-manager]password simple <password>`
	`[Comware5-luser-manager]authorization-attribute level 3`
		`Cisco(config)#username <name> privilege 15 password <password>`

`ProVision(config)# password operator user-name <name> plaintext <password>`	`[Comware5]local-user <name>`
	`[Comware5-luser-operator]password simple <password>`
	`[Comware5-luser-operator]authorization-attribute level 1`
		`Cisco(config)#username <name> privilege 0 password <password>`

`ProVision(config)# password manager user-name <name> sha1 <password>`	`[Comware5]local-user <name>`
	`[Comware5-luser-manager]password cipher <password>`
	`[Comware5-luser-manager]authorization-attribute level 3`	

`ProVision(config)# password operator user-name <name> sha1 <password>`	`[Comware5]local-user <name>`
	`[Comware5-luser-operator]password cipher <password>`
	`[Comware5-luser-operator]authorization-attribute level 1`	

	`[Comware5]user-interface aux 0`	`Cisco(config)#line console 0`

	[Comware5-ui-aux0]authentication-mode scheme	Cisco(config-line)#login local
	[Comware5]user-interface vty 0 4	Cisco(config)#line vty 0 4
	[Comware5-ui-vty0-4]authentication-mode scheme	Cisco(config-line)#login local

ProVision

```
ProVision(config)# password ?
 operator              Configure operator access.
 manager               Configure manager access.
 all                   Configure all available types of access.

ProVision(config)# password manager ?
 plaintext             Enter plaintext password.
 sha1                  Enter SHA-1 hash of password.
 user-name             Set username for the specified user category.
 <cr>

ProVision(config)# password manager user-name ?
 ASCII-STR             Enter an ASCII string for the 'user-name'
                       command/parameter.

ProVision(config)# password manager user-name manager ?
 plaintext             Enter plaintext password.
 sha1                  Enter SHA-1 hash of password.
 <cr>

ProVision(config)# password manager user-name manager plaintext ?
 PASSWORD-STR          Set password

ProVision(config)# password manager user-name manager plaintext password

ProVision(config)# password operator user-name operator plaintext password
```

Comware 5

```
[Comware5]super ?
  password  Specify password

[Comware5]super password ?
  cipher  Display password with cipher text
  level   Specify the entering password of the specified priority
  simple  Display password with plain text

[Comware5]super password level ?
  INTEGER<1-3>  Priority level

[Comware5]super password level 3 ?
  cipher  Display password with cipher text
  simple  Display password with plain text

[Comware5]super password level 3 simple ?
  STRING<1-16>  Plain text password string

[Comware5]super password level 3 simple password ?
```

```
  <cr>

[Comware5]super password level 3 simple password

[Comware5]super password level 3 cipher password


[Comware5]local-user ?
  STRING<1-55>           Specify the user name, the max length of username is
                         55 characters and the domainname can not be included.
  password-display-mode  Specify password display mode

[Comware5]local-user manager
New local user added.

[Comware5-luser-manager]password ?
  cipher  Display password with cipher text
  simple  Display password with plain text

[Comware5-luser-manager]password simple password ?
  <cr>

[Comware5-luser-manager]password simple password

[Comware5-luser-manager]?
Luser view commands:
  access-limit             Specify access limit of local user
  authorization-attribute  Specify authorization attribute of user
  bind-attribute           Specify bind attribute of user
  display                  Display current system information
  expiration-date          Specify expiration date configuration information
  group                    Specify user group of user
  mtracert                 Trace route to multicast source
  password                 Specify password of local user
  ping                     Ping function
  quit                     Exit from current command view
  return                   Exit to User View
  save                     Save current configuration
  service-type             Specify service-type of local user
  state                    Specify state of local user
  tracert                  Trace route function
  undo                     Cancel current setting

[Comware5-luser-manager]authorization-attribute ?
  acl              Specify ACL number of user
  callback-number  Specify dialing character string for callback user
  idle-cut         Specify idle-cut of local user
  level            Specify level of user
  user-profile     Specify user profile of user
  vlan             Specify VLAN ID of user
  work-directory   Specify directory of user

[Comware5-luser-manager]authorization-attribute level ?
  INTEGER<0-3>  Level of user

[Comware5-luser-manager]authorization-attribute level 3
```

```
[Comware5-luser-manager]service-type ?
  ftp         FTP service type
  lan-access  LAN-ACCESS service type
  portal      Portal service type
  ssh         Secure Shell service type
  telnet      TELNET service type
  terminal    TERMINAL service type

[Comware5-luser-manager]service-type terminal ?
  ssh     Secure Shell service type
  telnet  TELNET service type
  <cr>

[Comware5-luser-manager]service-type terminal


[Comware5]local-user manager
 New local user added.

[Comware5-luser-manager]password ?
  cipher  Display password with cipher text
  simple  Display password with plain text

[Comware5-luser-manager]password cipher ?
  STRING<1-63>/<88>  Plain/Encrypted password string

[Comware5-luser-manager]password cipher password


[Comware5]user-interface aux 0
[Comware5-ui-aux0]?
User-interface view commands:
  acl                    Specify acl filtering
  activation-key         Specify a character to begin a terminal session
  authentication-mode    Terminal interface authentication mode
  auto-execute           Do something automatically
  command                Specify command configuration information
  databits               Specify the databits of user terminal interface
  display                Display current system information
  escape-key             Specify a character to abort a process started by
                         previously executed command
  flow-control           Specify the flow control mode of user terminal interface
  history-command        Record history command
  idle-timeout           Specify the connection idle timeout for login user
  mtracert               Trace route to multicast source
  parity                 Specify the parity mode of user interface
  ping                   Ping function
  protocol               Set user interface protocol
  quit                   Exit from current command view
  return                 Exit to User View
  save                   Save current configuration
  screen-length          Specify the lines displayed on one screen
  set                    Specify user terminal interface parameters
  shell                  Enable terminal user service
  speed                  Specify the TX/RX rate of user terminal interface
  stopbits               Specify the stop bit of user terminal interface
  terminal               Specify terminal type
  tracert              Trace route function
  undo                 Cancel current setting
  user                 Specify user's parameter of terminal interface

[Comware5-ui-aux0]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-aux0]authentication-mode scheme ?
  <cr>

[Comware5-ui-aux0]authentication-mode scheme

[Comware5]user-interface vty 0 4
[Comware5-ui-vty0-4]authentication-mode scheme
```

Cisco

```
Cisco(config)#enable ?
  last-resort  Define enable action if no TACACS servers respond
  password     Assign the privileged level password
  secret       Assign the privileged level secret
  use-tacacs   Use TACACS to check enable passwords

Cisco(config)#enable password ?
  0      Specifies an UNENCRYPTED password will follow
  7      Specifies a HIDDEN password will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' password
  level  Set exec level password

Cisco(config)#enable password 0 ?
  LINE  The UNENCRYPTED (cleartext) 'enable' password

Cisco(config)#enable password 0 password ?
LINE    <cr>

Cisco(config)#enable password 0 password

Cisco(config)#enable secret ?
  0      Specifies an UNENCRYPTED password will follow
  5      Specifies an ENCRYPTED secret will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' secret
  level  Set exec level password

Cisco(config)#enable secret 0 ?
  LINE  The UNENCRYPTED (cleartext) 'enable' secret

Cisco(config)#enable secret 0 password ?
LINE    <cr>

Cisco(config)#enable secret 0 password

Cisco(config)#username ?
  WORD  User name

Cisco(config)#username manager ?
```

```
  access-class         Restrict access by access-class
  autocommand          Automatically issue a command after the user logs in
  callback-dialstring  Callback dialstring
  callback-line        Associate a specific line with this callback
  callback-rotary      Associate a rotary group with this callback
  dnis                 Do not require password when obtained via DNIS
  nocallback-verify    Do not require authentication after callback
  noescape             Prevent the user from using an escape character
  nohangup             Do not disconnect after an automatic command
  nopassword           No password is required for the user to log in
  password             Specify the password for the user
  privilege            Set user privilege level
  secret               Specify the secret for the user
  user-maxlinks        Limit the user's number of inbound links
  view                 Set view name
  <cr>

Cisco(config)#username manager privilege ?
  <0-15>  User privilege level

Cisco(config)#username manager privilege 15 ?
  access-class         Restrict access by access-class
  autocommand          Automatically issue a command after the user logs in
  callback-dialstring  Callback dialstring
  callback-line        Associate a specific line with this callback
  callback-rotary      Associate a rotary group with this callback
  dnis                 Do not require password when obtained via DNIS
  nocallback-verify    Do not require authentication after callback
  noescape             Prevent the user from using an escape character
  nohangup             Do not disconnect after an automatic command
  nopassword           No password is required for the user to log in
  password             Specify the password for the user
  privilege            Set user privilege level
  secret               Specify the secret for the user
  user-maxlinks        Limit the user's number of inbound links
  view                 Set view name
  <cr>

Cisco(config)#username manager privilege 15 password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) user password

Cisco(config)#username manager privilege 15 password password

Cisco(config)#username operator privilege 0 password password


[to set the use of uid/pw for login on console/vty]

Cisco(config)#line console 0

Cisco(config-line)#login ?
  local   Local password checking
  tacacs  Use tacacs server for password checking
  <cr>
```

```
Cisco(config-line)#login local ?
  <cr>
Cisco(config-line)#login local

Cisco(config)#line vty 0 4
Cisco(config-line)#login local ?
  <cr>
Cisco(config-line)#login local
```

b) Recover Lost Password

ProVision	Comware 5	Cisco
See details below	See details below	See details below

Each procedure requires direct access to the switch through a console cable.

ProVision

Requires direct access to the switch (with console cable)
(with default front panel security settings)

option 1) erase local usernames/passwords by depressing front panel clear button for one second. requires physical access to switch

option 2) execute a factory reset by using a combination/sequence of the "clear" button and the "reset" button. requires physical access to switch

option 3) password recovery procedure requires direct access to the switch (with console cable) and calling HP Networking technical support.

Comware 5

Requires direct access to the switch (with console cable)

enter the Boot Menu:

```
BOOT MENU
1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot
Enter your choice(0-9):
```

Select 7 and then Reboot the switch. The switch will restart in a default configuration.

Cisco

Depending on configuration of the "password-recovery" feature (see section c below), there are two methods available; both require direct access to the switch (with console cable) and depressing the appropriate front panel button.

See the Cisco manuals for exact procedure.

c) Protect Local Password

ProVision	Comware 5	Cisco
`ProVision(config)# no front-panel-security password-clear`	`<Comware5>undo startup bootrom-access enable`	`Cisco(config)#no service password-recovery`
`ProVision(config)# no front-panel-security factory-reset`		
`ProVision(config)# no front-panel-security password-recovery`		
`ProVision# show front-panel-security`	`<Comware5>display startup`	`Cisco#show version`

ProVision

```
Show default state of front panel security:

ProVision# show front-panel-security

Clear Password        - Enabled
  Reset-on-clear      - Disabled
Factory Reset         - Enabled
Password Recovery     - Enabled


ProVision(config)# front-panel-security
 factory-reset         Enable/Disable factory-reset ability
 password-clear        Enable/Disable password clear
 password-recovery     Enable/Disable password recovery.


ProVision(config)# no front-panel-security password-clear
                              **** CAUTION ****
Disabling the clear button prevents switch passwords from being easily reset or recovered.
Ensure that you are familiar with the front panel security options before proceeding.
Continue with disabling the clear button [y/n]? y


ProVision(config)# no front-panel-security factory-reset
                              **** CAUTION ****
Disabling the factory reset option prevents switch configuration and passwords from being
easily reset or recovered.  Ensure that you are familiar with the front panel security
options before proceeding.
Continue with disabling the factory reset option[y/n]? y


ProVision(config)# no front-panel-security password-recovery
Physical access procedure required.
Type 'front-panel-security password-recovery help' for more information.


ProVision# show front-panel-security
Clear Password        - Disabled
Factory Reset         - Disabled
Password Recovery     - Enabled
```

Note – ProVision ASIC will only allow up to two (2) of the above features to be disabled at a time, with one of them being the "clear" button disable, and then choice of the second feature to disable if desired.

Comware 5

From the 3Com Switch 4800G Family Configuration Guide:

"By default, you can press Ctrl+B to enter the Boot ROM menu to configure the Boot ROM. However, this may bring security problems to the device. Therefore, the device provides the function of disabling the Boot ROM access to enhance security of the device. After this function is configured, no matter whether you press Ctrl+B or not, the system does not enter the Boot ROM menu, but enters the command line configuration interface directly."

```
<Comware5>display startup
MainBoard:
 Current startup saved-configuration file: flash:/Comware5_main.cfg
 Next main startup saved-configuration file: flash:/Comware5_main.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: enabled
```

```
<Comware5>undo startup bootrom-access enable
```

```
<Comware5>display startup
MainBoard:
 Current startup saved-configuration file: flash:/Comware5_main.cfg
 Next main startup saved-configuration file: flash:/Comware5_main.cfg
 Next backup startup saved-configuration file: NULL
 Bootrom-access enable state: disabled
```

Cisco

From the Cisco Catalyst 3560 Switch Software Configuration Guide:

"By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted."

```
Cisco#show version
...
The password-recovery mechanism is enabled.
...
```

```
Cisco(config)#no service password-recovery
```

```
Cisco#show version
...
The password-recovery mechanism is disabled.
...
```

Chapter 3 Image File Management

This chapter compares the commands used to manage software images files on HP ProVision, Comware, and Cisco.

The HP ProVision operating system writes to or reads from specific areas of the file storage, depending on the commands you enter. Software image files, configuration files, and local user ID and passwords are stored in dedicated areas of flash. When you enter commands such as **copy** and **show**, the ProVision operating system writes to or reads from these dedicated areas of flash. (For more information, see the management and configuration guide for the HP ProVision ASIC switch you are managing.)

Comware 5 and Cisco platforms use basic file systems. There are no dedicated areas in flash for specific files. You are allowed to create subdirectories and copy and move files just as you would on other "regular" file systems.

ProVision	Comware 5	Cisco
ProVision# show flash	<Comware5>dir	Cisco#show flash:
ProVision# show version	<Comware5>display version	Cisco#show version
ProVision# copy tftp flash 10.0.100.21 K_14_41.swi	<Comware5>tftp 10.1.1.51 get S4800G-CMW520-R2202P12-S56.bin	Cisco#copy tftp://10.0.1.11/c3560-advipservicesk9-mz.122-40.SE.bin flash:c3560-advipservicesk9-mz.122-40.SE.bin
ProVision# copy usb flash K_14_41.swi		
ProVision# copy xmodem flash primary		
ProVision# copy flash flash secondary		
ProVision# copy flash tftp 10.0.100.21 K_14-41.swi	<Comware5>tftp 10.1.1.51 put s4800g-cmw520-r2202p12-s56.bin	Cisco# copy flash:c3560-advipservicesk9-mz.122-46.SE/c3560-advipservicesk9 -mz.122-46.SE.bin tftp://10.0.1.11/c3560-advipservicesk9-mz.122-46.SE.bin
ProVision# copy flash usb K_14_41.swi		
ProVision# copy flash xmodem		

ProVision

```
ProVision# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 9798890   08/27/09 K.14.41
Secondary Image : 9798890   08/27/09 K.14.41
Boot Rom Version: K.12.20
Default Boot    : Primary

ProVision# show version
Image stamp:    /sw/code/build/btm(t4a)
                Aug 27 2009 05:27:43
                K.14.41
                476
Boot Image:     Primary

ProVision# copy ?
 command-output        Specify a CLI command to copy output of.
 config                Copy named configuration file.
 crash-data            Copy the switch crash data file.
 crash-log             Copy the switch log file.
 event-log             Copy event log file.
 flash                 Copy the switch system image file.
 running-config        Copy running configuration file.
 startup-config        Copy in-flash configuration file.
 tftp                  Copy data from a TFTP server.
 usb                   Copy data from a USB flash drive.
 xmodem                Use xmodem on the terminal as the data source.

ProVision# copy tftp ?
 autorun-cert-file     Copy autorun trusted certificate to the switch.
 autorun-key-file      Copy autorun key file to the switch.
 command-file          Copy command script to switch and execute.
 config                Copy data to specified configuration file.
 flash                 Copy data to the switch system image file.
 pub-key-file          Copy the public keys to the switch.
 show-tech             Copy custom show-tech script to switch.
 startup-config        Copy data to the switch configuration file.

ProVision# copy tftp flash ?
 IP-ADDR               Specify TFTP server IPv4 address.
 IPV6-ADDR             Specify TFTP server IPv6 address.

ProVision# copy tftp flash 10.0.100.21 ?
 FILENAME-STR          Specify filename for the TFTP transfer.

ProVision# copy tftp flash 10.0.100.21 K_14_41.swi ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.
 <cr>

ProVision# copy tftp flash 10.0.100.21 K_14_41.swi

ProVision# copy usb ?
 autorun-cert-file     Copy autorun trusted certificate to the switch.
 autorun-key-file      Copy autorun key file to the switch.
 command-file          Copy command script to switch and execute.
 flash                 Copy data to the switch system image file.
 pub-key-file          Copy the public keys to the switch.
 startup-config        Copy data to the switch configuration file.

ProVision# copy usb flash ?
 IMAGE-NAME-STR        Specify filename for the USB transfer.
ProVision# copy usb flash K_14_41.swi ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.
 <cr>

ProVision# copy usb flash K_14_41.swi
```

```
ProVision# copy xmodem flash ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.
 <cr>

ProVision# copy xmodem flash primary ?
 <cr>

ProVision# copy xmodem flash primary
The Primary OS Image will be deleted, continue [y/n]?  y
Press 'Enter' and start XMODEM on your host...

ProVision# copy flash ?
 flash                 Copy to primary/secondary flash.
 tftp                  Copy data to a TFTP server.
 usb                   Copy data to a USB flash drive.
 xmodem                Use xmodem on the terminal as the data
                       destination.
ProVision#
 copy flash flash ?
 primary               Copy to primary flash.
 secondary             Copy to secondary flash.

ProVision# copy flash flash secondary

ProVision# copy flash tftp 10.0.100.21 K_14-41.swi ?
 primary               Copy image primary flash.
 secondary             Copy image secondary flash.
 <cr>

ProVision# copy flash tftp 10.0.100.21 K_14-41.swi

ProVision# copy flash usb ?
 FILENAME-STR          Specify filename for the TFTP transfer.

ProVision# copy flash usb K_14_41.swi

ProVision# copy flash xmodem ?
 primary               Copy image primary flash.
 secondary             Copy image secondary flash.
 <cr>

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

Comware 5

```
<Comware5>dir ?
  /all    List all files
  STRING  [drive][path][file name]
  flash:  Device name
  <cr>

<Comware5>dir
Directory of flash:/

   0     -rw-  10732579  Apr 27 2010 04:01:27   s4800g-cmw520-r2202p12-s56.bin
   1     -rw-    245887  Apr 26 2000 12:07:12   default.diag
   2     -rw-  10576749  Nov 23 2009 10:47:51   s4800g-cmw520-r2202p15-s56.bin
   3     -rw-      2371  Apr 27 2010 02:58:22   Comware5_main.cfg
   5     -rw-      5167  Apr 25 2010 19:27:47   Comware5_backup.cfg
   6     -rw-      2398  Apr 27 2010 04:02:34   Comware5_04272010_0400.cfg

31496 KB total (10420 KB free)

<Comware5>display version
3Com Corporation
Switch 4800G PWR 24-Port Software Version 5.20 Release 2202P15
Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
Switch 4800G PWR 24-Port uptime is 0 week, 0 day, 1 hour, 23 minutes

Switch 4800G PWR 24-Port with 1 Processor
256M    bytes SDRAM
32768K  bytes Flash Memory

Hardware Version is REV.C
CPLD Version is 002
Bootrom Version is 604
[SubSlot 0] 24GE+4SFP+POE Hardware Version is REV.C


<Comware5>tftp ?
  STRING<1-20>  IP address or hostname of a remote system
  ipv6          IPv6 TFTP client

<Comware5>tftp 10.1.1.51 ?
  get   Download file from remote TFTP server
  put   Upload local file to remote TFTP server
  sget  Download securely from remote TFTP server

<Comware5>tftp 10.1.1.51 get ?
  STRING<1-135>  Source filename

<Comware5>tftp 10.1.1.51 get S4800G-CMW520-R2202P12-S56.bin ?
  STRING<1-135>  Destination filename
  source         Specify a source
  <cr>

<Comware5>tftp 10.1.1.51 get S4800G-CMW520-R2202P12-S56.bin


<Comware5>tftp 10.1.1.51 put s4800g-cmw520-r2202p12-s56.bin ?
  STRING<1-135>  Destination filename
  source         Specify a source
  <cr>

<Comware5>tftp 10.1.1.51 put s4800g-cmw520-r2202p12-s56.bin
```

Cisco

```
Cisco#show flash:

Directory of flash:/
  354  drwx         256  Nov 14 2009 16:33:04 -06:00  c3560-advipservicesk9-mz.122-46.SE
  460  -rwx         103   Mar 1 1993 12:24:16 -06:00  info
  353  -rwx        1056   Dec 8 2009 22:33:40 -06:00  vlan.dat
  350  -rwx        7192  Dec 17 2009 17:26:37 -06:00  multiple-fs
  361  -rwx       10586  Dec 17 2009 17:26:37 -06:00  Cisco.cfg
  363  -rwx        5599  Sep 17 2009 22:29:01 -05:00  config.text
  364  -rwx        3121  Dec 17 2009 17:26:37 -06:00  private-config.text

Cisco#show version
Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(46)SE
...
System image file is "flash:c3560-advipservicesk9-mz.122-46.SE/c3560-advipservicesk9-mz.122-
46.SE.bin"
...

Cisco#copy ?
  /erase          Erase destination file system.
  /error          Allow to copy error file.
  /noverify       Don't verify image signature before reload.
  /verify         Verify image signature before reload.
  bs:             Copy from bs: file system
  cns:            Copy from cns: file system
  flash:          Copy from flash: file system
  ftp:            Copy from ftp: file system
  http:           Copy from http: file system
  https:          Copy from https: file system
  logging         Copy logging messages
  null:           Copy from null: file system
  nvram:          Copy from nvram: file system
  rcp:            Copy from rcp: file system
  running-config  Copy from current system configuration
  scp:            Copy from scp: file system
  startup-config  Copy from startup configuration
  system:         Copy from system: file system
  tar:            Copy from tar: file system
  tftp:           Copy from tftp: file system
  tmpsys:         Copy from tmpsys: file system
  vb:             Copy from vb: file system
  xmodem:         Copy from xmodem: file system
  ymodem:         Copy from ymodem: file system

Cisco#copy tftp://10.0.1.11/c3560-advipservicesk9-mz.122-40.SE.bin ?
  flash:          Copy to flash: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tmpsys:         Copy to tmpsys: file system
  vb:             Copy to vb: file system
```

```
Cisco#copy tftp://10.0.1.11/c3560-advipservicesk9-mz.122-40.SE.bin flash:c3560-
advipservicesk9-mz.122-40.SE.bin
Destination filename [c3560-advipservicesk9-mz.122-40.SE.bin]?

Cisco# copy flash:c3560-advipservicesk9-mz.122-46.SE/c3560-advipservicesk9 -mz.122-46.SE.bin
tftp://10.0.1.11/c3560-advipservicesk9-mz.122-46.SE.bin
Address or name of remote host [10.0.1.11]?
Destination filename [c3560-advipservicesk9-mz.122-46.SE.bin]?
```

Chapter 4 Configuration File Management

This chapter compares the commands used to manage configuration files on HP ProVision, Comware, and Cisco.

HP ProVision ASIC switches can store a maximum of three configuration files. Comware 5 and Cisco switches can store multiple configuration files; the only limitation is the amount of available storage space on the switch.

ProVision	Comware 5	Cisco
ProVision# show running-config ?	<Comware5>display current-configuration	Cisco#show running-config ?
ProVision# copy running-config tftp 10.0.100.21 config2		Cisco#copy running-config tftp://10.0.1.11/Cisco.cfg
ProVision# copy running-config usb config2		
ProVision# copy running-config xmodem		
ProVision# copy startup-config tftp 10.0.1.11 ProVision_startup-config.cfg	<Comware5>backup startup-configuration to 10.1.1.51 Comware5_startup-config.cfg	Cisco#copy startup-config tftp://10.0.1.11/Cisco_startup-config.cfg
ProVision# copy config config1 config config2	<Comware5>copy flash:/Comware5_main.cfg flash:/Comware5_main2.cfg	Cisco#copy flash:Cisco.cfg flash:Cisco_2.cfg
ProVision# copy config config1 tftp 10.0.100.21 config1	<Comware5>tftp 10.1.1.51 put Comware5_main.cfg Comware5_startup-config.cfg	Cisco#copy flash:Cisco.cfg tftp://10.0.1.11/Cisco_2.cfg
ProVision# copy config config1 xmodem		
ProVision# erase startup-config	<Comware5>reset saved-configuration main	Cisco#erase startup-config
ProVision# copy tftp startup-config 10.0.1.11 config6.cfg	<Comware5>tftp 10.1.1.51 get Comware5_main.cfg Comware5_main.cfg	Cisco#copy tftp://10.0.1.11/Cisco_config3.cfg startup-config
ProVision# copy tftp config config5 10.0.1.11 config5.cfg	<Comware5>tftp 10.1.1.51 get Comware5_main3.cfg Comware5_main3.cfg	Cisco#copy tftp://10.0.1.11/Cisco_config2.cfg flash:Cisco_config2.cfg
ProVision# show config files	<Comware5>dir	Cisco#show flash
ProVision# startup-default config config1	<Comware5>startup saved-configuration Comware5_main.cfg main	Cisco(config)#boot config-file flash:Cisco.cfg
ProVision# startup-default primary config config1		
ProVision# boot set-default flash primary	<Comware5>boot-loader file flash:/s4800g-cmw520-r2202p15-s56.bin slot 1 main	Cisco(config)# boot system flash:c3560-advipservicesk9-mz.122-46.SE/c3560-advipservicesk9-mz.122-46.SE.bin
ProVision# boot system flash primary config config1		

ProVision
ProVision# show running-config ? status   Check if the running configuration differs from

```
                       the startup configuration.
 <cr>

ProVision# copy running-config ?
 tftp                  Copy data to a TFTP server.
 usb                   Copy data to a USB flash drive.
 xmodem                Use xmodem on the terminal as the data
                       destination.

ProVision# copy running-config tftp 10.0.100.21 ?
 FILENAME-STR          Specify filename for the TFTP transfer.

ProVision# copy running-config tftp 10.0.100.21 config2

ProVision# copy running-config usb ?
 FILENAME-STR          Specify filename for the USB transfer.

ProVision# copy running-config usb config2

ProVision# copy running-config xmodem ?
 pc                    Change CR/LF to PC style.
 unix                  Change CR/LF to unix style.
 <cr>

ProVision# copy running-config xmodem
Press 'Enter' and start XMODEM on your host...

ProVision# show config

ProVision# copy startup-config
 tftp                  Copy data to a TFTP server.
 usb                   Copy data to a USB flash drive.
 xmodem                Use xmodem on the terminal as the data destination.

ProVision# copy startup-config tftp 10.0.1.11 ProVision_startup-config.cfg

ProVision# copy config ?
 config1
 config2
 config3

ProVision# copy config config1 ?
 config                Copy data to specified configuration file.
 tftp                  Copy data to a TFTP server.
 xmodem                Use xmodem on the terminal as the data
                       destination.

ProVision# copy config config1 config ?
 ASCII-STR             Enter an ASCII string for the 'config'
                       command/parameter.

ProVision# copy config config1 config config2 ?
<cr>

ProVision# copy config config1 config config2

ProVision# copy config config1 tftp 10.0.100.21 config1
```

```
ProVision# copy config config1 xmodem ?
 pc                     Change CR/LF to PC style.
 unix                   Change CR/LF to unix style.
 <cr>
ProVision# copy config config1 xmodem
Press 'Enter' and start XMODEM on your host...

ProVision# erase startup-config

ProVision# copy tftp startup-config 10.0.1.11 config6.cfg

ProVision# copy tftp config config5 10.0.1.11 config5.cfg

ProVision# show config files
Configuration files:
 id | act pri sec | name
 ---+-------------+-------------------------------------------------
  1 |  *   *      | config1
  2 |          *  | config2
  3 |             | config3

ProVision# startup-default ?
 config                 Specify configuration file to set as default.
 primary                Primary flash image.
 secondary              Secondary flash image.

ProVision# startup-default config ?
 config1
 config2
 config3
ProVision# startup-default config config1

ProVision# startup-default primary ?
 config                 Specify configuration file to set as default.

ProVision# startup-default primary config ?
 config1
 config2
 config3

ProVision# startup-default primary config config1

ProVision# boot ?
 set-default            Specify the default flash boot image.
 system                 Allows user to specify boot image to use after
                        reboot.
 <cr>

ProVision# boot set-default ?
 flash                  Specify the default flash boot image.

ProVision# boot set-default flash ?
 primary                Primary flash image.
 secondary              Secondary flash image.

ProVision# boot set-default flash primary ?
```

```
 <cr>

ProVision# boot set-default flash primary

ProVision# boot system ?
 flash                 Specify boot image to use after reboot.
 <cr>

ProVision# boot system flash ?
 primary               Primary flash image.
 secondary             Secondary flash image.

ProVision# boot system flash primary ?
 config                Specify configuration file to use on boot.
 <cr>

ProVision# boot system flash primary config ?
 config1
 config2
 config3

ProVision# boot system flash primary config config1 ?
 <cr>

ProVision# boot system flash primary config config1
```

Comware 5

```
<Comware5>display current-configuration ?
  by-linenum     Display configuration with line number
  configuration  The pre-positive and post-positive configuration information
  interface      The interface configuration information
  |              Matching output
  <cr>

<Comware5>backup ?
  startup-configuration  Startup configuration

<Comware5>backup startup-configuration ?
  to  Indicate operation direction

<Comware5>backup startup-configuration to ?
  STRING<1-20>  IP address or hostname of TFTP Server

<Comware5>backup startup-configuration to 10.1.1.51 Comware5_startup-config.cfg


<Comware5>tftp ?
  STRING<1-20>  IP address or hostname of a remote system
  ipv6          IPv6 TFTP client

<Comware5>tftp 10.1.1.51 ?
  get   Download file from remote TFTP server
  put   Upload local file to remote TFTP server
  sget  Download securely from remote TFTP server

<Comware5>tftp 10.1.1.51 put Comware5_main.cfg ?
```

```
  STRING<1-135>  Destination filename
  source         Specify a source
  <cr>

<Comware5>tftp 10.1.1.51 put Comware5_main.cfg Comware5_startup-config.cfg ?
  source  Specify a source
  <cr>

<Comware5>tftp 10.1.1.51 put Comware5_main.cfg Comware5_startup-config.cfg


<Comware5>copy ?
  STRING  [drive][path][file name]
  flash:  Device name

<Comware5>copy flash:/Comware5_main.cfg ?
  STRING  [drive][path][file name]
  flash:  Device name

<Comware5>copy flash:/Comware5_main.cfg flash:/Comware5_main2.cfg ?
  <cr>

<Comware5>copy flash:/Comware5_main.cfg flash:/Comware5_main2.cfg


<Comware5>reset saved-configuration ?
  backup  Backup config file
  main    Main config file
  <cr>

<Comware5>reset saved-configuration main ?
  <cr>

<Comware5>reset saved-configuration main


<Comware5>tftp 10.1.1.51 get Comware5_main.cfg Comware5_main.cfg


<Comware5>tftp 10.1.1.51 get Comware5_main3.cfg Comware5_main3.cfg


<Comware5>dir
Directory of flash:/

   0     -rw-  10732579  Apr 27 2010 04:01:27   s4800g-cmw520-r2202p12-s56.bin
   1     -rw-    245887  Apr 26 2000 12:07:12   default.diag
   2     -rw-  10576749  Nov 23 2009 10:47:51   s4800g-cmw520-r2202p15-s56.bin
   3     -rw-      2371  Apr 27 2010 05:00:01   Comware5_main.cfg
   4     -rw-      5248  Apr 26 2010 02:10:38   Comware5_04262010_0200.cfg
   5     -rw-      5167  Apr 25 2010 19:27:47   Comware5_backup.cfg
   6     -rw-      2398  Apr 27 2010 04:02:34   Comware5_04272010_0400.cfg
   7     -rw-      2371  Apr 27 2010 04:53:11   Comware5_main2.cfg
   8     -rw-      2371  Apr 27 2010 05:04:56   Comware5_main3.cfg

(will need to view files to determine which are configuration files)
```

```
<Comware5>startup ?
  bootrom-access       Bootrom access control
  saved-configuration  Saved-configuration file for starting system

<Comware5>startup saved-configuration ?
  Comware5_04272010_0400.cfg
  Comware5_main2.cfg
  Comware5_main3.cfg
  Comware5_main.cfg
  Comware5_04262010_0200.cfg
  Comware5_backup.cfg

<Comware5>startup saved-configuration Comware5_main.cfg ?
  backup  Backup config file
  main    Main config file
  <cr>

<Comware5>startup saved-configuration Comware5_main.cfg main ?
  <cr>

<Comware5>startup saved-configuration Comware5_main.cfg main


<Comware5>boot-loader file ?
  STRING  [drive][path][file name]
  flash:  Device name

<Comware5>boot-loader file flash:/s4800g-cmw520-r2202p15-s56.bin ?
  slot  Specify the slot number

<Comware5>boot-loader file flash:/s4800g-cmw520-r2202p15-s56.bin slot ?
  INTEGER<1>  Slot number
  all         All current slot number

<Comware5>boot-loader file flash:/s4800g-cmw520-r2202p15-s56.bin slot 1 ?
  backup  Set backup attribute
  main    Set main attribute

<Comware5>boot-loader file flash:/s4800g-cmw520-r2202p15-s56.bin slot 1 main ?
  <cr>

<Comware5>boot-loader file flash:/s4800g-cmw520-r2202p15-s56.bin slot 1 main
```

Cisco

```
Cisco#show running-config ?
  all        Configuration with defaults
  brief      configuration without certificate data
  full       full configuration
  identity   Show identity profile/policy information
  interface  Show interface configuration
  ipe        IPe information
  map-class  Show map class information
  partition  Configuration corresponding a partition
  view       View options
  vlan       Show L2 VLAN information
  |          Output modifiers
  <cr>

Cisco#copy running-config ?
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system|
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system
  vb:             Copy to vb: file system
Cisco#copy running-config tftp://10.0.1.11/Cisco.cfg
Address or name of remote host [10.0.1.11]?
Destination filename [Cisco.cfg]?

Cisco#show startup-config

Cisco#copy startup-config ?
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system|
  tmpsys:         Copy to tmpsys: file system
  vb:             Copy to vb: file system
Cisco#copy startup-config tftp://10.0.1.11/Cisco_startup-config.cfg
Address or name of remote host [10.0.1.11]?
Destination filename [Cisco_startup-config]?
```

```
Cisco#copy flash:?
flash:Cisco.cfg
flash:config.text
flash:info
flash:multiple-fs
flash:private-config.text
flash:vlan.dat

Cisco#copy flash:Cisco.cfg ?
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  http:           Copy to http: file system
  https:          Copy to https: file system
  null:           Copy to null: file system
  nvram:          Copy to nvram: file system
  rcp:            Copy to rcp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  syslog:         Copy to syslog: file system
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
  tmpsys:         Copy to tmpsys: file system
  vb:             Copy to vb: file system

Cisco#copy flash:Cisco.cfg flash:Cisco_2.cfg

Cisco#copy flash:Cisco.cfg tftp://10.0.1.11/Cisco_2.cfg
Address or name of remote host [10.0.1.11]?
Destination filename [Cisco_2.cfg]?

Cisco#erase startup-config

Cisco#copy tftp://10.0.1.11/Cisco_config3.cfg startup-config
Destination filename [startup-config]?
Accessing tftp://10.0.1.11/Cisco_config3.cfg...

Cisco#copy tftp://10.0.1.11/Cisco_config2.cfg flash:Cisco_config2.cfg
Destination filename [Cisco_config2.cfg]?

Cisco#show flash:
Directory of flash:/
  354  drwx         256  Nov 14 2009 16:33:04 -06:00  c3560-advipservicesk9-mz.122-46.SE
  460  -rwx         103   Mar 1 1993 12:24:16 -06:00  info
  353  -rwx        1056   Dec 8 2009 22:33:40 -06:00  vlan.dat
  361  -rwx        3121  Dec 17 2009 17:56:54 -06:00  private-config.text
  363  -rwx        5599  Sep 17 2009 22:29:01 -05:00  config.text
  364  -rwx        7192  Dec 17 2009 17:56:54 -06:00  multiple-fs
  366  -rwx       10586  Dec 17 2009 17:56:54 -06:00  Cisco.cfg
  367  -rwx       10586  Dec 17 2009 18:00:08 -06:00  Cisco_2.cfg
(will need to view files to determine which are configuration files)

Cisco(config)#boot ?
  boothlpr            Boot Helper System Image
  config-file         Configuration File
  enable-break        Enable Break while booting
  helper               Helper Image(s)
  helper-config-file   Helper Configuration File
  host                 Router-specific config file
  manual               Manual Boot
  private-config-file  Private Configuration File
  system               System Image

Cisco(config)#boot config-file ?
  WORD  config file name

Cisco(config)#boot config-file flash:Cisco.cfg

Cisco(config)#boot system ?
  WORD  pathlist of boot file(s) ... file1;file2;...

Cisco(config)# boot system flash:c3560-advipservicesk9-m z.122-46.SE/c3560-advipservicesk9-
mz.122-46.SE.bin ?
  <cr>

Cisco(config)# boot system flash:c3560-advipservicesk9-m z.122-46.SE/c3560-advipservicesk9-
mz.122-46.SE.bin
```

Chapter 5 Syslog Services

This chapter compares the commands used to set up syslog services (such as the syslog server's IP address and the logging facility) and to view logged events.

ProVision	Comware 5	Cisco
`ProVision(config)# logging 10.0.100.21`	`[Comware5]info-center loghost 10.0.100.21`	`Cisco(config)#logging 10.0.100.21`
`ProVision(config)# logging facility ?`	`[Comware5]info-center loghost 10.0.100.21 facility ?`	`Cisco(config)#logging facility ?`
`ProVision(config)# logging severity ?`		`Cisco(config)#logging console ?`
	`[Comware5]info-center timestamp loghost date`	`Cisco(config)#service timestamps log datetime localtime`
`ProVision# show logging ?`	`[Comware5]display logbuffer ?`	`Cisco#show logging ?`

ProVision

```
ProVision(config)# logging ?
 facility              Specify the syslog facility value that will be used for
                       all syslog servers.
 IP-ADDR               Add an IP address to the list of receiving syslog
                       servers.
 priority-descr        A text string associated with the values of facility,
                       severity, and system-module.
 severity              Event messages of the specified severity or higher will
                       be sent to the syslog server.
 system-module         Event messages of the specified system module
                       (subsystem) will be sent to the syslog server.
ProVision(config)# logging 10.0.100.21

ProVision(config)# logging facility ?
 kern
 user
 mail
 daemon
 auth
 syslog
 lpr
 news
 uucp
 sys9
 sys10
 sys11
 sys12
 sys13
 sys14
 cron
 local0
 local1
 local2
 local3
 local4
 local5
 local6
 local7

ProVision(config)# logging severity ?
 major
 error
 warning
 info debug

ProVision# show logging ?
 -a                     Display all log events, including those from previous
                        boot cycles.
 -r                     Display log events in reverse order (most recent first).
 -m                     Major event class.
 -p                     Performance event class.
 -w                     Warning event class.
 -i                     Information event class.
 -d                     Debug event class.
 OPTION-STR             Filter events shown.
 <cr>
```

Comware 5

```
[Comware5]info-center ?
  channel      Specify the name of information channel
  console      Settings of console configuration
  enable       Enable the information center
  logbuffer    Settings of logging buffer configuration
  loghost      Settings of logging host configuration
  monitor      Settings of monitor configuration
  snmp         Settings of snmp configuration
  source       Informational source settings
  synchronous  Synchronize info-center output
  timestamp    Set the time stamp type of information
  trapbuffer   Settings of trap buffer configuration

[Comware5]info-center loghost ?
  X.X.X.X  Logging host ip address
  source   Set the source address of packets sent to loghost

[Comware5]info-center loghost 10.0.100.21 ?
  channel   Assign channel to the logging host
  facility  Set logging host facility
  <cr>

[Comware5]info-center loghost 10.0.100.21

[Comware5]info-center loghost 10.0.100.21 facility ?
  local0  Logging host facility
  local1  Logging host facility
  local2  Logging host facility
  local3  Logging host facility
  local4  Logging host facility
  local5  Logging host facility
  local6  Logging host facility
  local7  Logging host facility

[Comware5]info-center timestamp ?
  debugging  Set the time stamp type of the debug information
  log        Set the time stamp type of the log information
  loghost    Set the time stamp type of the information to loghost
  trap       Set the time stamp type of the alarm information

[Comware5]info-center timestamp loghost?
   loghost

[Comware5]info-center timestamp loghost ?
  date          Information time stamp of date type
  no-year-date  Information time stamp of date without year type
  none          None information time stamp

[Comware5]info-center timestamp loghost date ?
  <cr>

[Comware5]info-center timestamp loghost date

[Comware5]display logbuffer ?
  level    Only show items whose level match the designated level
  reverse  reverse
  size     Limit display to the most recent specified number of events
  slot     Only show items which are from the designated slot
  summary  A summary of the logging buffer
  |        Output modifiers
  <cr>
```

Cisco

```
Cisco(config)#logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  buginf               Enable buginf logging for debugging
  cns-events           Set CNS Event logging level
  console              Set console logging parameters
  count                Count every log message and timestamp last occurrence
  discriminator        Create or modify a message discriminator
  exception            Limit size of exception flush output
  facility             Facility parameter for syslog messages
  file                 Set logging file parameters
  history              Configure syslog history table
  host                 Set syslog server IP address and parameters
  message-counter      Configure log message to include certain counter value
  monitor              Set terminal line (monitor) logging parameters
  on                   Enable logging to all enabled destinations
  origin-id            Add origin ID to syslog messages
  rate-limit           Set messages per second limit
  reload               Set reload logging level
  source-interface     Specify interface for source address in logging
                       transactions
  trap                 Set syslog server logging level
Cisco(config)#logging 10.0.100.21

Cisco(config)#logging facility ?
  auth    Authorization system
  cron    Cron/at facility
  daemon  System daemons
  kern    Kernel
  local0  Local use
  local1  Local use
  local2  Local use
  local3  Local use
  local4  Local use
  local5  Local use
  local6  Local use
  local7  Local use
  lpr     Line printer system
  mail    Mail system
  news    USENET news
  sys10   System use
  sys11   System use
  sys12   System use
  sys13   System use
  sys14   System use
  sys9    System use
  syslog  Syslog itself
  user    User process
  uucp    Unix-to-Unix copy system

Cisco(config)#logging console ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  discriminator  Establish MD-Console association
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  guaranteed     Guarantee console messages
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  xml            Enable logging in XML
  <cr>

Cisco(config)#service ?
  compress-config        Compress the configuration file
  config                 TFTP load config files
  counters               Control aging of interface counters
  dhcp                   Enable DHCP server and relay agent
  disable-ip-fast-frag   Disable IP particle-based fast fragmentation
  exec-callback          Enable exec callback
  exec-wait              Delay EXEC startup on noisy lines
  finger                 Allow responses to finger requests
  hide-telnet-addresses  Hide destination addresses in telnet command
  linenumber             enable line number banner for each exec
  nagle                  Enable Nagle's congestion control algorithm
  old-slip-prompts       Allow old scripts to operate with slip/ppp
  pad                    Enable PAD commands
  password-encryption    Encrypt system passwords
  password-recovery      Disable password recovery
  prompt                 Enable mode specific prompt
  pt-vty-logging         Log significant VTY-Async events
  sequence-numbers       Stamp logger messages with a sequence number
  slave-log              Enable log capability of slave IPs
  tcp-keepalives-in      Generate keepalives on idle incoming network
                         connections
  tcp-keepalives-out     Generate keepalives on idle outgoing network
                         connections
  tcp-small-servers      Enable small TCP servers (e.g., ECHO)
  telnet-zeroidle        Set TCP window 0 when connection is idle
  timestamps             Timestamp debug/log messages
  udp-small-servers      Enable small UDP servers (e.g., ECHO)

Cisco(config)#service timestamps ?
  debug  Timestamp debug messages
  log    Timestamp log messages
  <cr>
Cisco(config)#service timestamps log ?
  datetime  Timestamp with date and time
  uptime    Timestamp with system uptime
  <cr>
Cisco(config)#service timestamps log datetime ?
  localtime      Use local time zone for timestamps
  msec           Include milliseconds in timestamp
  show-timezone  Add time zone information to timestamp
  <cr>
Cisco(config)#service timestamps log datetime localtime ?
  msec           Include milliseconds in timestamp
  show-timezone  Add time zone information to timestamp
  <cr>
Cisco(config)#service timestamps log datetime localtime

Cisco#show logging ?
  count    Show counts of each logging message
  history  Show the contents of syslog history table
  xml      Show the contents of XML logging buffer
  |        Output modifiers
  <cr>
```

Chapter 6 Time Service

This chapter compares commands used to configure the switch time using time protocols, such as TimeP, network time protocol (NTP), or Simple NTP (SNTP).

a) TimeP or NTP

ProVision	Comware 5	Cisco
ProVision(config)# ip timep manual 10.0.100.251 interval 5	[Comware5]ntp-service unicast-server 10.0.100.251	Cisco(config)#ntp server 10.0.100.251
ProVision(config)# timesync timep		
ProVision# show timep	[Comware5]display ntp-service sessions	Cisco#show ntp associations
ProVision(config)# clock timezone us central	[Comware5]clock timezone CST minus 06:00:00	Cisco(config)#clock timezone CST -6
ProVision(config)# clock summer-time		
ProVision(config)# time daylight-time-rule continental-us-and-canada	[Comware5]clock summer-time CDT one-off 02:00:00 03/14/2010 02:00:00 11/14/2010 01:00:00	Cisco(config)#clock summer-time CDT date 8 mar 2009 02:00 1 nov 2009 02:00
ProVision# show time	[Comware5]display clock	Cisco#show clock

ProVision

```
ProVision(config)# ip timep ?
 dhcp                    Use DHCP to acquire Timep server address.
 manual                  Manually configure the Timep server address.

ProVision(config)# ip timep manual 10.0.100.251 interval 5

ProVision(config)# timesync ?
 sntp                    Set the time protocol to SNTP
 timep                   Set the time protocol to the TIME protocol
ProVision(config)# timesync timep

ProVision# show timep
 Timep Configuration
  Time Sync Mode: Timep
  TimeP Mode [Disabled] : Manual
  Server Address : 10.0.100.251
  Poll Interval (min) [720] : 1
  OOBM : No

ProVision(config)# clock ?
 set                     Set current time and/or date.
 summer-time             Enable/disable daylight-saving time changes.
 timezone                Set the number of hours your location is to the West(-)
                         or East(+) of GMT.
 <cr>

ProVision(config)# clock timezone|
 gmt                     Number of hours your timezone is to the West(-) or
```

```
                       East(+) of GMT.
 us                    Timezone for US locations.

ProVision(config)# clock timezone us
 Alaska
 Aleutian
 Arizona
 central
 east_indiana
 eastern
 Hawaii
 Michigan
 mountain
 pacific
 samoa

ProVision(config)# clock timezone us central
 <cr>

ProVision(config)# clock summer-time
 <cr>

ProVision(config)# time daylight-time-rule continental-us-and-canada

ProVision# show time
Tue Nov 24 12:51:21 2009
```

Comware 5

```
[Comware5]ntp-service ?
  access                NTP access control
  authentication        Authenticate NTP time source
  authentication-keyid  Specify NTP authentication keyid
  max-dynamic-sessions  Specify the maximum connections
  reliable              Specify trusted keyid of NTP
  source-interface      Interface corresponding to sending NTP packet
  unicast-peer          Specify NTP peer
  unicast-server        Specify NTP server

[Comware5]ntp-service unicast-server ?
  STRING<1-20>  Host name of a remote system
  X.X.X.X       IP address
  vpn-instance  Specify VPN-Instance of MPLS VPN

[Comware5]ntp-service unicast-server 10.0.100.251 ?
  authentication-keyid  Specify authentication keyid
  priority              Prefer to this remote host if possible
  source-interface      Interface corresponding to sending NTP packet
  version               Specify NTP version
  <cr>

[Comware5]ntp-service unicast-server 10.0.100.251

[Comware5]display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
********************************************************************************
[12345]10.0.100.251    10.0.12.14        11   255   64   17   -1.2   11.0    1.0
```

```
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1


[Comware5]display ntp-service status
 Clock status: synchronized
 Clock stratum: 12
 Reference clock ID: 10.0.100.251
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: -1.1988 ms
 Root delay: 75.71 ms
 Root dispersion: 510.97 ms
 Peer dispersion: 500.41 ms
 Reference time: 06:38:27.249 UTC Apr 26 2010(CF7FB363.3FF327AA)


[Comware5]clock ?
  summer-time  Configure summer time
  timezone     Configure time zone

[Comware5]clock timezone CST ?
  add    Add time zone offset
  minus  Minus time zone offset

[Comware5]clock timezone CST minus ?
  TIME  Time zone offset (HH:MM:SS)

 [Comware5]clock timezone CST minus 06:00:00 ?
  <cr>

[Comware5]clock timezone CST minus 06:00:00


[Comware5]clock summer-time ?
  STRING<1-32>  Name of time zone in summer

[Comware5]clock summer-time CDT ?
  one-off    Configure absolute summer time
  repeating  Configure recurring summer time

[Comware5]clock summer-time CDT one-off ?
  TIME  Time to start (HH:MM:SS)

[Comware5]clock summer-time CDT one-off 02:00:00 ?
  DATE  Date to start (MM/DD/YYYY or YYYY/MM/DD, valid year: 2000-2035)

[Comware5]clock summer-time CDT one-off 02:00:00 03/14/2010 ?
  TIME  Time to end (HH:MM:SS)

[Comware5]clock summer-time CDT one-off 02:00:00 03/14/2010 02:00:00 ?
  DATE  Date to end (MM/DD/YYYY or YYYY/MM/DD, valid year: 2000-2035)

[Comware5]clock summer-time CDT one-off 02:00:00 03/14/2010 02:00:00 11/14/2010 ?
  TIME  Time added to the current system time (HH:MM:SS)
```

```
[Comware5]clock summer-time CDT one-off 02:00:00 03/14/2010 02:00:00 11/14/2010 01:0
0:00 ?
  <cr>

[Comware5]clock summer-time CDT one-off 02:00:00 03/14/2010 02:00:00 11/14/2010 01:0
0:00


[Comware5]display clock
01:54:59 CDT Mon 04/26/2010
Time Zone : CST minus 06:00:00
Summer-Time : CDT one-off 02:00:00 03/14/2010 02:00:00 11/14/2010  01:00:00
```

Cisco

```
Cisco(config)#ntp ?
  access-group        Control NTP access
  authenticate        Authenticate time sources
  authentication-key  Authentication key for trusted time sources
  broadcastdelay      Estimated round-trip delay
  clock-period        Length of hardware clock tick
  logging             Enable NTP message logging
  max-associations    Set maximum number of associations
  peer                Configure NTP peer
  server              Configure NTP server
  source              Configure interface for source address
  trusted-key         Key numbers for trusted time sources

Cisco(config)#ntp server 10.0.100.251

Cisco#show ntp ?
  associations  NTP associations
  status        NTP status
Cisco#show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
*~10.0.100.251     10.0.12.14       11    39   128  377     2.7  -19.97     1.5

 * master (synced), # master (unsynced), + selected, - candidate, ~ configured

Cisco#show ntp status
Clock is synchronized, stratum 12, reference is 10.0.100.251
nominal freq is 119.2092 Hz, actual freq is 119.2097 Hz, precision is 2**18
reference time is CEB6A6EA.7C8CA52B (12:39:38.486 CST Tue Nov 24 2009)
clock offset is -19.9684 msec, root delay is 67.43 msec
root dispersion is 521.67 msec, peer dispersion is 1.51 msec

Cisco(config)#clock ?
  summer-time  Configure summer (daylight savings) time
  timezone     Configure time zone

Cisco(config)#clock timezone ?
  WORD  name of time zone

Cisco(config)#clock timezone CST ?
  <-23 - 23>  Hours offset from UTC
```

```
Cisco(config)#clock timezone CST -6 ?
  <0-59>  Minutes offset from UTC
  <cr>

Cisco(config)#clock timezone CST -6 00 ?
  <cr>

Cisco(config)#clock timezone CST -6

Cisco(config)#clock summer-time CDT date 8 mar 2009 02:00 1 nov 2009 02:00


Cisco#show clock
12:41:21.816 CST Tue Nov 24 2009


Cisco#show clock detail
12:41:30.155 CST Tue Nov 24 2009
Time source is NTP
Summer time starts 02:00:00 CST Sun Mar 8 2009
Summer time ends 02:00:00 CDT Sun Nov 1 2009
```

b) SNTP

ProVision	Comware 5	Cisco
`ProVision(config)# sntp server priority 1 10.0.100.251`	***not supported***	***not supported on newer Cisco switches***
`ProVision(config)# sntp unicast`		
`ProVision(config)# sntp 60`		
`ProVision(config)# timesync sntp`		
`ProVision# show sntp`		

ProVision

```
ProVision(config)# sntp server priority 1 10.0.100.251

ProVision(config)# sntp unicast

ProVision(config)# sntp 60

ProVision(config)# timesync sntp

ProVision# show sntp
 SNTP Configuration
  SNTP Authentication : Disabled
  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 60
  Source IP Selection: Outgoing Interface
  Priority SNTP Server Address                      Version Key-id
  -------- ---------------------------------------  ------- ----------
  1        10.0.100.251                             3       0
```

Comware 5

not supported

Cisco

not supported on newer Cisco switches

Chapter 7 SNMP

This chapter compares the commands used to configure Simple Network Management Protocol (SNMP).

- On HP ProVision, SNMP v1/v2c is enabled by default.
- On Comware 5, SNMP v3 is enabled by default.
- On Cisco, SNMP is disabled by default.

a) SNMP Version 1 and Version 2c

ProVision	Comware 5	Cisco
`[snmp v1/v2c is default version]`		

`ProVision(config)# snmp-server host 10.0.100.21 private all`	`[Comware5]snmp-agent trap enable`
	`[Comware5]snmp-agent target-host trap address udp-domain 10.0.100.21 udp-port 161 params securityname public`
		`Cisco(config)#snmp-server host 10.0.100.21 version 2c private`

`ProVision(config)# snmp-server community public operator restricted`	`[Comware5]snmp-agent community read public`	`Cisco(config)#snmp-server community public ro`
`ProVision(config)# snmp-server community private manager unrestricted`	`[Comware5]snmp-agent community write private`	`Cisco(config)#snmp-server community private rw`
`ProVision(config)# snmp-server location Lab`	`[Comware5]snmp-agent sys-info location Lab`	`Cisco(config)#snmp-server location Lab`
`ProVision(config)# snmp-server contact Lab_Engr`	`[Comware5]snmp-agent sys-info contact Lab_Engr`	`Cisco(config)#snmp-server contact Lab_Engr`

	`[Comware5]snmp-agent sys-info version v1 v2c`
	`[Comware5]undo snmp-agent sys-info version v3`	

`ProVision(config)# snmp-server enable`	`[Comware5]snmp-agent`	`Cisco(config)#snmp-server enable traps`

`ProVision# show snmp-server`	`[Comware5]display snmp-agent sys-info`
	`[Comware5]display snmp-agent community`
		`Cisco#show snmp`

ProVision

```
[snmp v1/v2c is default version]


ProVision(config)# snmp-server ?
 community              Add/delete SNMP community.
 contact                Name of the switch administrator.
 enable                 Enable/Disable SNMPv1/v2.
 host                   Define SNMP traps and their receivers.
 location               Description of the switch location.
 mib                    Enable/Disable SNMP support for the
                        hpSwitchAuthentication MIB.
 response-source        Specify the source ip-address policy for the response
                        pdu.
 trap-source            Specify the source ip-address policy for the trap pdu.
```

```
ProVision(config)# snmp-server host ?
 IP-ADDR               IP address of SNMP notification host.
 IPV6-ADDR             IPv6 address of SNMP notification host.

ProVision(config)# snmp-server host 10.0.100.21 ?
 COMMUNITY-STR         Name of the SNMP community (up to 32 characters).
 none                  Send no log messages.
 debug                 Send debug traps (for Internal use).
 all                   Send all log messages
 not-info              Send all but informational-only messages.
 critical              Send critical-level log messages.
 informs               Specify if informs will be sent, rather than
                       notifications.

ProVision(config)# snmp-server host 10.0.100.21 private ?
 none                  Send no log messages.
 debug                 Send debug traps (for Internal use).
 all                   Send all log messages
 not-info              Send all but informational-only messages.
 critical              Send critical-level log messages.
 informs               Specify if informs will be sent, rather than
                       notifications.
 <cr>

ProVision(config)# snmp-server host 10.0.100.21 private all ?
 informs               Specify if informs will be sent, rather than
                       notifications.
 <cr>

ProVision(config)# snmp-server host 10.0.100.21 private all


ProVision(config)# snmp-server community ?
 ASCII-STR             Enter an ASCII string for the 'community'
                       command/parameter.

ProVision(config)# snmp-server community public ?
 operator              The community can access all except the CONFIG MIB.
 manager               The community can access all MIB objects.
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>

ProVision(config)# snmp-server community public operator ?
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>

ProVision(config)# snmp-server community public operator restricted ?
 <cr>

ProVision(config)# snmp-server community public operator restricted


ProVision(config)# snmp-server community private ?
 operator              The community can access all except the CONFIG MIB.
 manager               The community can access all MIB objects.
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>

ProVision(config)# snmp-server community private manager ?
 restricted            MIB variables cannot be set, only read.
 unrestricted          Any MIB variable that has read/write access can be set.
 <cr>
```

```
ProVision(config)# snmp-server community private manager unrestricted?
 <cr>

ProVision(config)# snmp-server community private manager unrestricted


ProVision(config)# snmp-server location Lab

ProVision(config)# snmp-server contact Lab_Engr

ProVision(config)# snmp-server enable


ProVision# show snmp-server

 SNMP Communities

  Community Name       MIB View Write Access
  -------------------- -------- ------------
  public               Operator Restricted
  private              Manager  Unrestricted

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All

  Traps Category                  Current Status
  _____________________________   __________________
  SNMP Authentication           : Extended
  Password change               : Enabled
  Login failures                : Enabled
  Port-Security                 : Enabled
  Authorization Server Contact  : Enabled
  DHCP-Snooping                 : Enabled
  Dynamic ARP Protection        : Enabled
  Dynamic IP Lockdown           : Enabled

  Address                Community              Events   Type   Retry   Timeout
  ---------------------- ---------------------- -------- ------ ------- -------
  10.0.100.21            private                All      trap   3       15


 Excluded MIBs


 Snmp Response Pdu Source-IP Information

  Selection Policy   : rfc1517

 Trap Pdu Source-IP Information

  Selection Policy   : rfc1517
```

Comware 5

```
[Comware5]snmp-agent ?
  calculate-password  Calculate the secret key of the plain password
  community           Set a community for the access of SNMPv1&SNMPv2c
  group               Set a SNMP group based on USM
  local-engineid      Set the engineID of local SNMP entity
  log                 Set the log function
  mib-view            Set SNMP MIB view information
  packet              Set SNMP packet's parameters
  sys-info            Set system information of the node
  target-host         Set the target hosts to receive SNMP notification/traps
  trap                Set the parameters of SNMP trap/notification
  usm-user            Set a new user for access to SNMP entity
  <cr>


[Comware5]snmp-agent trap enable ?
  bfd            Enable BFD traps
  bgp            Enable BGP trap
  configuration  Enable the configuration management traps
  flash          Enable Flash traps
  ospf           Enable OSPF traps
  standard       Enable the standard SNMP traps
  system         Enable SysMib traps
  vrrp           Enable VRRP traps
  <cr>

[Comware5]snmp-agent trap enable

[Comware5]snmp-agent target-host ?
  trap  Specify trap host target

[Comware5]snmp-agent target-host trap ?
  address  Specify the transport addresses to be used in the generation of SNMP
           messages

[Comware5]snmp-agent target-host trap address ?
  udp-domain  Specify transport domain over UDP for the target host

[Comware5]snmp-agent target-host trap address udp-domain ?
  X.X.X.X  IP address of target host
  ipv6     Specify an ipv6 address as the target host address

[Comware5]snmp-agent target-host trap address udp-domain 10.0.100.21 ?
  params        Specify SNMP target information to be used in the generation of
                SNMP messages
  udp-port      Set port to receive traps/notifications for this target host
  vpn-instance  Specify VPN instance

[Comware5]snmp-agent target-host trap address udp-domain 10.0.100.21 udp-port 161 ?
  params        Specify SNMP target information to be used in the generation of
                SNMP messages
  vpn-instance  Specify VPN instance

[Comware5]snmp-agent target-host trap address udp-domain 10.0.100.21 udp-port 161 pa
rams ?
  securityname  Specify the name for the principal on whose behalf SNMP
                messages will be generated

[Comware5]snmp-agent target-host trap address udp-domain 10.0.100.21 udp-port 161 pa
rams securityname ?
  STRING<1-32>  Specify the character string of security name

[Comware5]snmp-agent target-host trap address udp-domain 10.0.100.21 udp-port 161 pa
rams securityname public ?
  v1    Specify security model of SNMPv1 to generate SNMP messages
  v2c   Specify security model of SNMPv2c to generate SNMP messages
  v3    Specify security model of SNMPv3 to generate SNMP messages
  <cr>

[Comware5]snmp-agent target-host trap address udp-domain 10.0.100.21 udp-port 161 pa
rams securityname public


[Comware5]snmp-agent community ?
  read   Read-only access for this community string
  write  Read-write access for this community string

[Comware5]snmp-agent community read ?
  STRING<1-32>  SNMP community string

[Comware5]snmp-agent community read public

[Comware5]snmp-agent community write private ?
  acl       Set access control list for this community
  mib-view  MIB view for which this community is restricted
  <cr>

[Comware5]snmp-agent community write private


[Comware5]snmp-agent sys-info ?
  contact   Set the contact information for system maintenance
  location  Set the physical position information of this node
  version   Enable the SNMP protocol version

[Comware5]snmp-agent sys-info version ?
  all  Enable the device to support SNMPv1, SNMPv2c and SNMPv3
  v1   Enable the device to support SNMPv1
  v2c  Enable the device to support SNMPv2c
  v3   Enable the device to support SNMPv3

[Comware5]snmp-agent sys-info version v1 ?
  v2c   Enable the device to support SNMPv2c
  v3    Enable the device to support SNMPv3
  <cr>

[Comware5]snmp-agent sys-info version v1 v2c

[Comware5]undo snmp-agent sys-info version v3

[Comware5]snmp-agent sys-info contact ?
  TEXT  Contact person information for this node<1-200>

[Comware5]snmp-agent sys-info contact Lab_Engr

[Comware5]snmp-agent sys-info location ?
  TEXT  The physical location of this node<1-200>

[Comware5]snmp-agent sys-info location Lab


[Comware5]snmp-agent
```

```
[Comware5]display snmp-agent sys-info
   The contact person for this managed node:
           LabEngr

   The physical location of this node:
           Lab

   SNMP version running in the system:
           SNMPv1 SNMPv2c

[Comware5]display snmp-agent community ?
  read   Display the community information with read-only access
  write  Display the community information with read-write access
  <cr>

[Comware5]dis snmp-agent community
   Community name: public
       Group name: public
       Storage-type: nonVolatile

   Community name: private
       Group name: private
       Storage-type: nonvolatile
```

Cisco

```
Cisco(config)#snmp-server ?
  chassis-id        String to uniquely identify this chassis
  community         Enable SNMP; set community string and access privs
  contact           Text for mib object sysContact
  context           Create/Delete a context apart from default
  enable            Enable SNMP Traps
  engineID          Configure a local or remote SNMPv3 engineID
  file-transfer     File transfer related commands
  group             Define a User Security Model group
  host              Specify hosts to receive SNMP notifications
  ifindex           Enable ifindex persistence
  inform            Configure SNMP Informs options
  ip                IP ToS configuration for SNMP traffic
  location          Text for mib object sysLocation
  manager           Modify SNMP manager parameters
  packetsize        Largest SNMP packet size
  queue-length      Message queue length for each TRAP host
  source-interface  Assign an source interface
  system-shutdown   Enable use of the SNMP reload command
  tftp-server-list  Limit TFTP servers used via SNMP
  trap              SNMP trap options
  trap-source       Assign an interface for the source address of all traps
  trap-timeout      Set timeout for TRAP message retransmissions
  user              Define a user who can access the SNMP engine
  view              Define an SNMPv3 MIB view


Cisco(config)#snmp-server host ?
  WORD                                                 IP/IPV6 address of SNMP
                                                       notification host
  http://<Hostname or A.B.C.D>[:<port number>][/<uri>]  HTTP address of XML
                                                       notification host

Cisco(config)#snmp-server host 10.0.100.21 ?
```

```
  WORD     SNMPv1/v2c community string or SNMPv3 user name
  informs  Send Inform messages to this host
  traps    Send Trap messages to this host
  version  SNMP version to use for notification messages
  vrf      VPN Routing instance for this host

Cisco (config)#snmp-server host 10.0.100.21 version ?
  1   Use SNMPv1
  2c  Use SNMPv2c
  3   Use SNMPv3

Cisco(config)#snmp-server host 10.0.100.21 version 2c ?
  WORD  SNMPv1/v2c community string or SNMPv3 user name

Cisco(config)#snmp-server host 10.0.100.21 version 2c private ?
  bgp               Allow BGP state change traps
  bridge            Allow SNMP STP Bridge MIB traps
  cef               Allows cef traps
  cluster           Allow Cluster Member Status traps
  config            Allow SNMP config traps
  config-copy       Allow SNMP config-copy traps
  config-ctid       Allow SNMP config-ctid traps
  copy-config       Allow SNMP config-copy traps
  cpu               Allow cpu related traps
  dot1x             Allow dot1x traps
  eigrp             Allow SNMP EIGRP traps
  entity            Allow SNMP entity traps
  envmon            Allow environmental monitor traps
  errdisable        Allow errordisable notifications
  event-manager     Allow SNMP Embedded Event Manager traps
  flash             Allow SNMP FLASH traps
  hsrp              Allow SNMP HSRP traps
  ipmulticast       Allow SNMP ipmulticast traps
  mac-notification  Allow SNMP MAC Notification Traps
  msdp              Allow SNMP MSDP traps
  mvpn              Allow Multicast Virtual Private Network traps
  ospf              Allow OSPF traps
  pim               Allow SNMP PIM traps
  port-security     Allow SNMP port-security traps
  power-ethernet    Allow SNMP power ethernet traps
  rtr               Allow SNMP Response Time Reporter traps
  snmp              Allow SNMP-type notifications
  storm-control     Allow SNMP storm-control traps
  stpx              Allow SNMP STPX MIB traps
  syslog            Allow SNMP syslog traps
  tty               Allow TCP connection traps
  udp-port          The notification host's UDP port number (default port 162)
  vlan-membership   Allow SNMP VLAN membership traps
  vlancreate        Allow SNMP VLAN created traps
  vlandelete        Allow SNMP VLAN deleted traps
  vtp               Allow SNMP VTP traps
  <cr>

Cisco(config)#snmp-server host 10.0.100.21 version 2c private


Cisco(config)#snmp-server community ?
  WORD  SNMP community string

Cisco(config)#snmp-server community public ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ro           Read-only access with this community string
  rw           Read-write access with this community string
  view         Restrict this community to a named MIB view
  <cr>

Cisco(config)#snmp-server community public ro ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ipv6         Specify IPv6 Named Access-List
  <cr>

Cisco(config)#snmp-server community public ro


Cisco(config)#snmp-server community private ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ro           Read-only access with this community string
  rw           Read-write access with this community string
  view         Restrict this community to a named MIB view
  <cr>

Cisco(config)#snmp-server community private rw ?
  <1-99>       Std IP accesslist allowing access with this community string
  <1300-1999>  Expanded IP accesslist allowing access with this community
               string
  WORD         Access-list name
  ipv6         Specify IPv6 Named Access-List
  <cr>

Cisco(config)#snmp-server community private rw


Cisco(config)#snmp-server location Lab

Cisco(config)#snmp-server contact Lab_Engr

Cisco(config)#snmp-server enable traps


Cisco#show snmp
Chassis: CAT0948R4L0
Contact: Lab_Engr
Location: Lab
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

```
SNMP global trap: enabled

SNMP logging: enabled
    Logging to 10.0.100.21.162, 0/10, 0 sent, 0 dropped.
SNMP agent enabled


Cisco#show snmp host
Notification host: 10.0.100.21  udp-port: 162   type: trap
user: private   security model: v2c
```

b) SNMP Version 3

ProVision	Comware 5	Cisco
	[snmp v3 is default version]	
ProVision(config)# snmpv3 enable	[Comware5]snmp-agent sys-info version v3 [Comware5]undo snmp-agent sys-info version v1 v2c	
	[Comware5]snmp-agent group v3 <name> privacy	Cisco(config)#snmp-server group <name> v3 auth
ProVision(config)# snmpv3 user test auth md5 password priv des password		
	[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-mode 3des password	Cisco(config)#snmp-server user test managerpriv v3 auth md5 password
ProVision(config)# snmpv3 group managerpriv user test sec-model ver3		
		Cisco(config)#snmp-server host 10.0.100.21 version 3 auth test
ProVision# show snmpv3 enable	[Comware5]display snmp-agent sys-info	Cisco#show snmp host
ProVision# show snmpv3 user	[Comware5]display snmp-agent usm-user	Cisco#show snmp user
ProVision# show snmpv3 group	[Comware5]display snmp-agent group	Cisco#show snmp group

ProVision

```
ProVision(config)# snmpv3 ?
 community                Configure SNMPv3 Community entry.
 enable                   Enable SNMPv3.
 group                    Configure SNMPv3 User to Group entry.
 notify                   Configure SNMPv3 Notification entry.
 only                     Accept only SNMP v3 messages.
 params                   Configure SNMPv3 Target Parameter entry.
 restricted-access        Configure SNMPv1 and SNMPv2c access properties.
 targetaddress            Configure SNMPv3 Target Address entry.
 user                     Configure SNMPv3 User entry.

ProVision(config)# snmpv3 enable
SNMPv3 Initialization process.
Creating user 'initial'
Authentication Protocol: MD5
Enter authentication password: ********
Privacy protocol is DES
Enter privacy password: ********

User 'initial' is created
Would you like to create a user that uses SHA? y
Enter user name: initial
Authentication Protocol: SHA
Enter authentication password: ********
Privacy protocol is DES
Enter privacy password: ********
```

```
User creation is done.  SNMPv3 is now functional.
Would you like to restrict SNMPv1 and SNMPv2c messages to have read only
access (you can set this later by the command 'snmp restrict-access'): y


ProVision(config)# snmpv3 user ?
 USERNAME-STR          Set authentication parameters.

ProVision(config)# snmpv3 user test ?
 auth                  Set authentication parameters.
 <cr>

ProVision(config)# snmpv3 user test auth ?
 AUTHPASSWORD-STR      Set authentication password.
 md5                   Set the authentication protocol to md5.
 sha                   Set the authentication protocol to sha.

ProVision(config)# snmpv3 user test auth md5 ?
 AUTHPASSWORD-STR      Set authentication password.

ProVision(config)# snmpv3 user test auth md5 password ?
 priv                  Set Privacy password.
 <cr>
ProVision(config)# snmpv3 user test auth md5 password priv ?
 PRIVPASSWORD-STR      Set Privacy password.
 des                   Set the privacy protocol to des.
 aes                   Set the privacy protocol to aes-128.

ProVision(config)# snmpv3 user test auth md5 password priv des ?
 PRIVPASSWORD-STR      Set Privacy password.

ProVision(config)# snmpv3 user test auth md5 password priv des password ?
 <cr>

ProVision(config)# snmpv3 user test auth md5 password priv des password


ProVision(config)# snmpv3 group ?
 managerpriv           Require privacy and authentication, can access all
                       objects.
 managerauth           Require authentication, can access all objects.
 operatorauth          Requires authentication, limited access to objects.
 operatornoauth        No authentication required, limited access to objects.
 commanagerrw          Community with manager and unrestricted write access.
 commanagerr           Community with manager and restricted write access.
 comoperatorrw         Community with operator and unrestricted write access.
 comoperatorr          Community with operator and restricted write access.

ProVision(config)# snmpv3 group managerpriv ?
 user                  Set user to be added to the group.

ProVision(config)# snmpv3 group managerpriv user ?
 ASCII-STR             Enter an ASCII string for the 'user' command/parameter.

ProVision(config)# snmpv3 group managerpriv user test ?
 sec-model             Set security model to be used.

ProVision(config)# snmpv3 group managerpriv user test sec-model ?
 ver1                  SNMP version 1 security model.
 ver2c                 SNMP version v2c security model.
 ver3                  SNMP version 3 security model.

ProVision(config)# snmpv3 group managerpriv user test sec-model ver3 ?
 <cr>
```

```
ProVision(config)# snmpv3 group managerpriv user test sec-model ver3


ProVision# show snmpv3 enable

 Status and Counters - SNMP v3 Global Configuration Information

  SNMP v3 enabled : Yes


ProVision# show snmpv3 user

 Status and Counters - SNMP v3 Global Configuration Information

  User Name                        Auth. Protocol   Privacy Protocol
  -------------------------------- ---------------- ----------------
  initial                          SHA              CBC DES
  test                             MD5              CBC DES


ProVision# show snmpv3 group

 Status and Counters - SNMP v3 Global Configuration Information

  Security Name                 Security Model Group Name
  ----------------------------- -------------- --------------------------------
  CommunityManagerReadOnly      ver1           ComManagerR
  CommunityManagerReadWrite     ver1           ComManagerRW
  CommunityOperatorReadOnly     ver1           ComOperatorR
  CommunityOperatorReadWrite    ver1           ComOperatorRW
  CommunityManagerReadOnly      ver2c          ComManagerR
  CommunityManagerReadWrite     ver2c          ComManagerRW
  CommunityOperatorReadOnly     ver2c          ComOperatorR
  CommunityOperatorReadWrite    ver2c          ComOperatorRW
  test                          ver3           ManagerPriv
```

Comware 5

```
[snmp v3 is default version]

[Comware5]snmp-agent sys-info version v3

[Comware5]undo snmp-agent sys-info version v1 v2c


[Comware5]snmp-agent group ?
  v1   SNMPv1 security mode specified for this group name
  v2c  SNMPv2c security mode specified for this group name
  v3   USM(SNMPv3) security mode specified for this group name

[Comware5]snmp-agent group v3 ?
  STRING<1-32>  Group name

[Comware5]snmp-agent group v3 managerpriv ?
  acl             Set access control list for this group
  authentication  Specify a securityLevel of AuthNoPriv for this group name
  notify-view     Set a notify view for this group name
  privacy         Specify a securityLevel of AuthPriv for this group name
  read-view       Set a read view for this group name
  write-view      Set a write view for this group name
  <cr>
```

```
[Comware5]snmp-agent group v3 managerpriv privacy ?
  acl          Set access control list for this group
  notify-view  Set a notify view for this group name
  read-view    Set a read view for this group name
  write-view   Set a write view for this group name
  <cr>

[Comware5]snmp-agent group v3 managerpriv privacy


[Comware5]snmp-agent usm-user ?
  v1   SNMPv1 security model
  v2c  SNMPv2c security model
  v3   USM(SNMPv3) security model

[Comware5]snmp-agent usm-user v3 ?
  STRING<1-32>  User name

[Comware5]snmp-agent usm-user v3 test ?
  STRING<1-32>  The string of group to which the specified user belongs

[Comware5]snmp-agent usm-user v3 test managerpriv ?
  acl                  Set access control list for this user
  authentication-mode  Specify the authentication mode for the user
  cipher               Use secret key as password
  <cr>

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode ?
  md5  Authenticate with HMAC MD5 algorithm
  sha  Authenticate with HMAC SHA algorithm

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 ?
  STRING<1-64>  Plain password of user authentication

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password ?
  acl           Set access control list for this user
  privacy-mode  Specify the privacy mode for the user
  <cr>

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode ?
  3des    Use the 3DES encryption algorithm
  aes128  Use the 128bits AES encryption algorithm
  des56   Use the 56bits DES encryption algorithm

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode 3des ?
  STRING<1-64>  Plain password of user encryption

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode 3des password ?
  acl   Set access control list for this user
  <cr>

[Comware5]snmp-agent usm-user v3 test managerpriv authentication-mode md5 password privacy-
mode 3des password
```

```
[Comware5]display snmp-agent sys-info
   The contact person for this managed node:
           LabEngr

   The physical location of this node:
           Lab

   SNMP version running in the system:
           SNMPv3

[Comware5]display snmp-agent group

   Group name: managerpriv
       Security model: v3 AuthPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonVolatile

[Comware5]display snmp-agent usm-user
   User name: test
   Group name: managerpriv
       Engine ID: 8000002B03002257BCD941
       Storage-type: nonVolatile
       UserStatus: active
```

Cisco

```
Cisco(config)#snmp-server group ?
  WORD  Name of the group

Cisco(config)#snmp-server group managerpriv ?
  v1   group using the v1 security model
  v2c  group using the v2c security model
  v3   group using the User Security Model (SNMPv3)

Cisco(config)#snmp-server group managerpriv v3 ?
  auth    group using the authNoPriv Security Level
  noauth  group using the noAuthNoPriv Security Level
  priv    group using SNMPv3 authPriv security level

Cisco(config)#snmp-server group managerpriv v3 auth ?
  access   specify an access-list associated with this group
  context  specify a context to associate these views for the group
  notify   specify a notify view for the group
  read     specify a read view for the group
  write    specify a write view for the group
  <cr>

Cisco(config)#snmp-server group managerpriv v3 auth


Cisco(config)#snmp-server user ?
  WORD  Name of the user

Cisco(config)#snmp-server user test ?
  WORD  Group to which the user belongs

Cisco(config)#snmp-server user test managerpriv ?
  remote  Specify a remote SNMP entity to which the user belongs
  v1      user using the v1 security model
  v2c     user using the v2c security model
  v3      user using the v3 security model

Cisco(config)#snmp-server user test managerpriv v3 ?
  access     specify an access-list associated with this group
  auth       authentication parameters for the user
  encrypted  specifying passwords as MD5 or SHA digests
  <cr>

Cisco(config)#snmp-server user test managerpriv v3 auth ?
  md5  Use HMAC MD5 algorithm for authentication
  sha  Use HMAC SHA algorithm for authentication

Cisco(config)#snmp-server user test managerpriv v3 auth md5 ?
  WORD  authentication password for user

Cisco(config)#snmp-server user test managerpriv v3 auth md5 password ?
  access  specify an access-list associated with this group
  priv    encryption parameters for the user
  <cr>

Cisco(config)#snmp-server user test managerpriv v3 auth md5 password


Cisco(config)#snmp-server host 10.0.100.21 version ?
  1   Use SNMPv1
  2c  Use SNMPv2c
  3   Use SNMPv3

Cisco(config)#snmp-server host 10.0.100.21 version 3 ?
  auth    Use the SNMPv3 authNoPriv Security Level
  noauth  Use the SNMPv3 noAuthNoPriv Security Level
  priv    Use the SNMPv3 authPriv Security Level

Cisco(config)#snmp-server host 10.0.100.21 version 3 auth ?
  WORD  SNMPv1/v2c community string or SNMPv3 user name

Cisco(config)#snmp-server host 10.0.100.21 version 3 auth test ?
  bgp               Allow BGP state change traps
  bridge            Allow SNMP STP Bridge MIB traps
  cef               Allows cef traps
  cluster           Allow Cluster Member Status traps
  config            Allow SNMP config traps
  config-copy       Allow SNMP config-copy traps
  config-ctid       Allow SNMP config-ctid traps
  copy-config       Allow SNMP config-copy traps
  cpu               Allow cpu related traps
  dot1x             Allow dot1x traps
  eigrp             Allow SNMP EIGRP traps
  entity            Allow SNMP entity traps
  envmon            Allow environmental monitor traps
  errdisable        Allow errordisable notifications
  event-manager     Allow SNMP Embedded Event Manager traps
  flash             Allow SNMP FLASH traps
  hsrp              Allow SNMP HSRP traps
  ipmulticast       Allow SNMP ipmulticast traps
  mac-notification  Allow SNMP MAC Notification Traps
  msdp              Allow SNMP MSDP traps
  mvpn              Allow Multicast Virtual Private Network traps
  ospf              Allow OSPF traps
  pim               Allow SNMP PIM traps
  port-security     Allow SNMP port-security traps
  power-ethernet    Allow SNMP power ethernet traps
  rtr               Allow SNMP Response Time Reporter traps
  snmp              Allow SNMP-type notifications
  storm-control     Allow SNMP storm-control traps
  stpx              Allow SNMP STPX MIB traps
  syslog            Allow SNMP syslog traps
  tty               Allow TCP connection traps
  udp-port          The notification host's UDP port number (default port 162)
  vlan-membership   Allow SNMP VLAN membership traps
  vlancreate        Allow SNMP VLAN created traps
  vlandelete        Allow SNMP VLAN deleted traps
  vtp               Allow SNMP VTP traps
  <cr>

Cisco(config)#snmp-server host 10.0.100.21 version 3 auth test


Cisco#show snmp host
Notification host: 10.0.100.21  udp-port: 162   type: trap
user: test      security model: v3 auth


Cisco#show snmp user

User name: test
Engine ID: 800000090300001BD4FEF503
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: managerpriv


Cisco#show snmp group
groupname: test                             security model:v3 auth
readview : v1default                        writeview: <no writeview specified>

notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active

groupname: public                           security model:v1
readview : v1default                        writeview: <no writeview specified>

notifyview: <no notifyview specified>
row status: active

groupname: public                           security model:v2c
readview : v1default                        writeview: <no writeview specified>

notifyview: <no notifyview specified>
row status: active

groupname: private                          security model:v1
readview : v1default                        writeview: v1default

notifyview: <no notifyview specified>
row status: active

groupname: private                          security model:v2c
readview : v1default                        writeview: v1default

notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active

groupname: managerpriv                      security model:v3 auth
readview : v1default                        writeview: <no writeview specified>

notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active
```

Chapter 8 SSH

This chapter compares the commands used to enable and configure Secure Shell (SSH) access to the switch.

ProVision	Comware 5	Cisco
ProVision(config)# crypto key generate ssh	[Comware5]public-key local create rsa	Cisco(config)#crypto key generate
ProVision(config)# ip ssh	[Comware5]ssh server enable	Cisco(config)#ip ssh version 2
	[Comware5]user-interface vty 0 4 [Comware5-ui-vty0-4]authentication-mode scheme [Comware5-ui-vty0-4]protocol inbound ssh	Cisco(config)#line vty 0 15 Cisco(config-line)#transport input ssh
	[Comware5]local-user ssh-manager [Comware5-luser-ssh-manager]password simple password [Comware5-luser-ssh-manager]service-type ssh [Comware5-luser-ssh-manager]authorization-attribute level 3	
ProVision(config)# no telnet-server	[Comware5]undo telnet server enable	
ProVision# show ip ssh	[Comware5]display ssh server status [Comware5]display ssh server session	Cisco#show ip ssh
ProVision# show crypto host-public-key	[Comware5]display public-key local rsa public	Cisco#show crypto key mypubkey rsa
ProVision# show ip host-public-key		

ProVision

```
ProVision(config)# crypto ?
 host-cert              Install/remove self-signed certificate for https.
 key                    Install/remove RSA key file for ssh or https server.

ProVision(config)# crypto key ?
 generate               Generate a new key.
 zeroize                Delete existing key.

ProVision(config)# crypto key generate ?
 autorun-key            Install RSA key file for autorun
 cert                   Install RSA key file for https certificate.
 ssh                    Install host key file for ssh server.
```

```
ProVision(config)# crypto key generate ssh ?
 dsa                   Install DSA host key.
 rsa                   Install RSA host key.
 <cr>

ProVision(config)# crypto key generate ssh
Installing new key pair.  If the key/entropy cache is
depleted, this could take up to a minute.


ProVision(config)# ip ssh ?
 cipher                Specify a cipher to enable/disable.
 filetransfer          Enable/disable secure file transfer capability.
 mac                   Specify a mac to enable/disable.
 port                  Specify the TCP port on which the daemon should listen
                       for SSH connections.
 public-key            Configure a client public-key.
 timeout               Specify the maximum length of time (seconds) permitted
                       for protocol negotiation and authentication.
 <cr>

ProVision(config)# ip ssh


ProVision(config)# no telnet-server


ProVision# show ip ssh

  SSH Enabled     : Yes                 Secure Copy Enabled : No
  TCP Port Number : 22                  Timeout (sec)       : 120
  Host Key Type   : RSA                 Host Key Size       : 2048

  Ciphers : aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,
            rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
  MACs    : hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96

  Ses Type     | Source IP                                      Port
  --- -------- + ---------------------------------------------- -----
  1   console  |
  2   inactive |
  3   inactive |
  4   inactive |
  5   inactive |
  6   inactive |


ProVision# show crypto host-public-key

SSH host public key:

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2tfJ6jJIdewRSD8D5YV8/wqWPLa0leK5VDBDBZeqmAIJ
GL7JQmO+N+WgPVvbIm8V20QCqR1WHVsVNUAE6O6ErFybfk098Y089HuA7v6ej8lTF9r0U0BMQuNLp5C4
++92wCh/mWJmwTUBIqY2w2tfq4rtNxapHN+NTQAiPQIc/6o5wIHHC8fNjUf5pwil+nxYOk/migsklDAG
CyH6OdUWWO2Rb2J/nouBOyz/VKLLuT4kO8LF728rxPBQfk7m/a3cKBKkSAM9O+cuTDzT1u3hOnc3zKGh
Q38nMfTPvCCQZLTljhGGywHl0uGxzHbSFShRyIRyIrMpvQtX85GcLcZLhw==

-or-

ProVision# show ip host-public-key

SSH host public key:
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2tfJ6jJIdewRSD8D5YV8/wqWPLa0leK5VDBDBZeqmAIJ
GL7JQmO+N+WgPVvbIm8V20QCqR1WHVsVNUAE6O6ErFybfk098Y089HuA7v6ej8lTF9r0U0BMQuNLp5C4
++92wCh/mWJmwTUBIqY2w2tfq4rtNxapHN+NTQAiPQIc/6o5wIHHC8fNjUf5pwil+nxYOk/migsklDAG
CyH6OdUWWO2Rb2J/nouBOyz/VKLLuT4kO8LF728rxPBQfk7m/a3cKBKkSAM9O+cuTDzT1u3hOnc3zKGh
Q38nMfTPvCCQZLTljhGGywHl0uGxzHbSFShRyIRyIrMpvQtX85GcLcZLhw==
```

Comware 5

```
[Comware5]public-key ?
  local  Local public key pair operations
  peer   Peer public key configuration

[Comware5]public-key local ?
  create   Create new local key pair
  destroy  Destroy the local key pair
  export   Print or export the local key pair

[Comware5]public-key local create ?
  dsa  Key type DSA
  rsa  Key type RSA

[Comware5]public-key local create rsa ?
  <cr>

[Comware5]public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...


[Comware5]user-interface vty 0 4

[Comware5-ui-vty0-4]authentication-mode ?
  none      Login without checking
  password  Authentication use password of user terminal interface
  scheme    Authentication use AAA

[Comware5-ui-vty0-4]authentication-mode scheme ?
  <cr>

[Comware5-ui-vty0-4]authentication-mode scheme

[Comware5-ui-vty0-4]protocol ?
  inbound  Specify user interface incoming protocol

[Comware5-ui-vty0-4]protocol inbound ?
  all     All protocols
  ssh     SSH protocol
  telnet  Telnet protocol

[Comware5-ui-vty0-4]protocol inbound ssh ?
  <cr>

[Comware5-ui-vty0-4]protocol inbound ssh
```

```
[Comware5]local-user ssh-manager

[Comware5-luser-ssh-manager]password simple password

[Comware5-luser-ssh-manager]service-type ?
  ftp         FTP service type
  lan-access  LAN-ACCESS service type
  portal      Portal service type
  ssh         Secure Shell service type
  telnet      TELNET service type
  terminal    TERMINAL service type

[Comware5-luser-ssh-manager]service-type ssh ?
  telnet    TELNET service type
  terminal  TERMINAL service type
  <cr>

[Comware5-luser-ssh-manager]service-type ssh

[Comware5-luser-ssh-manager]authorization-attribute level 3


[Comware5]ssh ?
  client  Specify SSH client attribute
  server  Specify the server attribute
  user    SSH user

[Comware5]ssh server ?
  authentication-retries  Specify authentication retry times
  authentication-timeout  Specify authentication timeout
  compatible-ssh1x        Specify the compatible ssh1x
  enable                  Enable SSH Server
  rekey-interval          Specify the SSH server key rekey-interval

[Comware5]ssh server enable


[Comware5]display ssh server ?
  session  Server session
  status   Server state

[Comware5]display ssh server status
 SSH server: Enable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP server Idle-Timeout: 10 minute(s)

[Comware5]display ssh server session
 Conn   Ver   Encry    State          Retry    SerType  Username
 VTY 0  2.0   AES      Established    0        Stelnet  ssh-manager
```

```
[Comware5]display public-key local rsa public

=====================================================
Time of Key pair created: 18:08:25  2010/04/27
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100BF9873D61FE6971D0BC751
3FB6D289FD30F330C4A41DB4A114733D9A874C88B886F15B4E49D95F95DF92BB018B2C66E9307AFB
3404CC24E00630F6F1C2031C0C7B64048AD76AD5AC5B58DE79386D6BB4566C4EB9370B9054C851C7
547440B48CBB825A37E0A3EC4E67300055540FB449A7503A8F6926B0FBACFE9530F23ADC37020301
0001

=====================================================
Time of Key pair created: 18:08:26  2010/04/27
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100098935BBFE880CA4D7B791C9556C088
527B426061D5AA9FE176E45A880C380645C10CD4C78DF561A65C8ABD81BB87BE4E5E571580A2D8E1
4395A11E5064B7DD6A4868C848C95E7E63604FC3E484C990D1C656F2EBFF01460312983E29BBC803
C30203010001
```

Cisco

```
Cisco(config)#crypto ?
  ca      Certification authority
  engine  Crypto Engine Config Menu
  key     Long term key operations
  pki     Public Key components

Cisco(config)#crypto key ?
  decrypt       Decrypt a keypair.
  encrypt       Encrypt a keypair.
  export        Export keys
  generate      Generate new keys
  import        Import keys
  pubkey-chain  Peer public key chain management
  storage       default storage location for keypairs
  zeroize       Remove keys

Cisco(config)#crypto key generate ?
  rsa  Generate RSA keys
  <cr>

Cisco(config)#crypto key generate
The name for the keys will be: Cisco.test
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

Cisco(config)#ip ssh ?
  authentication-retries  Specify number of authentication retries
  dscp                    IP DSCP value for SSH traffic
  logging                 Configure logging for SSH
  precedence              IP Precedence value for SSH traffic
  source-interface        Specify interface for source address in SSH
```

```
                          connections
  time-out                Specify SSH time-out interval
  version                 Specify protocol version supported


Cisco(config)#ip ssh version ?
  <1-2>  Protocol version

Cisco(config)#ip ssh version 2


Cisco(config)#line vty 0 15

Cisco(config-line)#transport ?
  input      Define which protocols to use when connecting to the terminal
             server
  output     Define which protocols to use for outgoing connections
  preferred  Specify the preferred protocol to use

Cisco(config-line)#transport input ?
  all     All protocols
  none    No protocols
  ssh     TCP/IP SSH protocol
  telnet  TCP/IP Telnet protocol

Cisco(config-line)#transport input ssh ?
  telnet  TCP/IP Telnet protocol
  <cr>

Cisco(config-line)#transport input ssh


Cisco#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3


Cisco#show ssh
Connection Version Mode Encryption  Hmac         State                 Username
1          2.0     IN   3des-cbc    hmac-sha1    Session started       manager
1          2.0     OUT  3des-cbc    hmac-sha1    Session started       manager
%No SSHv1 server connections running.


Cisco#show crypto key mypubkey rsa
% Key pair was generated at: 18:00:53 CST Feb 28 1993
Key name: TP-self-signed-3573478656
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00DFA8C2
  B7ECEC95 5C4B9FB2 FD0AF282 DB02FC6A D5FA0438 C53BB33E E522FD6D DBED45B0
  DD5A2E8C 9B506873 5AA967B5 F348AB82 F0478A4F ECC87642 3DC9C438 2D873B47
  CA803771 AE5B11FE F300F3C2 429EF54D C5BE25B1 41E6528F 3182BBAD 19D84495
  C2F0C526 14CFB3DF 804ED491 5C884895 B7580021 98F119AF 2535BCB7 73020301 0001
% Key pair was generated at: 14:03:03 CST Nov 24 2009
Key name: Cisco.test
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D42E3E 08934426
  F103032E 4A618CC3 D4C7D9AE 4B9778D4 7648D45C 77EAD928 A3B37D27 7AB97E64
  5BDDEF22 9D5F770A 564CA74B 01B05A94 8A926A18 BD8299F7 87020301 0001
```

Chapter 9 SSL (Self-Signed Certificates)

This chapter compares the commands used to configure Secure Sockets Layer (SSL) to generate a self-signed certificate on ProVision and Cisco switches. Comware 5 supports only certificates signed by a certificate authority (CA).

ProVision	Comware 5	Cisco
`ProVision(config)# crypto key generate cert 512`	***Note: Comware 5 supports only CA-signed certificates.***	`Cisco(config)#crypto key generate rsa`
`ProVision(config)# crypto host-cert generate self-signed`		
`ProVision(config)# web-management ssl`		`Cisco(config)#ip http secure-server`
`ProVision(config)# no web-management plaintext`		`Cisco(config)#no ip http server`
`ProVision# show crypto host-cert`		`Cisco#show crypto pki certificates verbose`

ProVision

```
ProVision(config)# crypto ?
 host-cert              Install/remove self-signed certificate for https.
 key                    Install/remove RSA key file for ssh or https server.

ProVision(config)# crypto key ?
 generate               Generate a new key.
 zeroize                Delete existing key.

ProVision(config)# crypto key generate ?
 autorun-key            Install RSA key file for autorun
 cert                   Install RSA key file for https certificate.
 ssh                    Install host key file for ssh server.

ProVision(config)# crypto key generate cert ?
 512                    Install  512-bit RSA key.
 768                    Install  768-bit RSA key.
 1024                   Install 1024-bit RSA key.
 rsa                    Install RSA host key.

ProVision(config)# crypto key generate cert 512
Installing new key pair.  If the key/entropy cache is
depleted, this could take up to a minute.


ProVision(config)# crypto ?
 host-cert              Install/remove self-signed certificate for https.
 key                    Install/remove RSA key file for ssh or https server.

ProVision(config)# crypto host-cert ?
 generate               Create a self-signed certificate for the https server.
 zeroize                Delete an existing certificate.

ProVision(config)# crypto host-cert generate ?
 self-signed            Create a self-signed certificate for the https server.

ProVision(config)# crypto host-cert generate self-signed
Validity start date [01/07/1970]: 01/01/2009
Validity end date   [01/01/2010]: 01/01/2020
```

```
Common name           [10.0.1.2]: ProVision
Organizational unit  [Dept Name]: Lab
Organization      [Company Name]: Test
City or location          [City]: Any City
State name               [State]: Any State
Country code                [US]:


ProVision(config)# web-management ?
 management-url        Specify URL for web interface [?] button.
 plaintext             Enable/disable the http server (insecure).
 ssl                   Enable/disable the https server (secure).
 support-url           Specify URL for web interface Support page.
 <cr>

ProVision(config)# web-management ssl ?
 TCP/UDP-PORT          TCP port on which https server should accept
                       connections.
 <cr>

ProVision(config)# web-management ssl


ProVision(config)# no web-management plaintext


ProVision# show crypto ?
 autorun-cert          Display trusted certificate.
 autorun-key           Display autorun key.
 client-public-key     Display ssh authorized client public keys.
 host-cert             Display https certificate information.
 host-public-key       Display ssh host RSA public key.

ProVision# show crypto host-cert
Version: 1 (0x0)
Serial Number: 0 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: CN=ProVision, L=Any City, ST=Any State, C=us, O=Test, OU=Lab
Validity
    Not Before: Jan  1 00:00:00 2009 GMT
    Not After : Jan  1 23:59:59 2020 GMT
Subject: CN=ProVision, L=Any City, ST=Any State, C=us, O=Test, OU=Lab
Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (512 bit)
      Modulus (512 bit):
          00:a5:85:f9:49:ee:ec:45:dc:0e:be:36:7a:b3:fb:
          6e:f2:a5:6c:89:23:6d:cb:f1:b7:06:2f:5f:f9:85:
          d5:cc:a7:a2:8b:ea:b4:91:17:a4:b4:10:89:39:60:
          cb:1e:37:0a:6e:32:1e:c3:64:07:4e:d1:be:00:c0:
          15:9b:05:ed:0d
      Exponent: 35 (0x23)
Signature Algorithm: md5WithRSAEncryption
   99:98:39:6c:47:a1:02:4a:92:04:bc:1e:e3:32:b1:07:62:71:
   bd:11:22:4b:71:c4:28:87:d4:ce:fd:9a:14:d3:0f:d8:c8:95:
   c4:f4:3d:a6:be:63:4a:74:35:19:16:f7:60:04:77:54:3c:9e:
   c8:ab:99:03:d8:d0:38:e0:8f:90

MD5 Fingerprint: 287E 9510 5016 E8BE 711B 2115 31E8 5DEA
SHA1 Fingerprint: 61A6 6E27 C0E0 8B53 4EAF 11F8 EF75 DBC9 8DD8 E320
```

Comware 5

Note: Comware 5 supports only CA-signed certificates.

Cisco

```
Cisco(config)#crypto ?
  ca      Certification authority
  engine  Crypto Engine Config Menu
  key     Long term key operations
  pki     Public Key components

Cisco(config)#crypto key ?
  decrypt       Decrypt a keypair.
  encrypt       Encrypt a keypair.
  export        Export keys
  generate      Generate new keys
  import        Import keys
  pubkey-chain  Peer public key chain management
  storage       default storage location for keypairs
  zeroize       Remove keys

Cisco(config)#crypto key generate ?
  rsa  Generate RSA keys
  <cr>

Cisco(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  storage       Provide a storage location
  usage-keys    Generate separate RSA key pairs for signing and encryption
  <cr>

Cisco(config)#crypto key generate rsa


Cisco(config)#ip http ?
  access-class                  Restrict http server access by access-class
  active-session-modules        Set up active http server session modules
  authentication                Set http server authentication method
  client                        Set http client parameters
  help-path                     HTML help root URL
  max-connections               Set maximum number of concurrent http server
                                connections
  path                          Set base path for HTML
  port                          Set http server port
  secure-active-session-modules Set up active http secure server session
                                modules
  secure-ciphersuite            Set http secure server ciphersuite
  secure-client-auth            Set http secure server with client
                                authentication
  secure-port                   Set http secure server port number for
                                listening
  secure-server                 Enable HTTP secure server
  secure-trustpoint             Set http secure server certificate trustpoint
  server                        Enable http server
  session-module-list           Set up a http(s) server session module list
  timeout-policy                Set http server time-out policy parameters

Cisco(config)#ip http secure-server ?
  <cr>

Cisco(config)#ip http secure-server

(note: http secure-server is enabled by default and a self-signed certificate is
automatically generated)


Cisco(config)#no ip http server
```

```
Cisco#show crypto ?
  ca   Show certification authority policy
  eli  Encryption Layer Interface
  key  Show long term public keys
  pki  Show PKI

Cisco#show crypto pki ?
  certificates  Show certificates
  crls          Show Certificate Revocation Lists
  timers        Show PKI Timers
  trustpoints   Show trustpoints

Cisco#show crypto pki certificates ?
  WORD     Trustpoint Name
  storage  show certificate storage location
  verbose  Display in verbose mode
  |        Output modifiers
  <cr>

Cisco#show crypto pki certificates verbose
Router Self-Signed Certificate
  Status: Available
  Version: 3
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-3573478656
  Subject:
    Name: IOS-Self-Signed-Certificate-3573478656
    cn=IOS-Self-Signed-Certificate-3573478656
  Validity Date:
    start date: 22:21:36 CST Nov 24 2009
    end   date: 18:00:00 CST Dec 31 2019
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: C23976AE 635BF16D 3EA4F59F 1E51FFAF
  Fingerprint SHA1: 1E9A9ACB E9D190A5 E77D9FDD A7921494 4B234964
  X509v3 extensions:
    X509v3 Subject Key ID: 90EA0D3A C3773358 1B0F611B D32210AA 5EBBF159
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Subject Alternative Name:
        Cisco.test
    X509v3 Authority Key ID: 90EA0D3A C3773358 1B0F611B D32210AA 5EBBF159
    Authority Info Access:
  Associated Trustpoints: TP-self-signed-3573478656
  Storage: nvram:IOS-Self-Sig#3637.cer
```

Chapter 10 RADIUS Authentication for Switch Management

This chapter covers the commands required to authenticate management users to a network RADIUS server.

a) Basic Configuration

ProVision	Comware 5	Cisco
	(If you are planning to use SSH, you should configure it before you configure AAA support.) (See notes below concerning login procedures for RADIUS.)	
	[Comware5]radius scheme radius-auth	Cisco(config)#aaa new-model
ProVision(config)# radius-server host 10.0.100.111 key password	[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812 [Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813 [Comware5-radius-radius-auth]key authentication password [Comware5-radius-radius-auth]key accounting password [Comware5-radius-radius-auth]user-name-format without-domain [Comware5-radius-radius-auth]server-type extended	Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password
ProVision(config)# aaa authentication telnet login radius none		Cisco(config)#aaa authentication login default group radius
ProVision(config)# aaa authentication telnet enable radius none		
	[Comware5]domain lab	
	[Comware5-isp-lab]authentication login radius-scheme radius-auth [Comware5-isp-lab]authorization login radius-scheme radius-auth [Comware5-isp-lab]accounting login radius-scheme radius-auth	
	[Comware5]domain default enable lab	
		Cisco(config)#line vty 0 15
		Cisco(config-line)#login authentication default

ProVision# show radius	[Comware5]display radius scheme	Cisco#show aaa servers
ProVision# show authentication		
ProVision# show radius authentication		
ProVision# show radius host 10.0.100.111	[Comware5]display radius statistics	Cisco#show radius statistics

ProVision

```
ProVision(config)# radius-server ?
 dead-time              Server unavailability time (default is 0, use the 'no'
                        form of command to set the dead-time to 0).
 dyn-autz-port          UDP port number to listen for Change-of-Authorization
                        and Disconnect messages (default is 3799).
 host                   IP address of the RADIUS server to use.
 key                    Global encryption key (default is NULL).
 retransmit             Number of packet retransmits (default is 3).
 timeout                Server timeout interval (default is 5).

ProVision(config)# radius-server host 10.0.100.111 ?
 acct-port              Accounting UDP destination port number (default is
                        1813).
 auth-port              Authentication UDP destination port number (default is
                        1812).
 dyn-authorization      Enable/disable dynamic authorization control from this
                        host.
 key                    Encryption key to use with the RADIUS server (default is
                        NULL).
 time-window            time window (in seconds) within which the received
                        dynamic authorization requests are considered to be
                        current and accepted for processing.
 <cr>

ProVision(config)# radius-server host 10.0.100.111 key ?
 KEY-STR                Encryption key to use with the RADIUS server (default is
                        NULL).
 acct-port              Accounting UDP destination port number (default is
                        1813).
 auth-port              Authentication UDP destination port number (default is
                        1812).

ProVision(config)# radius-server host 10.0.100.111 key password ?
 acct-port              Accounting UDP destination port number (default is
                        1813).
 auth-port              Authentication UDP destination port number (default is
                        1812).
 <cr>

ProVision(config)# radius-server host 10.0.100.111 key password


ProVision(config)# aaa
 accounting             Configure accounting parameters on the switch.
 authentication         Configure authentication parameters on the switch.
 authorization          Configure authorization parameters on the switch.
 port-access            Configure 802.1X (Port Based Network Access), MAC
                        address based network access, or web authentication
                        based network access on the device.
 server-group           Place the server with the ip address into the radius
                        group.
```

```
ProVision(config)# aaa authentication ?
 console               Configure authentication mechanism used to control
                       access to the switch console.
 login                 Specify that switch respects the authentication server's
                       privilege level.
 mac-based             Configure authentication mechanism used to control
                       mac-based port access to the switch.
 num-attempts          Specify the maximum number of login attempts allowed.
 port-access           Configure authentication mechanism used to control
                       access to the network.
 ssh                   Configure authentication mechanism used to control SSH
                       access to the switch.
 telnet                Configure authentication mechanism used to control
                       telnet access to the switch.
 web                   Configure authentication mechanism used to control web
                       access to the switch.
 web-based             Configure authentication mechanism used to control
                       web-based port access to the switch.

ProVision(config)# aaa authentication telnet ?
 enable                Configure access to the privileged mode commands.
 login                 Configure login access to the switch.

ProVision(config)# aaa authentication telnet login ?
 local                 Use local switch user/password database.
 tacacs                Use TACACS+ server.
 radius                Use RADIUS server.
 peap-mschapv2         Use RADIUS server with PEAP-MSChapv2.

ProVision(config)# aaa authentication telnet login radius ?
 local                 Use local switch user/password database.
 none                  Do not use backup authentication methods.
 authorized            Allow access without authentication.
 server-group          Specify the server group to use.
 <cr>

ProVision(config)# aaa authentication telnet login radius none ?
 <cr>

ProVision(config)# aaa authentication telnet login radius none


ProVision(config)# aaa authentication telnet enable radius none


ProVision# show radius

 Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection : Outgoing Interface

                  Auth  Acct  DM/  Time

  Server IP Addr  Port  Port  CoA  Window  Encryption Key                   OOBM

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

  10.0.100.111    1812  1813  No   300     password                         No
```

```
ProVision# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

               | Login      Login         Login
  Access Task  | Primary    Server Group  Secondary
  ------------ + ---------- ------------- ----------
  Console      | Local                    None
  Telnet       | Radius     radius        None
  Port-Access  | Local                    None
  Webui        | Local                    None
  SSH          | Local                    None
  Web-Auth     | ChapRadius radius        None
  MAC-Auth     | ChapRadius radius        None

               | Enable     Enable        Enable
  Access Task  | Primary    Server Group  Secondary
  ------------ + ---------- ------------- ----------
  Console      | Local                    None
  Telnet       | Radius     radius        None
  Webui        | Local                    None
  SSH          | Local                    None


ProVision# show radius authentication

 Status and Counters - RADIUS Authentication Information

  NAS Identifier : ProCurve
  Invalid Server Addresses : 0

                  UDP
  Server IP Addr  Port  Timeouts   Requests   Challenges Accepts    Rejects
  --------------- ----- ---------- ---------- ---------- ---------- ----------
  10.0.100.111    1812  0          2          0          2          0

ProVision# show radius host 10.0.100.111

 Status and Counters - RADIUS Server Information


  Server IP Addr : 10.0.100.111

  Authentication UDP Port : 1812         Accounting UDP Port  : 1813
  Round Trip Time         : 3            Round Trip Time      : 0
  Pending Requests        : 0            Pending Requests     : 0
  Retransmissions         : 0            Retransmissions      : 30
  Timeouts                : 0            Timeouts             : 40
  Malformed Responses     : 0            Malformed Responses  : 0
  Bad Authenticators      : 0            Bad Authenticators   : 0
  Unknown Types           : 0            Unknown Types        : 0
  Packets Dropped         : 0            Packets Dropped      : 0
  Access Requests         : 5            Accounting Requests  : 67
  Access Challenges       : 0            Accounting Responses : 57
  Access Accepts          : 5
  Access Rejects          : 0
```

Comware 5

(If you are planning to use SSH, you should configure SSH before you configure AAA support.)

Special note on using AAA authentication. User must login as “user@domain”, even if the domain info is not sent to the authentication server. This action is what triggers the AAA authentication function in the switch.

Optionally, if the ‘default domain enable <name>’ parameter is configured, if the user does not include the “@domain” with the UID the system will insert the domain for the purposes of triggering the AAA authentication process.

```
[Comware5]radius ?
  client  Radius Client config
  nas-ip  Specify RADIUS client ip address
  scheme  Add RADIUS scheme or modify radius-scheme attributes
  trap    Specify trap configuration

[Comware5]radius scheme ?
  STRING<1-32>  Radius scheme name

[Comware5]radius scheme radius-auth
New Radius scheme

[Comware5-radius-radius-auth]?
Radius-template view commands:
  data-flow-format        Specify data flow format
  display                 Display current system information
  key                     Specify the shared encryption key of RADIUS server
  mtracert                Trace route to multicast source
  nas-ip                  Specify RADIUS client ip address
  ping                    Ping function
  primary                 Specify IP address of primary RADIUS server
  quit                    Exit from current command view
  retry                   Specify retransmission times
  return                  Exit to User View
  save                    Save current configuration
  secondary               Specify IP address of secondary RADIUS server
  security-policy-server  Specify IP address of security policy server
  server-type             Specify the type of RADIUS server
  state                   Specify state of primary/secondary
                          authentication/accounting RADIUS server
  stop-accounting-buffer  Enable stop-accounting packet buffer
  timer                   Specify timer parameters
  tracert                 Trace route function
  undo                    Cancel current setting
  user-name-format        Specify user-name format sent to RADIUS server

[Comware5-radius-radius-auth]primary ?
  accounting      Specify IP address of primary accounting RADIUS server
  authentication  Specify IP address of primary authentication RADIUS server

[Comware5-radius-radius-auth]primary authentication ?
  X.X.X.X  Any valid IP address
```

```
[Comware5-radius-radius-auth]primary authentication 10.0.100.111 ?
  INTEGER<1-65535>  Authentication-port : generally is 1812
  <cr>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812 ?
  <cr>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812


[Comware5-radius-radius-auth]primary accounting ?
  X.X.X.X  Any valid IP address

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 ?
  INTEGER<1-65535>  Accounting-port : generally is 1813
  <cr>

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813 ?
  <cr>

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813

[Comware5-radius-radius-auth]key ?
  accounting      Specify key for accounting RADIUS server
  authentication  Specify key for authentication RADIUS server

[Comware5-radius-radius-auth]key authentication ?
  STRING<1-64>  Key-string

[Comware5-radius-radius-auth]key authentication password ?
  <cr>

[Comware5-radius-radius-auth]key authentication password

[Comware5-radius-radius-auth]key accounting password

[Comware5-radius-radius-auth]user-name-format ?
  keep-original   User name unchanged
  with-domain     User name like XXX@XXX
  without-domain  User name like XXX

[Comware5-radius-radius-auth]user-name-format without-domain ?
  <cr>

[Comware5-radius-radius-auth]user-name-format without-domain


[Comware5-radius-radius-auth]server-type ?
  extended  Server based on RADIUS extensions
  standard  Server based on RFC protocol(s)

[Comware5-radius-radius-auth]server-type extended ?
  <cr>

[Comware5-radius-radius-auth]server-type extended
```

```
[Comware5]domain lab
New Domain added.

[Comware5-isp-lab]?
Isp view commands:
  access-limit      Specify access limit of domain
  accounting        Specify accounting scheme
  authentication    Specify authentication scheme
  authorization     Specify authorization scheme
  display           Display current system information
  idle-cut          Specify idle-cut attribute of domain
  mtracert          Trace route to multicast source
  ping              Ping function
  quit              Exit from current command view
  return            Exit to User View
  save              Save current configuration
  self-service-url  Specify self-service URL(Uniform Resource Locator) of
                    domain
  state             Specify state of domain
  tracert           Trace route function
  undo              Cancel current setting

[Comware5-isp-lab]authentication ?
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration

[Comware5-isp-lab]authentication login ?
  hwtacacs-scheme  Specify HWTACACS scheme
  local            Specify local scheme
  none             Specify none scheme
  radius-scheme    Specify RADIUS scheme

[Comware5-isp-lab]authentication login radius-scheme ?
  STRING<1-32>  Scheme name

[Comware5-isp-lab]authentication login radius-scheme radius-auth

[Comware5-isp-lab]authorization login radius-scheme radius-auth

[Comware5-isp-lab]accounting login radius-scheme radius-auth

[Comware5]domain default enable lab


[Comware5]display radius ?
  scheme      The RADIUS scheme information
  statistics  Statistics information

[Comware5]display radius scheme ?
  STRING<1-32>  The RADIUS scheme name in the system. If not inputted, show the
                information of all the RADIUS scheme(s)
  slot          Specify slot number
  <cr>
```

```
[Comware5]display radius scheme
------------------------------------------------------------------
SchemeName  : radius-auth
  Index : 0                            Type : extended
  Primary Auth IP  : 10.0.100.111      Port : 1812   State : active
  Primary Acct IP  : 10.0.100.111      Port : 1813   State : active
  Second  Auth IP  : 0.0.0.0           Port : 1812   State : block
  Second  Acct IP  : 0.0.0.0           Port : 1813   State : block
  Auth Server Encryption Key : password
  Acct Server Encryption Key : password
  Interval for timeout(second)                            : 3
  Retransmission times for timeout                        : 3
  Interval for realtime accounting(minute)                : 12
  Retransmission times of realtime-accounting packet      : 5
  Retransmission times of stop-accounting packet          : 500
  Quiet-interval(min)                                     : 5
  Username format                                         : without-domain
  Data flow unit                                          : Byte
  Packet unit                                             : one


------------------------------------------------------------------
Total 1 RADIUS scheme(s).

[Comware5]display radius statistics ?
  slot  Specify slot number
  <cr>

[Comware5]display radius statistics
 Slot  1:state statistic(total=4096):
     DEAD = 4095     AuthProc = 0        AuthSucc = 0
AcctStart = 0         RLTSend = 0         RLTWait = 1
 AcctStop = 0          OnLine = 1            Stop = 0
 StateErr = 0

Received and Sent packets statistic:
Sent PKT total   = 3594
Received PKT total = 3548
Resend Times     Resend total
1                30
2                30
Total            60
RADIUS received packets statistic:
Code =  2   Num = 578      Err = 0
Code =  3   Num = 3        Err = 0
Code =  5   Num = 662      Err = 37
Code = 11   Num = 2305     Err = 6

Running statistic:
RADIUS received messages statistic:
Normal auth request      Num = 7        Err = 0        Succ = 7
EAP auth request         Num = 2875     Err = 0        Succ = 2875
Account request          Num = 10       Err = 0        Succ = 10
Account off request      Num = 36       Err = 0        Succ = 36
PKT auth timeout         Num = 6        Err = 2        Succ = 4
PKT acct_timeout         Num = 83       Err = 27       Succ = 56
Realtime Account timer   Num = 606      Err = 0        Succ = 606
```

```
PKT response             Num = 3548     Err = 43       Succ = 3505
Session ctrl pkt         Num = 0        Err = 0        Succ = 0
Normal author request    Num = 0        Err = 0        Succ = 0
Set policy result        Num = 0        Err = 0        Succ = 0
RADIUS sent messages statistic:
Auth accept              Num = 578
Auth reject              Num = 5
EAP auth replying        Num = 2299
Account success          Num = 624
Account failure          Num = 1
Server ctrl req          Num = 0
RecError_MSG_sum     = 0
SndMSG_Fail_sum      = 0
Timer_Err            = 0
Alloc_Mem_Err        = 0
State Mismatch       = 0
Other_Error          = 0

No-response-acct-stop packet = 1
Discarded No-response-acct-stop packet for buffer overflow = 0
```

Cisco

```
Cisco(config)#aaa ?
  new-model  Enable NEW access control commands and functions.(Disables OLD
             commands.)

Cisco(config)#aaa new-model


Cisco(config)#radius-server ?
  attribute           Customize selected radius attributes
  authorization       Authorization processing information
  backoff             Retry backoff pattern(Default is retransmits with
                      constant delay)
  cache               AAA auth cache default server group
  challenge-noecho    Data echoing to screen is disabled during
                      Access-Challenge
  configure-nas       Attempt to upload static routes and IP pools at startup
  dead-criteria       Set the criteria used to decide when a radius server is
                      marked dead
  deadtime            Time to stop using a server that doesn't respond
  directed-request    Allow user to specify radius server to use with `@server'
  domain-stripping    Strip the domain from the username
  host                Specify a RADIUS server
  key                 encryption key shared with the radius servers
  load-balance        Radius load-balancing options.
  optional-passwords  The first RADIUS request can be made without requesting a
                      password
  retransmit          Specify the number of retries to active server
  retry               Specify how the next packet is sent after timeout.
  source-ports        source ports used for sending out RADIUS requests
  timeout             Time to wait for a RADIUS server to reply
  transaction         Specify per-transaction parameters
  unique-ident        Higher order bits of Acct-Session-Id
  vsa                 Vendor specific attribute configuration

Cisco(config)#radius-server host 10.0.100.111 ?
  acct-port     UDP port for RADIUS accounting server (default is 1646)
  alias         1-8 aliases for this server (max. 8)
  auth-port     UDP port for RADIUS authentication server (default is 1645)
  backoff       Retry backoff pattern (Default is retransmits with constant
                delay)
  key           per-server encryption key (overrides default)
  non-standard  Parse attributes that violate the RADIUS standard
  retransmit    Specify the number of retries to active server (overrides
                default)
  test          Configure server automated testing.
  timeout       Time to wait for this RADIUS server to reply (overrides
                default)
  <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 ?
  acct-port     UDP port for RADIUS accounting server (default is 1646)
  auth-port     UDP port for RADIUS authentication server (default is 1645)
  backoff       Retry backoff pattern (Default is retransmits with constant
                delay)
  key           per-server encryption key (overrides default)
  non-standard  Parse attributes that violate the RADIUS standard
  retransmit    Specify the number of retries to active server (overrides
                default)
  test          Configure server automated testing.
  timeout       Time to wait for this RADIUS server to reply (overrides
                default)
  <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 ?
  auth-port     UDP port for RADIUS authentication server (default is 1645)
  backoff       Retry backoff pattern (Default is retransmits with constant
                delay)
  key           per-server encryption key (overrides default)
  non-standard  Parse attributes that violate the RADIUS standard
  retransmit    Specify the number of retries to active server (overrides
                default)
  test          Configure server automated testing.
  timeout       Time to wait for this RADIUS server to reply (overrides
                default)
  <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key ?
  0     Specifies an UNENCRYPTED key will follow
  7     Specifies HIDDEN key will follow
  LINE  The UNENCRYPTED (cleartext) server key

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password ?
LINE    <cr>

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password


Cisco(config)#aaa ?
  accounting      Accounting configurations parameters.
  attribute       AAA attribute definitions
  authentication  Authentication configurations parameters.
  authorization   Authorization configurations parameters.
  cache           AAA cache definitions
  configuration   Authorization configuration parameters.
  dnis            Associate certain AAA parameters to a specific DNIS number
  group           AAA group definitions
  max-sessions    Adjust initial hash size for estimated max sessions
  nas             NAS specific configuration
  new-model       Enable NEW access control commands and functions.(Disables
                  OLD commands.)
  pod             POD processing
  server          Local AAA server
  session-id      AAA Session ID
  traceback       Traceback recording
  user            AAA user definitions
```

```
Cisco(config)#aaa authentication ?
  arap             Set authentication lists for arap.
  attempts         Set the maximum number of authentication attempts
  banner           Message to use when starting login/authentication.
  dot1x            Set authentication lists for IEEE 802.1x.
  enable           Set authentication list for enable.
  eou              Set authentication lists for EAPoUDP
  fail-message     Message to use for failed login/authentication.
  login            Set authentication lists for logins.
  nasi             Set authentication lists for NASI.
  password-prompt  Text to use when prompting for a password
  ppp              Set authentication lists for ppp.
  sgbp             Set authentication lists for sgbp.
  username-prompt  Text to use when prompting for a username

Cisco(config)#aaa authentication login ?
  WORD     Named authentication list.
  default  The default authentication list.

Cisco(config)#aaa authentication login default ?
  cache        Use Cached-group
  enable       Use enable password for authentication.
  group        Use Server-group
  krb5         Use Kerberos 5 authentication.
  krb5-telnet  Allow logins only if already authenticated via Kerberos V
               Telnet.
  line         Use line password for authentication.
  local        Use local username authentication.
  local-case   Use case-sensitive local username authentication.
  none         NO authentication.

Cisco(config)#aaa authentication login default group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authentication login default group radius ?
  cache       Use Cached-group
  enable      Use enable password for authentication.
  group       Use Server-group
  krb5        Use Kerberos 5 authentication.
  line        Use line password for authentication.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
  <cr>

Cisco(config)#aaa authentication login default group radius


Cisco(config)#line vty 0 15

Cisco(config-line)#login ?
  authentication  Authentication parameters.


Cisco(config-line)#login authentication ?
  WORD     Use an authentication list with this name.
  default  Use the default authentication list.


Cisco(config-line)#login authentication default ?
  <cr>
```

```
Cisco(config-line)#login authentication default


Cisco#show aaa servers

RADIUS: id 3, priority 1, host 10.0.100.111, auth-port 1812, acct-port 1813
     State: current UP, duration 76005s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 9, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 2091ms
             Transaction: success 9, failure 0
     Author: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Account: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Elapsed time since counters last cleared: 45m


Cisco#show radius statistics
                                  Auth.      Acct.       Both
         Maximum inQ length:         NA         NA          1
       Maximum waitQ length:         NA         NA          1
       Maximum doneQ length:         NA         NA          1
       Total responses seen:         17          0         17
     Packets with responses:          9          0          9
  Packets without responses:          1          0          1
 Average response delay(ms):       2091          0       2091
 Maximum response delay(ms):       2441          0       2441
  Number of Radius timeouts:          8          0          8
       Duplicate ID detects:          0          0          0
 Buffer Allocation Failures:          0          0          0
Maximum Buffer Size (bytes):         96          0         96
 Source Port Range: (2 ports only)
 1645 - 1646
 Last used Source Port/Identifier:
 1645/39
 1646/0

  Elapsed time since counters last cleared: 57m
```

b) Privilege Mode

This feature provides a dedicated login at a specific user level, based on the reply the authentication server sends to the switch.

ProVision	Comware 5	Cisco
(Requires special configuration on the RADIUS server)	***Not an available feature***	(Requires special configuration on the RADIUS server)
ProVision(config)# aaa authentication login privilege-mode		Cisco(config)#aaa group server radius radius_auth
		Cisco(config-sg-radius)#server 10.100.111 auth-port 1812 acct-port 1813
		Cisco(config)#aaa authorization exec default group radius_auth if-authenticated

ProVision

```
(Requires special configuration on the RADIUS server)


ProVision(config)# aaa authentication login privilege-mode


ProVision# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Enabled
...
```

Comware 5

Not an available feature

Cisco

```
(Requires special configuration on the RADIUS server)


Cisco(config)#aaa group server radius radius_auth

Cisco(config-sg-radius)#server 10.100.111 auth-port 1812 acct-port 1813

Cisco(config)#aaa authorization exec default group radius_auth if-authenticated
```

c) Commands Authorization

This feature provides a specific set of commands that a user can (or cannot) execute upon login at a specific user level, based on the reply the authentication server sends to the switch.

ProVision	Comware 5	Cisco
`(requires special configuration on the RADIUS server)`	***not an available feature***	***not an available feature***
`ProVision(config)# aaa authorization commands radius`		
`ProVision# show authorization`		

ProVision

```
(Requires special configuration on the RADIUS server)

ProVision(config)# aaa authorization commands radius

ProVision# show authorization

 Status and Counters - Authorization Information

  Type     | Method
  -------- + ------
  Commands | Radius
```

Comware 5

not an available feature

Cisco

Not an available feature

d) RADIUS Accounting

ProVision	Comware 5	Cisco
ProVision(config)# aaa accounting exec start-stop radius	(Basic support only; no other specific feature support)	Cisco(config)#aaa accounting exec default start-stop group radius
ProVision(config)# aaa accounting network start-stop radius		Cisco(config)#aaa accounting network default start-stop group radius
ProVision(config)# aaa accounting system start-stop radius		Cisco(config)#aaa accounting system default start-stop group radius
ProVision(config)# aaa accounting commands stop-only radius		
ProVision# show accounting		Cisco#show aaa user all

ProVision

```
ProVision(config)# aaa accounting ?
 commands              Configure 'commands' type of accounting.
 exec                  Configure 'exec' type of accounting.
 network               Configure 'network' type of accounting.
 suppress              Do not generate accounting records for a specific type
                       of user.
 system                Configure 'system' type of accounting.
 update                Configure update accounting records mechanism.

ProVision(config)# aaa accounting exec ?
 start-stop            Send start and stop record accounting notice.
 stop-only             Send stop record accounting notice only.

ProVision(config)# aaa accounting exec start-stop ?
 radius                Use RADIUS protocol as accounting method.

ProVision(config)# aaa accounting exec start-stop radius ?
 server-group          Specify the server group to use.
 <cr>

ProVision(config)# aaa accounting exec start-stop radius


ProVision(config)# aaa accounting network start-stop radius


ProVision(config)# aaa accounting system start-stop radius


ProVision(config)# aaa accounting commands stop-only radius


ProVision# show accounting

 Status and Counters - Accounting Information

  Interval(min) : 0
  Suppress Empty User : No

  Type     | Method Mode       Server Group
  -------- + ------ ---------- ------------
  Network  | Radius Start-Stop radius
  Exec     | Radius Start-Stop radius
  System   | Radius Start-Stop radius
  Commands | Radius Stop-Only  radius
```

Comware 5

```
(Basic support only, no other specific feature support)
```

Cisco

```
Cisco(config)#aaa accounting ?
  auth-proxy        For authentication proxy events.
  commands          For exec (shell) commands.
  connection        For outbound connections. (telnet, rlogin)
  delay-start       Delay PPP Network start record until peer IP address is
                    known.
  dot1x             For dot1x sessions.
  exec              For starting an exec (shell).
  gigawords         64 bit interface counters to support Radius attributes 52 &
                    53.
  nested            When starting PPP from EXEC, generate NETWORK records
                    before EXEC-STOP record.
  network           For network services. (PPP, SLIP, ARAP)
  resource          For resource events.
  send              Send records to accounting server.
  session-duration  Set the preference for calculating session durations
  suppress          Do not generate accounting records for a specific type of
                    user.
  system            For system events.
  update            Enable accounting update records.

Cisco(config)#aaa accounting exec ?
  WORD     Named Accounting list.
  default  The default accounting list.

Cisco(config)#aaa accounting exec default ?
  none        No accounting.
  start-stop  Record start and stop without waiting
  stop-only   Record stop when service terminates.

Cisco(config)#aaa accounting exec default start-stop ?
  broadcast  Use Broadcast for Accounting
  group      Use Server-group

Cisco(config)#aaa accounting exec default start-stop group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa accounting exec default start-stop group radius ?
  group  Use Server-group
  <cr>

Cisco(config)#aaa accounting exec default start-stop group radius


Cisco(config)#aaa accounting network default start-stop group radius


Cisco(config)#aaa accounting system default start-stop group radius



Cisco#show aaa user all
--------------------------------------------------
Unique id 1 is currently in use.
Accounting:
  log=0x18001
  Events recorded :
    CALL START
    INTERIM START
    INTERIM STOP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    03802C08 0 00000001 connect-progress(44) 4 No Progress
    03802C1C 0 00000001 pre-session-time(272) 4 269025(41AE1)
    03802C30 0 00000001 elapsed_time(339) 4 0(0)
    03802C44 0 00000001 pre-bytes-in(268) 4 0(0)
    03802C58 0 00000001 pre-bytes-out(269) 4 0(0)
    039A269C 0 00000001 pre-paks-in(270) 4 0(0)
    039A26B0 0 00000001 pre-paks-out(271) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
```

Chapter 11 TACACS Authentication for Switch Management

This chapter covers the commands required to authenticate management users to a TACACS server.

a) Basic Configuration

ProVision	Comware 5	Cisco
ProVision(config)# tacacs-server host 10.0.100.111 key password	[Comware5]hwtacacs scheme tacacs_auth	Cisco(config)#tacacs-server host 10.0.100.111 key password
ProVision(config)# aaa authentication telnet login tacacs none	[Comware5-hwtacacs-tacacs_auth]primary authentication 10.0.100.112	Cisco(config)#aaa authentication login default group tacacs+
ProVision(config)# aaa authentication telnet enable tacacs none	[Comware5-hwtacacs-tacacs_auth]primary authorization 10.0.100.112	Cisco(config)#line vty 0 15
	[Comware5-hwtacacs-tacacs_auth]primary accounting 10.0.100.112	Cisco(config-line)#login authentication default
	[Comware5-hwtacacs-tacacs_auth]key authentication password	
	[Comware5-hwtacacs-tacacs_auth]key authorization password	
	[Comware5-hwtacacs-tacacs_auth]key accounting password	
	[Comware5-hwtacacs-tacacs_auth]user-name-format without-domain	
	[Comware5]domain tacacs	
	[Comware5-isp-tacacs]authentication login hwtacacs-scheme tacacs_auth	
	[Comware5-isp-tacacs]authorization login hwtacacs-scheme tacacs_auth	
	[Comware5-isp-tacacs]accounting login hwtacacs-scheme tacacs_auth	
	[Comware5]domain default enable tacacs	
ProVision# show tacacs	[Comware5]display hwtacacs	Cisco#show tacacs
ProVision# show authentication		

ProVision

```
ProVision(config)# tacacs-server ?
 host                   IP address of the server to use.
 key                    Global encryption key.
 timeout                Server timeout interval.

ProVision(config)# tacacs-server host 10.0.100.111 ?
 key                    Encryption key to use with server.
 <cr>

ProVision(config)# tacacs-server host 10.0.100.111 key password ?
 <cr>

ProVision(config)# tacacs-server host 10.0.100.111 key password
ProVision(config)# aaa authentication ?
 console               Configure authentication mechanism used to control
                       access to the switch console.
 login                 Specify that switch respects the authentication server's
                       privilege level.
 mac-based             Configure authentication mechanism used to control
                       mac-based port access to the switch.
 num-attempts          Specify the maximum number of login attempts allowed.
 port-access           Configure authentication mechanism used to control
                       access to the network.
 ssh                   Configure authentication mechanism used to control SSH
                       access to the switch.
 telnet                Configure authentication mechanism used to control
                       telnet access to the switch.
 web                   Configure authentication mechanism used to control web
                       access to the switch.
 web-based             Configure authentication mechanism used to control
                       web-based port access to the switch.

ProVision(config)# aaa authentication telnet ?
 enable                Configure access to the privileged mode commands.
 login                 Configure login access to the switch.

ProVision(config)# aaa authentication telnet login ?
 local                 Use local switch user/password database.
 tacacs                Use TACACS+ server.
 radius                Use RADIUS server.
 peap-mschapv2         Use RADIUS server with PEAP-MSChapv2.

ProVision(config)# aaa authentication telnet login tacacs ?
 local                 Use local switch user/password database.
 none                  Do not use backup authentication methods.
 authorized            Allow access without authentication.
 server-group          Specify the server group to use.
 <cr>

ProVision(config)# aaa authentication telnet login tacacs none ?
 <cr>

ProVision(config)# aaa authentication telnet login tacacs none


ProVision(config)# aaa authentication telnet enable tacacs none


ProVision# show tacacs

 Status and Counters - TACACS Information

  Timeout : 5
  Source IP Selection : 10.0.100.24
  Encryption Key :


  Server IP Addr  Opens  Closes Aborts Errors Pkts Rx Pkts Tx OOBM
  --------------- ------ ------ ------ ------ ------- ------- ----
  10.0.100.111    0      0      0      0      0       0       0


ProVision# show authentication

 Status and Counters - Authentication Information
```

```
  Login Attempts : 3
  Respect Privilege : Disabled

               | Login      Login         Login
  Access Task  | Primary    Server Group  Secondary
  ------------ + ---------- ------------- ----------
  Console      | Local                    None
  Telnet       | Tacacs                   None
  Port-Access  | EapRadius  radius        None
  Webui        | Local                    None
  SSH          | Local                    None
  Web-Auth     | ChapRadius radius        None
  MAC-Auth     | ChapRadius radius        None

               | Enable     Enable        Enable
  Access Task  | Primary    Server Group  Secondary
  ------------ + ---------- ------------- ----------
  Console      | Local                    None
  Telnet       | Tacacs                   None
  Webui        | Local                    None
  SSH          | Local                    None
```

Comware 5

```
[Comware5]hwtacacs scheme tacacs_auth
Create a new HWTACACS-server scheme

[Comware5-hwtacacs-tacacs_auth]primary authentication 10.0.100.112

[Comware5-hwtacacs-tacacs_auth]primary authorization 10.0.100.112

[Comware5-hwtacacs-tacacs_auth]primary accounting 10.0.100.112

[Comware5-hwtacacs-tacacs_auth]key authentication password

[Comware5-hwtacacs-tacacs_auth]key authorization password

[Comware5-hwtacacs-tacacs_auth]key accounting password

[Comware5-hwtacacs-tacacs_auth]user-name-format without-domain


[Comware5]domain tacacs
New Domain added.

[Comware5-isp-tacacs]authentication login hwtacacs-scheme tacacs_auth

[Comware5-isp-tacacs]authorization login hwtacacs-scheme tacacs_auth

[Comware5-isp-tacacs]accounting login hwtacacs-scheme  tacacs_auth


[Comware5]domain default enable tacacs


[Comware5]display hwtacacs ?
  STRING<1-32>  Scheme name
  slot          Specify slot number
  <cr>
```

```
[Comware5]display hwtacacs
  ---------------------------------------------------------------------------
  HWTACACS-server template name     : tacacs_auth
  Primary-authentication-server     : 10.0.100.112:49
  Primary-authorization-server      : 10.0.100.112:49
  Primary-accounting-server         : 10.0.100.112:49
  Secondary-authentication-server   : 0.0.0.0:0
  Secondary-authorization-server    : 0.0.0.0:0
  Secondary-accounting-server       : 0.0.0.0:0
  Current-authentication-server     : 10.0.100.112:49
  Current-authorization-server      : 10.0.100.112:49
  Current-accounting-server         : 10.0.100.112:49
  Nas-IP address                    : 0.0.0.0
  key authentication                : password
  key authorization                 : password
  key accounting                    : password
  Quiet-interval(min)               : 5
  Realtime-accounting-interval(min) : 12
  Response-timeout-interval(sec)    : 5
  Acct-stop-PKT retransmit times    : 100
  Username format                   : without-domain
  Data traffic-unit                 : B
  Packet traffic-unit               : one-packet
  ---------------------------------------------------------------------------
  Total 1 HWTACACS scheme(s).
```

Cisco

```
Cisco(config)#tacacs-server ?
  administration    Start tacacs+ deamon handling administrative messages
  cache             AAA auth cache default server group
  directed-request  Allow user to specify tacacs server to use with `@server'
  dns-alias-lookup  Enable IP Domain Name System Alias lookup for TACACS
                    servers
  host              Specify a TACACS server
  key               Set TACACS+ encryption key.
  packet            Modify TACACS+ packet options
  timeout           Time to wait for a TACACS server to reply

Cisco(config)#tacacs-server host 10.0.100.111 ?
  key                per-server encryption key (overrides default)
  nat                To send client's post NAT address to tacacs+ server
  port               TCP port for TACACS+ server (default is 49)
  single-connection  Multiplex all packets over a single tcp connection to
                     server (for CiscoSecure)
  timeout            Time to wait for this TACACS server to reply (overrides
                     default)
  <cr>

Cisco(config)#tacacs-server host 10.0.100.111 key ?
  0     Specifies an UNENCRYPTED key will follow
  7     Specifies HIDDEN key will follow
  LINE  The UNENCRYPTED (cleartext) shared key

Cisco(config)#tacacs-server host 10.0.100.111 key password


Cisco(config)#aaa authentication ?
  arap             Set authentication lists for arap.
  attempts         Set the maximum number of authentication attempts
  banner           Message to use when starting login/authentication.
  dot1x            Set authentication lists for IEEE 802.1x.
  enable           Set authentication list for enable.
  eou              Set authentication lists for EAPoUDP
  fail-message     Message to use for failed login/authentication.
  login            Set authentication lists for logins.
  nasi             Set authentication lists for NASI.
  password-prompt  Text to use when prompting for a password
  ppp              Set authentication lists for ppp.
  sgbp             Set authentication lists for sgbp.
  username-prompt  Text to use when prompting for a username

Cisco(config)#aaa authentication login ?
  WORD     Named authentication list.
  default  The default authentication list.

Cisco(config)#aaa authentication login default ?
  cache        Use Cached-group
  enable       Use enable password for authentication.
  group        Use Server-group
  krb5         Use Kerberos 5 authentication.
  krb5-telnet  Allow logins only if already authenticated via Kerberos V
               Telnet.
  line         Use line password for authentication.
  local        Use local username authentication.
  local-case   Use case-sensitive local username authentication.
  none         NO authentication.

Cisco(config)#aaa authentication login default group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

Cisco(config)#aaa authentication login default group tacacs+ ?
  cache       Use Cached-group
  enable      Use enable password for authentication.
  group       Use Server-group
  krb5        Use Kerberos 5 authentication.
  line        Use line password for authentication.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
  <cr>


Cisco(config)#aaa authentication login default group tacacs+


Cisco(config)#line vty 0 15

Cisco(config-line)#login ?
  authentication  Authentication parameters.

Cisco(config-line)#login authentication ?
  WORD     Use an authentication list with this name.
  default  Use the default authentication list.

Cisco(config-line)#login authentication default ?
  <cr>

Cisco(config-line)#login authentication default


Cisco#show tacacs

Tacacs+ Server            : 10.0.100.111/49
              Socket opens:          6
             Socket closes:          6
             Socket aborts:          0
             Socket errors:          0
           Socket Timeouts:          0
   Failed Connect Attempts:          0
        Total Packets Sent:          0
        Total Packets Recv:          0
```

b) Privilege Mode

This feature provides a dedicated login at a specific user level, based on the reply the authentication server sends to the switch.

ProVision	Comware 5	Cisco
(Requires special configuration on the TACACS server)	***Not an available feature***	(Requires special configuration on the TACACS server)
`ProVision(config)# aaa authentication login privilege-mode`		`Cisco(config)#aaa new-model`
		`Cisco(config)#aaa group server tacacs+ tacacs_auth`
		`Cisco(config-sg-tacacs+)#server 10.0.100.111`
		`Cisco(config)#aaa authorization exec default group tacacs_auth if-authenticated`
`ProVision# show authentication`		

ProVision

```
(Requires special configuration on the TACACS server)


ProVision(config)# aaa authentication login privilege-mode


ProVision# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Enabled
...
```

Comware 5

Not an available feature

Cisco

```
(Requires special configuration on the TACACS server)


Cisco(config)#aaa new-model

Cisco(config)#aaa group server tacacs+ tacacs_auth

Cisco(config-sg-tacacs+)#server 10.0.100.111

Cisco(config)#aaa authorization exec default group tacacs_auth if-authenticated
```

c) TACACS Accounting

ProVision	Comware 5	Cisco
Not an available feature	(Basic support only; no other specific feature support)	`Cisco(config)#aaa accounting exec default start-stop group tacacs+`
		`Cisco(config)#aaa accounting network default start-stop group tacacs+`
		`Cisco(config)#aaa accounting system default start-stop group tacacs+`
		`Cisco(config)#aaa accounting commands 15 default stop-only group tacacs+`
		`Cisco#show aaa user all`

ProVision

Not an available feature

Comware 5

(Basic support only; no other specific feature support)

Cisco

```
Cisco(config)#aaa accounting exec default start-stop group tacacs+

Cisco(config)#aaa accounting network default start-stop group tacacs+

Cisco(config)#aaa accounting system default start-stop group tacacs+

Cisco(config)#aaa accounting commands 15 default stop-only group tacacs+


Cisco#show aaa user all
--------------------------------------------------
Unique id 1 is currently in use.
Accounting:
  log=0x18001
  Events recorded :
    CALL START
    INTERIM START
    INTERIM STOP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    03802C08 0 00000001 connect-progress(44) 4 No Progress
    03802C1C 0 00000001 pre-session-time(272) 4 269025(41AE1)
    03802C30 0 00000001 elapsed_time(339) 4 0(0)
    03802C44 0 00000001 pre-bytes-in(268) 4 0(0)
    03802C58 0 00000001 pre-bytes-out(269) 4 0(0)
    039A269C 0 00000001 pre-paks-in(270) 4 0(0)
    039A26B0 0 00000001 pre-paks-out(271) 4 0(0)
  ...
```

Chapter 12 Discovery Protocols

This chapter compares two protocols that are used to discover devices on the network:

- Link Layer Discovery Protocol (LLDP), an industry standard protocol for device discovery
- Cisco Discovery Protocol (CDP), a Cisco-specific protocol for device discovery.

ProVision and Comware 5 provide limited support for CDP.

a) LLDP

ProVision	Comware 5	Cisco
(Enabled by default)	(Enabled by default)	(Not enabled by default)
		Cisco(config)#lldp run
ProVision# show lldp info remote-device	[Comware5]display lldp neighbor-information brief	Cisco#show lldp neighbors
ProVision# show lldp info remote-device 9	[Comware5]display lldp neighbor-information interface g1/0/2	Cisco#show lldp neighbors fa0/9 detail

ProVision

```
(Enabled by default)


ProVision# show lldp ?
 auto-provision        Show LLDP auto-provision related info for radio-ports.
 config                Show LLDP configuration information.
 info                  Show LLDP information about the remote or local device.
 stats                 Show LLDP statistics.

ProVision# show lldp info ?
 local-device          Show LLDP local device information.
 remote-device         Show LLDP remote device information.

ProVision# show lldp info remote-device ?
 [ethernet] PORT-LIST  Show remote or local device information for the
                       specified ports.
 <cr>

ProVision# show lldp info remote-device

 LLDP Remote Devices Information

  LocalPort | ChassisId                 PortId PortDescr SysName
  --------- + ------------------------- ------ --------- ----------------------
  9         | 00 16 35 9d cd e0         5      5         2510_1


ProVision# show lldp info remote-device 9

 LLDP Remote Device Information Detail

  Local Port   : 9
  ChassisType  : mac-address
  ChassisId    : 00 16 35 9d cd e0
  PortType     : local
  PortId       : 5
  SysName      : 2510_1
  System Descr : ProCurve J9019A Switch 2510-24, revision Q.10.XX, ROM Q.1...
  PortDescr    : 5
  Pvid         :

  System Capabilities Supported  : bridge
  System Capabilities Enabled    : bridge

  Remote Management Address
     Type    : ipv4
     Address : 10.0.100.120
```

Comware 5

```
(Enabled by default)

[Comware5]display lldp ?
  local-information     Display local information
  neighbor-information  Display neighbor information
  statistics            Display statistics information
  status                Display LLDP status and configuration
  tlv-config            Display TLV configuration

[Comware5]display lldp neighbor-information ?
  brief      Brief message
  interface  Specify interface
  list       Neighbor list
  <cr>

[Comware5]display lldp neighbor-information brief ?
  <cr>

[Comware5]display lldp neighbor-information brief

LLDP neighbor-information of port 2[GigabitEthernet1/0/2]:
  Neighbor 1:
  ChassisID/subtype: 0016-359d-cde0/MAC address
  PortID/subtype   : 10/Locally assigned
  Capabilities     : Bridge

LLDP neighbor-information of port 14[GigabitEthernet1/0/14]:
  Neighbor 1:
  ChassisID/subtype: /Network address
  PortID/subtype   : 0800-0f1e-31f6/MAC address
  Capabilities     : Bridge,Telephone

[Comware5]display lldp neighbor-information interface g1/0/2

LLDP neighbor-information of port 2[GigabitEthernet1/0/2]:
  Neighbor index   : 1
  Update time      : 0 days,0 hours,0 minutes,40 seconds
  Chassis type     : MAC address
  Chassis ID       : 0016-359d-cde0
  Port ID type     : Locally assigned
  Port ID          : 10
  Port description : 10
  System name        : ProCurve_2510_1
  System description : ProCurve J9019A Switch 2510-24, revision Q.10.XX, ROM Q.1
0.X4 (/sw/code/build/harp(bh2))
  System capabilities supported : Bridge
  System capabilities enabled   : Bridge

  Management address type           : ipV4
  Management address                : 10.0.100.120
  Management address interface type : IfIndex
  Management address interface ID   : Unknown
  Management address OID            : 0
```

Cisco

```
(Not enabled by default)

Cisco(config)#lldp run


Cisco#show lldp ?
  entry      Information for specific neighbor entry
  errors     LLDP computational errors and overflows
  interface  LLDP interface status and configuration
  neighbors  LLDP neighbor entries
  traffic    LLDP statistics
  |          Output modifiers
  <cr>

Cisco#show lldp neighbors

Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
MITEL 5212 DM       Fa0/3          10         B,T             0800.0f1e.31f6
2510_1              Fa0/9          120        B               9

Total entries displayed: 2


Cisco#show lldp neighbors fa0/9

Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
2510_1              Fa0/9          120        B               9

Total entries displayed: 1


Cisco#show lldp neighbors fa0/9 detail


Chassis id: 0016.359d.cde0
Port id: 9
Port Description: 9
System Name: 2510_1

System Description:
ProCurve J9019A Switch 2510-24, revision Q.10.XX, ROM Q.10.X4 (/sw/code/build/ha
rp(bh2))

Time remaining: 114 seconds
System Capabilities: B
Enabled Capabilities: B
Management Addresses:
    IP: 10.0.100.120
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
---------------------------------------------

Total entries displayed: 1
```

b) CDP

ProVision	Comware 5	Cisco
(Receive only support)	(Supported only for Cisco CDP-enabled VoIP phones)	
ProVision# show cdp		Cisco#show cdp
ProVision# show cdp neighbors		Cisco#show cdp neighbors
ProVision# show cdp neighbors 9		Cisco#show cdp neighbors f0/3
	[Comware5]lldp compliance cdp	
	[Comware5-GigabitEthernet1/0/14]lldp admin-status txrx	
	[Comware5-GigabitEthernet1/0/14]lldp compliance admin-status cdp txrx	
	[Comware5]display lldp neighbor-information interface g1/0/14	

ProVision

```
ProVision# show cdp

 Global CDP information

  Enable CDP [Yes] : Yes (Receive Only)


  Port CDP
  ---- --------
  1    enabled
  2    enabled
  3    enabled


ProVision# show cdp ?
 neighbors              Show CDP neighbors.
 <cr>

ProVision# show cdp neighbors ?
 detail                 Show neighbor information field-per-line instead of
                        shortened table format.
 [ethernet] PORT-NUM    Show CDP neighbors on specified port only.
 <cr>

ProVision# show cdp neighbors

 CDP neighbors information

  Port Device ID                      | Platform                     Capability
  ---- ------------------------------ + ---------------------------- -----------
  9    00 16 35 9d cd e0              | ProCurve J9019A Switch 25... S


ProVision# show cdp neighbors 9

 CDP neighbors information

  Port Device ID                      | Platform                     Capability
  ---- ------------------------------ + ---------------------------- -----------
  9    00 16 35 9d cd e0              | ProCurve J9019A Switch 25... S
```

```
ProVision# show cdp neighbors detail 9

 CDP neighbors information for port 9

  Port : 9
  Device ID : 00 16 35 9d cd e0
  Address Type : IP
  Address      : 10.0.100.120
  Platform     : ProCurve J9019A Switch 2510-24, revision Q.10.XX, ROM Q....
  Capability   : Switch
  Device Port  : 5
  Version      : ProCurve J9019A Switch 2510-24, revision Q.10.XX, ROM Q....
```

Comware 5

```
(Supported only for Cisco CDP-enabled VoIP phones)

[Comware5]lldp ?
  compliance        Enable compliance with another link layer discovery protocol
  enable            Enable capability
  fast-count        The fast-start times of transmitting frames
  hold-multiplier   Hold multiplicator for TTL
  timer             Timer of LLDP

[Comware5]lldp com
[Comware5]lldp compliance ?
  cdp  Non standard IEEE discovery protocol

[Comware5]lldp compliance cdp ?
  <cr>

[Comware5]lldp compliance cdp


[Comware5-GigabitEthernet1/0/14]lldp ?
  admin-status               Specify transmit/receive mode of LLDP on the port
  check-change-interval      Specify interval of checking system changes
  compliance                 Specify the mode for transmitting/receiving frames
                             of the specified link layer discovery protocol on
                             the port
  enable                     Enable capability
  encapsulation              Specify lldp frame formats
  management-address-format  Specify management-address formats
  management-address-tlv     Management address for other protocol
  notification               Enable the trap capability
  tlv-enable                 Enable optional TLV

[Comware5-GigabitEthernet1/0/14]lldp admin-status ?
  disable  The port can neither transmit nor receive LLDP frames
  rx       The port can only receive LLDP frames
  tx       The port can only transmit LLDP frames
  txrx     The port can both transmit and receive LLDP frames

[Comware5-GigabitEthernet1/0/14]lldp admin-status txrx ?
  <cr>
```

```
[Comware5-GigabitEthernet1/0/14]lldp admin-status txrx

[Comware5-GigabitEthernet1/0/14]lldp compliance ?
  admin-status  Specify the mode for transmitting/receiving frames of the
                specified link layer discovery protocol on the port

[Comware5-GigabitEthernet1/0/14]lldp compliance admin-status ?
  cdp  Non standard IEEE discovery protocol

[Comware5-GigabitEthernet1/0/14]lldp compliance admin-status cdp ?
  disable  Disable transmitting and receiving frames of the specified link
           layer discovery protocol
  txrx     Enable transmitting and receiving frames of the specified link layer
           discovery protocol

[Comware5-GigabitEthernet1/0/14]lldp compliance admin-status cdp txrx ?
  <cr>

[Comware5-GigabitEthernet1/0/14]lldp compliance admin-status cdp txrx



[Comware5]display lldp neighbor-information interface g1/0/14

CDP neighbor-information of port 14[GigabitEthernet1/0/14]:
  CDP neighbor index : 1
  Chassis ID         : SEP0013C42863A0
  Port ID            : Port 1
  Software version   : P00308000400
  Platform           : Cisco IP Phone 7960
  Duplex             : Full
```

Cisco

```
Cisco#show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled

Cisco#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  |          Output modifiers
  <cr>

Cisco#show cdp neighbors ?
  Async              Async interface
  Auto-Template      Auto-Template interface
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Filter             Filter interface
  Filtergroup        Filter Group interface
  GigabitEthernet    GigabitEthernet IEEE 802.3z
  GroupVI            Group Virtual interface
  Lex                Lex interface
  Port-channel       Ethernet Channel of interfaces
  Portgroup          Portgroup interface
  Pos-channel        POS Channel of interfaces
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing
  Vlan               Catalyst Vlans
  detail             Show detailed information
  fcpa               Fiber Channel
  |                  Output modifiers
  <cr>

Cisco#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SEP08000F1E31F6  Fas 0/3           136           H P                Port 1


Cisco#show cdp neighbors f0/3
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SEP08000F1E31F6  Fas 0/3           132           H P                Port 1


Cisco#show cdp neighbors f0/3  detail
-------------------------
Device ID: SEP08000F1E31F6
Entry address(es):
Platform:                          ,  Capabilities: Host Phone
Interface: FastEthernet0/3,  Port ID (outgoing port): Port 1
Holdtime : 124 sec

Version :
B2030202

advertisement version: 2
Duplex: full
Power drawn: 6.100 Watts
Management address(es):
```

Chapter 13 Port Information and Nomenclature

This chapter compares the commands used to collect information about ports.

For these commands, it is useful to know how each operating system references ports. ProVision ASIC chassis-based (modular) switches and stackable switches that have a module slot designate ports using the format "slot/port." For example, on the HP 8212zl switch, port 24 on the module in slot A is referred to as port A24. Stackable switches simply use the port number.

Comware 5 and Cisco switches (both chassis-based and stackable) designate ports using the format "interface_type slot/sub-slot/port" or "interface_type slot/port."

ProVision	Comware 5	Cisco
`ProVision# show interfaces brief`	`<Comware5>display brief interface`	`Cisco#show interfaces status`
`ProVision# show interfaces brief 9`	`<Comware5>display brief interface g1/0/9`	`Cisco#show interfaces f0/9 status`
`ProVision# show interfaces 9`	`<Comware5>display interface g1/0/9`	`Cisco#show interfaces f0/9`
`ProVision(config)# interface 9`	`[Comware5]interface g1/0/9`	`Cisco(config)#interface f0/9`
`ProVision(eth-9)# name link_to_core`	`[Comware5-GigabitEthernet1/0/9]description link_to_core`	`Cisco(config-if)#description link_to_core`
`ProVision(eth-9)# speed-duplex auto`	`[Comware5-GigabitEthernet1/0/9]duplex auto`	`Cisco(config-if)#duplex auto`
	`[Comware5-GigabitEthernet1/0/9]speed auto`	`Cisco(config-if)#speed auto`
`ProVision(eth-9)# disable`	`[Comware5-GigabitEthernet1/0/9]shutdown`	`Cisco(config-if)#shutdown`
`ProVision(eth-9)# enable`	`[Comware5-GigabitEthernet1/0/9]undo shutdown`	`Cisco(config-if)#no shutdown`

ProVision

```
ProVision# show interfaces ?
 brief                  Show the ports' operational parameters.
 config                 Show configuration information.
 custom                 Show the ports' parameters in customized order.
 display                Show summary of network traffic handled by the ports.
 [ethernet] PORT-LIST   Show summary of network traffic handled by the ports.
 port-utilization       Show the ports' bandwidth-utilization.
 <cr>

ProVision# show interfaces brief?
 [ethernet] PORT-LIST   Show summary of network traffic handled by the ports.
 <cr>

ProVision# show interfaces brief

 Status and Counters - Port Status

                    | Intrusion                           MDI   Flow  Bcast
  Port    Type      | Alert     Enabled Status Mode       Mode  Ctrl  Limit
  ------- --------- + --------- ------- ------ ---------- ----- ----- ------
  1       100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  2       100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  3       100/1000T | No        Yes     Down   1000FDx    MDIX  off   0
  4       100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  5       100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  6       100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  7       100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  8       100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  9       100/1000T | No        Yes     Up     100FDx     MDIX  off   0
  10      100/1000T | No        Yes     Up     1000FDx    MDIX  off   0
  11      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  12      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  13      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  14      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  15      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  16      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  17      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  18      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  19      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  20      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  21      100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  22-Trk1 100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  23-Trk1 100/1000T | No        Yes     Down   1000FDx    Auto  off   0
  24      100/1000T | No        Yes     Down   1000FDx    Auto  off   0


ProVision# show interfaces brief 9

 Status and Counters - Port Status

                    | Intrusion                           MDI   Flow  Bcast
  Port    Type      | Alert     Enabled Status Mode       Mode  Ctrl  Limit
  ------- --------- + --------- ------- ------ ---------- ----- ----- ------
  9       100/1000T | No        Yes     Up     100FDx     MDIX  off   0


ProVision# show interfaces 9

 Status and Counters - Port Counters for port 9

  Name  :
  MAC Address      : 001635-b376f7
  Link Status      : Up
  Totals (Since boot or last clear) :
   Bytes Rx        : 2,069,285,321      Bytes Tx        : 214,736,598
   Unicast Rx      : 1,922,572          Unicast Tx      : 1,283,973
   Bcast/Mcast Rx  : 588,985            Bcast/Mcast Tx  : 326,260
  Errors (Since boot or last clear) :
   FCS Rx          : 0                  Drops Tx        : 0
   Alignment Rx    : 0                  Collisions Tx   : 0
   Runts Rx        : 0                  Late Colln Tx   : 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  (bps) : 510824             Total Tx  (bps) : 517072
   Unicast Rx (Pkts/sec) : 18           Unicast Tx (Pkts/sec) : 20
   B/Mcast Rx (Pkts/sec) : 0            B/Mcast Tx (Pkts/sec) : 0
   Utilization Rx  : 00.51 %            Utilization Tx  : 00.51 %


ProVision(config)# interface ?
 loopback              Enter the loopback Configuration Level.
 [ethernet] PORT-LIST  Enter the Interface Configuration Level, or execute one
                       command for that level.
```

```
ProVision(config)# interface 9

ProVision(eth-9)#?
 arp-protect           Configure the port as trusted or untrusted.
 bandwidth-min         Enable/disable and configure guaranteed minimum
                       bandwidth settings for outgoing traffic on the port(s).
 broadcast-limit       Set a broadcast traffic percentage limit.
 dhcp-snooping         Configure the port as trusted or untrusted.
 disable               Disable port(s).
 enable                Enable port(s).
 flow-control          Enable/disable flow control on the port(s).
 gvrp                  Set the GVRP timers on the port (hundredths of a
                       second).
 ip                    Apply the specified access control list to inbound
                       packets on this INTERFACE list.
 ipv6                  Configure various IP parameters for the VLAN.
 lacp                  Define whether LACP is enabled on the port, and whether
                       it is in active or passive mode when enabled.
 link-keepalive        Configure UDLD on port(s).
 mdix-mode             Set port MDI/MDIX mode (default: auto).
 monitor               Define either the port is to be monitored or not.
 name                  Set/unset a name for the port(s).
 poe-allocate-by       Control manual power over ethernet allocation.
 poe-lldp-detect       Enabling this feature causes the port to allocate power
                       based on the link-partner's capabilities via LLDP.
 poe-value             Maximum PoE allocation specified with a value in watts.
 power-over-ethernet   Enable/Disable per-port power distribution.
 qos                   Set port-based priority.
 rate-limit            Enable/disable and configure rate-limiting for all
                       traffic (or for incoming ICMP traffic) on the port(s).
 service-policy        Apply the QoS/Mirror policy on the interface.
 speed-duplex          Define mode of operation for the port(s).
 unknown-vlans         Configure GVRP on the port(s).
 <cr>


ProVision(eth-9g)# name ?
 PORT-NAME-STR         Specify a port name up to 64 characters length.

ProVision(eth-9)# name link_to_core


ProVision(eth-9)# speed-duplex ?
 10-half               10 Mbps, half duplex.
 100-half              100 Mbps, half duplex.
 10-full               10 Mbps, full duplex.
 100-full              100 Mbps, full duplex.
 1000-full             1000 Mbps, full duplex.
 auto                  Use Auto Negotiation for speed and duplex mode.
 auto-10               10 Mbps, use Auto Negotiation for duplex mode.
 auto-100              100 Mbps, use Auto Negotiation for duplex mode.
 auto-1000             1000 Mbps, use Auto Negotiation for duplex mode.
 auto-10-100           10 or 100 Mbps, and half or full duplex, using Auto
                       Negotiation.

ProVision(eth-9)# speed-duplex auto

ProVision(eth-9)# disable

ProVision(eth-9)# 9 enable
```

Comware 5

```
<Comware5>display brief interface ?
  GigabitEthernet  GigabitEthernet interface
  NULL             NULL interface
  Vlan-interface   VLAN interface
  |                Matching output
  <cr>


<Comware5>display brief interface
The brief information of interface(s) under route mode:
Interface            Link      Protocol-link  Protocol type    Main IP
NULL0                UP        UP(spoofing)   NULL             --
Vlan1                UP        UP             ETHERNET         10.0.100.48

The brief information of interface(s) under bridge mode:
Interface            Link      Speed        Duplex   Link-type  PVID
GE1/0/1              DOWN      auto         auto     access     1
GE1/0/2              DOWN      auto         auto     access     1
GE1/0/3              UP        1G(a)        full(a)  access     1
GE1/0/4              DOWN      auto         auto     access     1
GE1/0/5              DOWN      auto         auto     access     1
GE1/0/6              DOWN      auto         auto     access     1
GE1/0/7              DOWN      auto         auto     access     1
GE1/0/8              DOWN      auto         auto     access     1
GE1/0/9              UP        100M(a)      full(a)  access     1
GE1/0/10             DOWN      auto         auto     access     1
GE1/0/11             DOWN      auto         auto     access     1
GE1/0/12             DOWN      auto         auto     access     1
GE1/0/13             DOWN      auto         auto     access     1
GE1/0/14             DOWN      auto         auto     access     1
GE1/0/15             DOWN      auto         auto     access     1
GE1/0/16             DOWN      auto         auto     access     1
GE1/0/17             DOWN      auto         auto     access     1
GE1/0/18             DOWN      auto         auto     access     1
GE1/0/19             DOWN      auto         auto     access     1
GE1/0/20             DOWN      auto         auto     access     1
GE1/0/21             DOWN      auto         auto     access     1
GE1/0/22             DOWN      auto         auto     access     1
GE1/0/23             DOWN      auto         auto     access     1
GE1/0/24             DOWN      auto         auto     access     1
GE1/0/25             ADM DOWN  auto         auto     access     1
GE1/0/26             ADM DOWN  auto         auto     access     1
GE1/0/27             ADM DOWN  auto         auto     access     1
GE1/0/28             ADM DOWN  auto         auto     access     1


<Comware5>display brief interface g1/0/9
The brief information of interface(s) under bridge mode:
Interface            Link      Speed        Duplex   Link-type  PVID
GE1/0/9              UP        100M(a)      full(a)  access     1


<Comware5>display interface g1/0/9
 GigabitEthernet1/0/9 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0022-57bc-d949
 Description: GigabitEthernet1/0/9 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 100Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 1
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Port priority: 0
 Peak value of input: 213 bytes/sec, at 2010-04-29 16:50:22
 Peak value of output: 236 bytes/sec, at 2010-04-29 16:30:25
 Last 300 seconds input:  2 packets/sec 213 bytes/sec   0%
 Last 300 seconds output:  0 packets/sec 18 bytes/sec   0%
 Input (total):  4311 packets, 1269761 bytes
         781 unicasts, 2272 broadcasts, 1258 multicasts
 Input (normal):  4311 packets, - bytes
         781 unicasts, 2272 broadcasts, 1258 multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 9731 packets, 1114808 bytes
         372 unicasts, 5974 broadcasts, 3385 multicasts, 0 pauses
 Output (normal): 9731 packets, - bytes
         372 unicasts, 5974 broadcasts, 3385 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier


[Comware5]interface ?
  Bridge-Aggregation  Bridge-Aggregation interface
  GigabitEthernet     GigabitEthernet interface
  LoopBack            LoopBack interface
  NULL                NULL interface
  Tunnel              Tunnel interface
  Vlan-interface      VLAN interface


[Comware5]interface g1/0/9


[Comware5-GigabitEthernet1/0/9]?
Gigabitethernet_l2 interface view commands:
  apply                  Apply Poe-profile
  arp                    Configure ARP for the interface
  bpdu-drop              Drop BPDU packets
  bpdu-tunnel            Specify BPDU tunnel function
  broadcast-suppression  Specify the broadcast storm control
  cfd                    Connectivity fault detection (IEEE 802.1ag)
  description            Describe the interface
  dhcp-snooping          DHCP Snooping
  display                Display current system information
  dldp                   Specify configuration information of DLDP
  dot1x                  Specify 802.1X configuration information
  duplex                 Status of duplex
  enable                 Enable function
  flow-control           Flow control command
  flow-interval          Set interval of interface statistic
  garp                   Generic Attribute Registration Protocol
  gvrp                   GARP VLAN Registration Protocol
  igmp-snooping          Configure IGMP snooping characteristic
  ip                     IP
  jumboframe             Jumboframe command
  lacp                   Configure LACP Protocol
  link-delay             Set the delay time of holding link-up and link-down
  lldp                   Link Layer Discovery Protocol(802.1ab)
  loopback               Specify loopback of current port
  loopback-detection     Detect if loopback exists
  mac-address            Configure MAC address
  mac-authentication     Specify Mac-auth configuration information
  mac-forced-forwarding  Specify MAC-forced forwarding configuration
                         information
  mac-vlan               Specify MAC VLAN
  mdi                    Specify mdi type
  mirroring-group        Specify mirroring-group
  mirroring-port         Specify mirroring port
  mld-snooping           Configure MLD snooping characteristic
  monitor-port           Specify monitor port
  mtracert               Trace route to multicast source
  multicast-suppression  Specify the multicast storm control
  ndp                    Neighbor discovery protocol
  ntdp                   Specify NTDP configuration information
  oam                    OAM protocol
  packet-filter          Specify packet filter
  ping                   Ping function
  poe                    Configure PoE port
  port                   Specify Port characteristics
  port-isolate           Specify port-isolate configuration information
  port-security          Specify port-security configuration information
  qinq                   Specify 802.1Q-in-Q VPN function
  qos                    Command of QoS(Quality of Service)
  quit                   Exit from current command view
  return                 Exit to User View
  rmon                   Specify RMON
  save                   Save current configuration
  sflow                  Specify sFlow configuration information
  shutdown               Shut down this interface
  smart-link             Configure smart link
  speed                  Specify speed of current port
  storm-constrain        Port storm-constrain
  stp                    Spanning tree protocol
  tracert                Trace route function
  undo                   Cancel current setting
  unicast-suppression    Specify the unicast storm control
  user-bind              Bind user address
  virtual-cable-test     display virtual cable test information
  vlan                   Set VLAN precedence
  voice                  Specify voice VLAN


[Comware5-GigabitEthernet1/0/9]description ?
  TEXT  Up to 80 characters for description of the interface


[Comware5-GigabitEthernet1/0/9]description link_to_core


[Comware5-GigabitEthernet1/0/9]duplex ?
  auto  Enable port's duplex negotiation automatically
  full  Full-duplex
  half  Half-duplex


[Comware5-GigabitEthernet1/0/9]duplex auto


[Comware5-GigabitEthernet1/0/9]speed ?
  10    Specify speed as 10 Mbps
  100   Specify speed as 100 Mbps
  1000  Specify speed as 1000 Mbps
  auto  Enable port's speed negotiation automatically


[Comware5-GigabitEthernet1/0/9]speed auto


[Comware5-GigabitEthernet1/0/9]shutdown


[Comware5-GigabitEthernet1/0/9]undo shutdown
```

Cisco

```
Cisco#show interfaces ?
  Async              Async interface
  Auto-Template      Auto-Template interface
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Filter             Filter interface
  Filtergroup        Filter Group interface
  GigabitEthernet    GigabitEthernet IEEE 802.3z
  GroupVI            Group Virtual interface
  Loopback           Loopback interface
  Null               Null interface
  Port-channel       Ethernet Channel of interfaces
  Portgroup          Portgroup interface
  Pos-channel        POS Channel of interfaces
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing
  Vlan               Catalyst Vlans
  accounting         Show interface accounting
  capabilities       Show interface capabilities information
  counters           Show interface counters
  crb                Show interface routing/bridging info
  dampening          Show interface dampening info
  debounce           Show interface debounce time info
  description        Show interface description
  etherchannel       Show interface etherchannel information
  fair-queue         Show interface Weighted Fair Queueing (WFQ) info
  fcpa               Fiber Channel
  flowcontrol        Show interface flowcontrol information
  irb                Show interface routing/bridging info
  mac-accounting     Show interface MAC accounting info
  mpls-exp           Show interface MPLS experimental accounting info
  mtu                Show interface mtu
  precedence         Show interface precedence accounting info
  private-vlan       Show interface private vlan information
  pruning            Show interface trunk VTP pruning information
  random-detect      Show interface Weighted Random Early Detection (WRED) info
  rate-limit         Show interface rate-limit info
  stats              Show interface packets & octets, in & out, by switching
                     path
  status             Show interface line status
  summary            Show interface summary
  switchport         Show interface switchport information
  transceiver        Show interface transceiver
  trunk              Show interface trunk information
  |                  Output modifiers
  <cr>

Cisco#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        notconnect   1            auto   auto 10/100BaseTX
Fa0/2                        notconnect   1            auto   auto 10/100BaseTX
Fa0/3                        connected    12         a-full  a-100 10/100BaseTX
Fa0/4                        notconnect   1            auto   auto 10/100BaseTX
Fa0/5                        notconnect   1            auto   auto 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
Fa0/8                        notconnect   1            auto   auto 10/100BaseTX
Fa0/9                        connected    100        a-full  a-100 10/100BaseTX
Fa0/10                       notconnect   100          auto   auto 10/100BaseTX
Fa0/11                       notconnect   1            auto   auto 10/100BaseTX
Fa0/12                       notconnect   1            auto   auto 10/100BaseTX
Fa0/13                       notconnect   1            auto   auto 10/100BaseTX
Fa0/14                       notconnect   1            auto   auto 10/100BaseTX
Fa0/15                       notconnect   1            auto   auto 10/100BaseTX
Fa0/16                       notconnect   1            auto   auto 10/100BaseTX
Fa0/17                       notconnect   1            auto   auto 10/100BaseTX
Fa0/18                       notconnect   1            auto   auto 10/100BaseTX
Fa0/19                       notconnect   1            auto   auto 10/100BaseTX
Fa0/20                       notconnect   1            auto   auto 10/100BaseTX
Fa0/21                       notconnect   1            auto   auto 10/100BaseTX

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/22                       notconnect   1            auto   auto 10/100BaseTX
Fa0/23                       notconnect   trunk        auto   auto 10/100BaseTX
Fa0/24                       notconnect   trunk        auto   auto 10/100BaseTX
Gi0/1                        notconnect   1            auto   auto Not Present
Gi0/2                        notconnect   1            auto   auto Not Present
Po24                         notconnect   trunk        auto   auto


Cisco#show interfaces f0/9 status
```

```
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/9                        connected    100        a-full  a-100 10/100BaseTX


Cisco#show interfaces f0/9
FastEthernet0/9 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001b.d4fe.f50b (bia 001b.d4fe.f50b)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     109639 packets input, 11171829 bytes, 0 no buffer
     Received 105767 broadcasts (103564 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 103564 multicast, 0 pause input
     0 input packets with dribble condition detected
     27722 packets output, 4061153 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out


Cisco(config)#interface ?
  Async              Async interface
  Auto-Template      Auto-Template interface
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Filter             Filter interface
  Filtergroup        Filter Group interface
  GigabitEthernet    GigabitEthernet IEEE 802.3z
  Group-Async        Async Group interface
  GroupVI            Group Virtual interface
  Lex                Lex interface
  Loopback           Loopback interface
  Null               Null interface
  Port-channel       Ethernet Channel of interfaces
  Portgroup          Portgroup interface
  Pos-channel        POS Channel of interfaces
  Tunnel             Tunnel interface
  Vif                PGM Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing
  Vlan               Catalyst Vlans
  fcpa               Fiber Channel
  range              interface range command


Cisco(config)#interface f0/9

Cisco(config-if)#?
```

```
Interface configuration commands:
  arp                     Set arp type (arpa, probe, snap) or timeout
  auto                    Configure Automation
  bandwidth               Set bandwidth informational parameter
  bgp-policy              Apply policy propogated by bgp community string
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  channel-group           Etherchannel/port bundling configuration
  channel-protocol        Select the channel protocol (LACP, PAgP)
  dampening               Enable event dampening
  default                 Set a command to its defaults
  delay                   Specify interface throughput delay
  description             Interface specific description
  down-when-looped        Force looped interface down
  duplex                  Configure duplex operation.
  eigrp                   EIGRP interface specific commands
  eou                     EAPoUDP Interface Configuration Commands
  exit                    Exit from interface configuration mode
  flowcontrol             Configure flow operation.
  help                    Description of the interactive help system
  hold-queue              Set hold queue depth
  ip                      Interface Internet Protocol config commands
  ipe                     Configure IPe information
  keepalive               Enable keepalive
  l2protocol-tunnel       Tunnel Layer2 protocols
  lacp                    LACP interface subcommands
  link                    Configure Link
  lldp                    LLDP interface subcommands
  load-interval           Specify interval for load calculation for an
                          interface
  location                Interface location information
  logging                 Configure logging for interface
  mac                     MAC interface commands
  macro                   Command macro
  max-reserved-bandwidth  Maximum Reservable Bandwidth on an Interface
  mdix                    Set Media Dependent Interface with Crossover
  mls                     mls interface commands
  mvr                     MVR per port configuration
  no                      Negate a command or set its defaults
  pagp                    PAgP interface subcommands
  power                   Power configuration
  priority-queue          Priority Queue
  queue-set               Choose a queue set for this queue
  rmon                    Configure Remote Monitoring on an interface
  service-policy          Configure QoS Service Policy
  shutdown                Shutdown the selected interface
  small-frame             Set rate limit parameters for small frame
  snmp                    Modify SNMP interface parameters
  source                  Get config from another source
  spanning-tree           Spanning Tree Subsystem
  speed                   Configure speed operation.
  srr-queue               Configure shaped round-robin transmit queues
  storm-control           storm configuration
  switchport              Set switching mode characteristics
  timeout                 Define timeout values for this interface
  transmit-interface      Assign a transmit interface to a receive-only
                          interface
  tx-ring-limit           Configure PA level transmit ring limit
  udld                    Configure UDLD enabled or disabled and ignore global
                          UDLD setting


Cisco(config-if)#description ?
  LINE  Up to 240 characters describing this interface
```

```
Cisco(config-if)#description link_to_core


Cisco(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation

Cisco(config-if)#duplex auto


Cisco(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration

Cisco(config-if)#speed auto


Cisco(config-if)#shutdown

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

Chapter 14 VLANs

This chapter compares the commands that are used to configure VLANs. Note that there are some terminology differences among the three operating systems. In Comware 5 and Cisco, an interface that is configured to support multiple VLANs is called a *trunk*. In ProVision, an interface that supports multiple VLANs is *tagged*. (In ProVision, a *trunk* is an aggregated interface.)

a) Creating and Naming VLANs

ProVision	Comware 5	Cisco
`ProVision(config)# vlan 220`	`[Comware5]vlan 220`	`Cisco(config)#vlan 220`
`ProVision(vlan-220)# name test`	`[Comware5-vlan220]name test`	`Cisco(config-vlan)#name test`
`ProVision# show vlans`	`[Comware5]display vlan all`	`Cisco#show vlan brief`

ProVision

```
ProVision(config)# vlan 220

ProVision(vlan-220)# name test


(also as compound statement)

ProVision(config)# vlan 230 name test2


ProVision# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 256
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :

  VLAN ID Name                 | Status     Voice Jumbo
  ------- -------------------- + ---------- ----- -----
  1       DEFAULT_VLAN         | Port-based No    No
  100     lab_core             | Port-based No    No
  220     test                 | Port-based No    No
  230     test2                | Port-based Yes   No
```

Comware 5

```
[Comware5]vlan 220

[Comware5-vlan220]name test


[Comware5]display vlan
 Total 3 VLAN exist(s).
 The following VLANs exist:
  1(default), 100, 220


[Comware5]display vlan all
 VLAN ID: 1
 VLAN Type: static
 Route Interface: configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
    GigabitEthernet1/0/4     GigabitEthernet1/0/5     GigabitEthernet1/0/6
    GigabitEthernet1/0/7     GigabitEthernet1/0/8     GigabitEthernet1/0/10
    GigabitEthernet1/0/11    GigabitEthernet1/0/12    GigabitEthernet1/0/13
    GigabitEthernet1/0/14    GigabitEthernet1/0/15    GigabitEthernet1/0/16
    GigabitEthernet1/0/17    GigabitEthernet1/0/18    GigabitEthernet1/0/19
    GigabitEthernet1/0/20    GigabitEthernet1/0/21    GigabitEthernet1/0/22
    GigabitEthernet1/0/23    GigabitEthernet1/0/24    GigabitEthernet1/0/25
    GigabitEthernet1/0/26    GigabitEthernet1/0/27    GigabitEthernet1/0/28

 VLAN ID: 100
 VLAN Type: static
 Route Interface: configured
 IP Address: 10.0.100.48
 Subnet Mask: 255.255.255.0
 Description: lab_core
 Name: VLAN 0100
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet1/0/9

 VLAN ID: 220
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0220
 Name: test
 Tagged   Ports: none
 Untagged Ports: none
```

Cisco

```
Cisco(config)#vlan 220

Cisco(config-vlan)#name test


Cisco#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
11   Data                             active
12   Voice                            active    Fa0/3
13   WLAN                             active
100  lab_core                         active    Fa0/9, Fa0/10
220  test                             active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

b) Assigning Ports or Interfaces to VLANs

ProVision	Comware 5	Cisco
(tag/untag)	(trunk/access)	(trunk/access)
`ProVision(config)# vlan 220`	`[Comware5]interface g1/0/6`	`Cisco(config)#interface f0/6`
`ProVision(vlan-220)# tagged 6-8,20`	`[Comware5-GigabitEthernet1/0/6]port link-type trunk`	`Cisco(config-if)#switchport trunk encapsulation dot1q`
	`[Comware5-GigabitEthernet1/0/6]port trunk permit vlan 220`	`Cisco(config-if)#switchport trunk allowed vlan 220`
		`Cisco(config-if)#switchport mode trunk`
		`Cisco(config-if)#switchport nonegotiate`
`ProVision(vlan-220)# untagged 1-3,5`	`[Comware5-vlan220]port g1/0/4`	`Cisco(config)#interface f0/5`
		`Cisco(config-if)#switchport`
		`Cisco(config-if)#switchport access vlan 220`
		`Cisco(config-if)#switchport mode access`
`ProVision# show vlans 220`	`[Comware5]display vlan 220`	`Cisco#show vlan id 220`
`ProVision# show vlans ports 6 detail`	`[Comware5]display interface g1/0/6`	`Cisco#show interfaces f0/6 switchport`
`ProVision# show vlans ports 5 detail`	`[Comware5]display interface g1/0/5`	`Cisco#show interfaces f0/5 switchport`

ProVision

```
ProVision(config)# vlan 220

ProVision(vlan-220)# tagged 6-8,20


(also as compound statement)

ProVision(config)# vlan 220 tagged 6-8, 20


ProVision(config)# vlan 220

ProVision(vlan-220)# untagged 1-3,5


(also as compound statement)

ProVision(config)# vlan 220 untagged 1-3,5


ProVision# show vlans 220

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  1                 Untagged Learn        Down
  2                 Untagged Learn        Down
  3                 Untagged Learn        Down
  5                 Untagged Learn        Up
  6                 Tagged   Learn        Down
  7                 Tagged   Learn        Down
  8                 Tagged   Learn        Down
  20                Tagged   Learn        Down


ProVision# show vlans ports 6 detail

 Status and Counters - VLAN Information - for ports 6

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  1       DEFAULT_VLAN         | Port-based No    No    Untagged
  220     test                 | Port-based No    No    Tagged


ProVision# show vlans ports 5 detail

 Status and Counters - VLAN Information - for ports 5

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  220     test                 | Port-based No    No    Untagged
```

Comware 5

```
[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]port link-type ?
  access   Access link-type
  hybrid   Hybrid VLAN link-type
  trunk    VLAN Trunk link-type

[Comware5-GigabitEthernet1/0/6]port link-type trunk

[Comware5-GigabitEthernet1/0/6]port trunk permit vlan 100 220


[Comware5-vlan220]port g1/0/4


[Comware5]display vlan 220
 VLAN ID: 220
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0220
 Name: test
 Tagged   Ports:
    GigabitEthernet1/0/6
 Untagged Ports:
    GigabitEthernet1/0/4

[Comware5]display vlan 100
 VLAN ID: 100
 VLAN Type: static
 Route Interface: configured
 IP Address: 10.0.100.48
 Subnet Mask: 255.255.255.0
 Description: lab_core
 Name: VLAN 0100
 Tagged   Ports:
    GigabitEthernet1/0/6
 Untagged Ports:
    GigabitEthernet1/0/5     GigabitEthernet1/0/9


[Comware5]display interface g1/0/6
 GigabitEthernet1/0/6 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0022-57bc-d946
 Description: GigabitEthernet1/0/6 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 100Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 1
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: trunk
  VLAN passing  : 1(default vlan), 100, 220
  VLAN permitted: 1(default vlan), 100, 220
  Trunk port encapsulation: IEEE 802.1q
 Port priority: 0
 Peak value of input: 501 bytes/sec, at 2010-04-29 22:08:59
 Peak value of output: 118 bytes/sec, at 2010-04-29 22:11:05
 Last 300 seconds input:  5 packets/sec 476 bytes/sec   0%
 Last 300 seconds output:  1 packets/sec 115 bytes/sec  0%
 Input (total):  4933 packets, 451572 bytes
         1863 unicasts, 1672 broadcasts, 1398 multicasts
 Input (normal):  4933 packets, - bytes
         1863 unicasts, 1672 broadcasts, 1398 multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 1071 packets, 107529 bytes
         1002 unicasts, 14 broadcasts, 55 multicasts, 0 pauses
 Output (normal): 1071 packets, - bytes
         1002 unicasts, 14 broadcasts, 55 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier


[Comware5]display interface g1/0/5
 GigabitEthernet1/0/5 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0022-57bc-d945
 Description: GigabitEthernet1/0/5 Interface
 Loopback is not set
 Media type is twisted pair
 Port hardware type is  1000_BASE_T
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 100
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 100
 Port priority: 0
 Peak value of input: 0 bytes/sec, at 2000-04-26 06:00:45
 Peak value of output: 0 bytes/sec, at 2000-04-26 06:00:45
 Last 300 seconds input:  0 packets/sec 0 bytes/sec     -%
 Last 300 seconds output:  0 packets/sec 0 bytes/sec    -%
 Input (total):  0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts
 Input (normal):  0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, - bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

Cisco

```
Cisco(config)#interface f0/6

Cisco(config-if)#switchport trunk encapsulation dot1q

Cisco(config-if)#switchport trunk allowed vlan 220

Cisco(config-if)#switchport mode trunk

Cisco(config-if)#switchport nonegotiate


Cisco(config)#interface f0/5

Cisco(config-if)#switchport

Cisco(config-if)#switchport access vlan 220

Cisco(config-if)#switchport mode access


Cisco#show vlan id 220
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
220  test                             active    Fa0/5

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
220  enet  100220     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------



Cisco#show interfaces f0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 220
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none



Cisco#show interfaces f0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 220 (test)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

c) Assigning an IP Address to a VLAN

ProVision	Comware 5	Cisco
`ProVision(config)# vlan 220`	`[Comware5]interface Vlan-interface 220`	`Cisco(config)#interface vlan 220`
`ProVision(vlan-220)# ip address 10.1.220.1/24`	`[Comware5-Vlan-interface220]ip address 10.1.220.3 255.255.255.0`	`Cisco(config-if)#ip address 10.1.220.2 255.255.255.0`
		`Cisco(config-if)#no shutdown`

ProVision

```
ProVision(config)# vlan 220

ProVision(vlan-220)# ip address 10.1.220.1/24

-or-

ProVision(vlan-220)# ip address 10.1.220.1 255.255.255.0
```

Comware 5

```
[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]

[Comware5-Vlan-interface220]ip address 10.1.220.3 255.255.255.0
```

Cisco

```
Cisco(config)#interface vlan 220

Cisco(config-if)#ip address 10.1.220.2 255.255.255.0


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

d) IP Helper to Relay / Forward DHCP Requests

ProVision	Comware 5	Cisco
ProVision(config)# vlan 220		Cisco(config)#interface vlan 220
ProVision(vlan-220)# ip helper-address 10.0.100.251		Cisco(config-if)#ip helper-address 10.0.100.251
	[Comware5]dhcp enable	
	[Comware5]dhcp relay server-group 1 ip 10.0.100.251	
	[Comware5]interface Vlan-interface 220	
	[Comware5-Vlan-interface220]dhcp select relay	
	[Comware5-Vlan-interface220]dhcp relay server-select 1	
	[Comware5]display dhcp relay all	
	[Comware5]display dhcp relay server-group 1	
ProVision(vlan-220)# show ip helper-address vlan 220	[Comware5]display dhcp relay all	Cisco#show ip interface vlan 220
	[Comware5]display dhcp relay server-group 1	

ProVision

```
ProVision(config)# vlan 220

ProVision(vlan-220)# ip helper-address 10.0.100.251


(also as compound statement)

ProVision(config)# vlan 220 ip address 10.0.100.251


ProVision(vlan-220)# show ip helper-address vlan 220

 IP Helper Addresses

  IP Helper Address
  -----------------
  10.0.100.251
```

Comware 5

```
[Comware5]dhcp ?
  enable   DHCP service enable
  relay    Specify DHCP(Dynamic Host Configuration Protocol) relay configuration
           information
  server   DHCP server

[Comware5]dhcp enable
 DHCP is enabled successfully!

 [Comware5]dhcp relay ?
  release         Release one IP address
  security       Specify DHCP(Dynamic Host Configuration Protocol) relay
                 security configuration information
  server-detect  Detect fake DHCP server
  server-group   Specify the server group number

[Comware5]dhcp relay server-group ?
  INTEGER<0-19>  The DHCP server group number

[Comware5]dhcp relay server-group 1 ?
  ip  Specify DHCP server IP address

[Comware5]dhcp relay server-group 1 ip ?
  X.X.X.X  The IP address of the DHCP server

[Comware5]dhcp relay server-group 1 ip 10.0.100.251 ?
  <cr>

[Comware5]dhcp relay server-group 1 ip 10.0.100.251


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]dhcp ?
  relay   Specify DHCP(Dynamic Host Configuration Protocol) relay configuration
          information
  select  Specify process mode of DHCP packet
  server  DHCP server

[Comware5-Vlan-interface220]dhcp select ?
  relay   Relay mode
  server  Server mode

[Comware5-Vlan-interface220]dhcp select relay ?
  <cr>

[Comware5-Vlan-interface220]dhcp select relay

[Comware5-Vlan-interface220]dhcp relay ?
  address-check  Check address
  information    Specify option 82 service
  server-select  Choose DHCP server group

[Comware5-Vlan-interface220]dhcp relay server-select ?
  INTEGER<0-19>  The DHCP server group number

[Comware5-Vlan-interface220]dhcp relay server-select 1 ?
  <cr>

[Comware5-Vlan-interface220]dhcp relay server-select 1

[Comware5]display dhcp relay all
    Interface name                                    Server-group
    Vlan-interface220                                      1

[Comware5]display dhcp relay server-group 1
    No.            Group IP
    1              10.0.100.251
```

Cisco

```
Cisco(config)#interface vlan 220

Cisco(config-if)#ip helper-address 10.0.100.251



Cisco#show ip interface vlan 220
Vlan220 is up, line protocol is up
  Internet address is 10.1.220.2/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is 10.0.100.251
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.2 224.0.0.22 224.0.0.13
      224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Output features: Check hwidb
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

e) GVRP

ProVision	Comware 5	Cisco
`ProVision(config)# gvrp`	`[Comware5]gvrp`	***not an available feature***
	`[Comware5-GigabitEthernet1/0/9]gvrp`	

ProVision
`ProVision(config)# gvrp`
Comware 5

`[Comware5]gvrp`
`[Comware5-GigabitEthernet1/0/9]gvrp`

Cisco
Not an available feature

Chapter 15 VoIP

This chapter compares the commands used to configure VLANs, interfaces, or ports for VoIP operations.

ProVision	Comware 5	Cisco
	[Comware5]voice vlan mac-address 0008-5d00-0000 mask ffff-ff00-0000 description aastra	
ProVision(config)# vlan 230	[Comware5]vlan 230	
ProVision(vlan-230)# voice	[Comware5-vlan230]name voice	
ProVision(config)# vlan 220		
ProVision(vlan-220)# untagged 18		
	[Comware5]interface g1/0/18	Cisco(config)#interface f0/18
	[Comware5-GigabitEthernet1/0/18]port link-type access [Comware5-GigabitEthernet1/0/18]port link-type hybrid	Cisco(config-if)#switchport
	[Comware5-GigabitEthernet1/0/18]port hybrid vlan 220 untagged [Comware5-GigabitEthernet1/0/18]port hybrid pvid vlan 220	Cisco(config-if)#switchport access vlan 220
		Cisco(config-if)#switchport mode access
ProVision(vlan-230)# tagged 18	[Comware5-GigabitEthernet1/0/18]voice vlan 230 enable	Cisco(config-if)#switchport voice vlan 230
	[Comware5-GigabitEthernet1/0/18]poe enable	
ProVision# show vlans 230	<Comware5>display vlan 230	
ProVision# show vlan port 18 detail	<Comware5>display interface g1/0/18	Cisco#show interfaces f0/18 switchport
	<Comware5>display voice vlan state	
	<Comware5>display voice vlan oui	

ProVision

```
ProVision(config)# vlan 230

ProVision(vlan-230)# voice


ProVision(config)# vlan 220

ProVision(vlan-220)# untagged 18

ProVision(vlan-230)# tagged 18


ProVision# show vlans 230
```

```
 Status and Counters - VLAN Information - VLAN 230

  VLAN ID : 230
  Name : test2
  Status : Port-based
  Voice : Yes
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  18               Tagged   Learn        Down


ProVision# show vlan port 18 detail

 Status and Counters - VLAN Information - for ports 18

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  220     test                 | Port-based No    No    Untagged
  230     test2                | Port-based Yes   No    Tagged
```

Comware 5

```
[Comware5]voice vlan mac-address 0008-5d00-0000 mask ffff-ff00-0000 description aastra

[Comware5]vlan 230

[Comware5-vlan230]name voice


[Comware5]interface g1/0/18

[Comware5-GigabitEthernet1/0/18]port link-type access

[Comware5-GigabitEthernet1/0/18]port link-type hybrid

[Comware5-GigabitEthernet1/0/18]port hybrid vlan 220 untagged

[Comware5-GigabitEthernet1/0/18]port hybrid pvid vlan 220

[Comware5-GigabitEthernet1/0/18]voice vlan 230 enable

[Comware5-GigabitEthernet1/0/18]poe enable


<Comware5>display voice vlan state
 Maximum of Voice VLANs: 8
 Current Voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled port and its mode:
 PORT                        VLAN        MODE
 -----------------------------------------------
 GigabitEthernet1/0/18       230         AUTO


<Comware5>display vlan 230
```

```
 VLAN ID: 230
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0230
 Name: voice
 Tagged   Ports:
    GigabitEthernet1/0/18
 Untagged Ports: none


<Comware5>display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0008-5d00-0000  ffff-ff00-0000  aastra
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone


<Comware5>display interface g1/0/18
 GigabitEthernet1/0/18 current state: UP
...
PVID: 220
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: hybrid
  Tagged   VLAN ID : 230
  Untagged VLAN ID : 220
 Port priority: 0
...
```

Cisco

```
Cisco(config)#interface f0/18

Cisco(config-if)#switchport

Cisco(config-if)#switchport access vlan 220

Cisco(config-if)#switchport mode access

Cisco(config-if)#switchport voice vlan 230


Cisco#show interfaces f0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 220 (Data)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 230 (Voice)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Chapter 16 PoE

This chapter compares the commands used to configure Power over Ethernet (PoE). On ProVision and Cisco switches, PoE is enabled by default. On Comware 5, PoE is disabled by default.

ProVision	Comware 5	Cisco
(PoE enabled by default)	(PoE disabled by default)	(PoE enabled by default)
	[Comware5-GigabitEthernet1/0/18]poe enable	
ProVision# show power-over-ethernet	[Comware5]display poe device	
ProVision# show power-over-ethernet brief	[Comware5]display poe interface	Cisco#show power inline
ProVision# show power-over-ethernet 5	[Comware5]display poe interface g1/0/18	Cisco#show power inline f0/3
ProVision(config)# interface 5	[Comware5]interface g1/0/18	Cisco(config)#interface f0/3
ProVision(eth-5)# no power-over-ethernet	[Comware5-GigabitEthernet1/0/18]undo poe enable	Cisco(config-if)#power inline never
ProVision(eth-5)# power-over-ethernet	[Comware5-GigabitEthernet1/0/18]poe enable	Cisco(config-if)#power inline auto

ProVision

```
ProVision# show power-over-ethernet

 Status and Counters - System Power Status

  Pre-standard Detect    : On


 Chassis power-over-ethernet:

  Total Available Power  :  398 W
  Total Failover Power   :    0 W
  Total Redundancy Power :    0 W
  Total used Power       :    3 W +/- 6W
  Total Remaining Power  :  395 W

 Internal Power
        1   398W/POE  /Connected.
 External Power
        EPS1   /Not Connected.


ProVision# show power-over-ethernet brief

 Status and Counters - Port Power Status



  Available: 398 W  Used: 4 W  Remaining: 394 W

  Module 1-24 Power
  Available: 398 W  Used: 4 W  Remaining: 394 W

  PoE    | Power   Power     Alloc Alloc  Actual Configured  Detection   Power
  Port   | Enable  Priority  By    Power  Power  Type        Status      Class
  ------ + ------- --------- ----- ------ ------ ----------- ----------- ------
  1      | Yes     low       usage 17 W   0.0 W              Searching   0
  2      | Yes     low       usage 17 W   0.0 W              Searching   0
  3      | Yes     low       usage 17 W   0.0 W              Searching   0
  4      | Yes     low       usage 17 W   0.0 W              Searching   0
  5      | Yes     low       usage 17 W   3.4 W              Delivering  2
  6      | Yes     low       usage 17 W   0.0 W              Searching   0
  7      | Yes     low       usage 17 W   0.0 W              Searching   0


ProVision# show power-over-ethernet 5

 Status and Counters - Port Power Status for port 5

  Power Enable      : Yes
                                        LLDP Detect       : disabled
  Priority          : low               Configured Type   :
  AllocateBy        : usage             Value             : 17 W
  Detection  Status : Delivering        Power Class       : 2

  Over Current Cnt  : 0                 MPS Absent Cnt    : 0
  Power Denied Cnt  : 0                 Short Cnt         : 0

  Voltage           : 51.6 V            Current           : 54 mA
  Power             : 4.4 W


ProVision(config)# interface 5

ProVision(eth-5)# no power-over-ethernet


ProVision# show power-over-ethernet 5

 Status and Counters - Port Power Status for port 5

  Power Enable      : No


ProVision(config)# interface 5


ProVision(eth-5)# power-over-ethernet


ProVision# show power-over-ethernet 5

 Status and Counters - Port Power Status for port 5

  Power Enable      : Yes
                                        LLDP Detect       : disabled
  Priority          : low               Configured Type   :
  AllocateBy        : usage             Value             : 17 W
  Detection  Status : Delivering        Power Class       : 2

  Over Current Cnt  : 0                 MPS Absent Cnt    : 0
  Power Denied Cnt  : 0                 Short Cnt         : 0

  Voltage           : 51.6 V            Current           : 52 mA
  Power             : 2.7 W
```

Comware 5

```
Note - PoE disabled by default


[Comware5-GigabitEthernet1/0/18]poe ?
  enable          Port power enable
  max-power       Port maximum power
  mode            Port power mode
  pd-description  PD description
  priority        Port power priority

[Comware5-GigabitEthernet1/0/18]poe ena
[Comware5-GigabitEthernet1/0/18]poe enable ?
  <cr>

[Comware5-GigabitEthernet1/0/18]poe enable


[Comware5]display poe device
 PSE ID  SlotNo SubSNo PortNum  MaxPower(W)  State  Model
 1       1      0      24       370          on     LSP2LTSUC


[Comware5]display poe interface
 Interface  Enable   Priority  CurPower  Operating   IEEE  Detection
                               (W)       Status      Class Status

 GE1/0/12   disable  low       0.0       off         0     disabled
 GE1/0/13   disable  low       0.0       off         0     disabled
 GE1/0/14   enable   low       0.0       off         0     searching
 GE1/0/15   disable  low       0.0       off         0     disabled
 GE1/0/16   disable  low       0.0       off         0     disabled
 GE1/0/17   disable  low       0.0       off         0     disabled
 GE1/0/18   enable   low       2.3       on          0     delivering-power
 GE1/0/19   disable  low       0.0       off         0     disabled
  ---  1 port(s) on,    2.3 (W) consumed,   0.0 (W) remaining ---


[Comware5]display poe interface g1/0/18
 Port Power Enabled                  : enable
 Port Power Priority                 : low
 Port Operating Status               : on
 Port IEEE Class                     : 0
 Port Detection Status               : delivering-power
 Port Power Mode                     : signal
 Port Current Power                  : 2200     mW
 Port Average Power                  : 2225     mW
 Port Peak Power                     : 2300     mW
 Port Max Power                      : 15400    mW
 Port Current                        : 44       mA
 Port Voltage                        : 50.0     V
 Port PD Description                 :


[Comware5]interface g1/0/18
```

```
[Comware5-GigabitEthernet1/0/18]undo poe enable


[Comware5-GigabitEthernet1/0/18]display poe interface g1/0/18
 Port Power Enabled                 : disable
 Port Power Priority                : low
 Port Operating Status              : off
 Port IEEE Class                    : 0
 Port Detection Status              : disabled
 Port Power Mode                    : signal
 Port Current Power                 : 0         mW
 Port Average Power                 : 0         mW
 Port Peak Power                    : 0         mW
 Port Max Power                     : 15400     mW
 Port Current                       : 0         mA
 Port Voltage                       : 50.0      V
 Port PD Description                :


[Comware5-GigabitEthernet1/0/18]poe enable


[Comware5-GigabitEthernet1/0/18]display poe interface g1/0/18
 Port Power Enabled                 : enable
 Port Power Priority                : low
 Port Operating Status              : on
 Port IEEE Class                    : 0
 Port Detection Status              : delivering-power
 Port Power Mode                    : signal
 Port Current Power                 : 2200      mW
 Port Average Power                 : 2178      mW
 Port Peak Power                    : 2300      mW
 Port Max Power                     : 15400     mW
 Port Current                       : 43        mA
 Port Voltage                       : 50.1      V
 Port PD Description                :
```

Cisco

```
Cisco#show power inline
Available:370.0(w)  Used:6.1(w)  Remaining:363.9(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   off        0.0     n/a                 n/a   15.4
Fa0/2     auto   off        0.0     n/a                 n/a   15.4
Fa0/3     auto   on         6.1                         2     15.4
Fa0/4     auto   off        0.0     n/a                 n/a   15.4
Fa0/5     auto   off        0.0     n/a                 n/a   15.4
Fa0/6     auto   off        0.0     n/a                 n/a   15.4
Fa0/7     auto   off        0.0     n/a                 n/a   15.4
Fa0/8     auto   off        0.0     n/a                 n/a   15.4


Cisco#show power inline f0/3
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
```

```
Fa0/3     auto   on         6.1                         2     15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Fa0/3                 15.4                 15.4


Cisco(config)#interface f0/3

Cisco(config-if)#power inline never


Cisco#show power inline f0/3
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/3     off    off        0.0     n/a                 n/a   15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Fa0/3                 15.4                 15.4


Cisco(config)#interface f0/3

Cisco(config-if)#power inline auto


Cisco#show power inline f0/3
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/3     auto   on         6.1                         2     15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Fa0/3                 15.4                 15.4
```

Chapter 17 Link Aggregation

This chapter compares the commands used to aggregate interfaces. Note that for aggregated interfaces, there are some terminology differences among the operating systems. In ProVision, aggregated links are called *trunks*. In Comware 5 , the term is *bridge aggregation*; in Cisco it is *EtherChannel*. (In Cisco and Comware 5, *trunk* refers to an interface that is configured to support VLANs.)

a) Link Aggregation Control Protocol (LACP)

ProVision	Comware 5	Cisco
ProVision(config)# trunk 22-23 trk1 lacp	[Comware5]interface Bridge-Aggregation 1	Cisco(config)#interface port-channel 1
ProVision(config)# vlan 220 tagged trk1	[Comware5-Bridge-Aggregation1]description LACP_link_to_3560	Cisco(config-if)#switchport trunk encapsulation dot1q
	[Comware5-Bridge-Aggregation1]link-aggregation mode dynamic	Cisco(config-if)#switchport trunk allowed vlan 1,11,12,100
	[Comware5]interface g1/0/22	Cisco(config-if)#switchport mode trunk
	[Comware5-GigabitEthernet1/0/22]port link-aggregation group 1	Cisco(config-if)#switchport nonegotiate
	[Comware5-GigabitEthernet1/0/22]interface g1/0/23	Cisco(config)#interface range f0/22 - 23
	[Comware5-GigabitEthernet1/0/23]port link-aggregation group 1	Cisco(config-if-range)#switchport trunk encapsulation dot1q
	[Comware5]interface Bridge-Aggregation 1	Cisco(config-if-range)#switchport trunk allowed vlan 1,11,12,100
	[Comware5-Bridge-Aggregation1]port link-type trunk	Cisco(config-if-range)#switchport mode trunk
	[Comware5-Bridge-Aggregation1]port trunk permit vlan 100 220	Cisco(config-if-range)#switchport nonegotiate
		Cisco(config-if-range)#channel-group 1 mode active
ProVision# show trunks	[Comware5]display link-aggregation summary	Cisco#show lacp 1 internal
	[Comware5]display link-aggregation verbose	
ProVision# show lacp	[Comware5]display link-aggregation member-port	Cisco#show interfaces etherchannel
ProVision# show vlans 220	[Comware5]display vlan 220	

ProVision

```
ProVision(config)# trunk 22-23 trk1 lacp


ProVision(config)# vlan 220 tagged trk1


ProVision# show trunks

 Load Balancing
```

```
  Port | Name                             Type      | Group  Type
  ---- + -------------------------------- --------- + ------ --------
  22   |                                  100/1000T | Trk1   LACP
  23   |                                  100/1000T | Trk1   LACP


ProVision# show lacp

                           LACP

   PORT   LACP      TRUNK     PORT      LACP      LACP
   NUMB   ENABLED   GROUP     STATUS    PARTNER   STATUS
   ----   -------   --------  -------   -------   -------
   22     Active    Trk1      Down      No        Success
   23     Active    Trk1      Down      No        Success


ProVision# show vlans 220

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  3                Untagged Learn        Down
  5                Untagged Learn        Up
  6                Tagged   Learn        Down
  Trk1             Tagged   Learn        Down


ProVision# show vlans ports trk1 detail

 Status and Counters - VLAN Information - for ports Trk1

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  1       DEFAULT_VLAN         | Port-based No    No    Untagged
  220     test                 | Port-based No    No    Tagged
```

Comware 5

```
[Comware5]interface Bridge-Aggregation 1

[Comware5-Bridge-Aggregation1]description LACP_link_to_3560

[Comware5-Bridge-Aggregation1]link-aggregation mode dynamic

[Comware5]interface g1/0/22

[Comware5-GigabitEthernet1/0/22]port link-aggregation group 1

[Comware5-GigabitEthernet1/0/22]interface g1/0/23

[Comware5-GigabitEthernet1/0/23]port link-aggregation group 1

[Comware5]interface Bridge-Aggregation 1

[Comware5-Bridge-Aggregation1]port link-type trunk
```

```
[Comware5-Bridge-Aggregation1]port trunk permit vlan 100 220


[Comware5]dis link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 0022-57bc-d900

AGG         AGG       Partner ID               Select Unselect   Share
Interface   Mode                               Ports  Ports      Type
-------------------------------------------------------------------------------
BAGG1       D         0x8000, 001b-d4fe-f500   2      0          Shar


[Comware5]dis link-aggregation verbose

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 0022-57bc-d900
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/22         S       32768    1         {ACDEF}
  GE1/0/23         S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/22         24      32768    1         0x8000, 001b-d4fe-f500 {ACDEF}
  GE1/0/23         25      32768    1         0x8000, 001b-d4fe-f500 {ACDEF}


[Comware5]dis link-aggregation member-port

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/22:
Aggregation Interface: Bridge-Aggregation1
Local:
    Port Number: 22
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 001b-d4fe-f500
    Port Number: 24
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 12 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 12 packet(s)

GigabitEthernet1/0/23:
Aggregation Interface: Bridge-Aggregation1
Local:
    Port Number: 23
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 001b-d4fe-f500
    Port Number: 25
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 12 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 11 packet(s)


[Comware5]display vlan 220
 VLAN ID: 220
 VLAN Type: static
 Route Interface: configured
 IP Address: 10.1.220.3
 Subnet Mask: 255.255.255.0
 Description: VLAN 0220
 Name: test
 Tagged   Ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/6     GigabitEthernet1/0/22    GigabitEthernet1/0/23
 Untagged Ports:
    GigabitEthernet1/0/4     GigabitEthernet1/0/18
```

Cisco

```
Cisco(config)#interface port-channel 1

Cisco(config-if)#switchport trunk encapsulation dot1q

Cisco(config-if)#switchport trunk allowed vlan 1,11,12,100

Cisco(config-if)#switchport mode trunk

Cisco(config-if)#switchport nonegotiate


Cisco(config)#interface range f0/22 - 23

Cisco(config-if-range)#switchport trunk encapsulation dot1q

Cisco(config-if-range)#switchport trunk allowed vlan 1,11,12,100

Cisco(config-if-range)#switchport mode trunk
Cisco(config-if-range)#switchport nonegotiate

Cisco(config-if-range)#channel-group 1 mode active


Cisco#show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa0/22    SA      down      32768         0x1       0x0     0x18        0x45
Fa0/23    SA      down      32768         0x1       0x0     0x19        0x45


Cisco#show interfaces etherchannel
----
FastEthernet0/22:
Port state    = Down Not-in-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = null        GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa0/22    SA      down      32768         0x1       0x0     0x18        0x45

Age of the port in the current state: 2d:00h:44m:39s

----
FastEthernet0/23:
Port state    = Down Not-in-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = null        GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa0/23    SA      down      32768         0x1       0x0     0x19        0x45

Age of the port in the current state: 2d:00h:44m:39s

----
Port-channel1:Port-channel1   (Primary aggregator)

Age of the Port-channel   = 0d:00h:34m:26s
Logical slot/port   = 2/1          Number of ports = 0
HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   LACP
Port security       = Disabled
```

b) Trunk

ProVision	Comware 5	Cisco
ProVision(config)# trunk 22-23 trk1 trunk	[Comware5]interface Bridge-Aggregation 1	Cisco(config)#interface port-channel 1
ProVision(config)# vlan 220 tagged trk1	[Comware5-Bridge-Aggregation1]description Static-LACP_link_to_3560	Cisco(config-if)#switchport trunk encapsulation dot1q
	[Comware5]interface g1/0/22	Cisco(config-if)#switchport trunk allowed vlan 1,11,12,100
	[Comware5-GigabitEthernet1/0/22]port link-aggregation group 1	Cisco(config-if)#switchport mode trunk
	[Comware5-GigabitEthernet1/0/22]interface g1/0/23	Cisco(config-if)#switchport nonegotiate
	[Comware5-GigabitEthernet1/0/23]port link-aggregation group 1	Cisco(config)#interface range f0/22 - 23
	[Comware5]interface Bridge-Aggregation 1	Cisco(config-if-range)#switchport trunk encapsulation dot1q
	[Comware5-Bridge-Aggregation1]port link-type trunk	Cisco(config-if-range)#switchport trunk allowed vlan 1,11,12,100
	[Comware5-Bridge-Aggregation1]port trunk permit vlan 100 220	Cisco(config-if-range)#switchport mode trunk
		Cisco(config-if-range)#switchport nonegotiate
		Cisco(config-if-range)#channel-group 1 mode on
ProVision# show trunks	[Comware5]display link-aggregation summary	Cisco#show etherchannel 1 summary
	[Comware5]display link-aggregation verbose	
	[Comware5]display link-aggregation member-port	
ProVision# show vlans 220	[Comware5]display vlan 220	
ProVision# show vlans ports trk1 detail		

ProVision

```
ProVision(config)# trunk 22-23 trk1 trunk


ProVision(config)# vlan 220 tagged trk1


ProVision# show trunks

 Load Balancing

  Port | Name                             Type      | Group  Type
  ---- + -------------------------------- --------- + ------ --------
  22   |                                  100/1000T | Trk1   Trunk
  23   |                                  100/1000T | Trk1   Trunk
```

```
ProVision# show vlans 220

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  3                Untagged Learn        Down
  5                Untagged Learn        Up
  6                Tagged   Learn        Down
  Trk1             Tagged   Learn        Down


ProVision# show vlans ports trk1 detail

 Status and Counters - VLAN Information - for ports Trk1

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  1       DEFAULT_VLAN         | Port-based No    No    Untagged
  220     test                 | Port-based No    No    Tagged
```

Comware 5

```
[Comware5]interface Bridge-Aggregation 1

[Comware5-Bridge-Aggregation1]description Static-LACP_link_to_3560

[Comware5]interface g1/0/22

[Comware5-GigabitEthernet1/0/22]port link-aggregation group 1

[Comware5-GigabitEthernet1/0/22]interface g1/0/23

[Comware5-GigabitEthernet1/0/23]port link-aggregation group 1

[Comware5]interface Bridge-Aggregation 1

[Comware5-Bridge-Aggregation1]port link-type trunk

[Comware5-Bridge-Aggregation1]port trunk permit vlan 100 220


[Comware5]display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 0022-57bc-d900

AGG         AGG       Partner ID               Select Unselect   Share
Interface   Mode                               Ports  Ports      Type
--------------------------------------------------------------------------------
BAGG1       S         none                     2      0          Shar
```

```
[Comware5]display link-aggregation verbose

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status    Oper-Key
--------------------------------------------------------------------------------
  GE1/0/22         S         1
  GE1/0/23         S         1


[Comware5]display link-aggregation member-port

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/22:
Aggregation Interface: Bridge-Aggregation1
Port Number: 22
Oper-Key: 1

GigabitEthernet1/0/23:
Aggregation Interface: Bridge-Aggregation1
Port Number: 23
Oper-Key: 1


[Comware5]display vlan 220
 VLAN ID: 220
 VLAN Type: static
 Route Interface: configured
 IP Address: 10.1.220.3
 Subnet Mask: 255.255.255.0
 Description: VLAN 0220
 Name: test
 Tagged   Ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/6     GigabitEthernet1/0/22     GigabitEthernet1/0/23
 Untagged Ports:
    GigabitEthernet1/0/4     GigabitEthernet1/0/18
```

Cisco

```
Cisco(config)#interface port-channel 1

Cisco(config-if)#switchport trunk encapsulation dot1q

Cisco(config-if)#switchport trunk allowed vlan 1,11,12,100

Cisco(config-if)#switchport mode trunk

Cisco(config-if)#switchport nonegotiate


Cisco(config)#interface range f0/22 - 23

Cisco(config-if-range)#switchport trunk encapsulation dot1q

Cisco(config-if-range)#switchport trunk allowed vlan 1,11,12,100

Cisco(config-if-range)#switchport mode trunk

Cisco(config-if-range)#switchport nonegotiate

Cisco(config-if-range)#channel-group 1 mode on


Cisco#show etherchannel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)          -        Fa0/22(D)   Fa0/23(D)
```

Chapter 18 RSTP

This chapter compares the commands used to configure Rapid Spanning Tree Protocol (RSTP). The three operating systems implement RSTP differently:

- ProVision supports RSTP, but Multiple STP (MSTP) is the default STP version. MSTP is *not* enabled by default. When MSTP is enabled, all ports are auto-edge-ports by default.
- Comware 5 supports RSTP, but MSTP is the default STP version. By default, MSTP is *enabled*, and all ports are non-edge ports.
- Cisco does not support RSTP as an STP option.

ProVision	Comware 5	Cisco
`ProVision(config)# spanning-tree`	`[Comware5]stp enable`	***(Not an available feature)***
`ProVision(config)# spanning-tree force-version rstp-operation`	`[Comware5]stp mode rstp`	
`ProVision(config)# spanning-tree priority 9`	`[Comware5]stp priority 0`	
`ProVision(config)# spanning-tree 7 admin-edge-port`	`[Comware5-GigabitEthernet1/0/7]stp edged-port enable`	
`ProVision(config)# spanning-tree 7 path-cost 10000`	`[Comware5-GigabitEthernet1/0/7]stp cost 10000`	
`ProVision(config)# spanning-tree 7 priority 6`	`[Comware5-GigabitEthernet1/0/7]stp port priority 96`	
`ProVision# show spanning-tree`	`[Comware5]display stp`	
	`[Comware5]dis stp brief`	

ProVision

```
ProVision(config)# spanning-tree

ProVision(config)# spanning-tree force-version rstp-operation

ProVision(config)# spanning-tree priority 9
   (note - multiplier is 4096)

ProVision(config)# spanning-tree 7 admin-edge-port

ProVision(config)# spanning-tree 7 path-cost 10000

ProVision(config)# spanning-tree 7 priority 6
   (note - multiplier is 16)


ProVision# show spanning-tree

 Multiple Spanning Tree (MST) Information

  STP Enabled   : Yes
  Force Version : RSTP-operation
  IST Mapped VLANs : 2-10,14-219,221-4094
  Switch MAC Address : 001635-b376c0
  Switch Priority    : 36864
  Max Age  : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count  : 13
  Time Since Last Change : 15 mins

  CST Root MAC Address : 002257-bcd900
  CST Root Priority    : 0
  CST Root Path Cost   : 20000
  CST Root Port        : Trk1

  IST Regional Root MAC Address : 001635-b376c0
  IST Regional Root Priority    : 36864
  IST Regional Root Path Cost   : 0
  IST Remaining Hops            : 20

  Root Guard Ports     :
  TCN Guard Ports      :
  BPDU Protected Ports :
  BPDU Filtered Ports  :
  PVST Protected Ports :
  PVST Filtered Ports  :

                   |           Prio             | Designated    Hello
  Port   Type      | Cost      rity  State      | Bridge        Time  PtP Edge
  ------ --------- + --------- ----- ---------- + ------------- ----- --- ----
  1      100/1000T | Auto      128   Disabled   |
  2      100/1000T | Auto      128   Disabled   |
  3      100/1000T | Auto      128   Disabled   |
  4      100/1000T | Auto      128   Disabled   |
  5      100/1000T | Auto      128   Disabled   |
  6      100/1000T | 200000    128   Forwarding | 001635-b376c0 2     Yes No
  7      100/1000T | 10000     96    Disabled   |
  8      100/1000T | Auto      128   Disabled   |
  9      100/1000T | Auto      128   Disabled   |
  10     100/1000T | 20000     128   Forwarding | 001635-b376c0 2     Yes Yes
  11     100/1000T | Auto      128   Disabled   |
  12     100/1000T | 200000    128   Forwarding | 001635-b376c0 2     Yes Yes
  13     100/1000T | Auto      128   Disabled   |
  14     100/1000T | Auto      128   Disabled   |
  15     100/1000T | Auto      128   Disabled   |
  16     100/1000T | Auto      128   Disabled   |
  17     100/1000T | Auto      128   Disabled   |
  18     100/1000T | Auto      128   Disabled   |
  19     100/1000T | Auto      128   Disabled   |
  20     100/1000T | Auto      128   Disabled   |
  21     100/1000T | Auto      128   Disabled   |
  24     100/1000T | Auto      128   Disabled   |
  Trk1             | 20000     64    Forwarding | 002257-bcd900 2     Yes No
```

Comware 5

```
[Comware5]stp enable

[Comware5]stp mode rstp
```

```
[Comware5]stp priority 0
   (note – in steps of 4096)


[Comware5-GigabitEthernet1/0/7]stp edged-port enable

[Comware5-GigabitEthernet1/0/7]stp cost 10000

[Comware5-GigabitEthernet1/0/7]stp port priority 96
   (note – in steps of 16)



[Comware5]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :0.0022-57bc-d900
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0.0022-57bc-d900 / 0
CIST RegRoot/IRPC   :0.0022-57bc-d900 / 0
CIST RootPortId     :0.0
BPDU-Protection     :disabled
Bridge Config-
Digest-Snooping     :disabled
TC or TCN received  :148
Time since last TC  :0 days 0h:4m:35s

----[Port505(Bridge-Aggregation1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Designated Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=10000
 Desg. Bridge/Port   :0.0022-57bc-d900 / 128.505
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=802.1s
 Port Config-
 Digest-Snooping     :disabled
 Rapid transition    :true
 Num of Vlans Mapped :3
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 20
 BPDU Sent           :146
          TCN: 0, Config: 0, RST: 141, MST: 5
 BPDU Received       :181
          TCN: 0, Config: 0, RST: 181, MST: 0

----[Port1(GigabitEthernet1/0/1)][DOWN]----


[Comware5]dis stp brief
 MSTID      Port                         Role  STP State     Protection
   0        Bridge-Aggregation1          DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/3         DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/18        DESI  FORWARDING    NONE
```

Cisco
not an available feature Cisco switches operate with PVST+/Rapid PVST+ which is proprietary. PVST+ is comparable to STP on 802.1Q links (default) Rapid PVST+ is comparable to RSTP on 802.1Q links

Chapter 19 MSTP

This chapter compares the commands used to configure Multiple Spanning Tree Protocol (MSTP). The three operating systems implement MSTP differently:

- ProVision uses MSTP as the default STP version, but it is *not* enabled by default. When MSTP is enabled, all ports are auto-edge-ports by default.
- Comware 5 uses MSTP as the default STP version. By default, MSTP is *enabled,* and all ports are non-edge ports.
- Cisco uses Per VLAN Spanning Tree Plus (PVST+) as the default STP version, and it is *enabled* by default. If you enable MSTP, all ports are non-edge ports by default.

ProVision	Comware 5	Cisco
ProVision(config)# spanning-tree		Cisco(config)#spanning-tree mode mst
	[Comware5]stp region-configuration	Cisco(config)#spanning-tree mst configuration
ProVision(config)# spanning-tree config-name ProVision-Comware-Cisco	[Comware5-mst-region]region-name ProVision-Comware-Cisco	Cisco(config-mst)#name ProVision-Comware-Cisco
ProVision(config)# spanning-tree config-revision 1	[Comware5-mst-region]revision-level 1	Cisco(config-mst)#revision 1
ProVision(config)# spanning-tree instance 1 vlan 12 220	[Comware5-mst-region]instance 1 vlan 12 220	Cisco(config-mst)# instance 1 vlan 12 220
ProVision(config)# spanning-tree instance 2 vlan 11 13	[Comware5-mst-region]instance 2 vlan 11 13	Cisco(config-mst)# instance 2 vlan 11, 13
	[Comware5-mst-region]active region-configuration	
ProVision(config)# spanning-tree priority 9	[Comware5]stp priority 36864	Cisco(config)#spanning-tree mst 0 priority 36864
ProVision(config)# spanning-tree instance 1 priority 9	[Comware5]stp instance 1 priority 8192	Cisco(config)#spanning-tree mst 1 priority 8192
		Cisco(config)#interface f0/9
ProVision(config)# spanning-tree 7 path-cost 10000		Cisco(config-if)#spanning-tree cost 10000
ProVision(config)# spanning-tree 7 priority 6		Cisco(config-if)#spanning-tree port-priority 6
ProVision(config)# spanning-tree instance 1 7 path-cost 10000		Cisco(config-if)#spanning-tree mst 1 cost 10000
ProVision(config)# spanning-tree instance 1 7 priority 6		Cisco(config-if)#spanning-tree mst 1 port-priority 6
ProVision# show spanning-tree	[Comware5]display stp	Cisco#show spanning-tree
	[Comware5]display stp brief	
		Cisco#show spanning-tree mst
ProVision# show spanning-tree mst-config	[Comware5]display stp region-configuration	Cisco#show spanning-tree mst configuration
ProVision# show spanning-tree instance ist	[Comware5]display stp instance 0	Cisco#show spanning-tree mst 0
ProVision# show spanning-tree instance 1	[Comware5]display stp instance 1	Cisco#show spanning-tree mst 1

ProVision

```
ProVision(config)# spanning-tree


ProVision(config)# spanning-tree config-name ProVision-Comware-Cisco

ProVision(config)# spanning-tree config-revision 1

ProVision(config)# spanning-tree instance 1 vlan 12 220

ProVision(config)# spanning-tree instance 2 vlan 11 13

ProVision(config)# spanning-tree priority 9
   (note - multiplier is 4096)

ProVision(config)# spanning-tree instance 1 priority 9
   (note - multiplier is 4096)


ProVision(config)# spanning-tree 7 path-cost 10000

ProVision(config)# spanning-tree 7 priority 6
   (note - multiplier is 16)


ProVision(config)# spanning-tree instance 1 7 path-cost 10000

ProVision(config)# spanning-tree instance 1 7 priority 6


ProVision# show spanning-tree

 Multiple Spanning Tree (MST) Information

  STP Enabled   : Yes
  Force Version : MSTP-operation
  IST Mapped VLANs : 1-10,14-219,221-4094
  Switch MAC Address : 001635-b376c0
  Switch Priority    : 36864
  Max Age  : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count  : 26
  Time Since Last Change : 23 mins

  CST Root MAC Address : 001647-59ca00
  CST Root Priority    : 4096
  CST Root Path Cost   : 400000
  CST Root Port        : 6

  IST Regional Root MAC Address : 001bd4-fef500
  IST Regional Root Priority    : 4096
  IST Regional Root Path Cost   : 200000
  IST Remaining Hops            : 19

  Root Guard Ports     :
  TCN Guard Ports      :
  BPDU Protected Ports :
  BPDU Filtered Ports  :
  PVST Protected Ports :
  PVST Filtered Ports  :

                   |           Prio             | Designated    Hello
  Port   Type      | Cost      rity  State      | Bridge        Time  PtP Edge
  ------ --------- + --------- ----- ---------- + ------------- ----- --- ----
  1      100/1000T | Auto      128   Disabled   |
  2      100/1000T | Auto      128   Disabled   |
  3      100/1000T | Auto      128   Disabled   |
  4      100/1000T | Auto      128   Disabled   |
  5      100/1000T | Auto      128   Disabled   |
  6      100/1000T | 200000    128   Forwarding | 001bd4-fef500 2     Yes No
  7      100/1000T | 10000     96    Disabled   |
  8      100/1000T | Auto      128   Disabled   |
  9      100/1000T | Auto      128   Disabled   |
  10     100/1000T | 20000     128   Forwarding | 001635-b376c0 2     Yes Yes
  11     100/1000T | Auto      128   Disabled   |
  12     100/1000T | 200000    128   Forwarding | 001635-b376c0 2     Yes Yes
  13     100/1000T | Auto      128   Disabled   |
  14     100/1000T | Auto      128   Disabled   |
  15     100/1000T | Auto      128   Disabled   |
  16     100/1000T | Auto      128   Disabled   |
  17     100/1000T | Auto      128   Disabled   |
  18     100/1000T | Auto      128   Disabled   |
  19     100/1000T | Auto      128   Disabled   |
  20     100/1000T | Auto      128   Disabled   |
  21     100/1000T | Auto      128   Disabled   |
  24     100/1000T | Auto      128   Disabled   |
  Trk1             | 20000     64    Forwarding | 001635-b376c0 2     Yes No


ProVision# show spanning-tree mst-config

 MST Configuration Identifier Information

  MST Configuration Name : ProVision-Comware-Cisco
  MST Configuration Revision : 1
  MST Configuration Digest : 0x4208CE2DC3E8777BE5C71934E2A752D4

  IST Mapped VLANs : 1-10,14-219,221-4094

  Instance ID Mapped VLANs
  ----------- ---------------------------------------------------------
  1           12,220
  2           11,13


ProVision# show spanning-tree instance ist

 IST Instance Information

  Instance ID : 0
  Mapped VLANs : 1-10,14-219,221-4094
  Switch Priority         : 36864

  Topology Change Count   : 26
  Time Since Last Change  : 25 mins

  Regional Root MAC Address : 001bd4-fef500
  Regional Root Priority    : 4096
  Regional Root Path Cost   : 200000
  Regional Root Port        : 6
  Remaining Hops            : 19
                                                           Designated
  Port  Type      Cost      Priority Role       State      Bridge
  ----- --------- --------- -------- ---------- ---------- -------------
  1     100/1000T Auto      128      Disabled   Disabled
  2     100/1000T Auto      128      Disabled   Disabled
  3     100/1000T Auto      128      Disabled   Disabled
  4     100/1000T Auto      128      Disabled   Disabled
  5     100/1000T Auto      128      Disabled   Disabled
  6     100/1000T 200000    128      Root       Forwarding 001bd4-fef500
  7     100/1000T Auto      96       Disabled   Disabled
  8     100/1000T Auto      128      Disabled   Disabled
  9     100/1000T Auto      128      Disabled   Disabled
  10    100/1000T 20000     128      Designated Forwarding 001635-b376c0
  11    100/1000T Auto      128      Disabled   Disabled
  12    100/1000T 200000    128      Designated Forwarding 001635-b376c0
  13    100/1000T Auto      128      Disabled   Disabled
  14    100/1000T Auto      128      Disabled   Disabled
  15    100/1000T Auto      128      Disabled   Disabled
  16    100/1000T Auto      128      Disabled   Disabled
  17    100/1000T Auto      128      Disabled   Disabled
  18    100/1000T Auto      128      Disabled   Disabled
  19    100/1000T Auto      128      Disabled   Disabled
  20    100/1000T Auto      128      Disabled   Disabled
  21    100/1000T Auto      128      Disabled   Disabled
  24    100/1000T Auto      128      Disabled   Disabled
  Trk1            20000     64       Designated Forwarding 001635-b376c0


ProVision# show spanning-tree instance 1

 MST Instance Information

  Instance ID : 1
  Mapped VLANs : 12,220
  Switch Priority          : 36864

  Topology Change Count    : 26
  Time Since Last Change   : 54 mins

  Regional Root MAC Address : 001bd4-fef500
  Regional Root Priority    : 8192
  Regional Root Path Cost   : 200000
  Regional Root Port        : 6
  Remaining Hops            : 19
                                                           Designated
  Port  Type      Cost      Priority Role       State      Bridge
  ----- --------- --------- -------- ---------- ---------- -------------
  1     100/1000T Auto      128      Disabled   Disabled
  2     100/1000T Auto      128      Disabled   Disabled
  3     100/1000T Auto      128      Disabled   Disabled
  4     100/1000T Auto      128      Disabled   Disabled
  5     100/1000T Auto      128      Disabled   Disabled
  6     100/1000T 200000    128      Root       Forwarding 001bd4-fef500
  7     100/1000T Auto      96       Disabled   Disabled
  8     100/1000T Auto      128      Disabled   Disabled
  9     100/1000T 250000    128      Disabled   Disabled
  10    100/1000T 20000     128      Designated Forwarding 001635-b376c0
  11    100/1000T Auto      128      Disabled   Disabled
  12    100/1000T 200000    128      Designated Forwarding 001635-b376c0
  13    100/1000T Auto      128      Disabled   Disabled
  14    100/1000T Auto      128      Disabled   Disabled
  15    100/1000T Auto      128      Disabled   Disabled
  16    100/1000T Auto      128      Disabled   Disabled
  17    100/1000T Auto      128      Disabled   Disabled
  18    100/1000T Auto      128      Disabled   Disabled
  19    100/1000T Auto      128      Disabled   Disabled
  20    100/1000T Auto      128      Disabled   Disabled
  21    100/1000T Auto      128      Disabled   Disabled
  24    100/1000T Auto      128      Disabled   Disabled
  Trk1            20000     64       Designated Forwarding 001635-b376c0
```

Comware 5

```
[Comware5]stp region-configuration

[Comware5-mst-region]region-name ProVision-Comware-Cisco

[Comware5-mst-region]revision-level 1

[Comware5-mst-region]instance 1 vlan 12 220

[Comware5-mst-region]instance 2 vlan 1 11 13

[Comware5-mst-region]active region-configuration

[Comware5]stp priority 36864
   (note – in steps of 4096)

[Comware5]stp instance 1 priority 8192
   (note – in steps of 4096)


[Comware5]interface g1/0/7

[Comware5-GigabitEthernet1/0/7]stp cost 10000

[Comware5-GigabitEthernet1/0/7]stp port priority 96
   (note – in steps of 16)

[Comware5-GigabitEthernet1/0/7]stp instance 1 cost 10000

[Comware5-GigabitEthernet1/0/7]stp instance 1 port priority 96
   (note – in steps of 16)


[Comware5]display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :36864.0022-57bc-d900
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :4096.0016-4759-ca00 / 400000
CIST RegRoot/IRPC   :4096.001b-d4fe-f500 / 210000
CIST RootPortId     :128.505
BPDU-Protection     :disabled
Bridge Config-
Digest-Snooping     :disabled
TC or TCN received  :168
Time since last TC  :0 days 0h:28m:35s

----[Port505(Bridge-Aggregation1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Root Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=10000
 Desg. Bridge/Port   :36864.0016-35b3-76c0 / 64.290
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=802.1s
 Port Config-
 Digest-Snooping     :disabled
 Num of Vlans Mapped :2
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s RemHop 19
 BPDU Sent           :1110
          TCN: 0, Config: 0, RST: 1053, MST: 57
 BPDU Received       :2544
          TCN: 0, Config: 0, RST: 275, MST: 2269

----[Port1(GigabitEthernet1/0/1)][DOWN]----
 Port Protocol       :enabled
 Port Role           :CIST Disabled Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=200000000
 Desg. Bridge/Port   :36864.0022-57bc-d900 / 128.1
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=false
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Num of Vlans Mapped :1
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 0s RemHop 20
 BPDU Sent           :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0

...

-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :8192.0022-57bc-d900
MSTI RegRoot/IRPC   :8192.001b-d4fe-f500 / 210000
MSTI RootPortId     :128.505
Master Bridge       :4096.001b-d4fe-f500
Cost to Master      :210000
TC received         :5

 ----[Port505(Bridge-Aggregation1)][FORWARDING]----
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=10000
 Desg. Bridge/Port   :36864.0016-35b3-76c0 / 64.290
 Num of Vlans Mapped :1
 Port Times          :RemHops 19

 ----[Port18(GigabitEthernet1/0/18)][FORWARDING]----
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=200000
 Desg. Bridge/Port   :8192.0022-57bc-d900 / 128.18
 Rapid transition    :false
 Num of Vlans Mapped :2
 Port Times          :RemHops 18
```

```
-------[MSTI 2 Global Info]-------
MSTI Bridge ID      :32768.0022-57bc-d900
MSTI RegRoot/IRPC   :32768.0022-57bc-d900 / 0
MSTI RootPortId     :0.0
Master Bridge       :4096.001b-d4fe-f500
Cost to Master      :210000
TC received         :0


[Comware5]display stp brief
 MSTID      Port                         Role  STP State     Protection
   0        Bridge-Aggregation1          ROOT  FORWARDING    NONE
   0        GigabitEthernet1/0/3         DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/18        DESI  FORWARDING    NONE
   1        Bridge-Aggregation1          ROOT  FORWARDING    NONE
   1        GigabitEthernet1/0/18        DESI  FORWARDING    NONE


[Comware5]display stp region-configuration
 Oper configuration
   Format selector    :0
   Region name        :ProVision-Comware-Cisco
   Revision level     :1

   Instance   Vlans Mapped
      0       1 to 10, 14 to 219, 221 to 4094
      1       12, 220
      2       11, 13


[Comware5]display stp instance 0
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :36864.0022-57bc-d900
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :4096.0016-4759-ca00 / 400000
CIST RegRoot/IRPC   :4096.001b-d4fe-f500 / 210000
CIST RootPortId     :128.505
BPDU-Protection     :disabled
Bridge Config-
Digest-Snooping     :disabled
TC or TCN received  :170
Time since last TC  :0 days 0h:5m:9s
...
----[Port3(GigabitEthernet1/0/3)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Designated Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=20000
 Desg. Bridge/Port   :36864.0022-57bc-d900 / 128.3
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping     :disabled
 Rapid transition    :false
 Num of Vlans Mapped :1
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s RemHop 18
 BPDU Sent           :3794
          TCN: 0, Config: 0, RST: 1135, MST: 2659
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
...
----[Port505(Bridge-Aggregation1)][FORWARDING]----
 Port Protocol       :enabled
 Port Role           :CIST Root Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=10000
 Desg. Bridge/Port   :36864.0016-35b3-76c0 / 64.290
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transmit Limit      :10 packets/hello-time
 Protection Type     :None
 MST BPDU Format     :Config=auto / Active=802.1s
 Port Config-
 Digest-Snooping     :disabled
 Num of Vlans Mapped :2
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s RemHop 19
 BPDU Sent           :1110
          TCN: 0, Config: 0, RST: 1053, MST: 57
 BPDU Received       :2790
          TCN: 0, Config: 0, RST: 275, MST: 2515


[Comware5]display stp instance 1
-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :8192.0022-57bc-d900
MSTI RegRoot/IRPC   :8192.001b-d4fe-f500 / 210000
MSTI RootPortId     :128.505
Master Bridge       :4096.001b-d4fe-f500
Cost to Master      :210000
TC received         :5

 ----[Port18(GigabitEthernet1/0/18)][FORWARDING]----
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=200000
 Desg. Bridge/Port   :8192.0022-57bc-d900 / 128.18
 Rapid transition    :false
 Num of Vlans Mapped :2
 Port Times          :RemHops 18

 ----[Port505(Bridge-Aggregation1)][FORWARDING]----
 Port Role           :Root Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=10000
 Desg. Bridge/Port   :36864.0016-35b3-76c0 / 64.290
 Num of Vlans Mapped :1
 Port Times          :RemHops 19
```

Cisco

```
Cisco(config)#spanning-tree mode mst

Cisco(config)#spanning-tree mst configuration

Cisco(config-mst)#name ProVision-Comware-Cisco

Cisco(config-mst)#revision 1

Cisco(config-mst)# instance 1 vlan 12, 220

Cisco(config-mst)# instance 2 vlan 11, 13


Cisco(config)#spanning-tree mst 0 priority 36864
   (note - increments of 4096)

Cisco(config)#spanning-tree mst 1 priority 8192

Cisco(config)#interface f0/9

Cisco(config-if)#spanning-tree cost 10000

Cisco(config-if)#spanning-tree port-priority 6
   (note - increments of 16)

Cisco(config-if)#spanning-tree mst 1 cost 10000

Cisco(config-if)#spanning-tree mst 1 port-priority 6


Cisco#show spanning-tree

MST0
  Spanning tree enabled protocol mstp
  Root ID    Priority    4096
             Address     0016.4759.ca00
             Cost        400000
             Port        11 (FastEthernet0/9)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4096   (priority 4096 sys-id-ext 0)
             Address     001b.d4fe.f500
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/6               Desg FWD 200000    128.8    P2p
Fa0/9               Root FWD 200000    128.11   P2p Bound(RSTP)



MST1
  Spanning tree enabled protocol mstp
  Root ID    Priority    8193
             Address     001b.d4fe.f500
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    8193   (priority 8192 sys-id-ext 1)
```

```
             Address     001b.d4fe.f500
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/6               Desg FWD 200000    128.8    P2p


Cisco#show spanning-tree mst

##### MST0    vlans mapped:   1-10,14-219,221-4094
Bridge        address 001b.d4fe.f500  priority      4096  (4096 sysid 0)
Root          address 0016.4759.ca00  priority      4096  (4096 sysid 0)
              port    Fa0/9           path cost     400000
Regional Root this switch
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 200000    128.8    P2p
Fa0/9            Root FWD 200000    128.11   P2p Bound(RSTP)

##### MST1    vlans mapped:   12,220
Bridge        address 001b.d4fe.f500  priority      8193  (8192 sysid 1)
Root          this switch for MST1

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 200000    128.8    P2p


Cisco#show spanning-tree mst configuration
Name      [ProVision-Comware-Cisco]
Revision  1     Instances configured 3

Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-10,14-219,221-4094
1         12,220
2         11,13
```

```
Cisco#show spanning-tree mst 0

##### MST0    vlans mapped:   1-10,14-219,221-4094
Bridge        address 001b.d4fe.f500  priority      4096  (4096 sysid 0)
Root          address 0016.4759.ca00  priority      4096  (4096 sysid 0)
              port    Fa0/9           path cost     400000
Regional Root this switch
Operational   hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured    hello time 2 , forward delay 15, max age 20, max hops    20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 200000    128.8    P2p
Fa0/9            Root FWD 200000    128.11   P2p Bound(RSTP)
```

```
Cisco#show spanning-tree mst 1

##### MST1    vlans mapped:   12,220
Bridge        address 001b.d4fe.f500  priority      8193  (8192 sysid 1)
Root          this switch for MST1

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 200000    128.8    P2p
```

Chapter 20 RIP

This chapter compares the commands used to enable and configure Routing Information Protocol (RIP).

ProVision	Comware 5	Cisco
`ProVision(config)# router rip`	`[Comware5]rip 1`	`Cisco(config)#router rip`
`ProVision(config)# vlan 220 ip rip`	`[Comware5-rip-1]network 10.1.220.0`	`Cisco(config-router)#network 10.1.220.0`
	`[Comware5-rip-1]version 2`	`Cisco(config-router)#version 2`
`ProVision(rip)# redistribute connected`	`[Comware5-rip-1]import-route direct`	`Cisco(config-router)#redistribute connected`
`ProVision# show ip rip`	`[Comware5]display rip`	`Cisco#show ip rip database`

`ProVision# show ip rip interface vlan 220`	`[Comware5]display rip 1 interface Vlan-interface 220`
	`[Comware5]display rip 1 database`
		`Cisco#show ip rip database 10.1.220.0 255.255.255.0`

`ProVision# show ip rip redistribute`		

ProVision

```
ProVision(config)# router rip

ProVision(config)# vlan 220 ip rip


ProVision(rip)# redistribute connected


ProVision# show ip rip

 RIP global parameters

  RIP protocol    : enabled
  Auto-summary    : enabled
  Default Metric : 1
  Distance        : 120
  Route changes   : 0
  Queries         : 0

 RIP interface information

  IP Address       Status      Send mode         Recv mode  Metric      Auth
  ---------------- ----------- ----------------- ---------- ----------- ----
  10.1.220.1       enabled     V2-only           V2-only    1           none


 RIP peer information

  IP Address       Bad routes  Last update timeticks
  ---------------- ----------- ---------------------


ProVision# show ip rip interface vlan 220

 RIP configuration and statistics for VLAN 220

 RIP interface information for 10.1.220.1

  IP Address : 10.1.220.1
  Status     : enabled

  Send mode  : V2-only
  Recv mode  : V2-only
  Metric : 1
  Auth : none

  Bad packets received : 0
  Bad routes received  : 0
  Sent updates : 0


ProVision# show ip rip redistribute

 RIP redistributing

  Route type Status
  ---------- --------
  connected  enabled
  static     disabled
  ospf       disabled
```

Comware 5

```
[Comware5]rip 1

[Comware5-rip-1]version 2

[Comware5-rip-1]network 10.1.220.0

[Comware5-rip-1]import-route direct


[Comware5]display rip
  Public VPN-instance name :

    RIP process : 1
       RIP version : 2
       Preference : 100
       Checkzero : Enabled
       Default-cost : 0
       Summary : Disabled
       Hostroutes : Enabled
       Maximum number of balanced paths : 8
       Update time    :   30 sec(s)  Timeout time         :  180 sec(s)
       Suppress time :  120 sec(s)  Garbage-collect time :  120 sec(s)
       update output delay :   20(ms)  output count :    3
       TRIP retransmit time :    5 sec(s)
       TRIP response packets retransmit count :   36
       Silent interfaces : None
       Default routes : Disabled
       Verify-source : Enabled
       Networks :
           10.0.0.0
       Configured peers : None
       Triggered updates sent : 2
       Number of routes changes : 12
       Number of replies to queries : 0
```

```
[Comware5]display rip 1 interface Vlan-interface 220

 Interface-name: Vlan-interface220
    Address/Mask:10.1.220.3/24       Version:RIPv2
    MetricIn:0                       MetricIn route policy:Not designated
    MetricOut:1                      MetricOut route policy:Not designated
    Split-horizon/Poison-reverse:on/off  Input/Output:on/on
    Default route:off
    Current packets number/Maximum packets number:0/2000


[Comware5]display rip 1 database
   10.0.0.0/8, cost 0, ClassfulSumm
       10.0.1.0/24, cost 1, nexthop 10.0.100.60
       10.0.1.0/24, cost 1, nexthop 10.1.220.1
       10.0.1.0/24, cost 1, nexthop 10.1.220.2
       10.0.100.0/24, cost 0, nexthop 10.0.100.48, Rip-interface
       10.1.220.0/24, cost 0, nexthop 10.1.220.3, Rip-interface
```

Cisco

```
Cisco(config)#router rip

Cisco(config-router)#network 10.1.220.0

Cisco(config-router)#version 2


Cisco(config-router)#redistribute connected


Cisco#show ip rip database
10.0.0.0/8    auto-summary
10.0.100.0/24    directly connected, Vlan100
10.1.220.0/24    directly connected, Vlan220


Cisco#show ip rip database 10.1.220.0 255.255.255.0
10.1.220.0/24    directly connected, Vlan220
```

Chapter 21 OSPF

This chapter compares the commands used to enable and configure Open Shortest Path First (OSPF).

a) Single Area

ProVision	Comware 5	Cisco
ProVision(config)# ip router-id 10.0.0.24		
ProVision(config)# router ospf	[Comware5]ospf 1 router-id 10.0.0.48	Cisco(config)#router ospf 1
		Cisco(config-router)#router-id 10.0.0.60
ProVision(ospf)# area 0	[Comware5-ospf-1]area 0	
ProVision(ospf)# vlan 220 ProVision(vlan-220)# ip ospf area 0	[Comware5-ospf-1-area-0.0.0.0]network 10.1.220.0 0.0.0.255	Cisco(config-router)#network 10.1.220.0 0.0.0.255 area 0
ProVision(ospf)# redistribute ?	[Comware5-ospf-1]import-route ?	Cisco(config-router)#redistribute ?

ProVision

```
ProVision(config)# ip router-id 10.0.0.24


ProVision(config)# router ospf


ProVision(ospf)# area backbone
  -or-
ProVision(ospf)# area 0.0.0.0
  -or-
ProVision(ospf)# area 0


ProVision(ospf)# vlan 220

ProVision(vlan-220)# ip ospf area backbone
  -or-
ProVision(vlan-220)# ip ospf area 0.0.0.0
  -or-
ProVision(vlan-220)# ip ospf area 0


(also as compound statements)

ProVision(config)# vlan 220 ip ospf area backbone
  -or-
ProVision(config)# vlan 220 ip ospf area 0
  -or-
ProVision(config)# vlan 220 ip ospf area 0.0.0.0


ProVision(ospf)# redistribute ?
 connected
 static
 rip
```

Comware 5

```
[Comware5]ospf 1 router-id 10.0.0.48


[Comware5-ospf-1]area 0
-or-
[Comware5-ospf-1]area 0.0.0.0


[Comware5-ospf-1-area-0.0.0.0]network 10.1.220.0 0.0.0.255


[Comware5-ospf-1]import-route ?
  bgp     Border Gateway Protocol (BGP) routes
  direct  Direct routes
  isis    Intermediate System to Intermediate System (IS-IS) routes
  ospf    Open Shortest Path First (OSPF) routes
  rip     Routing Information Protocol (RIP) routes
  static  Static routes
```

Cisco

```
Cisco(config)#router ospf 1


Cisco(config-router)#router-id 10.0.0.60


Cisco(config-router)#network 10.1.220.0 0.0.0.255 area 0
-or-
Cisco(config-router)#network 10.1.220.0 0.0.0.255 area 0.0.0.0


Cisco(config-router)#redistribute ?
  bgp              Border Gateway Protocol (BGP)
  connected        Connected
  eigrp            Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis             ISO IS-IS
  iso-igrp         IGRP for OSI networks
  maximum-prefix   Maximum number of prefixes redistributed to protocol
  metric           Metric for redistributed routes
  metric-type      OSPF/IS-IS exterior metric type for redistributed routes
  mobile           Mobile routes
  nssa-only        Limit redistributed routes to NSSA areas
  odr              On Demand stub Routes
  ospf             Open Shortest Path First (OSPF)
  rip              Routing Information Protocol (RIP)
  route-map        Route map reference
  static           Static routes
  subnets          Consider subnets for redistribution into OSPF
  tag              Set tag for routes redistributed into OSPF
  <cr>
```

b) Multiple Areas

ProVision	Comware 5	Cisco
ProVision(config)# ip router-id 10.0.0.24		
ProVision(config)# router ospf	[Comware5]ospf 1 router-id 10.0.0.48	Cisco(config)#router ospf 1
ProVision(ospf)# area 1	[Comware5-ospf-1]area 1	
ProVision(ospf)# area 2		
		Cisco(config-router)#router-id 10.0.0.60
ProVision(ospf)# vlan 230 ProVision(vlan-230)# ip ospf area 1	[Comware5-ospf-1-area-0.0.0.1]network 10.1.230.0 0.0.0.255	Cisco(config-router)#network 10.1.230.0 0.0.0.255 area 1
	[Comware5-ospf-1]area 2	
ProVision(vlan-230)# vlan 240 ProVision(vlan-240)# ip ospf area 2	[Comware5-ospf-1-area-0.0.0.2]network 10.1.240.0 0.0.0.255	Cisco(config-router)#network 10.1.240.0 0.0.0.255 area 2

ProVision

```
ProVision(config)# ip router-id 10.0.0.24


ProVision(config)# router ospf


ProVision(ospf)# area 1
  -or-
ProVision(ospf)# area 0.0.0.1


ProVision(ospf)# area 2
  -or-
ProVision(ospf)# area 0.0.0.2


ProVision(ospf)# vlan 230

ProVision(vlan-230)# ip ospf area 1
  -or-
ProVision(vlan-230)# ip ospf area 0.0.0.1


ProVision(vlan-230)# vlan 240

ProVision(vlan-240)# ip ospf area 2
  -or-
ProVision(vlan-240)# ip ospf area 0.0.0.2


(also as compound statements)

ProVision(config)# vlan 230 ip ospf area 1
  -or-
ProVision(config)# vlan 230 ip ospf area 0.0.0.1


ProVision(config)# vlan 240 ip ospf area 2
  -or-
ProVision(config)# vlan 240 ip ospf area 0.0.0.2
```

Comware 5

```
[Comware5]ospf 1 router-id 10.0.0.48

[Comware5-ospf-1]area 1

[Comware5-ospf-1-area-0.0.0.1]network 10.1.230.0 0.0.0.255

[Comware5-ospf-1]area 2

[Comware5-ospf-1-area-0.0.0.2]network 10.1.240.0 0.0.0.255
```

Cisco

```
Cisco(config)#router ospf 1

Cisco(config-router)#router-id 10.0.0.60

Cisco(config-router)#network 10.1.230.0 0.0.0.255 area 1

Cisco(config-router)#network 10.1.240.0 0.0.0.255 area 2
```

c) Stub

ProVision	Comware 5	Cisco

`ProVision(ospf)# area 1 stub 11`	`[Comware5-ospf-1]area 1`
	`[Comware5-ospf-1-area-0.0.0.1]stub`
		`Cisco(config-router)#area 1 stub`

ProVision

```
ProVision(ospf)# area 1 stub 11
```

Comware 5

```
[Comware5-ospf-1]area 1

[Comware5-ospf-1-area-0.0.0.1]stub
```

Cisco

```
Cisco(config-router)#area 1 stub
```

d) Totally Stubby

ProVision	Comware 5	Cisco

`ProVision(ospf)# area 2 stub 22 no-summary`	`[Comware5-ospf-1]area 1`
	`[Comware5-ospf-1-area-0.0.0.1]stub no-summary`
		`Cisco(config-router)#area 2 stub no-summary`

`ProVision(config)# vlan 230`	`[Comware5]interface Vlan-interface 230`	`Cisco(config-if)#interface vlan 230`
`ProVision(vlan-230)# ip ospf cost 10`	`[Comware5-Vlan-interface230]ospf cost 10`	`Cisco(config-if)#ip ospf cost 10`

ProVision

`ProVision(ospf)# area 2 stub 22 no-summary`
`ProVision(config)# vlan 230`
`ProVision(vlan-230)# ip ospf cost 10`

Comware 5

`[Comware5-ospf-1]area 1`
`[Comware5-ospf-1-area-0.0.0.1]stub no-summary`
`[Comware5]interface Vlan-interface 230`
`[Comware5-Vlan-interface230]ospf cost 10`

Cisco

`Cisco(config-router)#area 2 stub no-summary`
`Cisco(config-if)#interface vlan 230`
`Cisco(config-if)#ip ospf cost 10`

e) Show or Display OSPF Commands

ProVision	Comware 5	Cisco
ProVision# show ip ospf interface	[Comware5]display ospf interface	Cisco#show ip ospf interface brief
ProVision# show ip ospf neighbor	[Comware5]display ospf peer	Cisco#show ip ospf neighbor
ProVision# show ip ospf link-state	[Comware5]display ospf lsdb	Cisco#show ip ospf database

ProVision

```
ProVision# show ip ospf
 area                  Show OSPF areas configured on the device.
 external-link-state   Show the Link State Advertisements from throughout the
                       areas to which the device is attached.
 general               Show OSPF basic configuration and operational
                       information.
 interface             Show OSPF interfaces' information.
 link-state            Show all Link State Advertisements from throughout the
                       areas to which the device is attached.
 neighbor              Show all OSPF neighbors in the locality of the
                       device.
 redistribute          List protocols which are being redistributed into OSPF.
 restrict              List routes which will not be redistributed via OSPF.
 spf-log               List the OSPF SPF(Shortes Path First Algorithm) run
                       count for all OSPF areas and last ten Reasons for
                       running SPF.
 statistics            List OSPF packet statistics( OSPF sent,recieved and
                       error packet count) of all OSPF enabled interfaces.
 traps                 Show OSPF traps enabled on the device.
 virtual-link          Show status of all OSPF virtual links configured.
 virtual-neighbor      Show all virtual neighbors of the device.
 <cr>


ProVision# show ip ospf interface

 OSPF Interface Status

  IP Address      Status   Area ID         State   Auth-type Cost  Pri Passive
  --------------- -------- --------------- ------- --------- ----- --- -------
  10.1.220.1      enabled  backbone        BDR     none      1     1   no
  10.1.230.1      enabled  0.0.0.1         DOWN    none      1     1   no
  10.1.240.1      enabled  0.0.0.2         DOWN    none      1     1   no


ProVision# show ip ospf neighbor

 OSPF Neighbor Information

                                                         Rxmt         Helper
  Router ID       Pri IP Address      NbIfState State    QLen  Events Status
  --------------- --- --------------- --------- -------- ----- ------ -------
  10.0.0.60       1   10.1.220.2      DR        FULL     0     6      None


ProVision# show ip ospf link-state

 OSPF Link State Database for Area 0.0.0.0

                             Advertising
  LSA Type   Link State ID   Router ID       Age  Sequence #  Checksum
  ---------- --------------- --------------- ---- ----------- ----------
  Router     10.0.0.24       10.0.0.24       761  0x8000045b  0x0000b20b
  Router     10.0.0.60       10.0.0.60       731  0x80000014  0x000019a6
  Network    10.1.220.2      10.0.0.60       757  0x80000007  0x0000108b

 OSPF Link State Database for Area 0.0.0.1

                             Advertising
  LSA Type   Link State ID   Router ID       Age  Sequence #  Checksum
  ---------- --------------- --------------- ---- ----------- ----------
  Router     10.0.0.24       10.0.0.24       138  0x80000452  0x00009019

 OSPF Link State Database for Area 0.0.0.2

                             Advertising
  LSA Type   Link State ID   Router ID       Age  Sequence #  Checksum
  ---------- --------------- --------------- ---- ----------- ----------
  Router     10.0.0.24       10.0.0.24       138  0x80000452  0x00009019
```

Comware 5

```
[Comware5]display ospf ?
  INTEGER<1-65535>  Process ID
  abr-asbr          Information of the OSPF ABR and ASBR
  asbr-summary      Information of aggregate addresses for OSPF(only for ASBR)
  brief             brief information of OSPF processes
  cumulative        Statistics information
  error             Error information
  interface         Interface information
  lsdb              Link state database
  nexthop           Nexthop information
  peer              Specify a neighbor router
  request-queue     Link state request list
  retrans-queue     Link state retransmission list
  routing           OSPF route table
  sham-link         Sham Link
  vlink             Virtual link information


[Comware5]display ospf interface

         OSPF Process 1 with Router ID 10.0.0.48
                 Interfaces

 Area: 0.0.0.0
 IP Address      Type      State    Cost  Pri   DR              BDR
 10.1.220.3      Broadcast DROther  1     1     10.1.220.1      10.1.220.2

 Area: 0.0.0.1
 IP Address      Type      State    Cost  Pri   DR              BDR
 10.1.230.3      Broadcast Down     1     1     0.0.0.0         0.0.0.0


[Comware5]display ospf peer

                  OSPF Process 1 with Router ID 10.0.0.48
                        Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time Interface       State
 10.0.0.24       10.1.220.1      1   31         Vlan220         Full/DR
 10.0.0.60       10.1.220.2      1   38        Vlan220         Full/BDR


[Comware5]display ospf lsdb

         OSPF Process 1 with Router ID 10.0.0.48
                 Link State Database

                        Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    10.0.0.60       10.0.0.60         1168  36    80000005       0
 Router    10.0.0.48       10.0.0.48          607  36    80000005       0
 Router    10.0.0.24       10.0.0.24         1406  36    80000006       0
 Network   10.1.220.1      10.0.0.24          266  36    80000006       0
                        Area: 0.0.0.1
```

Cisco

```
Cisco#show ip ospf ?
  <1-65535>             Process ID number
  border-routers        Border and Boundary Router Information
  database              Database summary
  flood-list            Link state flood list
  interface             Interface information
  max-metric            Max-metric origination information
  mpls                  MPLS related information
  neighbor              Neighbor list
  request-list          Link state request list
  retransmission-list   Link state retransmission list
  sham-links            Sham link information
  statistics            Various OSPF Statistics
  summary-address       Summary-address redistribution Information
  timers                OSPF timers information
  traffic               Traffic related statistics
  virtual-links         Virtual link information
  |                     Output modifiers
  <cr>


Cisco#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Vl220        1     0               10.1.220.2/24      1     DR    1/1
Vl230        1     1               10.1.230.2/24      1     DOWN  0/0
Vl240        1     2               10.1.240.2/24      1     DOWN  0/0


Cisco#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.0.0.24         1   FULL/BDR        00:00:30    10.1.220.1      Vlan220


Cisco#show ip ospf database

            OSPF Router with ID (10.0.0.60) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.24       10.0.0.24       1410        0x8000045B 0x00B20B 1
10.0.0.60       10.0.0.60       1378        0x80000014 0x0019A6 1

                Net Link States (Area 0)
```

```
Link ID         ADV Router      Age         Seq#       Checksum
10.1.220.2      10.0.0.60       1404        0x80000007 0x00108B

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.60       10.0.0.60       1378        0x80000008 0x00EEC0 0

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.60       10.0.0.60       1378        0x80000008 0x00EEC0 0
```

Chapter 22 VRRP

This chapter compares the commands used to configure Virtual Router Redundancy Protocol (VRRP) on ProVision and Comware 5. Cisco supports Hot Standby Router Protocol (HSRP), which is not compatible with VRRP.

ProVision	Comware 5	Cisco
`ProVision(config)# router vrrp`		***(Very limited availability in the Cisco product line)***
`ProVision(config)# vlan 220`	`[Comware5]interface vlan 220`	
`ProVision(vlan-220)# vrrp vrid 220`	`[Comware5-Vlan-interface220]vrrp vrid 220 virtual-ip 10.1.220.1`	
`ProVision(vlan-220-vrid-220)# owner`	`[Comware5-Vlan-interface220]vrrp vrid 220 priority 100`	
`ProVision(vlan-220-vrid-220)# virtual-ip-address 10.1.220.1/24`		
`ProVision(vlan-220-vrid-220)# enable`		
`ProVision# show vrrp config`	`[Comware5]display vrrp verbose`	
	`[Comware5]display vrrp`	
`ProVision# show vrrp vlan 220`	`[Comware5]display vrrp interface Vlan-interface 220`	

ProVision

```
ProVision(config)# router vrrp

ProVision(config)# vlan 220

ProVision(vlan-220)# vrrp vrid 220

ProVision(vlan-220-vrid-220)# owner
   (or 'backup' if not owner)

ProVision(vlan-220-vrid-220)# virtual-ip-address 10.1.220.1/24

ProVision(vlan-220-vrid-220)# enable


ProVision# show vrrp config

 VRRP Global Configuration Information

  VRRP Enabled    : Yes
  Traps Enabled   : Yes


 VRRP Virtual Router Configuration Information

  Vlan ID : 220
  Virtual Router ID : 220

  Administrative Status [Disabled] : Enabled
  Mode [Uninitialized] : Owner
  Priority [100] : 255
  Advertisement Interval [1] : 1
  Preempt Mode [True] : True
  Preempt Delay Time [0] : 0
  Primary IP Address : Lowest

  IP Address      Subnet Mask
  --------------- ---------------
  10.1.220.1      255.255.255.0


ProVision# show vrrp vlan 220

 VRRP Virtual Router Statistics Information

  Vlan ID                   : 220
  Virtual Router ID         : 220
  State                     : Master
  Up Time                   : 2 mins
  Virtual MAC Address       : 00005e-0001dc
  Master's IP Address       : 10.1.220.1
  Associated IP Addr Count : 1          Near Failovers            : 0
  Advertise Pkts Rx         : 0          Become Master             : 1
  Zero Priority Rx          : 0          Zero Priority Tx          : 0
  Bad Length Pkts           : 0          Bad Type Pkts             : 0
  Mismatched Interval Pkts : 0          Mismatched Addr List Pkts : 0
  Mismatched IP TTL Pkts    : 0          Mismatched Auth Type Pkts : 0
```

Comware 5

```
[Comware5]interface vlan 220

[Comware5-Vlan-interface220]vrrp vrid 220 virtual-ip 10.1.220.1

[Comware5-Vlan-interface220]vrrp vrid 220 priority 100


 [Comware5]display vrrp verbose
 IPv4 Standby Information:
 Run Method      : VIRTUAL-MAC
 Total number of virtual routers: 1
 Interface       : Vlan-interface220
 VRID            : 220                  Adver. Timer    : 1
 Admin Status    : UP                   State           : Backup
 Config Pri      : 100                  Run Pri         : 100
 Preempt Mode    : YES                  Delay Time      : 0
 Auth Type       : NONE
 Virtual IP      : 10.1.220.1
 Master IP       : 10.1.220.1


[Comware5]display vrrp
 IPv4 Standby Information:
 Run Method      : VIRTUAL-MAC
 Total number of virtual routers: 1
 Interface          VRID  State       Run     Adver.  Auth     Virtual
                                      Pri     Time    Type        IP
 ---------------------------------------------------------------------
 Vlan220              220 Backup      100     1       NONE     10.1.220.1


[Comware5]display vrrp interface Vlan-interface 220
 IPv4 Standby Information:
```

```
 Run Method      : VIRTUAL-MAC
 Total number of virtual routers on interface Vlan220: 1
 Interface          VRID  State       Run     Adver.  Auth     Virtual
                                      Pri     Time    Type        IP
 ---------------------------------------------------------------------
 Vlan220              220 Backup      100     1       NONE     10.1.220.1
```

Cisco

Very limited availability in Cisco product line

Cisco implements HSRP which is not compatible with VRRP

Chapter 23 ACLs

This chapter compares the commands for configuring access control lists (ACLs). When using these commands, keep in mind:

- On ProVision and Cisco, ACLs include an Implicit Deny. If traffic does not match an ACL rule, it is denied (or dropped).
- On Comware 5, ACLs include an Implicit Allow. If traffic does not match an ACL rule, it is allowed.

a) Standard or Basic ACLs and Extended or Advanced ACLs

ProVision

```
ProVision(config)# ip access-list standard
 NAME-STR               Specify name of Access Control List to configure.
 <1-99>                 Specify Access Control List to configure by number.

ProVision(config)# ip access-list extended
 NAME-STR               Specify name of Access Control List to configure.
 <100-199>              Specify Access Control List to configure by number.
```

Comware 5

```
[Comware5]acl number ?
  INTEGER<2000-2999>  Specify a basic acl
  INTEGER<3000-3999>  Specify an advanced acl
  INTEGER<4000-4999>  Specify an ethernet frame header acl

[Comware5]acl number <any-number> ?
  match-order  Set an acl's match order
  name         Specify a named acl
  <cr>
[Comware5]acl number 2000 name test2000
```

Cisco

```
Cisco(config)#ip access-list standard ?
  <1-99>        Standard IP access-list number
  <1300-1999>   Standard IP access-list number (expanded range)
  WORD          Access-list name

Cisco(config)#ip access-list extended ?
  <100-199>     Extended IP access-list number
  <2000-2699>   Extended IP access-list number (expanded range)
  WORD          Access-list name
```

b) ACL Fundamental Configuration Options

Standard/Basic

ProVision	Comware 5	Cisco
ProVision(config)# ip access-list standard 1	[Comware5]acl number 2000	Cisco(config)#ip access-list standard 1
ProVision(config-std-nacl)# permit 10.0.100.111 0.0.0.0	[Comware5-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ProVision(config)# ip access-list standard std_acl	[Comware5]acl number 2001 name test2001	Cisco(config)#ip access-list standard std_acl
ProVision(config-std-nacl)# permit 10.0.100.111/32	[Comware5-acl-basic-2001-test2001]rule permit source 10.0.100.111 0	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0

Extended/Advanced

ProVision	Comware 5	Cisco
ProVision(config)# ip access-list extended 100	[Comware5]acl number 3000	Cisco(config)#ip access-list extended 100
ProVision(config-ext-nacl)# deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0	[Comware5-acl-adv-3000]rule deny ip source 10.0.13.0 0.0.0.255 destination 10.0.100.111 0.0.0.0	Cisco(config-ext-nacl)#deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0
ProVision(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any
ProVision(config)# ip access-list extended ext_acl	[Comware5]acl number 3001 name test3001	Cisco(config)#ip access-list extended ext_acl
ProVision(config-ext-nacl)# deny ip 10.0.14.0/24 10.0.100.111/32	[Comware5-acl-adv-3001-test3001]rule deny ip source 10.0.14.0 0.0.0.255 destination 10.0.100.111 0	Cisco(config-ext-nacl)#deny ip 10.0.14.0 255.255.255.0 10.0.100.111 255.255.255.255
ProVision(config-ext-nacl)# permit ip any any		Cisco(config-ext-nacl)#permit ip any any

ProVision

```
              Standard ACL

ProVision(config)# ip access-list ?
 connection-rate-fi... Configure a connection-rate-filter Access Control List.
 extended              Configure an extended Access Control List.
 resequence            Renumber the entries in an Access Control List.
 standard              Configure a standard Access Control List.

ProVision(config)# ip access-list standard ?
 NAME-STR              Specify name of Access Control List to configure.
 <1-99>                Specify Access Control List to configure by number.

ProVision(config)# ip access-list standard 1

ProVision(config-std-nacl)# ?
 deny                  Deny packets matching <ACL-IP-SPEC-SRC>.
 permit                Permit packets matching <ACL-IP-SPEC-SRC>.
 remark                Insert a comment into an Access Control List.
 <1-2147483647>        Specify a sequence number for the ACE.
```

```
ProVision(config-std-nacl)# permit 10.0.100.111 0.0.0.0


ProVision(config)# ip access-list standard std_acl

ProVision(config-std-nacl)# permit 10.0.100.111/32



              Extended ACL

ProVision(config)# ip access-list ?
 connection-rate-fi... Configure a connection-rate-filter Access Control List.
 extended              Configure an extended Access Control List.
 resequence            Renumber the entries in an Access Control List.
 standard              Configure a standard Access Control List.

ProVision(config)# ip access-list extended ?
 NAME-STR              Specify name of Access Control List to configure.
 <100-199>             Specify Access Control List to configure by number.

ProVision(config)# ip access-list extended 100

ProVision(config-ext-nacl)# deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0

ProVision(config-ext-nacl)# permit ip any any


ProVision(config)# ip access-list extended ext_acl

ProVision(config-ext-nacl)# deny ip 10.0.14.0/24 10.0.100.111/32

ProVision(config-ext-nacl)# permit ip any any
```

Comware 5

```
              Basic ACL

[Comware5]acl ?
  copy     Specify a source acl
  ipv6     IPv6 acl
  logging  Log matched packet
  name     Specify a named acl
  number   Specify a numbered acl

[Comware5]acl number ?
  INTEGER<2000-2999>  Specify a basic acl
  INTEGER<3000-3999>  Specify an advanced acl
  INTEGER<4000-4999>  Specify an ethernet frame header acl

[Comware5]acl number 2000 ?
  match-order  Set an acl's match order
  name         Specify a named acl
  <cr>

[Comware5]acl number 2000

[Comware5-acl-basic-2000]?
Acl-basic view commands:
  description  Specify ACL description
  display      Display current system information
  mtracert     Trace route to multicast source
  ping         Ping function
  quit         Exit from current command view
  return       Exit to User View
  rule         Specify an acl rule
  save         Save current configuration
  step         Specify step of acl sub rule ID
  tracert      Trace route function
  undo         Cancel current setting

[Comware5-acl-basic-2000]rule ?
  INTEGER<0-65534>  ID of acl rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit

[Comware5-acl-basic-2000]rule permit ?
  fragment      Check fragment packet
  logging       Log matched packet
  source        Specify source address
  time-range    Specify a special time
  vpn-instance  Specify a VPN-Instance
  <cr>


[Comware5-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0


[Comware5]acl number 2001 name test2001

[Comware5-acl-basic-2001-test2001]rule permit source 10.0.100.111 0



             Advanced ACL

[Comware5]acl number ?
  INTEGER<2000-2999>  Specify a basic acl
  INTEGER<3000-3999>  Specify an advanced acl
  INTEGER<4000-4999>  Specify an ethernet frame header acl

[Comware5]acl number 3000 ?
  match-order  Set an acl's match order
  name         Specify a named acl
  <cr>

[Comware5]acl number 3000

[Comware5-acl-adv-3000]?
Acl-adv view commands:
  description  Specify ACL description
  display      Display current system information
  mtracert     Trace route to multicast source
  ping         Ping function
  quit         Exit from current command view
  return       Exit to User View
  rule         Specify an acl rule
  save         Save current configuration
  step         Specify step of acl sub rule ID
  tracert      Trace route function
  undo         Cancel current setting

[Comware5-acl-adv-3000]rule ?
  INTEGER<0-65534>  ID of acl rule
  deny              Specify matched packet deny
  permit            Specify matched packet permit

[Comware5-acl-adv-3000]rule deny ?
  <0-255>  Protocol number
  gre      GRE tunneling(47)
  icmp     Internet Control Message Protocol(1)
  igmp     Internet Group Management Protocol(2)
  ip       Any IP protocol
  ipinip   IP in IP tunneling(4)
  ospf     OSPF routing protocol(89)
  tcp      Transmission Control Protocol (6)
  udp      User Datagram Protocol (17)

[Comware5-acl-adv-3000]rule deny ip ?
  destination   Specify destination address
  dscp          Specify DSCP
  fragment      Check fragment packet
  logging       Log matched packet
  precedence    Specify precedence
  source        Specify source address
  time-range    Specify a special time
  tos           Specify tos
  vpn-instance  Specify a VPN-Instance
  <cr>

[Comware5-acl-adv-3000]rule deny ip source ?
  X.X.X.X  Address of source
  any      Any source IP address

[Comware5-acl-adv-3000]rule deny ip source 10.0.13.0 0.0.0.255 ?
  destination   Specify destination address
  dscp          Specify DSCP
  fragment      Check fragment packet
  logging       Log matched packet
  precedence    Specify precedence
  time-range    Specify a special time
  tos           Specify tos
  vpn-instance  Specify a VPN-Instance
  <cr>

[Comware5-acl-adv-3000]rule deny ip source 10.0.13.0 0.0.0.255 destination ?
  X.X.X.X  Address of destination
  any      Any destination IP address

[Comware5-acl-adv-3000]rule deny ip source 10.0.13.0 0.0.0.255 destination 10.0.100.
111 0.0.0.0
```

```
[Comware5]acl number 3001 name test3001

[Comware5-acl-adv-3001-test3001]rule deny ip source 10.0.14.0 0.0.0.255 destination
10.0.100.111 0
```

Cisco

```
             Standard ACL

Cisco(config)#ip access-list ?
  extended    Extended Access List
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  standard    Standard Access List

Cisco(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name


Cisco(config)#ip access-list standard 1

Cisco(config-std-nacl)#?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment


Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0


Cisco(config)#ip access-list standard std_acl

Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0




             Extended ACL

Cisco(config)#ip access-list ?
  extended    Extended Access List
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  standard    Standard Access List

Cisco(config)#ip access-list extended ?
  <100-199>    Extended IP access-list number
  <2000-2699>  Extended IP access-list number (expanded range)
  WORD         Access-list name


Cisco(config)#ip access-list extended 100

Cisco(config-ext-nacl)#deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0

Cisco(config-ext-nacl)#permit ip any any
Cisco(config)#ip access-list extended ext_acl

Cisco(config-ext-nacl)#deny ip 10.0.14.0 255.255.255.0 10.0.100.111 255.255.255.255

Cisco(config-ext-nacl)#permit ip any any
```

c) Routed/Layer 3 ACL (RACL)

On ProVision, an RACL is configured on a VLAN to filter:

- Routed traffic arriving on or being sent from the switch on that interface
- Traffic with a destination on the switch itself

On Comware 5 , you can apply a quality of service (QoS) policy to a Layer 3 interface to regulate traffic in a specific direction (inbound or outbound).

On Cisco, RACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).

Standard or Basic ACL

ProVision	Comware 5	Cisco
ProVision(config)# ip access-list standard 1	Step-1	Cisco(config)#ip access-list standard 1
ProVision(config-std-nacl)# permit 10.0.100.111 0.0.0.0	[Comware5]acl number 2000	Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0
ProVision(config-std-nacl)# vlan 230	[Comware5-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0	Cisco(config-std-nacl)#interface vlan 230
ProVision(vlan-230)# ip access-group 1 in	Step-2	Cisco(config-if)#ip access-group 1 in
ProVision(config)# vlan 240	[Comware5]traffic classifier srvr111	Cisco(config)#interface vlan 240
ProVision(vlan-240)# ip access-group std_acl in	[Comware5-classifier-srvr111]if-match acl 2000	Cisco(config-if)#ip access-group std_acl in
	Step-3	
	[Comware5]traffic behavior perm_stats	
	[Comware5-behavior-perm_stats]filter permit	
	[Comware5-behavior-perm_stats]accounting	
	Step-4	
	[Comware5]qos policy srvr1	
	[Comware5-qospolicy-srvr1]classifier srvr111 behavior perm_stats	
	Step-5	
	[Comware5]qos apply policy srvr1 global inbound	

Extended or Advanced ACL

ProVision	Comware 5	Cisco
ProVision(config)# ip access-list extended 100	Step-1	Cisco(config)#ip access-list extended 100
ProVision(config-ext-nacl)# deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0	[Comware5]acl number 3220	Cisco(config-ext-nacl)#deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0
ProVision(config-ext-nacl)# permit ip any any	[Comware5-acl-adv-3220]rule deny ip source 10.1.220.100 0 destination 10.1.100.111 0	Cisco(config-ext-nacl)#permit ip any any
ProVision(config)# ip access-list extended ext_acl	Step-2	Cisco(config)#ip access-list extended ext_acl

ProVision(config-ext-nacl)# deny ip 10.0.14.0/24 10.0.100.111/32	[Comware5]traffic classifier pc12srvr	Cisco(config-ext-nacl)#deny ip 10.0.14.0 255.255.255.0 10.0.100.111 255.255.255.255
ProVision(config-ext-nacl)# permit ip any any	[Comware5-classifier-pc12srvr]if-match acl 3220	Cisco(config-ext-nacl)#permit ip any any
ProVision(config)# vlan 230	Step-3	Cisco(config-ext-nacl)#interface vlan 230
ProVision(vlan-230)# ip access-group 100 in	[Comware5]traffic behavior deny_stats	Cisco(config-if)#ip access-group 100 in
ProVision(vlan-230)# vlan 240	[Comware5-behavior-deny_stats]filter deny	Cisco(config-if)#interface vlan 240
ProVision(vlan-240)# ip access-group ext_acl in	[Comware5-behavior-deny_stats]accounting	Cisco(config-if)#ip access-group ext_acl in
	Step-4	
	[Comware5]qos policy pc1acl	
	[Comware5-qospolicy-pc1acl]classifier pc12srvr behavior deny_stats	
	Step-5	
	[Comware5]qos apply policy pc1acl global inbound	

ProVision

```
              Standard ACL

ProVision(config)# ip access-list standard 1

ProVision(config-std-nacl)# permit 10.0.100.111 0.0.0.0


ProVision(config-std-nacl)# vlan 230

ProVision(vlan-230)# ip access-group ?
 ASCII-STR              Enter an ASCII string for the 'access-group'
                        command/parameter.

ProVision(vlan-230)# ip access-group 1 ?
 in                     Match inbound packets
 out                    Match outbound packets
 connection-rate-filter Manage packet rates
 vlan                   VLAN acl

ProVision(vlan-230)# ip access-group 1 in


ProVision(config)# vlan 240

ProVision(vlan-240)# ip access-group std_acl ?
 in                     Match inbound packets
 out                    Match outbound packets
 connection-rate-filter Manage packet rates
 vlan                   VLAN acl

ProVision(vlan-240)# ip access-group std_acl in ?
 <cr>

ProVision(vlan-240)# ip access-group std_acl in



              Extended ACL
```

```
ProVision(config)# ip access-list extended 100

ProVision(config-ext-nacl)# deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0

ProVision(config-ext-nacl)# permit ip any any


ProVision(config)# ip access-list extended ext_acl

ProVision(config-ext-nacl)# deny ip 10.0.14.0/24 10.0.100.111/32

ProVision(config-ext-nacl)# permit ip any any


ProVision(config)# vlan 230

ProVision(vlan-230)# ip access-group 100 in


ProVision(vlan-230)# vlan 240

ProVision(vlan-240)# ip access-group ext_acl in
```

Comware 5

```
             Basic ACL
step-1

[Comware5]acl number 2000

[Comware5-acl-basic-2000]rule permit source 10.0.100.111 0.0.0.0


step-2

[Comware5]traffic ?
  behavior    Specify traffic behavior
  classifier  Specify traffic classifier

[Comware5]traffic classifier ?
  STRING<1-31>  Name of classifier

[Comware5]traffic classifier srvr111 ?
  operator  Specify the operation relation for classification rules
  <cr>

[Comware5]traffic classifier srvr111

[Comware5-classifier-srvr111]?
Classifier view commands:
  display   Display current system information
  if-match  Specify matching statement for classification
  mtracert  Trace route to multicast source
  ping      Ping function
  quit      Exit from current command view
  return    Exit to User View
  save      Save current configuration
  tracert   Trace route function
  undo      Cancel current setting
```

```
[Comware5-classifier-srvr111]if-match ?
  acl               Specify ACL to match
  any               Specify any packets to match
  customer-dot1p    Specify IEEE 802.1p customer COS to match
  customer-vlan-id  Specify customer VLAN ID to match
  destination-mac   Specify destination MAC address to match
  dscp              Specify DSCP (DiffServ CodePoint) to match
  ip-precedence     Specify IP precedence to match
  protocol          Specify protocol to match
  service-dot1p     Specify IEEE 802.1p service COS to match
  service-vlan-id   Specify service VLAN ID to match
  source-mac        Specify source MAC address to match

[Comware5-classifier-srvr111]if-match acl ?
  INTEGER<2000-3999>  Apply basic or advanced acl
  INTEGER<4000-4999>  Apply ethernet frame header acl
  ipv6                Specify IPv6 acl number
  name                Specify a named acl

[Comware5-classifier-srvr111]if-match acl 2000 ?
  <cr>

[Comware5-classifier-srvr111]if-match acl 2000


step-3

[Comware5]traffic behavior ?
  STRING<1-31>  Name of behavior

[Comware5]traffic behavior perm_stats

[Comware5-behavior-perm_stats]?
Behavior view commands:
  accounting  Specify Accounting feature
  car         Specify CAR (Committed Access Rate) feature
  display     Display current system information
  filter      Specify packet filter feature
  mirror-to   Specify flow mirror feature
  mtracert    Trace route to multicast source
  nest        Nest top-most VLAN TAG or customer VLAN TAG
  ping        Ping function
  quit        Exit from current command view
  redirect    Specify Redirect feature
  remark      Remark QoS values of the packet
  return      Exit to User View
  save        Save current configuration
  tracert     Trace route function
  undo        Cancel current setting

[Comware5-behavior-perm_stats]filter ?
  deny    Specify filter deny
  permit  Specify filter permit

[Comware5-behavior-perm_stats]filter permit ?
  <cr>
```

```
[Comware5-behavior-perm_stats]filter permit

[Comware5-behavior-perm_stats]accounting ?
  <cr>

[Comware5-behavior-perm_stats]accounting


step-4

[Comware5]qos policy ?
  STRING<1-31>  Name of QoS policy

[Comware5]qos policy srvr1 ?
  <cr>

[Comware5]qos policy srvr1

[Comware5-qospolicy-srvr1]?
Qospolicy view commands:
  classifier  Specify the classifier to which policy relates
  display     Display current system information
  mtracert    Trace route to multicast source
  ping        Ping function
  quit        Exit from current command view
  return      Exit to User View
  save        Save current configuration
  tracert     Trace route function
  undo        Cancel current setting

[Comware5-qospolicy-srvr1]classifier srvr111 ?
  behavior  Specify traffic behavior

[Comware5-qospolicy-srvr1]classifier srvr111 behavior perm_stats ?
  mode  Specify the classifier-behavior mode
  <cr>

[Comware5-qospolicy-srvr1]classifier srvr111 behavior perm_stats


step-5

[Comware5]qos apply ?
  policy  Specify QoS policy

[Comware5]qos apply policy ?
  STRING<1-31>  Name of QoS policy

[Comware5]qos apply policy srvr1 ?
  global  Apply specific QoS policy globally

[Comware5]qos apply policy srvr1 global ?
  inbound   Assign policy to the inbound
  outbound  Assign policy to the outbound

[Comware5]qos apply policy srvr1 global inbound ?
```

```
  <cr>

[Comware5]qos apply policy srvr1 global inbound


             Advanced ACL

step-1

[Comware5]acl number 3220

[Comware5-acl-adv-3220]rule deny ip source 10.1.220.100 0 destination 10.1.100.111 0


step-2

[Comware5]traffic ?
  behavior    Specify traffic behavior
  classifier  Specify traffic classifier

[Comware5]traffic classifier ?
  STRING<1-31>  Name of classifier

[Comware5]traffic classifier pc12srvr ?
  operator  Specify the operation relation for classification rules
  <cr>

[Comware5]traffic classifier pc12srvr

[Comware5-classifier-pc12srvr]?
Classifier view commands:
  display   Display current system information
  if-match  Specify matching statement for classification
  mtracert  Trace route to multicast source
  ping      Ping function
  quit      Exit from current command view
  return    Exit to User View
  save      Save current configuration
  tracert   Trace route function
  undo      Cancel current setting

[Comware5-classifier-pc12srvr]if-match ?
  acl               Specify ACL to match
  any               Specify any packets to match
  customer-dot1p    Specify IEEE 802.1p customer COS to match
  customer-vlan-id  Specify customer VLAN ID to match
  destination-mac   Specify destination MAC address to match
  dscp              Specify DSCP (DiffServ CodePoint) to match
  ip-precedence     Specify IP precedence to match
  protocol          Specify protocol to match
  service-dot1p     Specify IEEE 802.1p service COS to match
  service-vlan-id   Specify service VLAN ID to match
  source-mac        Specify source MAC address to match

[Comware5-classifier-pc12srvr]if-match acl ?
  INTEGER<2000-3999>  Apply basic or advanced acl
  INTEGER<4000-4999>  Apply ethernet frame header acl
  ipv6                Specify IPv6 acl number
  name                Specify a named acl

[Comware5-classifier-pc12srvr]if-match acl 3220 ?
  <cr>

[Comware5-classifier-pc12srvr]if-match acl 3220


step-3

[Comware5]traffic behavior ?
  STRING<1-31>  Name of behavior

[Comware5]traffic behavior deny_stats ?
  <cr>

[Comware5]traffic behavior deny_stats

[Comware5-behavior-deny_stats]?
Behavior view commands:
  accounting  Specify Accounting feature
  car         Specify CAR (Committed Access Rate) feature
  display     Display current system information
  filter      Specify packet filter feature
  mirror-to   Specify flow mirror feature
  mtracert    Trace route to multicast source
  nest        Nest top-most VLAN TAG or customer VLAN TAG
  ping        Ping function
  quit        Exit from current command view
  redirect    Specify Redirect feature
  remark      Remark QoS values of the packet
  return      Exit to User View
  save        Save current configuration
  tracert     Trace route function
  undo        Cancel current setting

[Comware5-behavior-deny_stats]filter ?
  deny    Specify filter deny
  permit  Specify filter permit

[Comware5-behavior-perm_stats]filter deny ?
  <cr>

[Comware5-behavior-deny_stats]filter deny

[Comware5-behavior-deny_stats]accounting ?
  <cr>

[Comware5-behavior-deny_stats]accounting


step-4

[Comware5]qos policy ?
  STRING<1-31>  Name of QoS policy
```

```
[Comware5]qos policy pc1acl ?
  <cr>

[Comware5]qos policy pc1acl

[Comware5-qospolicy-pc1acl]?
Qospolicy view commands:
  classifier  Specify the classifier to which policy relates
  display     Display current system information
  mtracert    Trace route to multicast source
  ping        Ping function
  quit        Exit from current command view
  return      Exit to User View
  save        Save current configuration
  tracert     Trace route function
  undo        Cancel current setting

[Comware5-qospolicy-pc1acl]classifier ?
  STRING<1-31>  Name of classifier

[Comware5-qospolicy-pc1acl]classifier pc12srvr ?
  behavior  Specify traffic behavior

[Comware5-qospolicy-pc1acl]classifier pc12srvr behavior ?
  STRING<1-31>  Name of behavior

[Comware5-qospolicy-pc1acl]classifier pc12srvr behavior deny_stats ?
  mode  Specify the classifier-behavior mode
  <cr>

[Comware5-qospolicy-pc1acl]classifier pc12srvr behavior deny_stats


step-5

[Comware5]qos apply ?
  policy  Specify QoS policy

[Comware5]qos apply policy ?
  STRING<1-31>  Name of QoS policy

[Comware5]qos apply policy pc1acl ?
  global  Apply specific QoS policy globally

[Comware5]qos apply policy pc1acl global ?
  inbound   Assign policy to the inbound
  outbound  Assign policy to the outbound

[Comware5]qos apply policy pc1acl global inbound ?
  <cr>

[Comware5]qos apply policy pc1acl global inbound
```

Cisco

```
             Standard ACL

Cisco(config)#ip access-list standard 1
Cisco(config-std-nacl)#permit 10.0.100.111 0.0.0.0


Cisco(config-std-nacl)#interface vlan 230

Cisco(config-if)#ip access-group ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

Cisco(config-if)#ip access-group 1 ?
  in   inbound packets
  out  outbound packets

Cisco(config-if)#ip access-group 1 in


Cisco(config)#interface vl 240

Cisco(config-if)#ip access-group std_acl ?
  in   inbound packets
  out  outbound packets

Cisco(config-if)#ip access-group std_acl in ?
  <cr>

Cisco(config-if)#ip access-group std_acl in



             Extended ACL

Cisco(config)#ip access-list extended 100

Cisco(config-ext-nacl)#deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0

Cisco(config-ext-nacl)#permit ip any any


Cisco(config)#ip access-list extended ext_acl

Cisco(config-ext-nacl)#deny ip 10.0.14.0 255.255.255.0 10.0.100.111 255.255.255.255

Cisco(config-ext-nacl)#permit ip any any


Cisco(config-ext-nacl)#interface vlan 230

Cisco(config-if)#ip access-group 100 in


Cisco(config-if)#interface vlan 240

Cisco(config-if)#ip access-group ext_acl in
```

c) VLAN/Layer 2 Based ACL (VACL)

On ProVision, a VACL is an ACL that is configured on a VLAN to filter traffic entering the switch on that VLAN interface and having a destination on the same VLAN.

On Comware 5, you can apply a quality of service (QoS) policy to a VLAN to regulate VLAN traffic in a specific direction (inbound or outbound).

On Cisco, VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv4. Unsupported protocols are access-controlled through MAC addresses using Ethernet access control entries (ACEs). After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port.

Standard or Basic ACL

ProVision	Comware 5	Cisco
ProVision(config)# ip access-list standard 1	Step-1	Step - 1
ProVision(config-std-nacl)# permit 10.0.100.111 0.0.0.0	[Comware5]acl number 2220	Cisco(config)#access-list 10 permit host 10.1.220.102
ProVision(config-std-nacl)# vlan 230	[Comware5-acl-basic-2220]rule deny source 10.1.220.100 0	Step - 2
ProVision(vlan-230)# ip access-group 1 vlan	Step-2	Cisco(config)#vlan access-map vacl_1 10
ProVision(vlan-230)# vlan 240	[Comware5]traffic classifier pc1	Cisco(config-access-map)#match ip address 10
ProVision(vlan-240)# ip access-group std_acl vlan	[Comware5-classifier-pc1]if-match acl 2220	Cisco(config-access-map)#action drop
	Step-3	Step - 3
	[Comware5]traffic behavior deny_stats	Cisco(config)#vlan filter vacl_1 vlan-list 220
	[Comware5-behavior-deny_stats]filter deny	
	[Comware5-behavior-deny_stats]accounting	
	Step-4	
	[Comware5]qos policy pc1_deny	
	[Comware5-qospolicy-pc1_deny]classifier pc1 behavior deny_stats	
	Step-5	
	[Comware5]qos vlan-policy pc1_deny vlan 220 inbound	

Extended or Advanced ACL

ProVision	Comware 5	Cisco
ProVision(config)# ip access-list extended 100	Step - 1	Step - 1
ProVision(config-ext-nacl)# deny ip 10.0.13.0 0.0.0.255 10.0.100.111 0.0.0.0	[Comware5]acl number 3221	Cisco(config)#access-list 110 permit icmp any host 10.1.220.2

ProVision(config-ext-nacl)# permit ip any any	[Comware5-acl-adv-3221]rule deny ip source 10.1.220.100 0 destination 10.1.220.101 0	Cisco(config)#access-list 111 permit icmp any any
ProVision(config)# ip access-list extended ext_acl	Step - 2	Step - 2
ProVision(config-ext-nacl)# deny ip 10.0.14.0/24 10.0.100.111/32	[Comware5]traffic classifier pc12pc2	Cisco(config)#vlan access-map vacl_2 10
ProVision(config-ext-nacl)# permit ip any any	[Comware5-classifier-pc12pc2]if-match acl 3221	Cisco(config-access-map)#match ip address 110
ProVision(config)# vlan 230	Step - 3	Cisco(config-access-map)#action drop
ProVision(vlan-230)# ip access-group 100 vlan	[Comware5]traffic behavior deny_stats_2	Cisco(config)#vlan access-map vacl_2 20
ProVision(vlan-230)# vlan 240	[Comware5-behavior-deny_stats_2]filter deny	Cisco(config-access-map)#match ip address 111
ProVision(vlan-240)# ip access-group ext_acl vlan	[Comware5-behavior-deny_stats_2]accounting	Cisco(config-access-map)#action forward
	Step - 4	Step - 3
	[Comware5]qos policy pc1acl2	Cisco(config)#vlan filter vacl_2 vlan-list 220
	[Comware5-qospolicy-pc1acl2]classifier pc12pc2 behavior deny_stats_2	
	[Comware5]qos vlan-policy pc1acl2 vlan 220 inbound	

ProVision

```
             Standard ACL

ProVision(config)# vlan 230

ProVision(vlan-230)# ip access-group 1 ?
 in                     Match inbound packets
 out                    Match outbound packets
 connection-rate-filter Manage packet rates
 vlan                   VLAN acl

ProVision(vlan-230)# ip access-group 1 vlan

ProVision(vlan-230)# vlan 240

ProVision(vlan-240)# ip access-group std_acl vlan



             Extended ACL

ProVision(vlan-230)# ip access-group 100 ?
 in                     Match inbound packets
 out                    Match outbound packets ?
 connection-rate-filter Manage packet rates
 vlan                   VLAN acl

ProVision(vlan-230)# ip access-group 100 vlan

ProVision(vlan-230)# vlan 240

ProVision(vlan-240)# ip access-group ext_acl vlan
```

Comware 5

```
             Basic ACL
step-1

[Comware5]acl number 2220

[Comware5-acl-basic-2220]rule deny source 10.1.220.100 0


step-2

[Comware5]traffic classifier pc1

[Comware5-classifier-pc1]if-match acl 2220


step-3

[Comware5]traffic behavior deny_stats

[Comware5-behavior-deny_stats]filter deny

[Comware5-behavior-deny_stats]accounting


step-4

[Comware5]qos policy pc1_deny

[Comware5-qospolicy-pc1_deny]classifier pc1 behavior deny_stats


step-5

[Comware5]qos vlan-policy pc1_deny vlan 220 inbound



             Advanced ACL
step-1

[Comware5]acl number 3221

[Comware5-acl-adv-3221]rule deny ip source 10.1.220.100 0 destination 10.1.220.101 0


step-2

[Comware5]traffic classifier pc12pc2

[Comware5-classifier-pc12pc2]if-match acl 3221


step-3
```

```
[Comware5]traffic behavior deny_stats_2

[Comware5-behavior-deny_stats_2]filter deny

[Comware5-behavior-deny_stats_2]accounting


step-4

[Comware5]qos policy pc1acl2

[Comware5-qospolicy-pc1acl2]classifier pc12pc2 behavior deny_stats_2


step-5

[Comware5]qos vlan-policy pc1acl2 vlan 220 inbound
```

Cisco

```
             Standard ACL
step-1

Cisco(config)#access-list 10 permit host 10.1.220.102


step-2

Cisco(config)#vlan access-map ?
  WORD  Vlan access map tag

Cisco(config)#vlan access-map vacl_1 ?
  <0-65535>  Sequence to insert to/delete from existing vlan access-map entry
  <cr>

Cisco(config)#vlan access-map vacl_1 10

Cisco(config-access-map)#?
Vlan access-map configuration commands:
  action   Take the action
  default  Set a command to its defaults
  exit     Exit from vlan access-map configuration mode
  match    Match values.
  no       Negate a command or set its defaults


Cisco(config-access-map)#match ip address ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

Cisco(config-access-map)#match ip address 10

Cisco(config-access-map)#action ?
  drop     Drop packets
  forward  Forward packets

Cisco(config-access-map)#action drop ?
  <cr>

Cisco(config-access-map)#action drop
```

```
step-3

Cisco(config)#vlan filter vacl_1 vlan-list 220


             Extended ACL
step-1

Cisco(config)#access-list 110 permit icmp any host 10.1.220.2

Cisco(config)#access-list 111 permit icmp any any


step-2

Cisco(config)#vlan access-map ?
  WORD  Vlan access map tag

Cisco(config)#vlan access-map vacl_2 ?
  <0-65535>  Sequence to insert to/delete from existing vlan access-map entry
  <cr>

Cisco(config)#vlan access-map vacl_2 10 ?
  <cr>

Cisco(config)#vlan access-map vacl_2 10


Cisco(config-access-map)#?
Vlan access-map configuration commands:
  action   Take the action
  default  Set a command to its defaults
  exit     Exit from vlan access-map configuration mode
  match    Match values.
  no       Negate a command or set its defaults

Cisco(config-access-map)#match ip address ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

Cisco(config-access-map)#match ip address 110


Cisco(config-access-map)#action ?
  drop     Drop packets
  forward  Forward packets

Cisco(config-access-map)#action drop ?
  <cr>

Cisco(config-access-map)#action drop

Cisco(config-access-map)#exit

Cisco(config)#vlan access-map vacl_2 20

Cisco(config-access-map)#match ip address 111

Cisco(config-access-map)#action forward


step-3
```

```
Cisco(config)#vlan filter vacl_2 vlan-list 220
```

d) Port ACL (PACL)

On ProVision, a static PACL is configured on a port to filter traffic entering the switch on that port, regardless of whether the traffic is routed, switched, or addressed to a destination on the switch itself.

On Comware 5, a single QoS policy can be applied to an interface in a specific direction (inbound or outbound).

On Cisco, a PACL access-controls traffic entering a Layer 2 interface.

Standard or Basic ACL

ProVision	Comware 5	Cisco
`ProVision(eth-6)# ip access-group 1 in`	`[Comware5]interface g1/0/18`	`Cisco(config)#interface f0/5`
`ProVision(eth-6)# ip access-group std_acl in`	`[Comware5-GigabitEthernet1/0/18]qos apply policy pc1_deny in`	`Cisco(config-if)#ip access-group 11 in`

Extended or Advanced ACL

ProVision	Comware 5	Cisco
`ProVision(eth-6)# ip access-group 100 in`	`[Comware5]interface g1/0/18`	`Cisco(config)#interface f0/5`
`ProVision(eth-6)# ip access-group ext_acl in`	`[Comware5-GigabitEthernet1/0/18]qos apply policy pc1acl in`	`Cisco(config-if)#ip access-group 101 in`

ProVision

```
             Standard ACL

ProVision(eth-6)# ip access-group 1 in

ProVision(eth-6)# ip access-group std_acl in


             Extended ACL

ProVision(eth-6)# ip access-group 100 in

ProVision(eth-6)# ip access-group ext_acl in
```

Comware 5

```
             Basic ACL

[Comware5]interface g1/0/18

[Comware5-GigabitEthernet1/0/18]qos apply policy pc1_deny in



             Advanced ACL

[Comware5]interface g1/0/18

[Comware5-GigabitEthernet1/0/18]qos apply policy pc1acl in
```

Cisco

```
             Standard ACL

Cisco(config)#interface f0/5

Cisco(config-if)#ip access-group 11 in



             Extended ACL

Cisco(config)#interface f0/5

Cisco(config-if)#ip access-group 101 in
```

Chapter 24 QoS

This chapter compares the commands used to configure quality of service (QoS) on the ProVision, Comware 5, and Cisco operating systems.

QoS Operational Characteristics

	ProVision	Comware 5	Cisco
QoS default	Enabled by default and operates based on 802.1p setting in packet	Enabled by default and operates based on 802.1p setting in packet	Disabled by default
Classification	Configured primarily on a global basis. Can be configured globally, on VLAN and on port	Configured per port or on VLAN with QoS policy	Configured per port or on SVI
Marking	Configured primarily on a global basis. Some configuration options can be set globally and some also set at VLAN or port	Configured globally, VLAN or port, using QoS policy	Configured per port or on SVI
Queue Scheduling	Configured per port	Configured per port	Configured per port or on SVI

a) QoS

ProVision	Comware 5	Cisco
		Cisco(config)#mls qos
	[Comware5]interface g1/0/6	Cisco(config)#interface f0/5
	[Comware5-GigabitEthernet1/0/6]qos trust dscp	Cisco(config-if)#mls qos trust dscp
ProVision(config)# qos type-of-service diff-services		Cisco(config)#mls qos map dscp-cos 0 8 16 24 32 40 48 56 to 0
ProVision(config)# interface 6	[Comware5]interface g1/0/6	Cisco(config)#interface f0/5
ProVision(eth-6)# qos priority 6	[Comware5-GigabitEthernet1/0/6]qos priority 6	Cisco(config-if)#mls qos cos 6
ProVision(config)# vlan 220	Step-1	
ProVision(vlan-220)# qos priority 6	[Comware5]traffic classifier any	
	[Comware5-classifier-any]if-match any	
	Step-2	
	[Comware5]traffic behavior pri6	
	[Comware5-behavior-pri6]remark dot1p 6	
	[Comware5-behavior-pri6]accounting	
	Step-3	
	[Comware5]qos policy any-pri6	
	[Comware5-qospolicy-any-pri6]classifier any behavior pri6	
	Step-4	

	[Comware5]qos vlan-policy any-pri6 vlan 220 inbound	
ProVision# show qos ?	[Comware5]display qos ?	Cisco#show mls qos ?

ProVision

```
ProVision(config)# qos ?
 udp-port               Set UDP port based priority.
 tcp-port               Set TCP port based priority.
 device-priority        Configure device-based priority.
 dscp-map               Define mapping between a DSCP (Differentiated-Services
                        Codepoint) value and an 802.1p priority.
 protocol               Configure protocol-based priority.
 queue-config           Sets the number of outbound port queues that buffer the
                        packets depending on their 802.1p priority.
 type-of-service        Configure the Type-of-Service method the device uses to
                        prioritize IP traffic.


ProVision(config)# qos type-of-service diff-services


ProVision(config)# interface 6

ProVision(eth-6)# qos ?
 dscp                   Specify DSCP policy to use.
 priority               Specify priority to use.

ProVision(eth-6)# qos priority 6


ProVision(config)# vlan 220

ProVision(vlan-220)# qos ?
 dscp                   Specify DSCP policy to use.
 priority               Specify priority to use.

ProVision(vlan-220)# qos priority 6


ProVision# show qos ?
 device-priority        Show the device priority table (priority based on the IP
                        addresses).
 dscp-map               Show mappings between DSCP policy and 802.1p priority.
 port-priority          Show the port-based priority table.
 protocol-priority      Show the protocol priority.
 queue-config           Displays outbound port queues configuration information.
 resources              Show the qos resources.
 tcp-udp-port-priority  Show TCP/UDP port priorities.
 type-of-service        Show QoS priorities based on IP Type-of-Service.
 vlan-priority          Show the VLAN-based priority table.
```

Comware 5

```
[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]qos

[Comware5-GigabitEthernet1/0/6]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Queue bandwidth
  gts        Apply GTS(Generic Traffic Shaping) policy on interface
  lr         Apply LR(Line Rate) policy on physical interface
  priority   Configure port priority
  sp         Configure strict priority queue
  trust      Configure priority trust mode
  wfq        Configure weighted fair queue
  wred       Apply WRED(Weighted Random Early Detection) configuration
             information
  wrr        Configure weighted round robin queue

[Comware5-GigabitEthernet1/0/6]qos trust ?
  dot1p  Trust 802.1p Precedence
  dscp   Trust DSCP

[Comware5-GigabitEthernet1/0/6]qos trust dscp ?
  <cr>

[Comware5-GigabitEthernet1/0/6]qos trust dscp


[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Queue bandwidth
  gts        Apply GTS(Generic Traffic Shaping) policy on interface
  lr         Apply LR(Line Rate) policy on physical interface
  priority   Configure port priority
  sp         Configure strict priority queue
  trust      Configure priority trust mode
  wfq        Configure weighted fair queue
  wred       Apply WRED(Weighted Random Early Detection) configuration
             information
  wrr        Configure weighted round robin queue

[Comware5-GigabitEthernet1/0/6]qos priority ?
  INTEGER<0-7>  Port priority value

[Comware5-GigabitEthernet1/0/6]qos priority 6


Step-1

[Comware5]traffic classifier any
[Comware5-classifier-any]?
Classifier view commands:
  display   Display current system information
  if-match  Specify matching statement for classification
  mtracert  Trace route to multicast source
  ping      Ping function
  quit      Exit from current command view
  return    Exit to User View
  save      Save current configuration
  tracert   Trace route function
  undo      Cancel current setting

[Comware5-classifier-any]if-m
[Comware5-classifier-any]if-match ?
```

```
  acl                Specify ACL to match
  any                Specify any packets to match
  customer-dot1p     Specify IEEE 802.1p customer COS to match
  customer-vlan-id   Specify customer VLAN ID to match
  destination-mac    Specify destination MAC address to match
  dscp               Specify DSCP (DiffServ CodePoint) to match
  ip-precedence      Specify IP precedence to match
  protocol           Specify protocol to match
  service-dot1p      Specify IEEE 802.1p service COS to match
  service-vlan-id    Specify service VLAN ID to match
  source-mac         Specify source MAC address to match

[Comware5-classifier-any]if-match any


Step-2

[Comware5]traffic behavior pri6

[Comware5-behavior-pri6]?
Behavior view commands:
  accounting  Specify Accounting feature
  car         Specify CAR (Committed Access Rate) feature
  display     Display current system information
  filter      Specify packet filter feature
  mirror-to   Specify flow mirror feature
  mtracert    Trace route to multicast source
  nest        Nest top-most VLAN TAG or customer VLAN TAG
  ping        Ping function
  quit        Exit from current command view
  redirect    Specify Redirect feature
  remark      Remark QoS values of the packet
  return      Exit to User View
  save        Save current configuration
  tracert     Trace route function
  undo        Cancel current setting

[Comware5-behavior-pri6]remark ?
  customer-vlan-id  Remark Customer VLAN ID
  dot1p             Remark IEEE 802.1p COS
  drop-precedence   Remark drop precedence
  dscp              Remark DSCP (DiffServ CodePoint)
  ip-precedence     Remark IP precedence
  local-precedence  Remark local precedence
  service-vlan-id   Remark service VLAN ID

[Comware5-behavior-pri6]remark dot1p ?
  INTEGER<0-7>  Value of IEEE 802.1p COS

[Comware5-behavior-pri6]remark dot1p 6 ?
  <cr>

[Comware5-behavior-pri6]remark dot1p 6

[Comware5-behavior-pri6]accounting
```

```
Step-3

[Comware5]qos policy any-pri6

[Comware5-qospolicy-any-pri6]classifier any behavior pri6


Step-4

[Comware5]qos vlan-policy any-pri6 vlan 220 inbound



[Comware5]display qos ?
  gts          GTS(Generic Traffic Shaping) policy on interface
  lr           LR(Line Rate) policy on physical interface
  map-table    Priority map table configuration information
  policy       QoS policy configuration information
  sp           SP(strict priority queue) on port
  trust        Priority trust information
  vlan-policy  Vlan-policy configuration information
  wfq          Hardware WFQ(hardware weighted fair queue) on port
  wred         WRED(Weighted Random Early Detect) on interface
  wrr          WRR(weighted round robin queue) on port
```

Cisco

```
Cisco(config)#mls qos

Cisco(config)#interface f0/5

Cisco(config-if)#mls qos trust dscp


Cisco(config)#mls qos map dscp-cos 0 8 16 24 32 40 48 56 to 0

Cisco(config)#interface f0/5

Cisco(config-if)#mls qos ?
  cos             cos keyword
  dscp-mutation   dscp-mutation keyword
  ipe             ipe keyword
  trust           trust keyword
  vlan-based      vlan-based keyword


Cisco(config-if)#mls qos cos ?
  <0-7>     class of service value between 0 and 7
  override  override keyword

Cisco(config-if)#mls qos cos 6


Cisco#show mls qos ?
  aggregate-policer  aggregate-policer keyword
  input-queue        input-queue keyword
  interface          interface keyword
  maps               maps keyword
  queue-set          queue-set keyword
  vlan               VLAN keyword
  |                  Output modifiers
  <cr>
```

b) Rate Limiting

ProVision	Comware 5	Cisco
ProVision(eth-6)# rate-limit all in percent 10		ingress
		step-1
		Cisco(config)#ip access-list ext 120
		Cisco(config-ext-nacl)#permit ip any any
		step-2
		Cisco(config)#class-map all_traffic
		Cisco(config-cmap)#match access-group 120
		step-3
		Cisco(config)#policy-map rate_limit
		Cisco(config-pmap)#class all_traffic
		Cisco(config-pmap-c)#police 10000000 8000 exceed-action drop
		step-4
		Cisco(config)#interface f0/5
		Cisco(config-if)#service-policy input rate_limit
		egress
		Cisco(config)#interface f0/5
ProVision(eth-6)# rate-limit all out kbps 10000	[Comware5-GigabitEthernet1/0/6]qos lr outbound cir 10048	Cisco(config-if)#srr-queue bandwidth limit 10

ProVision

```
ProVision(eth-6)# rate-limit ?
 all                      Set limits for all traffic.
 bcast                    Set limits for broadcast traffic.
 icmp                     Set limits for ICMP traffic only.
 mcast                    Set limits for multicast traffic.

ProVision(eth-6)# rate-limit all ?
 in                       Set limits for all inbound traffic.
 out                      Set limits for all outbound traffic.

ProVision(eth-6)# rate-limit all in ?
 kbps                     Specify limit of allowed inbound or outbound traffic in
                          kilobits-per-second on the specified port(s).
 percent                  Specify limit as percent of inbound or outbound traffic.

ProVision(eth-6)# rate-limit all in percent 10


ProVision(eth-6)# rate-limit all out ?

ProVision(eth-6)# rate-limit all out kbps 10000
```

Comware 5

```
[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]qos ?
  apply      Apply specific QoS policy on interface
  bandwidth  Queue bandwidth
  gts        Apply GTS(Generic Traffic Shaping) policy on interface
  lr         Apply LR(Line Rate) policy on physical interface
  priority   Configure port priority
  sp         Configure strict priority queue
  trust      Configure priority trust mode
  wfq        Configure weighted fair queue
  wred       Apply WRED(Weighted Random Early Detection) configuration
             information
  wrr        Configure weighted round robin queue

[Comware5-GigabitEthernet1/0/6]qos lr ?
  outbound  Limit the rate on outbound

[Comware5-GigabitEthernet1/0/6]qos lr outbound ?
  cir  Target rate of physical interface(kbps)

[Comware5-GigabitEthernet1/0/6]qos lr outbound cir ?
  INTEGER<64-1000000>  Committed Information Rate(kbps), it must be a multiple
                       of 64

[Comware5-GigabitEthernet1/0/6]qos lr outbound cir 10048 ?
  cbs   Committed Burst Size (byte)
  <cr>

[Comware5-GigabitEthernet1/0/6]qos lr outbound cir 10048
```

Cisco

```
ingress limit

step-1

Cisco(config)#ip access-list ext 120

Cisco(config-ext-nacl)#permit ip any any


step-2

Cisco(config)#class-map all_traffic

Cisco(config-cmap)#match access-group 120


step-3

Cisco(config)#policy-map rate_limit

Cisco(config-pmap)#class all_traffic

Cisco(config-pmap-c)#police 10000000 8000 exceed-action drop


step-4
```

```
Cisco(config)#interface f0/5

Cisco(config-if)#service-policy input rate_limit


egress only

Cisco(config)#interface f0/5

Cisco(config-if)#srr-queue bandwidth limit 10
```

Chapter 25 IP Multicast

This chapter compares the commands used to configure Protocol Independent Multicast (PIM) dense and PIM sparse. It also covers Internet Group Management Protocol (IGMP).

a) PIM Dense

ProVision	Comware 5	Cisco
ProVision(config)# ip multicast-routing	[Comware5]multicast routing-enable	Cisco(config)#ip multicast-routing distributed
ProVision(config)# router pim		
ProVision(config)# vlan 220	[Comware5]interface Vlan-interface 220	Cisco(config)#interface vlan 220
ProVision(vlan-220)# ip pim-dense	[Comware5-Vlan-interface220]pim dm	Cisco(config-if)#ip pim dense-mode
ProVision# show ip pim ?	[Comware5]display pim ?	Cisco#show ip pim ?
ProVision# show ip mroute ?	[Comware5]display ip multicast routing-table ?	Cisco#show ip mroute ?

ProVision

```
ProVision(config)# ip multicast-routing

ProVision(config)# router pim


ProVision(config)# vlan 220

ProVision(vlan-220)# ip pim-dense


ProVision# show ip pim ?
 bsr                   Show Bootstrap Router information.
 interface             Show PIM interface information.
 mroute                Show PIM-specific information from the IP multicast
                       routing table.
 neighbor              Show PIM neighbor information.
 pending               Show (*,G) and (S,G) Join Pending Information.
 rp-candidate          Show Candidate-RP operational and configuration
                       information.
 rp-pending            Show (*,*,RP) Join Pending Information.
 rp-set                Show RP-Set information available on the router.
 <cr>


ProVision# show ip mroute ?
 interface             Show IP multicast routing interfaces' information.
 IP-ADDR               Show detailed information for the specified entry from
                       the IP multicast routing table.
 <cr>
```

Comware 5

```
[Comware5]multicast routing-enable


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]pim ?
  bsr-boundary           Bootstrap router boundary
  dm                       Enable PIM dense mode
  hello-option             Specify hello option
  holdtime                 Specify holdtime
  ipv6                     PIM IPv6 status and configuration information
  neighbor-policy          Policy to accept PIM hello messages
  require-genid            Require generation id
  sm                       Enable PIM sparse/SSM mode
  state-refresh-capable    State-refresh capability
  timer                    Specify PIM timer
  triggered-hello-delay    Triggered hello delay

[Comware5-Vlan-interface220]pim dm ?
  <cr>

[Comware5-Vlan-interface220]pim dm


[Comware5]display pim ?
  bsr-info          Bootstrap router information
  claimed-route     PIM claim route information
  control-message   PIM control message information
  grafts            PIM unacknowledged grafts' information
  interface         PIM-enabled interface
  ipv6              PIM IPv6 status and configuration information
  join-prune        PIM join prune queue
  neighbor          PIM neighbor information
  routing-table     PIM routing table
  rp-info           RP information


[Comware5]display ip multicast routing-table ?
  X.X.X.X  Destination IP address
  verbose  Verbose information of routing table
  <cr>
```

Cisco

```
Cisco(config)#ip multicast-routing distributed


Cisco(config)#interface vl 220

Cisco(config-if)#ip pim dense-mode


Cisco#show ip pim ?
  autorp      Global AutoRP information
  bsr-router  Bootstrap router (v2)
  interface   PIM interface information
  mdt         Multicast tunnel information
  neighbor    PIM neighbor information
  rp          PIM Rendezvous Point (RP) information
  rp-hash     RP to be chosen based on group selected
  vrf         Select VPN Routing/Forwarding instance


Cisco#show ip mroute ?
  Hostname or A.B.C.D  Source or group IP name or address
  active               Active multicast sources
  bidirectional        Show bidirectional multicast routes
  count                Route and packet count data
  dense                 Show dense multicast routes
  interface             Interface information
  proxy                 List proxies
  pruned                Pruned routes
  sparse                Show sparse multicast routes
  ssm                   show SSM multicast routes
  static                Static multicast routes
  summary               Provide abbreviated display
  vrf                   Select VPN Routing/Forwarding instance
  |                     Output modifiers
  <cr>
```

b) PIM Sparse

ProVision	Comware 5	Cisco
ProVision(config)# ip multicast-routing	[Comware5]multicast routing-enable	Cisco(config)#ip multicast-routing distributed
ProVision(config)# router pim		
ProVision(pim)# rp-address 100.0.220.12	[Comware5]pim [Comware5-pim]static-rp 10.0.220.12	
ProVision(pim)# rp-candidate source-ip-vlan 220	[Comware5-pim]c-rp Vlan-interface 220	Cisco(config)#ip pim rp-candidate vlan 220
ProVision(pim)# bsr-candidate source-ip-vlan 220	[Comware5-pim]c-bsr Vlan-interface 220	Cisco(config)#ip pim bsr-candidate vlan 220
ProVision(config)# vlan 220	[Comware5]interface Vlan-interface 220	Cisco(config)#interface vlan 220
ProVision(vlan-220)# ip pim-sparse	[Comware5-Vlan-interface220]pim sm	Cisco(config-if)#ip pim sparse-mode
ProVision# show ip pim ?	[Comware5]display pim ?	Cisco#show ip pim ?
ProVision# show ip mroute ?	[Comware5]display ip multicast routing-table ?	Cisco#show ip mroute ?

ProVision

```
ProVision(config)# ip multicast-routing

ProVision(config)# router pim

ProVision(pim)# rp-address 100.0.220.12

ProVision(pim)# rp-candidate source-ip-vlan 220

ProVision(pim)# bsr-candidate source-ip-vlan 220


ProVision(config)# vlan 220

ProVision(vlan-220)# ip pim-sparse


ProVision# show ip pim
 bsr                   Show Bootstrap Router information.
 interface             Show PIM interface information.
 mroute                Show PIM-specific information from the IP multicast
                       routing table.
 neighbor              Show PIM neighbor information.
 pending               Show (*,G) and (S,G) Join Pending Information.
 rp-candidate          Show Candidate-RP operational and configuration
                       information.
 rp-pending            Show (*,*,RP) Join Pending Information.
 rp-set                Show RP-Set information available on the router.
 <cr>


ProVision# show ip mroute
 interface             Show IP multicast routing interfaces' information.
 IP-ADDR               Show detailed information for the specified entry from
                       the IP multicast routing table.
 <cr>
```

Comware 5

```
[Comware5]multicast routing-enable

[Comware5]pim

[Comware5-pim]static-rp 10.0.220.12

[Comware5-pim]c-rp Vlan-interface 220

[Comware5-pim]c-bsr Vlan-interface 220


[Comware5]interface Vlan-interface 220

[Comware5-Vlan-interface220]pim sm


[Comware5]display pim ?
  bsr-info         Bootstrap router information
  claimed-route    PIM claim route information
  control-message  PIM control message information
  grafts           PIM unacknowledged grafts' information
  interface        PIM-enabled interface
  ipv6             PIM IPv6 status and configuration information
  join-prune       PIM join prune queue
  neighbor         PIM neighbor information
  routing-table    PIM routing table
  rp-info          RP information


[Comware5]display ip multicast routing-table ?
  X.X.X.X  Destination IP address
  verbose  Verbose information of routing table
  <cr>
```

Cisco

```
Cisco(config)#ip multicast-routing distributed

Cisco(config)#ip pim rp-candidate vlan 220

Cisco(config)#ip pim bsr-candidate vlan 220


Cisco(config)#interface vlan 220

Cisco(config-if)#ip pim sparse-mode


Cisco#show ip pim ?
  autorp       Global AutoRP information
  bsr-router   Bootstrap router (v2)
  interface    PIM interface information
  mdt          Multicast tunnel information
  neighbor     PIM neighbor information
  rp           PIM Rendezvous Point (RP) information
  rp-hash      RP to be chosen based on group selected
  vrf          Select VPN Routing/Forwarding instance
```

```
Cisco#show ip mroute ?
  Hostname or A.B.C.D  Source or group IP name or address
  active               Active multicast sources
  bidirectional        Show bidirectional multicast routes
  count                Route and packet count data
  dense                Show dense multicast routes
  interface            Interface information
  proxy                List proxies
  pruned               Pruned routes
  sparse               Show sparse multicast routes
  ssm                  show SSM multicast routes
  static               Static multicast routes
  summary              Provide abbreviated display
  vrf                  Select VPN Routing/Forwarding instance
  |                    Output modifiers
  <cr>
```

c) IGMP

ProVision	Comware 5	Cisco
`ProVision(vlan-220)# ip igmp`	`[Comware5-Vlan-interface220]igmp enable`	Enabling PIM on an interface also enables IGMP operation on that interface.

ProVision
`ProVision(vlan-220)# ip igmp`
Comware 5
`[Comware5-Vlan-interface220]igmp enable`
Cisco
Enabling PIM on an interface also enables IGMP operation on that interface.

Chapter 26 Spanning Tree Hardening

This chapter compares the commands used to configure:

- UniDirectional Link Detection (UDLD) and Device Link Detection Protocol (DLDP)
- Bridge Protocol Data Unit (BPDU) protection and BPDU guard
- Loop protection
- Root guard

a) UDLD and DLDP

ProVision	Comware 5	Cisco
`ProVision(config)# interface 6`	`[Comware5]dldp enable`	`Cisco(config)#interface f0/5`
`ProVision(eth-6)# link-keepalive`	`[Comware5]interface g1/0/7`	`Cisco(config-if)#udld port`
	`[Comware5-GigabitEthernet1/0/7]dldp enable`	

ProVision

```
ProVision(config)# interface 6

ProVision(eth-6)# link-keepalive ?
 vlan                   Set vlan-id for tagged UDLD control packets.
 <cr>

ProVision(eth-6)# link-keepalive
```

Comware 5

```
[Comware5]dldp ?
  authentication-mode      Specify password and authentication mode of DLDP
                           packet
  delaydown-timer          Specify the value of delaydown timer
  enable                   DLDP enable
  interval                 Specify the value of advertisement packet timer
  reset                    DLDP reset
  unidirectional-shutdown  Specify the mode of DLDP unidirectional shutdown
  work-mode                Set the work mode of DLDP

[Comware5]dldp enable


[Comware5]interface g1/0/7

[Comware5-GigabitEthernet1/0/7]dldp ?
  enable  DLDP enable
  reset   DLDP reset

[Comware5-GigabitEthernet1/0/7]dldp enable
```

Cisco

```
Cisco(config)#interface f0/5
Cisco(config-if)#udld ?
  port  Enable UDLD protocol on this interface

Cisco(config-if)#udld port ?
  aggressive  Enable UDLD protocol in aggressive mode on this interface
  <cr>

Cisco(config-if)#udld port
```

b) BPDU Protection and BPDU Guard

ProVision	Comware 5	Cisco
ProVision(config)# spanning-tree bpdu-protection-timeout 300		Cisco(config)#interface f0/5
ProVision(config)# spanning-tree 6 bpdu-protection		Cisco(config-if)#spanning-tree bpduguard enable
ProVision(config)# spanning-tree 6 bpdu-filter		Cisco(config-if)#spanning-tree bpdufilter enable
	[Comware5]stp bpdu-protection	

ProVision

```
ProVision(config)# spanning-tree bpdu-protection-timeout 300


ProVision(config)# spanning-tree 6 bpdu-protection


ProVision(config)# spanning-tree 6 bpdu-filter

Warning: The BPDU filter allows the port to go into a continuous
         forwarding mode and spanning-tree will not interfere, even if
         the port would cause a loop to form in the network topology.
         If you suddenly experience high traffic load, disable the port
         and reconfigure the BPDU filter with the CLI command(s):
           "no spanning-tree PORT_LIST bpdu-filter"
```

Comware 5

Make this configuration on a device with edge ports configured.

Global command.

```
[Comware5]stp bpdu-protection
```

Cisco

```
Cisco(config)#interface f0/5

Cisco(config-if)#spanning-tree bpduguard enable

   (note - the port must manually put back in service if this feature is triggered)


Cisco(config)#interface f0/5

Cisco(config-if)#spanning-tree bpdufilter enable
```

c) Loop Protection

ProVision	Comware 5	Cisco
ProVision(config)# loop-protect trap loop-detected		Cisco(config)#errdisable detect cause loopback
		Cisco(config)#errdisable recovery cause loopback
		Cisco(config)#errdisable recovery interval 300
ProVision(config)# loop-protect 6 receiver-action send-disable	[Comware5]interface g1/0/7	Cisco(config)#interface f0/5
	[Comware5-GigabitEthernet1/0/7]stp loop-protection	Cisco(config-if)#spanning-tree guard loop

ProVision

```
ProVision(config)# loop-protect trap loop-detected


ProVision(config)# loop-protect 6 receiver-action send-disable
```

Comware 5

```
[Comware5]interface g1/0/7

[Comware5-GigabitEthernet1/0/7]stp loop-protection
```

Cisco

```
Cisco(config)#errdisable detect cause loopback

Cisco(config)#errdisable recovery cause loopback

Cisco(config)#errdisable recovery interval 300


Cisco(config)#interface f0/5

Cisco(config-if)#spanning-tree guard loop
```

d) Root Guard

ProVision	Comware 5	Cisco
ProVision(config)# spanning-tree 6 root-guard	[Comware5]interface g1/0/7	Cisco(config)#interface f0/5
ProVision(config)# spanning-tree 6 tcn-guard	[Comware5-GigabitEthernet1/0/7]stp root-protection	Cisco(config-if)#spanning-tree guard root

ProVision
ProVision(config)# spanning-tree 6 root-guard ProVision(config)# spanning-tree 6 tcn-guard
Comware 5
[Comware5]interface g1/0/7 [Comware5-GigabitEthernet1/0/7]stp root-protection
Cisco
Cisco(config)#interface f0/5 Cisco(config-if)#spanning-tree guard root

Chapter 27 DHCP Snooping

This chapter compares commands that are used to enable protections for DHCP, thereby preventing malicious users from using DHCP to gather information about the network or attack it.

ProVision	Comware 5	Cisco
ProVision(config)# dhcp-snooping	[Comware5]dhcp-snooping	Cisco(config)#ip dhcp snooping
ProVision(config)# dhcp-snooping authorized-server 10.0.100.111		
ProVision(config)# dhcp-snooping database file tftp://10.0.100.21/ProVision_dhcp.txt		Cisco(config)#ip dhcp snooping database tftp://10.0.100.21/Cisco_dhcp.txt
ProVision(config)# dhcp-snooping vlan 220		Cisco(config)#ip dhcp snooping vlan 220
ProVision(config)# dhcp-snooping trust 9	[Comware5]interface g1/0/9	Cisco(config)#interface f0/9
	[Comware5-GigabitEthernet1/0/9]dhcp-snooping trust	Cisco(config-if)#ip dhcp snooping trust
ProVision# show dhcp-snooping	[Comware5]display dhcp-snooping [Comware5]display dhcp-snooping trust	Cisco#show ip dhcp snooping
		Cisco#show ip dhcp snooping database
ProVision# show dhcp-snooping stats		Cisco#show ip dhcp snooping statistics detail

ProVision

```
ProVision(config)# dhcp-snooping ?
 authorized-server     Configure valid DHCP Servers.
 database              Configure lease database transfer options.
 option                Configure DHCP snooping operational behavior.
 trust                 Configure trusted interfaces.
 verify                Enable/Disable DHCP packet validation.
 vlan                  Enable/Disable snooping on a VLAN.
 <cr>

ProVision(config)# dhcp-snooping


ProVision(config)# dhcp-snooping authorized-server 10.0.100.111


ProVision(config)# dhcp-snooping database file tftp://10.0.100.21/ProVision_dhcp.txt


ProVision(config)# dhcp-snooping option ?
 82

ProVision(config)# dhcp-snooping option 82 ?
 remote-id             Set relay information option remote-id value to use.
 untrusted-policy      Policy for DHCP packets received on untrusted ports
                       that contain option 82.
 <cr>

ProVision(config)# dhcp-snooping option 82 remote-id ?
```

```
 mac                   switch MAC address.
 subnet-ip             subnet VLAN IP address.
 mgmt-ip               management VLAN IP address.

ProVision(config)# dhcp-snooping option 82 untrusted-policy ?
 drop                  drop the packet.
 keep                  forward the packet unchanged.
 replace               generate new option.


ProVision(config)# dhcp-snooping vlan 220


ProVision(config)# dhcp-snooping trust 9


ProVision# show dhcp-snooping

 DHCP Snooping Information

  DHCP Snooping               : Yes
  Enabled Vlans               :
  Verify MAC                  : Yes
  Option 82 untrusted policy : drop
  Option 82 Insertion        : Yes
  Option 82 remote-id        : mac

  Store lease database : Yes
  URL            : tftp://10.0.100.21/ProVision_dhcp.txt
  Read at boot   : no
  Write delay    : 300
  Write timeout  : 300
  File status    : delaying
  Write attempts : 0
  Write failures : 0
  Last successful file update :


  Port    Trust
  ------- -----
  1       No
  2       No
  3       No
  4       No
  5       No
  6       No
  7       No
  8       No
  9       Yes
  10      No
  11      No
  12      No
  13      No
  14      No
  15      No
  16      No
  17      No
  18      No
  19      No
  20      No
  21      No
  24      No
  Trk1    No
```

```
ProVision# show dhcp-snooping stats


 Packet type  Action   Reason                        Count
 -----------  -------  ----------------------------  ---------
 server       forward  from trusted port              0
 client       forward  to trusted port                0
 server       drop     received on untrusted port     0
 server       drop     unauthorized server            0
 client       drop     destination on untrusted port  0
 client       drop     untrusted option 82 field      0
 client       drop     bad DHCP release request       0
 client       drop     failed verify MAC check        0
```

Comware 5

```
[Comware5]dhcp-snooping ?
  <cr>

[Comware5]dhcp-snooping


[Comware5]interface g1/0/9

[Comware5-GigabitEthernet1/0/9]dhcp-snooping ?
  information  Specify Option 82 service
  trust        Trusted port

[Comware5-GigabitEthernet1/0/9]dhcp-snooping trust ?
  no-user-binding  Forbid DHCP snooping learning
  <cr>

[Comware5-GigabitEthernet1/0/9]dhcp-snooping trust


[Comware5-GigabitEthernet1/0/9]dhcp-snooping information ?
  circuit-id  Specify the circuit ID
  enable      Enable Option 82
  format      Specify the mode of option 82
  remote-id   Specify the remote ID
  strategy    Specify the strategy to handle Option 82
  vlan        Specify a VLAN


[Comware5-GigabitEthernet1/0/9]dhcp-snooping information enable ?
  <cr>

[Comware5-GigabitEthernet1/0/9]dhcp-snooping information format ?
  normal   Normal mode
  verbose  Verbose mode

[Comware5-GigabitEthernet1/0/9]dhcp-snooping information remote-id ?
  format-type  Specify the format of remote ID
  string       Specify the content of remote ID

[Comware5-GigabitEthernet1/0/9]dhcp-snooping information strategy ?
  drop     Drop strategy
  keep     Keep strategy
  replace  Replace strategy
```

```
[Comware5-GigabitEthernet1/0/9]dhcp-snooping information vlan ?
  INTEGER<1-4094>  VLAN ID

[Comware5-GigabitEthernet1/0/9]dhcp-snooping information vlan 220 ?
  circuit-id  Specify the circuit ID
  remote-id   Specify the remote ID


[Comware5]display dhcp-snooping ?
  information  Specify Option 82 service
  ip           Single client ip
  packet       Packet statistics function
  trust        Trusted port
  <cr>


[Comware5]dis dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static
 Type IP Address      MAC Address    Lease        VLAN Interface
 ==== =============== ============== ============ ==== =================
 D    10.1.220.101    0016-d4fa-e6d5 86195        220  GigabitEthernet1/0/19
---   1 dhcp-snooping item(s) found   ---


[Comware5]display dhcp-snooping trust ?
  <cr>

[Comware5]display dhcp-snooping trust
 DHCP Snooping is enabled.
 DHCP Snooping trust becomes active.
 Interface                                       Trusted
 =========================                       ============
 Bridge-Aggregation1                             Trusted
 GigabitEthernet1/0/9                            Trusted
```

Cisco

```
Cisco(config)#ip dhcp snooping ?
  database     DHCP snooping database agent
  information  DHCP Snooping information
  verify       DHCP snooping verify
  vlan         DHCP Snooping vlan
  <cr>


Cisco(config)#ip dhcp snooping


Cisco(config)#ip dhcp snooping database tftp://10.0.100.21/Cisco_dhcp.txt


Cisco(config)#ip dhcp snooping information ?
  option  DHCP Snooping information option

Cisco(config)#ip dhcp snooping information option ?
  allow-untrusted  DHCP Snooping information option allow-untrusted
  format           Option 82 information format
  <cr>


Cisco(config)#ip dhcp snooping information option allow-untrusted ?
  <cr>


Cisco(config)#ip dhcp snooping information option format ?
  remote-id  Remote id option 82 format

Cisco(config)#ip dhcp snooping information option format remote-id ?
  hostname  Use configured hostname for remote id
  string    User defined string for remote id


Cisco(config)#ip dhcp snooping verify ?
  mac-address             DHCP snooping verify mac-address
  no-relay-agent-address  DHCP snooping verify giaddr

Cisco(config)#ip dhcp snooping verify mac-address ?
  <cr>

Cisco(config)#ip dhcp snooping verify no-relay-agent-address ?
  <cr>


Cisco(config)#ip dhcp snooping vlan 220


Cisco(config)#interface f0/9

Cisco(config-if)#ip dhcp snooping trust


Cisco#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
220
DHCP snooping is operational on following VLANs:
220
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/6              yes         unlimited
FastEthernet0/9              yes         unlimited


Cisco#show ip dhcp snooping database
Agent URL : tftp://10.0.100.21/Cisco_dhcp.txt
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
```

```
Last Succeeded Time : 02:33:49 CST Thu Dec 10 2009
Last Failed Time : 01:29:41 CST Wed Dec 2 2009
Last Failed Reason : Expected more data on read.

Total Attempts       :       20   Startup Failures :        3
Successful Transfers :       16   Failed Transfers :        4
Successful Reads     :        0   Failed Reads     :        1
Successful Writes    :       16   Failed Writes    :        0
Media Failures       :        0




Cisco#show ip dhcp snooping statistics detail
 Packets Processed by DHCP Snooping                    = 297
 Packets Dropped Because
   IDB not known                                       = 0
   Queue full                                          = 0
   Interface is in errdisabled                         = 0
   Rate limit exceeded                                 = 0
   Received on untrusted ports                         = 0
   Nonzero giaddr                                      = 0
   Source mac not equal to chaddr                      = 0
   Binding mismatch                                    = 0
   Insertion of opt82 fail                             = 0
   Interface Down                                      = 0
   Unknown output interface                            = 1
   Reply output port equal to input port               = 0
   Packet denied by platform                           = 0
```

Chapter 28 ARP Protection , ARP Detection, and Dynamic ARP Inspection

This chapter compares commands designed to secure the Address Resolution Protocol (ARP). Note that DHCP snooping must be enabled for ARP protection, ARP detection, and dynamic ARP inspection to operate.

ProVision	Comware 5	Cisco
ProVision(config)# arp-protect	[Comware5]arp detection mode dhcp-snooping	
ProVision(config)# arp-protect vlan 220	[Comware5]vlan 220	Cisco(config)#ip arp inspection vlan 220
	[Comware5-vlan220]arp detection enable	
ProVision(config)# arp-protect trust 9	[Comware5]interface g1/0/9	Cisco(config)#interface f0/9
	[Comware5-GigabitEthernet1/0/9]arp detection trust	Cisco(config-if)#ip arp inspection trust
ProVision# show arp-protect	[Comware5]display arp detection	Cisco# show ip arp inspection
	[Comware5]display arp detection statistics	Cisco#show ip arp inspection interfaces

ProVision

```
ProVision(config)# arp-protect ?
 trust                  Configure port(s) as trusted or untrusted.
 validate               Configure additional ARP Protection validation checks.
 vlan                   Enable/disable Dynamic ARP Protection on a VLAN(s).
 <cr>

ProVision(config)# arp-protect

ProVision(config)# arp-protect vlan 220


ProVision(config)# arp-protect trust 9


ProVision# show arp-protect

 ARP Protection Information

  ARP Protection Enabled : Yes
  Protected Vlans   : 220
  Validate          :

  Port    Trust
  ------- -----
  1       No
  2       No
  3       No
  4       No
  5       No
  6       No
  7       No
  8       No
  9       Yes
  10      No
  11      No
  12      No
  13      No
  14      No
  15      No
  16      No
  17      No
  18      No
  19      No
  20      No
  21      No
  24      No
  Trk1    No
```

Comware 5

```
[Comware5]arp detection ?
  mode          Specify ARP detection check mode
  static-bind   Bind IP and MAC address for ARP detection check
  validate      Enable validate check mode

[Comware5]arp detection mode ?
  dhcp-snooping   ARP detection check using DHCP snooping entries
  dot1x           ARP detection check using 802.1X entries
  static-bind     ARP detection check using static binding entries

[Comware5]arp detection mode dhcp-snooping ?
  <cr>

[Comware5]arp detection mode dhcp-snooping


[Comware5]vlan 220

[Comware5-vlan220]arp ?
  detection  Specify ARP detection function

[Comware5-vlan220]arp detection ?
  enable  Enable ARP detection function

[Comware5-vlan220]arp detection enable ?
  <cr>

[Comware5-vlan220]arp detection enable


[Comware5]interface g1/0/9

[Comware5-GigabitEthernet1/0/9]arp ?
  detection          Specify ARP detection function
  max-learning-num   Set the maximum number of dynamic arp entries learned on
                     the interface
  rate-limit         Limit ARP packet rate

[Comware5-GigabitEthernet1/0/9]arp detection ?
  trust  Specify port trust state

[Comware5-GigabitEthernet1/0/9]arp detection trust ?
  <cr>
```

```
[Comware5-GigabitEthernet1/0/9]arp detection trust


[Comware5]display arp detection
 ARP detection is enabled in the following VLANs:
 220

[Comware5]display arp detection statistics ?
  interface  Display statistics by interface
  <cr>

[Comware5]display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)           IP            Src-MAC       Dst-MAC       Inspect
BAGG1(U)                   0             0             0             0
GE1/0/1(U)                 0             0             0             0
GE1/0/2(U)                 0             0             0             0
GE1/0/3(U)                 0             0             0             0
GE1/0/4(U)                 0             0             0             0
GE1/0/5(U)                 0             0             0             0
GE1/0/6(U)                 0             0             0             0
GE1/0/7(U)                 0             0             0             0
GE1/0/8(U)                 0             0             0             0
GE1/0/9(T)                 0             0             0             0
GE1/0/10(U)                0             0             0             0
GE1/0/11(U)                0             0             0             0
GE1/0/12(U)                0             0             0             0
GE1/0/13(U)                0             0             0             0
GE1/0/14(U)                0             0             0             0
GE1/0/15(U)                0             0             0             0
GE1/0/16(U)                0             0             0             0
GE1/0/17(U)                0             0             0             0
GE1/0/18(U)                0             0             0             0
GE1/0/19(U)                0             0             0             88
GE1/0/20(U)                0             0             0             0
GE1/0/21(U)                0             0             0             0
GE1/0/22(U)                0             0             0             0
GE1/0/23(U)                0             0             0             0
GE1/0/24(U)                0             0             0             0
GE1/0/25(U)                0             0             0             0
GE1/0/26(U)                0             0             0             0
GE1/0/27(U)                0             0             0             0
GE1/0/28(U)                0             0             0             0
```

Cisco

```
Cisco(config)#ip arp inspection ?
  filter      Specify ARP acl to be applied
  log-buffer  Log Buffer Configuration
  validate    Validate addresses
  vlan        Enable/Disable ARP Inspection on vlans

Cisco(config)#ip arp inspection vlan 220


Cisco(config)#interface f0/9
Cisco(config-if)#ip arp inspection trust


Cisco# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  220     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  220     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  220           2560            172            172              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  220            624              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  220                   0                        0                       0

Cisco#show ip arp inspection interfaces

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa0/1            Untrusted               15                 1
 Fa0/2            Untrusted               15                 1
 Fa0/3            Untrusted               15                 1
 Fa0/4            Untrusted               15                 1
 Fa0/5            Untrusted               15                 1
 Fa0/6            Trusted               None               N/A
 Fa0/7            Untrusted               15                 1
 Fa0/8            Untrusted               15                 1
 Fa0/9            Trusted               None               N/A
```

Chapter 29 Connection Rate Filtering

ProVision provides a feature called connection rate filtering, which is based on HP's Virus Throttle™ technology. Connection rate filtering detects hosts that are generating IP traffic typical of viruses or worms and either throttles or drops all IP traffic from the offending hosts. (For more information, see the access security guide for your HP switch.)

Comware 5 and Cisco do not support this exact feature. However, their ARP commands provide rate limiting capabilities for incoming ARP packets.

ProVision	Comware 5	Cisco
	No exact Comware 5 feature compared to this ProVision feature. Comware 5 ARP Defense & ARP Packet Rate Limit features provide rate limiting capability of incoming ARP packets.	No exact Cisco feature compared to this ProVision feature. Cisco's Dynamic ARP Inspection provides rate limiting capability of incoming ARP packets.
`ProVision(config)# connection-rate-filter sensitivity medium`	`[Comware5]arp source-suppression enable`	`Cisco(config-if)#interface f 0/20`
`ProVision(config)# filter connection-rate 6 notify-only`	`[Comware5]arp source-suppression limit 15`	`Cisco(config-if)#ip arp inspection limit rate 100`
`ProVision(config)# filter connection-rate 10 block`	`[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 150 drop`	-optional- `Cisco(config)#errdisable recovery cause arp-inspection`
`ProVision(config)# filter connection-rate 20 throttle`		
`ProVision# show connection-rate-filter`	`[Comware5]display arp source-suppression`	`Cisco#show ip arp inspection interfaces`
		`Cisco#show errdisable recovery`

ProVision

```
ProVision(config)# connection-rate-filter ?
 sensitivity            Sets the level of filtering required
 unblock                Resets a host previously blocked by the connection rate
                        filter

ProVision(config)# connection-rate-filter sensitivity
 low                    Sets the level of connection rate filtering to low (most
                        permissive)
 medium                 Sets the level of connection rate filtering to medium
                        (permissive)
 high                   Sets the level of connection rate filtering to high
                        (restrictive)
 aggressive             Sets the level of connection rate filtering to
                        aggressive (most restrictive)

ProVision(config)# connection-rate-filter sensitivity medium


ProVision(config)# filter connection-rate ?
 [ethernet] PORT-LIST
```

```
ProVision(config)# filter connection-rate 6 ?
 block                 Disable the host until an administrator explicitly
                       re-enables access.
 notify-only           Log a message/send a SNMP trap when the filter is
                       tripped.
 throttle              Deny network access for a period before automatically
                       re-enabling access.

ProVision(config)# filter connection-rate 6 notify-only ?
 <cr>

ProVision(config)# filter connection-rate 10 block ?
 <cr>

ProVision(config)# filter connection-rate 20 throttle ?
 <cr>


ProVision# show connection-rate-filter

 Connection Rate Filter Configuration

  Global Status:    Enabled
  Sensitivity:      Medium

  Port         | Filter Mode
  ------------+------------------
  6            | NOTIFY-ONLY
  10           | BLOCK
  20           | THROTTLE
```

Comware 5

```
[Comware5]arp ?
  anti-attack         Specify ARP anti-attack function
  check               Specify arp item check status
  detection           Specify ARP detection function
  resolving-route     arp resolving-route
  source-suppression  Specify ARP source suppression
  static              Static ARP entry
  timer               Specify ARP timer

[Comware5]arp source-suppression ?
  enable  Enable ARP source suppression
  limit   Specify ARP source suppression limit information

[Comware5]arp source-suppression enable ?
  <cr>

[Comware5]arp source-suppression enable

[Comware5]arp source-suppression limit ?
  INTEGER<2-1024>  Specify ARP source suppression limit number

[Comware5]arp source-suppression limit 15 ?
  <cr>

[Comware5]arp source-suppression limit 15


[Comware5-GigabitEthernet1/0/20]arp ?
```

```
  detection         Specify ARP detection function
  max-learning-num  Set the maximum number of dynamic arp entries learned on
                    the interface
  rate-limit        Limit ARP packet rate


[Comware5-GigabitEthernet1/0/20]arp rate-limit ?
  disable  Disable ARP packet rate limit
  rate     Specify ARP packet rate

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate ?
  INTEGER<50-500>  Rate value (packet per second)

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 150 ?
  drop  Drop ARP packets over limited rate

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 150 drop ?
  <cr>

[Comware5-GigabitEthernet1/0/20]arp rate-limit rate 150 drop


[Comware5]display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 15
 Current cache length: 16
```

Cisco

No specific Cisco feature compared to this ProVision feature.

Cisco’s Dynamic ARP Inspection provides rate limiting capability of incoming ARP packets.

```
Cisco(config-if)#interface f 0/20


Cisco(config-if)#ip arp inspection limit ?
  none  No limit
  rate  Rate Limit

Cisco(config-if)#ip arp inspection limit rate ?
  <0-2048>  Packets per second

Cisco(config-if)#ip arp inspection limit rate 100 ?
  burst  Configure Burst parameters for ARP packets
  <cr>

Cisco(config-if)#ip arp inspection limit rate 100


-optional-

Cisco(config)#errdisable recovery cause arp-inspection


Cisco#show ip arp inspection interfaces

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa0/1            Untrusted               15                 1
 Fa0/2            Untrusted               15                 1
 Fa0/3            Untrusted               15                 1
 Fa0/4            Untrusted               15                 1
 Fa0/5            Untrusted               15                 1
 Fa0/6            Trusted               None               N/A
 Fa0/7            Untrusted               15                 1
 Fa0/8            Untrusted               15                 1
 Fa0/9            Trusted                100                 1
 Fa0/10           Untrusted               15                 1


Cisco#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Enabled
bpduguard                    Disabled
channel-misconfig            Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
link-flap                    Disabled
mac-limit                    Disabled
loopback                     Enabled
pagp-flap                    Disabled
port-mode-failure            Disabled
psecure-violation            Disabled
security-violation           Disabled
sfp-config-mismatch          Disabled
small-frame                  Disabled
storm-control                Disabled
udld                         Disabled
vmps                         Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

Chapter 30 802.1X Authentication

This chapter compares the commands that enforce 802.1X authentication for devices and users accessing the network.

a) 802.1X Authentication

ProVision	Comware 5	Cisco
ProVision(config)# radius-server host 10.0.100.111 key password	[Comware5]radius scheme <radius-auth>	Cisco(config)#aaa new-model
ProVision(config)# aaa authentication port-access eap-radius	[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812 [Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813 [Comware5-radius-radius-auth]key authentication password [Comware5-radius-radius-auth]user-name-format without-domain [Comware5-radius-radius-auth]server-type extended	Cisco(config)#aaa authentication dot1x default group radius
ProVision(config)# aaa port-access authenticator 13,17-18	[Comware5]domain 8021x	Cisco(config)#dot1x system-auth-control
ProVision(config)# aaa port-access authenticator 13,17-18 unauth-vid 99	[Comware5-isp-8021x]authentication lan-access radius-scheme radius-auth	Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password
ProVision(config)# aaa port-access authenticator 13 client-limit 4	[Comware5-isp-8021x]authorization lan-access radius-scheme radius-auth	Cisco(config)#interface f0/13
ProVision(config)# aaa port-access authenticator 17-18 client-limit 3	[Comware5-isp-8021x]accounting lan-access radius-scheme radius-auth	Cisco(config-if)#switchport mode access
ProVision(config)# aaa port-access authenticator active	[Comware5]domain default enable 8021x	Cisco(config-if)#dot1x host-mode multi-host
	[Comware5]dot1x	Cisco(config-if)#dot1x port-control auto
	[Comware5]dot1x authentication-method eap	Cisco(config-if)#dot1x auth-fail vlan 99
	[Comware5]interface g1/0/13	
	[Comware5-GigabitEthernet1/0/13]dot1x	
	[Comware5-GigabitEthernet1/0/13]undo dot1x handshake	
	[Comware5-GigabitEthernet1/0/13]dot1x auth-fail vlan 99	
	[Comware5-GigabitEthernet1/0/13]dot1x max-user 4	
ProVision# show port-access	[Comware5]display dot1x	Cisco#show dot1x all summary

authenticator	sessions	
ProVision# show port-access authenticator vlan		
ProVision# show vlans ports 13 detail	[Comware5]display dot1x interface g1/0/13	Cisco#show dot1x interface f0/13 details
ProVision# show vlans 220	[Comware5]display vlan 220	Cisco#show vlan brief

ProVision

```
ProVision(config)# radius-server host 10.0.100.111 key password


ProVision(config)# aaa authentication port-access eap-radius


ProVision(config)# aaa port-access ?
 authenticator          Configure 802.1X (Port Based Network Access)
                        authentication on the device or the device's port(s).
 gvrp-vlans             Enable/disable the use of RADIUS-assigned dynamic (GVRP)
                        VLANs.
 mac-based              Configure MAC address based network authentication on
                        the device or the device's port(s).
 [ethernet] PORT-LIST  Manage general port security features on the device
                        port(s).
 supplicant             Manage 802.1X (Port Based Network Access) supplicant on
                        the device ports.
 web-based              Configure web authentication based network
                        authentication on the device or the device's port(s).


ProVision(config)# aaa port-access authenticator 13,17-18

ProVision(config)# aaa port-access authenticator 13,17-18 unauth-vid 99

ProVision(config)# aaa port-access authenticator 13 client-limit 4

ProVision(config)# aaa port-access authenticator 17-18 client-limit 3

ProVision(config)# aaa port-access authenticator active


ProVision# show port-access authenticator

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

       Auth     Unauth   Untagged Tagged           Kbps In     RADIUS Cntrl
  Port Clients  Clients  VLAN     VLANs  Port COS  Limit       ACL    Dir
  ---- -------- -------- -------- ------ --------- ----------- ------ -----
  13   1        0        220      No     00000000  No          No     both
  17   0        0        0        No     No        No          No     both
  18   0        0        0        No     No        No          No     both


ProVision# show port-access authenticator vlan

 Port Access Authenticator VLAN Configuration

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

       Access   Unauth   Auth
  Port Control  VLAN ID  VLAN ID
  ---- -------- -------- --------
  13   Auto     99       220
  17   Auto     99       220
  18   Auto     99       220


ProVision# show vlans ports 13 detail

 Status and Counters - VLAN Information - for ports 13

  VLAN ID Name                 | Status     Voice Jumbo Mode
  ------- -------------------- + ---------- ----- ----- --------
  220     test                 | Port-based No    No    Untagged


ProVision# show vlans 220

 Status and Counters - VLAN Information - VLAN 220

  VLAN ID : 220
  Name : test
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  1                Untagged Learn        Down
  2                Untagged Learn        Down
  3                Untagged Learn        Down
  5                Untagged Learn        Down
  6                Tagged   Learn        Up
  7                Tagged   Learn        Down
  8                Tagged   Learn        Down
  13               802.1x   Learn        Up
  18               Untagged Learn        Down
  19               Untagged Learn        Down
  20               Tagged   Learn        Down
  Trk1             Tagged   Learn        Down

  Overridden Port VLAN configuration

  Port Mode
  ---- ------------
   13    No


ProVision# show vlans 1

 Status and Counters - VLAN Information - VLAN 1

  VLAN ID : 1
  Name : DEFAULT_VLAN
  Status : Port-based
  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  4                Untagged Learn        Down
  7                Untagged Learn        Down
  8                Untagged Learn        Down
  14               Untagged Learn        Down
  15               Untagged Learn        Down
  16                Untagged Learn        Down
  17                Untagged Learn        Down
  20                Untagged Learn        Down
  21                Untagged Learn        Down
  24                Untagged Learn        Down
  Trk1              Untagged Learn        Down

  Overridden Port VLAN configuration

  Port Mode
  ---- ------------
  13   Untagged
```

Comware 5

```
[Comware5]radius scheme <radius-auth>

[Comware5-radius-radius-auth]primary authentication 10.0.100.111 1812

[Comware5-radius-radius-auth]primary accounting 10.0.100.111 1813

[Comware5-radius-radius-auth]key authentication password

[Comware5-radius-radius-auth]user-name-format without-domain

[Comware5-radius-radius-auth]server-type extended


[Comware5]domain 8021x
New Domain added.

[Comware5-isp-8021x]authentication ?
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration

[Comware5-isp-8021x]authentication lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-8021x]authentication lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  <cr>

[Comware5-isp-8021x]authentication lan-access radius-scheme radius-auth


[Comware5-isp-8021x]authorization ?
  command     Specify command AAA configuration
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  portal      Specify portal AAA configuration

[Comware5-isp-8021x]authorization lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-8021x]authorization lan-access radius-scheme radius-auth ?
  local  Specify local scheme
  <cr>

[Comware5-isp-8021x]authorization lan-access radius-scheme radius-auth


[Comware5-isp-8021x]accounting ?
  command     Specify command AAA configuration
  default     Specify default AAA configuration
  lan-access  Specify lan-access AAA configuration
  login       Specify login AAA configuration
  optional    Optional accounting mode
  portal      Specify portal AAA configuration

[Comware5-isp-8021x]accounting lan-access ?
  local          Specify local scheme
  none           Specify none scheme
  radius-scheme  Specify RADIUS scheme

[Comware5-isp-8021x]accounting lan-access radius-scheme radius-auth


[Comware5]domain default enable 8021x


[Comware5]dot1x
 802.1x is enabled globally.

[Comware5]dot1x ?
  authentication-method  Specify system authentication method
  free-ip                Specify free IP configurations
  guest-vlan             Specify guest vlan configuration information of port
  interface              Specify interface configuration information
  max-user               Specify maximal on-line user number per port
  port-control           Specify port authenticated status
  port-method            Specify port controlled method
  quiet-period           Enable quiet period function
  retry                  Specify maximal request times
  timer                  Specify timer parameters
  url                    Specify URL of the redirection server
  <cr>

[Comware5]dot1x authentication-method ?
  chap  CHAP(Challenge Handshake Authentication Protocol) authentication
        method. It's default.
  eap   EAP(Extensible Authentication Protocol) authentication method
  pap   PAP(Password Authentication Protocol) authentication method

[Comware5]dot1x authentication-method eap ?
  <cr>

[Comware5]dot1x authentication-method eap
 EAP authentication is enabled
```

```
[Comware5]interface g1/0/13
[Comware5-GigabitEthernet1/0/13]dot1x ?
  auth-fail          Specify a VLAN for clients failing the 802.1X
                     authentication on the port
  guest-vlan         Specify guest vlan configuration information of port
  handshake          Enable handshake with online user(s)
  mandatory-domain   Specify the domain for 802.1X
  max-user           Specify maximal on-line user number per port
  multicast-trigger  Enable multicast trigger at specify interface
  port-control       Specify port authenticated status
  port-method        Specify port controlled method
  re-authenticate    Enable periodic reauthentication of the online user(s)
  <cr>

[Comware5-GigabitEthernet1/0/13]dot1x
 802.1x is enabled on port GigabitEthernet1/0/13.

[Comware5-GigabitEthernet1/0/13]undo dot1x handshake

[Comware5-GigabitEthernet1/0/13]dot1x auth-fail vlan 99

[Comware5-GigabitEthernet1/0/13]dot1x max-user 4



[Comware5]display dot1x sessions
 Equipment 802.1X protocol is enabled
 EAP authentication is enabled

 The maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/1  is link-down
   802.1X protocol is disabled
   Handshake is enabled
   Handshake secure is disabled
...
GigabitEthernet1/0/13  is link-up
   802.1X protocol is enabled
   Handshake is disabled
   Handshake secure is disabled
 1. Authenticated user : MAC address: 001a-4b92-5e24

   Controlled User(s) amount to 1
...


[Comware5]display dot1x interface g1/0/13
 Equipment 802.1X protocol is enabled
 EAP authentication is enabled
 EAD quick deploy is disabled

 Configuration: Transmit Period   30 s,  Handshake Period       15 s
                Quiet Period      60 s,  Quiet Period Timer is disabled
                Supp Timeout      30 s,  Server Timeout        100 s
                Reauth Period   3600 s
                The maximal retransmitting times    2
 EAD quick deploy configuration:
                EAD timeout:   30 m

 The maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/13  is link-up
   802.1X protocol is enabled
   Handshake is disabled
   Handshake secure is disabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   802.1X Multicast-trigger is enabled
   Mandatory authentication domain: NOT configured
   Guest VLAN: NOT configured
   Auth-Fail VLAN: 99
   Max number of on-line users is 4

   EAPOL Packet: Tx 659, Rx 648
   Sent EAP Request/Identity Packets : 194
        EAP Request/Challenge Packets: 0
        EAP Success Packets: 92, Fail Packets: 0
   Received EAPOL Start Packets : 92
            EAPOL LogOff Packets: 0
            EAP Response/Identity Packets : 92
            EAP Response/Challenge Packets: 281
            Error Packets: 0
 1. Authenticated user : MAC address: 001a-4b92-5e24

   Controlled User(s) amount to 1


[Comware5]display brief interface
The brief information of interface(s) under route mode:
Interface            Link      Protocol-link  Protocol type    Main IP
NULL0                UP        UP(spoofing)   NULL             --
Vlan1                UP        DOWN           ETHERNET         --
Vlan100              UP        UP             ETHERNET         10.0.100.48
Vlan220              UP        UP             ETHERNET         10.1.220.3
Vlan230              DOWN      DOWN           ETHERNET         10.1.230.3

The brief information of interface(s) under bridge mode:
Interface            Link      Speed        Duplex   Link-type  PVID
BAGG1                ADM DOWN  auto         auto     trunk      1
GE1/0/1              DOWN      auto         auto     access     1
GE1/0/2              DOWN      auto         auto     access     1
GE1/0/3              UP        1G(a)        full(a)  access     100
GE1/0/4              DOWN      auto         auto     access     220
GE1/0/5              DOWN      auto         auto     access     100
GE1/0/6              UP        100M(a)      full(a)  trunk      1
GE1/0/7              DOWN      auto         auto     access     1
GE1/0/8              DOWN      auto         auto     access     1
GE1/0/9              ADM DOWN  auto         auto     access     100
GE1/0/10             DOWN      auto         auto     access     1
```

```
GE1/0/11             DOWN      auto         auto     access     1
GE1/0/12             DOWN      auto         auto     access     1
GE1/0/13             UP        100M(a)      full(a)  access     220
GE1/0/14             DOWN      auto         auto     access     1
GE1/0/15             DOWN      auto         auto     access     1
GE1/0/16             DOWN      auto         auto     access     1
GE1/0/17             DOWN      auto         auto     access     1
GE1/0/18             UP        100M(a)      full(a)  hybrid     220
GE1/0/19             UP        100M(a)      full(a)  access     220
GE1/0/20             DOWN      auto         auto     access     1
GE1/0/21             DOWN      auto         auto     access     1
GE1/0/22             DOWN      auto         auto     trunk      1
GE1/0/23             DOWN      auto         auto     trunk      1
GE1/0/24             DOWN      auto         auto     access     1
GE1/0/25             ADM DOWN  auto         auto     access     1
GE1/0/26             ADM DOWN  auto         auto     access     1
GE1/0/27             ADM DOWN  auto         auto     access     1
GE1/0/28             ADM DOWN  auto         auto     access     1


[Comware5]display vlan 220
 VLAN ID: 220
 VLAN Type: static
 Route Interface: configured
 IP Address: 10.1.220.3
 Subnet Mask: 255.255.255.0
 Description: VLAN 0220
 Name: test
 Tagged   Ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/6     GigabitEthernet1/0/22    GigabitEthernet1/0/23
 Untagged Ports:
    GigabitEthernet1/0/4     GigabitEthernet1/0/13    GigabitEthernet1/0/18
    GigabitEthernet1/0/19
```

Cisco

```
Cisco(config)#aaa new-model

Cisco(config)#aaa authentication dot1x default group radius

Cisco(config)#dot1x system-auth-control

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password


Cisco(config)#interface f0/13

Cisco(config-if)#switchport mode access

Cisco(config-if)#dot1x ?
  auth-fail          Configure Authentication Fail values for this port
  control-direction  Set the control-direction on the interface
  critical           Enable 802.1x Critical Authentication
  default            Configure Dot1x with default values for this port
  fallback           Enable the Webauth fallback mechanism
  guest-vlan         Configure Guest-vlan on this interface
  host-mode          Set the Host mode for 802.1x on this interface
  mac-auth-bypass    Enable MAC Auth Bypass
  max-reauth-req     Max No.of Reauthentication Attempts
  max-req            Max No.of Retries
  pae                 Set 802.1x interface pae type
  port-control        set the port-control value
  reauthentication    Enable or Disable Reauthentication for this port
  timeout             Various Timeouts
  violation-mode      Set the Security Violation mode on this interface


Cisco(config-if)#dot1x host-mode ?
  multi-domain  Multiple Domain Mode
  multi-host    Multiple Host Mode
  single-host   Single Host Mode


Cisco(config-if)#dot1x host-mode multi-host


Cisco(config-if)#dot1x port-control ?
  auto                 PortState will be set to AUTO
  force-authorized     PortState set to Authorized
  force-unauthorized  PortState will be set to UnAuthorized


Cisco(config-if)#dot1x port-control auto


Cisco(config-if)#dot1x auth-fail vlan 99


Cisco#show dot1x all summary
Interface       PAE     Client          Status
--------------------------------------------------------
Fa0/13          AUTH    000f.b001.bda4  AUTHORIZED
Fa0/17          AUTH    none            UNAUTHORIZED


Cisco#show dot1x interface f0/13 details

Dot1x Info for FastEthernet0/13
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
Violation Mode            = PROTECT
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Auth-Fail-Vlan            = 99
Auth-Fail-Max-attempts    = 3

Dot1x Authenticator Client List
-------------------------------
Domain                    = DATA

Supplicant                = 000f.b001.bda4
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
```

```
Authorized By             = Authentication Server
Vlan Policy               = 220


Cisco#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/11, Fa0/12, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
11   Data                             active    Fa0/18
12   Voice                            active    Fa0/3, Fa0/18
13   WLAN                             active
99   VLAN99                           active
100  lab_core                         active    Fa0/9, Fa0/10
220  test                             active    Fa0/5, Fa0/13
230  VLAN0230                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

b) MAC Authentication

ProVision	Comware 5	Cisco
`ProVision(config)# aaa port-access mac-based 19`	`[Comware5]mac-authentication`	`Cisco(config)#interface f0/13`
	`[Comware5]interface g1/0/19`	`Cisco(config-if)#dot1x mac-auth-bypass`
`ProVision(config)# aaa port-access mac-based 19 auth-vid 230`	`[Comware5-GigabitEthernet1/0/19]mac-authentication`	
`ProVision(config)# aaa port-access mac-based 19 unauth-vid 99`	`[Comware5]mac-authentication domain 8021x`	
	`[Comware5]mac-authentication user-name-format mac-address without-hyphen`	
`ProVision# show port-access mac-based config 19`	`[Comware5]display mac-authentication`	`Cisco#show dot1x interface f0/13 details`
	`[Comware5]display mac-authentication interface g1/0/19`	

ProVision

```
ProVision(config)# aaa port-access mac-based 19

ProVision(config)# aaa port-access mac-based 19 auth-vid 230

ProVision(config)# aaa port-access mac-based 19 unauth-vid 99


ProVision# show port-access mac-based config 19

 Port Access MAC-Based Configuration

  MAC Address Format : no-delimiter

  Mac password :

  Unauth Redirect Configuration URL :

  Unauth Redirect Client Timeout (sec) : 1800
  Unauth Redirect Restrictive Filter : Disabled
  Total Unauth Redirect Client Count : 0

                  Client Client Logoff    Re-Auth   Unauth   Auth     Cntrl
  Port   Enabled  Limit  Moves  Period    Period    VLAN ID  VLAN ID  Dir
  ------ --------- ------ ------ ---------- ---------- -------- -------- -----
  19     Yes       1      No     300        0          99       230      both
```

Comware 5

```
[Comware5]mac-authentication ?
  domain            Specify domain server configuration
  interface         Specify interface configuration information
  timer             Specify timer configuration
  user-name-format  Specify user name format
  <cr>

[Comware5]mac-authentication
 Mac-auth is enabled globally.
```

```
[Comware5]interface g1/0/19

[Comware5-GigabitEthernet1/0/19]mac-authentication ?
  guest-vlan  Specify guest VLAN configuration information
  <cr>

[Comware5-GigabitEthernet1/0/19]mac-authentication
 Mac-auth is enabled on port GigabitEthernet1/0/19.


[Comware5]mac-authentication domain 8021x

[Comware5]mac-authentication user-name-format ?
  fixed        Use fixed account
  mac-address  Use user's source MAC address as user name

[Comware5]mac-authentication user-name-format mac-address ?
  with-hyphen     MAC address with '-', just like XX-XX-XX-XX-XX-XX
  without-hyphen  MAC address without '-', just like XXXXXXXXXXXX
  <cr>

[Comware5]mac-authentication user-name-format mac-address without-hyphen ?
  <cr>

[Comware5]mac-authentication user-name-format mac-address without-hyphen



[Comware5]display mac-authentication ?
  interface  Display MAC-authentication interface configuration
  <cr>

[Comware5]display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address, like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
         Offline detect period is 300s
         Quiet period is 60s
         Server response timeout value is 100s
         The max allowed user number is 1024 per slot
         Current user number amounts to 1
         Current domain is 8021x
...


[Comware5]display mac-authentication interface g1/0/19
MAC address authentication is enabled.
 User name format is MAC address, like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
         Offline detect period is 300s
         Quiet period is 60s
         Server response timeout value is 100s
         The max allowed user number is 1024 per slot
         Current user number amounts to 1
         Current domain is 8021x

Silent MAC User info:
         MAC Addr         From Port                    Port Index

GigabitEthernet1/0/19 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Current online user number is 1
         MAC Addr         Authenticate State           Auth Index
         001a-4b92-5e24   MAC_AUTHENTICATOR_SUCCESS     34
```

Cisco

```
Cisco(config)#interface f0/13

Cisco(config-if)#dot1x mac-auth-bypass


Cisco#show dot1x interface f0/13 details

Dot1x Info for FastEthernet0/13
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
Violation Mode            = PROTECT
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Mac-Auth-Bypass           = Enabled
    Inactivity Timeout    = None
Auth-Fail-Vlan            = 99
Auth-Fail-Max-attempts    = 3


Dot1x Authenticator Client List Empty

Port Status               = UNAUTHORIZED
```

c) Web or Portal Authentication

ProVision	Comware 5	Cisco
	(note – requires an external Portal Authentication server)	(note - requires special configuration on the RADIUS server)
ProVision(config)# aaa port-access web-based 20-21		
ProVision(config)# aaa port-access web-based 20-21 auth-vid 240	[Comware5]domain web-auth	Cisco(config)#aaa new-model
ProVision(config)# aaa port-access web-based 20-21 unauth-vid 99	[Comware5-isp-web-auth]authentication portal radius-scheme radius-auth	Cisco(config)#aaa authorization auth-proxy default group radius
ProVision(config)# aaa port-access web-based 20-21 client-limit 5	[Comware5-isp-web-auth]authorization portal radius-scheme radius-auth	Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password
	[Comware5-isp-web-auth]accounting portal radius-scheme radius-auth	Cisco(config)#radius-server attribute 8 include-in-access-req
	[Comware5]domain default enable web-auth	Cisco(config)#radius-server vsa send authentication
	[Comware5]portal server weblogin ip 10.0.100.137 key password port 50100 url http://10.0.100.137/portal	Cisco(config)#ip access-list extended web-auth-policy1
	[Comware5]dhcp enable	Cisco(config-ext-nacl)#permit udp any any
	[Comware5]dhcp relay server-group 2 ip 10.0.100.251	Cisco(config-ext-nacl)#permit tcp any any eq www
	[Comware5]vlan 240	Cisco(config-ext-nacl)#deny ip any any
	[Comware5-vlan240]name portal-web_auth	Cisco(config)#ip admission name web-auth-rule1 proxy http
	[Comware5]interface Vlan-interface 240	Cisco(config)#interface f0/13
	[Comware5-Vlan-interface240]ip address 5.5.5.1 255.255.255.0	Cisco(config-if)#switchport mode access
	[Comware5-Vlan-interface240]ip address 10.1.240.3 255.255.255.0 sub	Cisco(config-if)#ip access-group web-auth-policy1 in
	[Comware5-Vlan-interface240]dhcp select relay	Cisco(config-if)#ip admission web-auth-rule1
	[Comware5-Vlan-interface240]dhcp relay server-select 2	
	[Comware5-Vlan-interface240]dhcp relay address-check enable	(web authentication as fallback to 802.1X authentication)
	[Comware5-Vlan-interface240]portal server weblogin method redhcp	Cisco(config)#fallback profile web-auth
	[Comware5-Vlan-interface240]portal domain web-auth	Cisco(config-fallback-profile)#ip access-group web-auth-policy1 in
	[Comware5]vlan 240	Cisco(config-fallback-profile)#ip admission web-

		auth-rule1
	[Comware5-vlan240]port g1/0/20	Cisco(config)#interface f0/13
		Cisco(config-if)#dot1x fallback web-auth
ProVision# show port-access web-based config 20-21	[Comware5]display portal connection statistics all	Cisco#show dot1x interface f0/13 details

ProVision

```
ProVision(config)# aaa port-access web-based 20-21

ProVision(config)# aaa port-access web-based 20-21 auth-vid 240

ProVision(config)# aaa port-access web-based 20-21 unauth-vid 99

ProVision(config)# aaa port-access web-based 20-21 client-limit 5


ProVision# show port-access web-based config 20-21

 Port Access Web-Based Configuration

  DHCP Base Address : 192.168.0.0
  DHCP Subnet Mask  : 255.255.255.0
  DHCP Lease Length : 10
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

                  Client Client Logoff     Re-Auth    Unauth   Auth     Cntrl
  Port   Enabled  Limit  Moves  Period     Period     VLAN ID  VLAN ID  Dir
  ------ -------- ------ ------ ---------- ---------- -------- -------- -----
  20     Yes      5      No     300        0          99       240      both
  21     Yes      5      No     300        0          99       240      both
```

Comware 5

```
(note - requires an external Portal Authentication server)


[Comware5]domain web-auth
New Domain added.

[Comware5-isp-web-auth]authentication portal radius-scheme radius-auth

[Comware5-isp-web-auth]authorization portal radius-scheme radius-auth

[Comware5-isp-web-auth]accounting portal radius-scheme radius-auth

[Comware5]domain default enable web-auth


[Comware5]portal ?
  delete-user  Delete user
  free-rule    Configure free rule
  server       Configure portal server

[Comware5]portal server ?
  STRING<1-32>  Portal server name

[Comware5]portal server weblogin ?
```

```
  ip  Configure IP address

[Comware5]portal server weblogin ip ?
  X.X.X.X  IP address

[Comware5]portal server weblogin ip 10.0.100.137 ?
  key   Configure shared encryption key of portal server
  port  Configure receive port of portal server
  url   Configure URL of portal server
  <cr>

[Comware5]portal server weblogin ip 10.0.100.137 key ?
  STRING<1-16>  Key string

[Comware5]portal server weblogin ip 10.0.100.137 key password ?
  port  Configure receive port of portal server
  url   Configure URL of portal server
  <cr>

[Comware5]portal server weblogin ip 10.0.100.137 key password port ?
  INTEGER<1-65534>  Portal server received packets on this port. Default:50100

[Comware5]portal server weblogin ip 10.0.100.137 key password port 50100 ?
  url   Configure URL of portal server
  <cr>

[Comware5]portal server weblogin ip 10.0.100.137 key password port 50100 url ?
  STRING<1-127>  URL string of portal server

[Comware5]portal server weblogin ip 10.0.100.137 key password port 50100 url http://
10.0.100.137/portal ?
  <cr>

[Comware5]portal server weblogin ip 10.0.100.137 key password port 50100 url http://
10.0.100.137/portal


[Comware5]dhcp enable

[Comware5]dhcp relay server-group 2 ip 10.0.100.251


[Comware5]vlan 240

[Comware5-vlan240]name portal-web_auth


[Comware5]interface Vlan-interface 240

[Comware5-Vlan-interface240]ip address 5.5.5.1 255.255.255.0

[Comware5-Vlan-interface240]ip address 10.1.240.3 255.255.255.0 sub

[Comware5-Vlan-interface240]dhcp select relay

[Comware5-Vlan-interface240]dhcp relay server-select 2
```

```
[Comware5-Vlan-interface240]dhcp relay address-check enable

[Comware5-Vlan-interface240]portal ?
  auth-network  Authenticate network
  domain        Configure domain
  server        Enable portal on the interface

[Comware5-Vlan-interface240]portal server ?
  STRING<1-32>  Portal server name

[Comware5-Vlan-interface240]portal server weblogin ?
  method  Configure portal running method

[Comware5-Vlan-interface240]portal server weblogin method ?
  direct  Direct method
  layer3  Layer3 method
  redhcp  Redhcp method

[Comware5-Vlan-interface240]portal server weblogin method redhcp ?
  <cr>

[Comware5-Vlan-interface240]portal server weblogin method redhcp

[Comware5-Vlan-interface240]portal domain web-auth


[Comware5]vlan 240

[Comware5-vlan240]port g1/0/20



[Comware5]display portal connection statistics all
 ---------------Interface: Vlan-interface240-----------------------
 User state statistics:
 State-Name                 User-Num
 VOID                       0
 DISCOVERED                 0
 WAIT_AUTHEN_ACK            0
 WAIT_AUTHOR_ACK            0
 WAIT_LOGIN_ACK             0
 WAIT_ACL_ACK               0
 WAIT_NEW_IP                0
 WAIT_USERIPCHANGE_ACK      0
 ONLINE                     0
 WAIT_LOGOUT_ACK            0
 WAIT_LEAVING_ACK           0

 Message statistics:
 Msg-Name                   Total         Err           Discard
 MSG_AUTHEN_ACK             0             0             0
 MSG_AUTHOR_ACK             0             0             0
 MSG_LOGIN_ACK              0             0             0
 MSG_LOGOUT_ACK             0             0             0
 MSG_LEAVING_ACK            0             0             0
 MSG_CUT_REQ                0             0             0
 MSG_AUTH_REQ               0             0             0
 MSG_LOGIN_REQ             0             0             0
 MSG_LOGOUT_REQ            0             0             0
 MSG_LEAVING_REQ           0             0             0
 MSG_ARPPKT                0             0             0
 MSG_TMR_REQAUTH           0             0             0
 MSG_TMR_AUTHEN            0             0             0
 MSG_TMR_AUTHOR            0             0             0
 MSG_TMR_LOGIN             0             0             0
 MSG_TMR_LOGOUT            0             0             0
 MSG_TMR_LEAVING           0             0             0
 MSG_TMR_NEWIP             0             0             0
 MSG_TMR_USERIPCHANGE      0             0             0
 MSG_PORT_REMOVE           0             0             0
 MSG_VLAN_REMOVE           0             0             0
 MSG_IF_REMOVE             0             0             0
 MSG_L3IF_SHUT             5             0             0
 MSG_CUT_L3IF              0             0             0
 MSG_IP_REMOVE             0             0             0
 MSG_ALL_REMOVE            0             0             0
 MSG_IFIPADDR_CHANGE       0             0             0
 MSG_SOCKET_CHANGE         1             0             0
 MSG_NOTIFY                0             0             0
 MSG_SETPOLICY             0             0             0
 MSG_SETPOLICY_RESULT      0             0             0
```

Cisco

```
(note - requires special configuration on the RADIUS server)


Cisco(config)#aaa new-model

Cisco(config)#aaa authorization auth-proxy default group radius

Cisco(config)#radius-server host 10.0.100.111 auth-port 1812 acct-port 1813 key password

Cisco(config)#radius-server attribute 8 include-in-access-req

Cisco(config)#radius-server vsa send authentication


Cisco(config)#ip access-list extended web-auth-policy1

Cisco(config-ext-nacl)#permit udp any any

Cisco(config-ext-nacl)#permit tcp any any eq www

Cisco(config-ext-nacl)#deny ip any any


Cisco(config)#ip admission name web-auth-rule1 proxy http

Cisco(config)#interface f0/13

Cisco(config-if)#switchport mode access

Cisco(config-if)#ip access-group web-auth-policy1 in

Cisco(config-if)#ip admission web-auth-rule1


(web authentication as fallback to 802.1X authentication)
```

```
Cisco(config)#fallback profile web-auth

Cisco(config-fallback-profile)#ip access-group web-auth-policy1 in

Cisco(config-fallback-profile)#ip admission web-auth-rule1

Cisco(config)#interface f0/13

Cisco(config-if)#dot1x fallback web-auth


Cisco#show dot1x interface f0/13 details

Dot1x Info for FastEthernet0/13
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
Violation Mode            = PROTECT
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Webauth                   = Enabled
Auth-Fail-Vlan            = 99
Auth-Fail-Max-attempts    = 3

Dot1x Authenticator Client List Empty


Port Status               = UNAUTHORIZED
```

Chapter 31 Port Mirroring or Span

This chapter compares the commands used to configure local mirroring and remote mirroring.

a) Local Mirror or SPAN

ProVision	Comware 5	Cisco
(Note: ProVision manual indicates to configure destination then source)	(Note: Comware 5 manual indicates to configure destination then source)	(Note: Cisco manual indicates to configure source then destination)
ProVision(config)# mirror 1 port 12	[Comware5]mirroring-group 1 local	Cisco(config)#monitor session 1 source interface f0/6 both
ProVision(config)# interface 11 monitor all both mirror 1	[Comware5]mirroring-group 1 mirroring-port g1/0/18 both	Cisco(config)# monitor session 1 destination interface f0/12 encapsulation replicate
	[Comware5]mirroring-group 1 monitor-port g1/0/2	
ProVision# show monitor		Cisco#show monitor
ProVision# show monitor 1	[Comware5]display mirroring-group 1	Cisco#show monitor session 1
		Cisco#show monitor session 1 detail

ProVision

```
(note - ProVision manual indicates to configure destination then source)


ProVision(config)# mirror ?
 endpoint              Remote mirroring destination configuration.
 <1-4>                 Mirror destination number.

ProVision(config)# mirror 1 ?
 name                  Mirroring destination name string.
 port                  Mirroring destination monitoring port.
 remote                Remote mirroring destination configuration.

ProVision(config)# mirror 1 port ?
 [ethernet] PORT-NUM   Enter a port name for the 'port' command/parameter.

ProVision(config)# mirror 1 port 12 ?
 <cr>

ProVision(config)# mirror 1 port 12


ProVision(config)# interface 11 monitor ?
 all                   Monitor all traffic.
 <cr>

ProVision(config)# interface 11 monitor all ?
 in                    Monitor all inbound traffic
 out                   Monitor all outbound traffic
 both                  Monitor all inbound and outbound traffic

ProVision(config)# interface 11 monitor all both ?
 mirror                Mirror destination.

ProVision(config)# interface 11 monitor all both mirror ?
 <1-4>                 Mirror destination number.
```

```
ProVision(config)# interface 11 monitor all both mirror 1 ?
 no-tag-added          Don't add VLAN tag for this untagged-port
 <1-4>                 Mirror destination number.
 <cr>

ProVision(config)# interface 11 monitor all both mirror 1


ProVision# show monitor

Network Monitoring

   Sessions  Status       Type    Sources  Mirror-Policy
   --------  -----------  -----   -------  -------------
   1         active        port   1        no
   2         not defined
   3         not defined
   4         not defined

There are no Remote Mirroring endpoints currently assigned.


ProVision# show monitor 1
Network Monitoring

   Session: 1    Session Name:
   Mirror Policy: no mirror policy exists

      Mirror Destination:  12    (Port)

      Monitoring Sources  Direction
      ------------------  ---------
      Port: 11            Both
```

Comware 5

```
(note - Comware 5 manual indicates to configure destination then source)


[Comware5]mirroring-group ?
  INTEGER<1-4>  Mirroring group number

[Comware5]mirroring-group 1 ?
  local                Local mirroring group
  mirroring-port       Specify mirroring port
  monitor-egress       Specify monitor-egress port
  monitor-port         Specify monitor port
  remote-destination   Remote destination mirroring group
  remote-probe         Specify remote probe VLAN
  remote-source        Remote source mirroring group

[Comware5]mirroring-group 1 local ?
  <cr>

[Comware5]mirroring-group 1 local


[Comware5]mirroring-group 1 mirroring-port ?
  GigabitEthernet  GigabitEthernet interface

[Comware5]mirroring-group 1 mirroring-port g1/0/18 ?
```

```
  GigabitEthernet  GigabitEthernet interface
  both             Monitor the inbound and outbound packets
  inbound          Monitor the inbound packets
  outbound         Monitor the outbound packets
  to               Range of interfaces

[Comware5]mirroring-group 1 mirroring-port g1/0/18 both ?
  <cr>

[Comware5]mirroring-group 1 mirroring-port g1/0/18 both


[Comware5]mirroring-group 1 monitor-?
   monitor-egress
   monitor-port

[Comware5]mirroring-group 1 monitor-port ?
  Bridge-Aggregation  Bridge-Aggregation interface
  GigabitEthernet     GigabitEthernet interface

[Comware5]mirroring-group 1 monitor-port g1/0/2 ?
  <cr>

[Comware5]mirroring-group 1 monitor-port g1/0/2


[Comware5]display mirroring-group ?
  INTEGER<1-4>        Mirroring group number
  all                 all mirroring group
  local               Local mirroring group
  remote-destination  Remote destination mirroring group
  remote-source       Remote source mirroring group

[Comware5]display mirroring-group 1 ?
  <cr>

[Comware5]display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/18  both
    monitor port: GigabitEthernet1/0/2
```

Cisco

```
(note - Cisco manual indicates to configure source then destination)


Cisco(config)#monitor ?
  event-trace  Tracing of system events
  session      Configure a SPAN session

Cisco(config)#monitor session ?
  <1-66>  SPAN session number

Cisco(config)#monitor session 1 ?
  destination  SPAN destination interface or VLAN
  filter       SPAN filter VLAN
  source       SPAN source interface, VLAN

Cisco(config)#monitor session 1 source ?
  interface  SPAN source interface
  remote     SPAN source Remote
  vlan       SPAN source VLAN

Cisco(config)#monitor session 1 source interface f0/6 ?
  ,     Specify another range of interfaces
  -     Specify a range of interfaces
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

Cisco(config)#monitor session 1 source interface f0/6 both ?
  <cr>

Cisco(config)#monitor session 1 source interface f0/6 both


Cisco(config)#monitor session 1 ?
  destination  SPAN destination interface or VLAN
  filter       SPAN filter VLAN
  source       SPAN source interface, VLAN

Cisco(config)#monitor session 1 destination ?
  interface  SPAN destination interface
  remote     SPAN destination Remote


Cisco(config)#monitor session 1 destination interface f0/12 ?
  ,              Specify another range of interfaces
  -              Specify a range of interfaces
  encapsulation  Set encapsulation for destination interface
  ingress        Enable ingress traffic forwarding
  <cr>


Cisco(config)#monitor session 1 destination interface f0/12 encapsulation ?
  dot1q      interface uses only dot1q encapsulation
  isl        interface uses only isl encapsulation
  replicate  interface replicates source encapsulation

Cisco(config)#monitor session 1 destination interface f0/12 encapsulation replicate ?
  ingress  Enable ingress traffic forwarding
  <cr>

Cisco(config)# monitor session 1 destination interface Fa0/12 encapsulation replicate


Cisco#show monitor
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/6
Destination Ports      : Fa0/12
    Encapsulation      : Replicate
          Ingress      : Disabled


Cisco#show monitor session 1
Session 1
---------
```

```
Type                   : Local Session
Source Ports           :
    Both               : Fa0/6
Destination Ports      : Fa0/12
    Encapsulation      : Replicate
          Ingress      : Disabled


Cisco#show monitor session 1 detail
Session 1
---------
Type                   : Local Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Fa0/6
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : Fa0/12
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : None
Dest RSPAN VLAN        : None
```

b) Remote Mirror or RSPAN

With remote mirroring on ProVision, mirrored traffic can traverse IP networks. With remote mirroring on Comware 5 and Cisco, mirrored traffic must be in the same subnet.

ProVision	Comware 5	Cisco
(switch where analyzer is connected)	(switch with traffic of interest)	(switch where analyzer is connected)
ProVision(config)# mirror endpoint ip 10.0.1.1 7922 10.0.100.24 port 12	[Comware5]mirroring-group 1 remote-source	Cisco(config)#vlan 950
	[Comware5]vlan 960	Cisco(config-vlan)#remote-span
	[Comware5]mirroring-group 1 remote-probe vlan 960	Cisco(config)#interface f0/9
	[Comware5]mirroring-group 1 mirroring-port g1/0/18 both	Cisco(config-if)#switchport trunk encapsulation dot1q
	[Comware5]mirroring-group 1 monitor-egress g1/0/6	Cisco(config-if)#switchport trunk allowed vlan 100,950
		Cisco(config-if)#switchport mode trunk
		Cisco(config-if)#switchport nonegotiate
		Cisco(config)#monitor session 1 source remote vlan 950
		Cisco(config)#monitor session 1 destination interface f0/12 encapsulation replicate
ProVision# show monitor		Cisco#show monitor
ProVision# show monitor endpoint		Cisco#show monitor session 1
(switch with traffic of interest)	(switch where analyzer is connected)	(switch with traffic of interest)
ProVision2(config)# mirror 1 remote ip 10.0.1.1 7922 10.0.100.24	[Comware52]vlan 960	Cisco2(config)#vlan 950
ProVision2(config)# interface 18 monitor all both mirror 1	[Comware52]interface g1/0/1	Cisco2(config-vlan)#remote-span
	[Comware52-GigabitEthernet1/0/1]port link-type trunk	Cisco2(config)#interface f0/17
	[Comware52-GigabitEthernet1/0/1]port trunk permit vlan 960	Cisco2(config-if)#switchport trunk encapsulation dot1q
	[Comware52]mirroring-group 1 remote-destination	Cisco2(config-if)#switchport trunk allowed vlan 100,950
	[Comware52]mirroring-group 1 remote-probe vlan 960	Cisco2(config-if)#switchport mode trunk
	[Comware52]mirroring-group 1 monitor-port g1/0/2	Cisco2(config-if)#switchport nonegotiate
		Cisco2(config)# monitor session 1 source interface FastEthernet0/22
		Cisco2(config)# monitor session 1 destination remote vlan 950
ProVision2# show monitor 1	[Comware5]display mirroring-group 1	Cisco2#show monitor
		Switch2#show monitor session 1 detail

ProVision

```
(switch where analyzer is connected)


ProVision(config)# mirror endpoint ip 10.0.1.1 7922 10.0.100.24 port 12


ProVision# show monitor
Network Monitoring

   Sessions  Status       Type    Sources  Mirror-Policy
   --------  -----------  -----   -------  -------------
   1         active        port   1        no
   2         not defined
   3         not defined
   4         not defined

Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr    Dest Port
 ----  ---------------  --------  ---------------  ---------
 IPv4  10.0.1.1         7922      10.0.100.24      12


ProVision# show monitor endpoint
Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr    Dest Port
 ----  ---------------  --------  ---------------  ---------
 IPv4  10.0.1.1         7922      10.0.100.24      12



(switch with traffic of interest)

ProVision2(config)# mirror 1 remote ip 10.0.1.1 7922 10.0.100.24
Caution: Please configure destination switch first.
         Do you want to continue [y/n]?  y

ProVision2(config)# interface 18 monitor all both mirror 1


ProVision2# show monitor 1
Network Monitoring

   Session: 1    Session Name:
   Mirror Policy: no mirror policy exists

      Mirror Destination:  IPv4
         UDP Source Addr  UDP port  UDP Dest Addr    Status
         ---------------  --------  ---------------  --------
         10.0.1.1         7922      10.0.100.24      active

      Monitoring Sources  Direction
      ------------------  ---------
      Port: 18            Both
```

Comware 5

```
(switch with traffic of interest)
```

```
[Comware5]mirroring-group 1 ?
  local               Local mirroring group
  mirroring-port      Specify mirroring port
  monitor-egress      Specify monitor-egress port
  monitor-port        Specify monitor port
  remote-destination  Remote destination mirroring group
  remote-probe        Specify remote probe VLAN
  remote-source       Remote source mirroring group

[Comware5]mirroring-group 1 remote-source ?
  <cr>

[Comware5]mirroring-group 1 remote-source


[Comware5]vlan 960

[Comware5-vlan960]quit


[Comware5]mirroring-group 1 ?

[Comware5]mirroring-group 1 remote-probe ?
  vlan  Specify VLAN

[Comware5]mirroring-group 1 remote-probe vlan 10 ?
  <cr>

[Comware5]mirroring-group 1 remote-probe vlan 960


[Comware5]mirroring-group 1 mirroring-port g1/0/18 ?
  GigabitEthernet  GigabitEthernet interface
  both             Monitor the inbound and outbound packets
  inbound          Monitor the inbound packets
  outbound         Monitor the outbound packets
  to               Range of interfaces

[Comware5]mirroring-group 1 mirroring-port g1/0/18 both


[Comware5]mirroring-group 1 monitor-egress g1/0/6 ?
  <cr>

[Comware5]mirroring-group 1 monitor-egress g1/0/6


[Comware5]interface g1/0/6

[Comware5-GigabitEthernet1/0/6]port link-type trunk

[Comware5-GigabitEthernet1/0/6]port trunk permit vlan 960



(switch where analyzer is connected)
```

```
[Comware52]vlan 960

[Comware52-vlan960]port g1/0/2

[Comware52-vlan960]quit


[Comware52]interface g1/0/1

[Comware52-GigabitEthernet1/0/1]port link-type trunk

[Comware52-GigabitEthernet1/0/1]port trunk permit vlan 960

[Comware52-GigabitEthernet1/0/1]quit


[Comware52]mirroring-group 1 remote-destination

[Comware52]mirroring-group 1 remote-probe vlan 960

[Comware52]mirroring-group 1 monitor-port g1/0/2
```

Cisco

```
(switch where analyzer is connected)


Cisco(config)#vlan 950

Cisco(config-vlan)#remote-span

Cisco(config)#interface FastEthernet0/9

Cisco(config-if)#switchport trunk encapsulation dot1q

Cisco(config-if)#switchport trunk allowed vlan 100,950

Cisco(config-if)#switchport mode trunk

Cisco(config-if)#switchport nonegotiate


Cisco(config)#monitor session 1 source ?
  interface  SPAN source interface
  remote     SPAN source Remote
  vlan       SPAN source VLAN

Cisco(config)#monitor session 1 source remote ?
  vlan  Remote SPAN source RSPAN VLAN

Cisco(config)#monitor session 1 source remote vlan 950 ?
  <cr>

Cisco(config)#monitor session 1 source remote vlan 950

Cisco(config)#monitor session 1 destination interface f0/12 encapsulation replicate


Cisco#show monitor
Session 1
---------
```

```
Type                    : Remote Destination Session
Source RSPAN VLAN       : 950
Destination Ports       : Fa0/12
    Encapsulation       : Replicate
          Ingress       : Disabled


Cisco#show monitor session 1
Session 1
---------
Type                    : Remote Destination Session
Source RSPAN VLAN       : 950
Destination Ports       : Fa0/12
    Encapsulation       : Replicate
          Ingress       : Disabled


Cisco#show monitor session 1 detail
Session 1
---------
Type                    : Remote Destination Session
Description             : -
Source Ports            :
    RX Only             : None
    TX Only             : None
    Both                : None
Source VLANs            :
    RX Only             : None
    TX Only             : None
    Both                : None
Source RSPAN VLAN       : 950
Destination Ports       : Fa0/12
    Encapsulation       : Replicate
          Ingress       : Disabled
Filter VLANs            : None
Dest RSPAN VLAN         : None



(switch with traffic of interest)


Cisco2(config)#vlan 950

Cisco2(config-vlan)#remote-span


Cisco2(config)#interface FastEthernet0/17

Cisco2(config-if)#switchport trunk encapsulation dot1q

Cisco2(config-if)#switchport trunk allowed vlan 100,950

Cisco2(config-if)#switchport mode trunk

Cisco2(config-if)#switchport nonegotiate


Cisco2(config)# monitor session 1 source interface FastEthernet0/22

Cisco2(config)# monitor session 1 destination remote vlan 950



Cisco2#show monitor
```

```
Session 1
---------
Type                   : Remote Source Session
Source Ports           :
    Both               : Fa0/22
Dest RSPAN VLAN        : 950


Switch2#show monitor session 1 detail
Session 1
---------
Type                   : Remote Source Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Fa0/22
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : None
Filter VLANs           : None
Dest RSPAN VLAN        : 950
```

Index

To learn more about HP Networking, visit www.hp.com/go/procurve