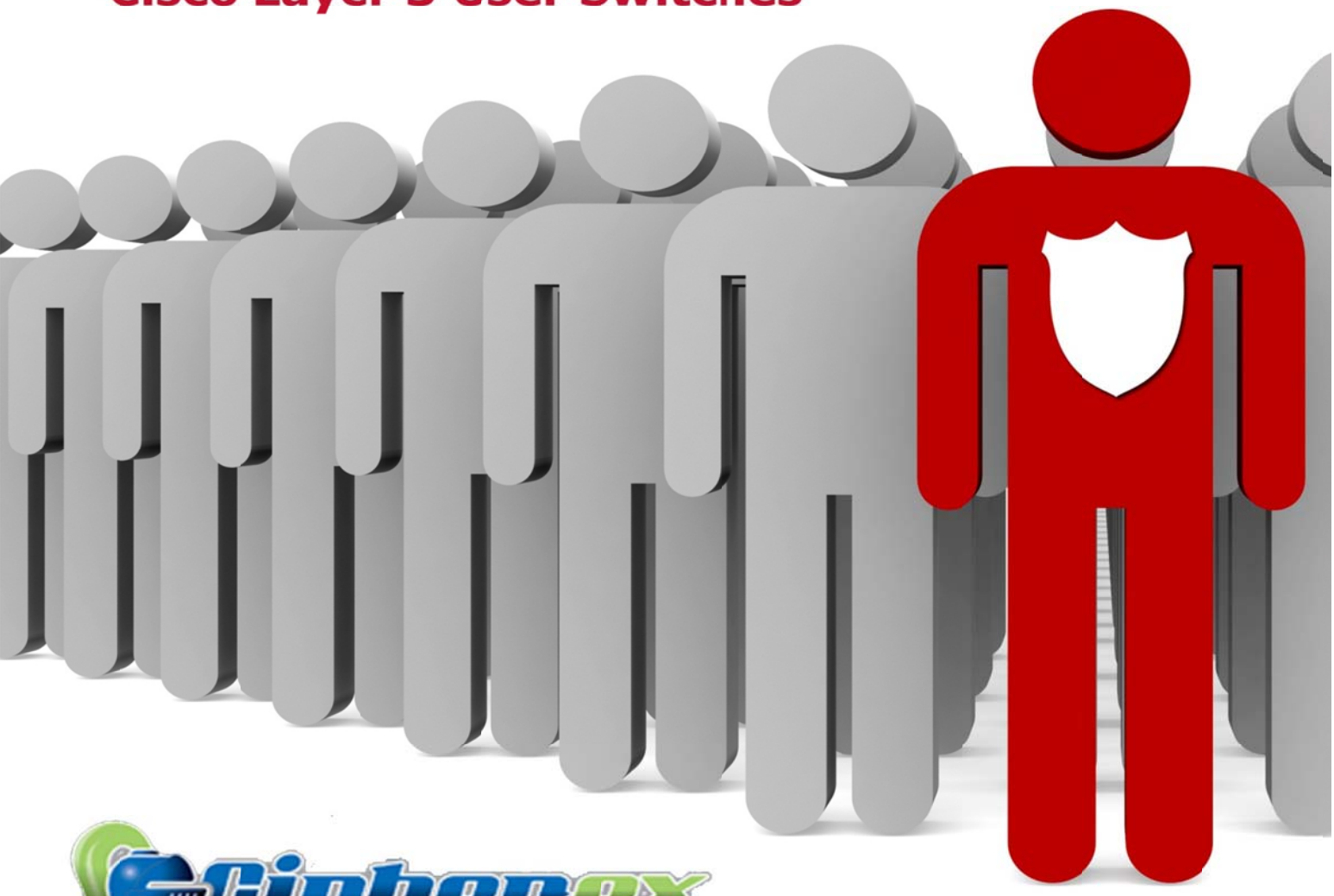
User Switch Hardening Guide

An interactive handbook for securing
Cisco Layer 3 User Switches



Cipherex

Layer 3 User-Switch Hardening Guide

Published by Web Direct Studio, 118 Gatley Road, Cheadle, Cheshire, SK8 4AD, UK.

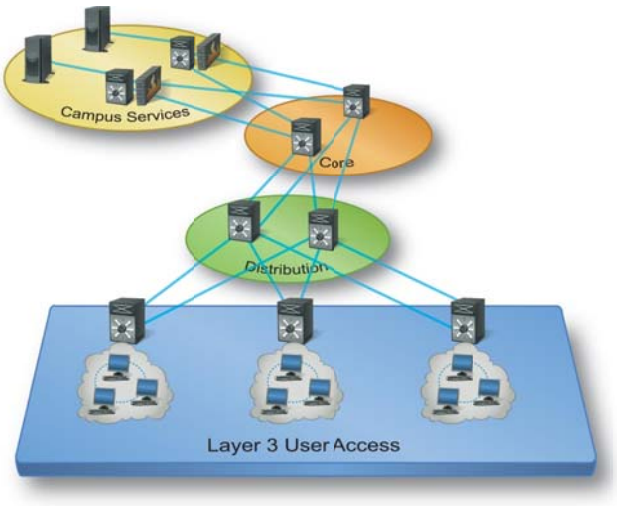
Editing, cover and interior design by WebDirectStudio
www.webdirectstudio.com (website)
info@webdirectstudio.com (email)

Layer 3 User-Switch Hardening Guide

Overview

This document provides detailed information on the recommended hardening standards for user switches at access layer 3. The configuration is based on the understanding that user switches can have many different types of devices connected to them, including workstations, Internet Protocol (IP) phones, access points, and printers. The objective of this hardening standard is to reduce the risk of layer 2 and layer 3 attacks that can be launched against internal user switches. Moreover, this standard guards against unauthorized connections of rogue devices to the corporate infrastructure. Some of the main security countermeasures recommended in this document are as follows:

- Port Security to prevent Media Access Control (MAC) flooding attacks
- Dynamic Host Configuration Protocol (DHCP) snooping to prevent man-in-the-middle attacks against clients and servers
- Address Resolution Protocol (ARP) inspection using the DHCP snooping table to enhance security
- IP Source Guard using the DHCP snooping table to enhance protection against IP source address spoofing
- Bridge Protocol Data Unit (BPDU) guard to defend against spanning-tree attacks
- Routing protocol security to prevent false route injections into the network
- Implementation of guest Virtual Local Area Networks (VLANs) to provide limited access for vendors and visitors



Audience

The intended audience comprises network and security engineers interested in hardening Cisco switches.

Assumptions

All user access switches are layer 3 Cisco switches.

A stable and bug-free Cisco Internet Operating System has been selected.

All unused switch ports will be configured in a shutdown state.

QoS (Quality of Service) will be configured by the system administrator as appropriate.

Trademark Information

IOS is a registered trademark of Cisco Systems, Inc., in the United States and other countries.

Hardening Steps

This document is for use as a general guide to harden user switches. Users should modify it as needed to meet corporate policy standards.

Command	Description
service nagle	The Nagle algorithm is used to alleviate excess traffic generated by many small packs. Operation of the algorithm is as follows: • The first character typed is sent in a single packet. • TCP (Transmission Control Protocol) holds additional packets until it receives an acknowledgment. • Additional queued characters are then sent. TCP waits until it receives an acknowledgment for each transmission. Characters are grouped together for transmission, thereby reducing the overall network traffic.
no service pad	The Packet Assembler/Disassembler (PAD) is used to buffer, assemble, and disassemble packets in X.25 networks. This user switch has no need to run X.25; therefore it is disabled.
service tcp-keepalives-in	This command configures the switch to send keep-alive packets to a remote station that has an idle incoming TCPconnection. In the event of an abrupt termination of Telnet or of a Secure Shell (SSH) connection to the switch, the command clears orphan VTY (Virtual Teletype Terminal) lines to allow the establishment of another connection.
service tcp-keepalives-out	This command performs the same functionality as **service tcp-keepalives-in**, except for outgoing TCP connections from the switch.
service timestamp debug datetime msec localtime show-timezone	Time-stamp system-generated debug messages with date and time **datetime**: stamps date and time in MMM,DD HH:MM:SS format. **msec**: adds millisecond accuracy to the time stamp in

	mmm format (MMM,DD HH:MM:SS:mmm). **localtime**: uses local time of the switch. **show-timezone**: appends the time zone: UTC, PST, EST, etc.
service timestamp log datetime msec localtime show-timezone	Time-stamp system-generated log messages with date and time **datetime**: stamps date and time in MMM,DD HH:MM:SS format. **msec**: adds millisecond accuracy to the time stamp in mmm format (MMM,DD HH:MM:SS:mmm). **localtime**: uses local time of the switch. **show-timezone**: appends the time zone: UTC, PST, EST, etc.
service password-encryption	Obscures all clear-text passwords on the system. The encryption is easily reversible, but it is still better than having passwords in the clear. The command does not apply to "secret password," which uses MD5 for hashing and is a stronger algorithm. Password encryption applies to all of the following: • passwords • user-name passwords • authentication key passwords • privileged command passwords • console and virtual terminal-line access passwords • Border Gateway Protocol (BGP) neighbor passwords
service sequence-numbers	Service sequence numbers add visible line numbers to system log messages. Sequence numbers increase by one for each message the system generates. Missing numbers indicate that data are missing or have been tampered with.
no service tcp-small-servers	TCP and UDP (User Datagram Protocol) small servers (daemons in Unix parlance) run on the switch and may be useful for diagnostics. The TCP small servers: **echo:** Echoes back whatever is typed through TCP. **chargen**: Generates a stream of ASCII data. **discard:** Throws away whatever is typed. **daytime:** Returns system date and time. TCP small services on the switch are disabled because they are not being

used and thus pose a security risk.

no service udp-small-servers

The UDP small servers:

echo: Echoes the payload of the datagram sent.
discard: Silently discards the datagram sent.
chargen: Discards the datagram sent and responds with a 72-character string of ASCII characters terminated with a CR+LF

UDP small services on the switch are being disabled because they are not being used and pose a security risk.

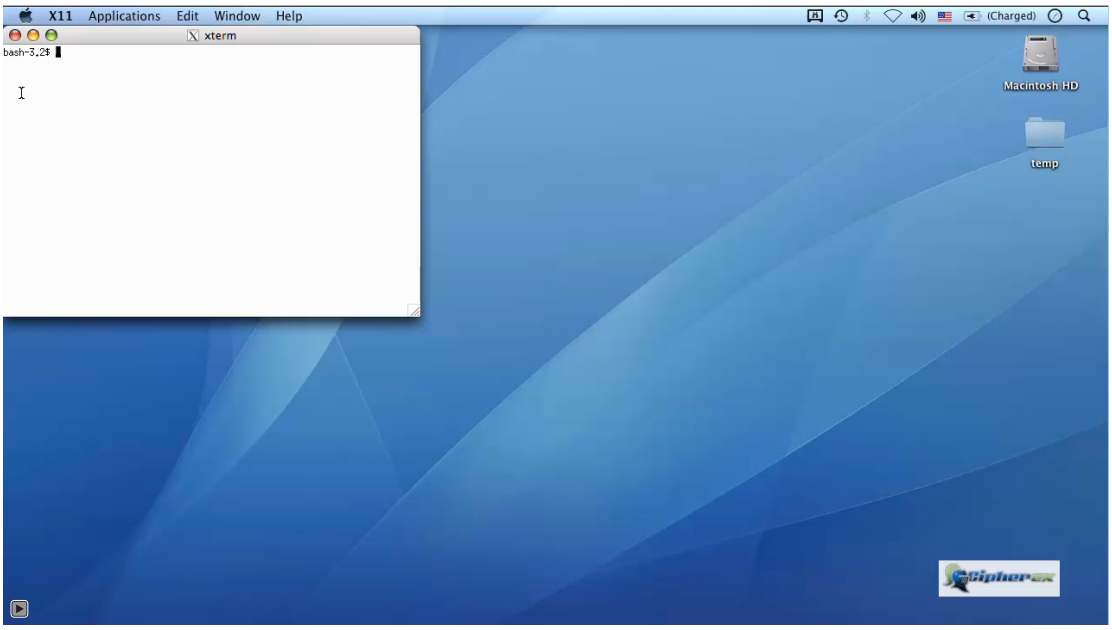
no service finger

The IP Finger service provides information about current logged-in administrators on the switch. This feature is disabled to minimize user-name leakage.

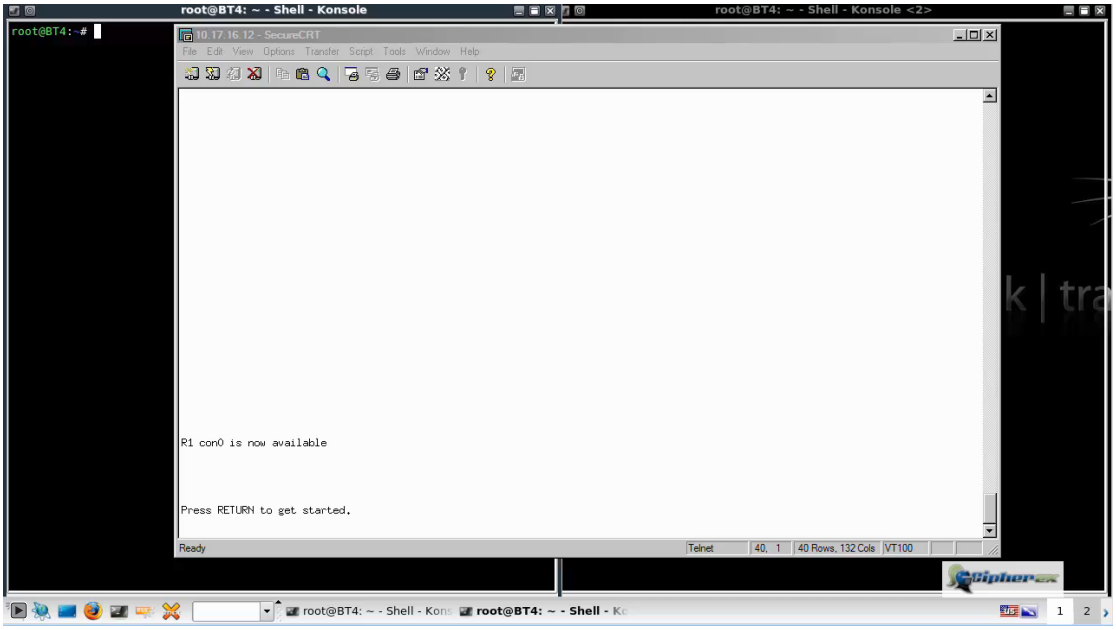
no service config

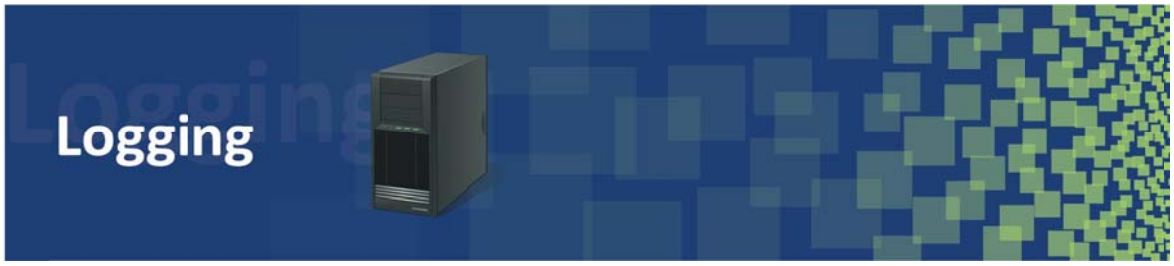
This command disables the functionality to load configuration files at system restart.

Video: Click on the image below to play the Video



Video: Click on the image below to play the Video





Command	Description
logging buffered 32000 informational	Logs system messages to the switch's Random Access Memory (RAM). The buffer is circular and is overwritten when the specified allocated memory is full. The buffered memory size is dependent on the amount of memory available. In general, a buffer size of 10,000 to 32,000 bytes is an acceptable range and should not overwhelm the switch. The **buffered** key word specifies RAM as the destination of logging information. The **32000** parameter allocates 32,000 bytes of memory for buffered logs. The **informational** key word instructs the system to send log messages to the buffer that range from informational (level 6) to emergency (level 0). Debug (level 7) messages will not be logged. Logging debug messages during normal system operation is not recommended.
no logging console	Do not send log messages to the console port.
no logging monitor	Do not send log messages to remote monitor sessions.
logging rate-limit all 10 except errors	This command may reduce switch load and network traffic. Here the logs are rate limited to 10 events per second, except for events ranging from errors (level 3) to emergency (level 0). The **all** key word limits all messages, including debug when it is logged. The **except errors** key word will not rate limit errors and higher priority log messages; only warning (level 4) to debug (level 7) messages will be rate limited.
logging trap warnings	Log warnings (level 6) and higher-level messages to the log server.

logging facility local2	When sending logs, mark them for facility local2. (Any facility that matches the reporting structure may be chosen). The syslog server will group different facilities together.
logging source-interface Loopback0	Uses the IP address of loopback0 interface to source log messages to the syslog server.

See related commands.

Service sequence-numbers

service timestamp log datetime msec localtime show-timezone

Command	Description
aaa new-model	Authentication, authorization, and accounting (AAA) network security services provide the primary framework to set up access controls on the switch. The **aaa new-model** enables the AAA process.
aaa local authentication attempts max-fail 4	Sets the maximum authentication attempts to 4 for user names configured locally on the system. *Note: With current configuration, local authentication will take effect only when TACAC+* (Terminal Access Controller Access Control System) *services are not available.*
aaa authentication login default group tacacs+ local	Authenticates administrator access to the switch. Upon successful authentication, the administrator will be presented the switch level 1 (switch_name>) command prompt. **Login:** Authentication for console log-in. This is the log-in to the switch prior to enable-mode authentication. **Default:** Defines the default method used to authenticate administrator access to the switch when a named method is not used on a VTY, a Con line, or the Aux ports. **Group tacacs+:** Uses the list of all TACACS+ servers for authentication. **Local**: If TACACS+ is unavailable, uses the local user name and password account configured on the switch for log-in. If this key word is not included and access to the TACACS+ server is cut off, administrators will be unable to log in.
aaa authentication enable default group tacacs+ local	Authenticates administrative access to the switch's enable mode. Upon successful authentication, the administrator will

be presented the switch-privileged level (switch_name#) command prompt.

Enable: Authentication for enable mode access.

Default: Defines the default method used to authenticate administrator access to the switch when a named method is not used on a VTY, a Con line, or the Aux ports.

Group tacacs+: Uses the list of all TACACS+ servers for authentication.

Local: If TACACS+ is unavailable, use the local user name and password account configured on the switch for log-in. If this key word is not input and access to the TACACS+ server is cut off, administrators will be unable to log in.

aaa authorization commands 0 default group tacacs+ none

Authorizes level 0 commands issued by the device administrator.

Commands: Authorizes commands.

0: Level 0 (switch>) commands.

Default: Defines the default method used to authorize level 0 commands.

Group tacacs+: Uses TACACS+ servers for authentication.

None: This is a fail-safe measure allowing device administrators to run any command at their current authorization level when the TACACS+ server is unavailable.

*As an option, the key word **local** can replace **none** to facilitate local authorization.*

A local authorization command will need to be added.

aaa authorization commands 1 default group tacacs+ none

Authorizes level 1 commands issued by the device administrator.

Commands: Authorizes commands.

1: Level 1 (switch>) commands.

Default: Defines the default method used to authorize

level 1 commands.

Group tacacs+: Uses TACACS+ servers for authentication.

None: This is a fail-safe measure allowing device administrators to run any command at their current authorization level when the TACACS+ server is unavailable.

*Note: As an option, the key word **local** can replace **none** to facilitate local authorization.*

A local authorization command will need to be added.

aaa authorization commands 15 default group tacacs+ none

Authorizes level 15 commands issued by the device administrator.

Commands: Authorizes commands.

15: Level 15 (switch#) commands.

Default: Defines the default method used to authorize level 15 commands.

Group tacacs+: Uses TACACS+ servers for authorization.

None: This is a fail-safe measure allowing device administrators to run any command at their current authorization level when the TACACS+ server is unavailable.

*Note: As an option, the key word **local** can replace **none** to facilitate local authorization.*

A local authorization command will need to be added.

aaa authorization exec default group tacacs+ none

Authorizes exec-level access on the switch.

Exec: Authorizes exec shell.

Default: Defines the default method used to authorize exec-shell access.

Group tacacs+: Uses TACACS+ servers for authorization.

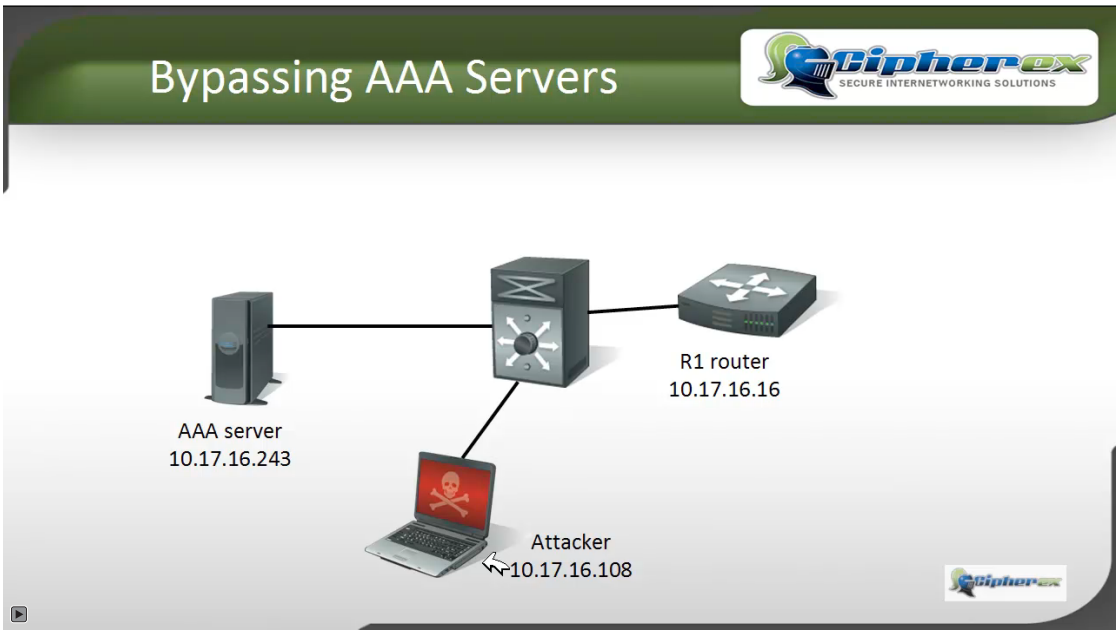
None: If TACACS+ is unavailable, allows administrator access to exec shell without authorization.

*As an option, the key word **local** can replace **none***

	to facilitate local authorization. *A local authorization command will need to be added.*
aaa accounting send stop-record authentication failure	Sends an accounting notification to the TACACS+ server whenever the switch experiences an administrative failed log-in attempt.
aaa accounting exec default start-stop group tacacs+	Sends an accounting notification to the TACACS+ server at the start of an exec shell and a second notification upon its termination.
aaa accounting commands 0 default stop-only group tacacs+	Sends an accounting notification to the TACACS+ server at the end of execution of a level 0 command.
aaa accounting commands 1 default stop-only group tacacs+	Sends an accounting notification to the TACACS+ server at the end of execution of a level 1 command. Sends this notification only when the command has completed executing.
aaa accounting commands 15 default stop-only group tacacs+	Sends an accounting notification to the TACACS+ server at the end of execution of a level 15 command. Sends this notification only when the command has completed executing.
aaa accounting connection default start-stop group tacacs+	Sends an accounting notification to the TACACS+ server at the start of an outbound connection and a second notification upon its termination.
aaa accounting system default stop-only group tacacs+	Sends an accounting notification to the TACACS+ server for system-level events, such as reboots or interface bounces.
aaa session-id common	This command specifies whether the same-session ID will be used for each AAA accounting service type within a call. **Common:** Ensures that all identification information sent out for a given call will be identical. This is the default behavior.
tacacs-server host 192.168.253.25 **tacacs-server host 192.168.20.21**	Defines TACACS+ servers that are used for authentication, authorization, and accounting.
tacacs-server key Some_secure_TACACS_Key	This command creates a shared key used between the switch and the TACACS+ server for authenticating communications between these devices.

	Key Some_secure_TACACS_Key: Defines the key used to authenticate communication to the TACACS+ server.
aaa authentication dot1x default group radius none	Authenticates users connected to a switch-user port. Upon successful authentication, a user will have access to network resources; if authentication fails, the user will have no access, or only limited access if a guest VLAN is configured. **Dot1x:** Authenticates with 802.1x protocol to gain access to networked resources. **Default:** Defines the default method used to authenticate user access to networked resources. **Group radius:** Uses the list of all RADIUS (Remote Authentication Dial-In User Service) servers for authentication. **None**: If RADIUS is unavailable, allows network access without authentication. If this key word is not included and access to the RADIUS server is cut off, users will be unable to use network resources.
Aaa accounting dot1x default start-stop group radius	Sends an accounting notification to the RADIUS server at the start of an 802.1x authentication shell and a second notification upon its termination.
Radius-server host 192.168.253.25 auth-port 1812 acct-port 1813 **radius-server host 192.168.20.21 auth-port 1812 acct-port 1813**	The **radius-server host** command defines the RADIUS servers that authenticate users connecting to the switch. In this configuration, ports 1812 and 1813 have been defined for use in communication with the RADIUS server.
Radius-server key Some_secure_RADIUS_Key	This command creates a shared key used between the switch and the RADIUS server for authenticating communication. **Key Some_Secure_RADIUS_Key**: Defines the key used to authenticate communication to the RADIUS
ip radius source-interface Loopback0	Specifies Loopback0 as the source interface for all outgoing RADIUS packets.
Ip tacacs source-interface Loopback0	Specifies Loopback0 as the source interface for all outgoing TACACS+ packets.

Video: Click on the image below to play the Video



Command	Description
no ip source-route	Disables source routing on the switch. IP source routing allows the sender of an IP packet to control the route it will take to reach a destination. *Note: Enable source routing only if the network has a need for it.*
Security passwords min-length 8	Sets the minimum password length to be eight characters.
Enable secret *Some_Secure_Password*	Facilitates level 15 (switch#) log-in. **Some_Secure_Password:** Use this password to access the switch-enable mode.
Username admin1 secret Some_Secret_Password	Creates a local user account for administrative log-in access. **Username *admin1:*** Defines admin1 as a local user account. **Some_Secret_Password:** Use this password to authenticate the user named admin1.
Ip tcp synwait-time 10	Defines the amount of time Cisco Internet Operating System (IOS) software will wait to complete a TCP connection. The default is 30 seconds. This waiting time does not pertain to connections going through the device, but only to TCP connections originating from it.
no boot system	Will not allow the switch to load its operating system image from the network.
No ip domain-lookup	Disables IP Domain Name System lookup of host name to IP address translations. If outbound connections from this device, such as Telnet or SSH, are made to other devices using host names, enable this service.

Key chain secure-1	Key chains are used to authenticate HSRP (Hot Standby Routing Protocol) communications. This command creates a key chain named secure-1.
Key 1	This command identifies the first authentication key on a key chain.
Key-string secure-123	This command defines key string secure-123 for HSRP authentication.
No ip bootp server	BOOTP (Bootstrap Protocol) allows network devices to download their configuration data and software from a BOOTP server. This service can be used to bring up switches that have no configuration (over a Wide Area Network [WAN] or Local Area Network [LAN] connection).
File verify auto	The file-verify auto command enables image verification globally; that is, all images to be copied (via the copy command) or reloaded (via the reload command) are automatically verified.
Route-map Guest-Access-Policy permit 10 **match ip address Guest-Access** **set ip next-hop 192.168.50.1**	This route map is used to policy route guest-user access to the next hop router. In this example, users with the IP address defined in the Guest-Access ACL (Access Control List) will be policy routed to the switch with the IP address of 192.168.50.1

Command	Description
ip dhcp snooping	The DHCP-snooping process acts like a firewall between DHCP servers and hosts attached to the switch. While forwarding DHCP requests from access ports to the DHCP server, the process builds and maintains a DHCP-snooping binding table. DHCP traffic that does not conform to the information stored in the DHCP binding table is dropped.
Ip dhcp snooping vlan 10-1000	Enables DHCP snooping for VLANs 10 through 1000.
Ip arp inspection vlan 100-101,192,200	Dynamic ARP inspection is a security feature that validates ARP packets in a network. Based on information stored in the DHCP-snooping table, this process intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. For Dynamic ARP to function, DHCP snooping must be enabled. In this example, the command performs ARP inspections on VLANs 100, 101, 192, and 200. TIP *Devices configured with static IP addressing will need to be entered manually by the* **ip source binding** *command shown below.*
Crypto key generate rsa	Generates RSA key pairs for the switch—public and private. This command is not saved in the switch configuration; however, the keys it generates are saved in the private configuration in nonvolatile RAM, which is never displayed to the system administrators and will not be copied to another device. TIP *Before this command can be issued, the switch must have a host name and an IP domain name configured. It is not possible to complete the* ***Crypto key generate rsa*** *command*

	without them.
Ip ssh time-out 60	Sets the time interval for the router to wait for the SSH client to respond during SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the VTY line apply. This command sets the SSH time-out to 60 seconds.
Ip ssh authentication-retries 2	This command sets the number of attempts, after which the interface is reset. There is a maximum of five (5) authentication retries with a default of three (3).
Dot1x system-auth-control	Enabling 802.1X authentication for the entire system is required before individual ports can be configured. This command performs that task.
vtp domain CorpAccess	When a new VLAN is created on a switch, the VLAN Trunk Protocol (VTP) is used to distribute the VLAN through all switches in the domain. This reduces the need to configure the same VLAN everywhere. The **vtp domain CorpAccess** command configures this switch as part of the CorpAccess domain.  *To have the newly created VLAN(s) distributed in a VTP domain, the switch that the VLAN is configured on must be in VTP server mode.*
vtp mode client	Configures the switch as a VTP client and allows it to learn VLAN information from VTP servers in that domain.  *Depending on implementation, the switch may be configured in "transparent" mode, in which it will not learn VLAN information from VTP servers.*
vtp password SomeSecurePassword	Creates an MD5 hash that is sent with VTP summary advertisements for authentication.
errdisable recovery cause bpduguard	When spanning-tree protocol BPDU guard disables a port, the port remains in the disabled state unless it is enabled manually.

	This command allows the switch to reenable the port after a predefined time.
errdisable recovery interval 500	Defines the timeout period (500 seconds) for ports that have been error disabled because of BPDU guard violations. The default recovery interval is 300 seconds.
spanning-tree mode pvst	A Per-VLAN Spanning Tree (PVST) maintains a spanning-tree instance for each VLAN configured in the network. This command enables PVST on the switch.
spanning-tree portfast bpduguard default	When enabled on a port, the BPDU Guard feature shuts down the port that receives a BPDU message. This configuration option is operational only on ports in the Port-Fast state.
spanning-tree extend system-id	Cisco switches support 4096 VLANs in accordance with IEEE standard 802.1Q. To use all 4096 VLANs, use the extended-system ID command. Extended-system IDs are the VLAN IDs from 1025 to 4096.
vlan internal allocation policy ascend	The internal VLAN allocation feature allows assigning both "internal" and "user-defined" VLANs. Traditionally, internal VLANs (those assigned by the system) have been allocated for WAN interfaces, routed interfaces, and certain other features starting from VLAN 1006 (by default). When allocated, these VLANs are not available for user-defined VLAN assignments. This feature allows internal VLAN allocation beginning with VLAN ID 4096, rather than ascending from VLAN ID 1006.  *Modify the internal allocation policy to "descending" when planning to use VLAN assignments above 1006.*
spanning-tree vlan 100-101, 300 root primary	Configures the switch as the primary root bridge for the specified VLANs, and those specified in this command will be configured with a priority of 8192. Those not configured as root will have the default priority of 32768. VLANs configured with lower priority bridge values are chosen as root bridges.  *The actual command put into the configurations is **spanning-tree vlan 100-101, 300 priority 8192**.*

spanning-tree vlan 192, 200 root secondary

Configures the switch as a secondary root bridge for the specified VLANs. Those specified will be assigned the priority of 28672, and this switch will become their secondary root bridge. VLANs not configured as a primary or secondary bridge will default to 32768. Those configured with lower priority bridge values will be chosen as root bridges.

The actual command put into the configurations is ***spanning-tree vlan 100-101, 300 priority 28672.***

Command

interface Loopback0

ip address 10.1.1.1 255.255.255.255

Description

Switches have multiple interfaces; therefore it's a good idea to use a logical interface, which is always available to represent the switch for identification. This interface will be used to access the switch; to source logs to the syslog server; to send Simple Network Management Protocol (SNMP) traps to network management servers; to perform Network Time Protocol (NTP) synchronization with NTP servers; and to identify this device to TACACS+/RADIUS authentication servers.

Command	Description
interface FastEthernet0/1 **description secure user port**	Configures an interface for user access with no IP phone access required.
switchport access vlan 100	Designates this port to send and receive traffic on VLAN 100.
switchport mode access	Configures this interface as an access port to be a nontrunking port.
switchport nonegotiate	Specifies that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on layer 2 interfaces, and the switch will not participate in DTP negotiations on this interface.
switchport port-security maximum 1	Defines the number of MAC addresses to a maximum of one (1) that can send and receive data on this port.
switchport port-security	Enables port security on this interface, which is used to limit the number of MAC addresses that can send and receive frames.
switchport port-security aging time 5	Sets the aging time to five (5) minutes for the MAC address learned on this port. When a learned MAC address is aged out, a new device can connect and use the port.
switchport port-security violation restrict	Connecting more devices to this port than allowed will cause the switch to restrict them from accessing the network.
dot1x port-control auto	Enables 802.1X port-based authentication and causes the port

	to begin in the unauthorized state, allowing only Extensible Authentication Protocol Over LAN (EAPOL) frames to be sent and received through the port until the device to the port is authenticated and authorized to access the network.
dot1x guest-vlan 192	This command configures the port to support guest VLANS. When a user device fails 802.1x authentication, the port is put into a guest VLAN, which is configured for limited network access.
storm-control broadcast level 30.00	Limits broadcast traffic on the interface to 30% of the port bandwidth.
storm-control multicast level 30.00	Limits multicast traffic on the interface to 30% of the port bandwidth.
no cdp enable	Disables Cisco Discovery Protocol (CDP) on the switch port. This will stop the port from advertising CDP information to users. User devices have no need to receive CDP messages from the switch.
spanning-tree portfast	Port Fast immediately brings an interface to a forwarding state from a blocking state, bypassing the listening and learning states. This command allows devices connected to the port to immediately connect to the network for communication, rather than having to wait for the spanning-tree protocol to converge.
spanning-tree bpduguard enable	This command causes the spanning tree to shut down the port when BPDU traffic is received on it.
ip verify source port-security	Enables IP Source Guard with source IP and MAC address filtering. If the source IP and MAC address of a packet match a valid entry in IP source binding, the switch forwards the packet; otherwise it will drop all other types of packets except DHCP packets.  *This command uses the DHCP-snooping binding database and manually configured IP source bindings. Therefore DHCP snooping must be enabled on the switch.* *When IP Source Guard is enabled on an interface on which IP*

source bindings are not configured, the switch creates and applies a port ACL that denies all IP traffic on the interface. If IP Source Guard is disabled, the switch removes the port ACL from the interface.

See related commands.

no ip domain-lookup

ip dhcp snooping vlan 10-1000

ip arp inspection vlan 100-101,192,200

As an option, port ACLs may be configured for added security.

Command	Description
interface FastEthernet0/2 **description Secure User port with IP Phone**	Interfaces configuration for secure user port with IP phones.
switchport access vlan 100	Designates this port to send and receive traffic on VLAN 100.
switchport mode access	Configures this interface as an access port to be a nontrunking port.
switchport nonegotiate	Specifies that DTP negotiation packets are not sent on layer 2 interfaces and that the switch will not participate in DTP negotiations on this interface.
switchport voice vlan 101	Instructs the Cisco IP Phone to forward all voice traffic through VLAN 101.
switchport port-security maximum 2	Defines the number of MAC addresses to a maximum of two (2) that can send and receive data on this port.
switchport port-security	Enables port security on this interface, which is used to limit the number of MAC addresses that can send and receive frames.
switchport port-security aging time 5	Sets the aging time to five (5) minutes for the MAC address learned on this port. When a learned MAC address is aged

	out, a new device can connect and use the port.
switchport port-security violation restrict	Connecting more devices to this port than allowed will cause the switch to restrict them from accessing the network.
dot1x port-control auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port until the device is authenticated and authorized to access the network.
dot1x guest-vlan 192	This command configures the port to support guest VLANS. When a user/device fails 802.1x authentication, the port is put into a guest VLAN, which is configured for limited network access.
storm-control broadcast level 30.00	Limits broadcast traffic on the interface to 30% of the port bandwidth.
storm-control multicast level 30.00	Limits multicast traffic on the interface to 30% of the port bandwidth.
spanning-tree portfast	Port Fast immediately brings an interface to a forwarding state from a blocking state, bypassing the listening and learning states. This command allows devices connected to the port to immediately connect to the network for communication, rather than having to wait for the spanning-tree protocol to converge.
spanning-tree bpduguard enable	This command causes the spanning tree to shut down the port when BPDU traffic is received on it.
ip verify source port-security	Enables IP Source Guard with source IP and MAC address filtering. If the source IP and MAC address of a packet match a valid entry in IP source binding, the switch will forward the packet; otherwise it will drop all other types of packets except DHCP packets.  *This command uses the DHCP-snooping binding database and manually configured IP source bindings. Therefore DHCP snooping must be enabled on the switch.*

When IP Source Guard is enabled on an interface on which IP source bindings are not configured, the switch creates and applies a port ACL that denies all IP traffic on the interface. If IP Source Guard is disabled, the switch removes the port ACL from the interface.

See related commands.

No ip domain-lookup

ip dhcp snooping vlan 10-1000

ip arp inspection vlan 100-101,192,200

As an option, port ACLs may be configured for added security.

Command	Description
interface FastEthernet0/3 **description device with no_801.x support**	This command applies to interface configuration for ports that don't support 802.1x authentication and are not assigned IP addressing by DHCP, such as printers, access points, and statically configured user workstations.
switchport access vlan 200	Designates this port to send and receive traffic on VLAN 200.
switchport mode access	Configures this interface as an access port to be a nontrunking port.
switchport nonegotiate	Specifies that DTP negotiation packets are not sent on layer 2 interfaces and that the switch will not participate in DTP negotiations on this interface.
switchport port-security maximum 1	Defines the number of MAC addresses to a maximum of one (1) that can send and receive data on this port.
switchport port-security	Enables port security on this interface, which is used to limit the number of MAC addresses that can send and receive frames.
switchport port-security violation restrict	Connecting more devices to this port than allowed will cause the switch to restrict them from accessing the network.
switchport port-security mac-address sticky	Enables sticky learning of MAC addresses. Sticky learning happens when a device is connected to a port, and the MAC address is learned when the device sends traffic and is then applied to the interface as a statically configured MAC address.
switchport port-security mac-	This command statically binds a MAC address to the switch

address sticky 00b0.6456.50e0	port.  *This command was added automatically to the configuration with the use of the "**switchport port-security mac-address sticky**" command above.*
storm-control broadcast level 30.00	Limits broadcast traffic on the interface to 30% of the port bandwidth.
storm-control multicast level 30.00	Limits multicast traffic on the interface to 30% of the port bandwidth.
no cdp enable	Disables Cisco Discovery Protocol (CDP) on the switch port. This will stop the port from advertising CDP information to users. User devices have no need to receive CDP messages from this switch.
spanning-tree portfast	Port Fast immediately brings an interface to a forwarding state from a blocking state, bypassing the listening and learning states. This command allows devices connected to the port to immediately connect to the network for communication, rather than having to wait for the spanning-tree protocol to converge.
spanning-tree bpduguard enable	This command causes the spanning tree to shut down the port when BPDU traffic is received on it.
ip verify source port-security	Enables IP Source Guard with source IP and MAC address filtering. If the source IP and MAC address of a packet match a valid entry in IP source binding, the switch forwards the packet; otherwise it drops all other types of packets except DHCP packets. *Note: This command uses the DHCP-snooping binding database and manually configured IP source bindings. Therefore DHCP snooping must be enabled on the switch.* *When IP Source Guard is enabled on an interface on which IP source bindings are not configured, the switch creates and applies a port ACL (Access Control List) that denies all IP traffic on the interface. If IP Source Guard is disabled, the switch removes the port ACL from the interface.*

See related commands.

No ip domain-lookup

ip dhcp snooping vlan 10-1000

ip arp inspection vlan 100-101,192,200

As an option , port ACLs may be configured for added security.

Command	Description
interface GigabitEthernet0/1 **description Connection to first Distribution Switch**	Configures a trusted trunk port that is connected to a distribution switch.
switchport trunk encapsulation dot1q	Configures the interface as a trunk port, with 802.1Q encapsulation.
switchport trunk native vlan 1000	Changes the native VLAN from 1 to 1000, guarding against VLAN-hopping attacks.
switchport mode trunk	Puts the interface into permanent trunking mode. TIP *The interface becomes a trunk interface even if the neighboring interface does not change its mode to a trunk port.*
switchport nonegotiate	Specifies that DTP negotiation packets are not sent on layer 2 interfaces and that the switch will not participate in DTP negotiations on this interface.
switchport trunk allowed vlan 100,101,192,200,300,1000	This command allows only specific VLAN traffic to traverse the trunk link. In this instance, only traffic on VLANs 100, 101, 192, 200, 300, and 1000 are allowed to traverse this link
ip arp inspection trust	Configures this trunk port to trust all ARP packets entering the network from the neighboring switch and thus bypasses the ARP security check.
Ip dhcp snooping trust	Trusts all DHCP packets entering the network from the neighboring switch and thus bypasses the DHCP-snooping security check.

: See related commands.

No ip domain-lookup

ip dhcp snooping vlan 10-1000

ip arp inspection vlan 100-101,192,200

Command	Description
interface Vlan100 **description Trusted User VLAN** **ip address 192.168.100.2 255.255.255.0**	Configures the trusted user VLAN and assigns an IP address to the interface.
Ip helper-address 10.17.20.243	Forwards DHCP request from user port to the DHCP server defined by the IP with the IP address of 10.17.20.243.
no ip redirects	This command instructs the switch not to send ICMP (Internet Control Message Protocol) redirects. These messages are used by switches to notify the hosts on the data link that a better route is available for a particular destination. Cisco switches send ICMP redirects when all of the following conditions are met: • The interface on which the packet enters the switch is the same interface on which it exits. • The subnet or network of the source IP address is on the same subnet or network of the next-hop IP address of the routed packet. • The datagram is not source routed. • The kernel is configured to send redirects. TIP *ICMP redirects are disabled by default if HSRP is configured on the interface. In Cisco IOS Software Release 12.1(3)T and later, ICMP redirects are allowed to be enabled on interfaces configured with HSRP.*
no ip mask-reply	Disables responses to IP mask queries. An attacker may use this service to map the network; therefore it is disabled.

no ip directed-broadcast	Disables responses to directed broadcast requests generated by remote hosts.  *The switch will still respond to directed broadcast requests from directly connected devices on this VLAN.*
no ip unreachables	Host Unreachable messages provide the requester with a subnet mask for a particular network. An attacker may use this service to map the network; therefore it is disabled.
no ip proxy-arp	Switches have the ability to proxy ARP messages from one domain to another. Unless a switch needs to provide intermediary ARP requests, the service should be disabled.
standby authentication md5 key-chain secure-1	This command uses a preshared key to authenticate HSRP messages. **md5:** Encrypts the key chain by utilizing the MD5 hashing algorithm. **key-chain secure-1**: Uses the key defined in the key-chain named secure-1 to authenticate standby communication.

interface Vlan101

description Voice VLAN

ip address 192.168.101.2 255.255.255.0

Configures Voice VLAN and assigns an IP address to the interface.

ip helper-address 10.17.20.243

Forwards incoming DHCP requests from user port to the DHCP server defined by the IP address of 10.17.20.243.

no ip redirects

This command instructs the switch not to send ICMP redirects. These messages are used by switches to notify hosts on the data link that a better route is available for a particular destination. Cisco switches send ICMP redirects when all of the following conditions are met:

- The interface on which the packet enters the switch is the same interface on which exits.
- The network or subnet of the source IP address is on the same network or subnet of the next-hop IP address of the routed packet.
- The datagram is not source routed.
- The kernel is configured to send redirects.

TIP *ICMP redirects are disabled by default if HSRP is configured on the interface. In Cisco IOS Software Release 12.1(3)T and later, ICMP redirects are allowed to be enabled on interfaces configured with HSRP.*

no ip mask-reply

Because an attacker may use this service to map the network, this command disables responses to IP mask queries."

no ip directed-broadcast

Disables responses to directed broadcast requests generated by remote hosts.

The switch will still respond to directed broadcast requests from directly connected devices on this VLAN.

no ip unreachables	Host Unreachable messages provide the subnet mask for a particular network to the requester. An attacker may use this service to map the network; therefore it is disabled.
no ip proxy-arp	Switches have the ability to proxy ARP messages from one domain to another. Unless a switch needs to provide intermediary ARP requests, this service should be disabled.
standby 2 authentication md5 key-chain secure-1	This command uses a preshared key to authenticate HSRP messages. **md5:** Encrypts the key chain by utilizing the MD5 hashing algorithm. **key-chain secure-1**: Uses the key defined in the key-chained name secure-1 to authenticate standby communication.
standby 2 ip 192.168.101.1	Creates HSRP standby group 2 and assigns the standby IP for this group.
standby 2 priority 200	Assigns a priority of 200 to this switch's standby group. The switch with the highest priority becomes the active switch. The default priority is 100.
standby 2 preempt	The **standby preempt** command enables the HSRP switch with the highest priority to immediately become the active switch.
standby 2 name VLAN-101-Voice	This command defines the name "**VLAN-101-Voice"** for this standby group.

As an option, VLAN Maps may be configured for added security.

Command	Description
interface vlan192 **description Guest VLAN** **ip address 192.168.192.2 255.255.255.0**	Configures the Untrusted Guest VLAN and **assigns** an IP address to the interface.
ip helper-address 10.17.20.243	Forwards incoming DHCP requests from the user port to the DHCP server defined by the IP address of 10.17.20.243.
ip policy route-map Guest-Access-Policy	This command uses the route map named Guest-Access-Policy to route all traffic from guest users to a defined next hop. *Note: See related commands.* ***route-map Guest-Access-Policy permit 10*** ***match ip address Guest-Access*** ***set ip next-hop 192.168.50.1***
no ip redirects	It instructs the switch not to send ICMP redirects. These messages are used by switches to notify the hosts on the data link that a better route is available for a particular destination. Cisco switches send ICMP redirects when all of the following conditions are met: • The interface on which the packet enters the switch is the same interface on which exits. • The subnet or network of the source IP address is on the same subnet or network of the next-hop IP address of the routed packet. • The datagram is not source routed. • The kernel is configured to send redirects.

	 *ICMP redirects are disabled by default if HSRP is configured on the interface. In Cisco IOS Software Release 12.1(3)T and later, ICMP redirects may be enabled on interfaces configured with HSRP.*
no ip mask-reply	Disables responses to IP mask queries. An attacker may use this service to map the network; therefore it is disabled.
no ip directed-broadcast	Disables responses to directed broadcast requests generated by remote hosts. *Note: The switch will still respond to directed broadcast requests from directly connected devices on this VLAN.*
no ip unreachables	Host Unreachable messages provide the subnet mask for a particular network to the requester. An attacker may use this service to map the network; therefore it is disabled.
no ip proxy-arp	Switches have the ability to proxy ARP messages from one domain to another. Unless a switch needs to provide intermediary ARP requests, the service should be disabled.
standby 3 authentication md5 key-chain secure-1	This command uses a preshared key to authenticate HSRP messages. **md5:** Encrypts the key chain by utilizing the MD5 hashing algorithm. **key-chain secure-1**: Uses the key defined in the key-chained name secure-1 to authenticate standby communication.
standby 3 ip 192.168.192.1	Creates HSRP standby group 3 and assigns the standby IP for this group.
standby 3 priority 150	This command assigns a priority of 150 to this switch's standby group. The switch with the highest priority becomes the active switch. The default priority is 100.
standby 3 preempt	The **standby preempt** command enables the HSRP switch with the highest priority to immediately become the active switch.

standby 3 name VLAN-192-Guest	This command defines the name "**VLAN-192-Untrusted-Guest-User"** for this standby group.  *As an option, VLAN Maps may be configured for added security.*

Command	Description
interface vlan200 **description Wireless VLAN** **ip address 192.168.200.2 255.255.255.0**	Configures the Wireless VLAN and assigns an IP address to the interface.
ip helper-address 10.17.20.243	Forwards incoming DHCP request from user port to the DHCP server defined by the IP address of 10.17.20.243.
no ip redirects	This command instructs the switch not to send ICMP redirects. These messages are used by switches to notify the hosts on the data link that a better route is available for a particular destination. Cisco switches send ICMP redirects when all of the following conditions are met: • The interface on which the packet comes into the switch is the same interface on which it is sent out. • The subnet or network of the source IP address is on the same subnet or network of the next-hop IP address of the routed packet. • The datagram is not source routed. • The kernel is configured to send redirects. TIP *ICMP redirects are disabled by default if HSRP is configured on the interface. In Cisco IOS Software Release 12.1(3)T and later, ICMP redirects may be enabled on interfaces configured with HSRP.*
no ip mask-reply	Disables responses to IP mask queries. Attacker may use this service to map the network; therefore it is disabled.
no ip directed-broadcast	Disables responses to directed broadcast requests generated by

	remote hosts. *Note: The switch will still respond to directed broadcast requests from directly connected devices on this VLAN.*
no ip unreachables	Host Unreachable messages provide the subnet mask for a particular network to the requester. An attacker may use this service to map the network; therefore it is disabled.
no ip proxy-arp	Switches have the ability to proxy ARP messages from one domain to another. Unless a switch needs to provide intermediary ARP requests; the service should be disabled.
standby 4 authentication md5 key-chain secure-1	This command uses a preshared key to authenticate HSRP messages. **md5:** Encrypts the key-chain by utilizing the MD5 hashing algorithm. **key-chain secure-1**: Uses the key defined in the key-chained name secure-1 to authenticate standby communication.
standby 4 ip 192.168.200.1	Creates HSRP standby group 4 and assigns the standby IP for this group.
standby 4 priority 150	This command assigns a priority of 150 to this switch's standby group. The switch with the highest priority becomes the active switch. The default priority is 100.
standby 4 preempt	The **standby preempt** command enables the HSRP switch with the highest priority to immediately become the active switch.
standby 4 name VLAN-200-Wireless	This command defines the name "**VLAN-200-Wireless"** for this standby group.  *As an option, VLAN Maps may be configured for added security.*

Command	Description
interface Vlan300 **description Management VLAN** **ip address 192.168.3.2 255.255.255.0**	Configures the Management VLAN used for managing the switch. Assigns an IP address to the interface.
no ip redirects	This command instructs the switch not to send ICMP redirects. These messages are used by switches to notify the hosts on the data link that a better route is available for a particular destination. Cisco switches send ICMP redirects when all of the following conditions are met: • The interface on which the packet comes into the switch is the same interface on which it is sent out. • The network or subnet of the source IP address is on the same network or subnet of the next-hop IP address of the routed packet. • The datagram is not source routed. • The kernel is configured to send redirects. TIP *ICMP redirects are disabled by default if HSRP is configured on the interface. In Cisco IOS Software Release 12.1(3)T and later, ICMP redirects may be enabled on interfaces configured with HSRP.*
no ip mask-reply	Disables responses to IP mask queries. An attacker may use this service to map the network; therefore it is disabled.
no ip directed-broadcast	Disables responses to directed broadcast requests generated by remote hosts.

The switch will still respond to directed broadcast requests from directly connected devices on this VLAN.

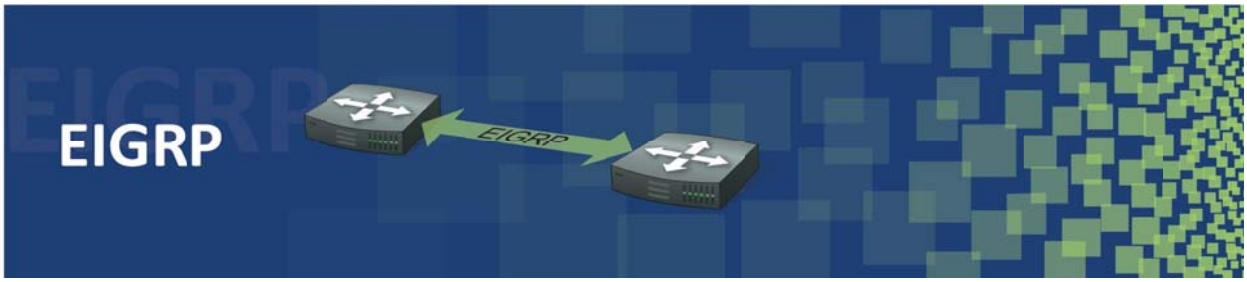
no ip unreachables	Host Unreachable messages provide the subnet mask for a particular network to the requester. An attacker may use this service to map the network; therefore it is disabled.
no ip proxy-arp	Switches have the ability to proxy -ARP messages from one domain to another. Unless a switch needs to provide intermediary ARP requests, the service should be disabled.
ip authentication mode eigrp 100 md5	Authenticates EIGRP routing updates with neighbors in the same autonomous system. In this example, routing updates for EIGRP 100 are authenticated using MD5 hashing.
ip authentication key-chain eigrp 100 secure-EIGRP	This command defines authentication as a key for EIGRP 100 routing updates. **key-chain**: Uses a key chain for authentication. **eigrp 100**: Defines EIGRP 100 routing updates to use the key chain. **secure-EIGRP**: Defines the name of the key chain secure-EIGRP to be used as the preshared key.
ip ospf authentication message-digest	Authenticates OSPF routing updates with neighbors in the same autonomous system. In this example, routing updates for OSPF 100 are authenticated using MD5 hashing.
ip ospf authentication-key SomeSecureOSPFKey	Uses the authentication key **SomeSecureOSPFKey** to authenticate OSPF messages that are received on this interface
ip rip authentication mode md5	Authenticates RIP (Routing Information Protocol) updates. In this example, they are authenticated using MD5 hashing.
ip rip authentication key-chain secure-RIP	**ip rip authentication Key-chain**: Uses a key chain for RIP authentication. **secure-RIP**: Defines the name of the key chain secure-RIP

to be used as the preshared key.

standby 5 authentication md5 key-chain secure-1	This command uses a preshared key to authenticate HSRP messages. **md5:** Encrypts the key chain by utilizing the MD5 hashing algorithm. **key-chain secure-1**: Uses the key defined in the key-chained name secure-1 to authenticate standby communication.
standby 5 ip 192.168.3.1	Creates HSRP standby group 5 and assigns the standby IP for this group.
standby 5 priority 200	This command assigns a priority of 200 to this switch's standby group. The switch with the highest priority becomes the active switch. The default priority is 100.
standby 5 preempt	The **standby preempt** command enables the HSRP switch with the highest priority to immediately become the active switch.
standby 5 name VLAN-300-Management	This command defines the name "**VLAN-300-Management"** for this standby group.

As an option, VLAN Maps may be configured for added security.

Command	Description
interface vlan1000 **description Native VLAN** **no ip address**	Configures the native VLAN to guard against VLAN hopping.

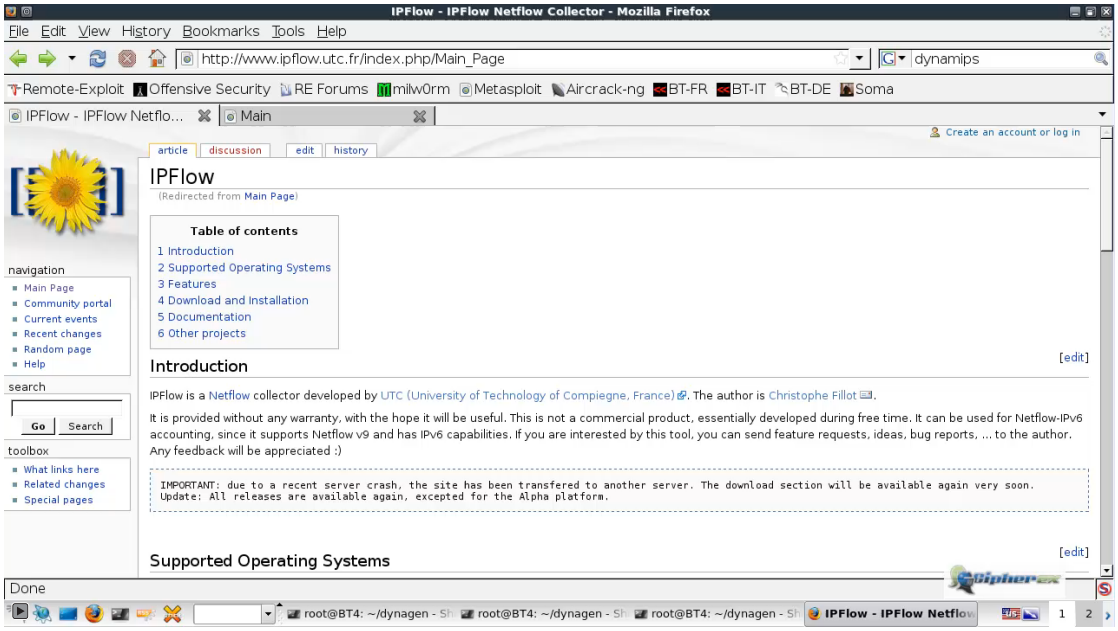


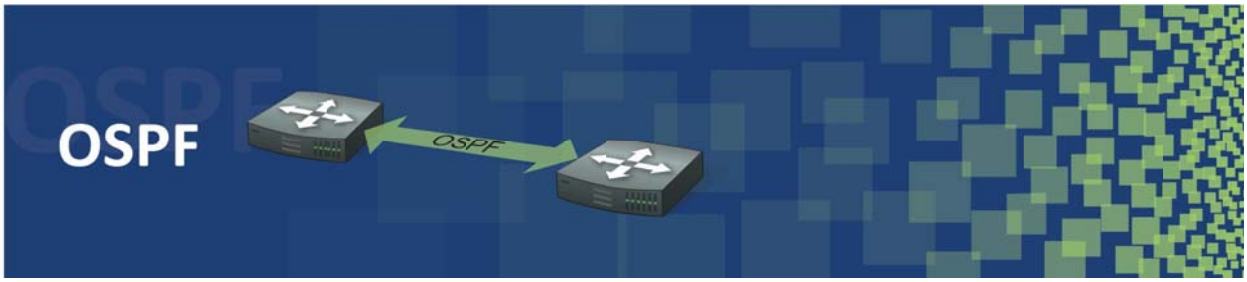
Command	Description
key chain secure-EIGRP	This key chain is used to authenticate EIGRP (Enhanced Interior Gateway Routing Protocol) communication. This command creates a key chain named **secure-EIGRP**.  *Cisco recommends using one key chain per routing protocol.*
key 1	This command identifies the first authentication key on a key chain.
key-string secure-123	This command defines the key string **secure-123** for EIGRP authentication.
router eigrp 100	Enables EIGRP with Autonomous System 100.
passive-interface default	Configures the switch not to send routing updates via any interface.
no passive-interface Vlan300	Configures the switch to send EIGRP routing updates only out of VLAN 300 interface.
network 192.168.3.0 **network 192.168.10.0** **network 192.168.100.0** **network 192.168.101.0** **network 192.168.192.0** **network 192.168.200.0**	The following networks will be advertised by the EIGRP routing process.
no auto-summary	Disables automatic summarization of subnet routes and allows

EIGRP to advertise subnets.

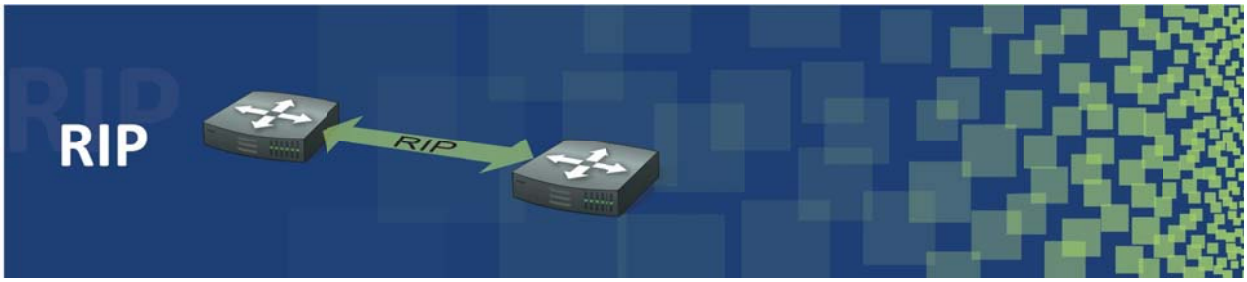
ip classless At times, the switch might receive packets destined for a network subnet that has no network default route defined. This command allows forwarding these packets to the best supernet route possible.

Video: Click on the image below to play the Video





Command	Description
router OSPF 100	Enables OSPF with Process-id of 100.
passive-interface default	Configures the switch not to send routing updates via any interface.
no passive-interface Vlan300	Configures the switch to send OSPF routing updates only out of VLAN 300 interface.
network 192.168.3.0 0.0.0.255 area 1	The following networks will be advertised by the OSPF routing process.
network 192.168.10.0 0.0.0.255 area 1	
network 192.168.100.0 0.0.0.255 area 1	
network 192.168.101.0 0.0.0.255 area 1	
network 192.168.192.0 0.0.0.255 area 1	
network 192.168.200.0 0.0.0.255 area 1	
no auto-summary	Disables automatic summarization of subnet routes and allows OSPF to advertise subnets.
ip classless	At times, the switch might receive packets destined for a network subnet that has no network default route defined. This command allows forwarding these packets to the best supernet route possible.



Command	Description
key chain secure-RIP	This key chain is used to authenticate RIP communication. This command creates a key chain named **secure-RIP**. *Note: Cisco recommends using one key chain per routing protocol.*
key 1	This command identifies the first authentication key on a key chain.
key-string secure-456	This command defines the key string **secure-456** for RIP authentication.
router rip	Enables RIP routing protocol.
version2	Sends and receives version 2 routing updates.
Passive interface default	Configures the switch not to send routing updates via any interface.
no passive interface vlan 300	Configures the switch to send RIP routing updates only out of VLAN 300 interface.
network 192.168.3.0 **network 192.168.10.0** **network 192.168.100.0** **network 192.168.101.0** **network 192.168.192.0** **network 192.168.200.0**	The following networks will be advertised by the RIP routing process.
no auto-summary	Disables automatic summarization of subnet routes and allows RIP to advertise subnets.

ip classless

At times, the switch might receive packets destined for a network subnet that has no network default route defined. This command allows forwarding these packets to the best supernet route possible.

Command	Description
snmp-server community SomeReadOnlyString RO 21	Defines the SNMP community string used to gather or read configuration values from the switch. **community SomeReadOnlyString:** Defines the SNMP community string used for authentication. **RO:** Defines the community string as the read-only community string. **21:** Restricts SNMP access to devices defined in access list 21.
snmp-server community SomeReadWriteString RW 21	Defines the SNMP community string used to read or write configuration values. **community SomeReadWriteString:** Defines the SNMP community string used for authentication. **RW:** Defines the community string as the read-write community string. **21:** Restricts SNMP access to devices defined in access list 21.
snmp-server trap-source Loopback0	Outbound SNMP traps will have the source IP address of the Loopback0 interface.
snmp-server location Some City, 123 some drive	Defines the physical location of this device.
snmp-server contact NOC @1-555-555-1212	This command defines contact information for the person or organization responsible for managing this device.
snmp-server chassis-id S/N: 123467901234	This command defines the chassis ID for this system. In this example we are configuring the serial number of the system as the chassis ID.
snmp-server enable traps snmp coldstart warmstart	Enables the switch to send SNMP cold-start and warm-start notifications.

coldstart: A cold-start (0) trap signifies that the sending device is reinitializing itself and may alter either the agent's configuration or the protocol entity implementation.

warmstart: A warm-start (1) trap signifies that the sending device is reinitializing itself and will alter neither the agent's configuration nor the protocol entity implementation.

snmp-server enable traps envmon

This command enables Environmental Monitor (EnvMon) status notifications for the system. Exceeding an environmental threshold triggers the EnvMon notifications.

The following notifications are sent:

Shutdown: Controls shutdown notifications. Sends a ciscoEnvMonShutdownNotification if the environmental monitor detects a test point reaching a critical state and is close to initiating a shutdown.

Voltage: Controls voltage notifications. Sends a ciscoEnvMonVoltageNotification if the voltage measured at a given test point is outside the normal range for the test point (i.e., at the warning, critical, or shutdown stage).

Temperature: Controls temperature notifications. Sends a ciscoEnvMonTemperatureNotification if the temperature measured at a given test point is outside the normal range.

Fan: Controls fan failure notifications. Sends a ciscoEnvMonFanNotification if any fan in a fan array fails.

Supply: Controls Redundant Power Supply (RPS) failure notifications. Sends a ciscoEnvMonRedundantSupplyNotification if a redundant power supply fails.

snmp-server host 192.168.10.5 SomeSNMPString

Defines the SNMP server.

host 192.168.10.5: Defines the SNMP server to which traps are sent.

SomeSNMPString: Defines the community string to use for sending traps.

access-list 21 remark SNMP servers

access-list 21 permit 192.168.10.1

access-list 21deny any

This access list limits devices that can communicate with this switch via SNMP.

As an option, SNMP views can be configured to further reduce access to the Management Information Base.

See SNMP V3 configuration example below.

Command	Description
banner exec	Banners provide legal protection, but not technical protection. The banner below displays after user authentication to exec level 1. It provides information about the company and states that authorization is required to access the system. It also provides the host name of the device and the line used to access it. banner exec @ This system is the property of CipherEx. UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED. Users must have explicit permission to access this device. All activities performed on this device are logged. Any violation of access policy will result in disciplinary action. ********** Host name: $(hostname) Line number: $(line) ********** @

Command	Description
banner motd	This banner is displayed before a log-in. It warns that only authorized users may use this system; however, it provides no information about the organization that owns the device. *Note: SSH connections do not display this banner, but console and Telnet connections do.* banner motd @ UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED. Users must have explicit permission to access this device. All activities performed on this device are logged. Any violation of access policy will result in disciplinary action. @

Command	Description
line con 0 **exec-timeout 5 0**	This command times out the exec shell on line Con0 if it is inactive for 5 minutes.
transport output none	This command disables any outbound connections on the console port.

Command	Description
line aux 0 **no exec**	No exec shell is permitted on Aux 0.
transport input none	This command disables any inbound connections on the aux port.
transport output none	This command disables any outbound connections on the aux port.
exec−timeout 0 1	This command sets exec shell timeout to one second.

Command	Description
access-list 101 remark list of host\networks that have SSH access to this switch **access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 0.0.0.0 eq 22 log-input** **access-list 101deny ip any any log-input**	This access list defines hosts or network segments that have SSH access to this switch. The **log-input** parameter logs access to the switch.
line vty 0 15 **access-class 101 in**	This access list limits remote access to the switch on VTY lines 0 to 15.
exec-timeout 5 0	This command times out the exec shell if it is inactive for 5 minutes.
transport input ssh	Allows incoming SSH connections.
transport output none	This command disables any outbound connections on the VTY lines.
Login tacacs	Uses the TACACS server to authenticate incoming VTY connections.

Command	Description
clock timezone PST -8	Reports the time in the local time zone. In this example, PST is the abbreviation for Pacific standard time, and -8 is the offset from UTC/GMT local time. TIP *Network time protocol (NTP) uses Coordinated Universal Time (UTC), the international standard of time (which is equivalent to GMT), for all time synchronizations; therefore it is not affected by different time zones configured on the switch.*
clock summer-time PDST recurring	This command configures the switch for daylight saving time adjustment. **PDST:** is the abbreviation for Pacific daylight saving time. **Recurring:** This automatically adjusts the clock when daylight-saving-defined dates are reached. *Note: Cisco switches are configured to change the clock based on U.S. daylight saving time standards.*
ntp authentication-key 10 md5 Some_NTP_Password	This command authenticates network time communication to NTP servers. Key numbers are used to select different authentication keys with different NTP devices. **authentication-key 10** : Defines authentication key number 10. **md5** : Uses the md5 algorithm to authenticate NTP sessions for authentication key number 10. **Some_NTP_Password** : Uses this key string for

authentication.

ntp authentication-key 11 md5 Some_NTP_Password

This command authenticates network time communication to internal NTP peers. Key numbers are used to select different authentication keys with different NTP devices.

authentication-key 11: Defines authentication key number 11.

md5: Uses the md5 algorithm to authenticate NTP sessions for authentication key number 11.

Some_NTP_Password: Uses this key string for authentication.

ntp authenticate

Enables NTP authentication on system.

NTP authentication does not require clients to use authentication; it merely enables them to use it. The switch will still respond to nonauthenticated requests. To limit NTP access, use ACL to define hosts that are allowed NTP requests.

ntp trusted-key 10

Defines key 10 to be a valid key for authentication.

ntp trusted-key 11

Defines key 11 to be a valid key for authentication.

ntp source Loopback0

Defines the Loopback0 interface as the IP address to be used in NTP communication.

ntp access-group peer 11

Defines which devices can participate with this switch in NTP peer communication.

peer 11: Defines access list 11 as a list of peers allowed for NTP communication with this system.

ntp access-group serve-only 10

Defines which servers can communicate with this switch as NTP servers.

serve-only 10: Defines access list 10 as a list of NTP servers allowed to communicate with this system.

ntp peer 10.3.1.1 key 11

ntp peer 10.4.1.1 key 11

Defines NTP peer devices.

peer {IP address}: Defines IP address of the peer.

key 11: Defines trusted key 11 to use with this peer.

ntp server 172.16.15.1 key 10

ntp server 172.16.17.1 key 10

ntp server 172.16.31.1 key 10

Defines NTP servers.

server {ip address}: Defines IP address of the server.

key 10: Defines trusted key 10 to use with this NTP server.

access-list 11 remark peer NTP servers

access-list 11 permit 10.3.1.1

access-list 11 permit 10.4.1.1

access-list 11deny any

This access list limits devices that can provide peer-level NTP time synchronization.

access-list 10 remark NTP servers

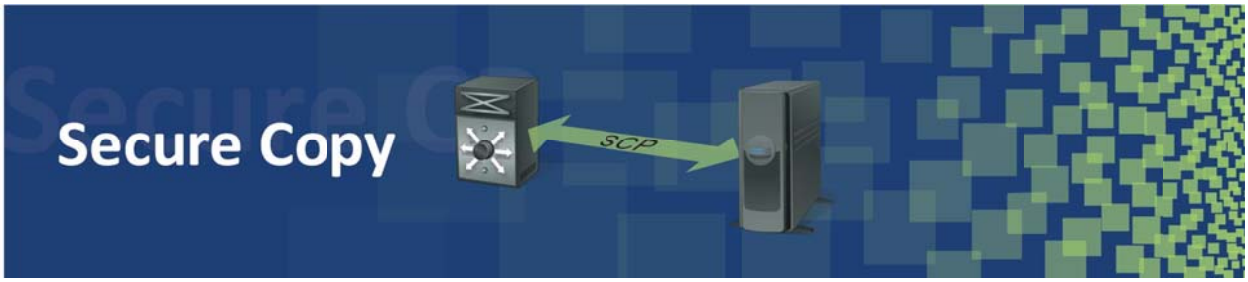
access-list 10 permit 63.17.112.7

access-list 10 permit 204.122.12.3

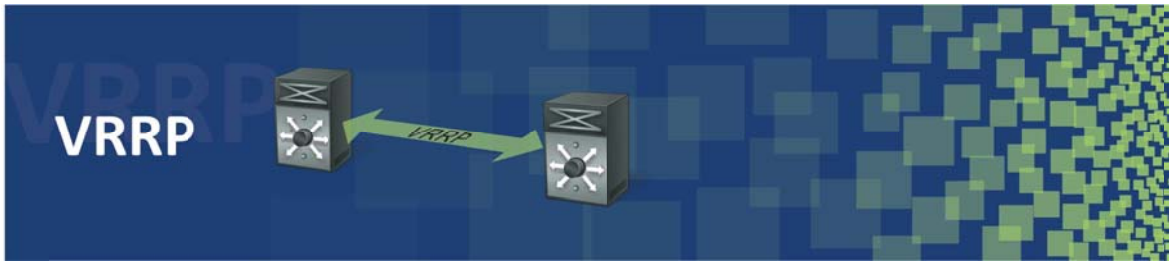
access-list 10 permit 194.192.12.204

access-list 10deny any

This access list limits devices that can provide server-level NTP time synchronization.



Command	Description
ip scp server enable	This command enables SCP (Secure Copy) server-side functionality. The SCP feature provides a secure and authenticated method for copying image or switch configuration files. For SCP to function on the switch, the following must be done: • Configure SSH, authentication, and authorization on the switch. • Enable AAA on the switch with the **aaa new-model** command. • Enable AAA authentication with the **aaa authentication login default group tacacs+** command. • Enable AAA authorization with the **aaa authorization exec default group tacacs+** command. The exec key word runs authorization to determine if the user has access to run an exec shell. • Because SCP relies on SSH for its secure transport, the switch must have an RSA (Rivest, Shamir, and Adelman) key pair. • The **crypto key generate rsa** command generates this key pair.



Command	Description
interface Vlan100 **description Trusted User VLAN** **ip address 192.168.100.2 255.255.255.0**	Configures the trusted user VLAN and assigns an IP address to the interface.
ip helper-address 10.17.20.243	Forwards DHCP request from user port to the DHCP server defined by the IP address of 10.17.20.243.
no ip redirects	This command instructs the switch not to send ICMP (Internet Control Message Protocol) redirects. These messages are used by switches to notify the hosts on the data link that a better route is available for a particular destination. Cisco switches send ICMP redirects when all of the following conditions are met: • The interface on which the packet comes into the switch is the same interface on which it is sent out. • The subnet or network of the source IP address is on the same subnet or network of the next-hop IP address of the routed packet. • The datagram is not source routed. • The kernel is configured to send redirects.  *ICMP redirects are disabled by default if HSRP is configured on the interface. In Cisco IOS Software Release 12.1(3)T and later, ICMP redirects are allowed to be enabled on interfaces configured with HSRP.*
vrrp 1 authentication md5 key-chain secure-1	This command authenticates VRRP (Virtual Router Redundancy Protocol) messages using a preshared key.

	md5: Encrypts the key chain by utilizing the MD5 hashing algorithm. **key-chain secure-1**: Uses the key defined in the key-chain name secure-1 to authenticate standby communication.
vrrp 1 ip 192.168.100.1	Creates VRRP standby group 1 and assigns the standby IP for this group.
vrrp 1 priority 200	Assigns a priority of 200 to this switch's VRRP group. The switch with the highest priority becomes the active switch. The default priority is 100.
VRRP1 preempt	The **VRRP preempt** command enables the switch with the highest priority to immediately become the active switch.
vrrp 1 descriptionVLAN-100-Trusted-User	Defines the name "**VLAN-100-Trusted-User"** for this standby group.

Command	Description
snmp-server group AdminGroup v3 priv	Creates an SNMP Version 3 group. **group AdminGroup:** defines the name of the group as AdminGroup. **priv:** requires authentication and authorization for access.
snmp-server user user1 AdminGroup v3 auth sha someSecurePassword priv d aes SomeEncryptionPasswrod access 21	Creates a user for SNMP access. **user user1 AdminGroup v3:** defines the name of the user as user1, who is a member of the SNMP version 3 group named AdminGroup. **auth sha SomeSecurePassword:** Uses the SHA (Secure Hash Algorithm) protocol with the key SomeSecurePassword to authenticate the user. **priv aes**: Sets the communication encryption to AES (Advanced Encryption Standard) with 256-bit encryption and uses the password SomeEncryptionPassword as the encryption key. **access 21**: Uses access list 21 to limit SNMP access.
snmp-server trap-source Loopback0	Outbound SNMP traps will have the source IP address of the Loopback0 interface.
snmp-server location Some City, 123 some drive	Defines the physical location of this device.
snmp-server contact NOC @1-555-555-1212	This command defines contact information for the person or organization responsible for managing this device.
snmp-server chassis-id S/N: 123467901234	This command defines the chassis ID for this system. In this example we are configuring the serial number of the system as the chassis ID.
snmp-server enable traps snmp	Enables the switch to send SNMP cold-start and warm-start

coldstart warmstart	notifications. **coldstart:** A cold-start (0) trap signifies that the sending device is reinitializing itself and may alter either the agent's configuration or the protocol entity implementation. **warmstart:** A warm-start (1) trap signifies that the sending device is reinitializing itself and will alter neither the agent's configuration nor the protocol entity implementation.
snmp-server enable traps envmon	This command enables Environmental Monitor (EnvMon) status notifications for the system. Exceeding an environmental threshold triggers the EnvMon notifications. The following notifications are sent: **Shutdown:** Controls shutdown notifications. Sends a ciscoEnvMonShutdownNotification if the environmental monitor detects a test point reaching a critical state and is close to initiating a shutdown. **Voltage:** Controls voltage notifications. Sends a ciscoEnvMonVoltageNotification if the voltage measured at a given test point is outside the normal range for the test point (i.e., at the warning, critical, or shutdown stage). **Temperature:** Controls temperature notifications. Sends a ciscoEnvMonTemperatureNotification if the temperature measured at a given test point is outside the normal range. **Fan:** Controls fan failure notifications. Sends a ciscoEnvMonFanNotification if any fan in a fan array fails. **Supply**: Controls Redundant Power Supply (RPS) failure notifications. Sends a ciscoEnvMonRedundantSupplyNotification if a redundant power supply fails.
snmp-server host 192.168.10.5 version 3 auth user1	Defines the SNMP server. **host 192.168.10.5 version 3:** Defines the SNMP version 3 server to which traps are sent. **user1: use user1's credentials to authenticate and encrypt the communication**
access-list 21 remark SNMP servers **access-list 21 permit 192.168.10.1**	This access list limits devices that can communicate with this switch via SNMP.

access-list 21deny any

References

Every work is the result of many different sources:

http://www.cisco.com/application/pdf/paws/13608/21.pdf

https://www.cisecurity.org/tools2/cisco/CIS_Cisco_IOS_Benchmark_v2.2.pdf

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf

Hacking Exposed Cisco Networks: Cisco Security Secrets & Solutions [Paperback] - Andrew Vladimirov (Author), Konstantin Gavrilenko (Author), Andrei Mikhailovsky (Author)

LAN Switch Security: What Hackers Know About Your Switches [Paperback] - Author Eric Vyncke, Christoher Paggen

Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd Edition)

Hardening Cisco Routers (O'Reilly Networking) by Thomas Akin (Paperback - Feb 2002)