

# Cisco Routers

## Table of Contents

1. [Monitor Cisco Security Advisories and Responses](#)
2. [Develop Network Security Policy](#)
3. [Implement Password Management Controls](#)
4. [Centralize Log Collection and Monitoring](#)
5. [Leverage Authentication, Authorization, and Accounting](#)
6. [Access Control with MAC](#)
7. [Access Control with PACLs](#)
8. [Access Control with VLAN Maps](#)
9. [Classification ACLs](#)
10. [Anti-Spoofing ACLs](#)
11. [Dynamic ARP Inspection](#)
12. [Port Security](#)
13. [IP Source Guard](#)
14. [Configure Unicast RPF](#)
15. [Disable IP Source Routing](#)
16. [IP Options Selective Drop](#)
17. [Securing First Hop Redundancy Protocols](#)
18. [Routing Process Resource Consumption](#)
19. [Route Filtering](#)
20. [Passive-Interface Commands](#)
21. [Routing Protocol Authentication and Verification with Message Digest 5](#)
22. [Disable or Limit IP Directed Broadcasts](#)
23. [Filtering BGP Prefixes with Autonomous System Path Access Lists](#)
24. [Filtering BGP Prefixes with Prefix Lists](#)
25. [Configuring Maximum Prefixes](#)
26. [BGP Peer Authentication with MD5](#)
27. [Secure Simple Network Management Protocol\(SNMP\)](#)
28. [TTL-based Security Protections](#)
29. [Hardware Rate Limiters](#)
30. [Control Plane Protection](#)
31. [Control Plane Policing](#)
32. [Configure Receive ACLs\(rACL\)](#)
33. [Configure trusted time source for network time protocol](#)
34. [No Proxy ARP](#)
35. [Limit ICMP Unreachables](#)
36. [No IP ICMP Redirects](#)
37. [Configuration Change Notification and Logging](#)
38. [Cisco IOS Software Resilient Configuration](#)
39. [Enable exclusive configuration change access mode](#)
40. [Do not include router information in warning banners](#)

41. [Control transport for vty and tty Lines](#)
42. [Use authentication to control vty and tty lines](#)
43. [Secure console port access](#)
44. [Encrypt management Sessions](#)
45. [Enable Control Plane Protection\(CPPr\)](#)
46. [Enable Management Plane Protection\(MPP\)](#)
47. [ACL Support for Filtering on TTL Value](#)
48. [ACL Support for Filtering IP Options](#)
49. [Filter IP Fragments](#)
50. [ICMP Packet Filtering](#)
51. [Configure Infrastructure ACLs\(iACL\)](#)
52. [Enhanced Crashinfo File Collection](#)
53. [Detect and Correct Redzone Corruption](#)
54. [Memory Leak Detector](#)
55. [Reserve Memory for Console Access](#)
56. [CPU Thresholding Notification](#)
57. [Memory Threshold Notifications](#)
58. [Loopback Management Interfaces](#)
59. [Keepalives for TCP Sessions](#)
60. [Set EXEC timeout interval](#)
61. [Disable Unused Services](#)
62. [Secure and archive configuration settings](#)
63. [Enable traffic monitoring using NetFlow](#)
64. [Use Secure Protocols](#)

## 1. Monitor Cisco Security Advisories and Responses

The Cisco Product Security Incident Response Team (PSIRT) creates and maintains publications, commonly referred to as PSIRT Advisories, for security-related issues in Cisco products. Subscribe to Cisco Security Advisory RSS feeds at [http://ewsroom.cisco.com/data/syndication/rss2/SecurityAdvisories\\_20.xml](http://ewsroom.cisco.com/data/syndication/rss2/SecurityAdvisories_20.xml)

### REFERENCE

[http://newsroom.cisco.com/data/syndication/rss2/SecurityAdvisories\\_20.xml](http://newsroom.cisco.com/data/syndication/rss2/SecurityAdvisories_20.xml)

### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA  
ISO: 10.10.4

---

## 2. Develop Network Security Policy

### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA, ISO 27001

---

### 3. Implement Password Management Controls

As a security best practice, passwords must be managed with a TACACS+ or RADIUS authentication server. However, note that a locally configured password for privileged access is still needed in the event of failure of the TACACS+ or RADIUS services. A device can also have other password information present within its configuration, such as an NTP key, SNMP community string, or Routing Protocol key.

The enable secret command is used in order to set the password that grants privileged administrative access to the Cisco IOS system. The enable secret command must be used, rather than the older enable password command. The enable password command uses a weak encryption algorithm.

If no enable secret is set and a password is configured for the console tty line, the console password can be used in order to receive privileged access, even from a remote virtual tty (vty) session. This action is almost certainly unwanted and is another reason to ensure configuration of an enable secret.

The service password-encryption global configuration command directs the Cisco IOS software to encrypt the passwords, Challenge Handshake Authentication Protocol (CHAP) secrets, and similar data that are saved in its configuration file. Such encryption is useful in order to prevent casual observers from reading passwords, such as when they look at the screen over the shoulder of an administrator. However, the algorithm used by the service password-encryption command is a simple Vigenère cipher. The algorithm is not designed to protect configuration files against serious analysis by even slightly sophisticated attackers and must not be used for this purpose. Any Cisco IOS configuration file that contains encrypted passwords must be treated with the same care that is used for a cleartext list of those same passwords.

While this weak encryption algorithm is not used by the enable secret command, it is used by the enable password global configuration command, as well as the password line configuration command. Passwords of this type must be eliminated and the enable secret command or the Enhanced Password Security feature needs to be used.

The enable secret command and the Enhanced Password Security feature use Message Digest 5 (MD5) for password hashing. This algorithm has had considerable public review and is not known to be reversible. However, the algorithm is subject to dictionary attacks. In a dictionary attack, an attacker tries every word in a dictionary or other list of candidate passwords in order to find a match. Therefore, configuration files must be securely stored and only shared with trusted individuals.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 4. Centralize Log Collection and Monitoring

In order to track existing, emerging, and historic events related to security incidents, a unified strategy is required for event logging and correlation. This unified approach must leverage logging from all network devices and use pre-packaged and customizable correlation capabilities.

#### MAINOPTIONS

Compliance: PCI-DSS

---

### 5. Leverage Authentication, Authorization, and Accounting

The Authentication, Authorization, and Accounting (AAA) framework is vital to securing network devices. The AAA framework provides authentication of management sessions and can also limit users to specific, administrator-defined commands and log all commands entered by all users. The Authentication, Authorization, and Accounting (AAA) framework is critical to securing interactive access to network devices.

The AAA framework provides a highly configurable environment that can be tailored depending on the needs of the network.

## REFERENCE

## MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 6. Access Control with MAC

MAC access control lists or extended lists can be applied on IP network with the use of this command in interface configuration mode:

```
Cat6K-IOS(config-if)#mac packet-classify
```

---

### 7. Access Control with PACLs

PACLs can only be applied to the inbound direction on Layer 2 physical interfaces of a switch. Similar to VLAN maps, PACLs provide access control on non-routed or Layer 2 traffic. The syntax for creating PACLs, which take precedence over VLAN maps and router ACLs, is the same as router ACLs. If an ACL is applied to a Layer 2 interface, then it is referred to as a PACL. Configuration involves creating an IPv4, IPv6, or MAC ACL and applying it to the Layer 2 interface.

---

### 8. Access Control with VLAN Maps

VACLs, or VLAN maps that apply to all packets that enter the VLAN, provide the capability to enforce access control on intra-VLAN traffic. This is not possible using ACLs on routed interfaces. For example, a VLAN map may be used in order to prevent hosts that are contained within the same VLAN from communicating with each other, thereby minimizing opportunities for local attackers or worms to exploit a host on the same network segment. In order to deny packets from using a VLAN map, you can create an access control list (ACL) that matches the traffic and, in the VLAN map, set the action to drop. Once a VLAN map is configured, all packets that enter the LAN are sequentially evaluated against the configured VLAN map. VLAN access maps support IPv4 and MAC access lists; however, they do not support logging or IPv6 ACLs.

---

### 9. Classification ACLs

Classification ACLs provide visibility into traffic that traverses an interface. Classification ACLs do not alter the security policy of a network and are typically constructed to classify individual protocols, source addresses, or destinations. For example, an ACE that permits all traffic could be separated into specific protocols or ports. This more granular classification of traffic into specific ACEs can help provide an understanding of the network traffic because each traffic category has its own hit counter. An administrator may also separate the implicit deny at the end of an ACL into granular ACEs to help identify the types of denied traffic.

An administrator can expedite an incident response by using classification ACLs with the show access-list and clear ip access-list counters EXEC commands.

---

### 10. Anti-Spoofing ACLs

Manually configured ACLs can provide static anti-spoofing protection against attacks that utilize known unused and untrusted address space. Commonly, these anti-spoofing ACLs are applied to ingress traffic at network boundaries as a component of a larger ACL. Anti-spoofing ACLs require regular monitoring as they

can frequently change. Spoofing can be minimized in traffic originating from the local network by applying outbound ACLs that limit the traffic to valid local addresses.

## REFERENCE

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_configuration\\_example09186a0080100548.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml)

## MAINOPTIONS

Compliance: PCI-DSS

---

### 11. Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) can be utilized to mitigate ARP poisoning attacks on local segments. An ARP poisoning attack is a method in which an attacker sends falsified ARP information to a local segment. This information is designed to corrupt the ARP cache of other devices. Often an attacker uses ARP poisoning in order to perform a man-in-the-middle attack.

---

### 12. Port Security

Port Security is used in order to mitigate MAC address spoofing at the access interface. Port Security can use dynamically learned (sticky) MAC addresses to ease in the initial configuration. Once port security has determined a MAC violation, it can utilize one of four violation modes. These modes are protect, restrict, shutdown, and shutdown VLAN. In instances when a port only provides access for a single workstation utilizing standard protocols, a maximum number of one may be sufficient. Protocols that leverage virtual MAC addresses such as HSRP do not function when the maximum number is set to one.

---

### 13. IP Source Guard

IP Source Guard is an effective means of spoofing prevention that can be used if you have control over Layer 2 interfaces. IP Source Guard uses information from DHCP snooping to dynamically configure a port access control list (PACL) on the Layer 2 interface, denying any traffic from IP addresses that are not associated in the IP source binding table.

---

### 14. Configure Unicast RPF

Unicast RPF enables a device to verify that the source address of a forwarded packet can be reached through the interface that received the packet. You must not rely on Unicast RPF as the only protection against spoofing. Spoofed packets could enter the network through a Unicast RPF-enabled interface if an appropriate return route to the source IP address exists. Unicast RPF relies on you to enable Cisco Express Forwarding on each device, and is configured on a per-interface basis.

Unicast RPF can be configured in one of two modes: loose or strict. In cases where there is asymmetric routing, loose mode is preferred because strict mode is known to drop packets in these situations. During configuration of the `ip verify interface configuration` command, the keyword `any` configures loose mode while the keyword `rx` configures strict mode.

---

### 15. Disable IP Source Routing

IP source routing leverages the Loose Source Route and Record Route options in tandem or the Strict Source Route along with the Record Route option to enable the source of the IP datagram to specify the network path a packet takes. This functionality can be used in attempts to route traffic around security

controls in the network.

If IP options have not been completely disabled via the IP Options Selective Drop feature, it is important that IP source routing is disabled. IP source routing, which is enabled by default in all Cisco IOS Software Releases, is disabled via the `no ip source-route` global configuration command.

---

## 16. IP Options Selective Drop

There are two security concerns presented by IP options. Traffic that contains IP options must be process-switched by Cisco IOS devices, which can lead to elevated CPU load. IP options also include the functionality to alter the path that traffic takes through the network, potentially allowing it to subvert security controls.

Due to these concerns, the global configuration command `ip options {drop | ignore}` has been added by Cisco. In the first form of this command, `ip options drop`, all IP packets containing IP options that are received by the Cisco IOS device are dropped. This prevents both the elevated CPU load and possible subversion of security controls that IP options can enable.

The second form of this command, `ip options ignore`, configures the Cisco IOS device to ignore IP options that are contained in received packets. While this does mitigate the threats related to IP options for the local device, it is possible that downstream devices could be affected by the presence of IP options. It is for this reason that the drop form of this command is highly recommended.

---

## 17. Securing First Hop Redundancy Protocols

First Hop Redundancy Protocols (FHRPs) provide resiliency and redundancy for devices that are acting as default gateways. This situation and these protocols are commonplace in environments where a pair of Layer 3 devices provides default gateway functionality for a network segment or set of VLANs that contain servers or workstations.

The Gateway Load-Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), and Virtual Router Redundancy Protocol (VRRP) are all FHRPs. By default, these protocols communicate using unauthenticated communications. This kind of communication can allow an attacker to pose as an FHRP-speaking device to assume the default gateway role on the network. This takeover would allow an attacker to perform a man-in-the-middle attack and intercept all user traffic that exits the network.

---

## 18. Routing Process Resource Consumption

Routing Protocol prefixes are stored by a router in memory, and resource consumption increases with additional prefixes that a router must hold. In order to prevent resource exhaustion, it is important to configure the routing protocol to limit resource consumption. This is possible with OSPF by utilizing the Link State Database Overload Protection feature.

## REFERENCE

[http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp\\_ospf\\_lk\\_state\\_db\\_ps6350\\_TSD\\_Products\\_Configuration\\_Guide.html](http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_ospf_lk_state_db_ps6350_TSD_Products_Configuration_Guide.html)

---

## 19. Route Filtering

In order to reduce the possibility of introducing false routing information in the network, route filtering must be used. Unlike the passive-interface router configuration command, routing occurs on interfaces once route filtering is enabled, but the information that is advertised or processed is limited.

For EIGRP and RIP, using the distribute-list command with the out keyword limits what information is advertised, while usage of the in keyword limits what updates are processed. The distribute-list command is available for OSPF, but it does not prevent a router from propagating filtered routes. Instead, the area filter-list command can be used.

### REFERENCE

[http://www.cisco.com/en/US/docs/ios/12\\_2/ip/configuration/guide/1cfindep.html](http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfindep.html)

---

## 20. Passive-Interface Commands

Information leaks, or the introduction of false information into an IGP, can be mitigated through use of the passive-interface command that assists in controlling the advertisement of routing information. You are advised not to advertise any information to networks that are outside your administrative control.

### REFERENCE

[http://www.cisco.com/en/US/docs/ios/12\\_0t/12\\_0t2/feature/guide/defint.html](http://www.cisco.com/en/US/docs/ios/12_0t/12_0t2/feature/guide/defint.html)

---

## 21. Routing Protocol Authentication and Verification with Message Digest 5

Failure to secure the exchange of routing information allows an attacker to introduce false routing information

into the network. By using password authentication with routing protocols between routers, you can aid the security of the network. However, because this authentication is sent as cleartext, it can be simple for an attacker to subvert this security control.

By adding MD5 hash capabilities to the authentication process, routing updates no longer contain cleartext passwords, and the entire contents of the routing update is more resistant to tampering. However, MD5 authentication is still susceptible to brute force and dictionary attacks if weak passwords are chosen. MD5 authentication is much more secure when compared to password authentication.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 22. Disable or Limit IP Directed Broadcasts

IP Directed Broadcasts make it possible to send an IP broadcast packet to a remote IP subnet. Once it reaches the remote network, the forwarding IP device sends the packet as a Layer 2 broadcast to all stations on the subnet. This directed broadcast functionality has been leveraged as an amplification and reflection aid in several attacks, including the smurf attack.

#### MAINOPTIONS

Compliance: PCI-DSS

---

### 23. Filtering BGP Prefixes with Autonomous System Path Access Lists

BGP autonomous system (AS) path access lists allows the user to filter received and advertised prefixes based on the AS-path attribute of a prefix. This can be used in conjunction with prefix lists to establish a robust set of filters.

This configuration example uses AS path access lists to restrict inbound prefixes to those originated by the remote AS and outbound prefixes to those originated by the local autonomous system.

#### MAINOPTIONS

Router Role: Border

---

### 24. Filtering BGP Prefixes with Prefix Lists

Prefix lists allow a network administrator to permit or deny specific prefixes that are sent or received via BGP. Prefix lists should be used where possible to ensure network traffic is sent over the intended paths. Prefix lists should be applied to each eBGP peer in both the inbound and outbound directions.

Configured prefix lists limit the prefixes that are sent or received to those specifically permitted by the routing policy of a network. If this is not feasible due to the large number of prefixes received, a prefix list should be configured to specifically block known bad prefixes. These known bad prefixes include unallocated IP address space and networks that are reserved for internal or testing purposes by RFC 3330. Outbound prefix lists should be configured to specifically permit only the prefixes that an organization intends to advertise.

#### MAINOPTIONS

Router Role: Border

---

## 25. Configuring Maximum Prefixes

BGP prefixes are stored by a router in memory. The more prefixes that a router must hold results in BGP consuming more memory. In some configurations, a subset of all Internet prefixes can be stored, such as in configurations that leverage only a default route or routes for a provider's customer networks.

In order to prevent memory exhaustion, it is important to configure the maximum number of prefixes that is accepted on a per-peer basis. It is recommended that a limit be configured for each BGP peer.

### REFERENCE

[http://www.cisco.com/en/US/tech/tk365/technologies\\_configuration\\_example09186a008010a28a.shtml](http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a008010a28a.shtml)

### MAINOPTIONS

Router Role: Border

---

## 26. BGP Peer Authentication with MD5

Peer authentication using MD5 creates an MD5 digest of each packet sent as part of a BGP session. Specifically, portions of the IP and TCP headers, TCP payload, and a secret key are used in order to generate the digest.

Peer authentication with MD5 is configured by using the password option to the neighbor BGP router configuration command.

### MAINOPTIONS

Router Role: Border

---

## 27. Secure Simple Network Management Protocol(SNMP)

---

## 28. TTL-based Security Protections

Known as both the Generalized TTL-based Security Mechanism (GTSM) and BGP TTL Security Hack (BTSH), a TTL-based security protection leverages the TTL value of IP packets to ensure that the BGP packets that are received are from a directly connected peer. This feature often requires coordination from peering routers; however, once enabled, it can completely defeat many TCP-based attacks against BGP. Each IP packet contains a 1-byte field known as the Time to Live (TTL). Each device that an IP packet traverses decrements this value by one. The starting value varies by operating system and typically ranges from 64 to 255. A packet is dropped when its TTL value reaches zero.

### REFERENCE

[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t7/feature/guide/gt\\_btsh.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_btsh.html)

### MAINOPTIONS

## 29. Hardware Rate Limiters

Hardware rate limiters are referred to as special-case rate limiters because they cover a specific predefined set of IPv4, IPv6, unicast, and multicast DoS scenarios. HWRLs can protect the Cisco IOS device from a variety of attacks that require packets to be processed by the CPU.

### REFERENCE

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dos.html>

### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

## 30. Control Plane Protection

Control Plane Protection (CPPr) can be used in order to restrict or police control plane traffic that is destined to the CPU of the Cisco IOS device. While similar to CoPP, CPPr has the ability to restrict traffic with finer granularity. CPPr divides the aggregate control plane into three separate control plane categories known as subinterfaces. Subinterfaces exist for Host, Transit, and CEF-Exception traffic categories. In addition, CPPr includes these control plane protection features:

Port-filtering feature—This feature provides for policing and dropping of packets that are sent to closed or non-listening TCP or UDP ports.

Queue-thresholding feature—This feature limits the number of packets for a specified protocol that are allowed in the control-plane IP input queue.

### REFERENCE

[http://www.cisco.com/en/US/docs/ios/12\\_4t/12\\_4t4/htcpp.html](http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htcpp.html)

---

## 31. Control Plane Policing

The Control Plane Policing (CoPP) feature can also be used in order to restrict IP packets that are destined to the infrastructure device. For example, enabling this feature only SSH traffic from trusted hosts is permitted to reach the Cisco IOS device CPU.

### REFERENCE

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod\\_white\\_paper0900aecd804fa16a.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html)

---

## 32. Configure Receive ACLs(rACL)

The rACL protects the device from harmful traffic before the traffic impacts the route processor. Receive ACLs are designed to only protect the device on which it is configured and transit traffic is not affected by an rACL. As a result, the destination IP address any that is used in the example ACL entries below only refers to

the physical or virtual IP addresses of the router. Receive ACLs are also considered a network security best practice and should be considered as a long-term addition to good network security.

#### MAINOPTIONS

Compliance: PCI-DSS, HIPAA

---

#### 33. Configure trusted time source for network time protocol

The Network Time Protocol (NTP) is not an especially dangerous service, but any unneeded service can represent an attack vector. If NTP is used, it is important to explicitly configure a trusted time source and to use proper authentication. Accurate and reliable time is required for syslog purposes, such as during forensic investigations of potential attacks, as well as for successful VPN connectivity when depending on certificates for Phase 1 authentication.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

#### 34. No Proxy ARP

Proxy ARP is the technique in which one device, usually a router, answers ARP requests that are intended for another device. By "faking" its identity, the router accepts responsibility for routing packets to the real destination. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.

There are several disadvantages to utilizing proxy ARP. Utilizing proxy ARP can result in an increase in the amount of ARP traffic on the network segment and resource exhaustion and man-in-the-middle attacks. Proxy ARP presents a resource exhaustion attack vector because each proxied ARP request consumes a small amount of memory. An attacker can be able to exhaust all available memory by sending a large number of ARP requests.

Man-in-the-middle attacks enable a host on the network to spoof the MAC address of the router, resulting in unsuspecting hosts sending traffic to the attacker. Proxy ARP can be disabled using the interface configuration command `no ip proxy-arp`.

#### MAINOPTIONS

Compliance: PCI-DSS

---

#### 35. Limit ICMP Unreachables

Filtering with an interface access list elicits the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages can increase CPU utilization on the device. In Cisco IOS software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command `no ip unreachable`. ICMP unreachable rate limiting can be changed from the default using the global configuration command `ip icmp rate-limit unreachable interval-in-ms`.

#### 36. No IP ICMP Redirects

An ICMP redirect message can be generated by a router when a packet is received and transmitted on the

same interface. In this situation, the router forwards the packet and sends an ICMP redirect message back to the sender of the original packet. This behavior allows the sender to bypass the router and forward future packets directly to the destination (or to a router closer to the destination). In a properly functioning IP network, a router sends redirects only to hosts on its own local subnets. In other words, ICMP redirects should never go beyond a Layer 3 boundary.

There are two types of ICMP redirect messages: redirect for a host address and redirect for an entire subnet. A malicious user can exploit the ability of the router to send ICMP redirects by continually sending packets to the router, forcing the router to respond with ICMP redirect messages, resulting in an adverse impact on the CPU and performance of the router. In order to prevent the router from sending ICMP redirects, use the no ip redirects interface configuration command.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 37. Configuration Change Notification and Logging

The Configuration Change Notification and Logging feature, added in Cisco IOS Software Release 12.3(4)T, makes it possible to log the configuration changes made to a Cisco IOS device. The log is maintained on the Cisco IOS device and contains the user information of the individual who made the change, the configuration command entered, and the time that the change was made. This functionality is enabled using the logging enable configuration change logger configuration mode command. The optional commands hidekeys and logging size entries are used in order to improve the default configuration by preventing the logging of password data and increasing the length of the change log.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 38. Cisco IOS Software Resilient Configuration

The Resilient Configuration feature makes it possible to securely store a copy of the Cisco IOS software image and device configuration that is currently being used by a Cisco IOS device. When this feature is enabled, it is not possible to alter or remove these backup files. You are advised to enable this feature to prevent both inadvertent and malicious attempts to delete these files.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 39. Enable exclusive configuration change access mode

The Exclusive Configuration Change Access feature ensures that only one administrator makes configuration changes to a Cisco IOS device at a given time. This feature helps eliminate the undesirable impact of simultaneous changes made to related configuration components. This feature is configured using the global configuration command configuration mode exclusive mode and operates in one of two modes: auto and manual. In auto-mode, the configuration automatically locks when an administrator issues the configure terminal EXEC command. In manual mode, the administrator uses the configure terminal lock command to lock the configuration when entering configuration mode.

## MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 40. Do not include router information in warning banners

In some legal jurisdictions it can be impossible to prosecute and illegal to monitor malicious users unless they have been notified that they are not permitted to use the system. One method to provide this notification is to place this information into a banner message that is configured with the Cisco IOS software banner login command.

Legal notification requirements are complex, vary by jurisdiction and situation, and should be discussed with legal counsel. Even within jurisdictions, legal opinions can differ. In cooperation with counsel, a banner can provide some or all of the this information:

Notice that the system is to be logged into or used only by specifically authorized personnel and perhaps information about who can authorize use.

Notice that any unauthorized use of the system is unlawful and can be subject to civil and criminal penalties.

Notice that any use of the system can be logged or monitored without further notice and that the resulting logs can be used as evidence in court.

Specific notices required by local laws.

From a security point of view, rather than legal, a login banner should not contain any specific information about the router name, model, software, or ownership. This information can be abused by malicious users.

---

### 41. Control transport for vty and tty Lines

In an effort to prevent information disclosure or unauthorized access to the data that is transmitted between the administrator and the device, transport input ssh should be used instead of clear-text protocols, such as Telnet and rlogin. The transport input none configuration can be enabled on a tty, which in effect disables the tty line from being used for reverse-console connections. A vty and tty should be configured to accept only encrypted and secure remote access management connections to the device, or through the device if it is being used as a console server.

Both vty and tty lines allow an administrator to connect to other devices. In order to limit the type of transport that an administrator can use for outgoing connections, use the transport output line configuration command. If outgoing connections are not needed, then transport output none should be used. However, if outgoing connections are allowed, then an encrypted and secure remote access method for the connection should be enforced through the use of transport output ssh.

Note that IPSec can be used for encrypted and secure remote access connections to a device, if supported.

If you use IPSec, it also adds additional CPU overhead to the device. However, SSH must still be enforced as the transport even when IPSec is used.

## MAINOPTIONS

Compliance: PCI-DSS, HIPAA

---

### 42. Use authentication to control vty and tty lines

The simplest form of access control to a vty or tty of a device is through the use of authentication on all lines regardless of the device location within the network. This is critical for vty lines because they are accessible via the network. A tty line that is connected to a modem being used for remote access to the device, or a tty line that is connected to the console port of other devices are also accessible via the network. Other forms of vty and tty access controls can be enforced by using the transport input or access-class configuration commands, using the CoPP and CPPr features, or by applying access lists to interfaces on the device.

Authentication can be enforced through the use of AAA, which is the recommended method for authenticated access to a device, by using the local user database, or by simple password authentication configured directly on the vty or tty line.

The exec-timeout command must be used in order to logout sessions on vty or tty lines that are left idle. The service tcp-keepalive-in command must also be used in order to enable TCP keepalives on incoming connections to the device. This ensures that the device on the remote end of the connection is still accessible and that half-open or orphaned connections are removed from the local IOS device.

---

#### 43. Secure console port access

Any method used in order to access the console port of a device must be secured in a manner that is equal to the security that is enforced for privileged access to a device. Methods used in order to secure access must include the use of AAA, exec-timeout, and modem passwords if a modem is attached to the console. If password recovery is not required, then an administrator can remove the ability to perform the password recovery procedure using the no service password-recovery global configuration command; however, once the no service password-recovery command has been enabled, an administrator can no longer perform password recovery on a device.

#### MAINOPTIONS

Compliance: PCI-DSS, HIPAA

---

#### 44. Encrypt management Sessions

Because information can be disclosed during an interactive management session, this traffic must be encrypted so that a malicious user cannot gain access to the data being transmitted. Encrypting the traffic allows a secure remote access connection to the device. If the traffic for a management session is sent over the network in cleartext, an attacker can obtain sensitive information about the device and the network. An administrator is able to establish an encrypted and secure remote access management connection to a device by using the Secure Shell (SSH) or HTTPS (Secure Hypertext Transfer Protocol) features. Cisco IOS software supports SSH Version 1.0 (SSH1), SSH Version 2.0 (SSH2), and HTTPS that uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for authentication and data encryption. Note that SSH1 and SSH2 are not compatible.

#### REFERENCE

[http://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t15/feature/guide/ftsslsht.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftsslsht.html)

#### MAINOPTIONS

Compliance: PCI-DSS, HIPAA

---

#### 45. Enable Control Plane Protection(CPPr)

Control Plane Protection (CPPr) builds on the functionality of Control Plane Policing in order to restrict and police control plane traffic that is destined to the route processor of the IOS device. CPPr, added in Cisco IOS Software Release 12.4(4)T, divides the control plane into separate control plane categories that are known as subinterfaces. Three control plane subinterfaces exist: Host, Transit and CEF-Exception. In addition, CPPr includes these additional control plane protection features:

Port-filtering feature—This feature provides for the policing or dropping of packets going to closed or non-listening TCP and UDP ports.

Queue-threshold policy feature—This feature limits the number of packets for a specified protocol that are allowed in the control plane IP input queue.

CPPr allows an administrator to classify, police, and restrict traffic that is sent to a device for management purposes using the host subinterface. Examples of packets that are classified for the host subinterface category include management traffic such as SSH or Telnet and routing protocols.

---

#### 46. Enable Management Plane Protection(MPP)

The feature Management Plane Protection (MPP) allows an administrator to restrict on which interfaces management traffic can be received by a device. This allows the administrator additional control over a device and how the device is accessed.

---

#### 47. ACL Support for Filtering on TTL Value

Enable ACL support for filtering IP packets based on the Time to Live (TTL) value. The TTL value of an IP datagram is decremented by each network device as a packet flows from source to destination. Although initial values vary by operating system, when the TTL of a packet reaches zero, the packet must be dropped. The device that decrements the TTL to zero, and therefore drops the packet, is required to generate and send an ICMP Time Exceeded message to the source of the packet.

---

#### 48. ACL Support for Filtering IP Options

Use of ACLs to filter IP packets based on the IP options that are contained in the packet. IP options present a security challenge for network devices because these options must be processed as exception packets. This requires a level of CPU effort that is not required for typical packets that traverse the network. The presence of IP options within a packet can also indicate an attempt to subvert security controls in the network or otherwise alter the transit characteristics of a packet. It is for these reasons that packets with IP options must be filtered at the edge of the network.

---

#### 49. Filter IP Fragments

The filtering of fragmented IP packets can pose a challenge to security devices. This is because the Layer 4 information that is used in order to filter TCP and UDP packets is only present in the initial fragment. Cisco IOS software uses a specific method to check non-initial fragments against configured access lists. Cisco IOS software evaluates these non-initial fragments against the ACL and ignores any Layer 4 filtering information. This causes non-initial fragments to be evaluated solely on the Layer 3 portion of any configured ACE.

#### MAINOPTIONS

Compliance: PCI-DSS

---

#### 50. ICMP Packet Filtering

The Internet Control Message Protocol (ICMP) is designed as an IP control protocol. As such, the messages it conveys can have far-reaching ramifications to the TCP and IP protocols in general. While the network troubleshooting tools ping and traceroute use ICMP, external ICMP connectivity is rarely needed for the proper operation of a network.

#### MAINOPTIONS

### 51. [Configure Infrastructure ACLs\(iACL\)](#)

Infrastructure access control lists (iACLs) are one of the most critical security controls that can be implemented in networks. Infrastructure ACLs leverage the idea that nearly all network traffic traverses the network and is not destined to the network itself.

An iACL is constructed and applied to specify connections from hosts or networks that need to be allowed to network devices. Common examples of these types of connections are eBGP, SSH, and SNMP. After the required connections have been permitted, all other traffic to the infrastructure is explicitly denied. All transit traffic that crosses the network and is not destined to infrastructure devices is then explicitly permitted.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 52. [Enhanced Crashinfo File Collection](#)

The Enhanced Crashinfo File Collection feature automatically deletes old crashinfo files. This feature allows a device to reclaim space to create new crashinfo files when the device crashes. This feature also allows configuration of the number of crashinfo files to be saved.

---

### 53. [Detect and Correct Redzone Corruption](#)

The Buffer Overflow: Detection and Correction of Redzone Corruption feature can be enabled by on a device in order to detect and correct a memory block overflow and to continue operations.

These global configuration commands can be used in order to enable this feature. Once configured, the show memory overflow command can be used in order to display the buffer overflow detection and correction statistics.

---

### 54. [Memory Leak Detector](#)

The Memory Leak Detector feature allows you to detect memory leaks on a device. Memory Leak Detector is able to find leaks in all memory pools, packet buffers, and chunks. Memory leaks are static or dynamic allocations of memory that do not serve any useful purpose. This feature focuses on memory allocations that are dynamic. You can use the show memory debug leaks EXEC command in order to detect if a memory leak exists.

---

### 55. [Reserve Memory for Console Access](#)

The Reserve Memory for Console Access feature can be used in order to reserve enough memory to ensure console access to a Cisco IOS device for administrative and troubleshooting purposes. This feature is especially beneficial when the device runs low on memory. You can issue the memory reserve console global configuration command in order to enable this feature. This example configures a Cisco IOS device to reserve 4096 kilobytes for this purpose.

---

### 56. [CPU Thresholding Notification](#)

Introduced in Cisco IOS Software Release 12.3(4)T, the CPU Thresholding Notification feature allows you to detect and be notified when the CPU load on a device crosses a configured threshold. When the threshold is crossed, the device generates and sends an SNMP trap message. Two CPU utilization thresholding methods

are supported on Cisco IOS software: Rising Threshold and Falling Threshold.

---

### 57. Memory Threshold Notifications

The feature Memory Threshold Notification, added in Cisco IOS Software Release 12.3(4)T, allows you to mitigate low-memory conditions on a device. This feature uses two methods to accomplish this: Memory Threshold Notification and Memory Reservation.

Memory Threshold Notification generates a log message in order to indicate that free memory on a device has fallen lower than the configured threshold. This configuration example shows how to enable this feature with the memory free low-watermark global configuration command. This enables a device to generate a notification when available free memory falls lower than the specified threshold, and again when available free memory rises to five percent higher than the specified threshold.

---

### 58. Loopback Management Interfaces

The management plane of a device is accessed in-band or out-of-band on a physical or logical management interface. Ideally, both in-band and out-of-band management access exists for each network device so that the management plane can be accessed during network outages.

One of the most common interfaces that is used for in-band access to a device is the logical loopback interface. Loopback interfaces are always up, whereas physical interfaces can change state, and the interface can potentially not be accessible. It is recommended to add a loopback interface to each device as a management interface and that it be used exclusively for the management plane. This allows the administrator to apply policies throughout the network for the management plane. Once the loopback interface is configured on a device, it can be used by management plane protocols, such as SSH, SNMP, and syslog, in order to send and receive traffic.

---

### 59. Keepalives for TCP Sessions

The service tcp-keepalive-in and service tcp-keepalive-out global configuration commands enable a device to send TCP keepalives for TCP sessions. This configuration must be used in order to enable TCP keepalives on inbound connections to the device and outbound connections from the device. This ensures that the device on the remote end of the connection is still accessible and that half-open or orphaned connections are removed from the local Cisco IOS device.

---

### 60. Set EXEC timeout interval

In order to set the interval that the EXEC command interpreter waits for user input before it terminates a session, issue the exec-timeout line configuration command. The exec-timeout command must be used in order to logout sessions on vty or tty lines that are left idle. By default, sessions are disconnected after 10 minutes of inactivity.

---

### 61. Disable Unused Services

Any unnecessary service must be disabled. These unneeded services, especially those that use UDP (User Datagram Protocol), are infrequently used for legitimate purposes, but can be used in order to launch DoS and other attacks that are otherwise prevented by packet filtering.

The following TCP and UDP small services must be disabled. These services include:

echo (port number 7)

discard (port number 9)

daytime (port number 13)

chargen (port number 19)

Although abuse of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services must be disabled on any device accessible within the network. The small services are disabled

by default in Cisco IOS Software Releases 12.0 and later. In earlier software, the `no service tcp-small-servers` and `no service udp-small-servers` global configuration commands can be issued in order to disable them.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 62. Secure and archive configuration settings

Configuration management is a process by which configuration changes are proposed, reviewed, approved, and deployed. Within the context of a Cisco IOS device configuration, two additional aspects of configuration management are critical: configuration archival and security.

Configuration archives can be used to roll back changes that are made to network devices. In a security context, configuration archives can also be used in order to determine which security changes were made and when these changes occurred. In conjunction with AAA log data, this information can assist in the security auditing of network devices.

The configuration of a Cisco IOS device contains many sensitive details. Usernames, passwords, and the contents of access control lists are examples of this type of information. The repository that you use in order to archive Cisco IOS device configurations needs to be secured. Insecure access to this information can undermine the security of the entire network.

#### MAINOPTIONS

Compliance: SOX, PCI-DSS, HIPAA

---

### 63. Enable traffic monitoring using NetFlow

NetFlow monitors traffic flows in the network. Originally intended to export traffic information to network management applications, NetFlow can also be used in order to show flow information on a router. This capability allows to see what traffic traverses the network in real time. Regardless of whether flow information is exported to a remote collector, configure network devices for NetFlow so that it can be used reactively if needed.

### 64. Use Secure Protocols

Many protocols are used in order to carry sensitive network management data. Use secure protocols whenever possible. A secure protocol choice includes the use of SSH instead of Telnet so that both authentication data and management information are encrypted. In addition, use secure file transfer protocols when copying configuration data. An example is the use of the Secure Copy Protocol (SCP) in place of FTP or TFTP.

#### MAINOPTIONS

Compliance: PCI-DSS

---