# SECURING MANAGEMENT AND REPORTING FEATURES

# Management Reporting Considerations

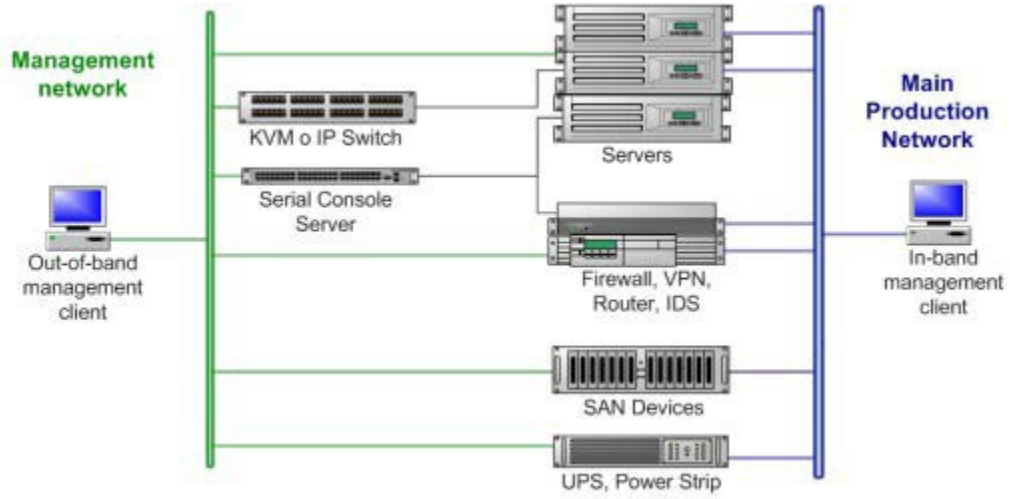
- Configuring logging for a few devices is a fairly simple and straightforward operation.
- Configuring logging for hundreds of devices can be very challenging.

# Information Paths

- Information flow between management hosts and the managed devices can take two paths.

Out of Band (OOB):
- Information flows within a network on which no production traffic resides.

In-Band:
- Information flows across the enterprise production network or the Internet (or both).



# Logging Management Considerations

- Some questions that must be considered when designing an in-band management solution:
  - Which management protocols does each device support?
  - Does the management channel need to be active at all times?
  - Is SNMP necessary?
  - Which are the most important logs?
  - How are important messages separated from routine notifications?
  - **How do you prevent tampering with logs?**
  - How do you make sure time stamps are consistent?
  - What log data is needed in criminal investigations?
  - How do you deal with the volume of log messages?
  - How do you manage all the devices?
  - How can you track changes when attacks or network failures occur?

# In-Band Management Guidelines

- Apply only to devices needing to be managed or monitored.
- Use IPsec when possible.
- Use SSH or SSL instead of Telnet (never use Telnet unless you are talking about Telnet over TLS).
- Decide whether the management channel needs to be open at all times.
- Keep clocks on hosts and network devices synchronized.
- Record changes and archive configurations.

# OOB Management Guidelines

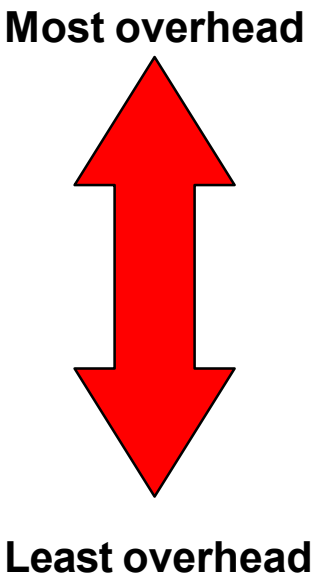
- Provide highest level of security and mitigate the risk of passing insecure management protocols over the production network.
- Keep clocks on hosts and network devices synchronized.
- Record changes and archive configurations.

# Implementing Log Messaging for Security

- Routers should be configured to send log messages to one or more of these:
  - Console
  - Terminal lines
  - Memory buffer
  - SNMP Server
  - Syslog Server

# Logging Destinations

- Be aware that the logging destination used affects system overhead.
  - Logging to the **console**.
  - Logging to **VTY**.
  - Logging to a **Syslog Server**.
  - Logging to an internal **buffer**.

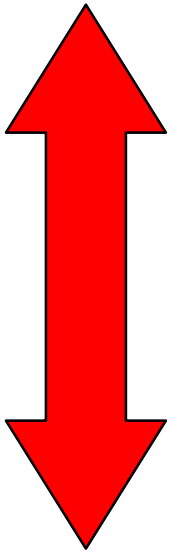


# Components of Syslog Systems

- Syslog server:
  - A host that accepts and processes log messages from one or more syslog clients.
- Syslog client:
  - A host that generates log messages and forwards them to a syslog server.
  - Routers, switches, PIXs, ASAs, APs, servers, …

# Syslog Error Message Levels

**Highest Level**



| Level | Keyword | Description | Syslog Definition |
|---|---|---|---|
| 0 | **emergencies** | System is unusable. | LOG_EMERG |
| 1 | **alerts** | Immediate action is needed. | LOG_ALERT |
| 2 | **critical** | Critical conditions exist. | LOG_CRIT |
| 3 | **errors** | Error conditions exist. | LOG_ERR |
| 4 | **warnings** | Warning conditions exist. | LOG_WARNING |
| 5 | **notification** | Normal but significant condition. | LOG_NOTICE |
| 6 | **informational** | Informational messages only. | LOG_INFO |
| 7 | **debugging** | Debugging messages. | LOG_DEBUG |

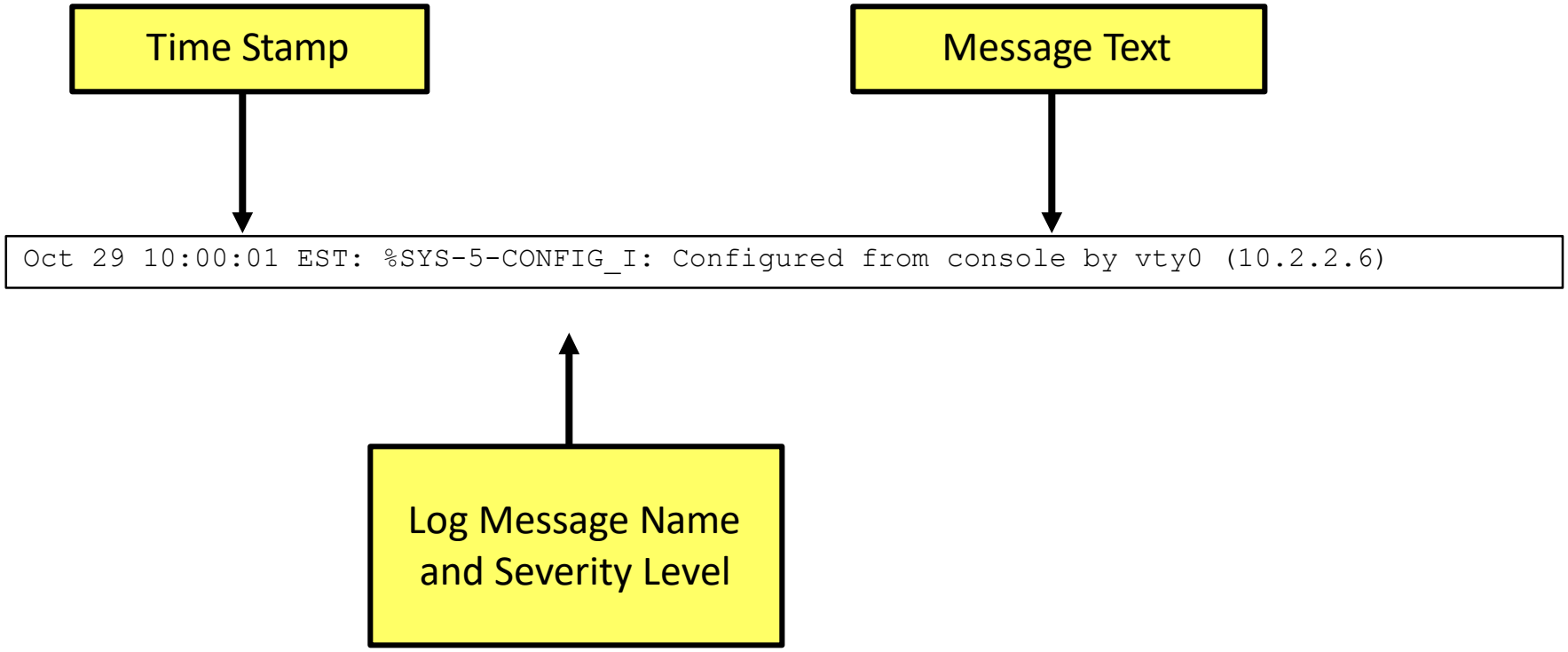
**Lowest Level**

- By default, Severity level 7 (debugging) messages are sent to the router's console port (line con0).
- Note: Level varies by platform and IOS release.

# Cisco Log Severity Levels

| Level and Name | Definition | Example |
|---|---|---|
| **0 LOG_EMERG** | A panic condition normally broadcast to all users | Cisco IOS software could not load |
| **1 LOG_ALERT** | A condition that should be corrected immediately, such as a corrupted system database | Temperature too high |
| **2 LOG_CRIT** | Critical conditions; for example, hard device errors | Unable to allocate memory |
| **3 LOG_ERR** | Errors | Invalid memory size |
| **4 LOG_WARNING** | Warning messages | Crypto operation failed |
| **5 LOG_NOTICE** | Conditions that are not error conditions but should possibly be addressed | Interface changed state, up or down |
| **6 LOG_INFO** | Informational messages | Packet denied by ACL |
| **7 LOG_DEBUG** | Messages that contain information that is normally used only when debugging | Packet type invalid |

# Log Message Format




Note: The log message name is not the same as a severity level name.

# Configuring Syslog Step 1

1. Set the destination logging host.
   - You can specify the IP address or the DNS name.

```
Router(config)# logging host [host-name | ip-address]
```

| Parameter | Description |
|---|---|
| *host-name* | The name of the host you want to use as a syslog server |
| *ip-address* | The IP address of the host you want to use as a syslog server |

# Configuring Syslog Step 2

2. (Optional) Set the log severity (trap) level.

```
Router(config)# logging trap level
```

| Parameter | Description |
|---|---|
| *level* | Limits the logging of messages to the syslog servers to a specified level.<br>You can enter the level number (0 to 7) or level name. |

# Configuring Syslog Step 3

3. (Optional) Set the source interface.
   - Specifies that syslog packets contain the IP or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router

```
Router(config)# logging source-interface interface-type interface-number
```

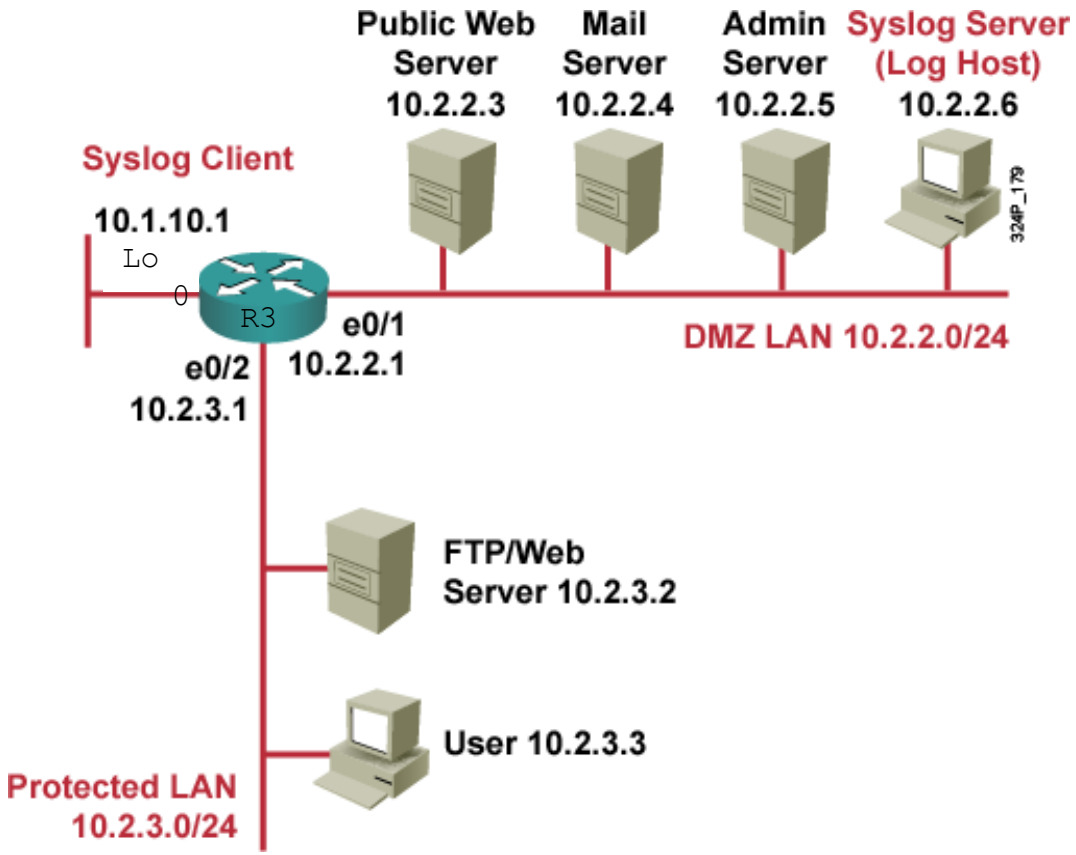
| Parameter | Description |
|---|---|
| *interface-type* | The interface type (for example, FastEthernet) |
| *interface-number* | The interface number (for example, 0/1) |

# Configuring Syslog Step 4

4. Enable logging
   - You can enable or disable logging individually:
     - **`[no] logging buffered`**
     - **`[no] logging monitor`**
   - However, if the **`no logging`** on command is configured, no messages will be sent to these destinations.

```
Router(config)# logging on
```

# Syslog Implementation Example




```
R3(config)# logging 10.2.2.6
R3(config)# logging trap informational
R3(config)# logging source-interface loopback 0
R3(config)# logging on
```

# VTY Monitor Logging

- The VTY monitoring option is the most practical method for viewing logging events in real time.
- To view system messages over a VTY session (line vty 0 - 4), **`logging monitor`** must be configured.
- To enable monitor logging, use the configuration command **`logging monitor [`***`severity`***`]`**.

# VTY Monitor Logging

- Hmmm … I made an SSH connection to a router and entered **`debug ip packet`** but don't see any output. Why?
- You have to enter the enable exec command **`terminal monitor`** to activate logging and see console message output to the vty.

# VTY Monitor Logging

- SSH from another host and use the EXEC command **`terminal monitor`** to view the output.

```
R3(config)# logging monitor
R3(config)# logging monitor error
```

# VTY Monitor Logging Tip

- It is recommended to establish two VTY sessions:
  - One for displaying event reporting data.
  - The other for command execution.
- Why?
  - Once terminal monitoring is enabled, it cannot be disabled on that VTY session.
  - A large amount of logging data can be generated, obscuring the VTY with logging output and making command entry quite difficult at times.

# `logging synchronous`

- The **`logging synchronous`** line configuration command also affects the display of messages to the console.
- When enabled, messages will appear only after the user types a carriage return.
- Without the this command, console messages displayed can interfere with command line entry.

# CONFIGURING NTP (Network Time Protocol)

# Understanding NTP

- “Time has been invented in the universe so that everything would not happen at once.”
  - The NTP FAQ and HOWTO - http://www.ntp.org/ntpfaq/

- Many features in a computer network depend on time synchronization:
  - For accurate time information in log messages.
  - Certificate-based authentication in VPNs.
  - ACLs with time range configuration.

# System Clock

- The heart of the router time service is the software-based system clock.
  - This clock keeps track of time from the moment the system starts.
- The system clock can be set from a number of sources and can be used to distribute the current time through various mechanisms to other systems.
  - When a router with a system calendar is initialized or rebooted, the system clock is set based on the time in the internal battery-powered system calendar.
- The system clock can then be set:
  - Manually using the **`set clock`** privileged EXEC command.
  - Automatically using the Network Time Protocol (NTP).
- NTP is an Internet protocol used to synchronize the clocks of network connected devices to some time reference.
  - NTP is an Internet standard protocol currently at v3 and specified in RFC-1305.

# NTP

- NTP is designed to time-synchronize a network.
  - NTP uses UDP.
- An NTP network usually obtains the time from an authoritative time source, such as a radio clock or an atomic clock.
  - NTP then distributes this time across the network.
  - NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within 1 ms of one another.
- Cisco devices support specifications for NTP v3 (RFC 1305).
  - NTP v4 is under development but NTP v3 is the Internet standard.
- NTP services are enabled on all interfaces by default.
  - To disable NTP on a specific interface, use the **`ntp disable`** command in the interface configuration mode.

# Configuring an NTP Master and Client

- To configure a router as the authoritative time source, use the **`ntp master`** command in global configuration mode.
- To configure a router as an NTP client, either:
  - Create an association to a server using the **`ntp server`** command.
  - Configure the router to listen to NTP broadcast packets using the **`ntp broadcast client`** command.

# Identifying the NTP Server

- Although the router can be configured with either a peer or a server association, NTP clients are typically configured with a server association (meaning that only this system will synchronize to the other system, and not vice versa).
- To allow the software clock to be synchronized by an NTP time server, use the **`ntp server`** command in global configuration mode.

```
Router(config)# ntp server {ip-address | hostname} [version number] [key keyed]
  [source interface] [prefer]
```

# Configuring NTP Associations

- NTP broadcast client:
  - In addition to or instead of creating unicast NTP associations, the system can be configured to listen to broadcast packets on an interface-by-interface basis.

- To do this, use the **`ntp broadcast client`** command in interface configuration mode.

```
Router(config-if)# ntp broadcast client
```

# NTP Security

- The time that a machine keeps is a critical resource, so the security features of NTP should be used to avoid the accidental or malicious setting of incorrect time.
- Two mechanisms are available:
  - ACL-based restriction scheme
  - Encrypted authentication

# NTP Authentication Commands

| Command | Description |
| --- | --- |
| **ntp authenticate** | Enables the NTP authentication feature.<br>If this command is specified, the system will not synchronize to another system unless the other system's NTP messages carry one of the specified authentication keys. |
| **ntp authentication-key** *number* **md5** *value* | Defines an authentication key supported by using MD5.<br>The key type md5 is currently the only key type that this command supports.<br>The key value can be any arbitrary string of up to eight characters. |
| **ntp trusted-key** *key-number* | Defines trusted authentication keys. |

# Configuring NTP Authentication

- Enable the authentication feature.

```
Router(config)# ntp authentication
```

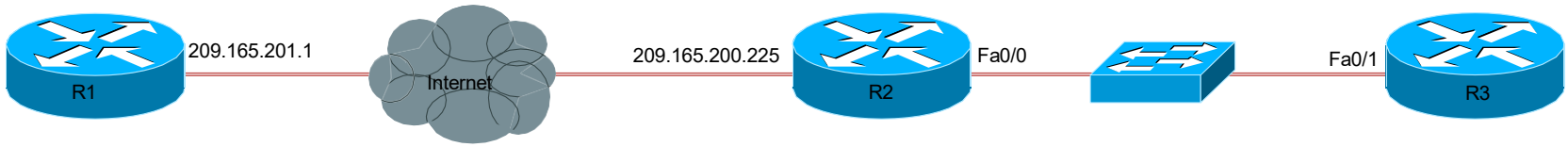
- Define the authentication key to be used for both peer and server associations.

```
Router(config)# ntp authentication-key key-number md5 value
```

- Define which key is to be trusted.

```
Router(config)# ntp trusted-key key-number
```

# NTP Configuration Example




```
R1(config)# ntp master 5
R1(config)# ntp authentication-key 1 md5 R1-SECRET
R1(config)# ntp peer 209.165.200.225 key 1
```

```
R2(config)# ntp authentication-key 1 md5 R1-SECRET
R2(config)# ntp authentication-key 2 md5 R2-SECRET
R2(config)# ntp trusted-key 1
R2(config)# ntp server 209.165.201.1
R2(config)# interface Fastethernet0/0
R2(config-if)# ntp broadcast
```

```
R3(config)# ntp authentication-key 1 md5 R2-SECRET
R3(config)# ntp trusted-key 1
R3(config)# interface Fastethernet0/1
R3(config-if)# ntp broadcast client
```

# DISABLING UNUSED CISCO ROUTER NETWORK SERVICES AND INTERFACES

# Vulnerable Router Services

- Medium size and large networks typically use a firewall appliance (PIX / ASA) behind the perimeter router, which adds security features and performs user authentication and more advanced packet filtering.
- Firewall installations also facilitate the creation of Demilitarized Zones (DMZs), where the firewall ‘places’ hosts that are commonly accessed from the Internet.

# Vulnerable Router Services

- As an alternative, Cisco IOS software can incorporate many firewall features in the perimeter router.
  - Option is valid only for small-to-medium business perimeter security requirements.
- However, Cisco IOS routers run many services that create potential vulnerabilities.
  - To secure an enterprise network, all unneeded router services and interfaces must be disabled.

| Router Service | Description | Default | Best Practice |
|---|---|---|---|
| **BOOTP server** | • This service allows a router to act as a BOOTP server for other routers.<br>• If not required, disable this service. | Enabled | Disable.<br>`no ip bootp server` |
| **Cisco Discovery Protocol (CDP)** | • CDP obtains information of neighboring Cisco devices.<br>• If not required, disable this service globally or on a per-interface basis. | Enabled | Disable if not required.<br>**no cdp run** |
| **Configuration auto-loading** | • Auto-loading of configuration files from a network server should remain disabled when not in use by the router. | Disabled | Disable if not required.<br>**no service config** |
| **FTP server** | • The FTP server enables you to use your router as an FTP server for FTP client requests.<br>• Because this server allows access to certain files in the router Flash memory, this service should be disabled when not required. | Disabled | Disable if not required.<br>Otherwise encrypt traffic within an IPsec tunnel. |
| **TFTP server** | • Same as FTP. | Disabled | Disable if not required.<br>Otherwise encrypt traffic within an IPsec tunnel. |
| **Network Time Protocol (NTP) service** | • When enabled, the router acts as a time server for other network devices.<br>• If configured insecurely, NTP can be used to corrupt the router clock and potentially the clock of other devices that learn time from the router.<br>• If this service is used, restrict which devices have access to NTP. | Disabled | Disable if not required.<br>Otherwise configure NTPv3 and control access between permitted devices using ACLs. |

| Router Service | Description | Default | Best Practice |
|---|---|---|---|
| **Packet assembler and disassembler (PAD) service** | • The PAD service allows access to X.25 PAD commands when forwarding X.25 packets. | Enabled | Disable if not required. |
| **TCP and UDP minor services** | • The minor services are provided by small servers (daemons) that run in the router. The services are potentially useful for diagnostics, but are rarely used. | Enabled (pre 11.3) Disabled (11.3+) | Disable if not required. `no service tcp-small-servers` `no service udp-small-servers` |
| **Maintenance Operation Protocol (MOP) service** | • MOP is a Digital Equipment Corporation (DEC) maintenance protocol that should be explicitly disabled when not in use. | Enabled | Disable explicitly if not required. |

# Commonly Configured Management Services

| Service | Description | Default | Best Practice |
|---|---|---|---|
| **Simple Network Management Protocol (SNMP)** | • The SNMP service allows the router to respond to remote SNMP queries and configuration requests.<br>• If required, restrict which SNMP systems have access to the router SNMP agent and use SNMPv3 whenever possible because version 3 offers secure communication that is not available in earlier versions of SNMP. | Enabled | Disable the service. Otherwise configure SNMPv3. |
| **HTTP configuration and monitoring** | • This service allows the router to be monitored or have the router configuration modified from a web browser via an application such as the Cisco Security Device Manager (SDM). You should disable this service if the service is not required. If this service is required, restrict access to the router HTTP service by using access control lists (ACLs). | Device dependent | Disable if not required. Otherwise restrict access using ACLs.<br>**`no ip http server`** |
| **Domain Name System (DNS)** | • By default, Cisco routers broadcast name requests to 255.255.255.255.<br>• Restrict this service by disabling DNS when the service is not required.<br>• If the DNS lookup service is required, make sure that you set the DNS server address explicitly. | Client Service – Enabled | Disable if not required. Otherwise explicitly configure the DNS server address.<br>**`no ip domain-lookup`**<br>**`no ip name-server`** |

# Path Integrity Mechanisms

| Path Integrity Mechanisms | Description | Default | Best Practice |
|---|---|---|---|
| ICMP redirects | • ICMP redirects cause the router to send ICMP redirect messages whenever the router is forced to resend a packet through the same interface on which the packet was received.<br>• This information can be used by attackers to redirect packets to an untrusted device. | Enabled | Disable the service. |
| IP source routing | • The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that a datagram will take toward the datagram's ultimate destination, and generally the route that any reply will take.<br>• These options can be exploited by an attacker to bypass the intended routing path and security of the network.<br>• Also, some older IP implementations do not process source-routed packets properly, and hackers may be able to crash machines that run these implementations by sending datagrams with source routing options. | Enabled | Disable if not required.<br>`no ip source-route` |

# Probe and Scan Features

| Probes and Scan Features | Description | Default | Best Practice |
|---|---|---|---|
| Finger service | • The finger protocol (port 79) can obtain a list of the users who are currently logged into a device.<br>• Unauthorized persons can use this information for reconnaissance attacks. | Enabled | Disable if not required.<br>`no ip finger`<br>`no service finger` |
| ICMP unreachable notifications | • ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Cisco routers automatically send ICMP messages.<br>• Attackers commonly use three ICMP messages:<br>  • Host unreachable<br>  • Redirect<br>  • Mask Reply<br>• Automatic generation of these messages should be disabled on all interfaces, especially interfaces that are connected to untrusted networks. | Enabled | Disable explicitly on untrusted interfaces. |
| ICMP mask reply | • When enabled, this service tells the router to respond to ICMP mask requests by sending ICMP mask reply messages that contain the interface IP address mask.<br>• This information can be used to map the network | Disabled | Disable explicitly on untrusted interfaces. |

# Terminal Access Security

| Terminal Access Security | Description | Default | Best Practice |
|---|---|---|---|
| **IP identification service** | • The identification protocol (specified in RFC 1413) reports the identity of a TCP connection initiator to the receiving host.<br>• This data can be used by an attacker to gather information about your network | Enabled | Disable. |
| **TCP Keepalives** | • TCP keepalives help “clean up” TCP connections where a remote host has rebooted or otherwise stopped processing TCP traffic.<br>• Keepalives should be enabled globally to manage TCP connections and prevent certain DoS attacks. | Disabled | Enable. |

# ARP Service

| Terminal Access Security | Description | Default | Best Practice |
|---|---|---|---|
| **Gratuitous ARP** | • Gratuitous ARP is the main mechanism that hackers use in ARP poisoning attacks. | Enabled | Disable if not required. |
| **Proxy ARP** | • Proxy ARP enables a Cisco router to act as an intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments.<br>• Proxy ARP should be used only between two LAN segments at the same trust level, and only when absolutely necessary to support legacy network architectures. | Enabled | Disable if not required. |

# IP Directed Broadcasts

| IP Directed Broadcasts | Description | Default | Best Practice |
|---|---|---|---|
| **IP Directed Broadcasts** | • IP directed broadcasts are used in the common and popular smurf DoS attack and other related attacks.<br>• Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment.<br>• This technique was used in some old DoS attacks, and the default Cisco IOS configuration is to reject directed broadcasts. | Enabled (pre 12.0)<br>Disabled (12.0+) | Disable if not required. |

```
•Router(config)# no ip bootp server
•Router(config)# no cdp run
•Router(config)# no ip source-route
•Router(config)# no ip classless
•Router(config)# no service tcp-small-servers
•Router(config)# no service udp-small-servers
•Router(config)# no ip finger
•Router(config)# no service finger
•Router(config)# no ip http server
•Router(config)# no ip name-server
•Router(config)# no boot network
•Router(config)# no service config
```

# IP Classless Routing

- By default, a Cisco router will make an attempt to route almost any IP packet.
  - If a packet arrives addressed to a subnet of a network with no default network route, then IOS will use IP classless routing to forward the packet along the best available route.
- This feature is often not needed therefore on routers where IP classless routing is not needed. Disable it using the **`no ip classless`** command.

# Protecting Routing Table Integrity

- Use only static routes:
  - Works well in small networks.
  - Unsuitable for large networks.
- Authenticate route table updates:
  - Configure routing authentication.
  - Authenticated router updates ensure that the update messages come from legitimate sources.

# Passive Interfaces

- Configure the **`passive-interface`** command to prevent hackers from learning about the existence of certain routes or routing protocols used.

# Router Hardening Considerations

- Attackers can exploit unused router services and interfaces.
- Administrators do not need to know how to exploit the services, but they should know how to disable them.
- It is tedious to disable the services individually.
- An automated method is needed to speed up the hardening process.

# Locking Down Routers with AutoSecure

- The **AutoSecure** feature was released in Cisco IOS Release 12.3.
- AutoSecure is a single privileged EXEC program that allows elimination of many potential security threats quickly and easily.
  - AutoSecure helps to make you more efficient at securing Cisco routers.
- AutoSecure allows two modes of operation:
  - **Interactive mode**: Prompts to choose the way you want to configure router services and other security-related features.
  - **Noninteractive mode**: Configures security-related features on your router based on a set of Cisco defaults.

# AutoSecure "Planes"

- Management plane services and functions:
  - Finger, PAD, UDP and TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, ICMP (redirects, mask-replies), directed broadcast, MOP, banner
  - password security and SSH access
- Forwarding plane services and functions:
  - CEF, traffic filtering with ACLs
- Firewall services and functions:
  - Cisco IOS Firewall inspection for common protocols
- Login functions:
  - Password security
- NTP protocol
- SSH access
- TCP Intercept services

# AutoSecure Rollback Feature

- If AutoSecure fails to complete its operation, the running configuration may be corrupt:
  - In Cisco IOS Release 12.3(8)T and later releases a pre-AutoSecure configuration snapshot is stored in the flash under filename **`pre_autosec.cfg`**.
  - Rollback reverts the router to the router's pre-autosecure configuration using the **`configure replace flash:pre_autosec.cfg`** command.
  - If the router is using software prior to Cisco IOS Release 12.3(8)T, the running configuration should be saved before running AutoSecure.

# AutoSecure Process Overview

- Cisco AutoSecure Interactive Steps:
  - Step 1 – Identify outside interfaces.
  - Step 2 – Secure the management plane.
  - Step 3 – Create the security banner.
  - Step 4 – Configure passwords, AAA, and SSH.
  - Step 5 – Secure the forwarding plane.

```
Router#
```

```
auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh |
firewall | tcp-intercept]
```

# Auto Secure Parameters

| Parameter | Description |
|---|---|
| **management** | (Optional) Only the management plane will be secured. |
| **forwarding** | (Optional) Only the forwarding plane will be secured. |
| **no-interact** | (Optional) The user will not be prompted for any interactive configurations. No interactive dialogue parameters will be configured, including usernames or passwords. |
| **full** | (Optional) The user will be prompted for all interactive questions. This is the default setting. |
| **ntp** | (Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command-line interface (CLI). |
| **login** | (Optional) Specifies the configuration of the Login feature in the AutoSecure CLI. |
| **ssh** | (Optional) Specifies the configuration of the SSH feature in the AutoSecure CLI. |
| **firewall** | (Optional) Specifies the configuration of the Firewall feature in the AutoSecure CLI. |
| **tcp-intercept** | (Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI. |

# Step 1: Identify Outside Interfaces

```
Router# auto secure
          --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router but it will not
make router absolutely secure from all security attacks ***
All the configuration done as part of AutoSecure will be shown here. For more
details of why and how this configuration is useful, and any possible side effects,
please refer to Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: y
Enter the number of interfaces facing internet [1]: 1
Interface     IP-Address      OK? Method Status  Protocol
Ethernet0/0   10.0.2.2        YES NVRAM  up      up
Ethernet0/1   172.30.2.2      YES NVRAM  up      up

Enter the interface name that is facing internet: Ethernet0/1
```

# Step 2: Secure Management Plane

```
Securing Management plane services..
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
```

# Step 3: Create Security Banner

```
Here is a sample Security Banner to be shown at every access to device. Modify it
to suit your enterprise requirements.
Authorised Access only
  This system is the property of Woolloomooloo Pty Ltd.
  UNAUTHORISED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged and violations of of this policy result
  in disciplinary action.
Enter the security banner {Put the banner between
k and k, where k is any character}:
%This system is the property of Cisco Systems, Inc.
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.%
```

# Step 4: Passwords, AAA and Login Blocking

```
Enable secret is either not configured or is same as enable password
Enter the new enable secret: Curium96
Configuration of local user database
Enter the username: student1
Enter the password: student1
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Securing device against Login Attacks
Configure the following parameters
Blocking Period when Login Attack detected: 300
Maximum Login failures with the device: 3
Maximum time period for crossing the failed login attempts: 60
```

# Step 5: SSH and Interface-Specifics

```
Configure SSH server? [yes]: y
Enter the hostname: R2
Enter the domain-name: cisco.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces
```

# Step 6: Forwarding Plane and Firewall

```
Securing Forwarding plane services..
Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet
Configure CBAC Firewall feature? [yes/no]: yes
This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
.
.
Apply this configuration to running-config? [yes]: y
```