Chapter 2: Securing Network Devices

CCNA-Security

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2: Objectives

In this chapter you will:

- Explain how to secure a network perimeter.
- Configure secure administrative access to Cisco routers.
- Configure enhanced security for virtual logins.
- Configure an SSH daemon for secure remote management.
- Configure administrative privilege levels to control command availability.
- Configure role-based CLI access to control command availability.
- Use the Cisco IOS resilient configuration feature to secure the Cisco IOS image and configuration files.
- Compare in-band and out-of-band management access.
- Configure syslog to log system events.
- Configure SNMP to monitor system status.
- Configure NTP to enable accurate time stamping between all devices.
- Use security audit tools to determine IOS-based router vulnerabilities.
- Use AutoSecure to enable security on IOS-based routers.
- Use CCP to enable security on IOS-based routers.

Chapter 2

2.0 Introduction

2.1 Securing Device Access

2.2 Assigning Administrative Roles

2.3 Monitoring and Managing Devices

2.4 Using Automated Security Features

2.5 Summary

2.1 Securing Device Access

Cisco | Networking Academy®
Mind Wide Open™

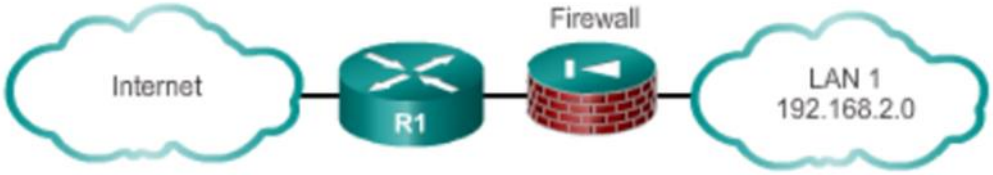
Securing Network Infrastructure

- Securing the network infrastructure is critical to overall network security.
- To prevent unauthorized access to all infrastructure devices, appropriate security policies, and controls must be implemented.
- Although all infrastructure devices are at risk, routers are a primary target for network attackers, because routers act as traffic police, directing traffic into, out of, and between networks.
- All of an organization's Internet traffic goes through this edge router.
- Through initial and final filtering, the edge router helps to secure the perimeter of a protected network and implements security actions that are based on the security policies of the organization.

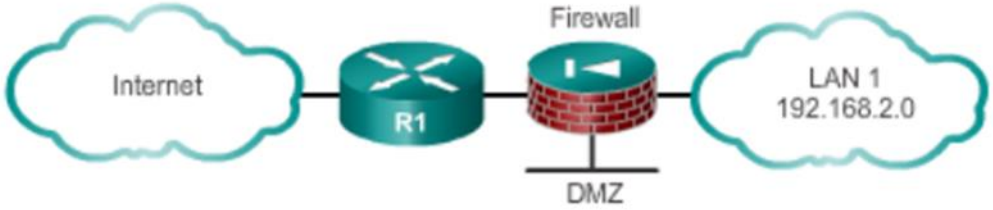
Implementing Security

- Single Router Approach

- Defense-in-Depth Approach



- DMZ Approach



Securing Routers

Three areas of router security must be maintained:

Secure Administrative Access

- **Restrict device accessibility** - Limits the accessible ports, restricts the permitted communicators, and restricts permitted methods of access.
- **Log and account for all access** - Records anyone who accesses a device, including what occurs and when.
- **Authenticate access** - Ensures that access is granted only to authenticated users, groups, and services.
- **Authorize actions** - Restricts the actions and views permitted by any particular user, group, or service.
- **Present legal notification** - Displays a legal notice.
- **Ensure the confidentiality of data** - Protects locally stored sensitive data from viewing and copying.

Securing Passwords

Weak Password	Why it is weak
secret	Simple dictionary password
smith	Mother's maiden name
toyota	Make of car
bob1967	Name and birthday of user
Blueleaf23	Simple words and numbers

Strong Password	Why it is strong
b67n42d39c	Combines alphanumeric characters
12^h u4@1p7	Combines alphanumeric characters, symbols and also includes a space

Configuring Secure Administrative Access

Securing Administrative Access

```
R1(config)# line console 0
R1(config-line)# password csc5io
R1(config-line)# login
```

```
R1(config)# line vty 0 4
R1(config-line)# password csc5io
R1(config-line)# login
```

```
R1(config)# line aux 0
R1(config-line)# password csc5io
R1(config-line)# login
```

```
R1(config)# enable secret csc5io
```

Increase Password Security

To increase password security:

- Enforce minimum password lengths.

  Administrators can set the minimum character length for all router passwords from 0 to 16 characters using the **security passwords min-length** *length* global configuration mode command.

- Disable unattended connections.

  The timeout period can be adjusted using the **exec-timeout** command in line configuration mode.

- Encrypt all passwords in the configuration file.

  Use the **service password-encryption** command in global configuration mode.

Configuring Secure Local Database Entries

```
username name secret ([0] password | 5 encrypted-secret)
```

Parameter	Description
name	Specifies the **username**
0	(Optional) Indicates that the plaintext *password* is to be hashed by the router using MD5
password	The plaintext *password* to be hashed using MD5
5	Indicates that the *encrypted-secret password* was hashed using MD5
encrypted-secret	The MD5 *encrypted-secret password* that is stored as the encrypted user *password*

Configuring Secure Local Database Entries Cont.

Sample Configuration

```
R1# conf t
R1(config)# username JR-ADMIN password cisco12345
R1(config)# username ADMIN secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
R1(config-line)# end
R1#
R1# show run | include username
username JR-ADMIN password 7 060506324F41584B564347
username ADMIN secret 5 $1$G3oQ$hEvsd5iz76WJuSJvtzs8I0
R1#
```

Configuring Enhanced Security for Virtual Logins

Enhancing the Login Process

Virtual Login Security Enhancements

- Implement delays between successive login attempts.
- Enable login shutdown if DoS attacks are suspected.
- Generate system-logging messages for login detection.

Enhanced Login Configuration Example

```
R1(config)# login block-for 15 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)#
```

Configuring Enhanced Security for Virtual Logins

Configuring Login Enhancement Features

If more than 5 login failures occur within 60 seconds, then all login will be disabled for 120 seconds.

- Must be issued before any other **login** command can be used.
- Helps provide DoS detection and prevention.

```
R1# configure terminal
R1(config)# username ADMIN secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config)# exit
R1(config)# login block-for 120 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)# exit
```

Configuring Enhanced Security for Virtual Logins

Configuring Login Enhancement Features Cont.

These commands exempt to administrative stations from the disabled login. If not configured, all login requests will be denied during the Quiet-Mode.

```
R1# configure terminal
R1(config)# username ADMIN secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config)# exit
R1(config)# login block-for 120 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)# exit
```

Configuring Enhanced Security for Virtual Logins

Configuring Login Enhancement Features Cont.

This optional command configures a delay of 10 seconds in between consecutive login attempt. If not set, a default delay of 1 second is enforced after the **`login block-for`** command is configured.

```
R1# configure terminal
R1(config)# username ADMIN secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config)# exit
R1(config)# login block-for 120 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)# exit
```

Logging Failed Attempts

To detect a password attack use the following commands:

```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]

R1(config)# security authentication failure rate threshold-
            rate log
```

Verifying R1 Login Status

```
R1#
*Dec 10 15:38:54.455: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft
for watching failures is 12 secs, [user: admin] [Source:
10.10.10.10] [localport: 23] [Reason: Login Authentication Failed
- BadUser] [ACL: PERMIT-ADMIN] at 15:38:54 UTC Wed Dec 10 2008
R1# show login
     A login delay of 3 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.
     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or
     less,logins will be disabled for 120 seconds.
     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 105 seconds.
     Restricted logins filtered by applied ACL PERMIT-ADMIN.
R1#
```

Logging Failed Attempts Cont.

In this example, the command identifies the amount of failures, usernames tried, and offending IP addresses with a timestamp added to each failed attempt.

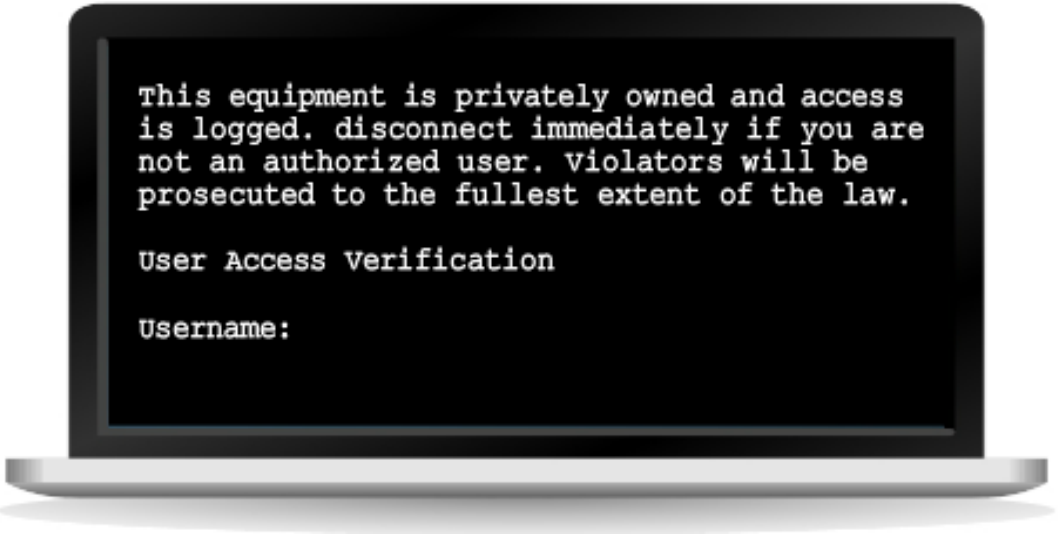
```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username     SourceIPAddr     lPort Count TimeStamp
admin        1.1.2.1          23    5     15:38:54 UTC Wed Dec 10 2008
Admin        10.10.10.10      23    13    15:58:43 UTC Wed Dec 10 2008
admin        10.10.10.10      23    3     15:57:14 UTC Wed Dec 10 2008
cisco        10.10.10.10      23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

Provide Legal Notification

Use banner messages to present legal notification to potential intruders.




```
R1(config)#
banner {motd | exec | login} delimiter message delimiter
```

SSH Implementation Configuring Before

Four steps must be completed prior to configuring routers for the SSH protocol:

Step 1. Ensure that the target routers are running a Cisco IOS release that supports SSH.

Step 2. Ensure that each of the target routers has a unique hostname.

Step 3. Ensure that each of the target routers is using the correct domain name of the network.

Step 4. Ensure that the target routers are configured for local authentication or AAA services for username and password authentication. This is mandatory for a router-to-router SSH connection.

Configuring SSH

Using the CLI, there are four steps to configure a Cisco router to support SSH:

Step 1. Configure domain name using the **ip domain-name** *domain-name* command in global configuration mode.

Step 2. Generate one-way secret keys ~~must be generated~~ for a router to encrypt the SSH traffic. To create the RSA key, use the **crypto key generate rsa general-keys modulus** *modulus-size* command in global configuration mode.

Step 3. Ensure that there is a valid local database username entry. If not, create one using the **username** *name* **secret** *secret* command.

Step 4. Enable vty inbound SSH sessions using the **login local** and **transport input ssh** commands in line vty configuration mode.

To verify SSH and display the generated keys, use the **show crypto key mypubkey rsa** command.

Additional SSH Commands

SSH commands can be used to configure the following:

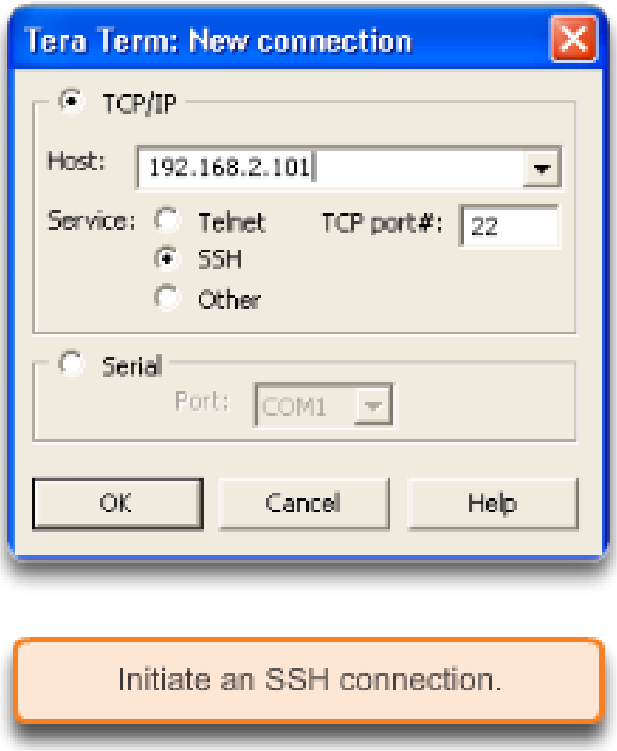
- SSH version
- SSH timeout period
- Number of authentication retries

```
R1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R1#
R1# conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 2
R1#
```

Connecting to an SSH-Enabled Router

There are two ways to connect to an SSH-enabled router:

- Using the **ssh** privileged EXEC mode command
- Using a publicly and commercially available SSH client running on a host, such as PuTTY, OpenSSH, or TeraTerm



Enabling SSH Using CCP

The Cisco Configuration Professional (CCP) can be used to configure an SSH daemon on a router.

- To view the current SSH key settings, on the CCP window, click **Configure > Router > Router Access > SSH**.
  - **RSA key is not set on this router** - If there is no key configured, enter a modulus size and generate a key.
  - **RSA key is set on this router** - Means a cryptographic key has been generated and SSH is enabled.
- The **Generate RSA** Key button configures a cryptographic key if one is currently set.
- After SSH is enabled on the router, the vty lines to support SSH must be configured. On the CCP window, click **Configure > Router > Router Access > VTY**.

2.2 Assigning Administrative Roles

Cisco | Networking Academy®
Mind Wide Open™

Limiting Command Availability

- Configuring privilege levels is the next step for the system administrator to secure the network.
- Privilege levels determine who should be allowed to connect to the device and what that person should be able to do with it.
- The Cisco IOS software CLI has two levels of access to commands:
  - **User EXEC mode (privilege level 1)**
  - **Privileged EXEC mode (privilege level 15)**
- Cisco IOS software has two methods of providing infrastructure access and a more precise method of controlling access:
  - **privilege level**
  - **role-based CLI**

Privilege Levels

- Level 0:
  - Predefined for user-level access privileges.
  - Seldom used, but includes five commands: **`disable`**, **`enable`**, **`exit`**, **`help`**, and **`logout`**
- Level 1(User EXEC mode):
  - The default level for login with the router prompt **Router>.**
  - A user cannot make any changes or view the running configuration file.
- Levels 2 –14:
  - May be customized for user-level privileges.
  - Commands from lower levels may be moved up to a higher level, or commands from higher levels may be moved down to a lower level.
- Level 15 (Privileged EXEC mode):
  - Reserved for the enable mode privileges (**`enable`** command).
  - Users can change configurations and view configuration files.

Privilege Levels Cont.

```
router(config)#
privilege mode {level level command | reset command}
```

Command	Description
mode	This command argument specifies the configuration mode. Use the **privilege ?** command to see a list of router modes.
level	(Optional) This command enables setting a privilege level with a specified command.
level command	(Optional) This parameter is the privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) This command resets the privilege level of a command.
command	(Optional) This is the command argument to use when you want to reset the privilege level.

Configuring Privilege Levels

Two methods for assigning passwords to the different levels:

- To the privilege level, use the **`enable secret level`** *password* global configuration mode command.
- To a user that is granted a specific privilege level, use the **`username`** *name* **`privilege`** *level* **`secret`** *password* global configuration mode command.

```
R1# conf t
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
R1(config)#
```

Assigning Privilege Levels

- To assign level 10 and the **reload** privileged EXEC mode command to the JR-ADMIN account, use the following command sequence:
  - **privilege exec level 10 reload**
  - **enable secret level 10 cisco10**
  - **username JR-ADMIN privilege 10 secret cisco10**
- To access established privilege levels, enter the **enable** *level* command from user mode, and enter the password that was assigned to the custom privilege level.

```
R1# enable 15
Password: <cisco123>
R1# show privilege
Current privilege level is 15
R1# show running-config
Building configuration...

Current configuration : 1145 bytes
!
version 12.4

<Output omitted)
```

Role-Based CLI Access

- Introduced in Cisco IOS Release 12.3(11)T, provides more granular access by controlling specific commands that are available to specific roles.
- Enhances the security of the device by defining the set of CLI commands accessible by a specific user.
- Prevents unintentional execution of CLI commands by unauthorized personnel.
- Users only see the CLI commands applicable to the ports and CLI to which they have access.

Role-Based Views

- **Root view:**
  - Can configure any view for the system, the administrator must be in root view.
  - Has the same access privileges as a user who has level 15 privileges. However, a root view is not the same as a level 15 user.
  - Only a root view user can configure a new view and add or remove commands from the existing views.
- **CLI view**

  A specific set of commands can be bundled into a CLI view
- **Superview**

  A superview consists of one or more CLI views. Administrators can define which commands are accepted and which configuration information is visible.

Configuring Role-Based Views

There are five steps to create and manage a specific view:

Step 1. Enable AAA with the **aaa new-model** global configuration mode command. Exit and enter the root view with the **enable view** command.

Step 2. Create a view using the **parser view** *view-name* router configuration mode command. This enables the view configuration mode. Excluding the root view, there is a maximum limit of 15 views in total.

Step 3. Assign a secret password to the view using the **secret** *encrypted-password* view configuration mode command.

Step 4. Assign commands to the selected view using the **commands** ***parser-mode*** {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*] command in view configuration mode.

Step 5. Exit view configuration mode by typing the **exit** command.

Configuring Role-Based CLI Superviews

There are four steps to create and manage a superview:

Step 1. Create a view using the **parser view** *view-name* **superview** command and enter superview configuration mode.

Step 2. Assign a secret password to the view using the **secret** *encrypted-password* command.

Step 3. Assign an existing view using the **view** *view-name* command in view configuration mode.

Step 4. Exit superview configuration mode by typing the **exit** command.

To access existing views, enter the **enable view** *view-name* command in user mode and enter the password that was assigned to the custom view.

Verify Role-Based CLI Views

To verify a view, use the **enable view** command. Enter the name of the view to verify, and provide the password to log into the view.

```
R1# enable view SUPPORT
Password:
*Mar  1 10:00:11.353: %PARSER-6-VIEW_SWITCH: successfully set to view 'SUPPORT'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  show    Show running system information

R1#
```

Verify Role-Based CLI Views Cont.

From the root view, use the **`show parser view all`** command to see a summary of all views

```
R1# show parser view
No view is active ! Currently in Privilege Level Context
R1#
R1# enable view
Password:
*Mar  1 10:38:56.233: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1#
R1# show parser view
Current view is 'root'
R1#
R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 SUPPORT *
 USER *
 JR-ADMIN *
 ADMIN *
-------(*) represent superview-------
R1#
```

2.3 Monitoring and Managing Devices

Cisco | Networking Academy®
Mind Wide Open™

Cisco IOS Resilient Configuration Feature

Cisco IOS Resilient Configuration Facts

- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.

- To secure the IOS image and enable Cisco IOS image resilience, use the **`secure boot-image`** command.
- To take a snapshot of the router running configuration and securely archive it in persistent storage, use the **`secure boot-config`** global configuration mode command.

Restoring a Primary Bootset Image

Secured files do not appear in the output of a **dir** command. Use the **show secure bootset** command to verify the existence of the archive.

To restore a primary bootset from a secure archive after the router has been tampered with, follow these steps:

Step 1. Reload the router using the **reload** command.

Step 2. From ROMmon mode, enter the **dir** command to list the contents of the device that contains the secure bootset file. From the CLI, the device name can be found in the output of the **show secure bootset** command.

Step 3. Boot the router with the secure bootset image using the **boot** command with the filename found in Step 2. When the compromised router boots, change to privileged EXEC mode and restore the configuration.

Step 4. Enter global configuration mode.

Step 5. Restore the secure configuration to the supplied filename using the **secure boot-config restore** *filename* command.

Recovering a Router Password

Procedure to recover the router password.

- Connect to the console port.
- Record the configuration register setting
- Power cycle the router.
- Issue the break sequence.
- Type **`confreg 0x2142`** to change the register settings.
- Type **`reset`** to reboot router.
- Skip the initial setup procedure.
- Enter privileged EXEC mode.
- Copy the startup configuration to the running configuration.
- Verify the running configuration.
- Enter global configuration and change enable secret password.
- Re-enable the shutdown interfaces.
- Change the configuration register settings using **`config-register 0x2102`**
- Save the configuration changes and reboot.

Disabling Password Recovery

An administrator can mitigate this potential security breach by using the **no service password-recovery** global configuration mode command.

```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery
 mechanism.
Do not execute this command without another plan for
 password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)#
```

To recover a device after entering the **no service password-recovery** command:

Step 1. Initiate the break sequence within five seconds after the image decompresses during the boot.

Step 2. Confirm the break key action.

The startup configuration is completely erased and the password recovery procedure is enabled.

Managing and Monitoring Network Devices

Consider these factors when implementing secure management and syslog:

Syslog questions:

- What are the most important logs?
- How are important messages separated from routine notifications?
- How do you prevent tampering with logs?
- How do you ensure the time stamps match?
- What log data is needed in criminal investigations?
- How do you deal with the volume of messages?
- How do you manage all of the devices?
- How can you track when attacks or network failures occur?

In-Band and Out-of-Band Access

When logging and managing information, the information flow between management hosts and the managed devices can take two paths:

- **In-band** - Information flows across an enterprise production network, the Internet, or both, using regular data channels.

In-Band Management Guidelines:

- Apply only to devices that need to be managed or monitored.
- Use IPsec, SSH, or SSL when possible.
- Decide whether the management channel needs to be open at all times.

- **Out-of-band (OOB)** - Information flows on a dedicated management network on which no production traffic resides.

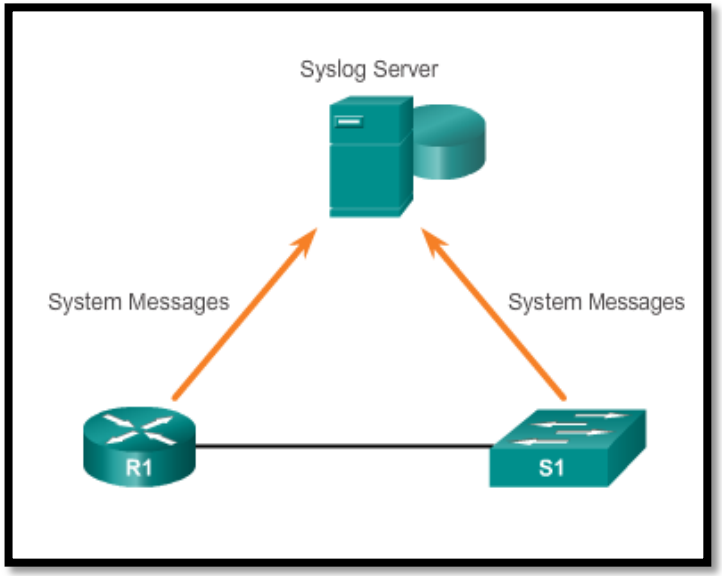
OOB Management Guidelines:

- Provide the highest level of security and mitigate the risk of passing insecure management protocols over the production network.

Introduction to Syslog

The syslog logging service provides three primary functions:

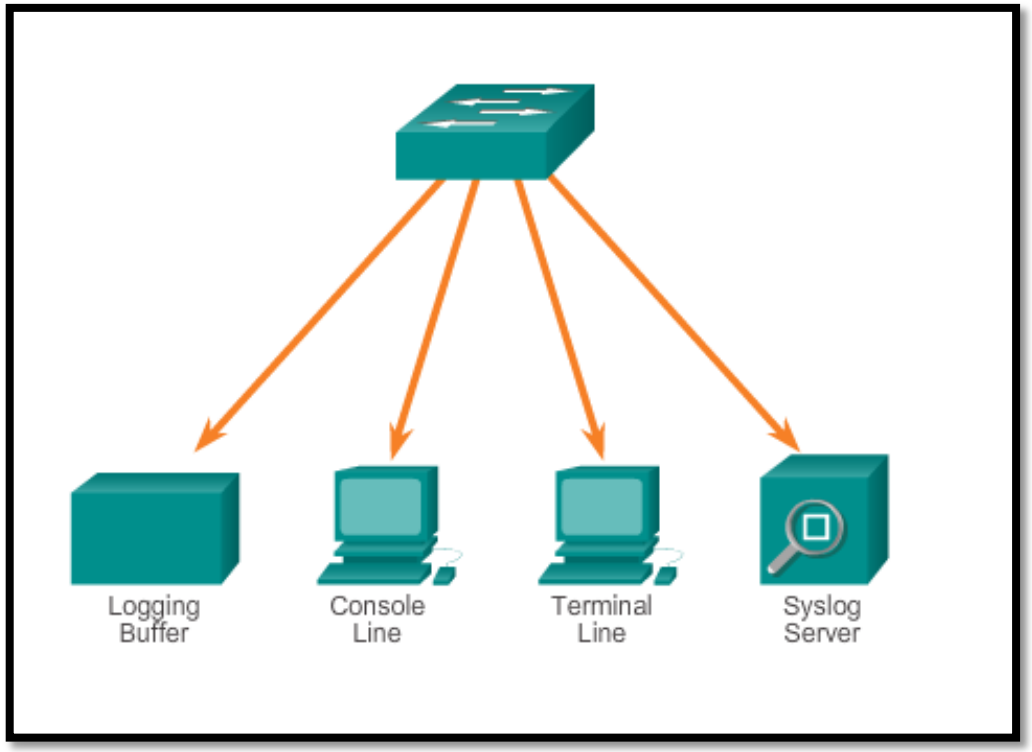
- The ability to gather logging information for monitoring and troubleshooting
- The ability to select the type of logging information that is captured
- The ability to specify the destinations of captured syslog messages



Syslog Operation

Cisco routers can log information regarding configuration changes, ACL violations, interface status, and many other types of events.

The router can be configured to send syslog messages to one or more of the locations in diagram below.



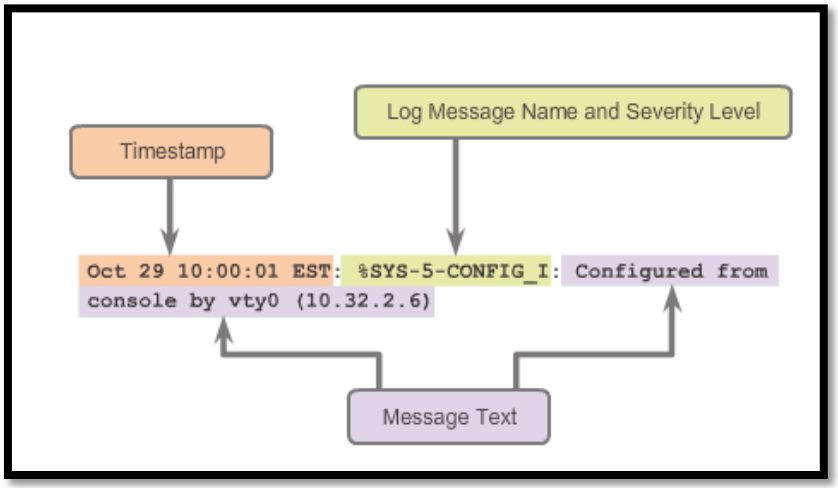
Syslog Operation Cont.

Cisco devices produce syslog messages as a result of network events.

Security Levels

	Level	Keyword	Description	Definition
Highest Level	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	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

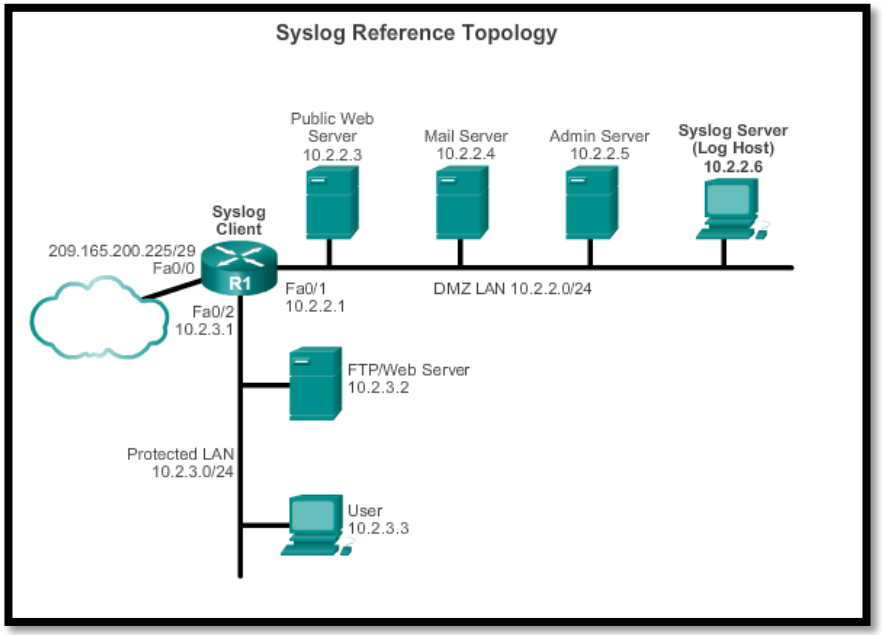
Level 5 Syslog Message



Syslog Systems

Syslog implementations always contain two types of systems:

- **Syslog servers** - Also known as log hosts, these systems accept and process log messages from syslog clients.
- **Syslog clients** - Routers or other types of equipment that generate and forward log messages to syslog servers.



Configuring System Logging

Step 1. Set the destination logging host using the **`logging host`** command.

Step 2. (Optional) Set the log severity (trap) level using the **`logging trap`** *level* command.

Step 3. Set the source interface using the **`logging source-interface`** command. This command specifies that syslog packets contain the IPv4 or IPv6 address of a specific interface, regardless of which interface the packet uses to exit the router.

Step 4. Enable logging with the **`logging on`** command. Logging can be turned on and off for these destinations individually using the **`logging buffered`**, **`logging monitor`**, and **`logging`** global configuration mode commands. However, if the **`logging con`** command is disabled, no messages are sent to these destinations. Only the console receives messages.

Configuring Syslog Using CCP

Step 1. On the Cisco Configuration Professional menu bar, click **Configure > Router > Logging**.

Step 2. On the Logging dialog box, click **Edit.**

Step 3. Click the **Enable Logging Level** check box and select the logging level from the **Logging Level** drop-down list. Messages will be logged for the level selected and below.

Step 4. Click **Add** and enter an IP address of a logging host in the **IP Address/Hostname** field.

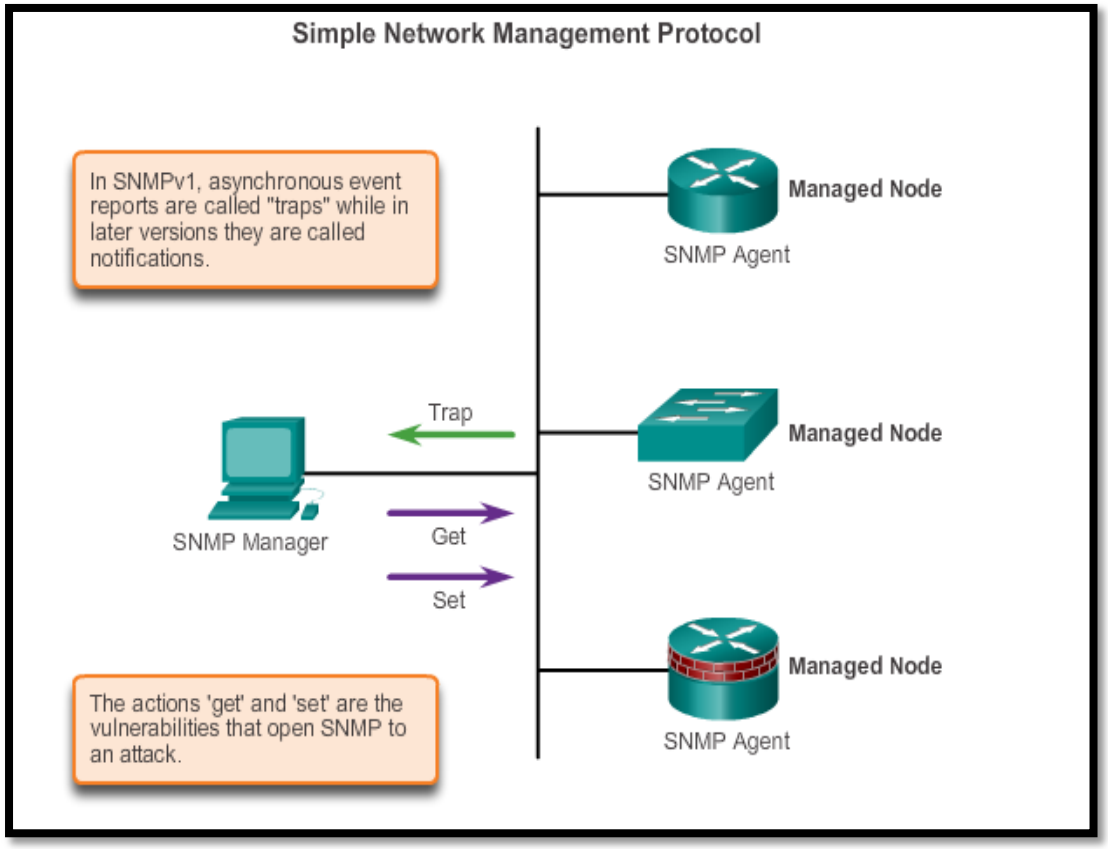
Step 5. Click **OK** to return to the Logging dialog box.

Step 6. Click **OK** to accept the changes and return to the Logging pane.

Introduction to SNMP

The SNMP system consists of three elements:

- SNMP manager
- SNMP agents (managed node)
- Management Information Base (MIB)



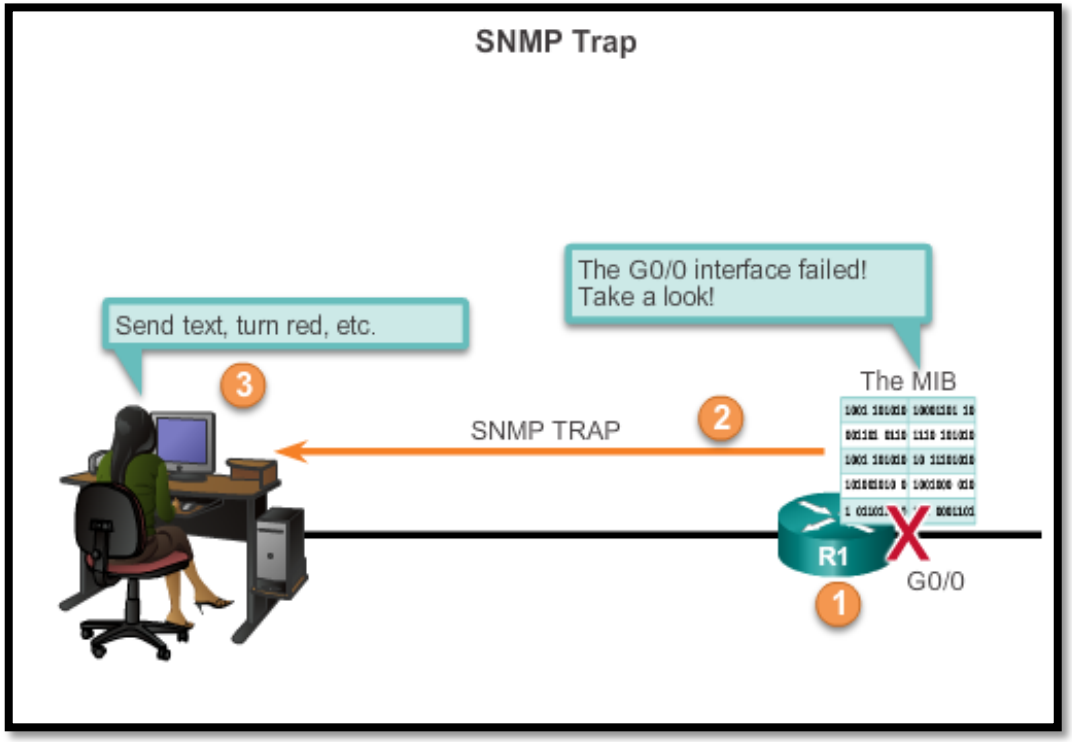
SNMP Operation

- SNMP agents that reside on managed devices collect and store information about the device and its operation.
- This information is stored by the agent locally in the MIB.
- The SNMP manager then uses the SNMP agent to access information within the MIB.

Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request` sent by an NMS.
`set-request`	Stores a value in a specific variable.

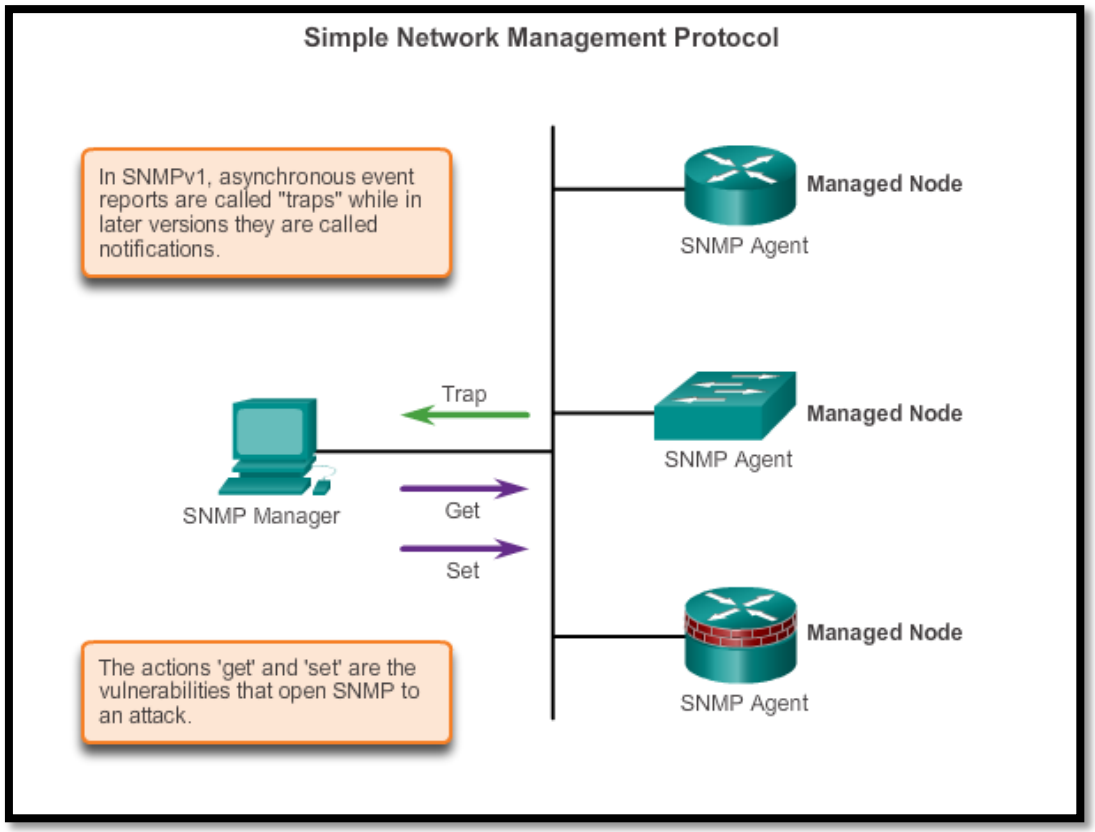
SNMP Agent Traps

- SNMP agents can generate and send traps to inform the NMS immediately of certain events.
- Traps are unsolicited messages alerting the SNMP manager to a condition or event on the network.



SNMP Vulnerabilities

The get and set actions create vulnerabilities that open SNMP to attack.



SNMP Community Strings

Community Strings Facts

- Community strings are used to authenticate messages between a management station and an SNMPv1 or SNMPv2 engine.
- Read-write community strings can get and set information in an agent.
- Set access is equivalent to having the enable password for a device.

There are two types of community strings:

- **Read-only community strings** - Provides read-only access to all objects in the MIB, except the community strings.
- **Read-write community strings** - Provides read-write access to all objects in the MIB, except the community strings.

SNMPv3

SNMPv3 provides the following security features:

- **Message integrity and authentication** - Ensures that a packet has not been tampered with in transit and is from a valid source.
- **Encryption** - Scrambles the contents of a packet to prevent it from being seen by an unauthorized source.
- **Access Control** - Restricts each principal to certain actions on specific portions of data.

Enabling SNMP Using CCP

Step 1. On the Cisco Configuration Professional menu bar, click **Configure > Router > SNMP**.

Step 2. On the SNMP Properties dialog box, click **Edit**.

Step 3. On the SNMP Properties dialog box, click the **Enable SNMP** check box to enable SNMP support.

Step 4. Set community strings and enter trap manager information from the same SNMP Properties window used to enable support.

Step 5. On the SNMP Properties dialog box, click **Add** to create new community strings click **Edit** to edit an existing community q string, or click **Delete** to delete a community string.

Setting SNMP Traps Using CCP

To add, edit, or delete a trap receiver use the following steps:

Step 1. From the SNMP pane in CCP, click **Edit**.

Step 2. On the SNMP Properties window > Trap Receiver section~~of~~, click **Add** to add a new trap receiver.

Step 3. On the Add a Trap Receiver window, enter the IP address or hostname of the trap receiver and the password used to connect to the trap receiver. Typically, this is the IP address of the SNMP management station that monitors the domain.

Step 4. Click **OK**.

Step 5. To edit an existing trap receiver, choose a trap receiver from the trap receiver list and click **Edit**. To delete an existing trap receiver, choose a trap receiver from the trap receiver list and click **Delete**.

Step 6. When the trap receiver list is complete, click **OK** to return to the SNMP pane.

Network Time Protocol

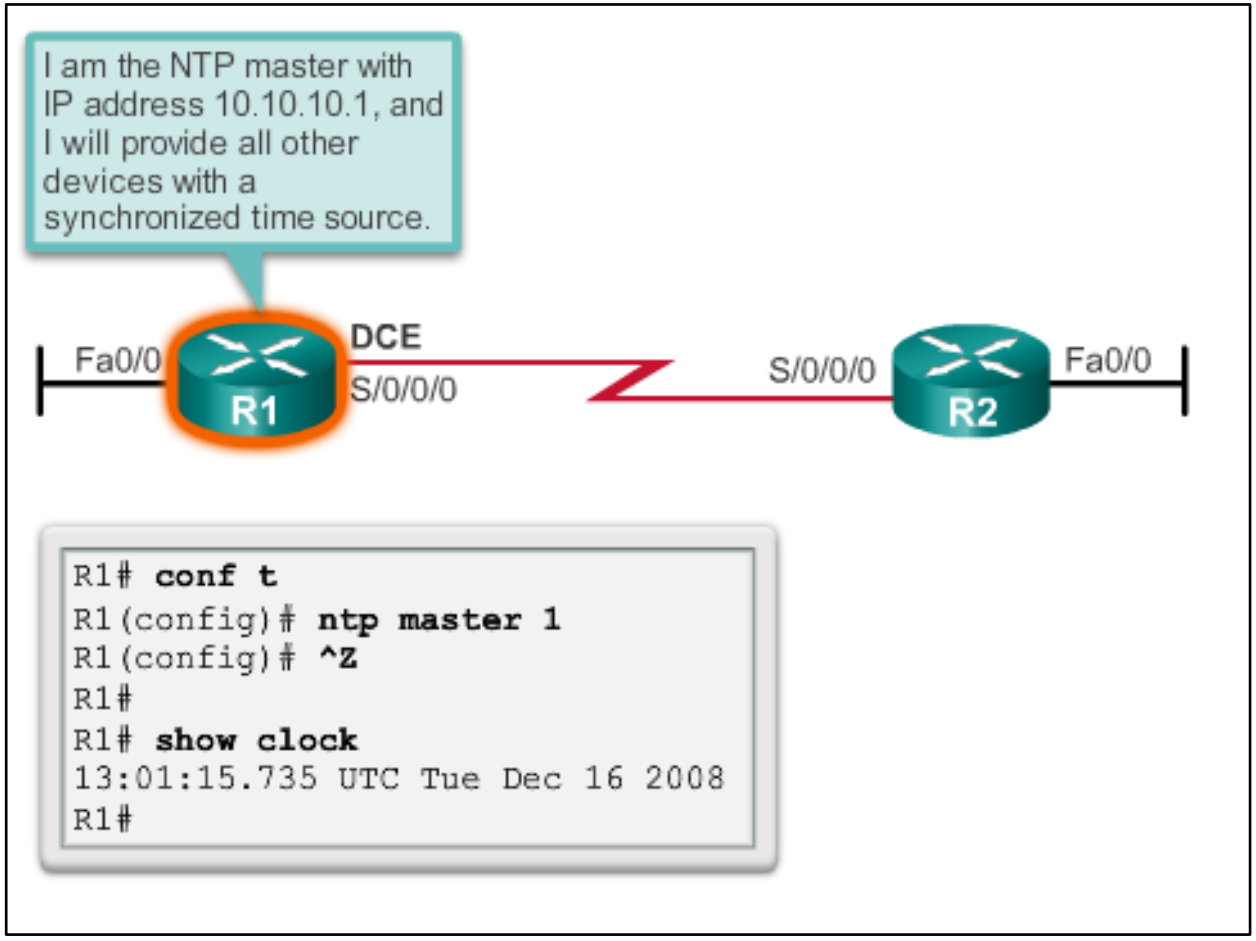
- The date and time settings of the router can be set using one of two methods:
  - Manually editing the date and time.
  - Configuring the Network Time Protocol (NTP).
- NTP is designed to time-synchronize a network. NTP runs over UDP.
- An NTP network usually obtains the time from an authoritative 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 1ms of one another
- 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.

Network Time Protocol Cont.

- In a NTP configured network, one or more routers are designated as the master clock keeper, also known as an NTP master, using the **ntp master** global configuration mode command.
- NTP clients either contact the master or listen for messages from the master to synchronize their clocks. To contact the master, use the **ntp server** *ip-address* command.
- In a LAN environment, NTP can be configured to use IP broadcast messages instead by using the **ntp broadcast client** interface configuration mode command.

NTP Server

Sample NTP Configuration



NTP Authentication

There are two security mechanisms available:

- ACL-based restriction scheme
- Encrypted authentication mechanism offered by NTP version 3 or later

It is strongly recommended that NTP version 3 or later is implemented. Use the following commands on both the NTP master and the NTP client:

- **ntp authenticate ntp authentication-key** *key-number*
- **md5** *key-value*
- **ntp trusted-key** *key-number*


```
R1# conf t
R1(config)# ntp authenticate
R1(config)# ntp authentication-key 1 md5 cisco123
R1(config)# ntp trusted-key 1
R1(config)# ^Z
```

Enabling NTP Using CCP

Step 1. On the Cisco Configuration Protocol menu bar, click **Configure > Router > Time > NTP and SNTP.**

Step 2. The NTP pane appears, displaying the information for all configured NTP servers. To add a new NTP server, click **Add.**

Step 3. On the Add NTP Server Details dialog box, add an NTP server by name (if the router is configured to use a DNS server) or by IP address. To add by IP address, enter the IP address in the field next to the **NTP Server IP Address** option.

Step 4. (Optional) From the **NTP Source Interface** drop-down list, select the interface that the router uses to communicate with the NTP server. If left blank, NTP messages are sent out from the closest interface per the routing table.

Step 5. Click the **Prefer** check box if this NTP server has been designated as a preferred NTP server.

Step 6. Click the **Authentication Key** check box and enter the key number and key value if the NTP server uses authentication.

Step 7. Click **OK** to finish adding the server.

2.4 Using Automated Security Features

Cisco | Networking Academy®
Mind Wide Open™

Cisco Discovery Protocol

- The Cisco Discovery Protocol (CDP) is an example of a service that is enabled by default on Cisco routers.
- The intent of CDP is to make it easier for administrators to discover and troubleshoot other Cisco devices on the network.
- An attacker on the network can use CDP to discover devices on the local network.
- Readily available software, such as the Cisco CDP Monitor, can be downloaded to gain the CDP information.
- Because of the security implications, CDP should be used with caution.
- Edge devices are an example of a device that should have this CDP disabled.

Protocols and Services Default Settings

Disabling and restricting the following components helps ensure that a device is secure:

- Unnecessary services and interfaces
- Commonly configured management services, such as SNMP
- Probes and scans, such as ICMP. Ensure terminal access security
- Gratuitous and proxy Address Resolution Protocol (ARP)
- IP-directed broadcasts

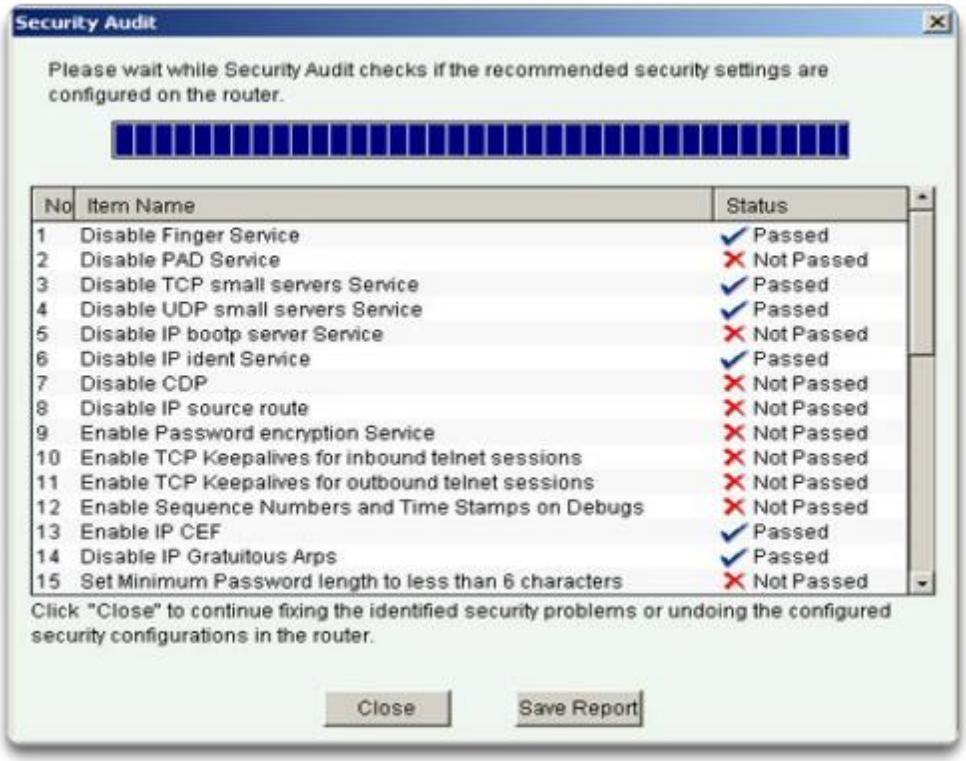
Cisco IOS Security Tools

The three security audit tools that are available:

- **Security Audit wizard** - A security audit feature provided through CCP. Provides a list of vulnerabilities and allows the administrator to choose which potential security-related configuration changes to implement on a router.
- **Cisco AutoSecure** - A security audit feature available through the Cisco IOS CLI. The **auto secure** command initiates a security audit and then allows for configuration changes. Based on the mode selected, configuration changes can be automatic or require network administrator input.
- **One-Step Lockdown** - A security audit feature provided through CCP. Provides a list of vulnerabilities and then automatically makes all recommended security-related configuration changes.

CCP Security Audit Wizard

The Security Audit wizard tests to determine if any potential security problems exist in the router configuration, and then presents a screen that lets the administrator determine which of those security problems to fix.



Cisco AutoSecure

The Cisco AutoSecure feature is initiated from the CLI and executes a script. It first makes recommendations for fixing security vulnerabilities, and then modifies the security configuration of the router.

```
R1# 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]:yes
```

Using the Cisco AutoSecure Feature

Use the **auto secure** command to enable the Cisco AutoSecure feature setup. This setup can be interactive or non-interactive.

- In interactive mode (the default), the router prompts with options to enable and disable services and other security features.
- The non-interactive mode automatically executes the Cisco AutoSecure command with the recommended Cisco default settings. Enable this mode using the **auto secure no-interact** command.

Using the Cisco AutoSecure Feature Cont.

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

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.

Cisco AutoSecure vs. CCP One-Step Lockdown

- CCP One-Step Lockdown tests a router configuration for any potential security problems and automatically makes the necessary configuration changes to correct any problems.
- CCP does not implement all the features of Cisco AutoSecure.
  - CCP does not support disabling NTP.
  - CCP does not support AAA configuration.
  - CCP does not set SPD values.
  - CCP does not enable TCP intercepts.
  - CCP does not configure anti-spoofing ACLs.
  - CCP enables and configures SSH on Cisco IOS images that have the IPsec feature set. However, unlike Cisco AutoSecure, CCP does not enable Secure Copy Protocol (SCP) or disable other access and file transfer services, such as FTP.
  - CCP disables SNMP. However, unlike Cisco AutoSecure, CCP does not provide an option for configuring SNMPv3.

Summary

- When securing a network device, hardening should be the first step, which includes:
  - Securing the network perimeter.
  - Securing administrative access to infrastructure devices.
  - Enhancing virtual login security.
  - Using secure protocols like SSH, instead of Telnet, and HTTPS instead of HTTP.
- Administrators should provide access to infrastructure devices based on privilege levels and implement a role-based CLI.
- IOS images and configuration files should also be protected using the Cisco IOS resilient configuration feature.
- Network monitoring should be implemented, including configuring Syslog, SNMP, and NTP.
- Administrators must routinely perform security audits to identify all services, interfaces, and management services that are vulnerable to network attacks.
- Administrators should use the CCP One-Step Lockdown feature or the IOS CLI **`auto secure`** command before deploying new devices into a production environment.