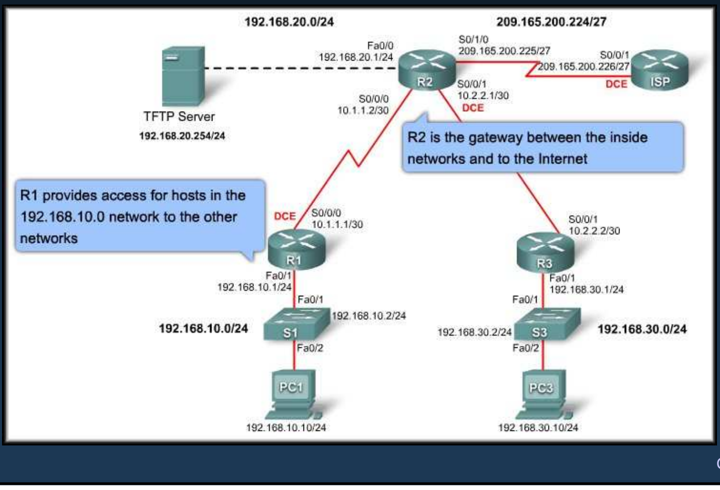
# Chapter 4

## Network Security

## Part II

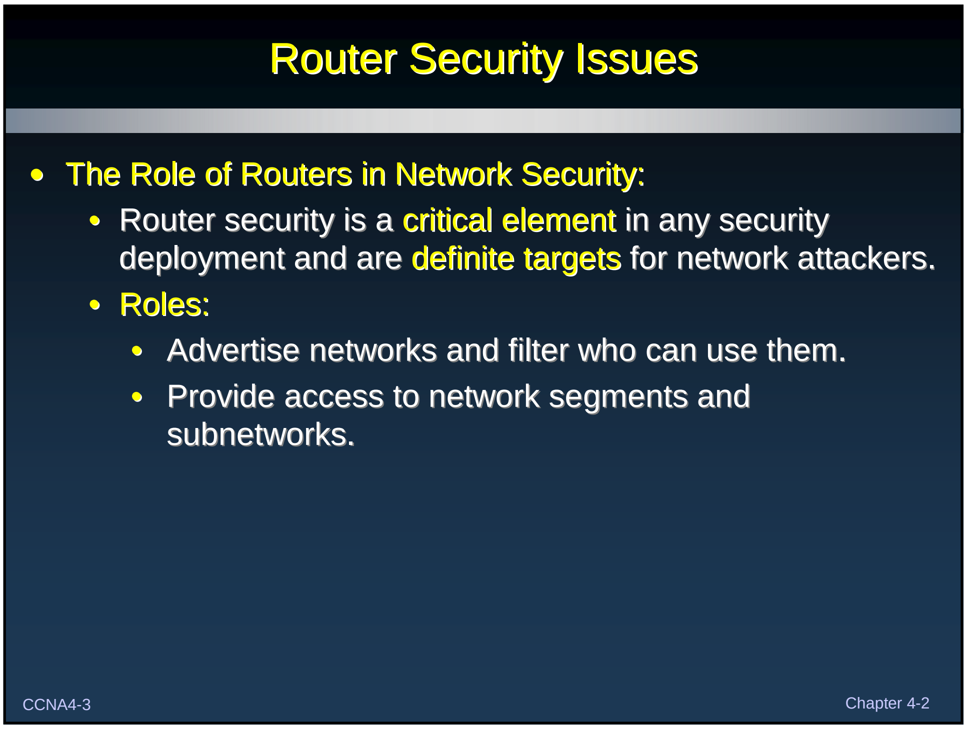
## Introducing Network Security

### Securing Cisco Routers



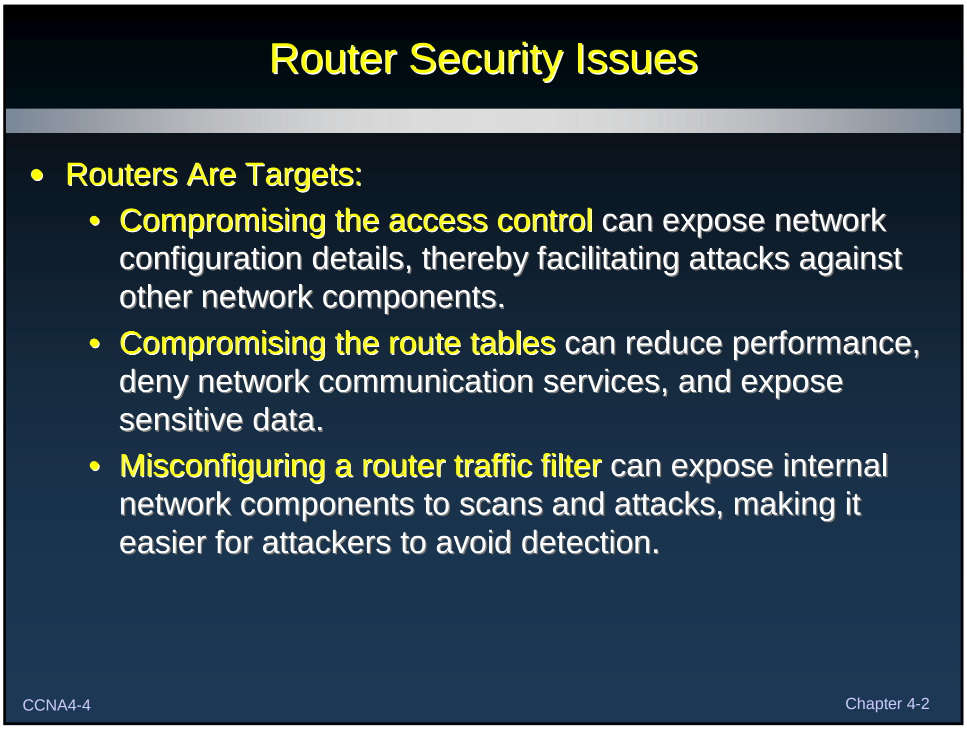
R2 is the gateway between the inside networks and to the Internet

R1 provides access for hosts in the 192.168.10.0 network to the other networks



## Router Security Issues

- The Role of Routers in Network Security:
  - Router security is a critical element in any security deployment and are definite targets for network attackers.
  - Roles:
    - Advertise networks and filter who can use them.
    - Provide access to network segments and subnetworks.

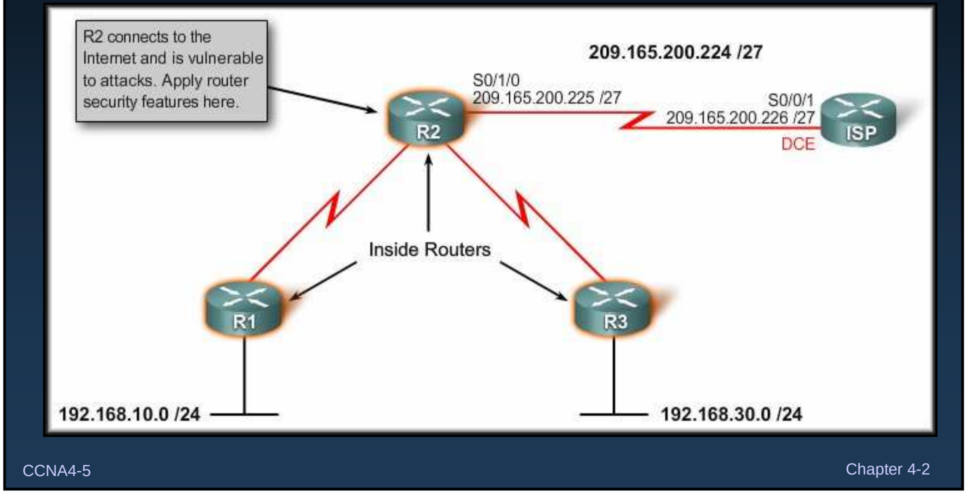


## Router Security Issues

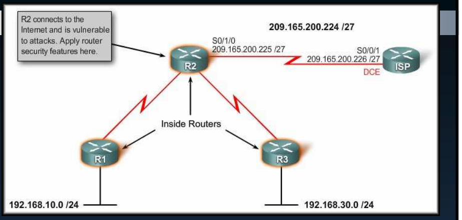
- Routers Are Targets:
  - Compromising the access control can expose network configuration details, thereby facilitating attacks against other network components.
  - Compromising the route tables can reduce performance, deny network communication services, and expose sensitive data.
  - Misconfiguring a router traffic filter can expose internal network components to scans and attacks, making it easier for attackers to avoid detection.

# Router Security Issues

- Securing routers at the network perimeter is an important first step in securing the network.

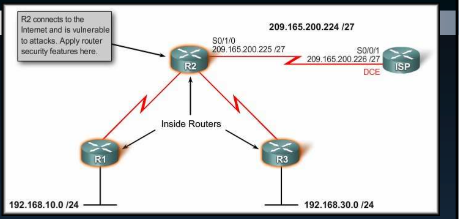


# Router Security Issues



- Securing Your Network:
  - Physical:
    - Locate the router in a locked room that is accessible only to authorized personnel.
    - UPS.
  - Update the router IOS:
    - Note that the latest version of an operating system may not be the most stable version available.
    - Use the latest, stable release that meets the feature requirements of your network.

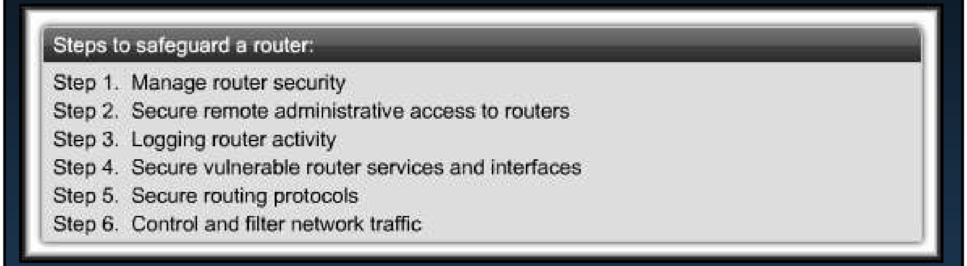
# Router Security Issues



- Securing Your Network:
  - Configuration and IOS:
    - Keep a secure copy of the router IOS and router configuration file on a TFTP server for backup purposes.
  - Unused Services:
    - A router has many services enabled by default.
    - Harden your router configuration by disabling unnecessary services and unused ports.

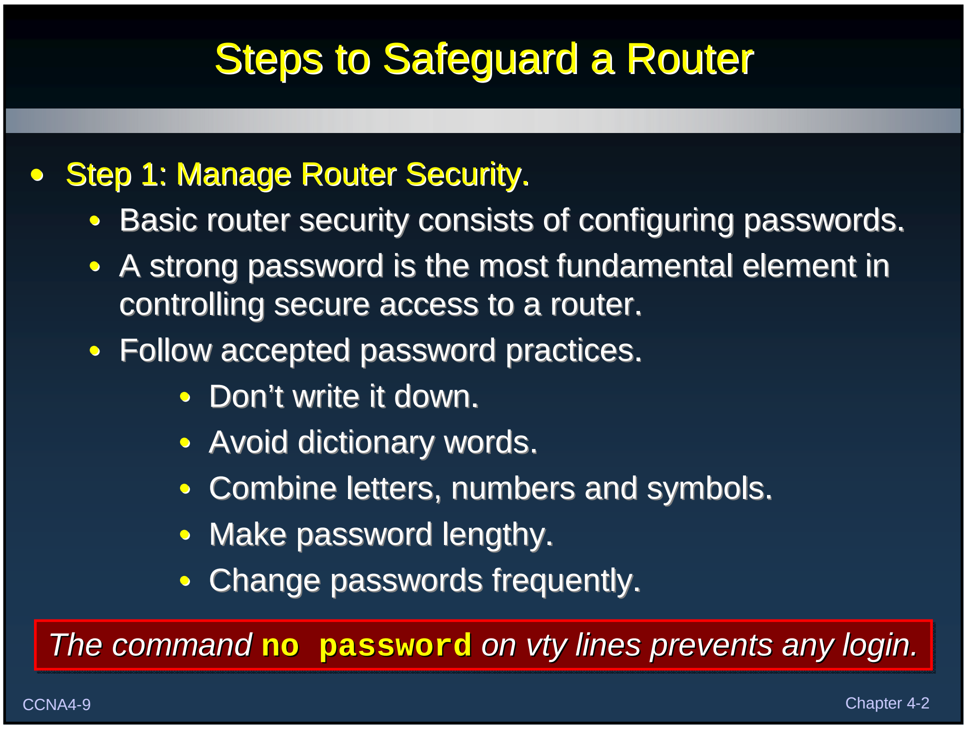
# Applying Cisco IOS Security Features

- Steps to safeguard a router:



Steps to safeguard a router:

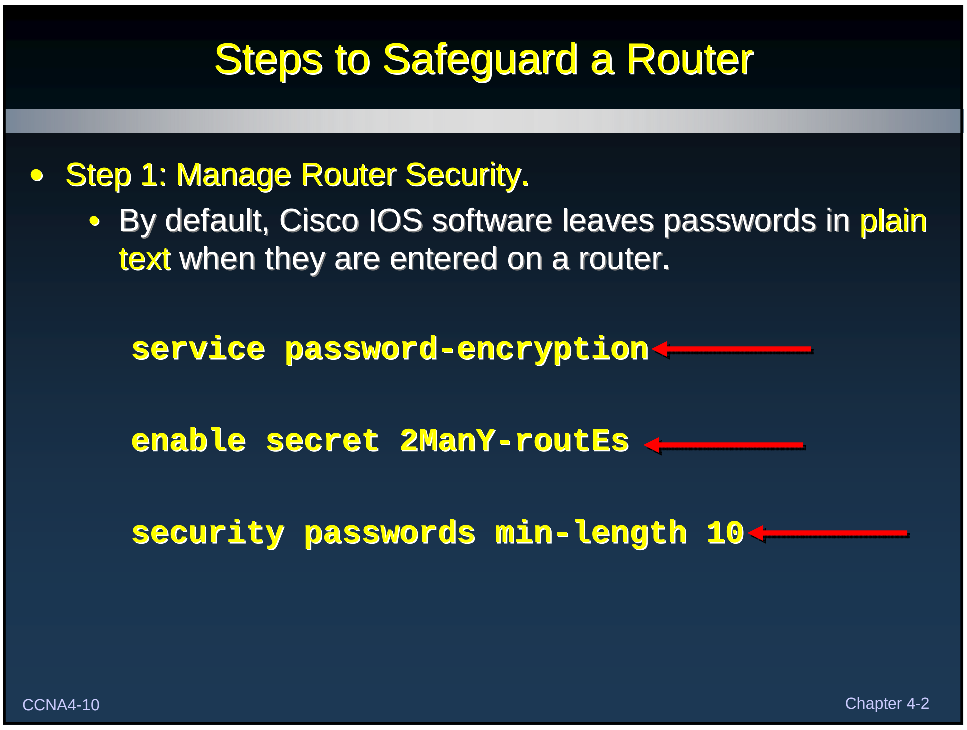
Step 1. Manage router security
Step 2. Secure remote administrative access to routers
Step 3. Logging router activity
Step 4. Secure vulnerable router services and interfaces
Step 5. Secure routing protocols
Step 6. Control and filter network traffic



# Steps to Safeguard a Router

- Step 1: Manage Router Security.
  - Basic router security consists of configuring passwords.
  - A strong password is the most fundamental element in controlling secure access to a router.
  - Follow accepted password practices.
    - Don’t write it down.
    - Avoid dictionary words.
    - Combine letters, numbers and symbols.
    - Make password lengthy.
    - Change passwords frequently.

*The command* **`no password`** *on vty lines prevents any login.*



# Steps to Safeguard a Router

- Step 1: Manage Router Security.
  - By default, Cisco IOS software leaves passwords in plain text when they are entered on a router.

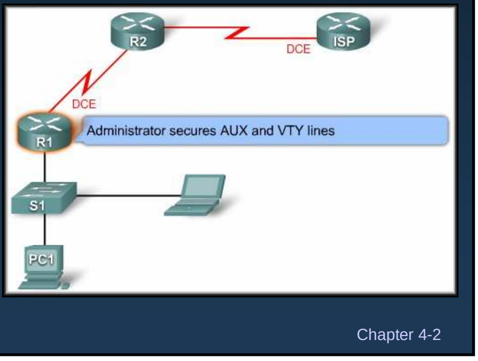
```
service password-encryption

enable secret 2ManY-routEs

security passwords min-length 10
```

## Steps to Safeguard a Router

- Step 2: Secure Remote Administrative Access.
  - Local access through the console port is the preferred way for an administrator to connect to a device to manage it because it is secure.
  - Remote administrative access is more convenient than local access.
  - Using Telnet can be very insecure because all network traffic is in plain text.
  - An attacker could capture network traffic and sniff the administrator passwords or router configuration.

## Steps to Safeguard a Router

- Step 2: Secure Remote Administrative Access.
  - Remote access typically involves allowing Telnet, Secure Shell (SSH), HTTP, HTTP Secure (HTTPS), or SNMP connections to the router from a computer.
  - Establish a dedicated management network.
  - Secure the administrative lines.
  - Encrypt all traffic between the administrator computer and the router.



## Steps to Safeguard a Router

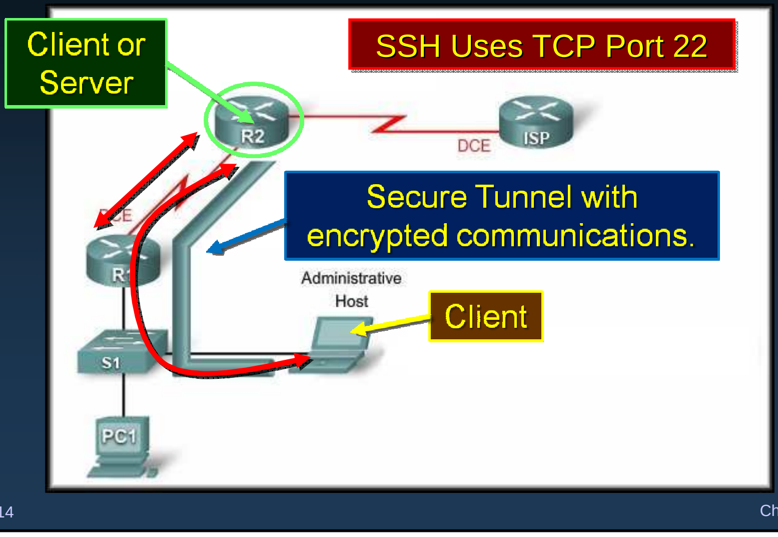
- Step 2: Secure Remote Administrative Access.
  - Logins may be prevented on any line by configuring the router with the login and no password commands.
  - VTY lines should be configured to accept connections only with the protocols actually needed.

    **`transport input telnet`** – only telnet

    **`transport input telnet ssh`** – telnet or ssh
  - Implement Access Control Lists (ACLs) - Chapter 5.
  - Configure VTY timeouts using the **`exec-timeout`** command.

## Steps to Safeguard a Router

- Step 2: Secure Remote Administrative Access.



Client or Server

SSH Uses TCP Port 22

Secure Tunnel with encrypted communications.

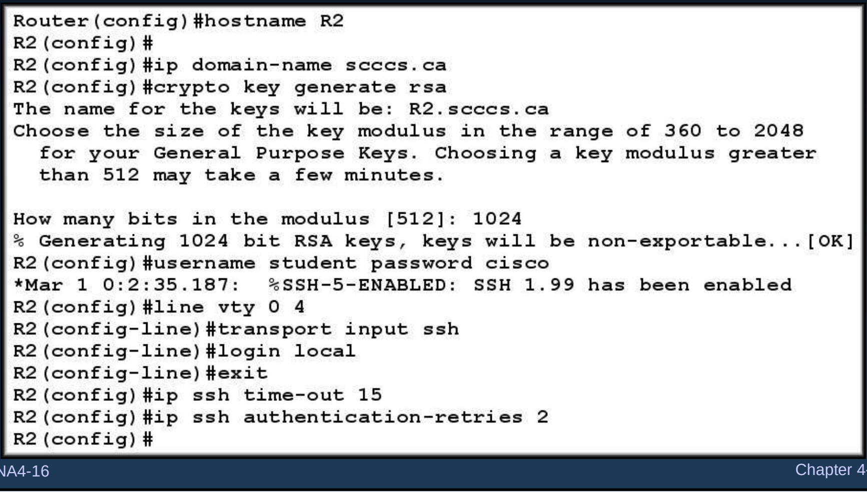
Client

## Configuring SSH Security

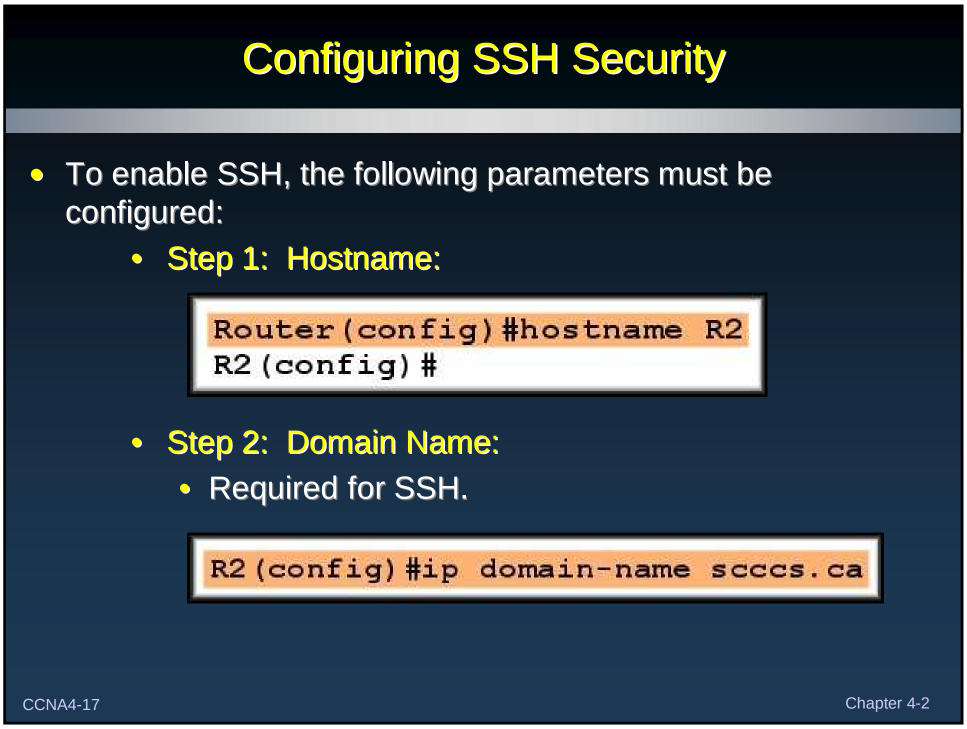
- To enable SSH, the following parameters must be configured:
  - Hostname
  - Domain Name
  - Asymmetrical Keys
  - Local Authentication

## Configuring SSH Security

- To enable SSH, the following parameters must be configured:



```
Router(config)#hostname R2
R2(config)#
R2(config)#ip domain-name scccs.ca
R2(config)#crypto key generate rsa
The name for the keys will be: R2.scccs.ca
Choose the size of the key modulus in the range of 360 to 2048
  for your General Purpose Keys. Choosing a key modulus greater
  than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#username student password cisco
*Mar 1 0:2:35.187:  %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config-line)#exit
R2(config)#ip ssh time-out 15
R2(config)#ip ssh authentication-retries 2
R2(config)#
```



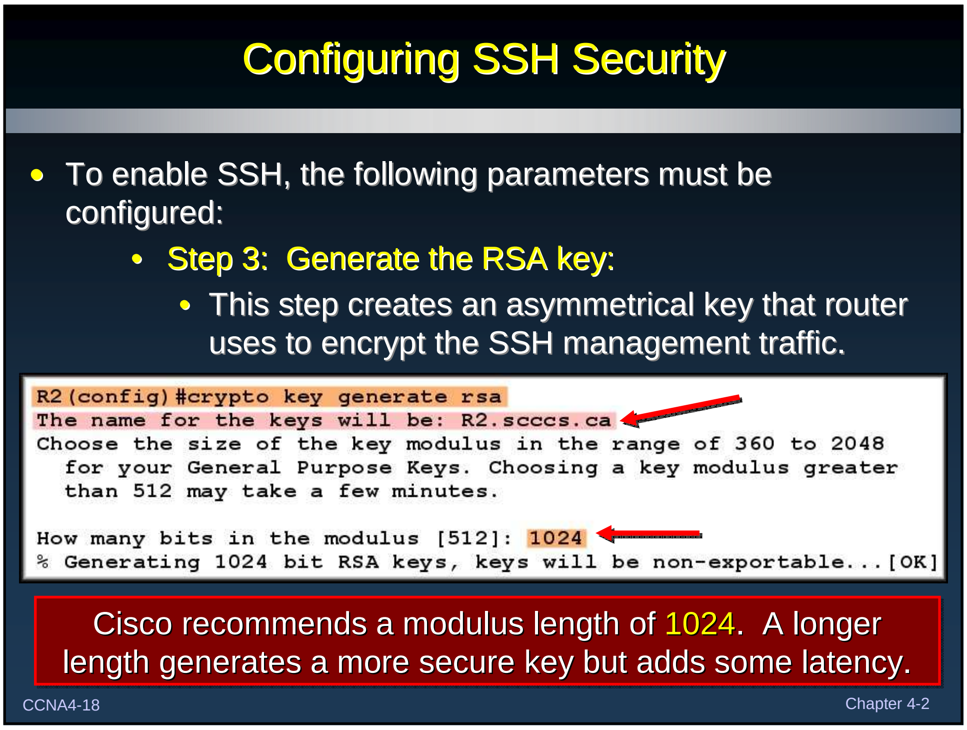
## Configuring SSH Security

- To enable SSH, the following parameters must be configured:
  - Step 1: Hostname:

```
Router(config)#hostname R2
R2(config)#
```

  - Step 2: Domain Name:
    - Required for SSH.

```
R2(config)#ip domain-name scccs.ca
```



## Configuring SSH Security

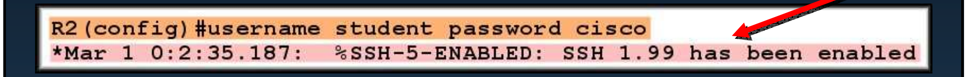
- To enable SSH, the following parameters must be configured:
  - Step 3: Generate the RSA key:
    - This step creates an asymmetrical key that router uses to encrypt the SSH management traffic.

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.scccs.ca
Choose the size of the key modulus in the range of 360 to 2048
  for your General Purpose Keys. Choosing a key modulus greater
  than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Cisco recommends a modulus length of 1024. A longer length generates a more secure key but adds some latency.

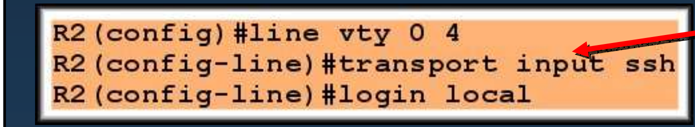
# Configuring SSH Security

- To enable SSH, the following parameters must be configured:
  - Step 4: Configure local authentication and vty:
    - You must define a local user.



```
R2(config)#username student password cisco
*Mar 1 0:2:35.187:  %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- Use the **login local** command to search the local database and assign ssh to the vty lines.

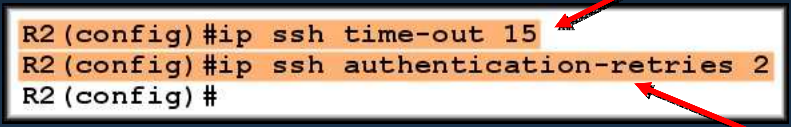


```
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
```

Makes SSH the only method.
NO TELNET

# Configuring SSH Security

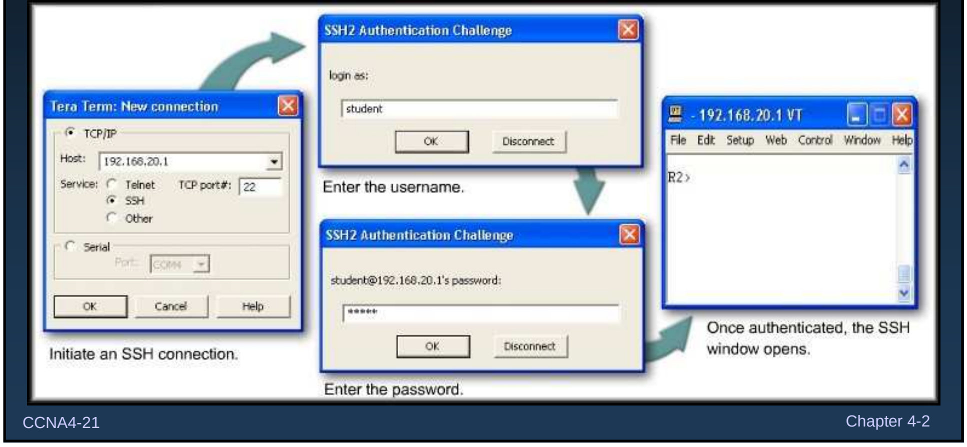
- To enable SSH, the following parameters must be configured:
  - Step 5: Configure SSH timeouts:
    - Not absolutely necessary for SSH but probably a good idea.



```
R2(config)#ip ssh time-out 15
R2(config)#ip ssh authentication-retries 2
R2(config)#
```

## Test SSH Security

- To connect to a router configured with SSH, you have to use an SSH client application such as **PuTTY** or **TeraTerm**.
  - Choose the SSH option and use **TCP port 22**.



Tera Term: New connection

● TCP/IP

Host: 192.168.20.1

Service: ○ Telnet ● SSH ○ Other

TCP port#: 22

○ Serial

Port: COM4

Initiate an SSH connection.

SSH2 Authentication Challenge

login as: student

Enter the username.

SSH2 Authentication Challenge

student@192.168.20.1's password: *****

Enter the password.

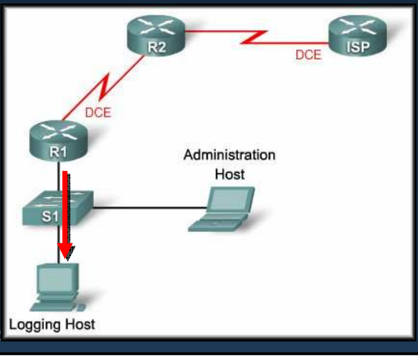
- 192.168.20.1 VT

```
R2>
```

Once authenticated, the SSH window opens.

## Steps to Safeguard a Router

- **Step 3: Log Router Activity.**
  - Logs allow you to verify router is working properly.
  - Routers support **8 levels** of logging.
    - The most important thing to remember about logging is that **logs must be reviewed regularly**.

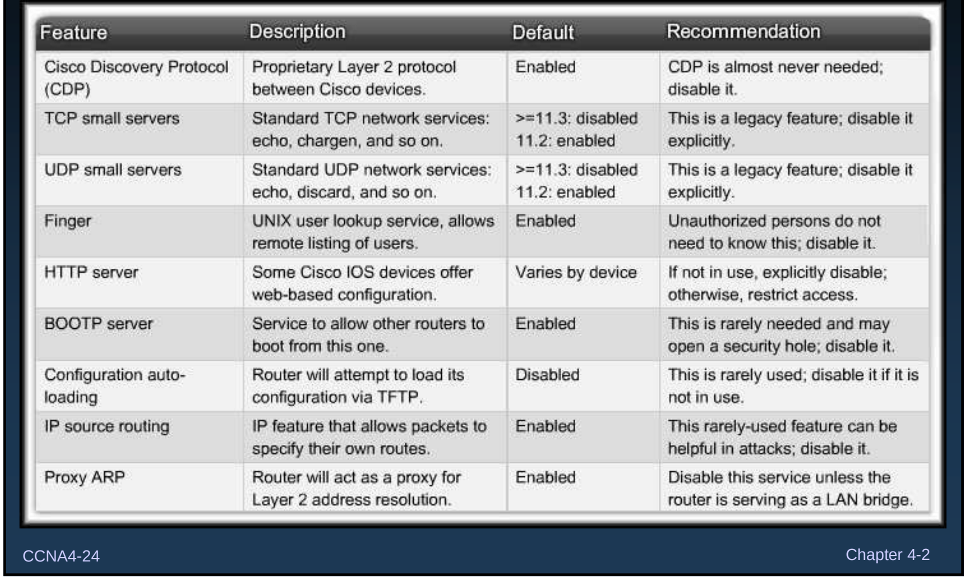


0: Emergencies
1: Alerts
2: Critical
3: Errors
4: Warnings
5: Notification
6: Informational
7: Debugging

## Steps to Safeguard a Router

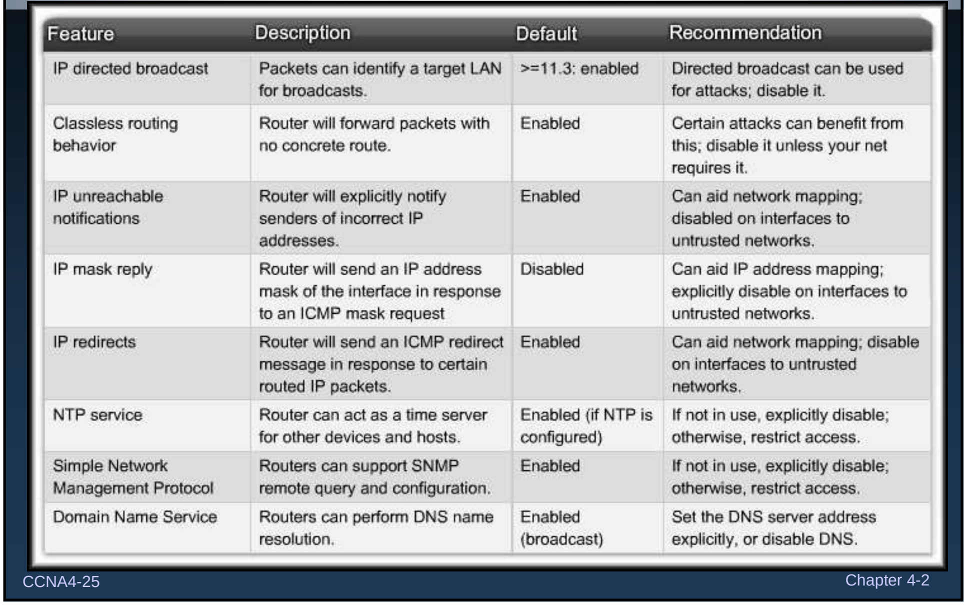
- Step 4: Securing Router Network Services.
  - Cisco routers support a large number of network services at layers 2, 3, 4, and 7.
    - Some of them are application layer protocols.
    - Others are automatic processes and settings intended to support legacy configurations that pose security risks.
  - Some of these services can be restricted or disabled to improve security without degrading the operational use of the router.
    - *Most of the services listed in this section are usually not required.*

## Steps to Safeguard a Router



| Feature | Description | Default | Recommendation |
|---|---|---|---|
| Cisco Discovery Protocol (CDP) | Proprietary Layer 2 protocol between Cisco devices. | Enabled | CDP is almost never needed; disable it. |
| TCP small servers | Standard TCP network services: echo, chargen, and so on. | >=11.3: disabled<br>11.2: enabled | This is a legacy feature; disable it explicitly. |
| UDP small servers | Standard UDP network services: echo, discard, and so on. | >=11.3: disabled<br>11.2: enabled | This is a legacy feature; disable it explicitly. |
| Finger | UNIX user lookup service, allows remote listing of users. | Enabled | Unauthorized persons do not need to know this; disable it. |
| HTTP server | Some Cisco IOS devices offer web-based configuration. | Varies by device | If not in use, explicitly disable; otherwise, restrict access. |
| BOOTP server | Service to allow other routers to boot from this one. | Enabled | This is rarely needed and may open a security hole; disable it. |
| Configuration auto-loading | Router will attempt to load its configuration via TFTP. | Disabled | This is rarely used; disable it if it is not in use. |
| IP source routing | IP feature that allows packets to specify their own routes. | Enabled | This rarely-used feature can be helpful in attacks; disable it. |
| Proxy ARP | Router will act as a proxy for Layer 2 address resolution. | Enabled | Disable this service unless the router is serving as a LAN bridge. |

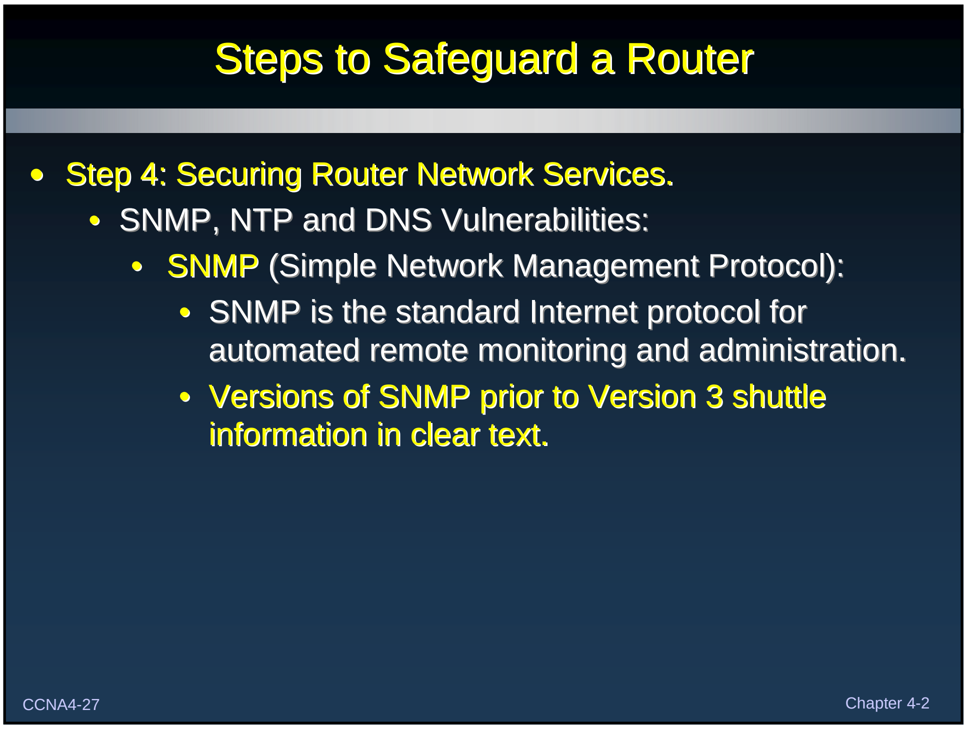
## Steps to Safeguard a Router



| Feature | Description | Default | Recommendation |
|---|---|---|---|
| IP directed broadcast | Packets can identify a target LAN for broadcasts. | >=11.3: enabled | Directed broadcast can be used for attacks; disable it. |
| Classless routing behavior | Router will forward packets with no concrete route. | Enabled | Certain attacks can benefit from this; disable it unless your net requires it. |
| IP unreachable notifications | Router will explicitly notify senders of incorrect IP addresses. | Enabled | Can aid network mapping; disabled on interfaces to untrusted networks. |
| IP mask reply | Router will send an IP address mask of the interface in response to an ICMP mask request | Disabled | Can aid IP address mapping; explicitly disable on interfaces to untrusted networks. |
| IP redirects | Router will send an ICMP redirect message in response to certain routed IP packets. | Enabled | Can aid network mapping; disable on interfaces to untrusted networks. |
| NTP service | Router can act as a time server for other devices and hosts. | Enabled (if NTP is configured) | If not in use, explicitly disable; otherwise, restrict access. |
| Simple Network Management Protocol | Routers can support SNMP remote query and configuration. | Enabled | If not in use, explicitly disable; otherwise, restrict access. |
| Domain Name Service | Routers can perform DNS name resolution. | Enabled (broadcast) | Set the DNS server address explicitly, or disable DNS. |

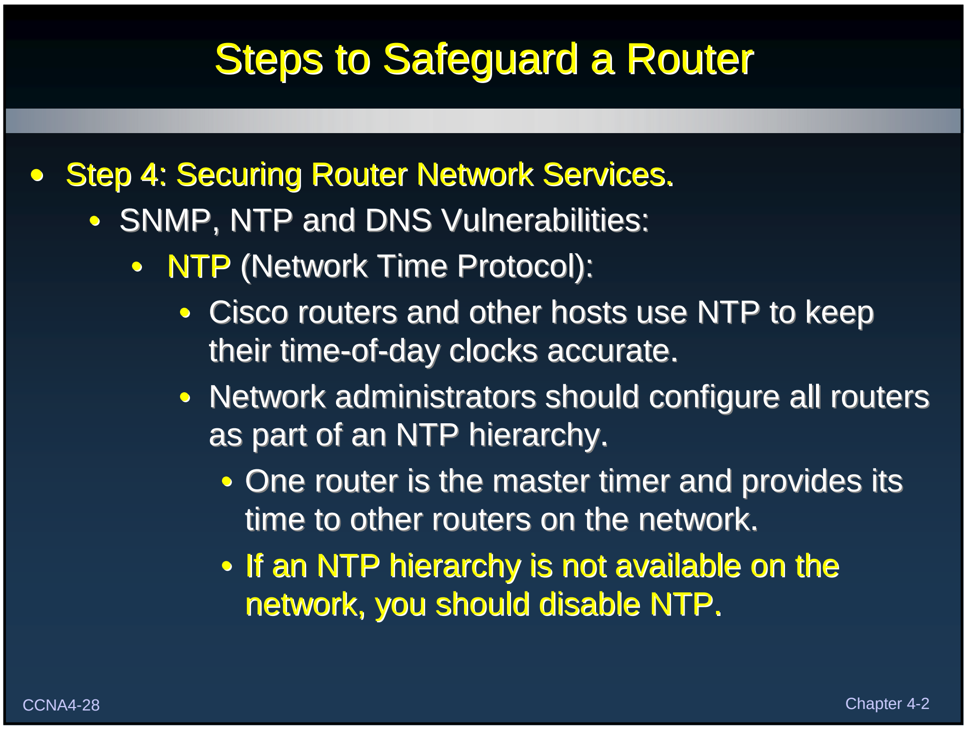
## Steps to Safeguard a Router

- Step 4: Securing Router Network Services.
  - Turning off a service on the router itself does not mean that the service or protocol cannot be used on the network.
    - For example:
      - TFTP (Trivial File Transfer Protocol)
      - DHCP (Dynamic Host Configuration Protocol)
  - Turning off an automatic network feature usually prevents a certain type of network traffic.
    - For example:
      - IP Source Routing is rarely used but can be used in network attacks.



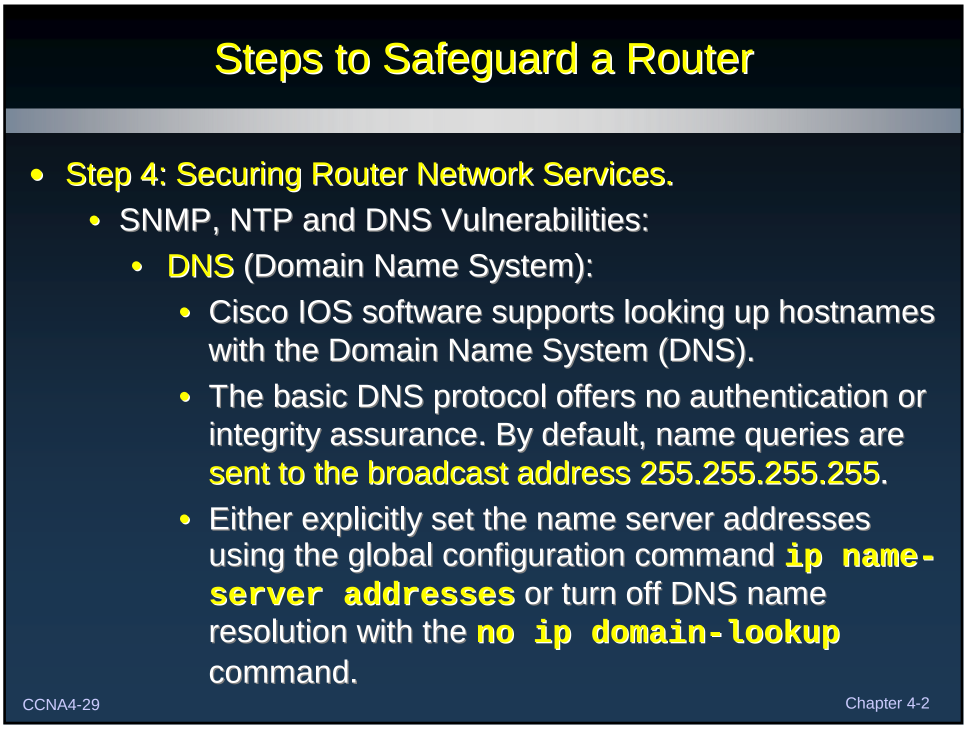
## Steps to Safeguard a Router

- Step 4: Securing Router Network Services.
  - SNMP, NTP and DNS Vulnerabilities:
    - SNMP (Simple Network Management Protocol):
      - SNMP is the standard Internet protocol for automated remote monitoring and administration.
      - Versions of SNMP prior to Version 3 shuttle information in clear text.



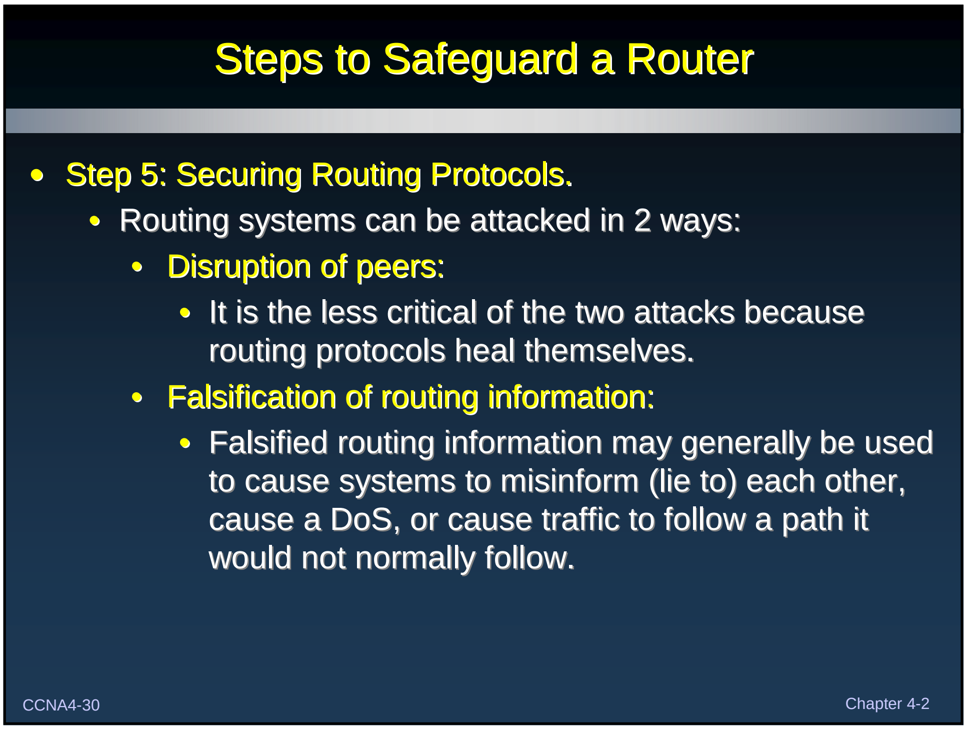
## Steps to Safeguard a Router

- Step 4: Securing Router Network Services.
  - SNMP, NTP and DNS Vulnerabilities:
    - NTP (Network Time Protocol):
      - Cisco routers and other hosts use NTP to keep their time-of-day clocks accurate.
      - Network administrators should configure all routers as part of an NTP hierarchy.
        - One router is the master timer and provides its time to other routers on the network.
        - If an NTP hierarchy is not available on the network, you should disable NTP.



## Steps to Safeguard a Router

- Step 4: Securing Router Network Services.
  - SNMP, NTP and DNS Vulnerabilities:
    - DNS (Domain Name System):
      - Cisco IOS software supports looking up hostnames with the Domain Name System (DNS).
      - The basic DNS protocol offers no authentication or integrity assurance. By default, name queries are sent to the broadcast address 255.255.255.255.
      - Either explicitly set the name server addresses using the global configuration command **`ip name-server addresses`** or turn off DNS name resolution with the **`no ip domain-lookup`** command.

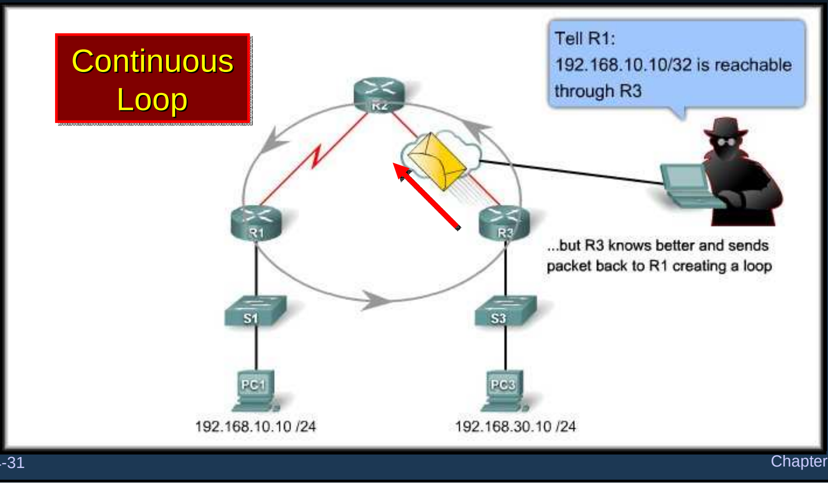


## Steps to Safeguard a Router

- Step 5: Securing Routing Protocols.
  - Routing systems can be attacked in 2 ways:
    - Disruption of peers:
      - It is the less critical of the two attacks because routing protocols heal themselves.
    - Falsification of routing information:
      - Falsified routing information may generally be used to cause systems to misinform (lie to) each other, cause a DoS, or cause traffic to follow a path it would not normally follow.

# Steps to Safeguard a Router

- Step 5: Securing Routing Protocols.
    - Falsification of routing information:

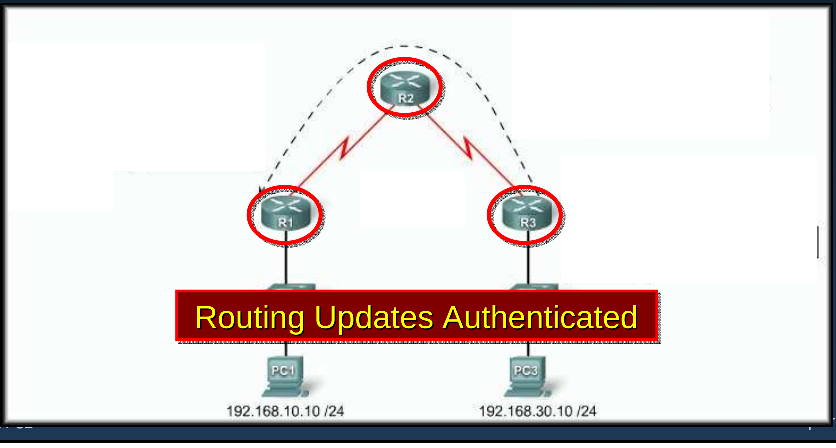


Tell R1:
192.168.10.10/32 is reachable through R3

...but R3 knows better and sends packet back to R1 creating a loop

# Steps to Safeguard a Router

- Step 5: Securing Routing Protocols.
    - Protect routing information using message digest algorithm 5 (MD5). Routers compare signatures.



# Steps to Safeguard a Router

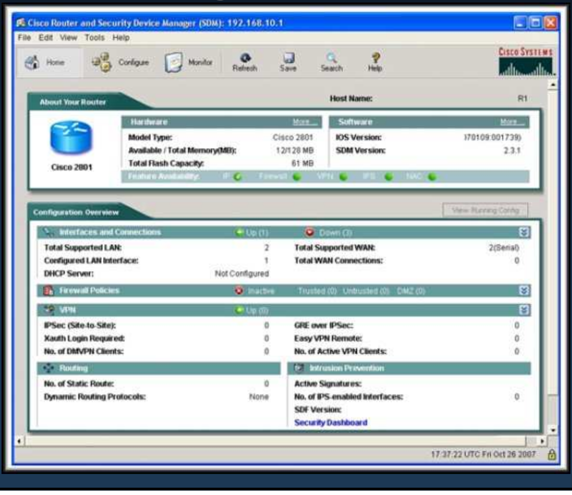
- Step 5: Securing Routing Protocols.
  - RIPv2, EIGRP, OSPF, IS-IS, and BGP all support various forms of MD5 authentication.
  - For Example:
    - Prevent RIP updates from being propagated out ports where there is no other router.
      - **`passive interface`** command.
    - Prevent unauthorized reception of RIP updates by implementing MD5 authentication with a specific key.
    - Verify RIP routing.
  - *While the commands are different, the same basic process is used for other protocols.*

# Steps to Safeguard a Router

- Locking Down Your Router With Cisco Auto Secure:
  - Cisco AutoSecure uses a single command to disable non-essential system processes and services.
  - Configure it in privileged EXEC mode using the auto secure command in one of these two modes:
  - Interactive mode:
    - This mode prompts you with options to enable and disable services and other security features. (default)
  - Non-interactive mode:
    - Automatically executes the auto secure command with the recommended Cisco default settings.

# Introducing Network Security

## Using Cisco SDM



Host Name: R1

Model Type: Cisco 2801
Available / Total Memory(MB): 12/128 MB
Total Flash Capacity: 61 MB

IOS Version: )70109:001739)
SDM Version: 2.3.1

Total Supported LAN: 2
Configured LAN Interface: 1
DHCP Server: Not Configured
Total Supported WAN: 2(Serial)
Total WAN Connections: 0

IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0

No. of Static Route: 0
Dynamic Routing Protocols: None

Active Signatures:
No. of IPS-enabled Interfaces: 0
SDF Version:

17:37:22 UTC Fri Oct 26 2007

# Using Cisco SDM

- Cisco SDM Overview:
  - The Cisco Security Device Manager (SDM) is a web-based device management tool designed for configuring LAN, WAN, and security features on Cisco IOS software-based routers.
    - It provides:
      - Easy-to-use smart wizards.
      - Automates router security management.
      - Assists through comprehensive online help.

## Using Cisco SDM

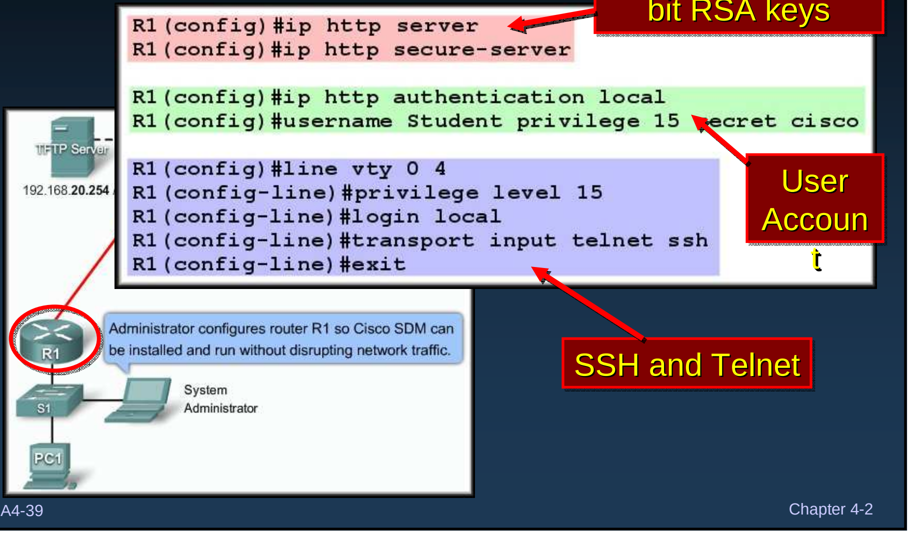
- Cisco SDM Overview:
  - Cisco SDM ships preinstalled by default on all new Cisco integrated services routers.
    - If it is not preinstalled, you will have to install it.
    - If SDM is pre-installed, Cisco recommends using Cisco SDM to perform the initial configuration
  - SDM files can be installed on router, PC, or both.
    - An advantage of installing SDM on the PC is that it saves router memory, and allows you to use SDM to manage other routers on the network.

## Using Cisco SDM

- Configuring Your Router to Support SDM:
  - Before you can install SDM on an operational router, you must ensure that a few configuration settings are present in the router configuration file.
    - Access the router's Cisco CLI interface using Telnet or the console connection.
    - Enable the HTTP and HTTPS servers on the router
    - Create a user account defined with privilege level 15.
    - Configure SSH and Telnet for local login and privilege level 15.

# Using Cisco SDM

- Configuring Your Router to Support SDM



```
R1(config)#ip http server
R1(config)#ip http secure-server

R1(config)#ip http authentication local
R1(config)#username Student privilege 15 secret cisco

R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#login local
R1(config-line)#transport input telnet ssh
R1(config-line)#exit
```

Administrator configures router R1 so Cisco SDM can be installed and run without disrupting network traffic.

HTTP and HTTPS Generates 1024 bit RSA keys

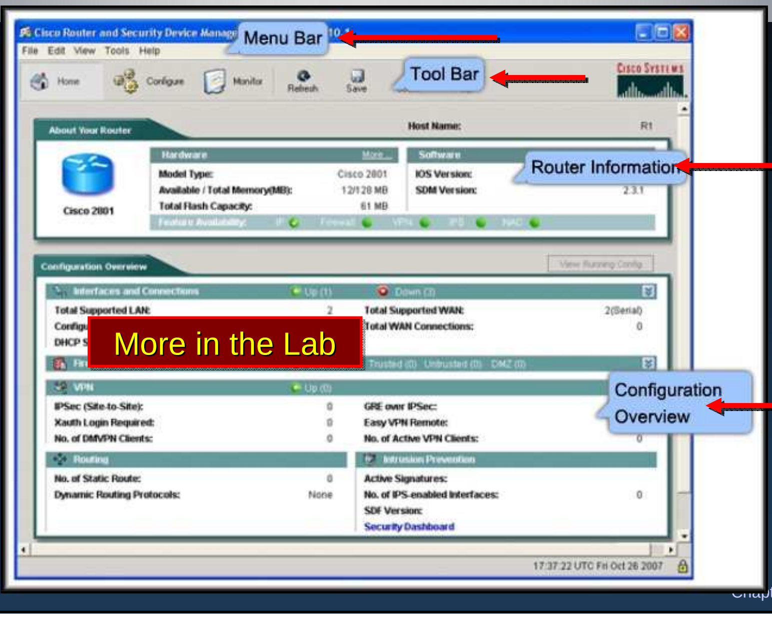
User Accoun t

SSH and Telnet

# Using Cisco SDM

- Starting SDM:
  - To launch the Cisco SDM use the HTTPS protocol and put the IP address of the router into the browser.
  - When the username and password dialog box appears, enter a username and password for the privileged (privilege level 15) account on the router.
  - After the launch page appears a signed Cisco SDM Java applet appears which must remain open while Cisco SDM is running.
  - Because it is a signed Cisco SDM Java applet you may be prompted to accept a certificate.

# Using Cisco SDM



Host Name: R1

Cisco 2801

Model Type: Cisco 2801

Available / Total Memory(MB): 12/128 MB

Total Flash Capacity: 61 MB

Feature Availability: IP ● Firewall ● VPN ● IPS ● NAC ●

IOS Version:

SDM Version: 2.3.1

Total Supported LAN: 2

Total Supported WAN: 2(Serial)

Total WAN Connections: 0

IPSec (Site-to-Site): 0

Xauth Login Required: 0

No. of DMVPN Clients: 0

GRE over IPSec:

Easy VPN Remote:

No. of Active VPN Clients: 0

No. of Static Route: 0

Dynamic Routing Protocols: None

Active Signatures:

No. of IPS-enabled Interfaces: 0

SDF Version:

17:37:22 UTC Fri Oct 26 2007

Menu Bar

Tool Bar

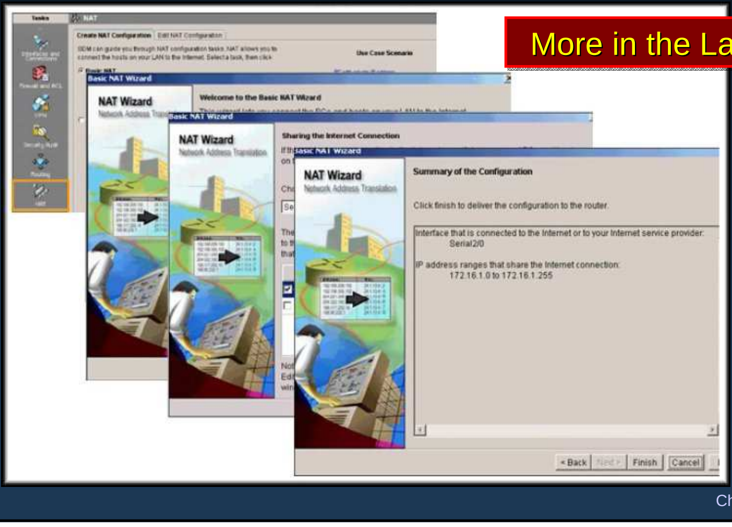
Router Information

Configuration Overview

More in the Lab

# Using Cisco SDM

- Cisco SDM Wizards:



Summary of the Configuration

Click finish to deliver the configuration to the router.

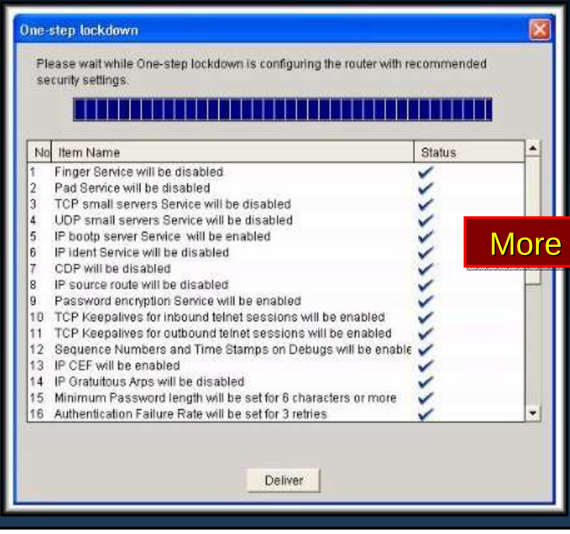
Interface that is connected to the Internet or to your Internet service provider:
Serial2/0

IP address ranges that share the Internet connection:
172.16.1.0 to 172.16.1.255

More in the Lab

# Using Cisco SDM

- Locking Down a Router with SDM:



One-step lockdown

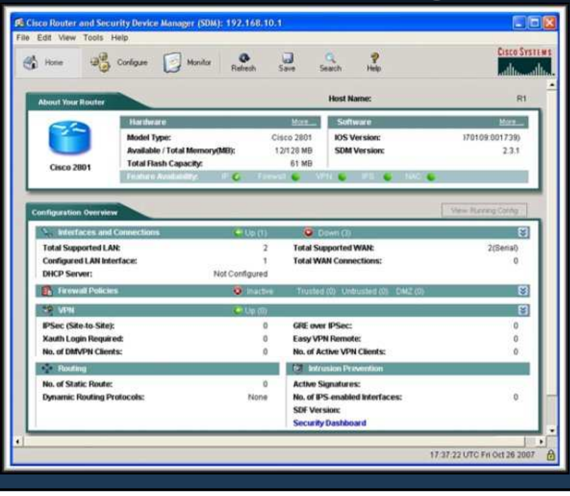
Please wait while One-step lockdown is configuring the router with recommended security settings.

| No | Item Name | Status |
|---|---|---|
| 1 | Finger Service will be disabled | ✓ |
| 2 | Pad Service will be disabled | ✓ |
| 3 | TCP small servers Service will be disabled | ✓ |
| 4 | UDP small servers Service will be disabled | ✓ |
| 5 | IP bootp server Service will be enabled | ✓ |
| 6 | IP ident Service will be disabled | ✓ |
| 7 | CDP will be disabled | ✓ |
| 8 | IP source route will be disabled | ✓ |
| 9 | Password encryption Service will be enabled | ✓ |
| 10 | TCP Keepalives for inbound telnet sessions will be enabled | ✓ |
| 11 | TCP Keepalives for outbound telnet sessions will be enabled | ✓ |
| 12 | Sequence Numbers and Time Stamps on Debugs will be enable | ✓ |
| 13 | IP CEF will be enabled | ✓ |
| 14 | IP Gratuitous Arps will be disabled | ✓ |
| 15 | Minimum Password length will be set for 6 characters or more | ✓ |
| 16 | Authentication Failure Rate will be set for 3 retries | ✓ |

More in the Lab

# Introducing Network Security

## Secure Router Management



Cisco Router and Security Device Manager (SDM): 192.168.10.1

Host Name: R1

Hardware
Model Type: Cisco 2801
Available / Total Memory(MB): 12/128 MB
Total Flash Capacity: 61 MB
Feature Availability: IP Firewall VPN IPS NAC

Software
IOS Version: )70109:001739)
SDM Version: 2.3.1

Configuration Overview

Interfaces and Connections Up (1) Down (3)
Total Supported LAN: 2
Configured LAN Interface: 1
DHCP Server: Not Configured
Total Supported WAN: 2(Serial)
Total WAN Connections: 0

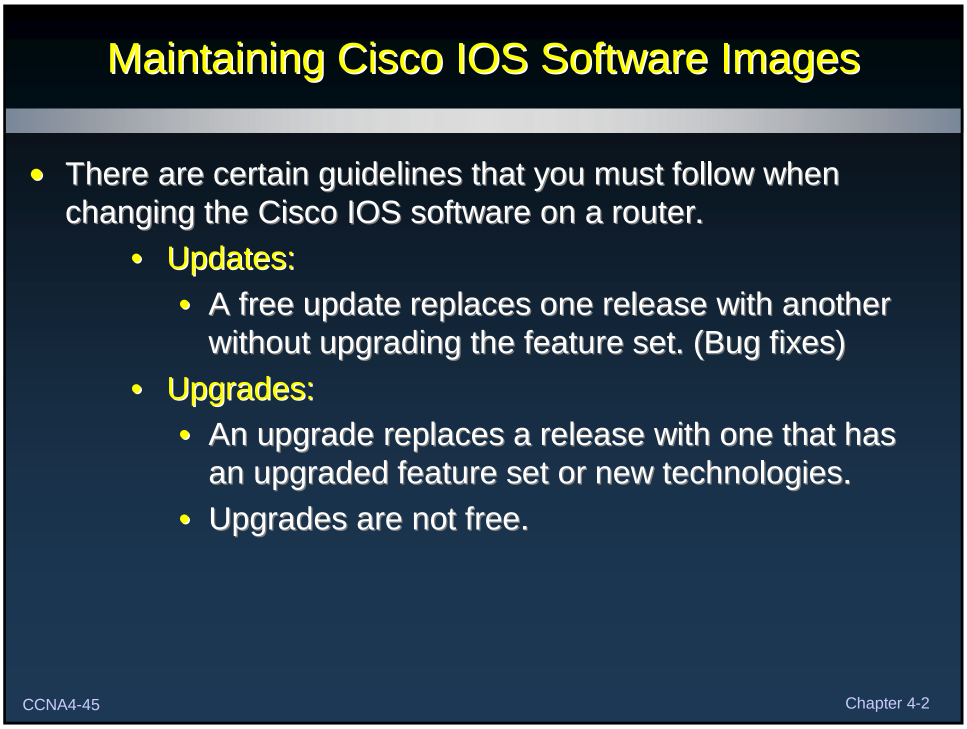
Firewall Policies Inactive Trusted (0) Untrusted (0) DMZ (0)

VPN Up (0)
IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0

Routing
No. of Static Route: 0
Dynamic Routing Protocols: None

Intrusion Prevention
Active Signatures:
No. of IPS-enabled Interfaces: 0
SDF Version:

17:37:22 UTC Fri Oct 26 2007

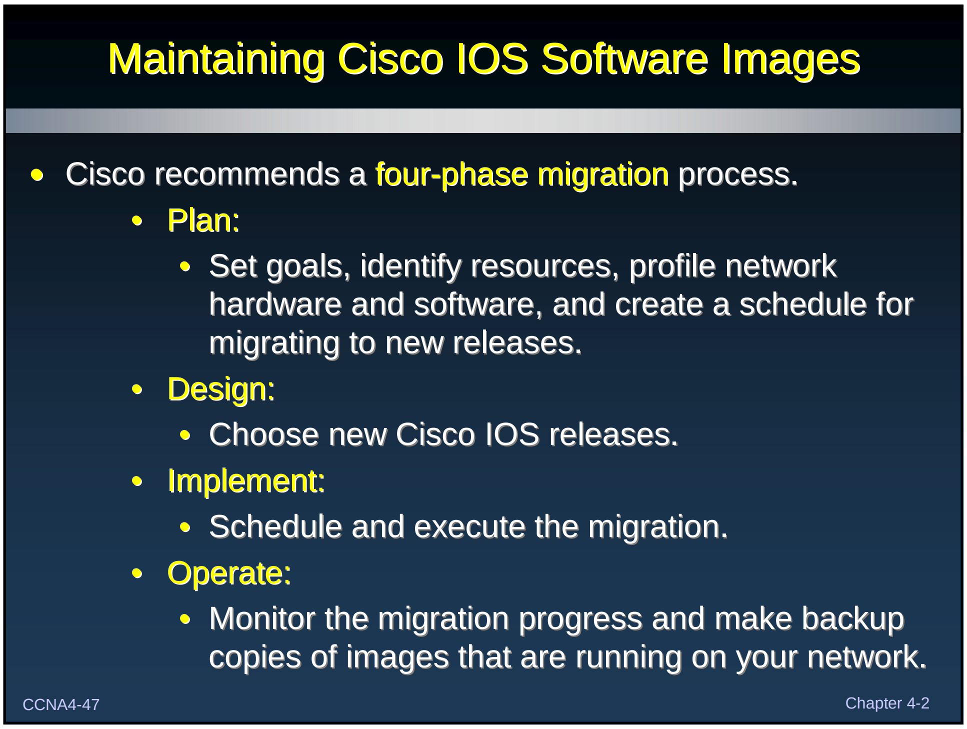


## Maintaining Cisco IOS Software Images

- There are certain guidelines that you must follow when changing the Cisco IOS software on a router.
  - Updates:
    - A free update replaces one release with another without upgrading the feature set. (Bug fixes)
  - Upgrades:
    - An upgrade replaces a release with one that has an upgraded feature set or new technologies.
    - Upgrades are not free.

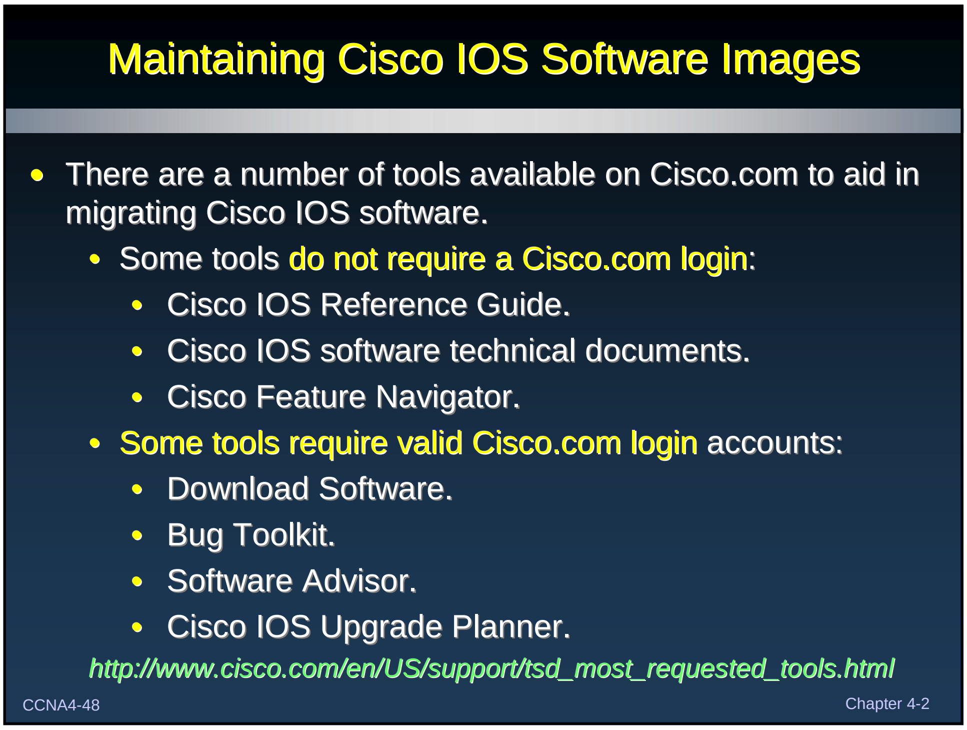
## Maintaining Cisco IOS Software Images

- It is not always a good idea to upgrade to the latest version of IOS software.
  - Many times that release is not stable.
  - It may include new features or technologies that are not needed in your enterprise.



## Maintaining Cisco IOS Software Images

- Cisco recommends a four-phase migration process.
  - Plan:
    - Set goals, identify resources, profile network hardware and software, and create a schedule for migrating to new releases.
  - Design:
    - Choose new Cisco IOS releases.
  - Implement:
    - Schedule and execute the migration.
  - Operate:
    - Monitor the migration progress and make backup copies of images that are running on your network.



## Maintaining Cisco IOS Software Images

- There are a number of tools available on Cisco.com to aid in migrating Cisco IOS software.
  - Some tools do not require a Cisco.com login:
    - Cisco IOS Reference Guide.
    - Cisco IOS software technical documents.
    - Cisco Feature Navigator.
  - Some tools require valid Cisco.com login accounts:
    - Download Software.
    - Bug Toolkit.
    - Software Advisor.
    - Cisco IOS Upgrade Planner.

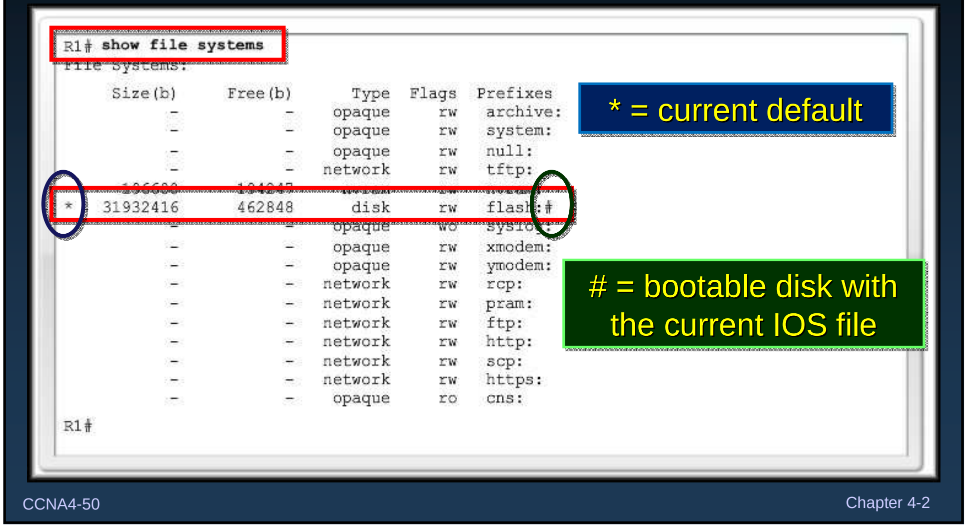
*http://www.cisco.com/en/US/support/tsd_most_requested_tools.html*

# Managing Cisco IOS Images

- Cisco IOS File Systems and Devices:
  - Cisco IOS devices provide a feature called the Cisco IOS Integrated File System (IFS).
    - The directories available depend on the platform.
    - The **`show file systems`** command lists all file systems.
    - It provides information such as the amount of available and free memory, type of file system and its permissions.
    - Permissions include read only (ro), write only (wo), and read and write (rw).

# Managing Cisco IOS Images

- Cisco IOS File Systems and Devices:



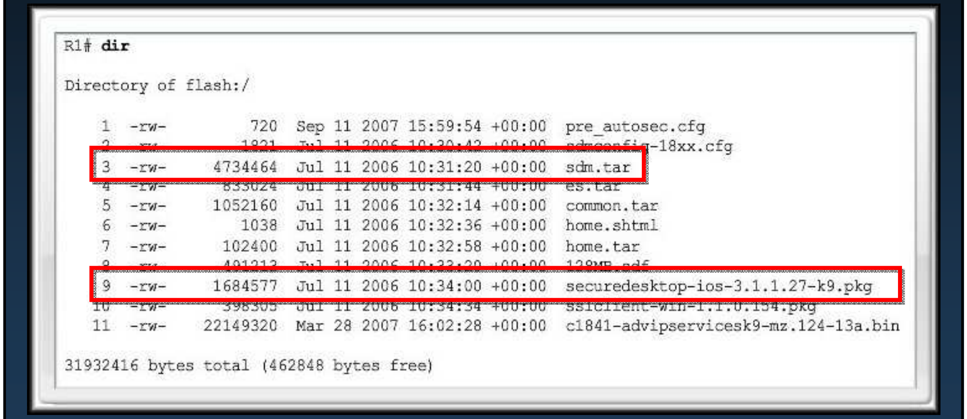
```
R1# show file systems
File Systems:

      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw   archive:
            -             -    opaque     rw   system:
            -             -    opaque     rw   null:
            -             -   network     rw   tftp:
       196600        184247     nvram     rw   nvram:
*    31932416        462848      disk     rw   flash:#
            -             -    opaque     wo   syslog:
            -             -    opaque     rw   xmodem:
            -             -    opaque     rw   ymodem:
            -             -   network     rw   rcp:
            -             -   network     rw   pram:
            -             -   network     rw   ftp:
            -             -   network     rw   http:
            -             -   network     rw   scp:
            -             -   network     rw   https:
            -             -    opaque     ro   cns:

R1#
```

* = current default

# = bootable disk with the current IOS file

# Managing Cisco IOS Images

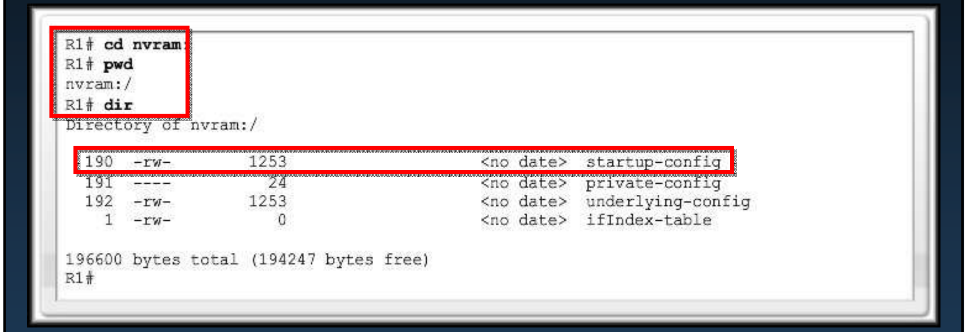
- Cisco IOS File Systems and Devices:
  - Flash:



```
R1# dir

Directory of flash:/

    1  -rw-         720  Sep 11 2007 15:59:54 +00:00  pre_autosec.cfg
    2  -rw-        1821  Jul 11 2006 10:30:42 +00:00  sdmconfig-18xx.cfg
    3  -rw-     4734464  Jul 11 2006 10:31:20 +00:00  sdm.tar
    4  -rw-      833024  Jul 11 2006 10:31:44 +00:00  es.tar
    5  -rw-     1052160  Jul 11 2006 10:32:14 +00:00  common.tar
    6  -rw-        1038  Jul 11 2006 10:32:36 +00:00  home.shtml
    7  -rw-      102400  Jul 11 2006 10:32:58 +00:00  home.tar
    8  -rw-      491213  Jul 11 2006 10:33:20 +00:00  128MB.sdf
    9  -rw-     1684577  Jul 11 2006 10:34:00 +00:00  securedesktop-ios-3.1.1.27-k9.pkg
   10  -rw-      398305  Jul 11 2006 10:34:34 +00:00  sslclient-win-1.1.0.154.pkg
   11  -rw-    22149320  Mar 28 2007 16:02:28 +00:00  c1841-advipservicesk9-mz.124-13a.bin

31932416 bytes total (462848 bytes free)
```

# Managing Cisco IOS Images

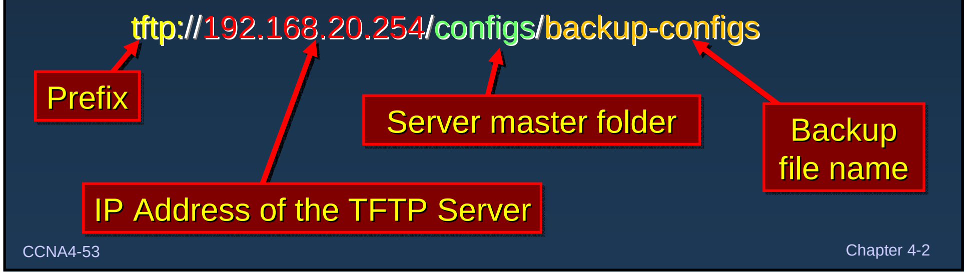
- Cisco IOS File Systems and Devices:
  - NVRAM:



```
R1# cd nvram:
R1# pwd
nvram:/
R1# dir
Directory of nvram:/

  190  -rw-        1253                     <no date>  startup-config
  191  ----          24                     <no date>  private-config
  192  -rw-        1253                     <no date>  underlying-config
    1  -rw-           0                     <no date>  ifIndex-table

196600 bytes total (194247 bytes free)
R1#
```

# Managing Cisco IOS Images

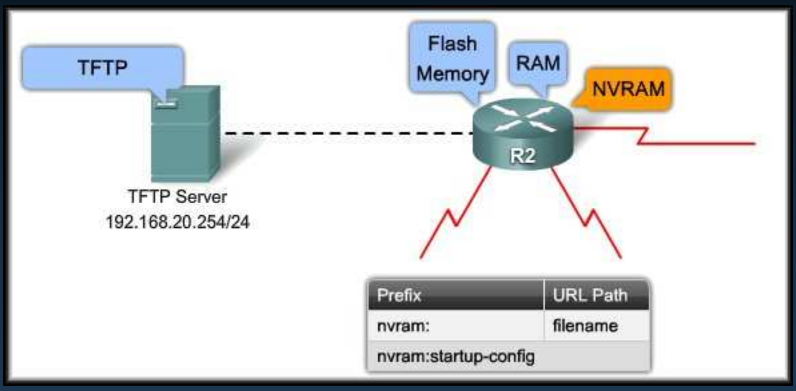
- URL Prefixes for Cisco Devices:
  - Administrators do not have visual cues when working at a router CLI.
    - File locations are specified in Cisco IFS using the URL convention.
    - Similar to the format you know from the web.
    - For Example:



tftp://192.168.20.254/configs/backup-configs

# Managing Cisco IOS Images

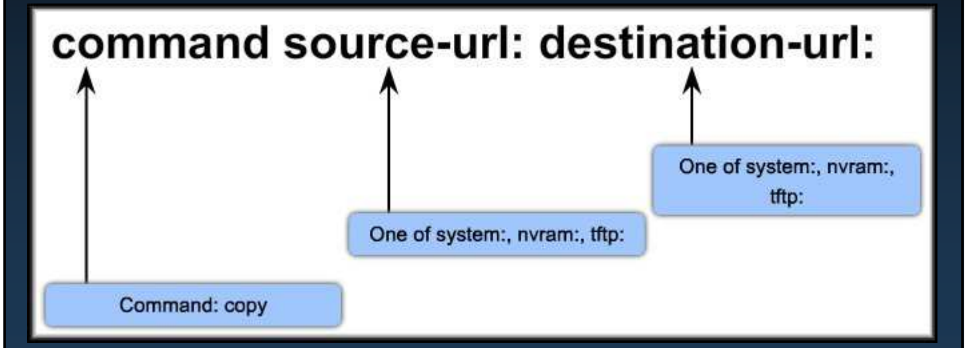
- URL Prefixes for Cisco Devices:



| Prefix | URL Path |
|---|---|
| nvram: | filename |
| nvram:startup-config | |

## Managing Cisco IOS Images

- URL Prefixes for Cisco Devices:
  - The copy command is used to move files from one device to another, such as RAM, NVRAM, or a TFTP server.



command source-url: destination-url:

Command: copy

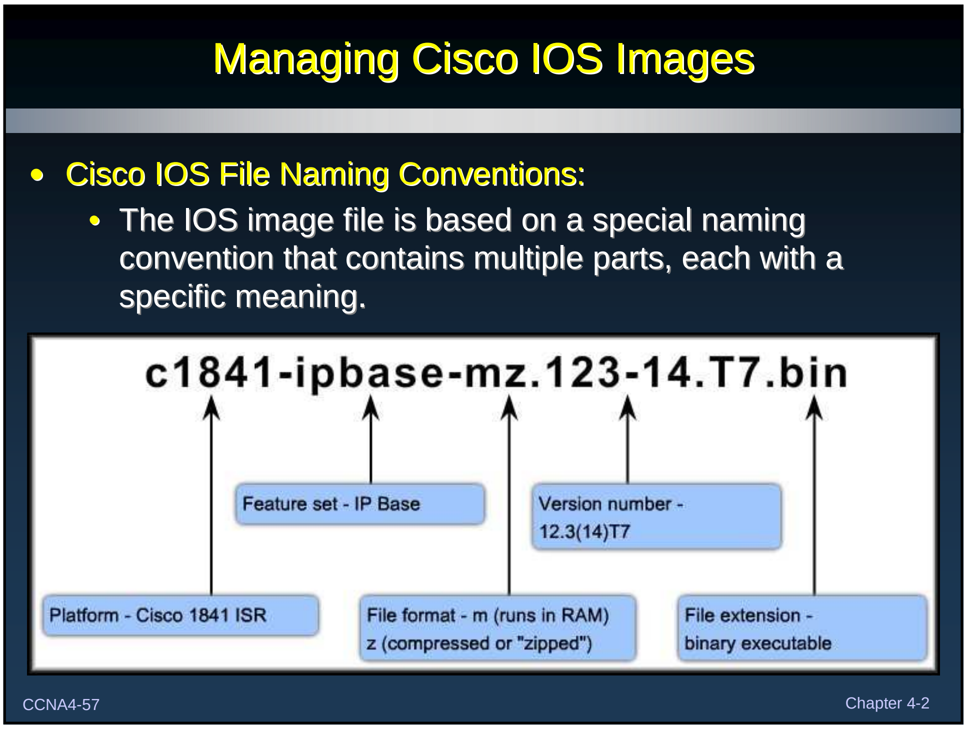
One of system:, nvram:, tftp:

One of system:, nvram:, tftp:

## Managing Cisco IOS Images

- URL Prefixes for Cisco Devices:
  - The copy command is used to move files from one device to another, such as RAM, NVRAM, or a TFTP server.

```
R2#copy run start
R2#copy system:running-config nvram:startup-config

R2#copy run tftp:
R2#copy system:running-config tftp:

R2#copy tftp: start
R2#copy tftp: nvram:startup-config
```



## Managing Cisco IOS Images

- Cisco IOS File Naming Conventions:
  - The IOS image file is based on a special naming convention that contains multiple parts, each with a specific meaning.

c1841-ipbase-mz.123-14.T7.bin

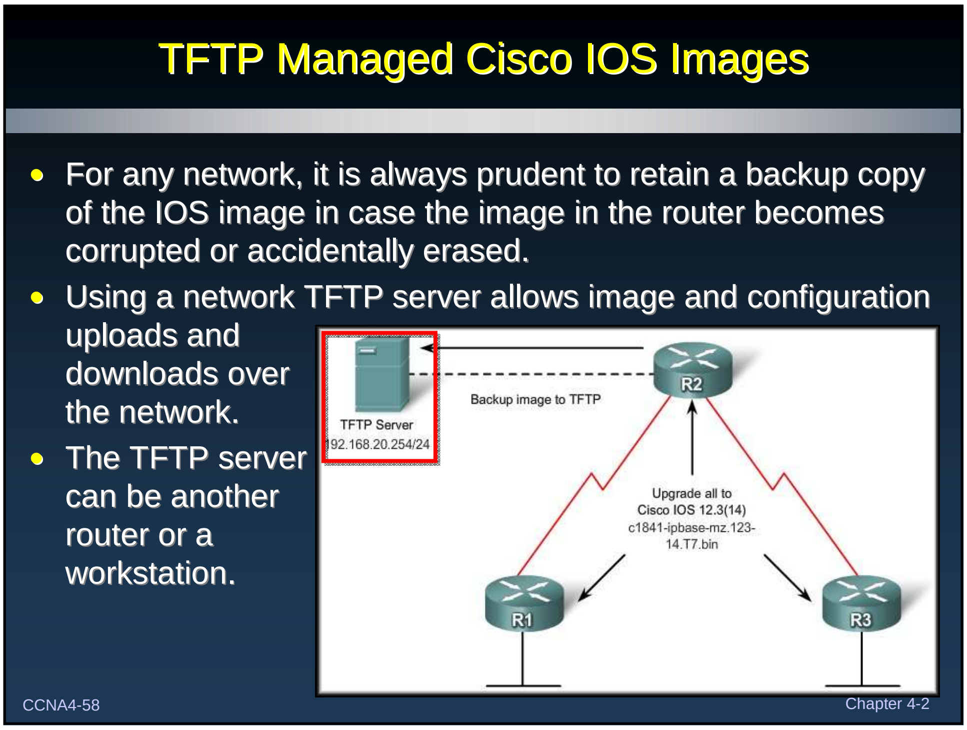
Feature set - IP Base

Version number - 12.3(14)T7

Platform - Cisco 1841 ISR

File format - m (runs in RAM) z (compressed or "zipped")

File extension - binary executable



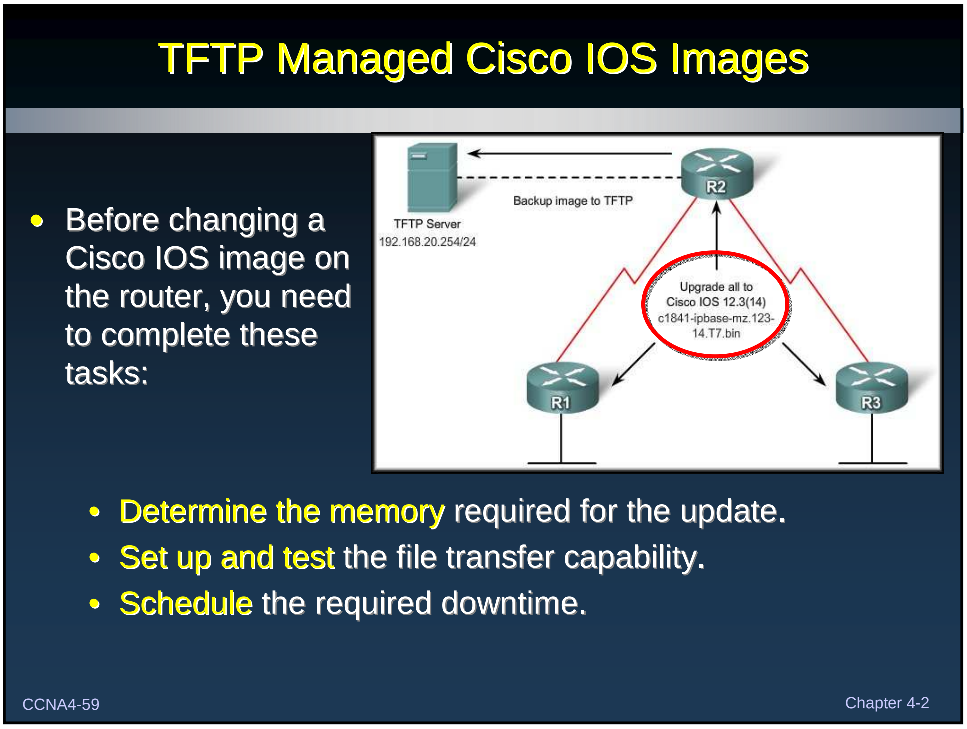
## TFTP Managed Cisco IOS Images

- For any network, it is always prudent to retain a backup copy of the IOS image in case the image in the router becomes corrupted or accidentally erased.
- Using a network TFTP server allows image and configuration uploads and downloads over the network.
- The TFTP server can be another router or a workstation.

TFTP Server
192.168.20.254/24

Backup image to TFTP

Upgrade all to Cisco IOS 12.3(14) c1841-ipbase-mz.123-14.T7.bin

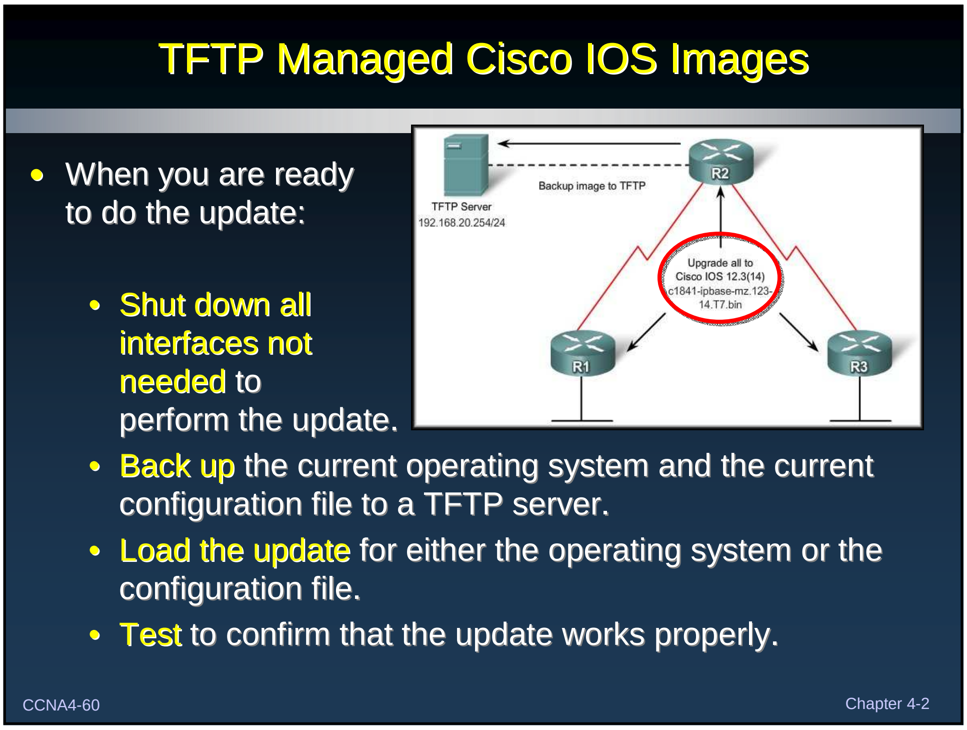


## TFTP Managed Cisco IOS Images

- Before changing a Cisco IOS image on the router, you need to complete these tasks:

TFTP Server
192.168.20.254/24
Backup image to TFTP
R2
Upgrade all to Cisco IOS 12.3(14) c1841-ipbase-mz.123-14.T7.bin
R1
R3

  - Determine the memory required for the update.
  - Set up and test the file transfer capability.
  - Schedule the required downtime.



## TFTP Managed Cisco IOS Images

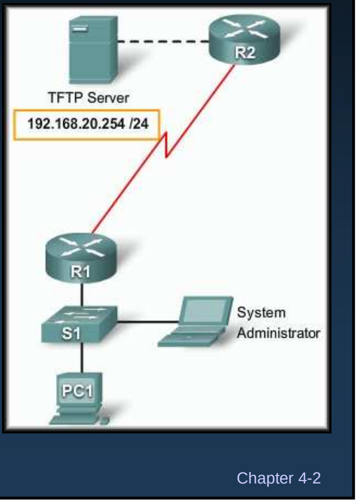
- When you are ready to do the update:

TFTP Server
192.168.20.254/24
Backup image to TFTP
R2
Upgrade all to Cisco IOS 12.3(14) c1841-ipbase-mz.123-14.T7.bin
R1
R3

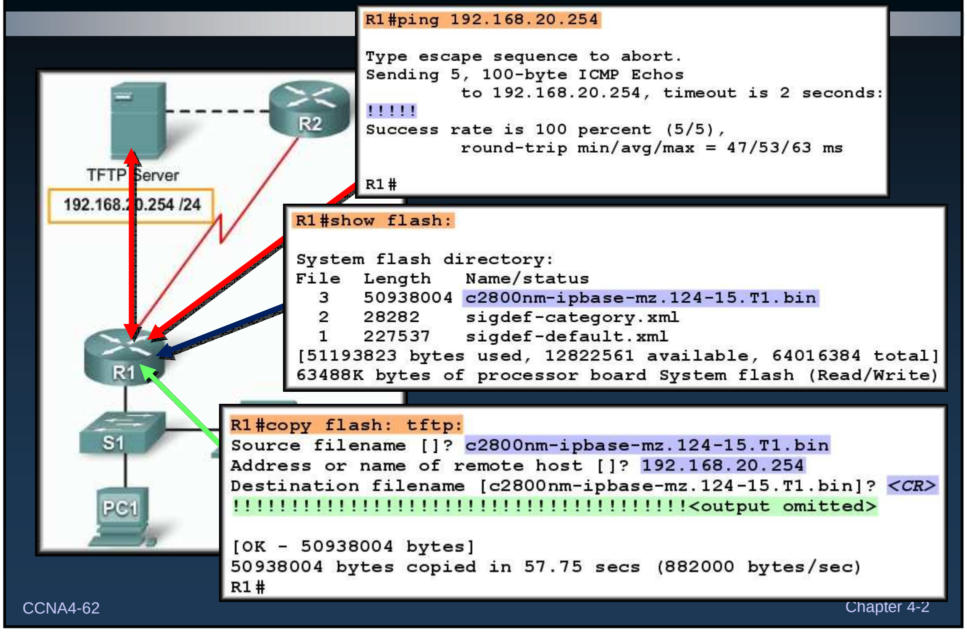
  - Shut down all interfaces not needed to perform the update.
  - Back up the current operating system and the current configuration file to a TFTP server.
  - Load the update for either the operating system or the configuration file.
  - Test to confirm that the update works properly.

# TFTP Managed Cisco IOS Images

- To copy IOS image software or any other files from a network device flash drive to a network TFTP server:
  - Ping the TFTP server to make sure you have access to it.
  - Verify that the TFTP server has sufficient disk space.
  - Use the **`show flash:`** command to determine the name of the files.
  - Copy the file(s) from the router to the TFTP server using the **`copy flash: tftp:`** command.
    - Each file requires a separate command.



# TFTP Managed Cisco IOS Images



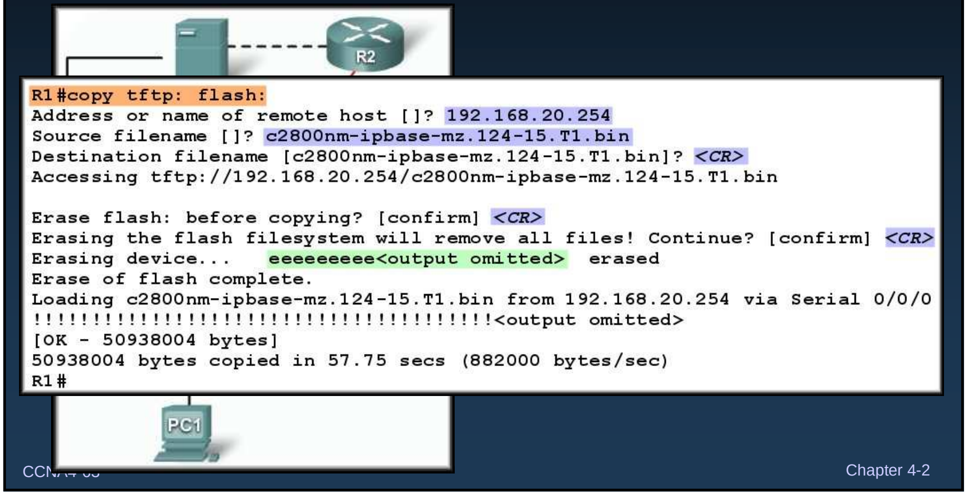
```
R1#ping 192.168.20.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos
        to 192.168.20.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
        round-trip min/avg/max = 47/53/63 ms

R1#
```

```
R1#show flash:

System flash directory:
File  Length    Name/status
  3   50938004  c2800nm-ipbase-mz.124-15.T1.bin
  2   28282     sigdef-category.xml
  1   227537    sigdef-default.xml
[51193823 bytes used, 12822561 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

```
R1#copy flash: tftp:
Source filename []? c2800nm-ipbase-mz.124-15.T1.bin
Address or name of remote host []? 192.168.20.254
Destination filename [c2800nm-ipbase-mz.124-15.T1.bin]? <CR>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!<output omitted>

[OK - 50938004 bytes]
50938004 bytes copied in 57.75 secs (882000 bytes/sec)
R1#
```

## TFTP Managed Cisco IOS Images

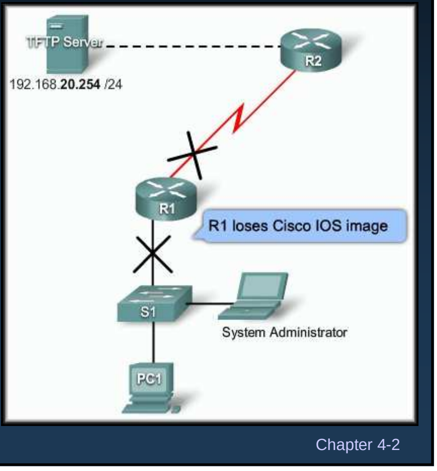
- Upgrading a system to a newer software version requires a different system image file to be loaded on the router.



```
R1#copy tftp: flash:
Address or name of remote host []? 192.168.20.254
Source filename []? c2800nm-ipbase-mz.124-15.T1.bin
Destination filename [c2800nm-ipbase-mz.124-15.T1.bin]? <CR>
Accessing tftp://192.168.20.254/c2800nm-ipbase-mz.124-15.T1.bin

Erase flash: before copying? [confirm] <CR>
Erasing the flash filesystem will remove all files! Continue? [confirm] <CR>
Erasing device...   eeeeeeeee<output omitted>  erased
Erase of flash complete.
Loading c2800nm-ipbase-mz.124-15.T1.bin from 192.168.20.254 via Serial 0/0/0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!<output omitted>
[OK - 50938004 bytes]
50938004 bytes copied in 57.75 secs (882000 bytes/sec)
R1#
```

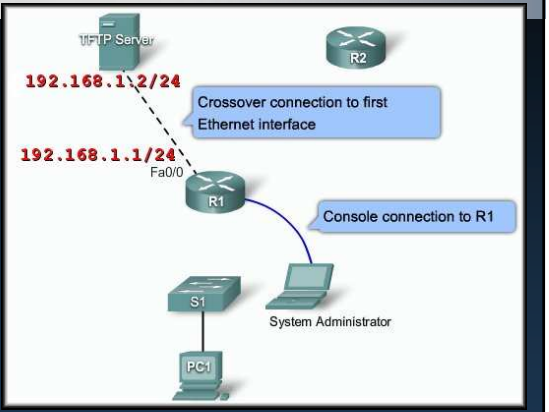
## Recovering Software Images

- When an IOS on a router is accidentally deleted from flash, the router is still operational because the IOS is running in RAM.
    - However, **it is crucial that the router is not rebooted as a production device** since it would not be able to find a valid IOS in flash.
    - When the router is rebooted and can no longer load an IOS it loads in ROMmon mode by default.
    - prompt = **`rommon >`**

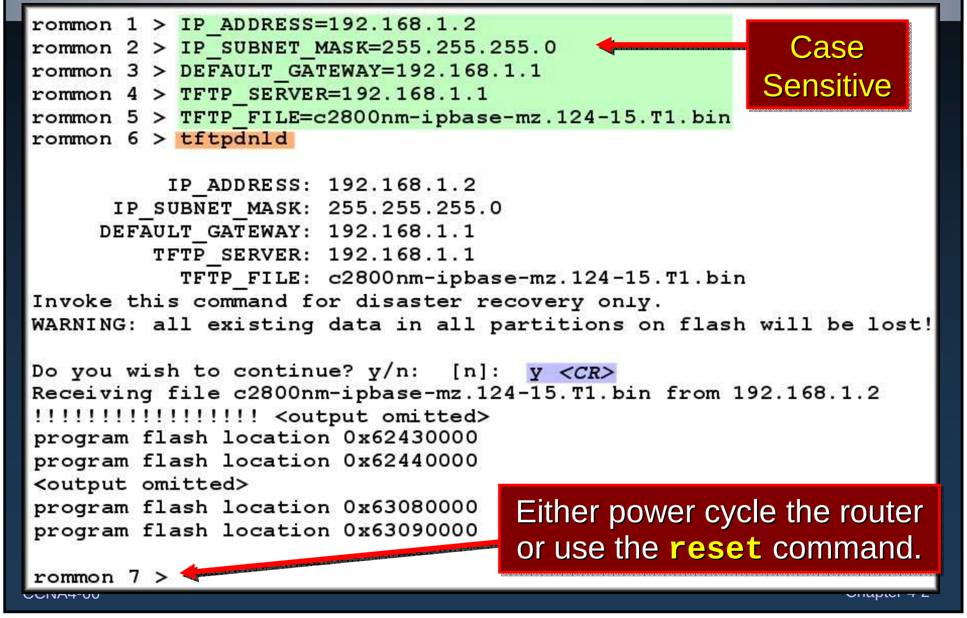


# Recovering Software Images

- Using **`tftpdnld`**:
  - Connect a PC to the console port.
  - Connect the first Ethernet port on the router to the TFTP server with a cross-over cable.
  - Configure the TFTP server with a static IP Address.
  - Boot the router and set the ROMmon variables.
  - Enter the **`tftpdnld`** command.



# Recovering Software Images



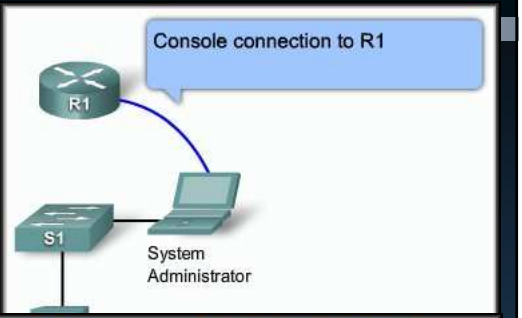
```
rommon 1 > IP_ADDRESS=192.168.1.2
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.1.1
rommon 4 > TFTP_SERVER=192.168.1.1
rommon 5 > TFTP_FILE=c2800nm-ipbase-mz.124-15.T1.bin
rommon 6 > tftpdnld

          IP_ADDRESS: 192.168.1.2
      IP_SUBNET_MASK: 255.255.255.0
     DEFAULT_GATEWAY: 192.168.1.1
         TFTP_SERVER: 192.168.1.1
           TFTP_FILE: c2800nm-ipbase-mz.124-15.T1.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n:  [n]:  y <CR>
Receiving file c2800nm-ipbase-mz.124-15.T1.bin from 192.168.1.2
!!!!!!!!!!!!!!!!! <output omitted>
program flash location 0x62430000
program flash location 0x62440000
<output omitted>
program flash location 0x63080000
program flash location 0x63090000

rommon 7 >
```

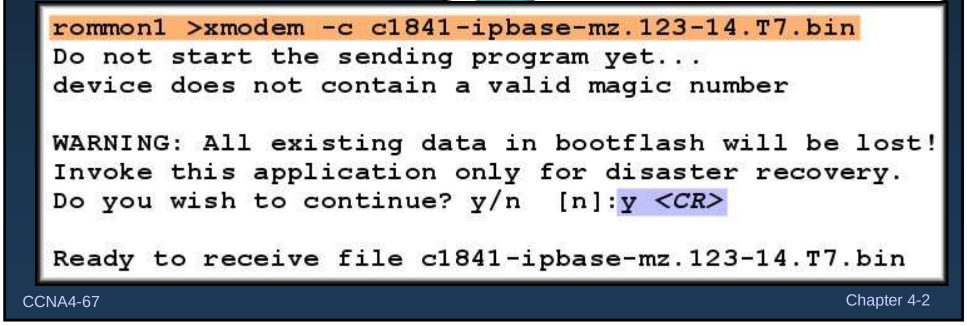
Case Sensitive

Either power cycle the router or use the **`reset`** command.

# Recovering Software Images

- Using **xmodem**:
  - Connect a PC to the console port.
  - Boot the router and issue the **xmodem** command.

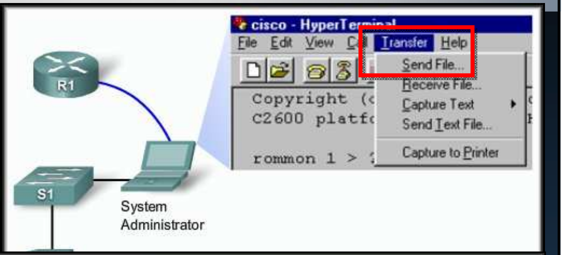




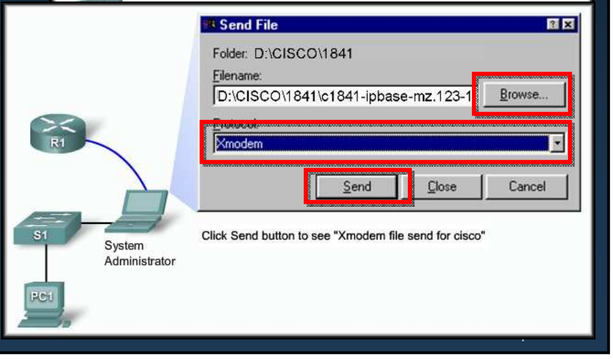
```
rommon1 >xmodem -c c1841-ipbase-mz.123-14.T7.bin
Do not start the sending program yet...
device does not contain a valid magic number

WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n  [n]:y <CR>

Ready to receive file c1841-ipbase-mz.123-14.T7.bin
```

# Recovering Software Images

- Using **xmodem**:
  - Load a terminal emulation program (e.g. Hyperterminal) that supports the Xmodem protocol.
  - Once the transfer has finished, reboot the router.



```
Copyright (c
C2600 platfo

rommon 1 > 
```



Folder: D:\CISCO\1841

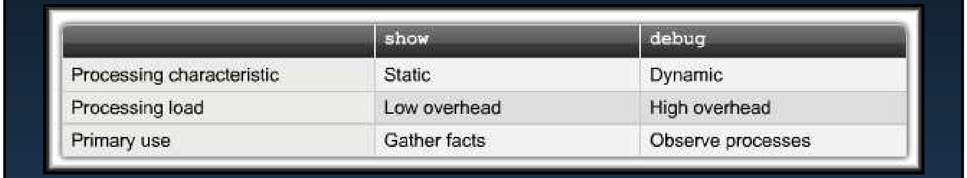
Filename: D:\CISCO\1841\c1841-ipbase-mz.123-1

Protocol: Xmodem

Click Send button to see "Xmodem file send for cisco"

## Troubleshooting Cisco IOS Configurations

- Cisco IOS troubleshooting commands:
  - **show** – configured parameters and their values.
  - **debug** – trace the execution of a process.



| | show | debug |
|---|---|---|
| Processing characteristic | Static | Dynamic |
| Processing load | Low overhead | High overhead |
| Primary use | Gather facts | Observe processes |

  - By default, the router sends the output from debug commands to the console but it can be redirected to a logging server.

## Troubleshooting Cisco IOS Configurations

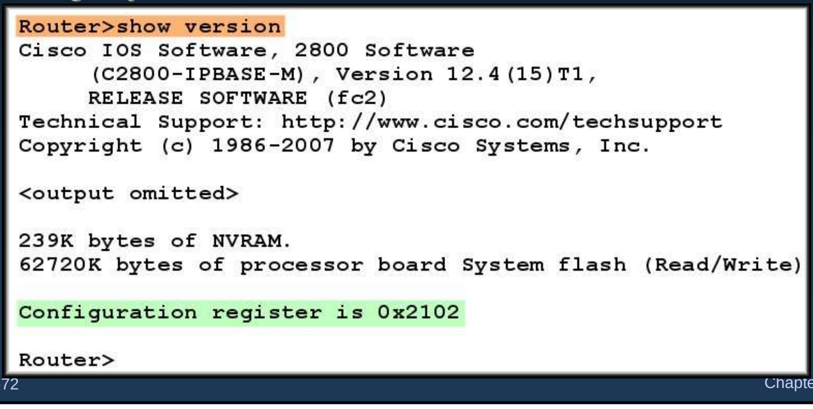
- Considerations when using the **debug** command:
  - Plan the use of the debug command. Use it carefully.
  - Gets CPU priority and may interfere with normal routing processes.
  - Can help resolve network issues even though you may take a temporary performance hit.
  - Can generate too much output. Know what you're looking for before you start.
  - Different debugs generate different output. Don't be caught by surprise.

# Recovering a Lost Password

- Password Recovery:
  - Recovering a password makes use of the router's configuration register.
  - This register is like the BIOS on a PC.
    - When a router boots, it will check the register and boot in the manner specified by the value in the register.
  - For this course, we will only concern ourselves with two registry values.
    - 0x2102: the default registry value.
    - 0x2142: instructs the router to bypass any startup configuration.

# Recovering a Lost Password

- Password Recovery Basic Steps:
  - Connect to the router console port.
  - Issue the **`show version`** command to obtain the current registry value.



```
Router>show version
Cisco IOS Software, 2800 Software
     (C2800-IPBASE-M), Version 12.4(15)T1,
     RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.

<output omitted>

239K bytes of NVRAM.
62720K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

Router>
```

## Recovering a Lost Password

- Password Recovery Basic Steps:
  - Power cycle the router and press the “Break” key within 60 seconds. This puts the router in ROMmon mode.
  - Type **`confreg 0x2142`** at the **`rommon 1 >`** prompt to specify bypassing the startup configuration.
  - Type **`reset`** or power cycle the router.
  - Bypass any default startup questions and type **`enable`**.
  - Copy the start up configuration to the running configuration.

## Recovering a Lost Password

- Password Recovery Basic Steps:
  - Change the password. (enable secret, Console or VTY)
  - Change the configuration register back to the default using the following command:

```
Router(config)#config-register 0x2102
```

  - Copy the running configuration to the startup configuration and reload or power cycle the router.

We will do this in the lab.