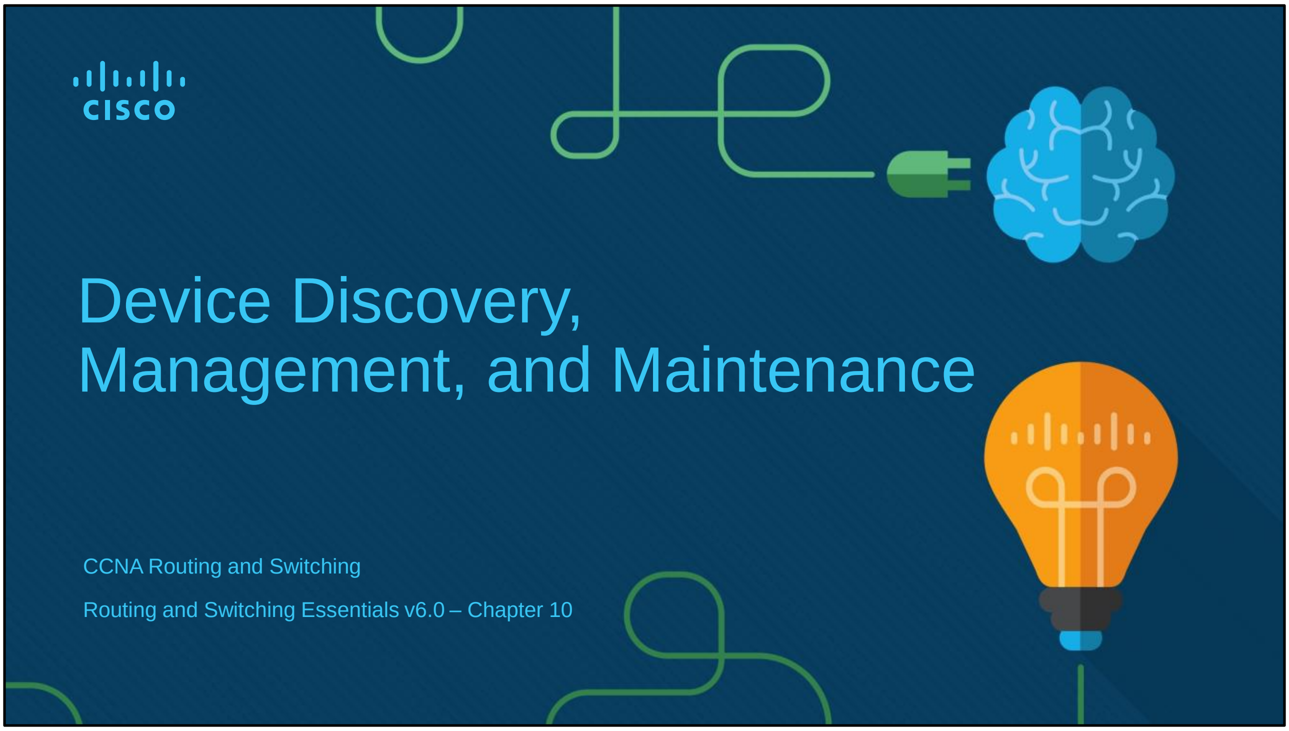
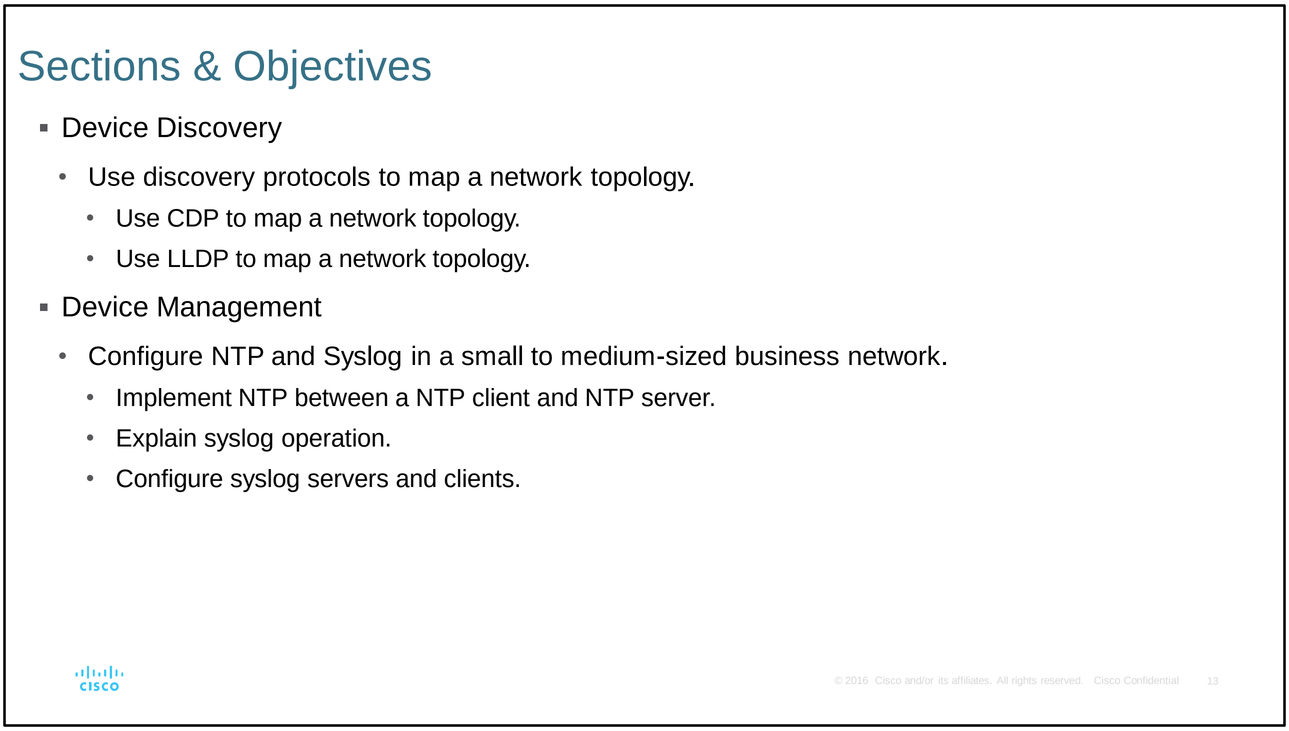


Device Discovery, Management, and Maintenance

CCNA Routing and Switching

Routing and Switching Essentials v6.0 – Chapter 10



Sections & Objectives

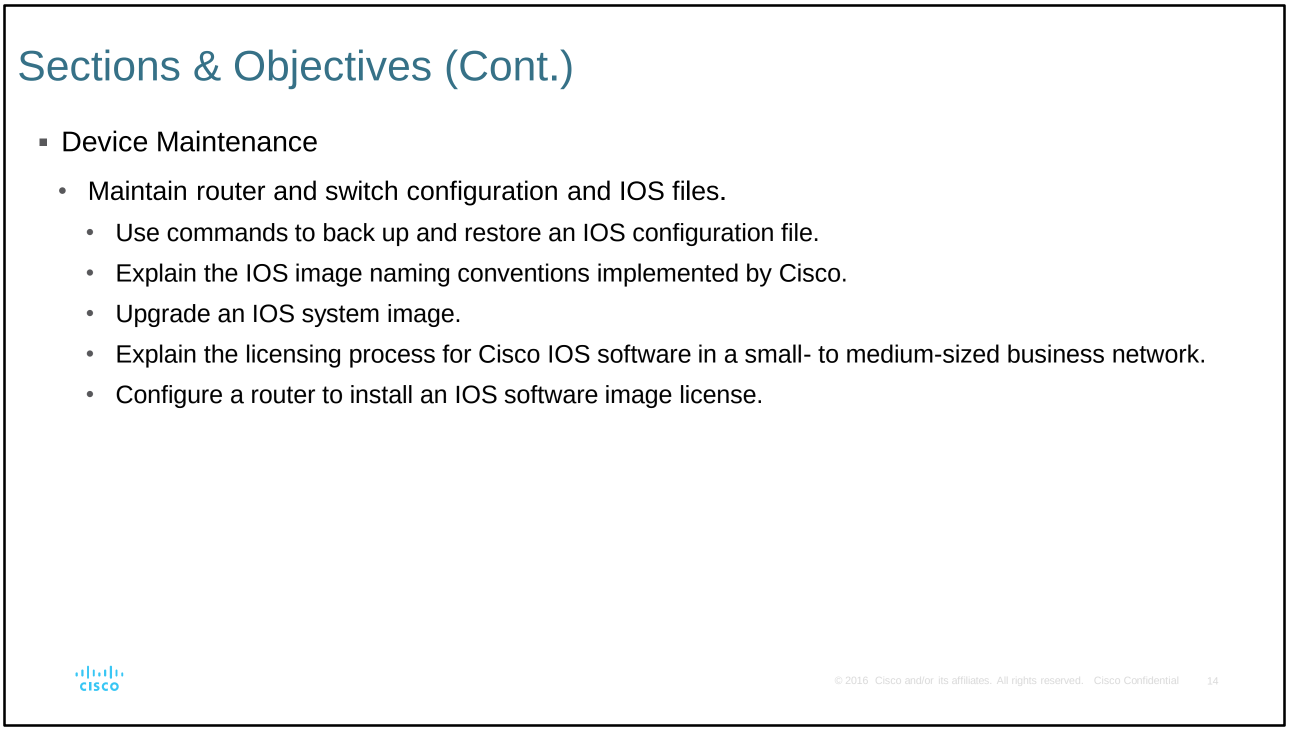
- Device Discovery
  - Use discovery protocols to map a network topology.
    - Use CDP to map a network topology.
    - Use LLDP to map a network topology.
- Device Management
  - Configure NTP and Syslog in a small to medium-sized business network.
    - Implement NTP between a NTP client and NTP server.
    - Explain syslog operation.
    - Configure syslog servers and clients.

Device Discovery, Management, and Maintenance

In this chapter, you will explore the tools network administrators can use for device discovery, device management, and device maintenance. Cisco Discovery Protocol (CDP) and Link Layer Discover Protocol (LLDP) are both capable of discovering information about directly connected devices.

Network Time Protocol (NTP) can be effectively used to synchronize the time across all your networking devices, which is especially important when trying to compare log files from different devices. Those log files are generated by the syslog protocol. Syslog messages can be captured and sent to a syslog server to aid in device management tasks.

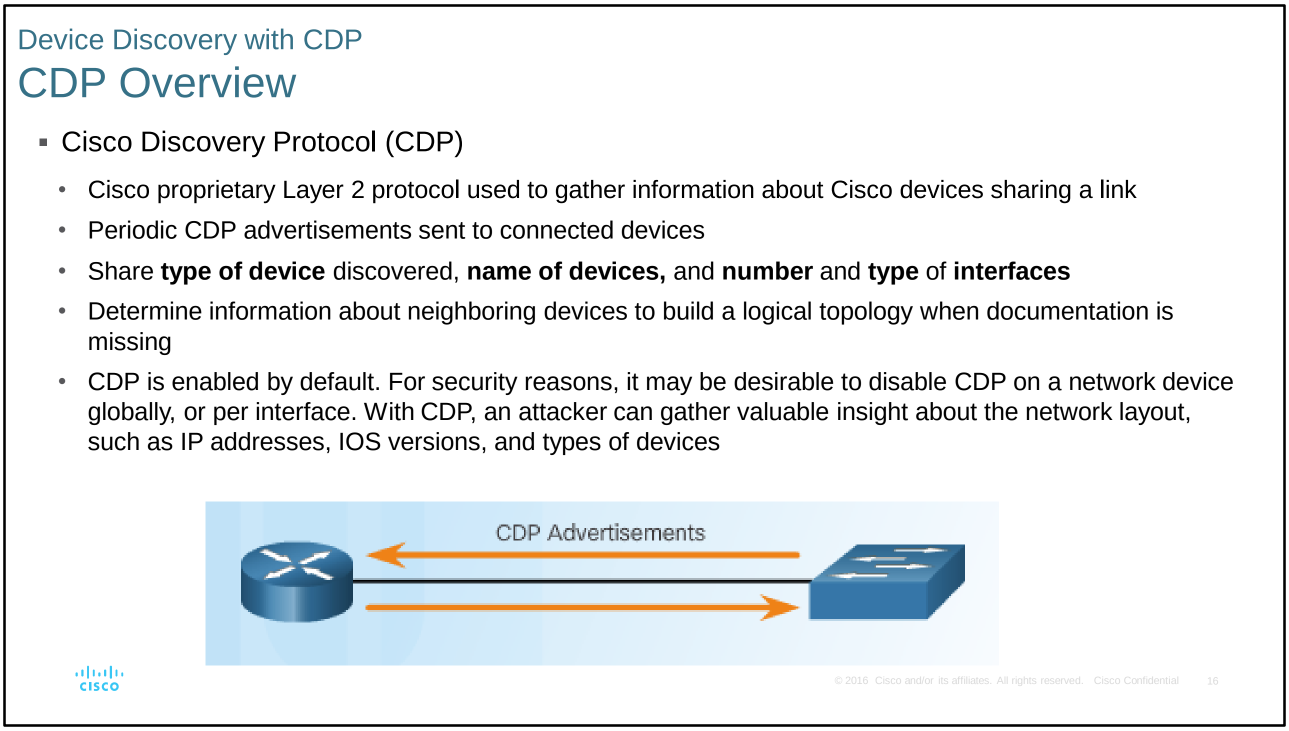
Device maintenance includes ensuring that Cisco IOS images and configuration files are backed up in a safe location in the event that the device memory is corrupted or erased, either maliciously or inadvertently. Maintenance also includes keeping the IOS image up to date. The device maintenance section of the chapter includes topics for file maintenance, image management, and software licensing.



Sections & Objectives (Cont.)

- Device Maintenance
  - Maintain router and switch configuration and IOS files.
    - Use commands to back up and restore an IOS configuration file.
    - Explain the IOS image naming conventions implemented by Cisco.
    - Upgrade an IOS system image.
    - Explain the licensing process for Cisco IOS software in a small- to medium-sized business network.
    - Configure a router to install an IOS software image license.

Device Discovery



Device Discovery with CDP

CDP Overview

- Cisco Discovery Protocol (CDP)
  - Cisco proprietary Layer 2 protocol used to gather information about Cisco devices sharing a link
  - Periodic CDP advertisements sent to connected devices
  - Share **type of device** discovered, **name of devices,** and **number** and **type** of **interfaces**
  - Determine information about neighboring devices to build a logical topology when documentation is missing
  - CDP is enabled by default. For security reasons, it may be desirable to disable CDP on a network device globally, or per interface. With CDP, an attacker can gather valuable insight about the network layout, such as IP addresses, IOS versions, and types of devices

CDP Overview

Cisco Discovery Protocol (CDP) is a Cisco proprietary Layer 2 protocol that is used to gather information about Cisco devices which share the same data link. CDP is media and protocol independent and runs on all Cisco devices, such as routers, switches, and access servers.

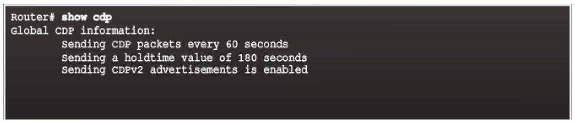
The device sends periodic CDP advertisements to connected devices, as shown in the figure. These advertisements share information about the type of device that is discovered, the name of the devices, and the number and type of the interfaces.

Because most network devices are connected to other devices, CDP can assist in network design decisions, troubleshooting, and making changes to equipment. CDP can also be used as a network discovery tool to determine the information about the neighboring devices. This information gathered from CDP can help build a logical topology of a network when documentation is missing or lacking in detail.

For Cisco devices, CDP is enabled by default. For security reasons, it may be desirable to disable CDP on a network device globally, or per interface. With CDP, an attacker can gather valuable insight about the network layout, such as IP addresses, IOS versions, and types of devices.

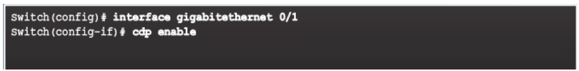
Device Discovery with CDP

Configure and Verify CDP



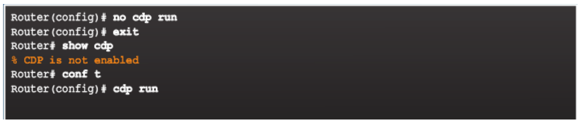
```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

Verify status and display information



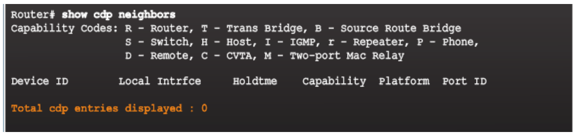
```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# cdp enable
```

Enables CDP on interface (**no CDP enable** disables)



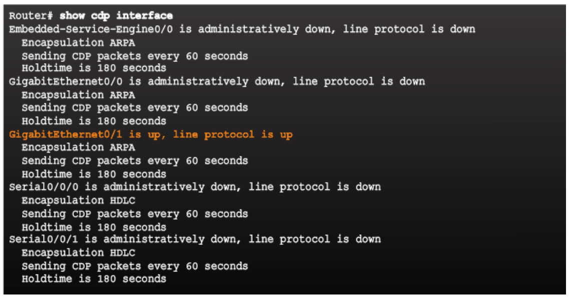
```
Router(config)# no cdp run
Router(config)# exit
Router# show cdp
% CDP is not enabled
Router# conf t
Router(config)# cdp run
```

no cdp run globally disables (**cdp run** enables)



```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Total cdp entries displayed : 0
```

No neighbors detected



```
Router# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/0 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/1 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Indicates the interfaces with CDP enabled

Configure and Verify CDP

To verify the status of CDP and display information about CDP, enter the **show cdp** command, as displayed in the 1st figure (left).

To enable CDP globally for all the supported interfaces on the device, enter **cdp run** in the global configuration mode. CDP can be disabled for all the interfaces on the device with the **no cdp run** command in the global configuration mode.

To disable CDP on a specific interface, such as the interface facing an ISP, enter **no cdp enable** in the interface configuration mode. CDP is still enabled on the device; however, no more CDP advertisements will be sent out that interface. To enable CDP on the specific interface again, enter **cdp enable**, as shown in the 2nd figure (left).

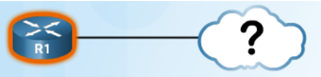
The 3th figure (left) shows CDP disabled globally using the command **no cdp run** and re-enabled using the **cdp run** command.

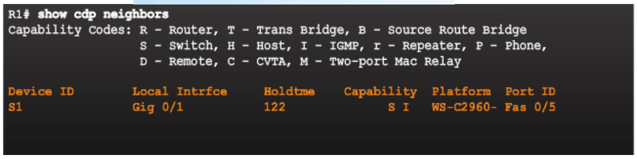
To verify the status of CDP and display a list of neighbors, use the **show cdp neighbors** command in the privileged EXEC mode. The **show cdp neighbors** command displays important information about the CDP neighbors. Currently, this device does not have any neighbors because it is not physically connected to any devices, as indicated by the results of the **show cdp neighbors** command displayed in the 4th figure (right).

Use the **show cdp interface** command to display the interfaces that are CDP enabled on a device. The status of each interface is also displayed. The last figure (right) shows that five interfaces are CDP enabled on the router with only one active connection to another device.

Device Discovery with CDP

Discover Devices Using CDP

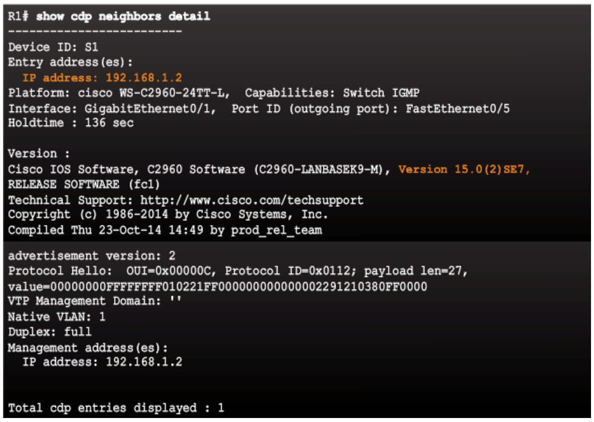




```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Gig 0/1           122              S I   WS-C2960- Fas 0/5
```

show cdp neighbors discovers:

- S1 (Device ID)
- Gig 0/1 (local port identifier)
- Fas 0/5 (remote port identified)
- S for switch (R for router)
- WS-C2960 (hardware platform)



```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team
advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010221FF000000000000002291210380FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 192.168.1.2


Total cdp entries displayed : 1
```

show cdp neighbors detail command provides additional information:

- IPv4 address
- IOS version

Discover Devices Using CDP

With CDP enabled on the network, the **show cdp neighbors** command can be used to determine the network layout.

For example, consider the lack of documentation in the topology shown in Figure 1. No information is available regarding the rest of the network. The **show cdp neighbors** command provides helpful information about each CDP neighbor device, including the following:

Device identifiers - The host name of the neighbor device (S1)

Port identifier - The name of the local and remote port (Gig 0/1 and Fas 0/5, respectively)

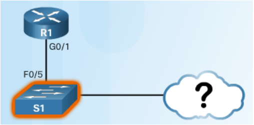
Capabilities list - Whether the device is a router or a switch (S for switch; I for IGMP is beyond scope for this course)

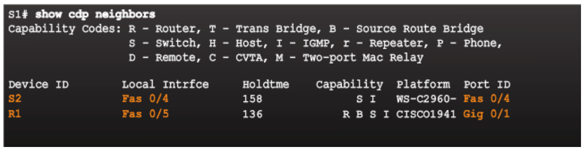
Platform - The hardware platform of the device (WS-C2960 for Cisco 2960 switch)

If more information is needed, the **show cdp neighbors** detail command can also provide information, such as the neighbors’ IOS version and IPv4 address, as displayed in Figure 2

Device Discovery with CDP

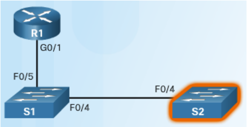
Discover Devices Using CDP (Cont.)

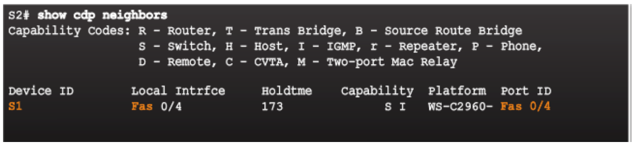




```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S2               Fas 0/4           158              S I   WS-C2960- Fas 0/4
R1               Fas 0/5           136          R B S I   CISCO1941 Gig 0/1
```

- Other devices connected to S1 can be determined
- S2 is revealed in the output!



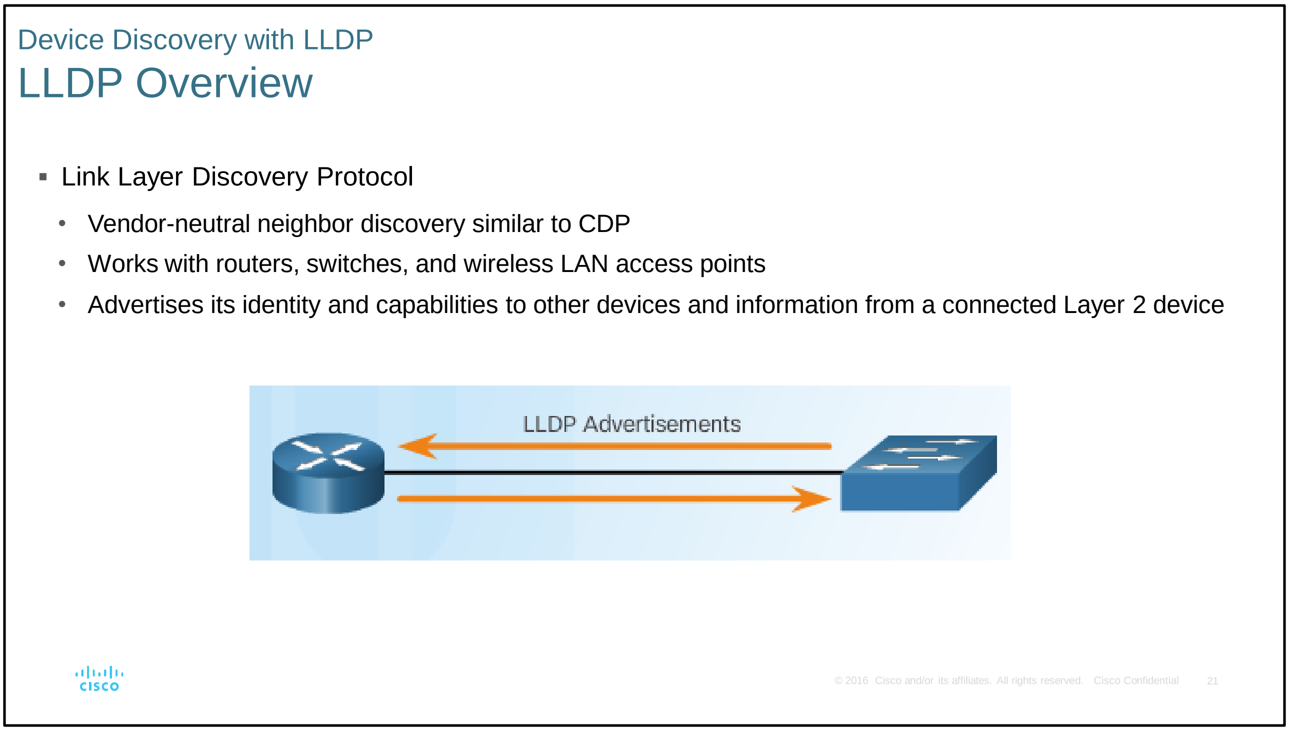


```
S2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Fas 0/4           173              S I   WS-C2960- Fas 0/4
```

- No more devices to discover!

By accessing S1 either remotely through SSH or physically through the console port, a network administrator can determine the other devices connected to S1, as displayed in the output of the **show cdp neighbors** in Figure 1.

Another switch, S2, is revealed in the output. The network administrator then accesses S2 and displays the CDP neighbors, as shown in Figure 2 The only device connected to S2 is S1. Therefore, there are no more devices to discover in the topology. The network administrator can now update the documentation to reflect the discovered devices.



Device Discovery with LLDP

LLDP Overview

- Link Layer Discovery Protocol
  - Vendor-neutral neighbor discovery similar to CDP
  - Works with routers, switches, and wireless LAN access points
  - Advertises its identity and capabilities to other devices and information from a connected Layer 2 device

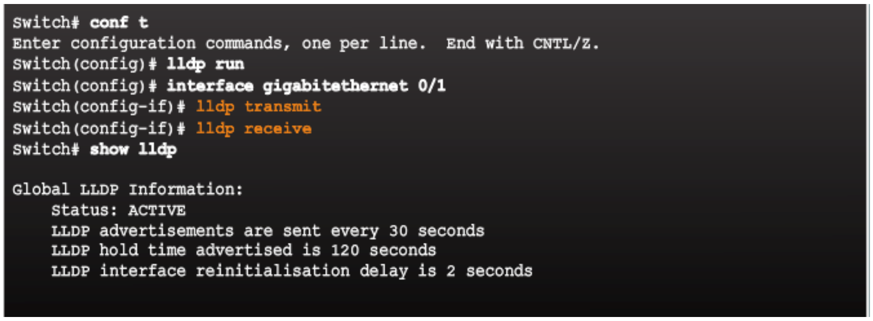
LLDP Overview

Cisco devices also support Link Layer Discovery Protocol (LLDP), which is a vendor-neutral neighbor discovery protocol similar to CDP.

LLDP works with network devices, such as routers, switches, and wireless LAN access points. This protocol advertises its identity and capabilities to other devices and receives the information from a physically connected Layer 2 device.

Device Discovery with LLDP

Configure and Verify LLDP



```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

- **lldp run** enables globally
- LLDP can be configured on separate interfaces, configured separately to transmit and receive
- To disable LLDP globally – **no lldp run**

Configure and Verify LLDP

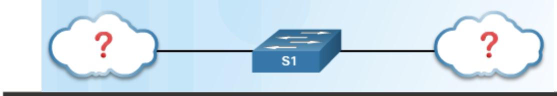
Depending on the device, LLDP may be enabled by default. To enable LLDP globally on a Cisco network device, enter the **lldp run** command in the global configuration mode. To disable LLDP, enter the **no lldp run** command in the global configuration mode.

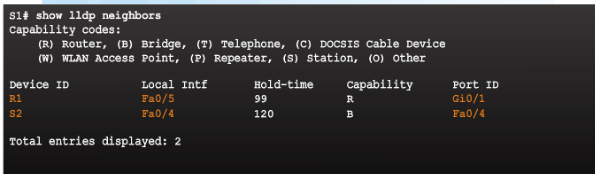
Similar to CDP, LLDP can be configured on specific interfaces. However, LLDP must be configured separately to transmit and receive LLDP packets, as shown in Figure 1.

To verify LLDP has been enabled on the device, enter the **show lldp** command in the privileged EXEC mode.

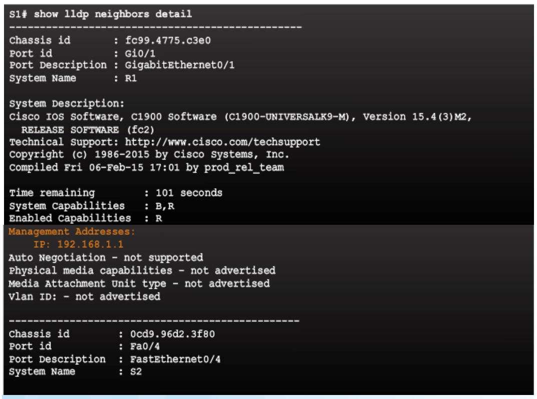
Device Discovery with LLDP

Discover Devices Using LLDP

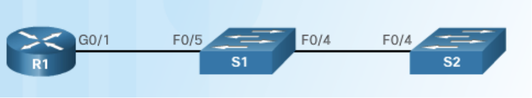




```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf       Hold-time     Capability      Port ID
R1                  Fa0/5            99            R               Gi0/1
S2                  Fa0/4            120           B               Fa0/4

Total entries displayed: 2
```



```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id       : fc99.4775.c3e0
Port id          : Gi0/1
Port Description : GigabitEthernet0/1
System Name      : R1

System Description:
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M2,
  RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 06-Feb-15 17:01 by prod_rel_team

Time remaining        : 101 seconds
System Capabilities   : B,R
Enabled Capabilities  : R
Management Addresses:
    IP: 192.168.1.1
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: - not advertised

------------------------------------------------
Chassis id        : 0cd9.96d2.3f80
Port id           : Fa0/4
Port Description  : FastEthernet0/4
System Name       : S2
```

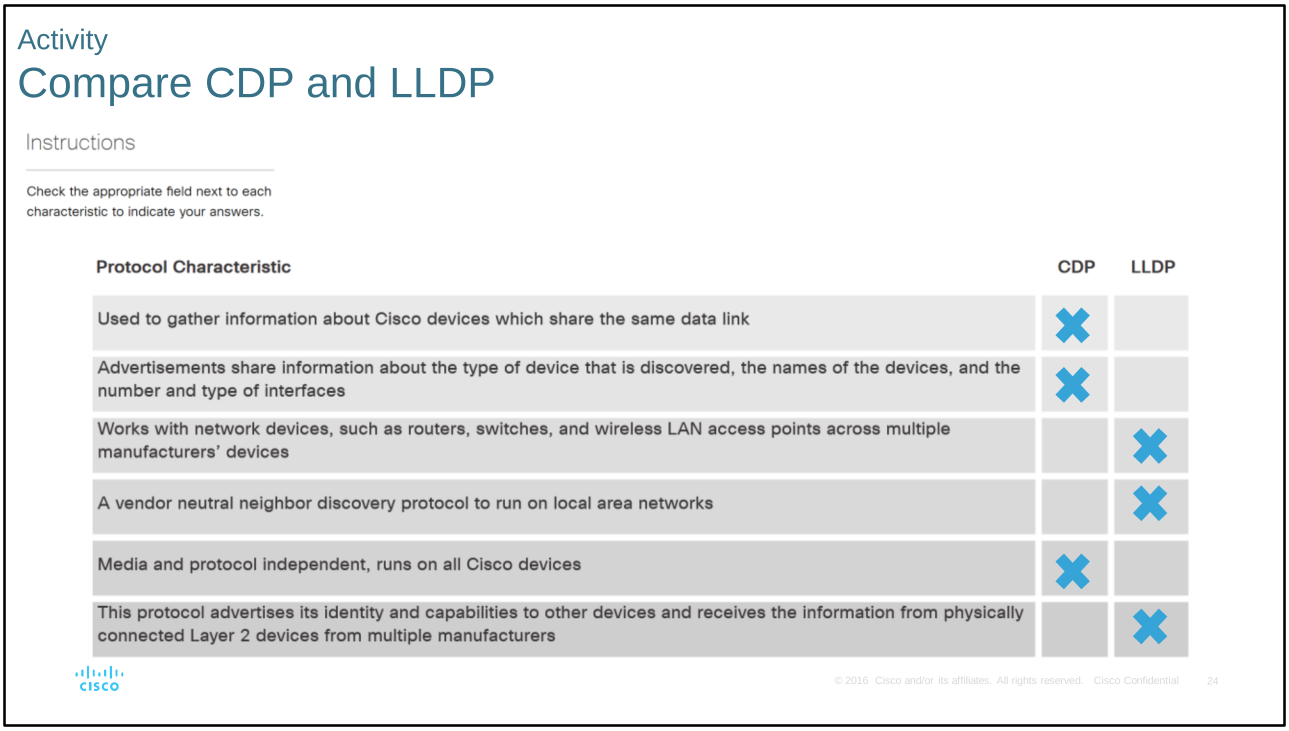


Discover Devices Using LLDP

With LLDP enabled, device neighbors can be discovered using the **show lldp neighbors** command. For example, consider the lack of documentation in the topology shown in Figure 1. The network administrator only knows that S1 is connected to two devices. Using the **show lldp neighbors** command, the network administrator discovers that S1 has a router and a switch as a neighbors.

Note: The letter B under capability for S2 represents a Bridge. For this output, the word bridge can also mean switch.

From the results of **show lldp neighbors**, a topology from switch S1 can be constructed as depicted in Figure 2. When more details about the neighbors are needed, the **show lldp neighbors detail** command can provide information, such as the neighbors’ IOS version, IP address, and device capability.



Activity

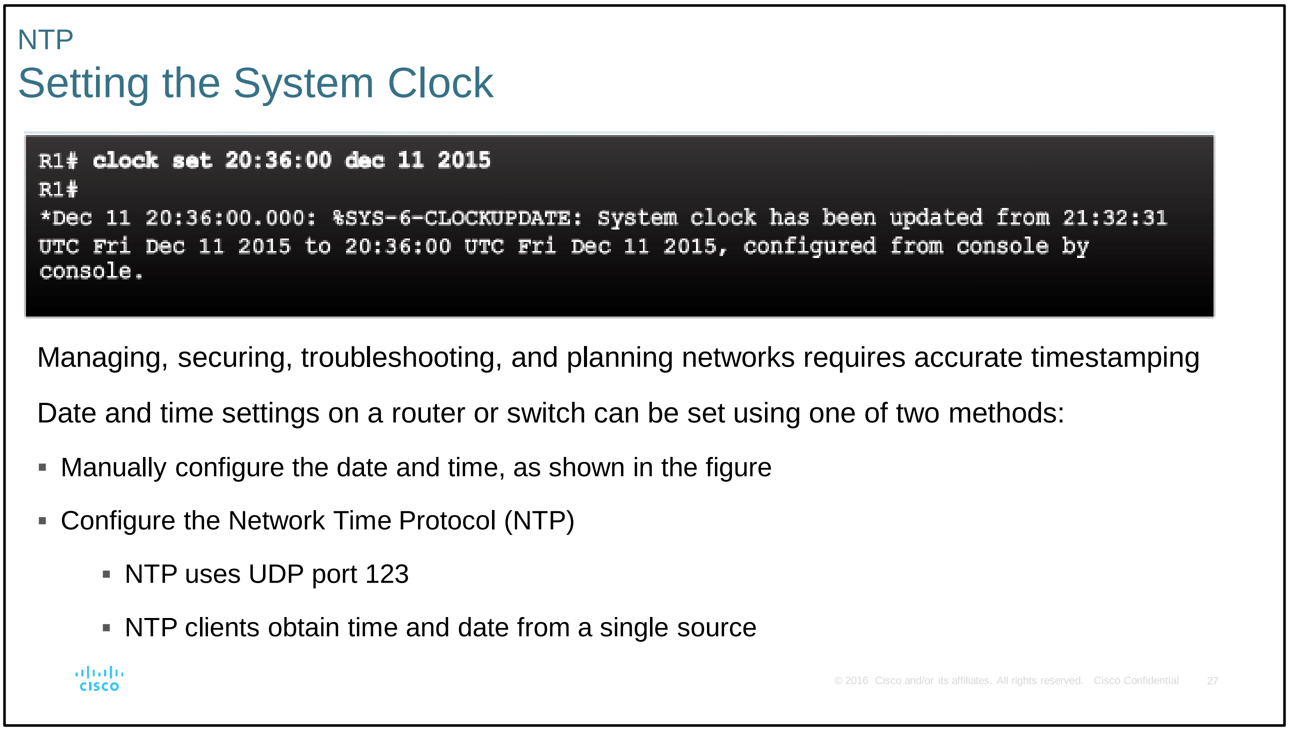
Compare CDP and LLDP

Instructions

Check the appropriate field next to each characteristic to indicate your answers.

Protocol Characteristic	CDP	LLDP
Used to gather information about Cisco devices which share the same data link	✖	
Advertisements share information about the type of device that is discovered, the names of the devices, and the number and type of interfaces	✖	
Works with network devices, such as routers, switches, and wireless LAN access points across multiple manufacturers' devices		✖
A vendor neutral neighbor discovery protocol to run on local area networks		✖
Media and protocol independent, runs on all Cisco devices	✖	
This protocol advertises its identity and capabilities to other devices and receives the information from physically connected Layer 2 devices from multiple manufacturers		✖

Device Management



NTP

Setting the System Clock

```
R1# clock set 20:36:00 dec 11 2015
R1#
*Dec 11 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 21:32:31
UTC Fri Dec 11 2015 to 20:36:00 UTC Fri Dec 11 2015, configured from console by
console.
```

Managing, securing, troubleshooting, and planning networks requires accurate timestamping

Date and time settings on a router or switch can be set using one of two methods:

- Manually configure the date and time, as shown in the figure
- Configure the Network Time Protocol (NTP)
  - NTP uses UDP port 123
  - NTP clients obtain time and date from a single source

Setting the System Clock

The software clock on a router or switch starts when the system boots and is the primary source of time for the system. It is important to synchronize the time across all devices on the network because all aspects of managing, securing, troubleshooting, and planning networks require accurate timestamping. When the time is not synchronized between devices, it will be impossible to determine the order of the events and the cause of an event.

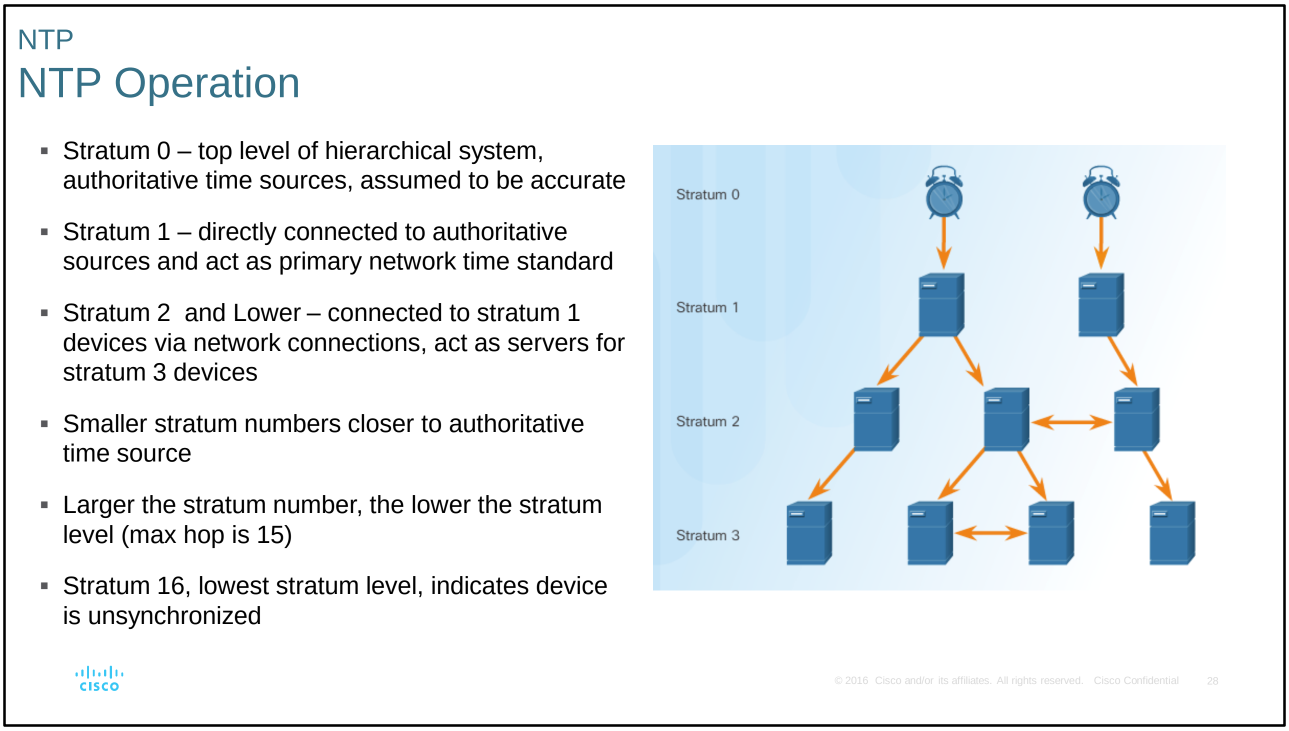
Typically, the date and time settings on a router or switch can be set using one of two methods:

- Manually configure the date and time, as shown in the figure
- Configure the Network Time Protocol (NTP)

As a network grows, it becomes difficult to ensure that all infrastructure devices are operating with synchronized time. Even in a smaller network environment, the manual method is not ideal. If a router reboots, how will it get an accurate date and timestamp?

A better solution is to configure the NTP on the network. This protocol allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent time settings. When NTP is implemented in the network, it can be set up to synchronize to a private master clock or it can synchronize to a publicly available NTP server on the Internet.

NTP uses UDP port 123 and is documented in RFC 1305.



NTP

NTP Operation

- Stratum 0 – top level of hierarchical system, authoritative time sources, assumed to be accurate
- Stratum 1 – directly connected to authoritative sources and act as primary network time standard
- Stratum 2 and Lower – connected to stratum 1 devices via network connections, act as servers for stratum 3 devices
- Smaller stratum numbers closer to authoritative time source
- Larger the stratum number, the lower the stratum level (max hop is 15)
- Stratum 16, lowest stratum level, indicates device is unsynchronized

NTP Operation

NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum level is defined as the number of hop counts from the authoritative source. The synchronized time is distributed across the network using NTP. The figure displays a sample NTP network.

NTP servers arranged in three levels showing the three strata. Stratum 1 is connected to Stratum 0 clocks.

Stratum 0

An NTP network gets the time from authoritative time sources. These authoritative time sources, also referred to as stratum 0 devices, are high-precision timekeeping devices assumed to be accurate and with little or no delay associated with them. Stratum 0 devices are represented by the clock in the figure.

Stratum 1

The stratum 1 devices are directly connected to the authoritative time sources. They act as the primary network time standard.

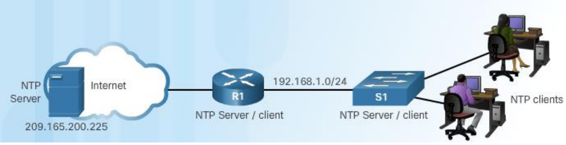
Stratum 2 and Lower

The stratum 2 servers are connected to stratum 1 devices through network connections. Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.

Smaller stratum numbers indicate that the server is closer to the authorized time source than larger stratum numbers. The larger the stratum number, the lower the stratum level. The max hop count is 15. Stratum 16, the lowest stratum level, indicates that a device is unsynchronized. Time servers on the same stratum level can be configured to act as a peer with other time servers on the same stratum level for backup or verification of time.

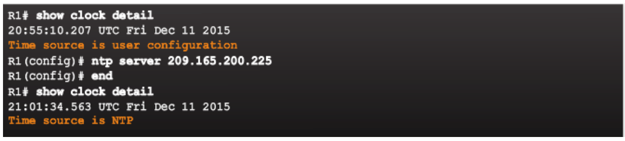
NTP

Configure and Verify NTP



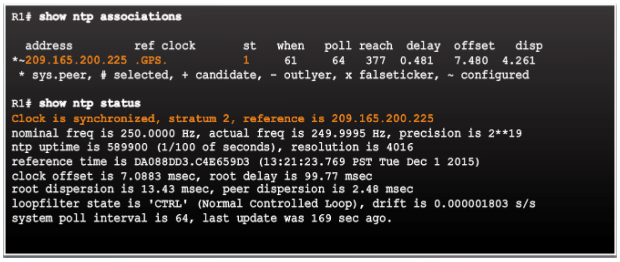
R1 is synchronized with a stratum 1 NTP server at 209.165.200.225 which is synchronized with a GPS clock

- R1 - Configure Stratum 2 NTP Server



```
R1# show clock detail
20:55:10.207 UTC Fri Dec 11 2015
Time source is user configuration
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Dec 11 2015
Time source is NTP
```

- R1 - Verify NTP Server Configuration



```
R1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~209.165.200.225 .GPS.           1     61     64   377  0.481   7.480  4.261
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Tue Dec 1 2015)
clock offset is 7.0883 msec, root delay is 99.77 msec
root dispersion is 13.43 msec, peer dispersion is 2.48 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803 s/s
system poll interval is 64, last update was 169 sec ago.
```

Configure and Verify NTP

Before NTP is configured on the network, the **show clock** command displays the current time on the software clock. With the **detail** option, the time source is also displayed. As shown in Figure 1, the software clock has been manually configured.

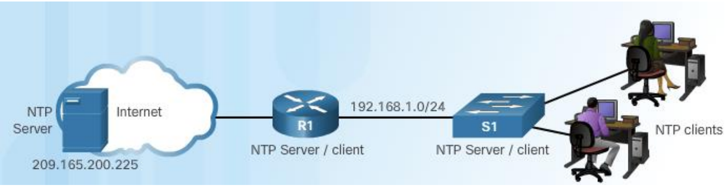
Use the **ntp server** *ip-address* command in global configuration mode to configure 209.165.200.225 as the NTP server for R1. To verify the time source is set to NTP, use the **show clock detail** command again.

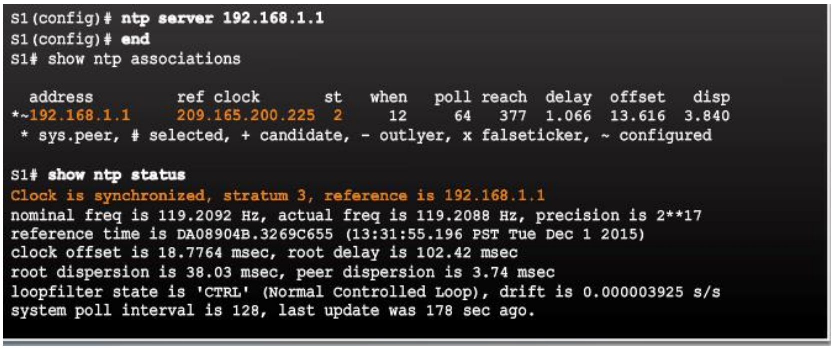
As shown in Figure 2, use the **show ntp associations** and **show ntp status** commands to verify that R1 is synchronized with the NTP server at 209.165.200.225. Notice that R1 is synchronized with a stratum 1 NTP server at 209.165.200.225, which is synchronized with a GPS clock. The **show ntp status** command displays that R1 is now a stratum 2 device synchronized with the NTP server at 209.165.220.225.

NTP

Configure and Verify NTP (Cont.)

- Configure Stratum 3 NTP Server

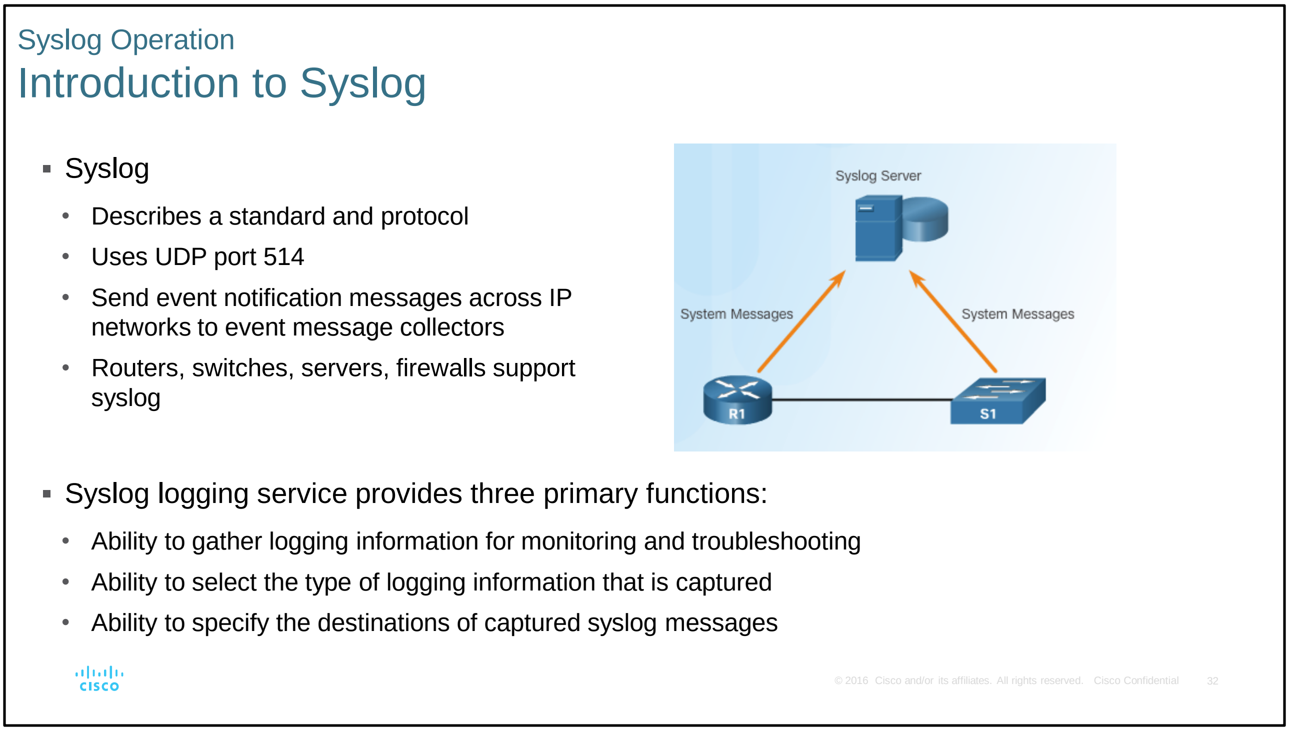




```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.168.1.1     209.165.200.225  2     12     64   377  1.066  13.616  3.840
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Dec 1 2015)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 msec, peer dispersion is 3.74 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003925 s/s
system poll interval is 128, last update was 178 sec ago.
```

- R1 is a stratum 2 device and NTP server to S1
- S1 is a stratum 3 device that can provide NTP service to end devices

The clock on S1 is configured to synchronize to R1, as shown in figure. Output from the **show ntp associations** command verifies that the clock on S1 is now synchronized with R1 at 192.168.1.1 via NTP. R1 is a stratum 2 device and NTP server to S1. Now S1 is a stratum 3 device that can provide NTP service to other devices in the network, such as end devices.



Syslog Operation

Introduction to Syslog

- Syslog
  - Describes a standard and protocol
  - Uses UDP port 514
  - Send event notification messages across IP networks to event message collectors
  - Routers, switches, servers, firewalls support syslog
- Syslog logging service provides three primary functions:
  - Ability to gather logging information for monitoring and troubleshooting
  - Ability to select the type of logging information that is captured
  - Ability to specify the destinations of captured syslog messages

Introduction to Syslog

When certain events occur on a network, networking devices have trusted mechanisms to notify the administrator with detailed system messages. These messages can be either non-critical or significant. Network administrators have a variety of options for storing, interpreting, and displaying these messages, and for being alerted to those messages that could have the greatest impact on the network infrastructure.

The most common method of accessing system messages is to use a protocol called syslog.

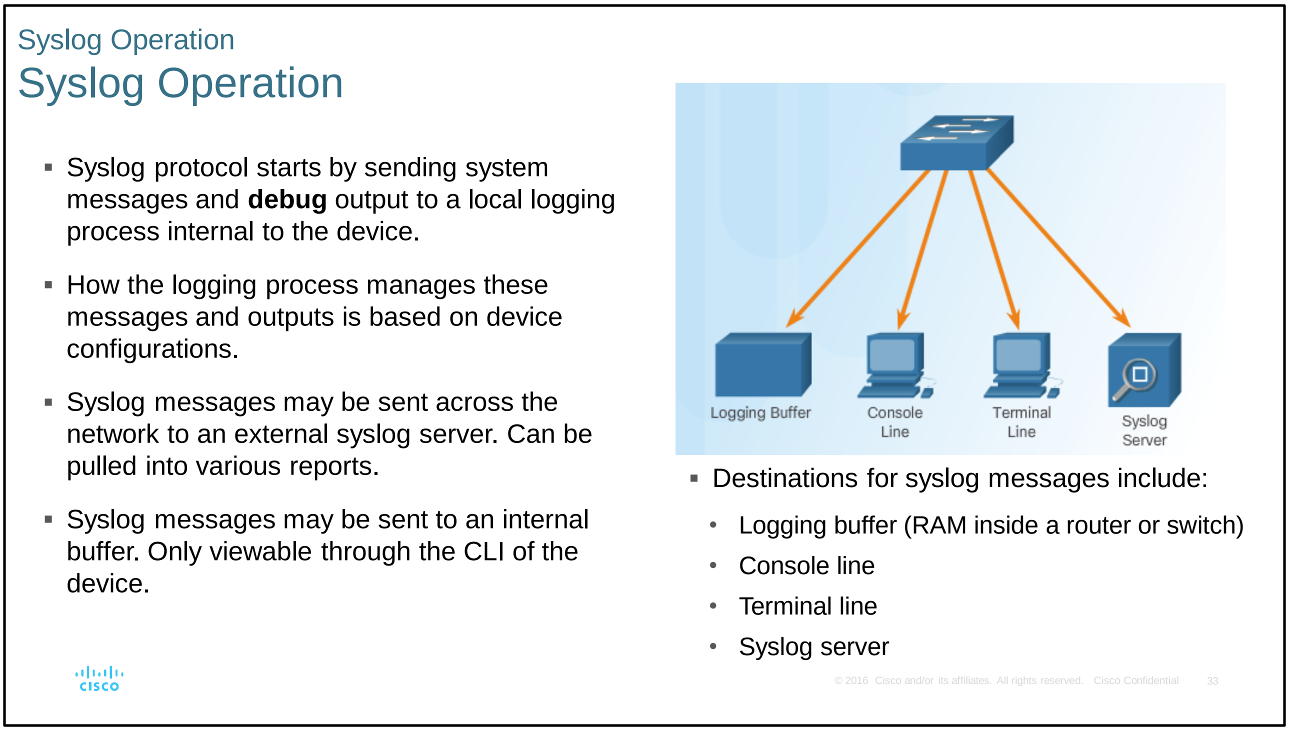
Syslog is a term used to describe a standard. It is also used to describe the protocol developed for that standard. The syslog protocol was developed for UNIX systems in the 1980s, but was first documented as RFC 3164 by IETF in 2001. Syslog uses UDP port 514 to send event notification messages across IP networks to event message collectors, as illustrated in the figure.

Many networking devices support syslog, including routers, switches, application servers, firewalls, and other network appliances. The syslog protocol allows networking devices to send their system messages across the network to syslog servers.

There are several different syslog server software packages for Windows and UNIX. Many of them are freeware.

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

Syslog Operation

- Syslog protocol starts by sending system messages and **debug** output to a local logging process internal to the device.
- How the logging process manages these messages and outputs is based on device configurations.
- Syslog messages may be sent across the network to an external syslog server. Can be pulled into various reports.
- Syslog messages may be sent to an internal buffer. Only viewable through the CLI of the device.

- Destinations for syslog messages include:
  - Logging buffer (RAM inside a router or switch)
  - Console line
  - Terminal line
  - Syslog server

Syslog Operation

The syslog protocol starts by sending system messages and **debug** output to a local logging process internal to the device. How the logging process manages these messages and outputs is based on device configurations. For example, syslog messages may be sent across the network to an external syslog server. These messages can be retrieved without the need of accessing the actual device. Log messages and outputs stored on the external server can be pulled into various reports for easier reading.

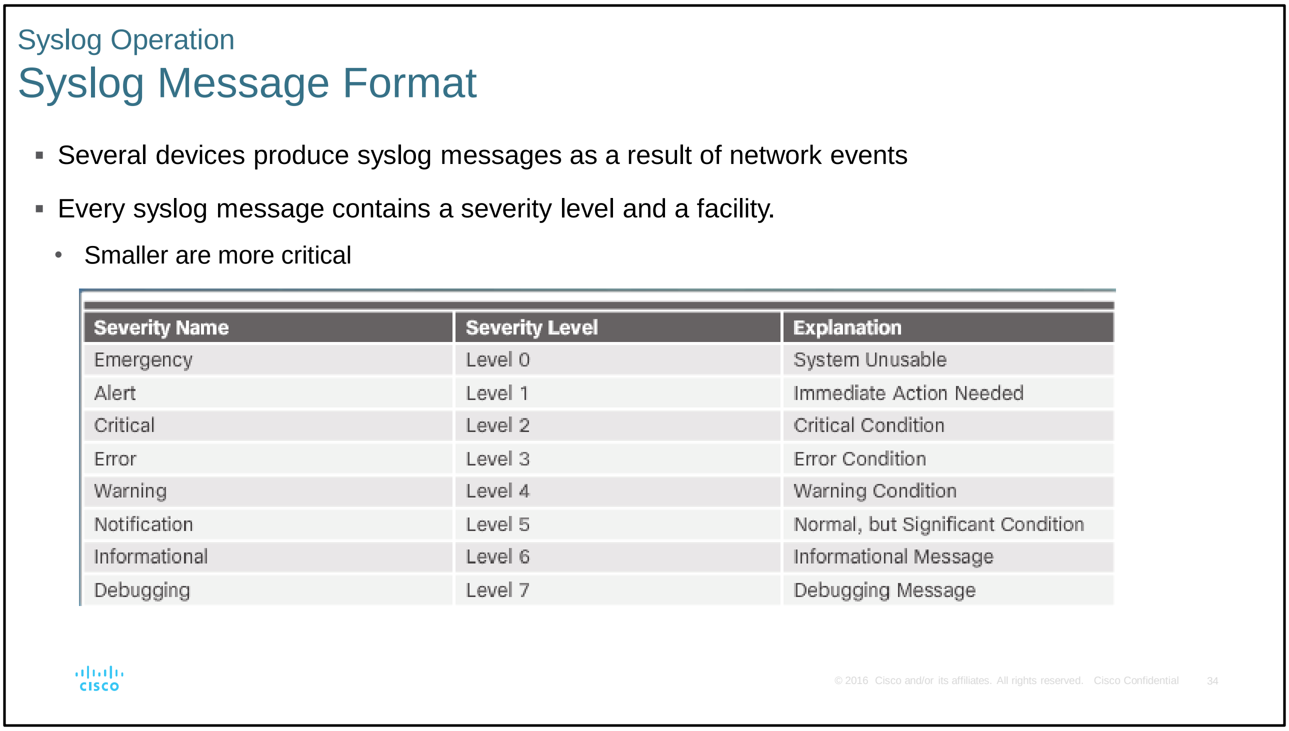
Alternatively, syslog messages may be sent to an internal buffer. Messages sent to the internal buffer are only viewable through the CLI of the device.

Finally, the network administrator may specify that only certain types of system messages are sent to various destinations. For example, the device may be configured to forward all system messages to an external syslog server. However, debug-level messages are forwarded to the internal buffer and are only accessible by the administrator from the CLI.

As shown in the figure, popular destinations for syslog messages include:

- Logging buffer (RAM inside a router or switch)
- Console line
- Terminal line
- Syslog server

It is possible to remotely monitor system messages by viewing the logs on a syslog server, or by accessing the device through Telnet, SSH, or through the console port.



Syslog Operation

Syslog Message Format

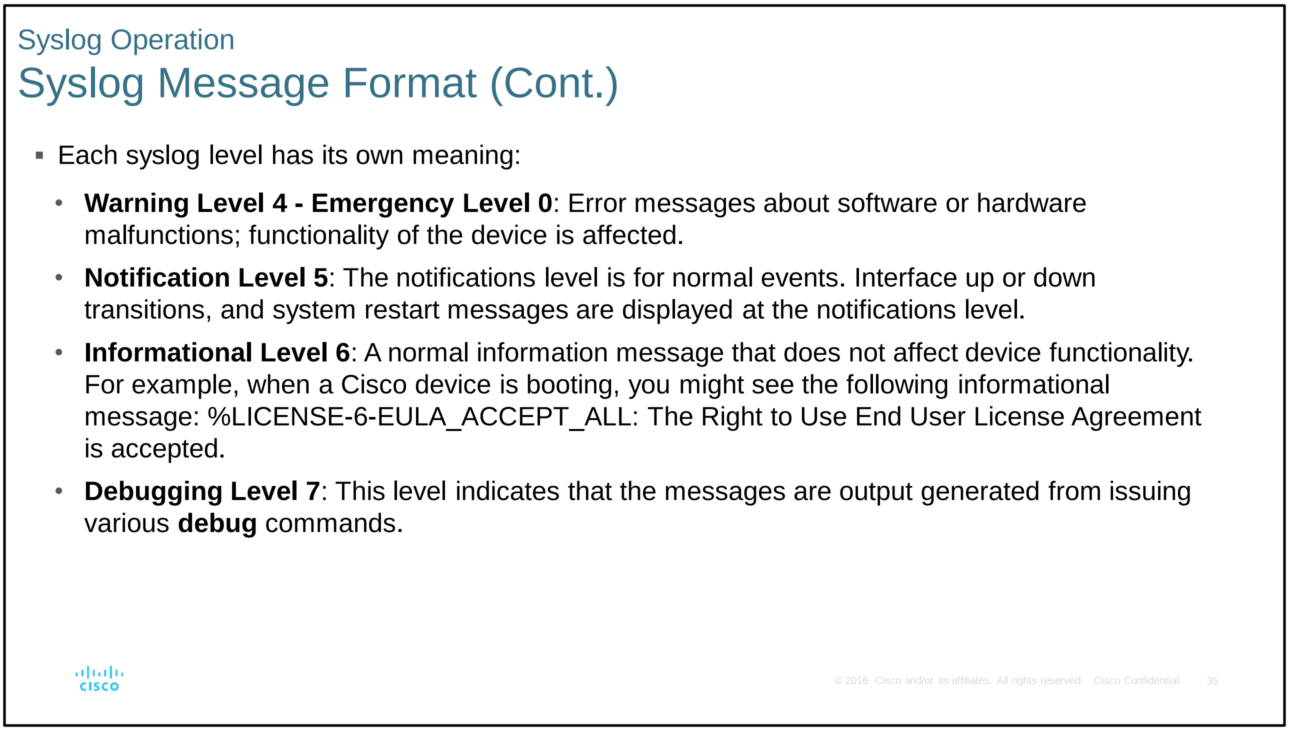
- Several devices produce syslog messages as a result of network events
- Every syslog message contains a severity level and a facility.
  - Smaller are more critical

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Syslog Message Format

Several devices produce syslog messages as a result of network events. Every syslog message contains a severity level and a facility.

The smaller numerical levels are the more critical syslog alarms. The severity level of the messages can be set to control where each type of message is displayed (i.e. on the console or the other destinations). The complete list of syslog levels is shown in Figure 1.



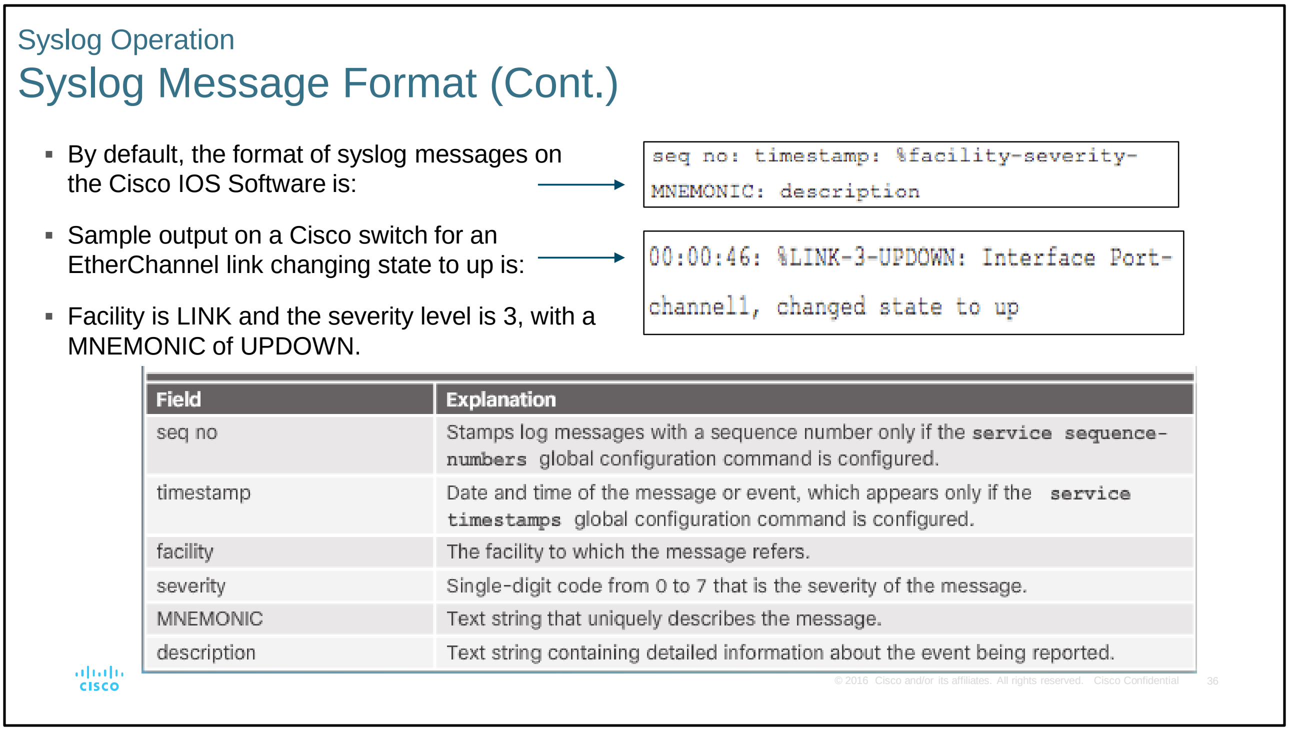
Syslog Operation

Syslog Message Format (Cont.)

- Each syslog level has its own meaning:
  - **Warning Level 4 - Emergency Level 0**: Error messages about software or hardware malfunctions; functionality of the device is affected.
  - **Notification Level 5**: The notifications level is for normal events. Interface up or down transitions, and system restart messages are displayed at the notifications level.
  - **Informational Level 6**: A normal information message that does not affect device functionality. For example, when a Cisco device is booting, you might see the following informational message: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.
  - **Debugging Level 7**: This level indicates that the messages are output generated from issuing various **debug** commands.

Each syslog level has its own meaning:

- **Warning Level 4 to Emergency Level 0**: These messages are error messages about software or hardware malfunctions; these types of messages mean that the functionality of the device is affected. The severity of the issue determines the actual syslog level applied.
- **Notification Level 5**: The notifications level is for normal, but significant events. For example, interface up or down transitions, and system restart messages are displayed at the notifications level.
- **Informational Level 6**: A normal information message that does not affect device functionality. For example, when a Cisco device is booting, you might see the following informational message: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.
- **Debugging Level 7**: This level indicates that the messages are output generated from issuing various **debug** commands.



Syslog Operation

Syslog Message Format (Cont.)

- By default, the format of syslog messages on the Cisco IOS Software is: →

```
seq no: timestamp: %facility-severity-
MNEMONIC: description
```

- Sample output on a Cisco switch for an EtherChannel link changing state to up is: →

```
00:00:46: %LINK-3-UPDOWN: Interface Port-
channel1, changed state to up
```

- Facility is LINK and the severity level is 3, with a MNEMONIC of UPDOWN.

Field	Explanation
seq no	Stamps log messages with a sequence number only if the `service sequence-numbers` global configuration command is configured.
timestamp	Date and time of the message or event, which appears only if the `service timestamps` global configuration command is configured.
facility	The facility to which the message refers.
severity	Single-digit code from 0 to 7 that is the severity of the message.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

In addition to specifying the severity, syslog messages also contain information on the facility. Syslog facilities are service identifiers that identify and categorize system state data for error and event message reporting. The logging facility options that are available are specific to the networking device. For example, Cisco 2960 Series switches running Cisco IOS Release 15.0(2) and Cisco 1941 routers running Cisco IOS Release 15.2(4) support 24 facility options that are categorized into 12 facility types. Some common syslog message facilities reported on Cisco IOS routers include:

- IP
- OSPF protocol
- SYS operating system
- IP security (IPsec)
- Interface IP (IF)

By default, the format of syslog messages on the Cisco IOS Software is as follows:

```
 – seq no: timestamp: %facility-severity-MNEMONIC:
description
```

The fields contained in the Cisco IOS Software syslog message are explained in Figure. For example, sample output on a Cisco switch for an EtherChannel link changing state to up is:

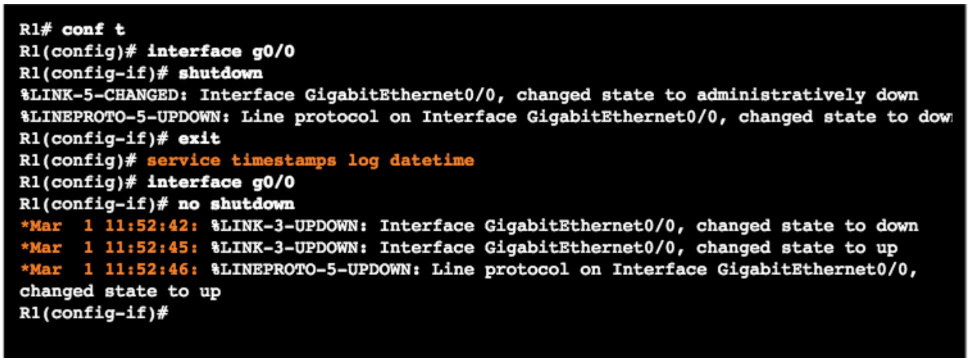
```
- 00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Here the facility is LINK and the severity level is 3, with a MNEMONIC of UPDOWN. The most common messages are link up and down messages, and messages that a device produces when it exits from configuration mode. If ACL logging is configured, the device generates syslog messages when packets match a parameter condition.

Syslog Operation

Service Timestamp

- By default, log messages are not timestamped
- Log messages should be timestamped so when sent to destination (syslog server) there is a record of when the message was generated
- Notice date below once timestamp is activated



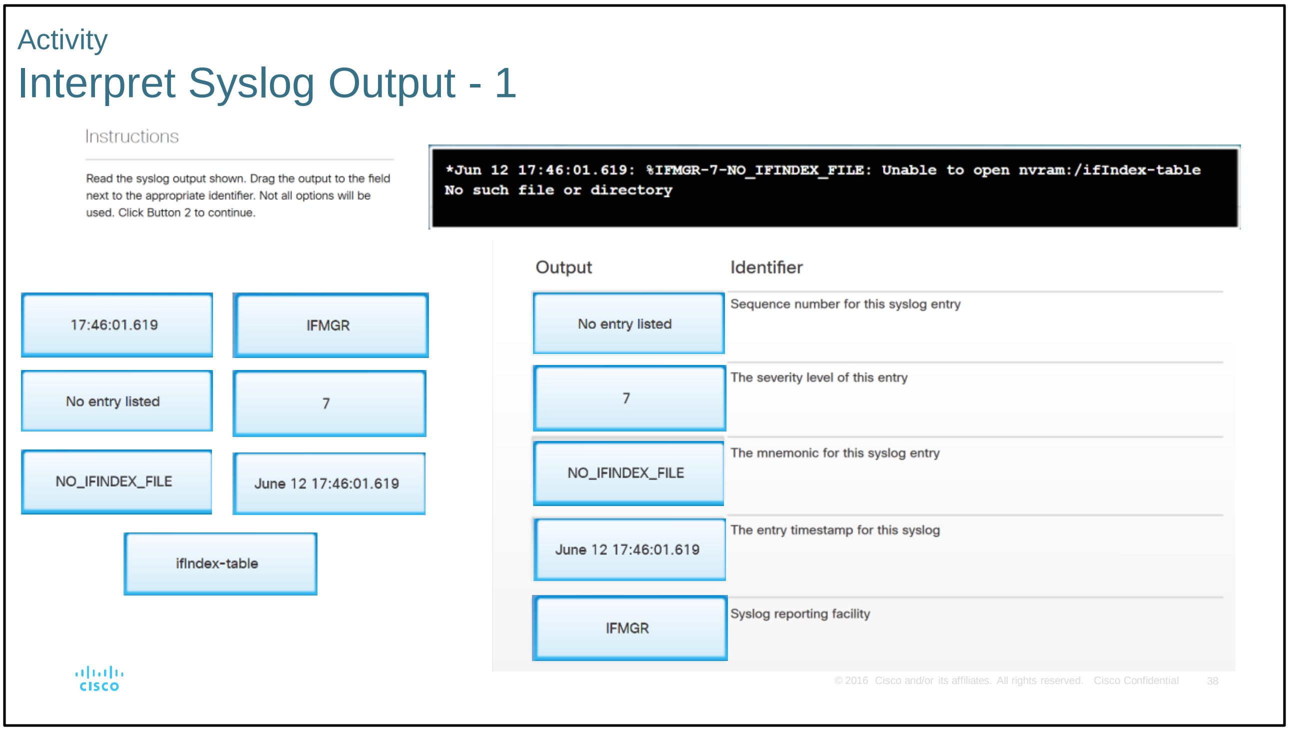
```
R1# conf t
R1(config)# interface g0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to dow
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar  1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Mar  1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Mar  1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)#
```

Service Timestamp

By default, log messages are not timestamped. For example, in the figure, the R1 GigabitEthernet 0/0 interface is shutdown. The message logged to the console does not identify when the interface state was changed. Log messages should be timestamped so that when they are sent to another destination, such as a Syslog server, there is record of when the message was generated.

Use the command **service timestamps log datetime** to force logged events to display the date and time. As shown in the figure, when the R1 GigabitEthernet 0/0 interface is reactivated, the log messages now contain the date and time.

Note: When using the **datetime** keyword, the clock on the networking device must be set, either manually or through NTP, as previously discussed.



Activity

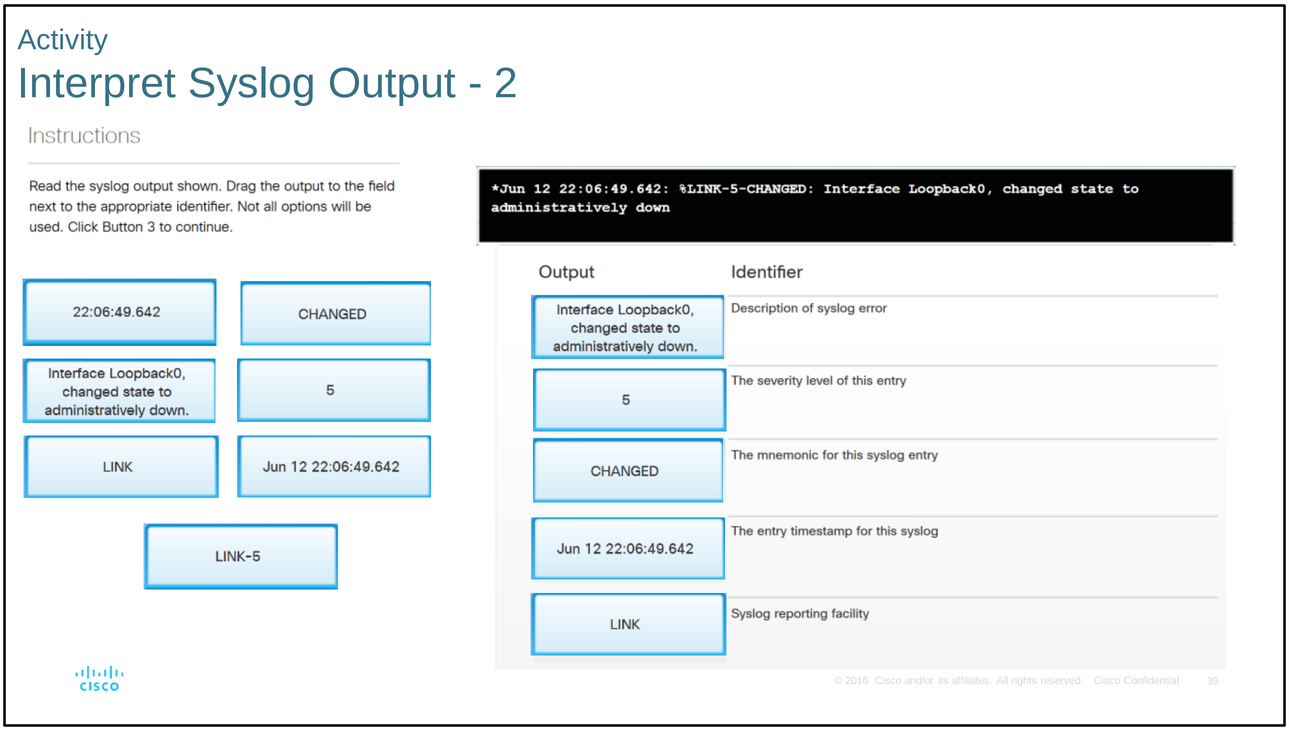
Interpret Syslog Output - 1

Instructions

Read the syslog output shown. Drag the output to the field next to the appropriate identifier. Not all options will be used. Click Button 2 to continue.

```
*Jun 12 17:46:01.619: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-table
No such file or directory
```

Output	Identifier
No entry listed	Sequence number for this syslog entry
7	The severity level of this entry
NO_IFINDEX_FILE	The mnemonic for this syslog entry
June 12 17:46:01.619	The entry timestamp for this syslog
IFMGR	Syslog reporting facility



Activity

Interpret Syslog Output - 2

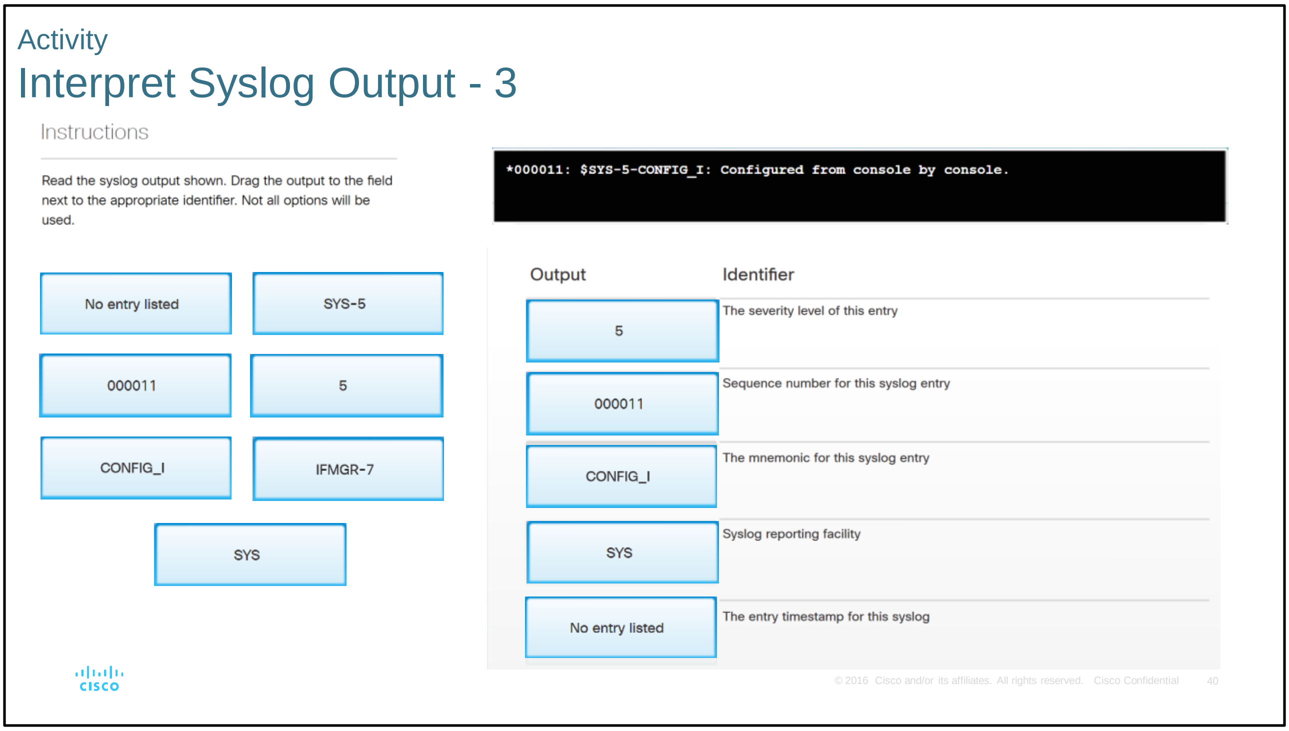
Instructions

Read the syslog output shown. Drag the output to the field next to the appropriate identifier. Not all options will be used. Click Button 3 to continue.

```
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
```

22:06:49.642
CHANGED
Interface Loopback0, changed state to administratively down.
5
LINK
Jun 12 22:06:49.642
LINK-5

Output	Identifier
Interface Loopback0, changed state to administratively down.	Description of syslog error
5	The severity level of this entry
CHANGED	The mnemonic for this syslog entry
Jun 12 22:06:49.642	The entry timestamp for this syslog
LINK	Syslog reporting facility



Activity

Interpret Syslog Output - 3

Instructions

Read the syslog output shown. Drag the output to the field next to the appropriate identifier. Not all options will be used.

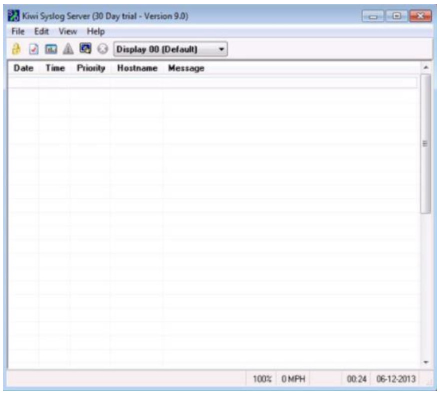
```
*000011: %SYS-5-CONFIG_I: Configured from console by console.
```

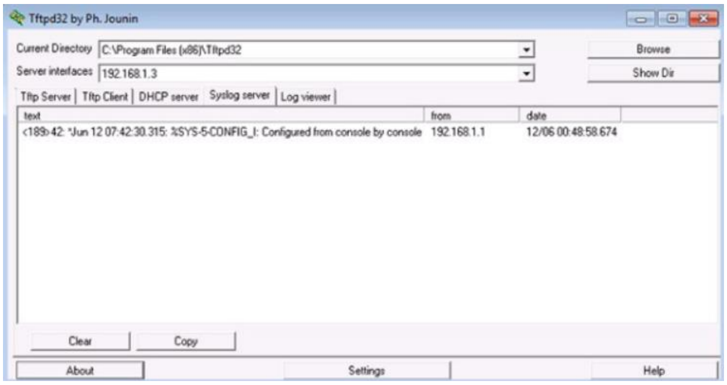
Output	Identifier
5	The severity level of this entry
000011	Sequence number for this syslog entry
CONFIG_I	The mnemonic for this syslog entry
SYS	Syslog reporting facility
No entry listed	The entry timestamp for this syslog

Syslog Configuration

Syslog Server

- To view syslog messages, a syslog server must be installed on a networked PC





Current Directory: C:\Program Files (x86)\Tftpd32

Server interfaces: 192.168.1.3

```
text                                                                      from          date
<189>42: *Jun 12 07:42:30.315: %SYS-5-CONFIG_I: Configured from console by console  192.168.1.1   12/06 00:48:58.674
```

Syslog Server

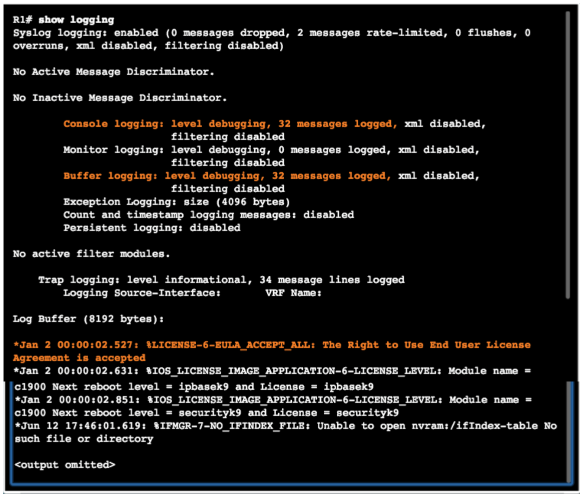
To view syslog messages, a syslog server must be installed on a workstation in the network. There are several freeware and shareware versions of syslog, as well as enterprise versions for purchase. In Figure 1 (left), an evaluation version of the Kiwi Syslog Daemon is displayed on a Windows 7 machine.

The syslog server provides a relatively user-friendly interface for viewing syslog output. The server parses the output and places the messages into pre-defined columns for easy interpretation. If timestamps are configured on the networking device sourcing the syslog messages, then the date and time of each message displays in the syslog server output, as shown in Figure 2 (right).

Network administrators can easily navigate the large amount of data compiled on a syslog server. One advantage of viewing syslog messages on a syslog server is the ability to perform granular searches through the data. Also, a network administrator can quickly delete unimportant syslog messages from the database.

Syslog Configuration

Default Logging



```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

        Console logging: level debugging, 32 messages logged, xml disabled,
                         filtering disabled
        Monitor logging: level debugging, 0 messages logged, xml disabled,
                         filtering disabled
        Buffer logging: level debugging, 32 messages logged, xml disabled,
                         filtering disabled
        Exception Logging: size (4096 bytes)
        Count and timestamp logging messages: disabled
        Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 34 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):

*Jan 2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License
Agreement is accepted
*Jan 2 00:00:02.631: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
c1900 Next reboot level = ipbasek9 and License = ipbasek9
*Jan 2 00:00:02.851: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
c1900 Next reboot level = securityk9 and License = securityk9
*Jun 12 17:46:01.619: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-table No
such file or directory

<output omitted>
```

- By default, log messages sent to the console.
- Some Cisco IOS versions buffer log messages by default too.
- First highlighted line states that this router logs to the console and includes debug messages.
  - all debug level messages, as well as any lower level messages are logged to the console
- Second highlighted line states that this router logs to an internal buffer.
- System messages that have been logged are at the end of the output.

Default Logging

By default, Cisco routers and switches send log messages for all severity levels to the console. On some IOS versions, the device also buffers log messages by default. To enable these two settings, use the **logging console** and **logging buffered** global configuration commands, respectively.

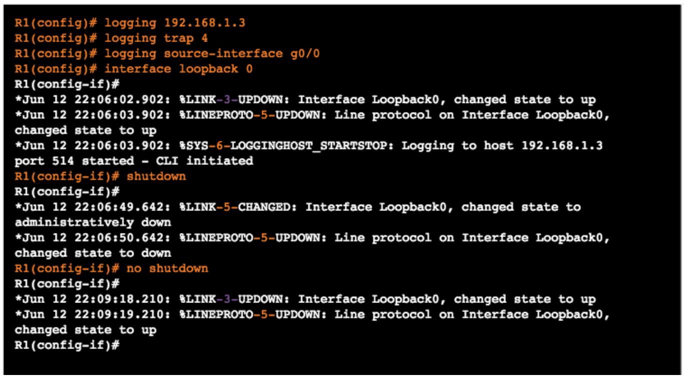
The **show logging** command displays the default logging service settings on a Cisco router, as shown in the figure. The first lines of output list information about the logging process, with the end of the output listing log messages.

The first highlighted line states that this router logs to the console and includes debug messages. This actually means that all debug level messages, as well as any lower level messages (such as notification level messages), are logged to the console. On most Cisco IOS routers, the default severity level is 7, debugging. The output also notes that 32 such messages have been logged.

The second highlighted line states that this router logs to an internal buffer. Because this router has enabled logging to an internal buffer, the **show logging** command also lists the messages in that buffer. You can view some of the system messages that have been logged at the end of the output.

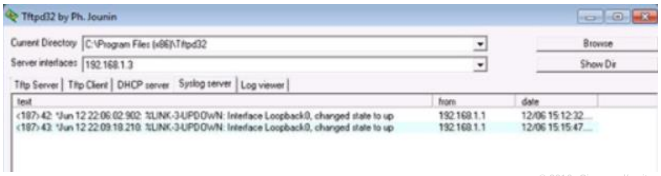
Syslog Configuration

Router and Switch Commands for Syslog Clients



```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface g0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.3
port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1(config-if)#
```

- R1 is configured to send log messages of levels 4 and lower to the syslog server at 192.168.1.3
- Source interface is set as the G0/0 interface
- Loopback interface is created, then shut down, and then brought back up
- Console output reflects these actions



Current Directory: C:\Program Files (x86)\Tftpd32

Server interfaces: 192.168.1.3

```
text                                                                        from         date
<187>42: *Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0, changed state to up   192.168.1.1  12/06 15:12:32...
<187>43: *Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0, changed state to up   192.168.1.1  12/06 15:15:47...
```

Router and Switch Commands for Syslog Clients

There are three steps to configuring the router to send system messages to a syslog server where they can be stored, filtered, and analyzed:

Step 1. In global configuration mode, use the **logging** command toconfigure the destination hostname or IPv4 address of the syslog.

Step 2. Control the messages that will be sent to the syslog server with the **logging trap** *level* global configuration mode command. For example, to limit the messages to levels 4 and lower (0 to 4), use one of the two equivalent commands.

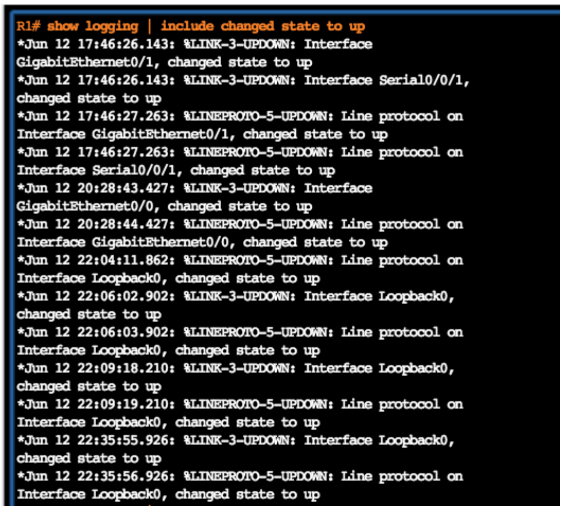
Step 3. Optionally, configure the source interface with the **logging source-interface** *interface-type interface-number* global configuration mode command. This specifies that syslog packets contain the IPv4 or IPv6 address of a specific interface, regardless of which interface the packet uses to exit the router.

In Figure 1, R1 is configured to send log messages of levels 4 and lower to the syslog server at 192.168.1.3. The source interface is set as the G0/0 interface. A loopback interface is created, then shut down, and then brought back up. The console output reflects these actions.

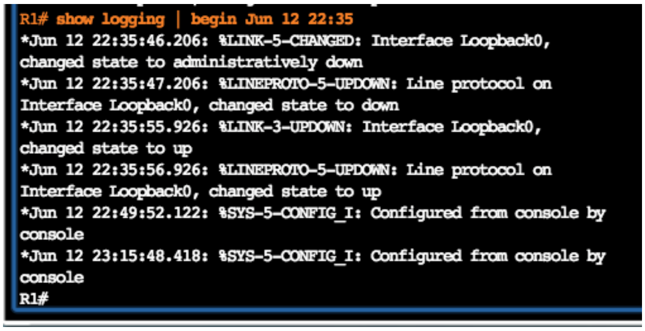
Shown in Figure 2, the Tftpd32 syslog server has been set up on a Windows 7 machine with IPv4 address 192.168.1.3. As you can see, the only messages that appear on the syslog server are those with severity level of 4 or lower (more severe). The messages with severity level of 5 or higher (less severe) appear on the router console output, but do not appear on the syslog server output, because the logging traplimits the syslog messages sent to the syslog server based on severity.

Syslog Configuration

Verifying Syslog



```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/1, changed state to up
*Jun 12 20:28:43.427: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Jun 12 20:28:44.427: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
*Jun 12 22:04:11.862: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:35:55.926: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:35:56.926: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
```



```
R1# show logging | begin Jun 12 22:35
*Jun 12 22:35:46.206: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:35:47.206: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
*Jun 12 22:35:55.926: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:35:56.926: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:49:52.122: %SYS-5-CONFIG_I: Configured from console by
console
*Jun 12 23:15:48.418: %SYS-5-CONFIG_I: Configured from console by
console
R1#
```

Verifying Syslog

You can use the **show logging** command to view any messages that are logged. When the logging buffer is large, it is helpful to use the pipe option (|) with the **show logging** command. The pipe option allows the administrator to specifically state which messages should be displayed. For example, you can use the pipe to filter only messages that **include changed state to up**, as shown in Figure 1.

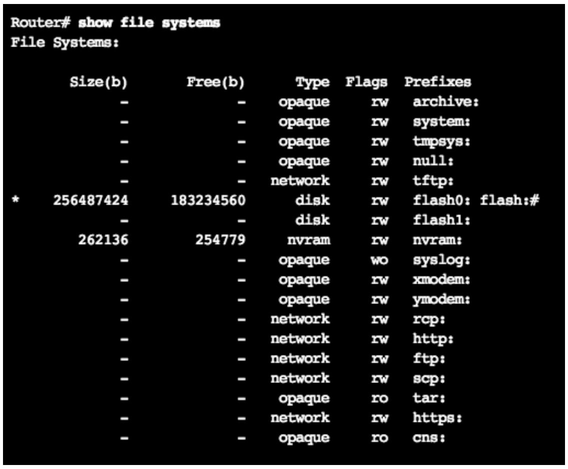
Scroll down in the output in Figure 1 to see another filtering example. To view only the messages that were logged to the buffer on or after Jun 12 10:35 PM, you would use the filter **begin June 12 22:35**.

Device Maintenance

10 – Device Discovery, Management, and Maintenance
10.3 – Device Maintenance

Router and Switch File Maintenance

Router File Systems



```
Router# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*    256487424     183234560      disk     rw   flash0: flash:#
             -             -      disk     rw   flash1:
        262136        254779     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
```

- **show file systems** lists all the available file systems
- Provides information such as memory, type of file system, and permissions (read only (ro), read and write (rw))
- Interested in tftp, flash, and nvram file systems
- Bootable IOS is located in flash so has a *

Router File Systems

The Cisco IOS File System (IFS) allows the administrator to navigate to different directories and list the files in a directory, and to create subdirectories in flash memory or on a disk. The directories available depend on the device.

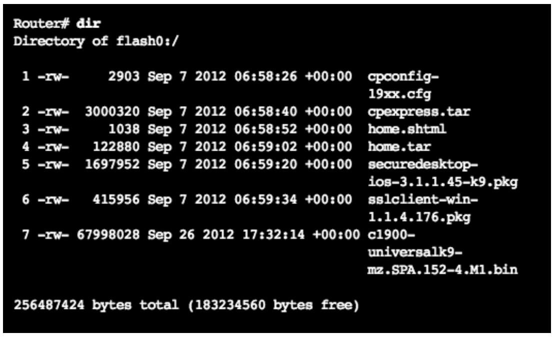
Figure 1 displays the output of the **show file systems** command, which lists all of the available file systems on a Cisco 1941 router. This command provides useful information such as the amount of available and free memory, the type of file system, and its permissions. Permissions include read only (ro), write only (wo), and read and write (rw), shown in the Flags column of the command output.

Although there are several file systems listed, of interest to us will be the tftp, flash, and nvram file systems.

Notice that the flash file system also has an asterisk preceding it. This indicates that flash is the current default file system. The bootable IOS is located in flash; therefore, the pound symbol (#) is appended to the flash listing, indicating that it is a bootable disk.

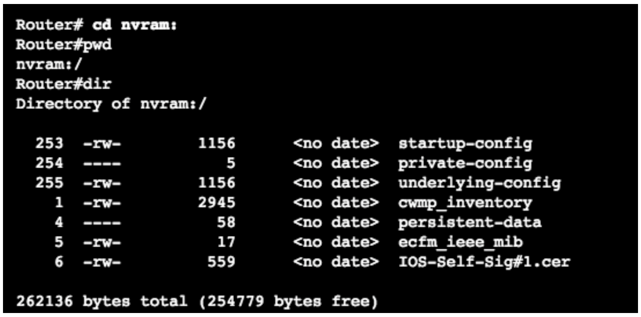
Router and Switch File Maintenance

Router File Systems (Cont.)



```
Router# dir
Directory of flash0:/

 1 -rw-     2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
                                             19xx.cfg
 2 -rw-  3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-     1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-   122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw-  1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
                                             ios-3.1.1.45-k9.pkg
 6 -rw-   415956 Sep 7 2012 06:59:34 +00:00  sslclient-win-
                                             1.1.4.176.pkg
 7 -rw- 67998028 Sep 26 2012 17:32:14 +00:00 c1900-
                                             universalk9-
                                             mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

- **dir** lists the contents of flash
- Last listing is the name of the current Cisco IOS file that is running in RAM



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

  253  -rw-        1156      <no date>  startup-config
  254  ----           5      <no date>  private-config
  255  -rw-        1156      <no date>  underlying-config
    1  -rw-        2945      <no date>  cwmp_inventory
    4  ----          58      <no date>  persistent-data
    5  -rw-          17      <no date>  ecfm_ieee_mib
    6  -rw-         559      <no date>  IOS-Self-Sig#1.cer

262136 bytes total (254779 bytes free)
```

- To view the contents of NVRAM, change the current default file system using the **cd** (change directory) command
- **pwd** (present working directory) command verifies that we are viewing the NVRAM directory
- **dir** lists the contents of NVRAM, included is the startup-configuration file

The Flash File System

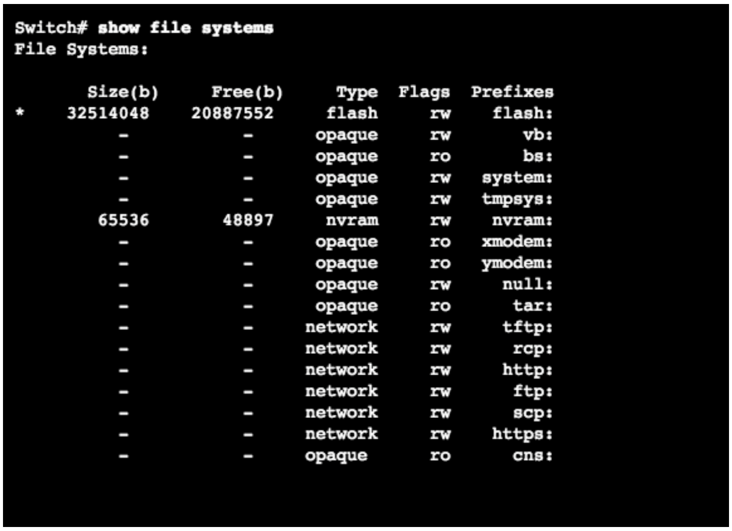
Figure 2 displays the output from the **dir** (directory) command. Because flash is the default file system, the **dir** command lists the contents of flash. Several files are located in flash, but of specific interest is the last listing. This is the name of the current Cisco IOS file image that is running in RAM.

The NVRAM File System

To view the contents of NVRAM, you must change the current default file system using the **cd** (change directory) command, as shown in Figure 3. The **pwd** (present working directory) command verifies that we are viewing the NVRAM directory. Finally, the **dir** command lists the contents of NVRAM. Although there are several configuration files listed, of specific interest is the startup-configuration file.

Router and Switch File Maintenance

Switch File Systems



```
Switch# show file systems
File Systems:

        Size(b)      Free(b)      Type  Flags  Prefixes
*     32514048     20887552      flash    rw     flash:
             -            -     opaque    rw        vb:
             -            -     opaque    ro        bs:
             -            -     opaque    rw    system:
             -            -     opaque    rw    tmpsys:
         65536        48897      nvram    rw     nvram:
             -            -     opaque    ro    xmodem:
             -            -     opaque    ro    ymodem:
             -            -     opaque    rw      null:
             -            -     opaque    ro       tar:
             -            -    network    rw      tftp:
             -            -    network    rw       rcp:
             -            -    network    rw      http:
             -            -    network    rw       ftp:
             -            -    network    rw       scp:
             -            -    network    rw     https:
             -            -    opaque     ro       cns:
```

Command is same as with the router!

Switch File Systems

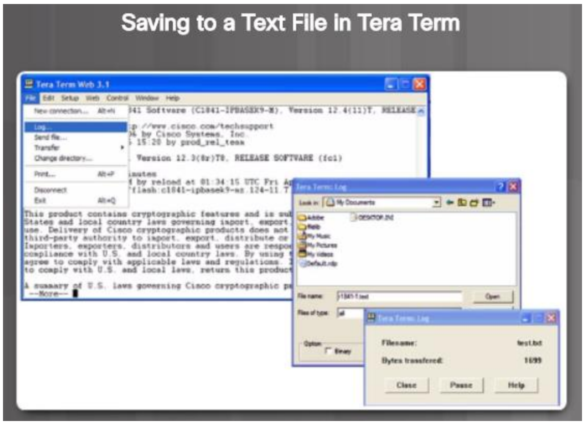
With the Cisco 2960 switch flash file system, you can copy configuration files, and archive (upload and download) software images.

The command to view the file systems on a Catalyst switch is the same as on a Cisco router: **show file systems**, as shown in the figure

Router and Switch File Maintenance

Backing up and Restoring using Text Files

1. On the File menu, click Log.
2. Choose the location to save the file. Tera Term will begin capturing text.
3. After capture has been started, execute the show running-config or show startup-config command at the privileged EXEC prompt. Text displayed in the terminal window will be directed to the chosen file.
4. When the capture is complete, select Close in the Tera Term Log window.
5. View the file to verify that it was not corrupted.



Saving to a Text File in Tera Term

```
341 Software (C1841-IPBASEK9-M), Version 12.4(11)T, RELEASE
tp://www.cisco.com/techsupport
04 by Cisco Systems, Inc.
6 15:20 by prod_rel_team

 Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

inutes
d by reload at 01:34:15 UTC Fri Ap
"flash:c1841-ipbasek9-mz.124-11.T

This product contains cryptographic features and is sub
States and local country laws governing import, export,
use. Delivery of Cisco cryptographic products does not
third-party authority to import, export, distribute or
Importers, exporters, distributors and users are respo
compliance with U.S. and local country laws. By using t
agree to comply with applicable laws and regulations. I
to comply with U.S. and local laws, return this product

A summary of U.S. laws governing Cisco cryptographic pr
 --More-- 
```

File name: c1841-1.txt

Files of type: all

Filename: test.txt

Bytes transferred: 1699

Backing Up and Restoring Using Text Files

Backup Configurations with Text Capture (Tera Term)

Configuration files can be saved/archived to a text file using Tera Term.

As shown in the figure, the steps are:

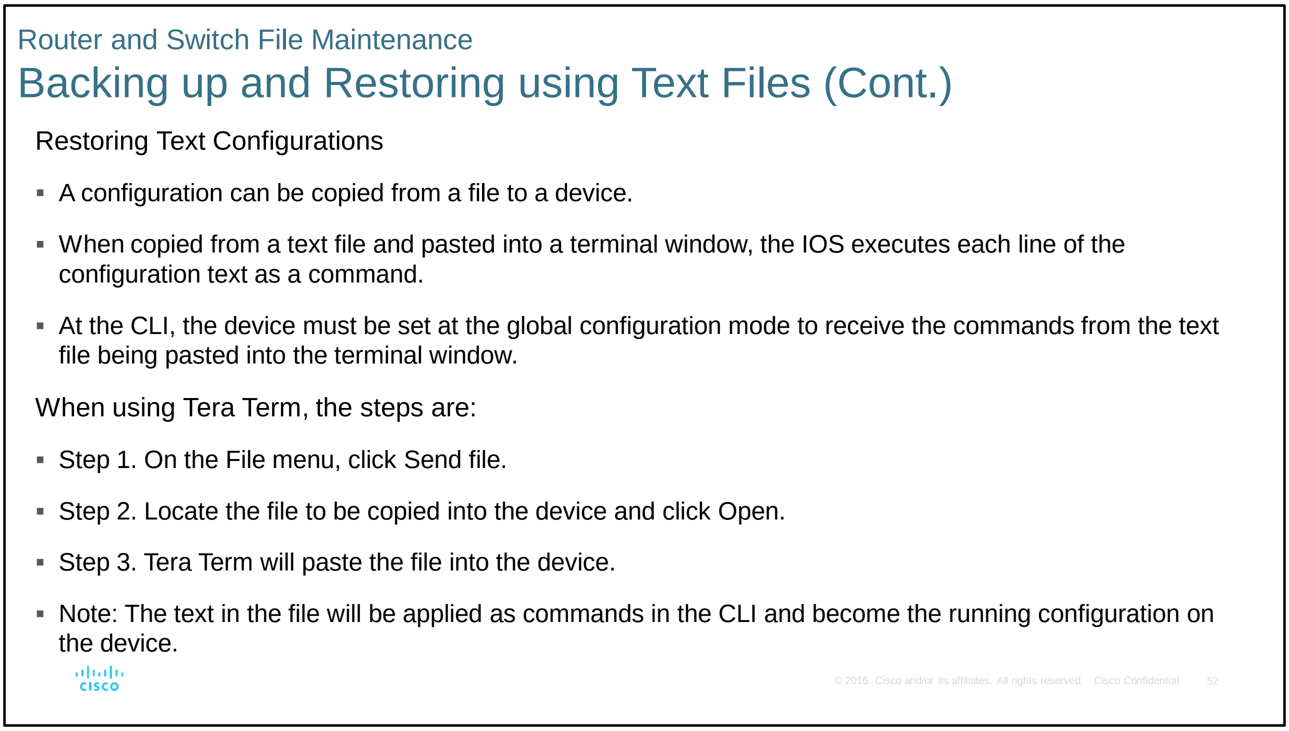
Step 1. On the File menu, click **Log**.

Step 2. Choose the location to save the file. Tera Term will begin capturing text.

Step 3. After capture has been started, execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be directed to the chosen file.

Step 4. When the capture is complete, select **Close** in the Tera Term: Log window.

Step 5. View the file to verify that it was not corrupted.



Router and Switch File Maintenance

Backing up and Restoring using Text Files (Cont.)

Restoring Text Configurations

- A configuration can be copied from a file to a device.
- When copied from a text file and pasted into a terminal window, the IOS executes each line of the configuration text as a command.
- At the CLI, the device must be set at the global configuration mode to receive the commands from the text file being pasted into the terminal window.

When using Tera Term, the steps are:

- Step 1. On the File menu, click Send file.
- Step 2. Locate the file to be copied into the device and click Open.
- Step 3. Tera Term will paste the file into the device.
- Note: The text in the file will be applied as commands in the CLI and become the running configuration on the device.

Restoring Text Configurations

A configuration can be copied from a file to a device. When copied from a text file and pasted into a terminal window, the IOS executes each line of the configuration text as a command. This means that the file will require editing to ensure that encrypted passwords are in plain text and that non-command text such as "--More--" and IOS messages are removed. This process is discussed in the lab.

Further, at the CLI, the device must be set at the global configuration mode to receive the commands from the text file being pasted into the terminal window.

When using Tera Term, the steps are:

Step 1. On the File menu, click **Send** file.

Step 2. Locate the file to be copied into the device and click **Open**.

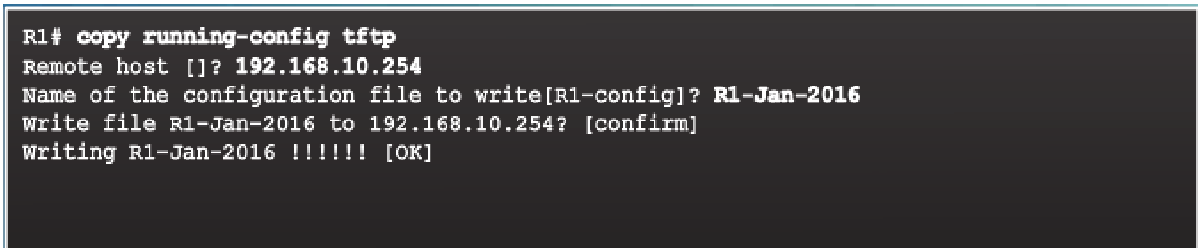
Step 3. Tera Term will paste the file into the device.

The text in the file will be applied as commands in the CLI and become the running configuration on the device. This is a convenient method for manually configuring a router.

Router and Switch File Maintenance

Backing up and Restoring using TFTP

- Configuration files should be backed up and included in network documentation
- Commands - **copy running-config tftp** (see figure) or **copy startup-config tftp**
- To restore the running configuration or the startup configuration from a TFTP server, use **copy tftp running-config** or **copy tftp startup-config** command



```
R1# copy running-config tftp
Remote host []? 192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2016
Write file R1-Jan-2016 to 192.168.10.254? [confirm]
Writing R1-Jan-2016 !!!!!! [OK]
```

Restoring Text Configurations

A configuration can be copied from a file to a device. When copied from a text file and pasted into a terminal window, the IOS executes each line of the configuration text as a command. This means that the file will require editing to ensure that encrypted passwords are in plain text and that non-command text such as "--More--" and IOS messages are removed. This process is discussed in the lab.

Further, at the CLI, the device must be set at the global configuration mode to receive the commands from the text file being pasted into the terminal window.

When using Tera Term, the steps are:

Step 1. On the File menu, click **Send** file.

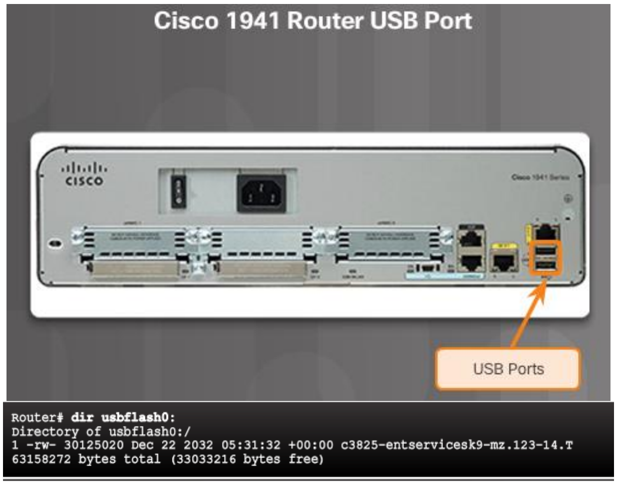
Step 2. Locate the file to be copied into the device and click **Open**.

Step 3. Tera Term will paste the file into the device.

The text in the file will be applied as commands in the CLI and become the running configuration on the device. This is a convenient method for manually configuring a router.

Router and Switch File Maintenance

Using USB Ports on a Cisco Router



Cisco 1941 Router USB Port

```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

- Certain models of Cisco routers support USB flash drives.
- USB can be used for storage and booting.
- USB flash can hold multiple copies of the Cisco IOS and multiple router configurations.
- Use the **dir** command to view the contents of the USB flash drive.

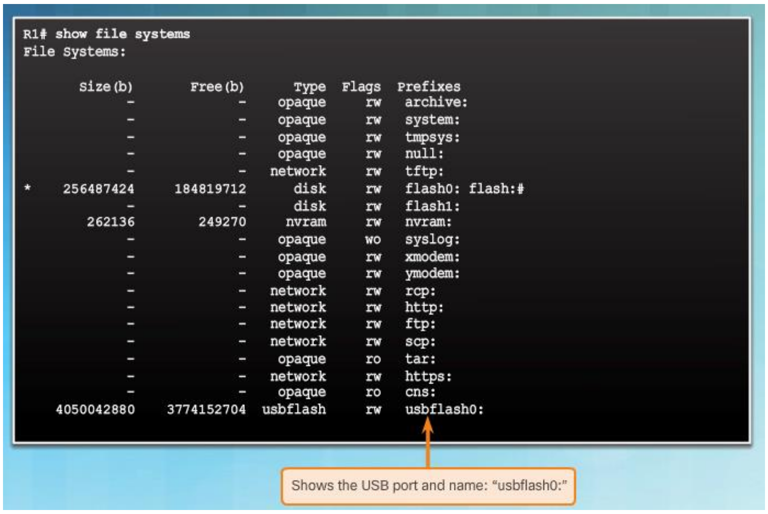
Using USB Ports on a Cisco Router

The Universal Serial Bus (USB) storage feature enables certain models of Cisco routers to support USB flash drives. The USB flash feature provides an optional secondary storage capability and an additional boot device. Images, configurations, and other files can be copied to or from the Cisco USB flash memory with the same reliability as storing and retrieving files using the Compact Flash card. In addition, modular integrated services routers can boot any Cisco IOS Software image saved on USB flash memory. Ideally, USB flash can hold multiple copies of the Cisco IOS and multiple router configurations.

Use the **dir** command to view the contents of the USB flash drive, as shown in the figure.

Router and Switch File Maintenance

Backing up and Restoring Using USB



```
R1# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*    256487424     184819712      disk     rw   flash0: flash:#
             -             -      disk     rw   flash1:
        262136        249270     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    4050042880    3774152704  usbflash     rw   usbflash0:
```

Shows the USB port and name: "usbflash0:"

- **show file systems** verifies USB drive and name

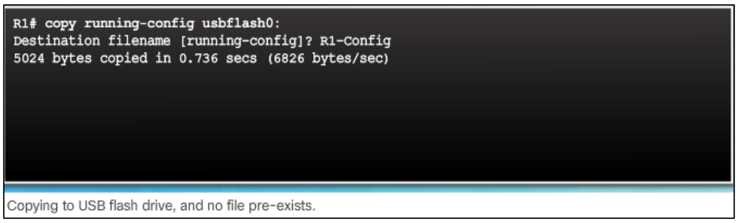
Backing Up and Restoring Using a USB

Backup Configurations with a USB Flash Drive

When backing up to a USB port, it is a good idea to issue the **show file systems** command to verify that the USB drive is there and confirm the name, as shown in Figure 1.

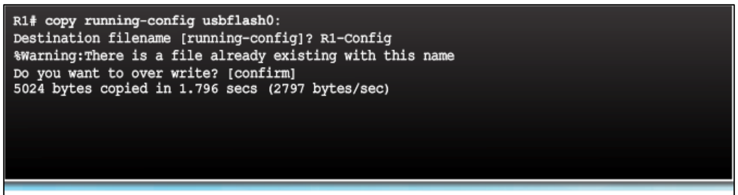
Router and Switch File Maintenance

Backing up and Restoring Using USB (Cont.)



```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Copying to USB flash drive, and no file pre-exists.

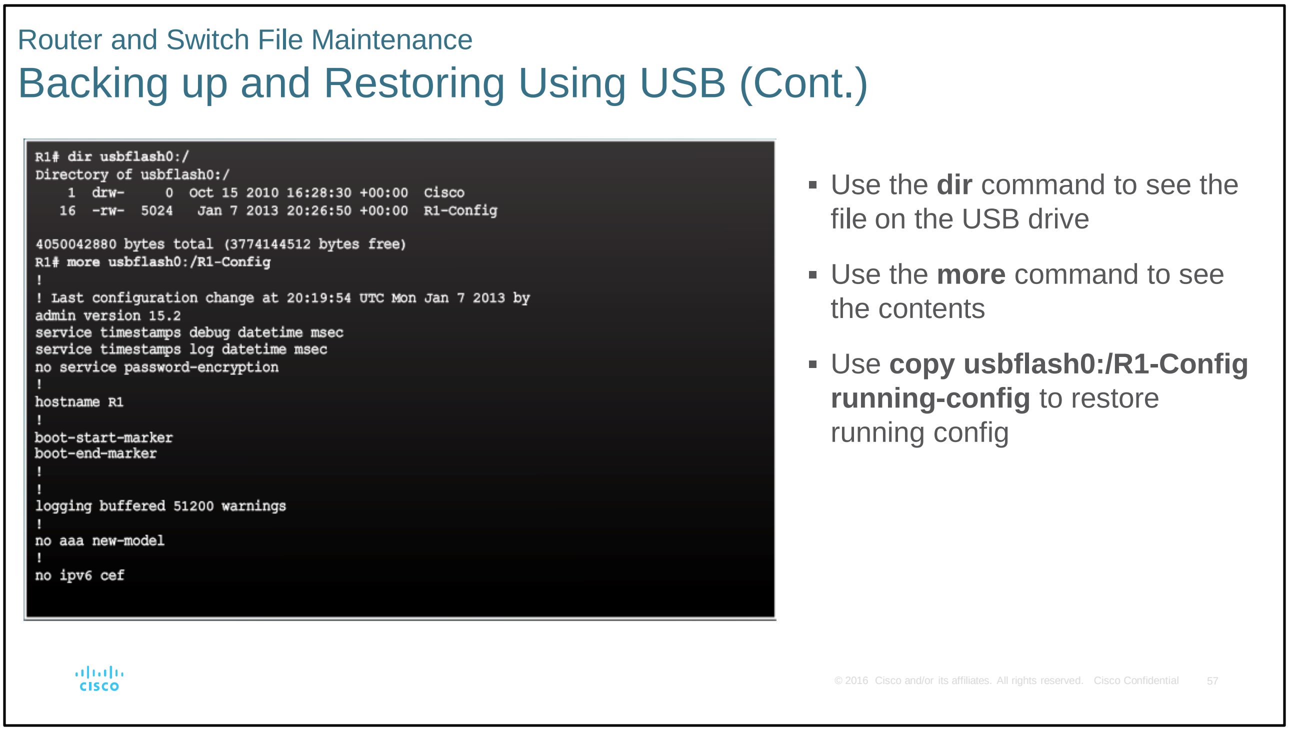


```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Copying to USB flash drive, and the same configuration file already exists on the drive.

- **copy run usbflash0:/** command copies the running-config file to the USB flash drive (slash is optional but indicates the root directory of the USB flash drive)
- IOS will prompt for the filename
- If the file already exists on the USB flash drive, the router will prompt to overwrite

Next, use the **copy run usbflash0:/** command to copy the configuration file to the USB flash drive. Be sure to use the name of the flash drive, as indicated in the file system. The slash is optional but indicates the root directory of the USB flash drive. The IOS will prompt for the filename. If the file already exists on the USB flash drive, the router will prompt to overwrite, as seen in Figure 2.



Router and Switch File Maintenance

Backing up and Restoring Using USB (Cont.)

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config

4050042880 bytes total (3774144512 bytes free)
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
logging buffered 51200 warnings
!
no aaa new-model
!
no ipv6 cef
```

- Use the **dir** command to see the file on the USB drive
- Use the **more** command to see the contents
- Use **copy usbflash0:/R1-Config running-config** to restore running config

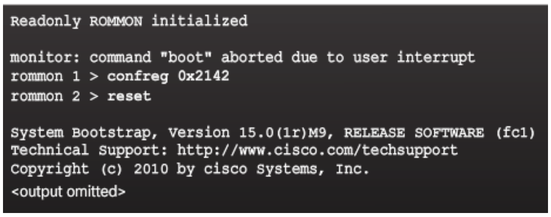
Use the **dir** command to see the file on the USB drive and use the **more** command to see the contents, as seen in Figure 3.

Restore Configurations with a USB Flash Drive

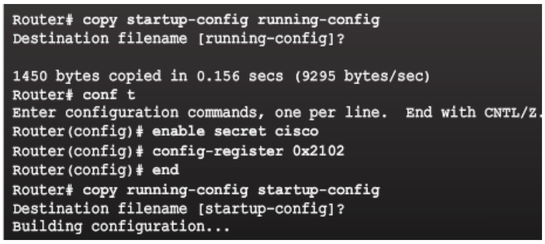
In order to copy the file back, it will be necessary to edit the USB R1-Config file with a text editor. Assuming the file name is **R1-Config**, use the command **copy usbflash0:/R1-Config** *running-config* to restore a running configuration.

Router and Switch File Maintenance

Password Recovery



```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
<output omitted>
```



```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# enable secret cisco
Router(config)# config-register 0x2102
Router(config)# end
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Step 1. Enter the ROMMON mode.

- With console access, a user can access the ROMMON mode by using a break sequence during the boot up process or removing the external flash memory when the device is powered off.

Step 2. Change the configuration register to 0x2142 to ignore the startup config file.

- Use the **confreg 0x2142** command
- Type reset at the prompt to restart the device

Step 3. Make necessary changes to the original startup config file.

- Copy the startup config to the running config
- Configure all necessary passwords
- Change the configuration register back to 0X2102

Step 4. Save the new configuration.

Password Recovery

Passwords on devices are used to prevent unauthorized access. For encrypted passwords, such as the enable secret passwords, the passwords must be replaced after recovery. Depending on the device, the detailed procedure for password recovery varies; however, all the password recovery procedures follow the same principle:

Step 1. Enter the ROMMON mode.
Step 2. Change the configuration register to 0x2142 to ignore the startup config file.
Step 3. Make necessary changes to the original startup config file.
Step 4. Save the new configuration.

Console access to the device through a terminal or terminal emulator software on a PC is required for password recovery. The terminal settings to access the device are:

9600 baud rate
No parity
8 data bits
1 stop bit
No flow control

With console access, a user can access the ROMMON mode by using a break sequence during the boot up process or removing the external flash memory when the device is powered off.

Note: The break sequence for PuTTY is Ctrl+Break. A list of standard break key sequences for other terminal emulators and operating systems can be found at:

http://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/12818-61.html

The ROMMON software supports some basic commands, such as **confreg**. The **confreg 0x2142** command allows the user to set the configuration register to 0x2142. With the configuration register at 0x2142, the device will ignore the startup config file during startup. The startup config file is where the forgotten passwords are stored.

After setting the configuration register to 0x2142, type **reset** at the prompt to restart the device. Enter the break sequence while the device is rebooting and decompressing the IOS. Figure 1 displays the terminal output of a 1941 router in the ROMMON mode after using a break sequence during the boot up process.

After the device has finished reloading, copy the startup config to the running config, as displayed in Figure 2.

CAUTION: Do *not* enter **copy running-config startup-config**. This command erases your original startup configuration.

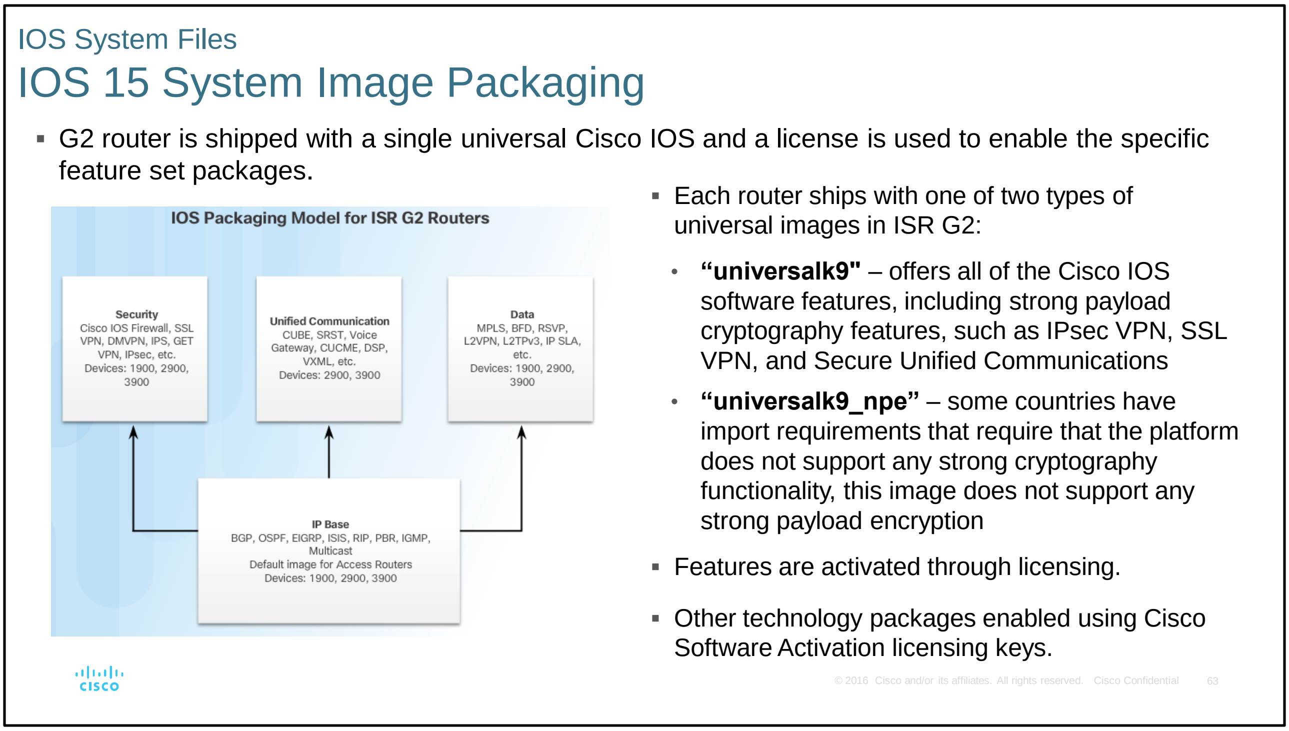
Because you are in privileged EXEC mode, you can now configure all the necessary passwords. After the new passwords are configured, change the configuration register back to 0x2102 using the **config-register 0x2102** command in the global configuration mode. Save the running-config to startup-config and reload the device, as shown in Figure 2.

Note: The password **cisco** is not a strong password and is used here only as an example.

The device now uses the newly configured passwords for authentication. Be sure to use **show** commands to verify that all the configurations are still in place. For example, verify that the appropriate interfaces are not shut down after password recovery.

The following link provides detailed instructions for password recovery procedure for a specific device:

http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/6130-index.html



IOS System Files

IOS 15 System Image Packaging

- G2 router is shipped with a single universal Cisco IOS and a license is used to enable the specific feature set packages.

IOS Packaging Model for ISR G2 Routers

Security
Cisco IOS Firewall, SSL VPN, DMVPN, IPS, GET VPN, IPsec, etc.
Devices: 1900, 2900, 3900

Unified Communication
CUBE, SRST, Voice Gateway, CUCME, DSP, VXML, etc.
Devices: 2900, 3900

Data
MPLS, BFD, RSVP, L2VPN, L2TPv3, IP SLA, etc.
Devices: 1900, 2900, 3900

IP Base
BGP, OSPF, EIGRP, ISIS, RIP, PBR, IGMP, Multicast
Default image for Access Routers
Devices: 1900, 2900, 3900

- Each router ships with one of two types of universal images in ISR G2:
  - **“universalk9"** – offers all of the Cisco IOS software features, including strong payload cryptography features, such as IPsec VPN, SSL VPN, and Secure Unified Communications
  - **“universalk9_npe”** – some countries have import requirements that require that the platform does not support any strong cryptography functionality, this image does not support any strong payload encryption
- Features are activated through licensing.
- Other technology packages enabled using Cisco Software Activation licensing keys.

IOS 15 System Image Packaging

Cisco Integrated Services Routers Generation Two (ISR G2) 1900, 2900, and 3900 Series support services on demand through the use of software licensing. The Services on Demand process enables customers to realize operational savings through ease of software ordering and management. When an order is placed for a new ISR G2 platform, the router is shipped with a single universal Cisco IOS Software image and a license is used to enable the specific feature set packages, as shown in Figure 1.

There are two types of universal images supported in ISR G2:

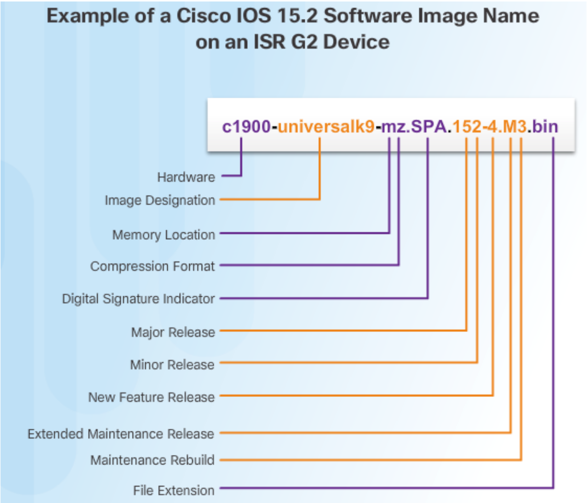
Universal images with the “universalk9" designation in the image name - This universal image offers all of the Cisco IOS Software features, including strong payload cryptography features, such as IPsec VPN, SSL VPN, and Secure Unified Communications.

Universal images with the “universalk9_npe" designation in the image name - The strong enforcement of encryption capabilities provided by Cisco Software Activation satisfies requirements for the export of encryption capabilities. However, some countries have import requirements that require that the platform does not support any strong cryptography functionality, such as payload cryptography. To satisfy the import requirements of those countries, the npe universal image does not support any strong payload encryption.

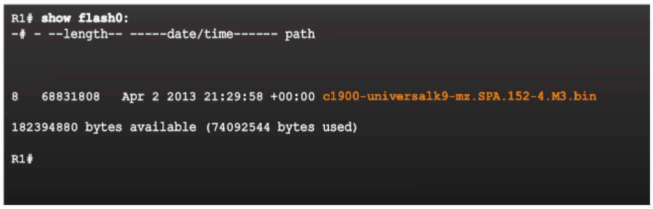
With the ISR G2 devices, IOS image selection has been made easier because all features are included within the universal image. Features are activated through licensing. Each device ships with Universal image. The technology packages IP Base, Data, UC (Unified Communications), and SEC (Security), are enabled in the universal image using Cisco Software Activation licensing keys. Each licensing key is unique to a particular device and is obtained from Cisco by providing the product ID and serial number of the router and a Product Activation Key (PAK). The PAK is provided by Cisco at the time of software purchase. The IP Base is installed by default.

IOS System Files

IOS Image Filenames


Example of a Cisco IOS 15.2 Software Image Name on an ISR G2 Device
c1900-universalk9-mz.SPA.152-4.M3.bin
Hardware
Image Designation
Memory Location
Compression Format
Digital Signature Indicator
Major Release
Minor Release
New Feature Release
Extended Maintenance Release
Maintenance Rebuild
File Extension

Displays the files stored in flash memory



```
R1# show flash0:
-# - --length-- -----date/time------ path


8   68831808   Apr 2 2013 21:29:58 +00:00 c1900-universalk9-mz.SPA.152-4.M3.bin

182394880 bytes available (74092544 bytes used)

R1#
```

- The most common designation for memory location and compression format is mz. The first letter indicates the location where the image is executed on the router. The locations can include:
  - f - flash
  - m - RAM
  - r - ROM
  - l - relocatable
- The compression format can be z for zip or x for mzip.

IOS Image Filenames

When selecting or upgrading a Cisco IOS router, it is important to choose the proper IOS image with the correct feature set and version. The Cisco IOS image file is based on a special naming convention. The name for the Cisco IOS image file contains multiple parts, each with a specific meaning. It is important to understand this naming convention when upgrading and selecting a Cisco IOS Software.

As shown in Figure 1, the **show flash** command displays the files stored in flash memory, including the system image files.

Figure 2 illustrates the different parts of an IOS 15 system image file on an ISR G2 device:

- **Image Name (c1900)** - Identifies the platform on which the image runs. In this example, the platform is a Cisco 1900 router.
- **universalk9** - Specifies the image designation. The two designations for an ISR G2 are universalk9 and universalk9_npe. Universalk9_npe does not contain strong encryption and is meant for countries with encryption restrictions. Features are controlled by licensing and can be divided into four technology packages. These are IP Base, Security, Unified Communications, and Data.
- **mz** - Indicates where the image runs and if the file is compressed. In this example, mz indicates that the file runs from RAM and is compressed.
- **SPA** - Designates that file is digitally signed by Cisco.
- **152-4.M3** - Specifies the filename format for the image 15.2(4)M3. This is the version of IOS, which includes the major release, minor release, maintenance

release, and maintenance rebuild numbers. The M indicates this is an extended maintenance release.
- **bin** - The file extension. This extension indicates that this file is a binary executable file.

The most common designation for memory location and compression format is mz. The first letter indicates the location where the image is executed on the router. The locations can include:

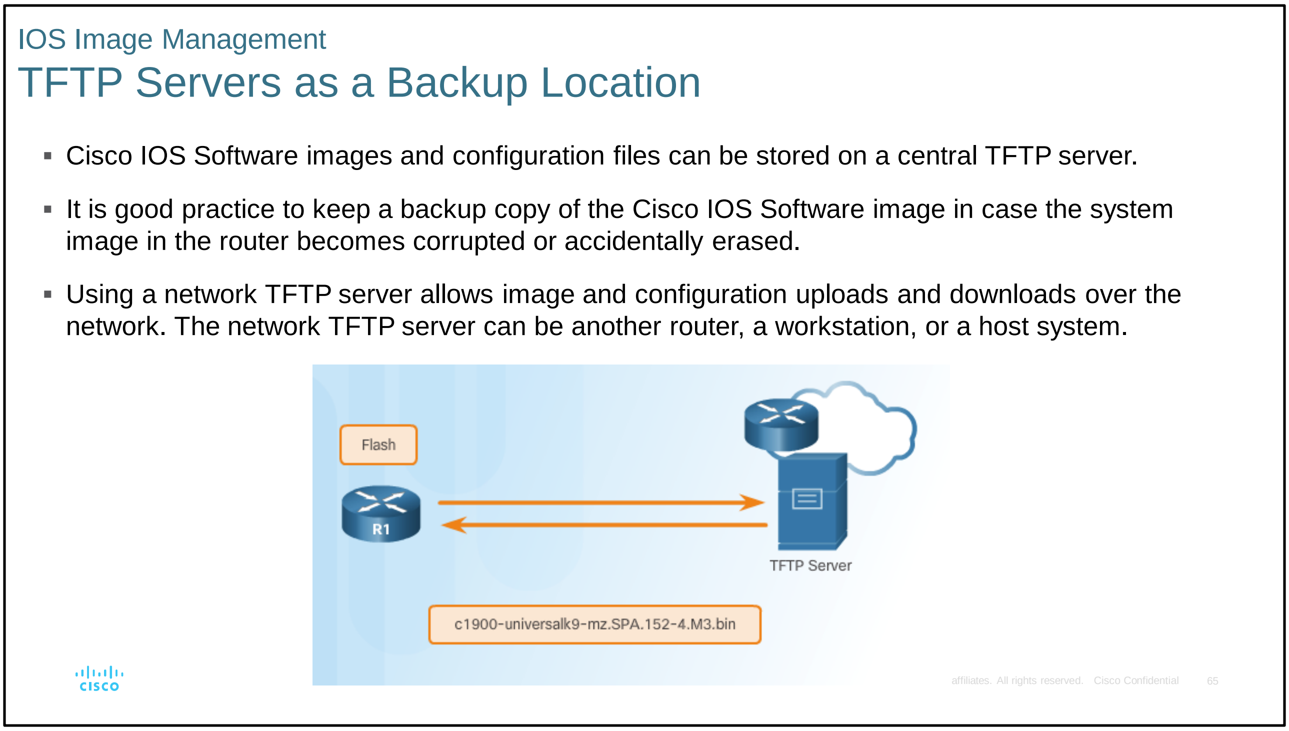
- **f** - flash
- **m** - RAM
- **r** - ROM
- **l** - relocatable

The compression format can be either z for zip or x for mzip. Zipping is a method Cisco uses to compress some run-from-RAM images that is effective in reducing the size of the image. It is self-unzipping, so when the image is loaded into RAM for execution, the first action is to unzip.

Note: The Cisco IOS Software naming conventions, field meaning, image content, and other details are subject to change.

Memory Requirements

On most Cisco routers including the integrated services routers, the IOS is stored in compact flash as a compressed image and loaded into DRAM during boot-up. The Cisco IOS Software Release 15.0 images available for the Cisco 1900 and 2900 ISR require 256MB of flash and 512MB of RAM. The 3900 ISR requires 256MB of flash and 1GB of RAM. This does not include additional management tools such as Cisco Configuration Professional (Cisco CP). For complete details, refer to the product data sheet for the specific router.



IOS Image Management

TFTP Servers as a Backup Location

- Cisco IOS Software images and configuration files can be stored on a central TFTP server.
- It is good practice to keep a backup copy of the Cisco IOS Software image in case the system 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 network TFTP server can be another router, a workstation, or a host system.

TFTP Servers as a Backup Location

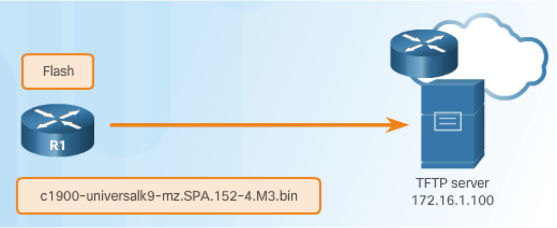
As a network grows, Cisco IOS Software images and configuration files can be stored on a central TFTP server. This helps to control the number of IOS images and the revisions to those IOS images, as well as the configuration files that must be maintained.

Production internetworks usually span wide areas and contain multiple routers. For any network, it is good practice to keep a backup copy of the Cisco IOS Software image in case the system image in the router becomes corrupted or accidentally erased.

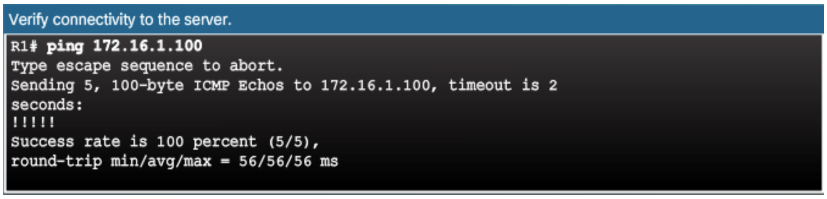
Widely distributed routers need a source or backup location for Cisco IOS Software images. Using a network TFTP server allows image and configuration uploads and downloads over the network. The network TFTP server can be another router, a workstation, or a host system.

IOS Image Management

Steps to Backup IOS Image to TFTP Server



- The network administrator wants to create a backup of the current image file on the router (c1900-universalk9-mz.SPA.152-4.M3.bin) to the TFTP server at 172.16.1.100.



Verify connectivity to the server.

```
R1# ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

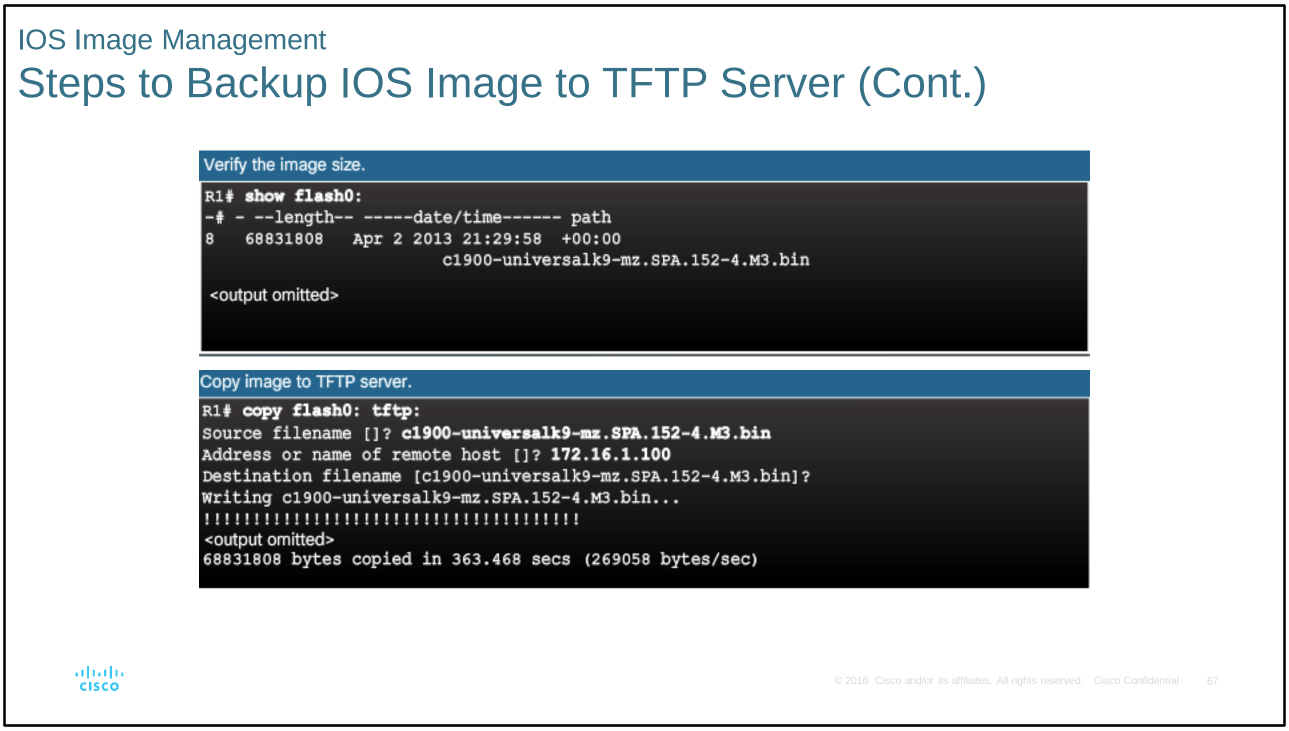
Steps to Backup IOS Image to TFTP Server

To maintain network operations with minimum down time, it is necessary to have procedures in place for backing up Cisco IOS images. This allows the network administrator to quickly copy an image back to a router in case of a corrupted or erased image.

In Figure 1, the network administrator wants to create a backup of the current image file on the router (c1900-universalk9-mz.SPA.152-4.M3.bin) to the TFTP server at 172.16.1.100.

To create a backup of the Cisco IOS image to a TFTP server, perform the following three steps:

Step 1. Ensure that there is access to the network TFTP server. Ping the TFTP server to test connectivity, as shown in Figure 2.



IOS Image Management

Steps to Backup IOS Image to TFTP Server (Cont.)

Verify the image size.

```
R1# show flash0:
-# - --length-- -----date/time------ path
8   68831808   Apr 2 2013 21:29:58  +00:00
                        c1900-universalk9-mz.SPA.152-4.M3.bin

<output omitted>
```

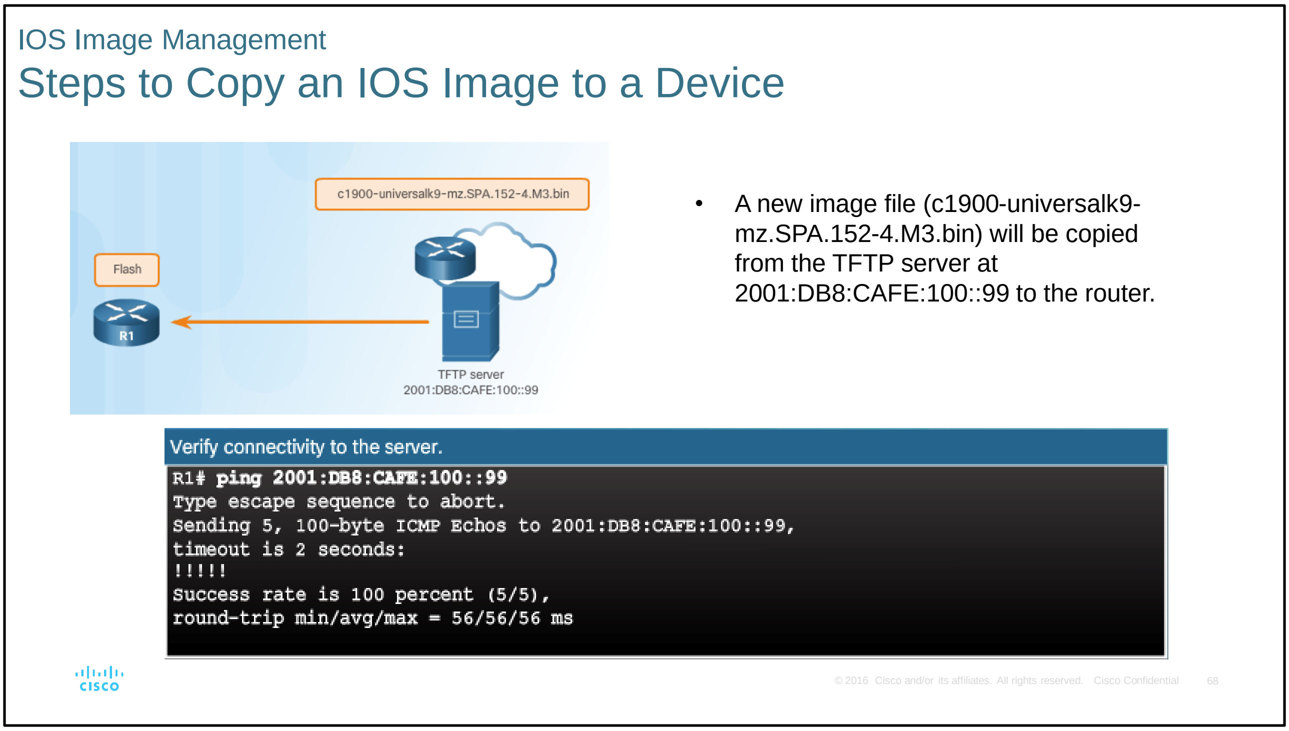
Copy image to TFTP server.

```
R1# copy flash0: tftp:
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin
Address or name of remote host []? 172.16.1.100
Destination filename [c1900-universalk9-mz.SPA.152-4.M3.bin]?
Writing c1900-universalk9-mz.SPA.152-4.M3.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
68831808 bytes copied in 363.468 secs (269058 bytes/sec)
```

Step 2. Verify that the TFTP server has sufficient disk space to accommodate the Cisco IOS Software image (Figure 1). Use the **show flash0:** command on the router to determine the size of the Cisco IOS image file. The file in the example is 68831808 bytes long.

Step 3. Copy the image to the TFTP server using the **copy** *source-url destination-url* command, as shown in Figure 2.

After issuing the command using the specified source and destination URLs, the user is prompted for the source file name, IP address of the remote host, and destination file name. The transfer will then begin.



IOS Image Management

Steps to Copy an IOS Image to a Device

- A new image file (c1900-universalk9-mz.SPA.152-4.M3.bin) will be copied from the TFTP server at 2001:DB8:CAFE:100::99 to the router.

Verify connectivity to the server.

```
R1# ping 2001:DB8:CAFE:100::99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:100::99,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

Steps to Copy an IOS Image to a Device

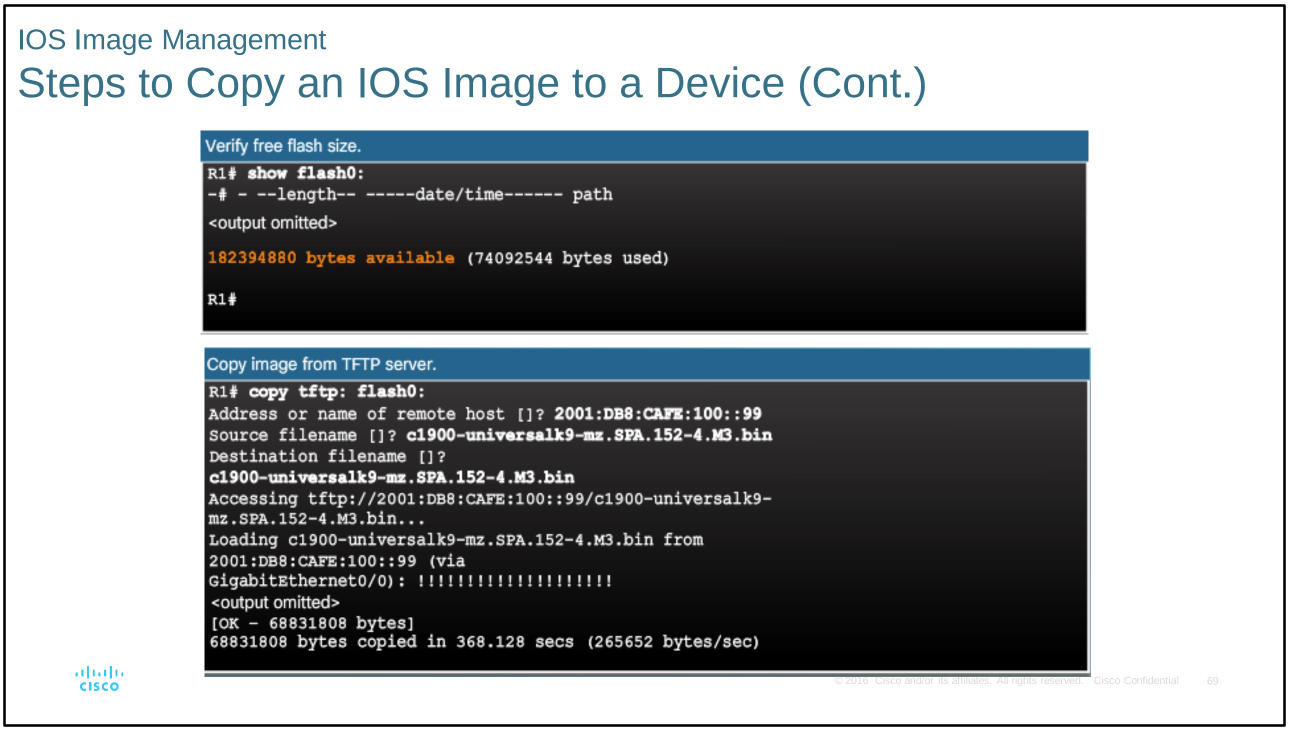
Cisco consistently releases new Cisco IOS software versions to resolve caveats and provide new features. This example uses IPv6 for the transfer to show that TFTP can also be used across IPv6 networks.

Figure 1 illustrates copying a Cisco IOS software image from a TFTP server. A new image file (c1900-universalk9-mz.SPA.152-4.M3.bin) will be copied from the TFTP server at 2001:DB8:CAFE:100::99 to the router.

Follow these steps to upgrade the software on the Cisco router:

Step 1. Select a Cisco IOS image file that meets the requirements in terms of platform, features, and software. Download the file from cisco.com and transfer it to the TFTP server.

Step 2. Verify connectivity to the TFTP server. Ping the TFTP server from the router. The output in Figure 2 shows the TFTP server is accessible from the router.



IOS Image Management

Steps to Copy an IOS Image to a Device (Cont.)

Verify free flash size.

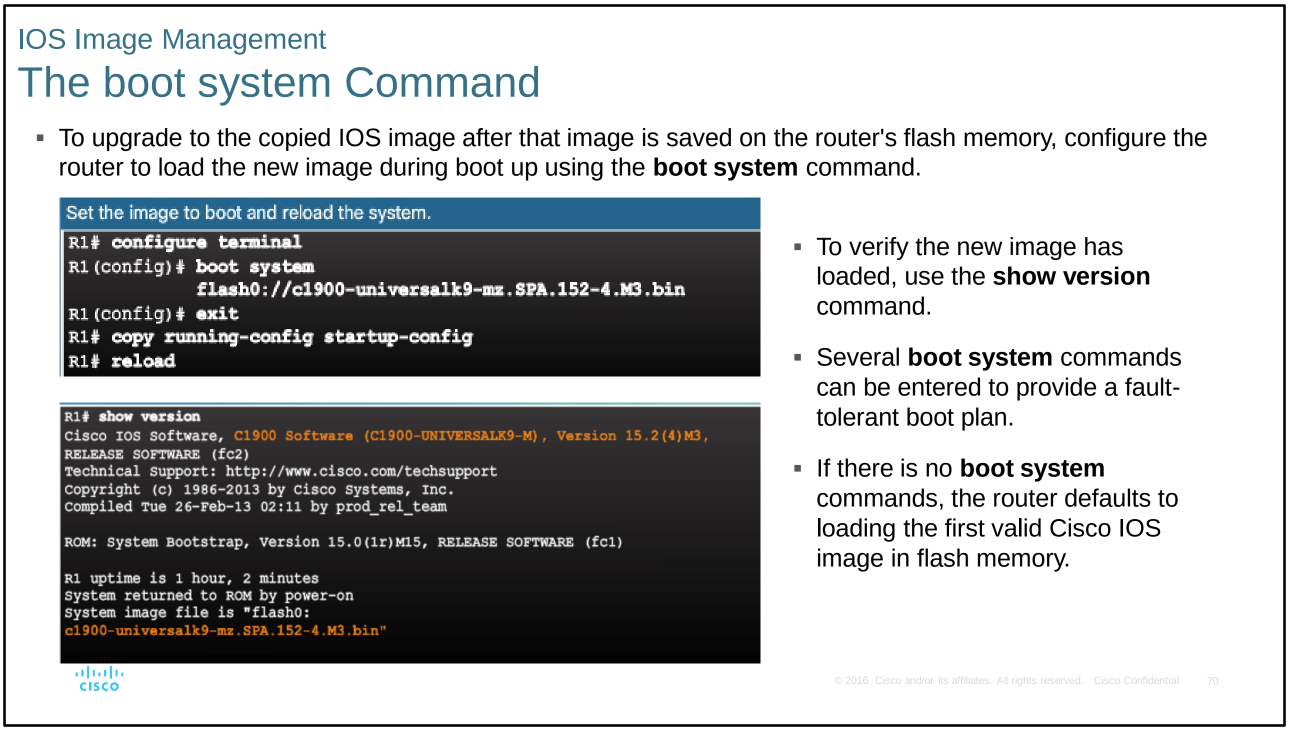
```
R1# show flash0:
-# - --length-- -----date/time------ path
<output omitted>
182394880 bytes available (74092544 bytes used)

R1#
```

Copy image from TFTP server.

```
R1# copy tftp: flash0:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin
Destination filename []?
c1900-universalk9-mz.SPA.152-4.M3.bin
Accessing tftp://2001:DB8:CAFE:100::99/c1900-universalk9-
mz.SPA.152-4.M3.bin...
Loading c1900-universalk9-mz.SPA.152-4.M3.bin from
2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0): !!!!!!!!!!!!!!!!!!!!
<output omitted>
[OK - 68831808 bytes]
68831808 bytes copied in 368.128 secs (265652 bytes/sec)
```

Step 3. Ensure that there is sufficient flash space on the router that is being upgraded. The amount of free flash can be verified using the **show flash0:** command. Compare the free flash space with the new image file size. The **show flash0:** command in Figure 1 is used to verify free flash size. Free flash space in the example is 182,394,880 bytes.

Step 4. Copy the IOS image file from the TFTP server to the router using the **copy** command shown in Figure 2. After issuing this command with specified source and destination URLs, the user will be prompted for IP address of the remote host, source file name, and destination file name. The transfer of the file will begin.



IOS Image Management

The boot system Command

- To upgrade to the copied IOS image after that image is saved on the router's flash memory, configure the router to load the new image during boot up using the **boot system** command.

Set the image to boot and reload the system.

```
R1# configure terminal
R1(config)# boot system
            flash0://c1900-universalk9-mz.SPA.152-4.M3.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```

```
R1# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Tue 26-Feb-13 02:11 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

R1 uptime is 1 hour, 2 minutes
System returned to ROM by power-on
System image file is "flash0:
c1900-universalk9-mz.SPA.152-4.M3.bin"
```

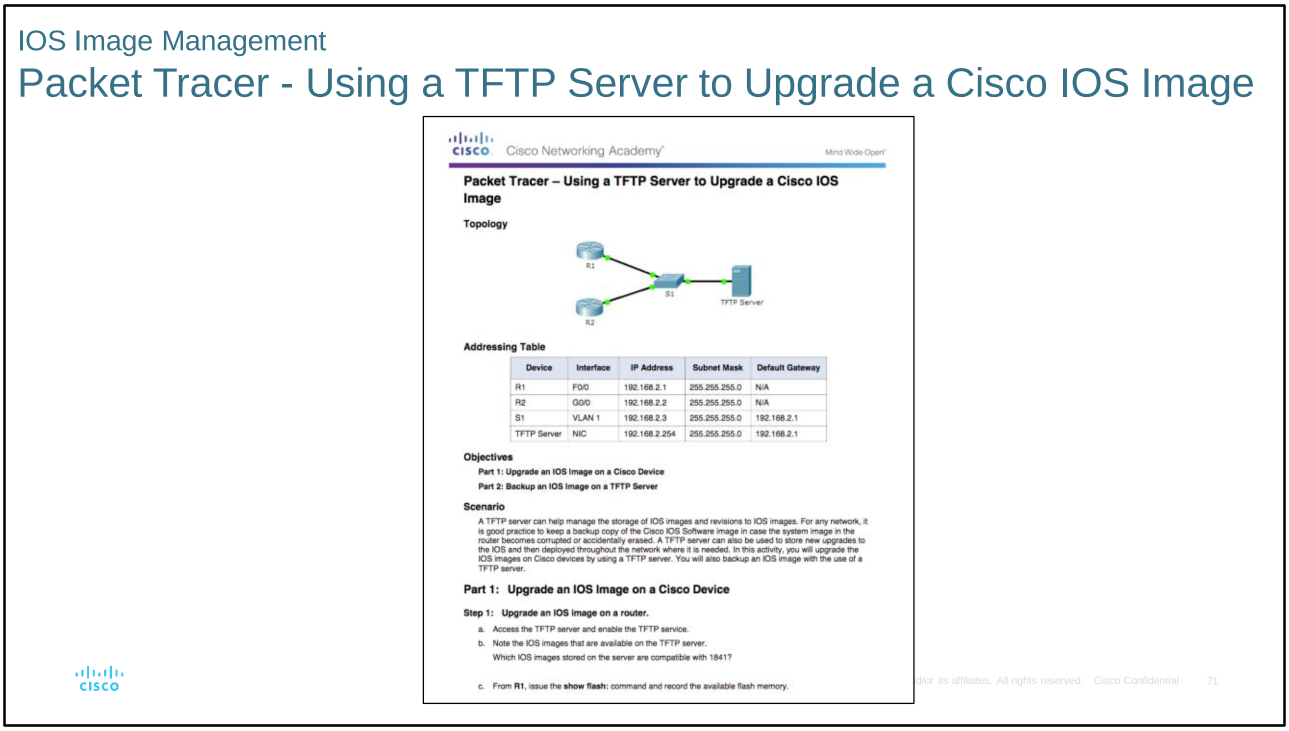
- To verify the new image has loaded, use the **show version** command.
- Several **boot system** commands can be entered to provide a fault-tolerant boot plan.
- If there is no **boot system** commands, the router defaults to loading the first valid Cisco IOS image in flash memory.

The boot system Command

To upgrade to the copied IOS image after that image is saved on the router's flash memory, configure the router to load the new image during bootup using the **boot system** command, as shown in Figure 1. Save the configuration. Reload the router to boot the router with new image. After the router has booted, to verify the new image has loaded, use the **show version** command, as shown in Figure 2.

During startup, the bootstrap code parses the startup configuration file in NVRAM for the **boot system** commands that specify the name and location of the Cisco IOS Software image to load. Several **boot system** commands can be entered in sequence to provide a fault-tolerant boot plan.

If there are no **boot system** commands in the configuration, the router defaults to loading the first valid Cisco IOS image in flash memory and running it.



IOS Image Management

Packet Tracer - Using a TFTP Server to Upgrade a Cisco IOS Image

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Using a TFTP Server to Upgrade a Cisco IOS Image

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.2.1	255.255.255.0	N/A
R2	G0/0	192.168.2.2	255.255.255.0	N/A
S1	VLAN 1	192.168.2.3	255.255.255.0	192.168.2.1
TFTP Server	NIC	192.168.2.254	255.255.255.0	192.168.2.1

Objectives

Part 1: Upgrade an IOS Image on a Cisco Device

Part 2: Backup an IOS Image on a TFTP Server

Scenario

A TFTP server can help manage the storage of IOS images and revisions to IOS images. For any network, it is good practice to keep a backup copy of the Cisco IOS Software image in case the system image in the router becomes corrupted or accidentally erased. A TFTP server can also be used to store new upgrades to the IOS and then deployed throughout the network where it is needed. In this activity, you will upgrade the IOS images on Cisco devices by using a TFTP server. You will also backup an IOS image with the use of a TFTP server.

Part 1: Upgrade an IOS Image on a Cisco Device

Step 1: Upgrade an IOS image on a router.

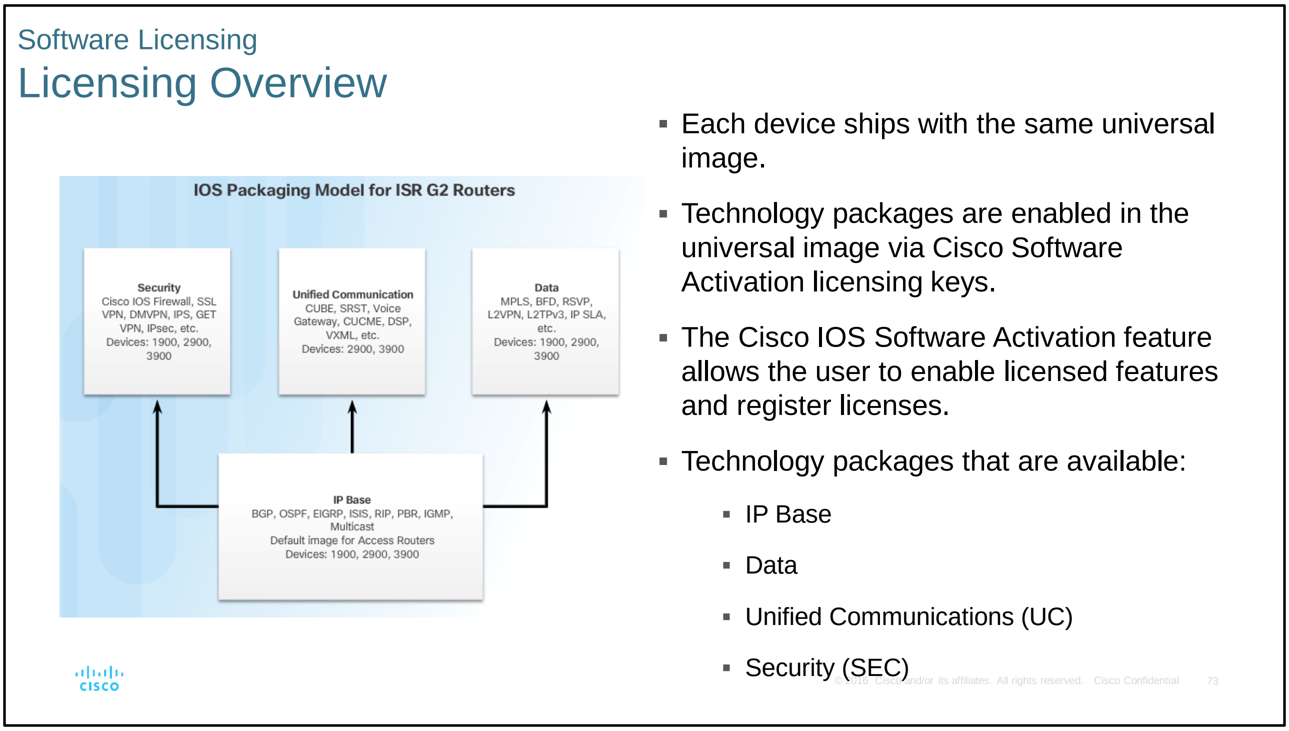
a. Access the TFTP server and enable the TFTP service.

b. Note the IOS images that are available on the TFTP server.

Which IOS images stored on the server are compatible with 1841?

c. From **R1**, issue the **show flash:** command and record the available flash memory.

10.3 – Device Maintenance
10.3.3 – IOS Image Management
10.3.3.5 - Packet Tracer - Using a TFTP Server to Upgrade a Cisco IOS Image



Software Licensing

Licensing Overview

IOS Packaging Model for ISR G2 Routers

Security
Cisco IOS Firewall, SSL VPN, DMVPN, IPS, GET VPN, IPsec, etc.
Devices: 1900, 2900, 3900

Unified Communication
CUBE, SRST, Voice Gateway, CUCME, DSP, VXML, etc.
Devices: 2900, 3900

Data
MPLS, BFD, RSVP, L2VPN, L2TPv3, IP SLA, etc.
Devices: 1900, 2900, 3900

IP Base
BGP, OSPF, EIGRP, ISIS, RIP, PBR, IGMP, Multicast
Default image for Access Routers
Devices: 1900, 2900, 3900

- Each device ships with the same universal image.
- Technology packages are enabled in the universal image via Cisco Software Activation licensing keys.
- The Cisco IOS Software Activation feature allows the user to enable licensed features and register licenses.
- Technology packages that are available:
  - IP Base
  - Data
  - Unified Communications (UC)
  - Security (SEC)

Licensing Overview

Beginning with Cisco IOS Software release 15.0, Cisco modified the process to enable new technologies within the IOS feature sets. Cisco IOS Software release 15.0 incorporates cross-platform feature sets to simplify the image selection process. It does this by providing similar functions across platform boundaries. Each device ships with the same universal image. Technology packages are enabled in the universal image via Cisco Software Activation licensing keys. The Cisco IOS Software Activation feature allows the user to enable licensed features and register licenses. The Cisco IOS Software Activation feature is a collection of processes and components used to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.

Figure shows the technology packages that are available:

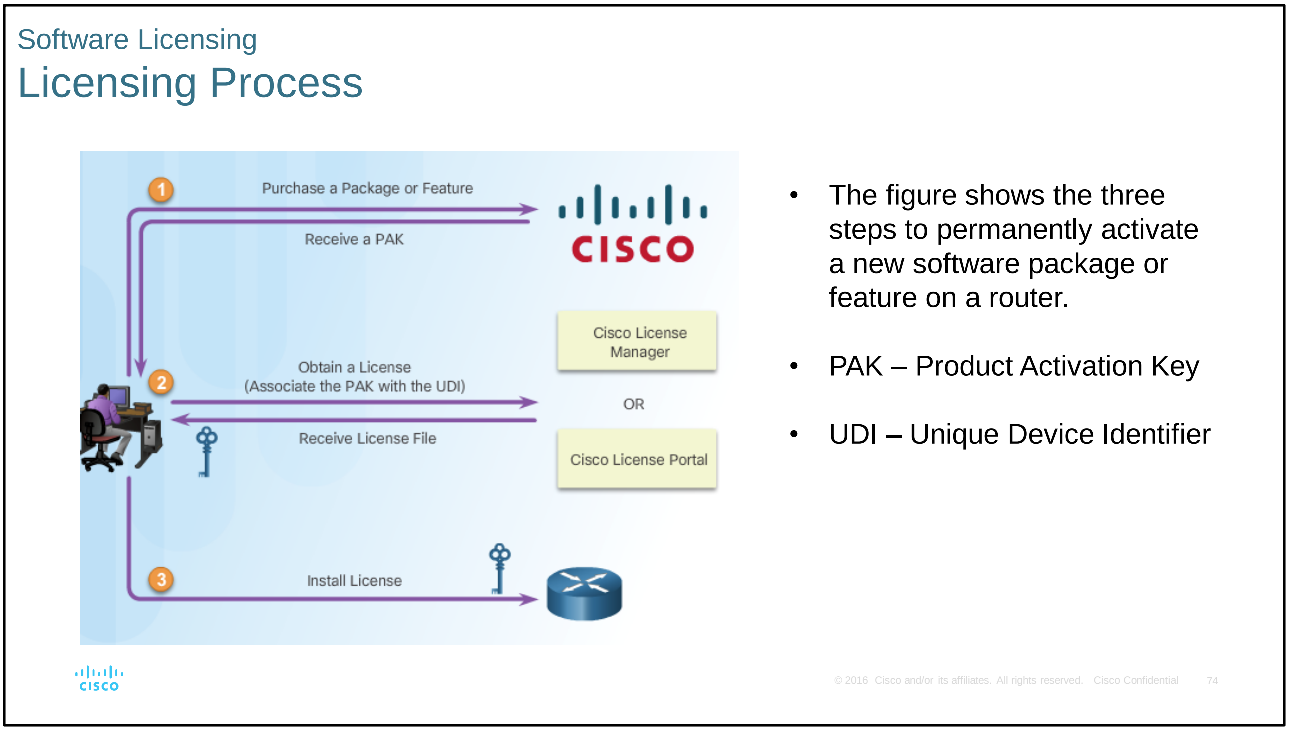
- IP Base
- Data
- Unified Communications (UC)
- Security (SEC)

Note: The IP Base license is a prerequisite for installing the Data, Security, and Unified Communications licenses. For earlier router platforms that can support Cisco IOS Software release 15.0, a universal image is not available. It is necessary to download a separate image that contains the desired features.

Technology Package Licenses

Technology package licenses are supported on Cisco ISR G2 platforms (Cisco 1900, 2900, and 3900 Series routers). The Cisco IOS universal image contains all packages and features in one image. Each package is a grouping of technology-specific features. Multiple technology package licenses can be activated on the Cisco 1900, 2900, and 3900 series ISR platforms.

Note: Use the **show license feature** command to view the technology package licenses and feature licenses supported on the router.



Software Licensing

Licensing Process

1 Purchase a Package or Feature

Receive a PAK

2 Obtain a License
(Associate the PAK with the UDI)

Receive License File

Cisco License Manager

OR

Cisco License Portal

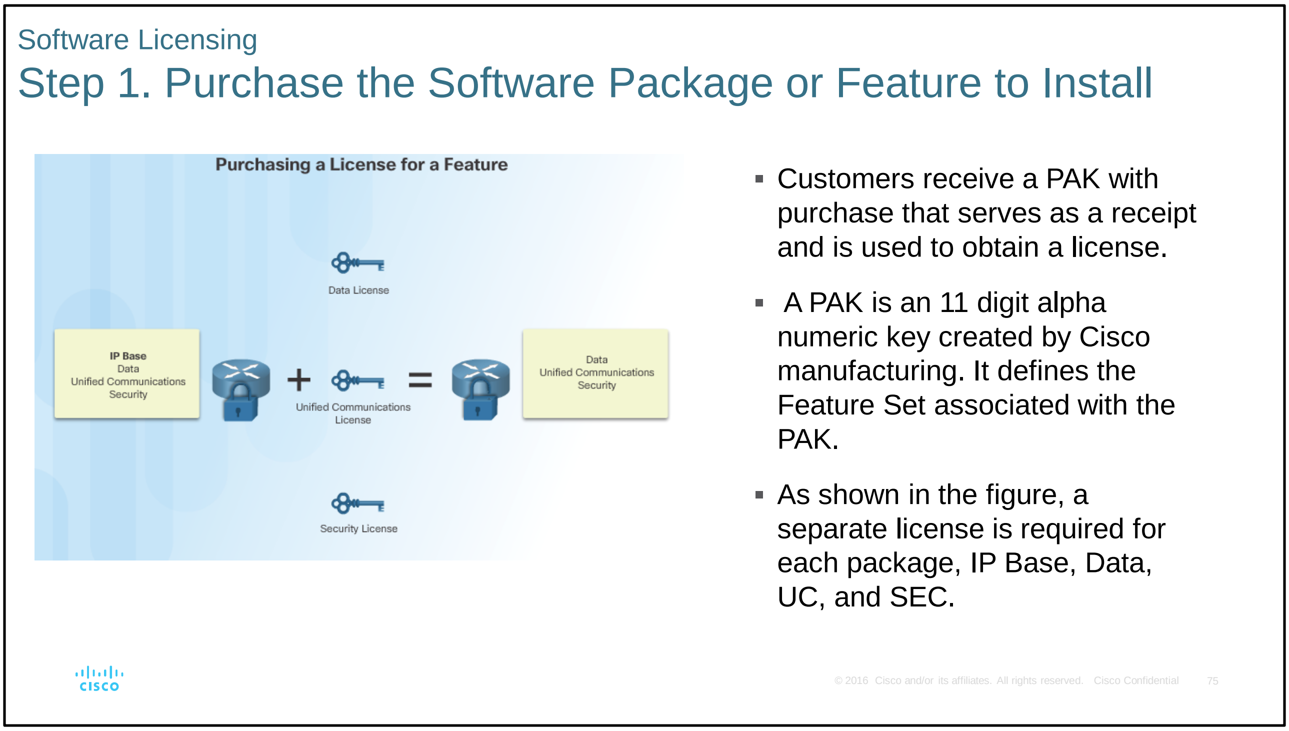
3 Install License

- The figure shows the three steps to permanently activate a new software package or feature on a router.
- PAK – Product Activation Key
- UDI – Unique Device Identifier

Licensing Process

When a new router is shipped, it comes preinstalled with the software image and the corresponding permanent licenses for the customer-specified packages and features. The router also comes with the evaluation license, known as a temporary license, for most packages and features supported on the specified router. This allows customers to try a new software package or feature by activating a specific evaluation license. If customers want to permanently activate a software package or feature on the router, they must get a new software license.

The figure shows the three steps to permanently activate a new software package or feature on the router.



Software Licensing

Step 1. Purchase the Software Package or Feature to Install

Purchasing a License for a Feature

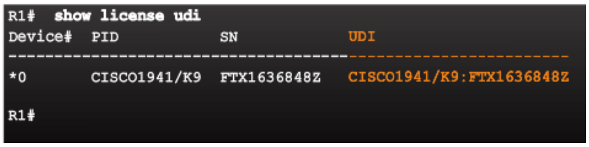
- Customers receive a PAK with purchase that serves as a receipt and is used to obtain a license.
- A PAK is an 11 digit alpha numeric key created by Cisco manufacturing. It defines the Feature Set associated with the PAK.
- As shown in the figure, a separate license is required for each package, IP Base, Data, UC, and SEC.

Step 1. Purchase the Software Package or Feature to Install
The first step is to purchase the software package or feature needed. This may be adding a package to IP Base, such as Security.
Software Claim Certificates are used for licenses that require software activation. The claim certificate provides the Product Activation Key (PAK) for the license and important information regarding the Cisco End User License Agreement (EULA). In most instances, Cisco or the Cisco channel partner will have already activated the licenses ordered at the time of purchase and no Software Claim Certificate is provided.
In either instance, customers receive a PAK with their purchase. The PAK serves as a receipt and is used to obtain a license. A PAK is an 11 digit alpha numeric key created by Cisco manufacturing. It defines the Feature Set associated with the PAK. A PAK is not tied to a specific device until the license is created. A PAK can be purchased that generates any specified number of licenses. As shown in the figure, a separate license is required for each package, IP Base, Data, UC, and SEC.

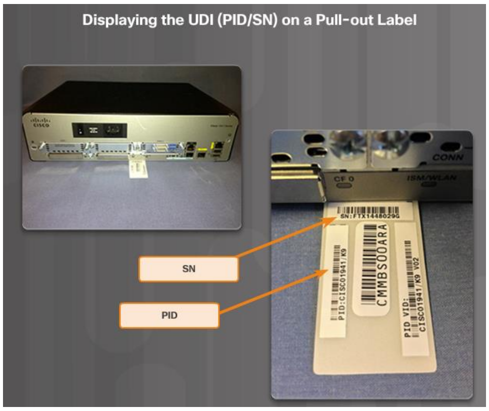
Software Licensing

Step 2. Obtain a License

- The UDI is a combination of the Product ID (PID), the Serial Number (SN), and the hardware version. The SN is an 11 digit number which uniquely identifies a device. The PID identifies the type of device. Only the PID and SN are used for license creation.
- This UDI can be displayed using the **show license udi** command shown.



```
R1#  show license udi
Device#  PID            SN            UDI
-------------------------------------------------------------
*0       CISCO1941/K9   FTX1636848Z   CISCO1941/K9:FTX1636848Z

R1#
```



Displaying the UDI (PID/SN) on a Pull-out Label

Step 2. Obtain a License

The second step is to obtain the license, which is actually a license file. A license file, also known as a Software Activation License, is obtained using one of the following options:

- **Cisco License Manager (CLM)** - This is a free software application available at http://www.cisco.com/go/clm. Cisco License Manager is a standalone application from Cisco that helps network administrators rapidly deploy multiple Cisco software licenses across their networks. Cisco License Manager can discover network devices, view their license information, and acquire and deploy licenses from Cisco. The application provides a GUI that simplifies installation and helps automate license acquisition, as well as perform multiple licensing tasks from a central location. CLM is free of charge and can be downloaded from CCO.
- **Cisco License Registration Portal** - This is the web-based portal for getting and registering individual software licenses, available at http://www.cisco.com/go/license.

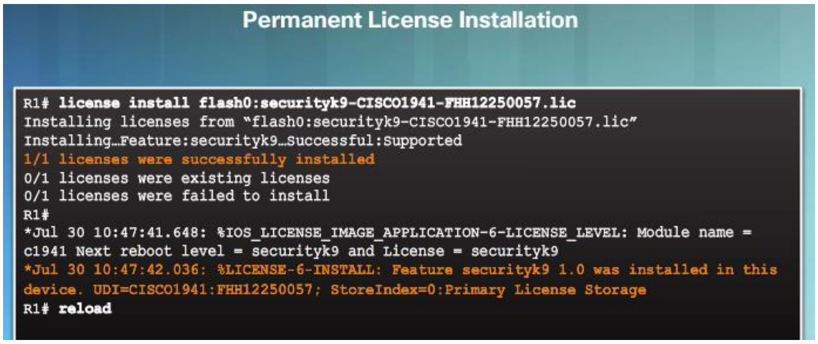
Both of these processes require a PAK number and a Unique Device Identifier (UDI). The PAK is received during purchase.

The UDI is a combination of the Product ID (PID), the Serial Number (SN), and the hardware version. The SN is an 11-digit number which uniquely identifies a device. The PID identifies the type of device. Only the PID and SN are used for license creation. This UDI can be displayed using the **show license udi** command shown in

Figure 1. This information is also available on a pull-out label tray found on the device. Figure 2 shows an example of the pull-out label on a Cisco 1941 router. After entering the appropriate information, the customer receives an email containing the license information to install the license file. The license file is an XML text file with a .lic extension.

Software Licensing

Step 3. Install the License



Permanent License Installation

```
R1# license install flash0:securityk9-CISCO1941-FHH12250057.lic
Installing licenses from "flash0:securityk9-CISCO1941-FHH12250057.lic"
Installing…Feature:securityk9…Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
R1#
*Jul 30 10:47:41.648: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
c1941 Next reboot level = securityk9 and License = securityk9
*Jul 30 10:47:42.036: %LICENSE-6-INSTALL: Feature securityk9 1.0 was installed in this
device. UDI=CISCO1941:FHH12250057; StoreIndex=0:Primary License Storage
R1# reload
```

- A permanent license is a license that never expires. After a permanent license is installed on a router, it is good for that particular feature set for the life of the router, even across IOS versions.

Step 3. Install the License

After the license has been purchased, the customer receives a license file. Installing a permanent license requires two steps:

Step 1. Use the **license install** *stored-location-url* privileged exec mode command to install a license file.

Step 2. Reload the router using the privileged exec command **reload**. A reload is not required if an evaluation license is active.

Figure shows the configuration for installing the permanent license for the Security package on the router.

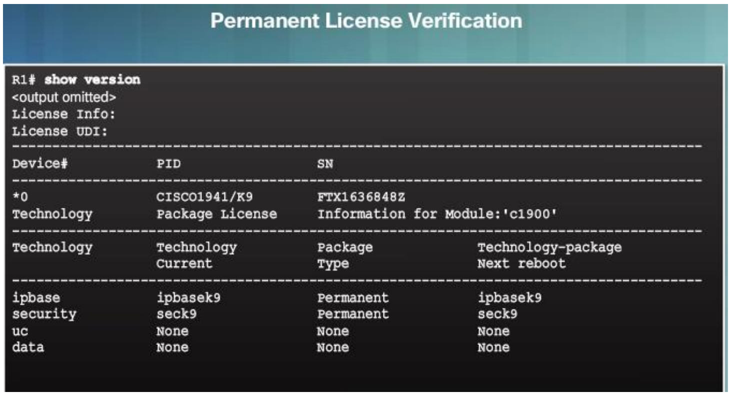
Note: Unified Communications is not supported on 1941 routers.

A permanent license is a license that never expires. After a permanent license is installed on a router, it is good for that particular feature set for the life of the router, even across IOS versions. For example, when a UC, SEC, or Data license is installed on a router, the subsequent features for that license are activated even if the router is upgraded to a new IOS release. A permanent license is the most common license type used when a feature set is purchased for a device.

Note: Cisco manufacturing preinstalls the appropriate permanent license on the ordered device for the purchased feature set. No customer interaction with the Cisco IOS Software Activation processes is required to enable that license on new hardware.

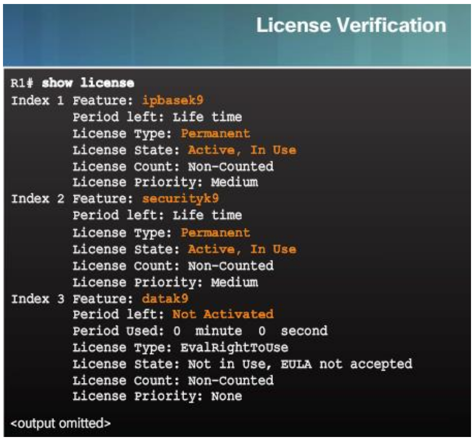
License Verification and Management

License Verification



Permanent License Verification

```
R1# show version
<output omitted>
License Info:
License UDI:
-------------------------------------------------------------------------------------
Device#          PID                SN
-------------------------------------------------------------------------------------
*0               CISCO1941/K9       FTX1636848Z
Technology       Package License    Information for Module:'c1900'
-------------------------------------------------------------------------------------
Technology       Technology         Package            Technology-package
                 Current            Type               Next reboot
-------------------------------------------------------------------------------------
ipbase           ipbasek9           Permanent          ipbasek9
security         seck9              Permanent          seck9
uc               None               None               None
data             None               None               None
```



License Verification

```
R1# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 3 Feature: datak9
        Period left: Not Activated
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None

<output omitted>
```

License Verification

After a new license has been installed the router must be rebooted using the **reload** command. As shown in Figure 1, the **show version** command is used after the router is reloaded to verify that license has been installed.

The **show license** command in Figure 2 is used to display additional information about Cisco IOS software licenses. This command displays license information used to help with troubleshooting issues related to Cisco IOS software licenses. This command displays all the licenses installed in the system. In this example, both the IP Base and Security licenses have been installed. This command also displays the features that are available, but not licensed to execute, such as the Data feature set. Output is grouped according to how the features are stored in license storage.

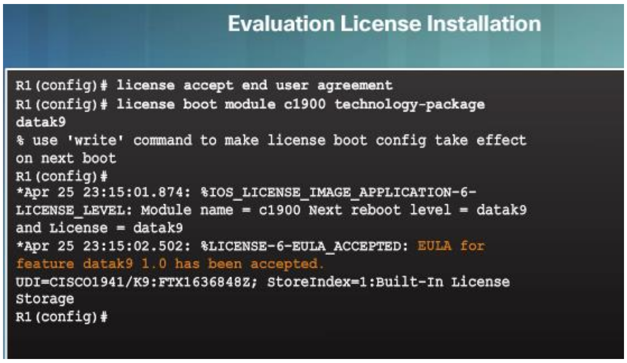
The following is a brief description of the output:

- **Feature** - Name of the feature
- **License Type** - Type of license; such as Permanent or Evaluation
- **License State** - Status of the license; such as Active or In Use
- **License Count** - Number of licenses available and in use, if counted. If non-counted is indicated, the license is unrestricted.
- **License Priority** - Priority of the license; such as high or low

Note: Refer to the Cisco IOS 15 command reference guide for complete details on the information displayed in the **show license** command.

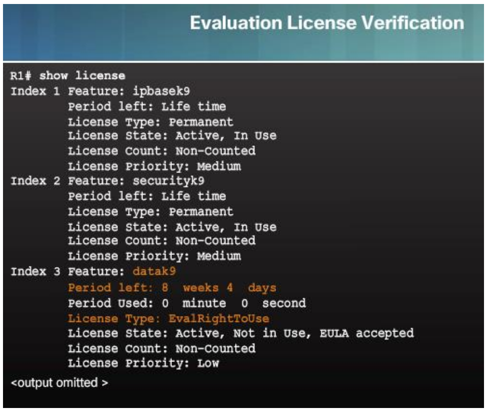
License Verification and Management

Activate an Evaluation Right-To-Use License



Evaluation License Installation

```
R1(config)# license accept end user agreement
R1(config)# license boot module c1900 technology-package
datak9
% use 'write' command to make license boot config take effect
on next boot
R1(config)#
*Apr 25 23:15:01.874: %IOS_LICENSE_IMAGE_APPLICATION-6-
LICENSE_LEVEL: Module name = c1900 Next reboot level = datak9
and License = datak9
*Apr 25 23:15:02.502: %LICENSE-6-EULA_ACCEPTED: EULA for
feature datak9 1.0 has been accepted.
UDI=CISCO1941/K9:FTX1636848Z; StoreIndex=1:Built-In License
Storage
R1(config)#
```



Evaluation License Verification

```
R1# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 3 Feature: datak9
        Period left: 8  weeks 4  days
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Active, Not in Use, EULA accepted
        License Count: Non-Counted
        License Priority: Low
<output omitted >
```

Activate an Evaluation Right-To-Use License

Evaluation licenses are replaced with Evaluation Right-To-Use licenses (RTU) after 60 days. An Evaluation license is good for a 60 day evaluation period. After the 60 days, this license automatically transitions into an RTU license. These licenses are available on the honor system and require the customer's acceptance of the EULA. The EULA is automatically applied to all Cisco IOS software licenses.

The **license accept end user agreement** global configuration mode command is used to configure a one-time acceptance of the EULA for all Cisco IOS software packages and features. After the command is issued and the EULA accepted, the EULA is automatically applied to all Cisco IOS software licenses and the user is not prompted to accept the EULA during license installation.

Figure 1 shows how to configure a one-time acceptance of the EULA:

Router(config)# **license accept end user agreement**

In addition, Figure 1 shows the command to activate an Evaluation RTU license:

Router# **license boot module** *module-name* **technology-package** *package-name*

Use the **?** in place of the arguments to determine which module names and supported software packages are available on the router. Technology package names for Cisco ISR G2 platforms are:

- **ipbasek9** - IP Base technology package
- **securityk9** - Security technology package
- **datak9** - Data technology package
- **uck9** - Unified Communications package (not available on 1900 series)

Note: A reload using the **reload** command is required to activate the software package.

Evaluation licenses are temporary, and are used to evaluate a feature set on new hardware. Temporary licenses are limited to a specific usage period (for example, 60 days).

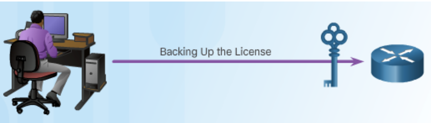
Reload the router after a license is successfully installed using the **reload** command.

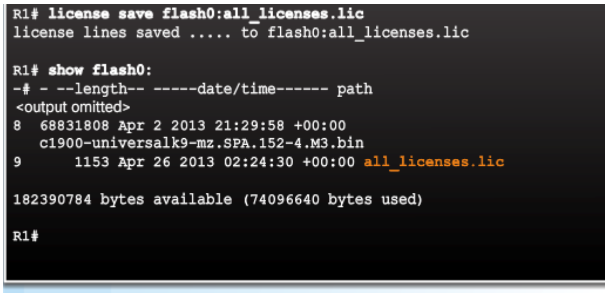
The **show license** command in Figure 2 verifies that the license has been installed.

License Verification and Management

Back up the License

- The **license save** command is used to copy all licenses in a device and store them.
- Saved licenses are restored by using the **license install** command.
- The command to back up a copy of the licenses on a device is:
  - Router# **license save** *file-sys://lic-location*
- Use the show flash0: command to verify that the licenses have been saved.





```
R1# license save flash0:all_licenses.lic
license lines saved ..... to flash0:all_licenses.lic

R1# show flash0:
-# - --length-- -----date/time------ path
<output omitted>
8  68831808 Apr 2 2013 21:29:58 +00:00
   c1900-universalk9-mz.SPA.152-4.M3.bin
9      1153 Apr 26 2013 02:24:30 +00:00 all_licenses.lic

182390784 bytes available (74096640 bytes used)

R1#
```

Back up the License

The **license save** command is used to copy all licenses in a device and store them in a format required by the specified storage location. Saved licenses are restored by using the **license install** command.

The command to back up a copy of the licenses on a device is:

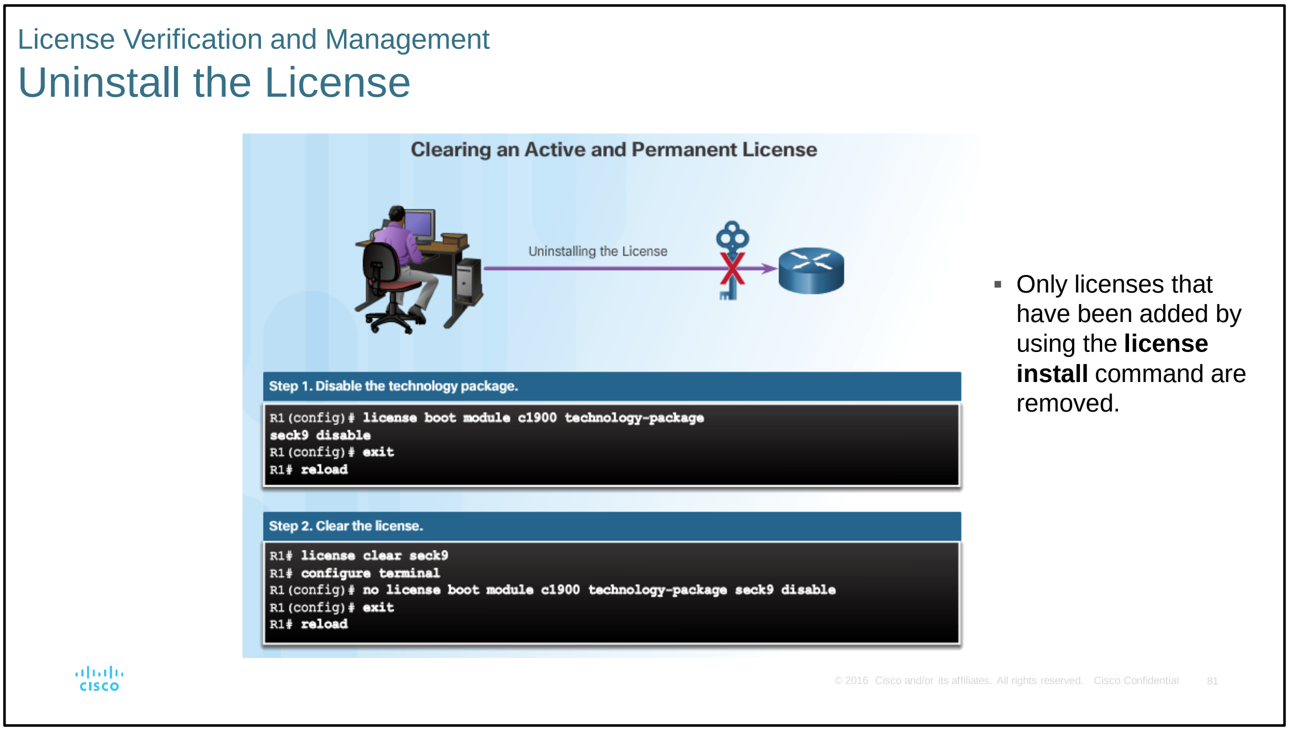
Router# **license save** *file-sys://lic-location*

Use the **show flash0:** command to verify that the licenses have been saved (Figure 1).

The license storage location can be a directory or a URL that points to a file system.

Use the **?** command to see the storage locations supported by a device.

Use the Syntax Checker in Figure 2 to save all license files on router R2.



License Verification and Management

Uninstall the License

Clearing an Active and Permanent License

Step 1. Disable the technology package.

```
R1(config)# license boot module c1900 technology-package
seck9 disable
R1(config)# exit
R1# reload
```

Step 2. Clear the license.

```
R1# license clear seck9
R1# configure terminal
R1(config)# no license boot module c1900 technology-package seck9 disable
R1(config)# exit
R1# reload
```

- Only licenses that have been added by using the **license install** command are removed.

Uninstall the License

To clear an active permanent license from the Cisco 1900 series, 2900 series, and 3900 series routers, perform the following steps:

Step 1. Disable the technology package.

- Disable the active license with the command:

```
    Router(config)# license boot module module-name
    technology-package package-name disable
```

- Reload the router using the **reload** command. A reload is required to make the software package inactive.

Step 2. Clear the license.

- Clear the technology package license from license storage.

```
    Router# license clear feature-name
```

- Clear the **license boot module** command used for disabling the active license:

```
    Router(config)# no license boot module module-name
technology-package package-name disable
```

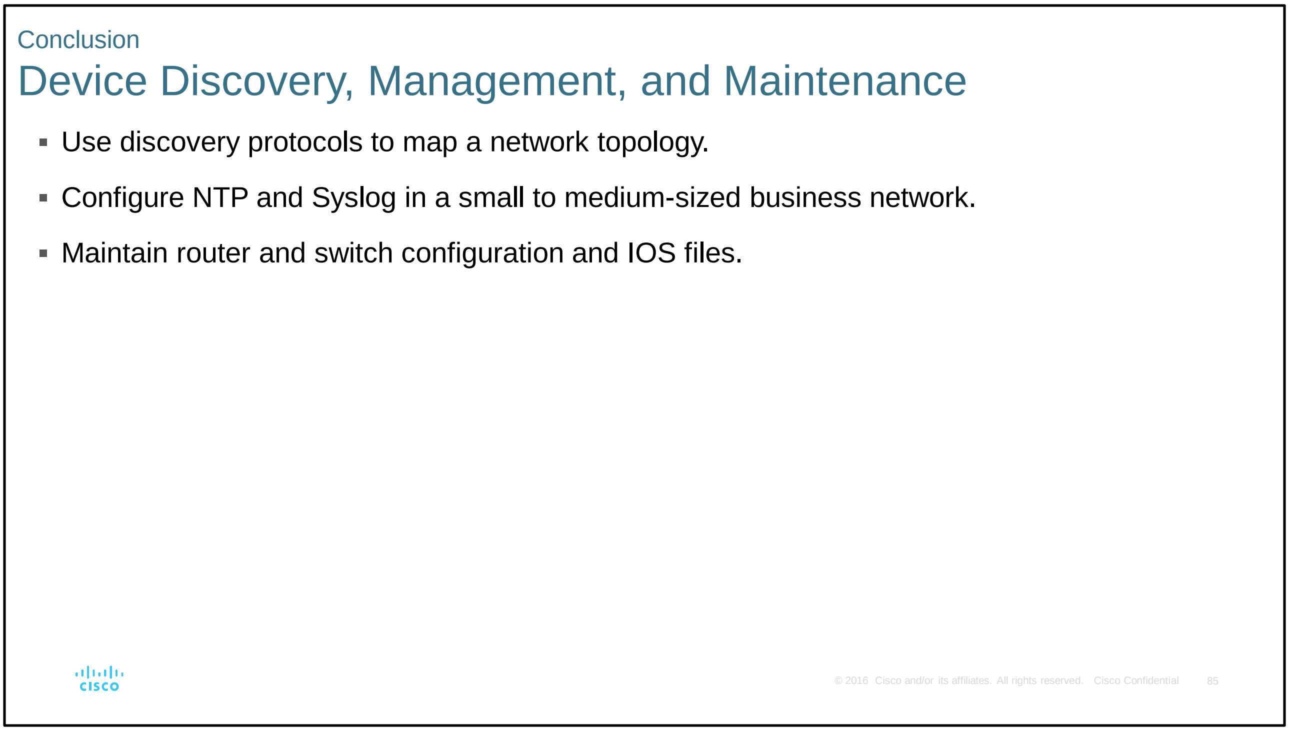
Note: Some licenses, such as built-in licenses, cannot be cleared. Only licenses that have been added by using the **license install** command are removed. Evaluation licenses are not removed.

Figure 1 shows an example of clearing an active license.

Use the Syntax Checker in Figure 2 to uninstall the security license on router R2.

Chapter Summary

10 - Device Discovery, Management, and Maintenance
10.4 – Summary



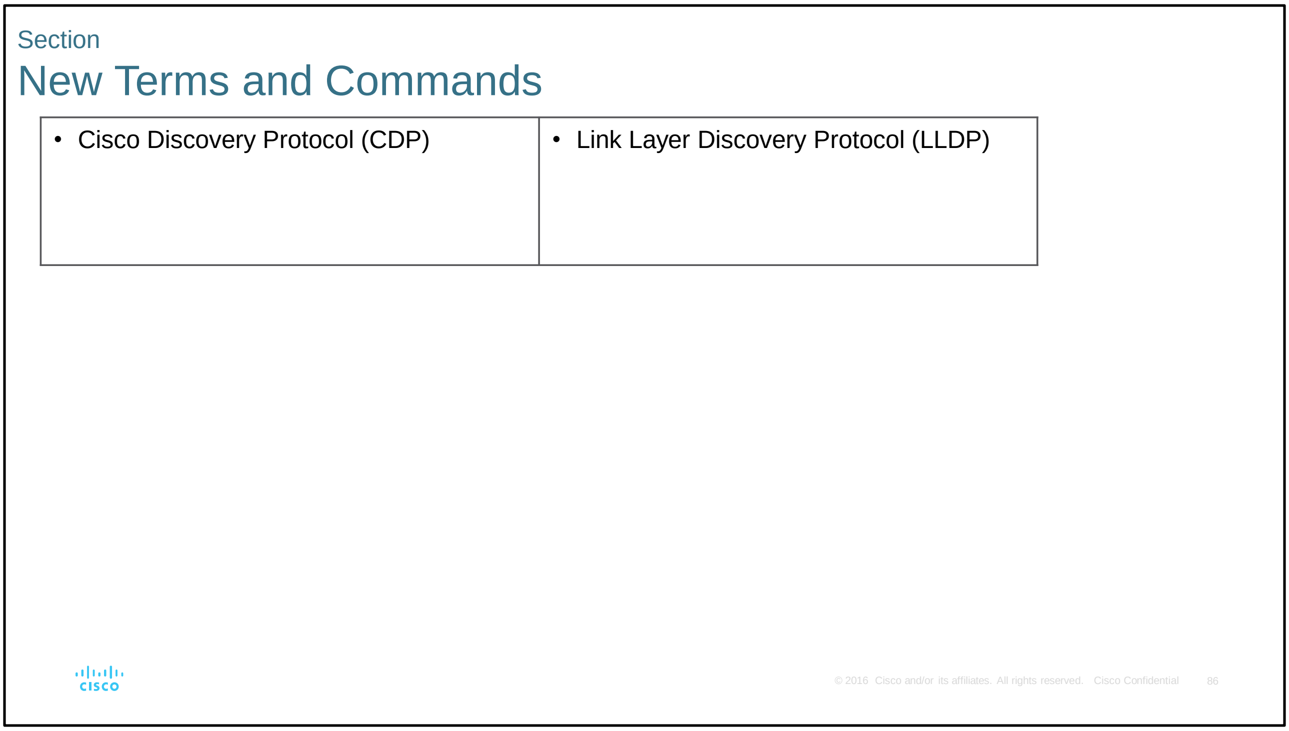
Conclusion

Device Discovery, Management, and Maintenance

- Use discovery protocols to map a network topology.
- Configure NTP and Syslog in a small to medium-sized business network.
- Maintain router and switch configuration and IOS files.

10.4 – Summary

10.4.1 – Conclusion
10.4.1.2 – Chapter 10: Device Discovery, Management, and Maintenance

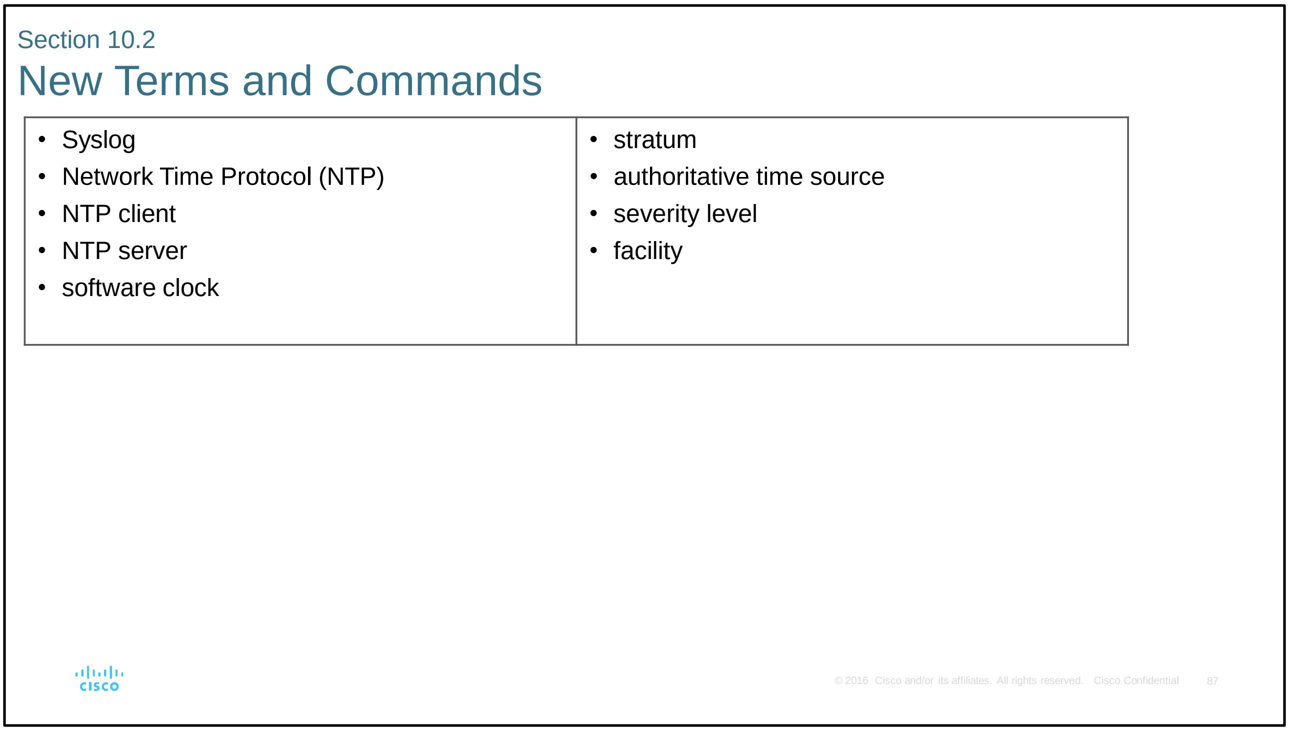


Section

New Terms and Commands

• Cisco Discovery Protocol (CDP)	• Link Layer Discovery Protocol (LLDP)

New Terms and Commands

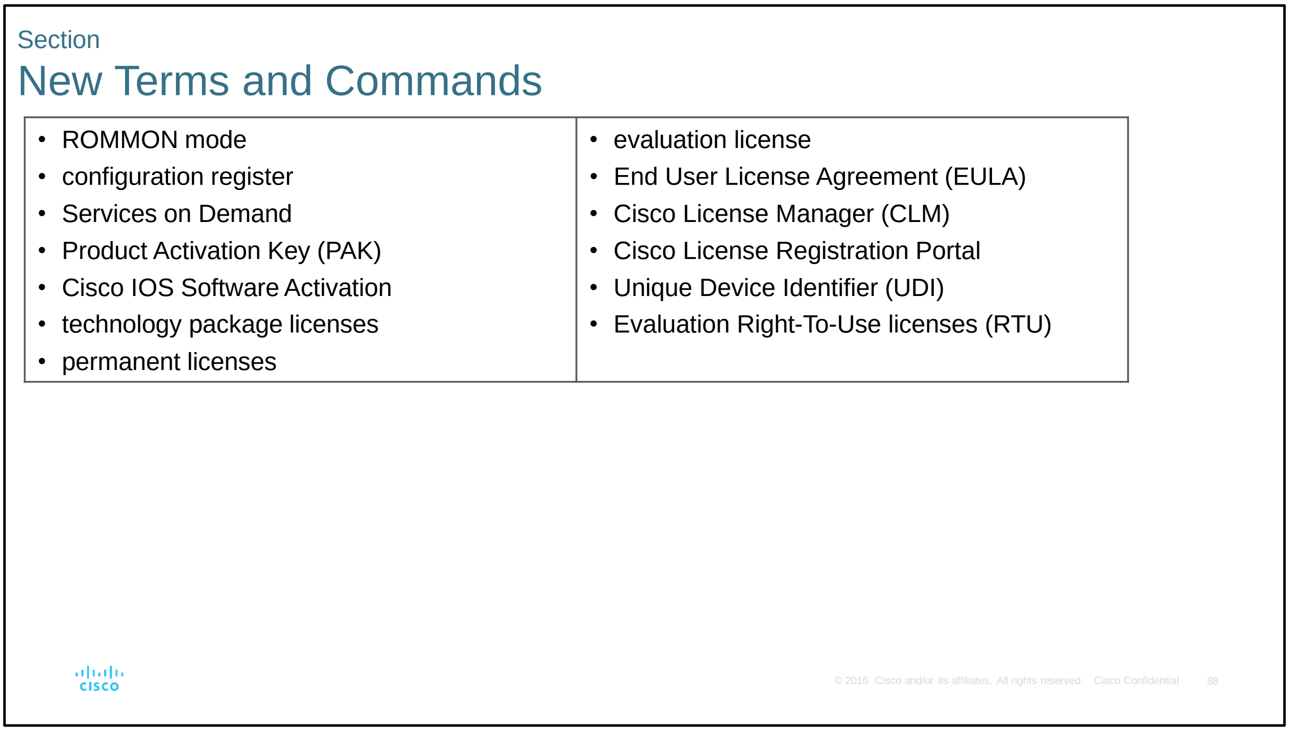


Section 10.2

New Terms and Commands

- Syslog
- Network Time Protocol (NTP)
- NTP client
- NTP server
- software clock
- stratum
- authoritative time source
- severity level
- facility

New Terms and Commands



Section

New Terms and Commands

- ROMMON mode
- configuration register
- Services on Demand
- Product Activation Key (PAK)
- Cisco IOS Software Activation
- technology package licenses
- permanent licenses

- evaluation license
- End User License Agreement (EULA)
- Cisco License Manager (CLM)
- Cisco License Registration Portal
- Unique Device Identifier (UDI)
- Evaluation Right-To-Use licenses (RTU)

New Terms and Commands