Chapter 10 - Sections & Objectives

- **10.1 Device Discovery**
  - Use discovery protocols to map a network topology.
    - Use CDP to map a network topology.
    - Use LLDP to map a network topology.

- **10.2 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.
10.3 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.
10.1 Device Discovery
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
Device Discovery with CDP

Configure and Verify CDP

Verify status and display information

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

```
switch(config)# interface gigabitethernet 0/1
switch(config-if)# no 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, F - Phone,
                D - Remote, C - CVT/Ana, M - Two-Port Mac Relay
Device ID   Local Interce   Holdtime 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
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)

show cdp neighbors detail command provides additional information:

- IPv4 address
- IOS version
Device Discovery with CDP

Discover Devices Using CDP (Cont.)

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

- No more devices to discover!
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
Device Discovery with LLDP

Configure and Verify LLDP

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

Discover Devices Using LLDP

### Sn1 show lldp neighbors
detail

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Local Intf</th>
<th>Hold-time</th>
<th>Capability</th>
<th>Port ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Fa0/5</td>
<td>99</td>
<td>R</td>
<td>G10/1</td>
</tr>
<tr>
<td>S2</td>
<td>Fa0/4</td>
<td>120</td>
<td>B</td>
<td>Fa0/4</td>
</tr>
</tbody>
</table>

Total entries displayed: 2

---

### Sn1 show lldp neighbors
detail

Chassis id : fc99.4775.c3e0
Port id : G10/1
Port Description : gigabitethernet0/1
System Name : S1

System description:
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(3)EQ,
RELEASE SOFTWARE (fc6)
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 : 0cd9.96d2.3fb0
Port id : Fa0/4
Port Description : FastEthernet0/4
System Name : S2
10.2 Device Management
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
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
Configure Stratum 2 NTP Server

- Configure Stratum 2 NTP Server
- Verify NTP Server Configuration
- R1 is synchronized with a stratum 1 NTP server at 209.165.200.225 which is synchronized with a GPS clock
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, - outlier, 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 12/18/2016 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
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
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
Cisco devices produce syslog messages as a result of network events.

Every syslog message contains a severity level and a facility.

- Smaller are more critical

### Syslog Message Format

<table>
<thead>
<tr>
<th>Severity Name</th>
<th>Severity Level</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>Level 0</td>
<td>System Unusable</td>
</tr>
<tr>
<td>Alert</td>
<td>Level 1</td>
<td>Immediate Action Needed</td>
</tr>
<tr>
<td>Critical</td>
<td>Level 2</td>
<td>Critical Condition</td>
</tr>
<tr>
<td>Error</td>
<td>Level 3</td>
<td>Error Condition</td>
</tr>
<tr>
<td>Warning</td>
<td>Level 4</td>
<td>Warning Condition</td>
</tr>
<tr>
<td>Notification</td>
<td>Level 5</td>
<td>Normal, but Significant Condition</td>
</tr>
<tr>
<td>Informational</td>
<td>Level 6</td>
<td>Informational Message</td>
</tr>
<tr>
<td>Debugging</td>
<td>Level 7</td>
<td>Debugging Message</td>
</tr>
</tbody>
</table>
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.
Syslog Operation

Syslog Message Format (Cont.)

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

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

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

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

Syslog Server

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

Default Logging

By default, log messages sent to the console.

Some 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.
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
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 23:15:48.418: %SYS-5-CONFIG_I: Configured from console by console

R1#
10.3 Device Maintenance
Router and Switch File Maintenance

Router File Systems

- **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 *

<table>
<thead>
<tr>
<th>Size(b)</th>
<th>Free(b)</th>
<th>Type</th>
<th>Flags</th>
<th>Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>archive:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>system:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>tmpsys:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>null:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rw</td>
<td>tftp:</td>
</tr>
<tr>
<td>* 256487424</td>
<td>183234560</td>
<td>disk</td>
<td>rw</td>
<td>flash0: flash:#</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>disk</td>
<td>rw</td>
<td>flash1:</td>
</tr>
<tr>
<td>262136</td>
<td>254779</td>
<td>nvram</td>
<td>rw</td>
<td>nvram:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>wo</td>
<td>syslog:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>xmodem:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>ymodem:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rw</td>
<td>rcp:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rw</td>
<td>http:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rw</td>
<td>ftp:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rw</td>
<td>scp:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>ro</td>
<td>tftp:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rw</td>
<td>https:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>ro</td>
<td>cns:</td>
</tr>
</tbody>
</table>
Router and Switch File Maintenance

Router File Systems (Cont.)

- **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:/

1 -rw- 2903 Sep 7 2012 06:50:26 +00:00 cpconfig-19xx.cfg
2 -rw- 3003230 Sep 7 2012 06:50:40 +00:00 cpeexpress.tar
3 -rw- 1038 Sep 7 2012 06:50:52 +00:00 home.shtml
4 -rw- 122880 Sep 7 2012 06:51:02 +00:00 home.tar
5 -rw- 1697952 Sep 7 2012 06:51:20 +00:00 securedesktop-ios-3.1.1.45-x9.pkg
6 -rw- 415956 Sep 7 2012 06:51:34 +00:00 supclient-win-1.1.4.176.pkg
7 -rw- 67998028 Sep 26 2012 17:32:14 +00:00 o1900-universalk9-mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 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
Router and Switch File Maintenance

Switch File Systems

```
Switch# show file systems
File Systems:

<table>
<thead>
<tr>
<th>Size(b)</th>
<th>Free(b)</th>
<th>Type</th>
<th>Flags</th>
<th>Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 32514048</td>
<td>20887552</td>
<td>flash</td>
<td>rw</td>
<td>flash:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>rw</td>
<td>vb:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>ro</td>
<td>bs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>rw</td>
<td>system:</td>
</tr>
<tr>
<td>65536</td>
<td>48897</td>
<td>nvram</td>
<td>rw</td>
<td>nvrmas:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>ro</td>
<td>xmodem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>ro</td>
<td>ymodem:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>rw</td>
<td>null:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>ro</td>
<td>tar:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network</td>
<td>rw</td>
<td>tftp:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network</td>
<td>rw</td>
<td>rcp:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network</td>
<td>rw</td>
<td>http:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network</td>
<td>rw</td>
<td>ftp:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network</td>
<td>rw</td>
<td>scp:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network</td>
<td>rw</td>
<td>https:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opaque</td>
<td>ro</td>
<td>cns:</td>
</tr>
</tbody>
</table>
```

Command is same as with the router!
Router and Switch File Maintenance
Back up and Restore 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.
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.
Router and Switch File Maintenance

Back up and Restore 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]
```
Router and Switch File Maintenance

Using USB Ports on a Cisco Router

- 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.
# 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 194819712 disk rw flash0: flash0:
  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 ushflash rw  ushflash0:
```

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

Shows the USB port and name: “ushflash0:”
Router and Switch File Maintenance

Backing up and Restoring Using USB (Cont.)

- **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
Router and Switch File Maintenance

Backing up and Restoring Using USB (Cont.)

- 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
Router and Switch File Maintenance
Password Recovery

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

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.
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.
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.
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
```
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)
```
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.

```
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
```
IOS Image Management

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

```
Verify free flash size.
R1# show flash:
-# --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)
```
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.

  ```
  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
  ```

- 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.
Objective:

- Use a TFTP server to upload an updated IOS image file to a Cisco Router.
- Use the boot system command to boot the router to the new IOS image file.
- Reload the router and successfully boot to the new IOS image file.
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)
• 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
Step 1. Purchase the Software Package or Feature to Install

- 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 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#`
```
Step 3. Install the License

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.
**License Verification and Management**

**License Verification**

### Permanent License Verification

```
R1# show version
License Info:
License UDI:

<table>
<thead>
<tr>
<th>Device#</th>
<th>FID</th>
<th>SN</th>
</tr>
</thead>
<tbody>
<tr>
<td>*0</td>
<td>CISCO1941/K9</td>
<td>P7X1636848Z</td>
</tr>
</tbody>
</table>

Technology Package License Information for Module:'c1900'

<table>
<thead>
<tr>
<th>Technology</th>
<th>Package</th>
<th>Technology-package</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipbase</td>
<td>ipbasek9</td>
<td>ipbasek9</td>
</tr>
<tr>
<td>security</td>
<td>seck9</td>
<td>seck9</td>
</tr>
<tr>
<td>uc</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>data</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
```

### 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 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>
```
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 6883108 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#
```
License Verification and Management

Uninstall the License

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

**Clearing an Active and Permanent License**

**Step 1. Disable the technology package.**
```
RI(config)# license boot module cl900 technology-package
RI(config)# seck9 disable
RI(config)# exit
RI# reload
```

**Step 2. Clear the license.**
```
RI# license clear seck9
RI# configure terminal
RI(config)# no license boot module cl900 technology-package seck9 disable
RI(config)# exit
RI# reload
```
License Verification and Management

Demonstration - Working with IOS 15 Image Licenses

Objective

• Identify the additional licensing types of Cisco ISR-G2 routers
• Identify the differences between permanent licensing and evaluation right-to-use licensing
• Activate the security technology package on a Cisco 1941 router
• Accept the end user license agreement
• Verify the securityk9 license and save it to flash memory
10.4 Chapter Summary
Conclusion

Packet Tracer – Skills Integration Challenge
Chapter 10: 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.