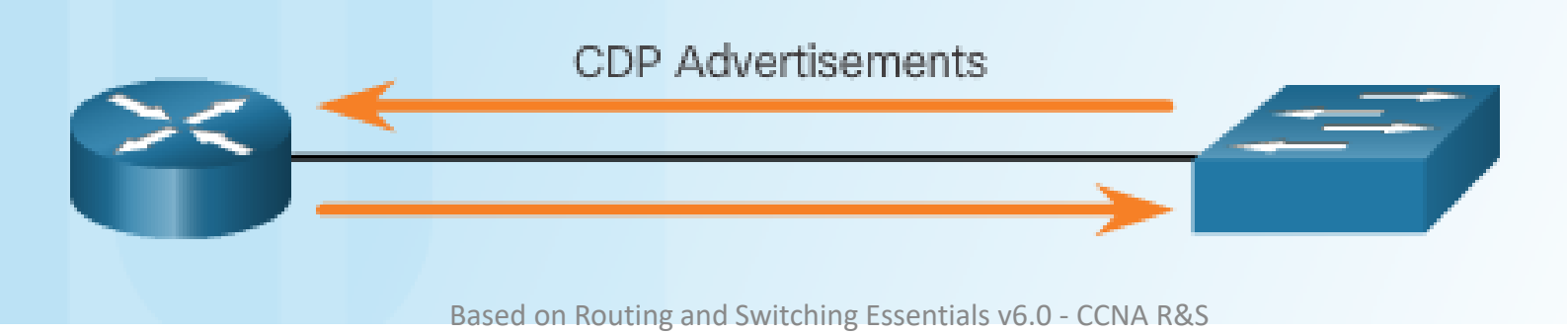
Device Discovery, Management, and Maintenance

Faculty of Technology
University of Sri Jayewardenepura
2019

Device Discovery

Device Discovery with CDP

- 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



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

```
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

```
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 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

Discover Devices Using CDP

- **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

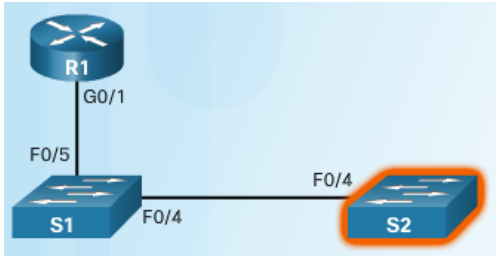
```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

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

```
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=00000000FFFFFFFF010221FF0000000000000002291210380FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 192.168.1.2

Total cdp entries displayed : 1
```

Discover Devices Using CDP


```
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!

Device Discovery with LLDP

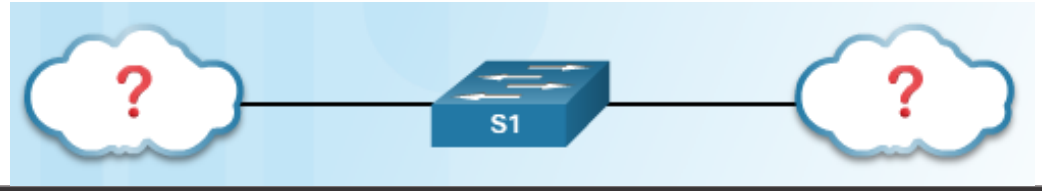
- Link Layer Discovery Protocol
  - Vendor-neutral neighbor discovery similar to CDP
  - Works with routers, switches, and wireless LAN access points
  - Advertises its identity and capabilities to other devices and information from a connected Layer 2 device

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

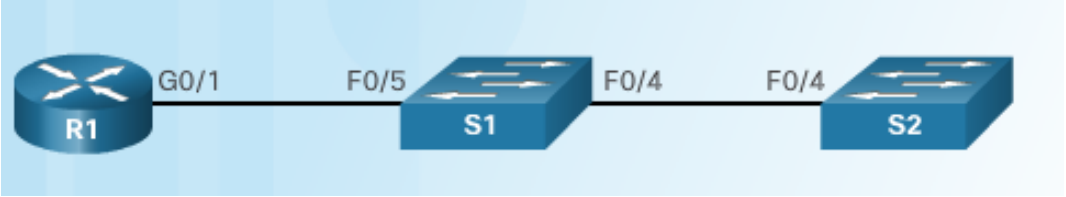
```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp

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
```

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
```



Device Management

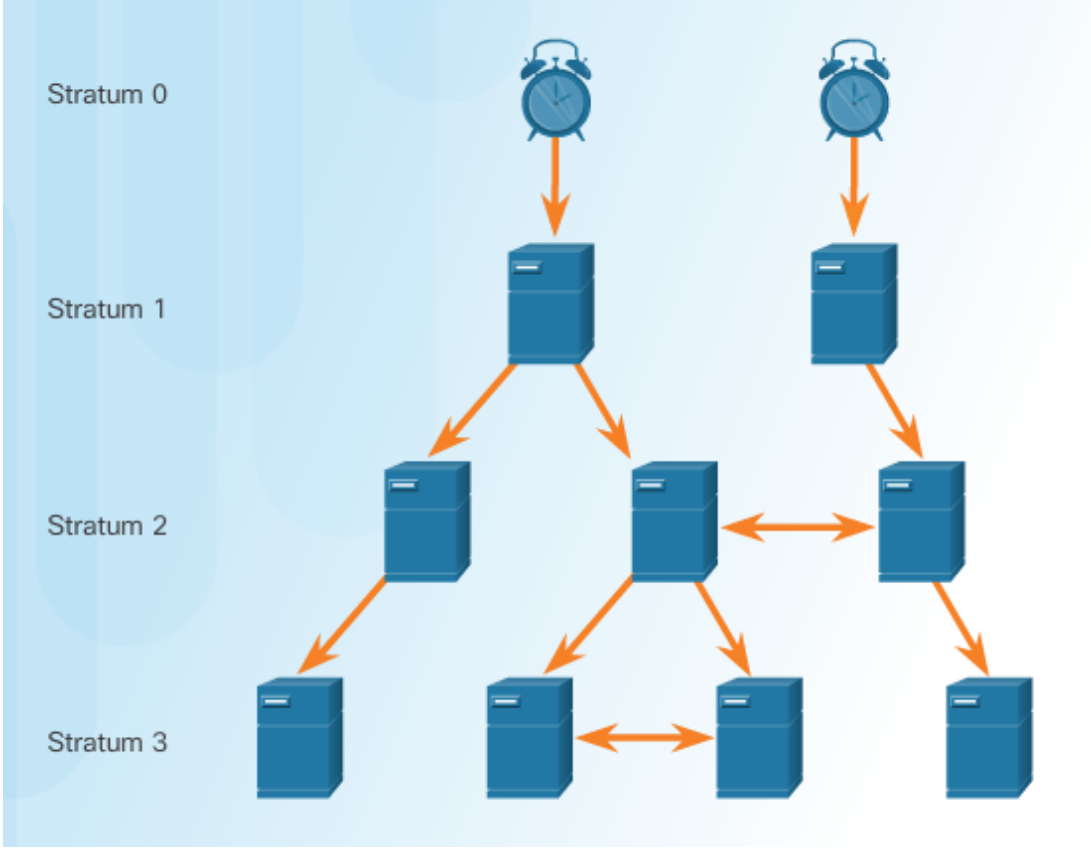
Setting the System Clock

- 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

```
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.
```

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



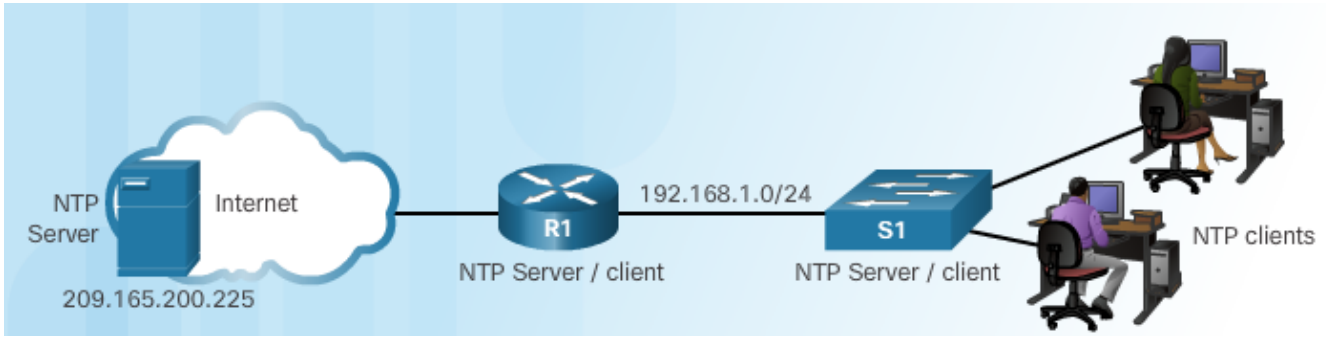
Configure and Verify NTP

- 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
```

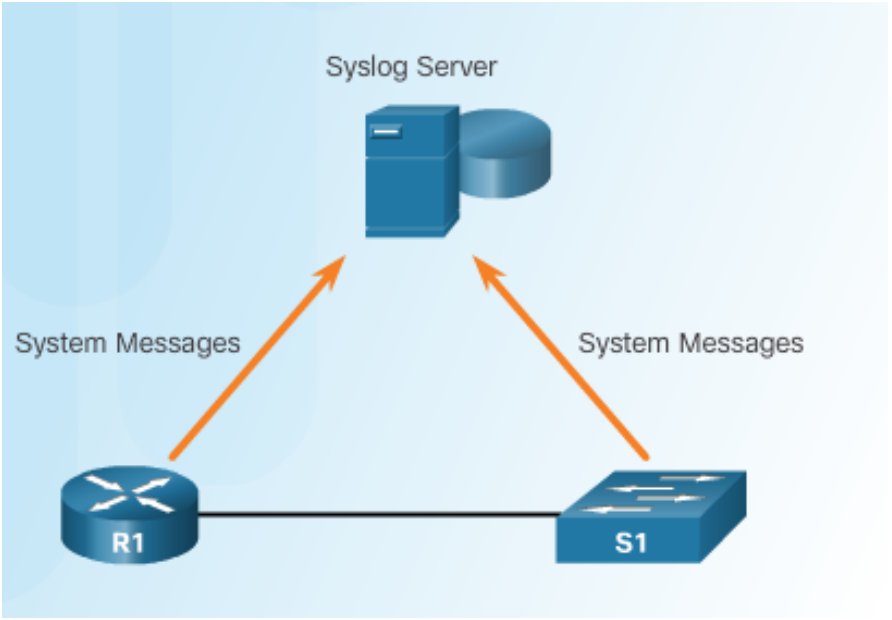
- Verify NTP Server Configuration

```
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.
```



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

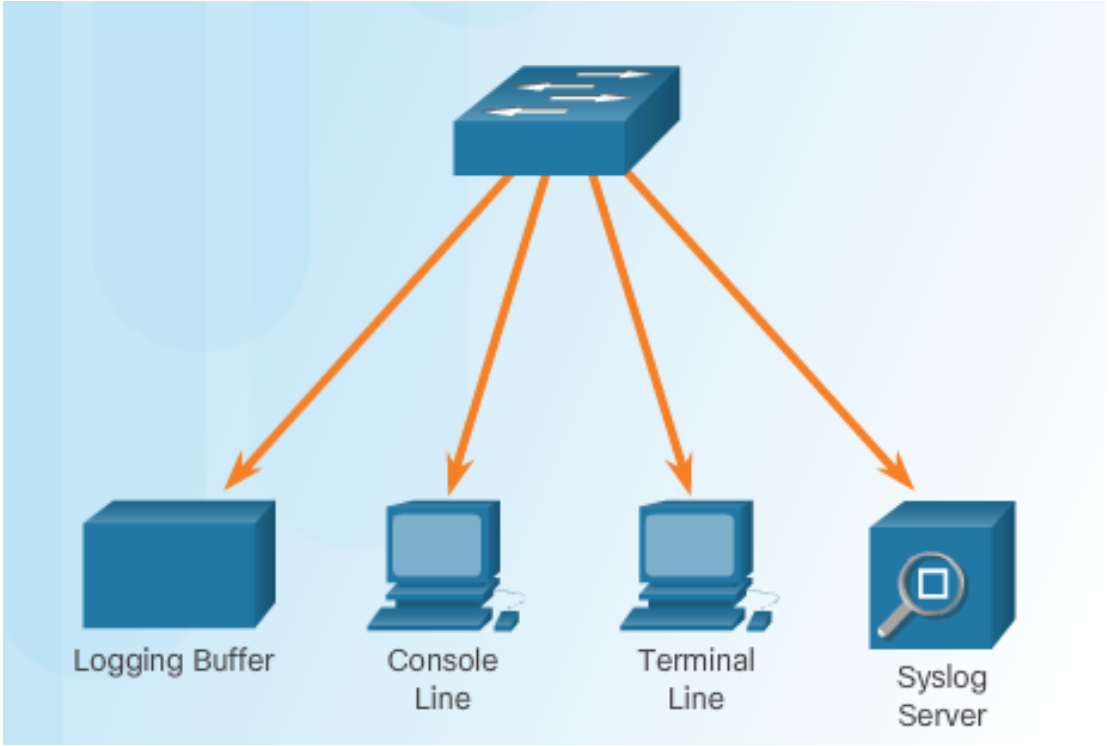
Introduction to Syslog



- 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 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 Message Format

- 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

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

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)#
```

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# 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>
```

Device Maintenance

Router and Switch File Maintenance

```
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:
```

```
Switch# show 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 *

Router File Systems

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


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)
```

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]
```

Password Recovery

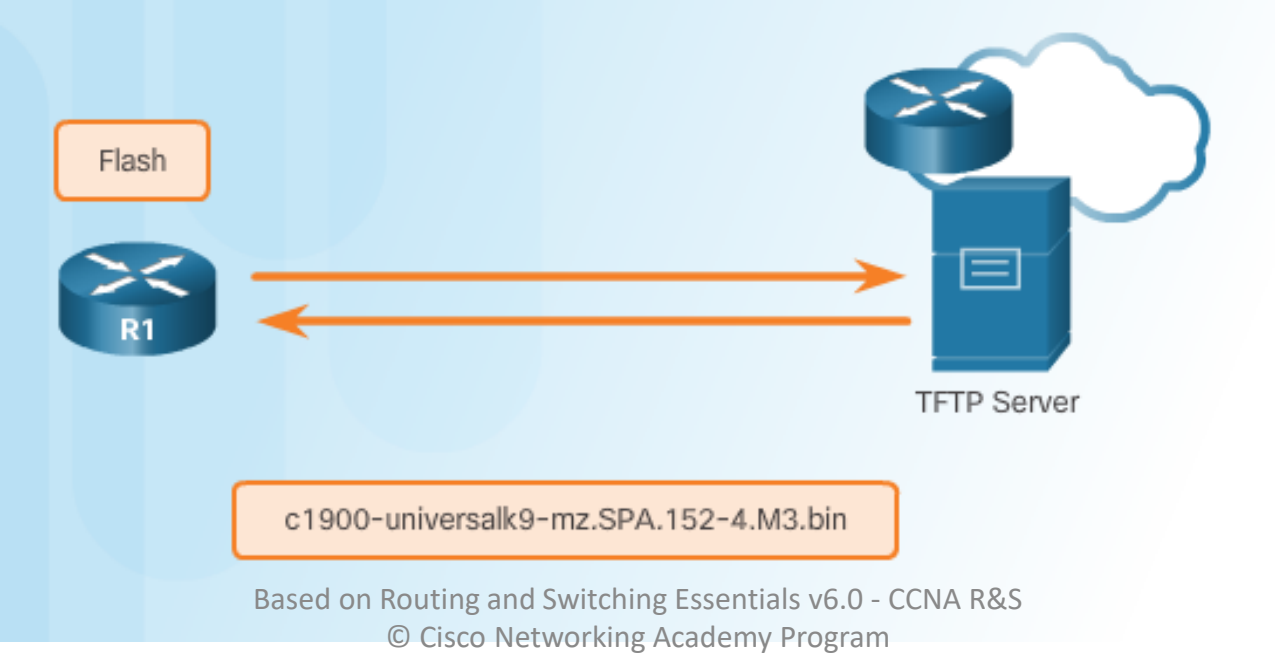
```
Readonly ROMMON initialized

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...
```

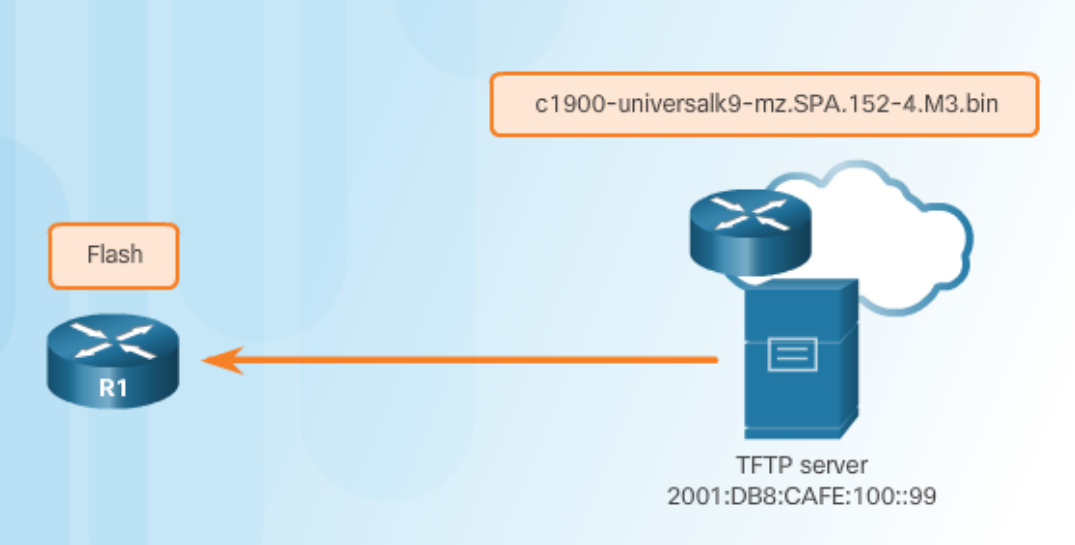
- Step 1. Enter the ROMMON mode.
  - With console access, a user can access the ROMMON mode by using a break sequence during the boot up process or removing the external flash memory when the device is powered off.
- Step 2. Change the configuration register to 0x2142 to ignore the startup config file.
  - 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.

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.



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
```

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.

Summary

- 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.