



# 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.

# 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

# 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



# 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

# 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=00000000FFFFFFFF010221FF00000000000000002291210380FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 192.168.1.2

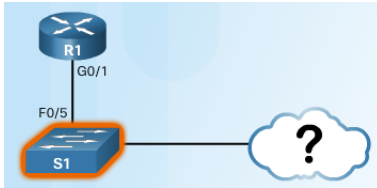
Total cdp entries displayed : 1
```

**show cdp neighbors detail** command provides additional information:

- IPv4 address
- IOS version

# Device Discovery with CDP

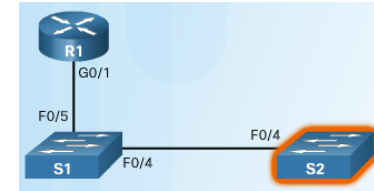
## Discover Devices Using CDP (Cont.)



```
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!



## 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



# Configure and Verify LLDP

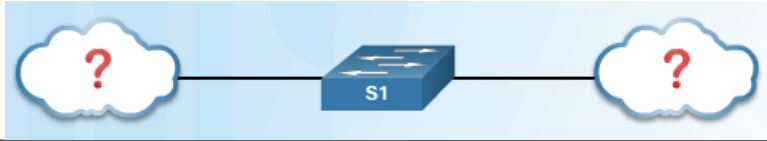
```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp
```

```
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**

# 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
```









## 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

# 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.
```

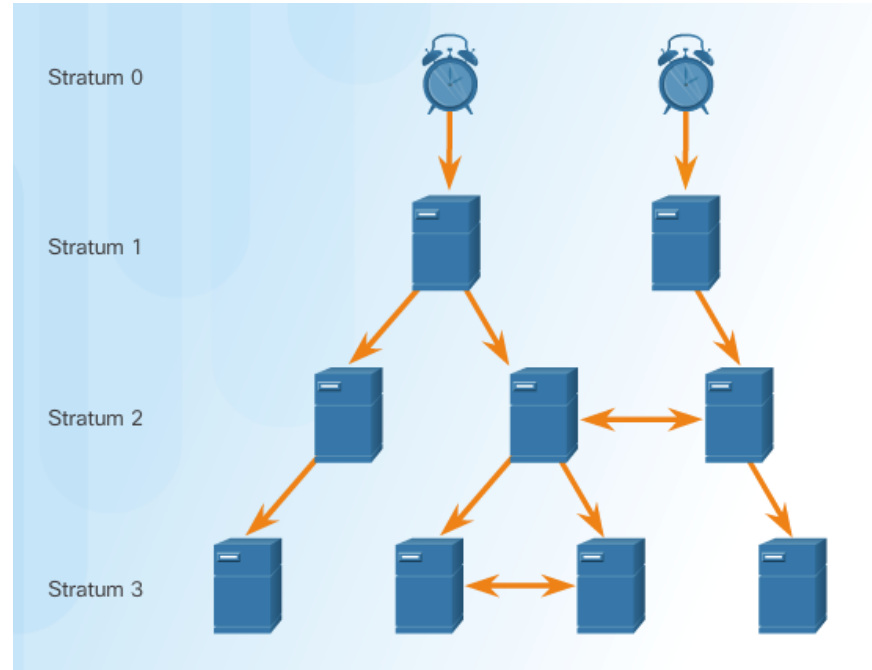
Managing, securing, troubleshooting, and planning networks requires accurate timestamping

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

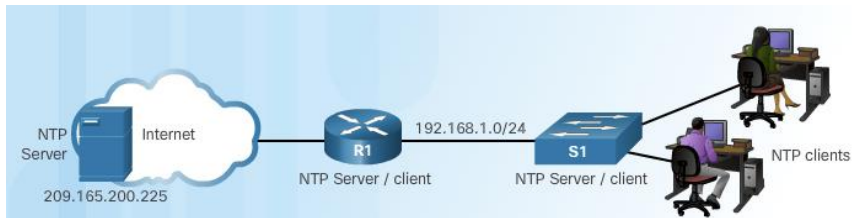
# NTP Operation

- 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

## 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

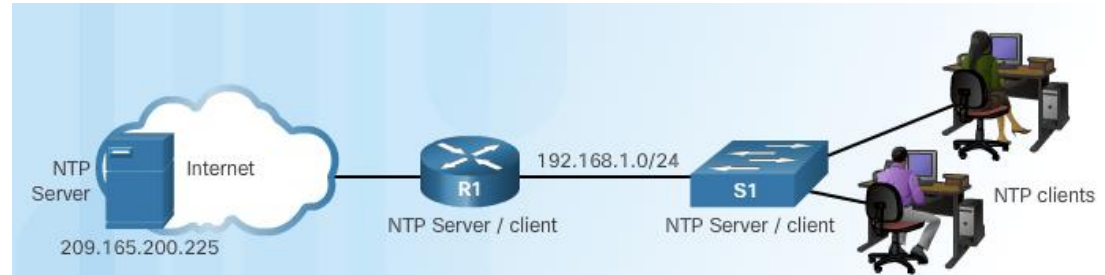
address          ref clock      st  when  poll reach delay offset disp
*~209.165.200.225 .GPS.      1   61    64   377  0.481  7.480  4.261
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

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 (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

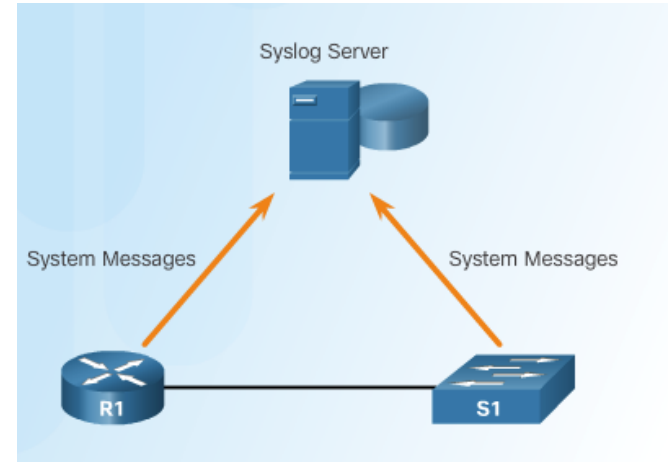
S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Dec 1 2015)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 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

# 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

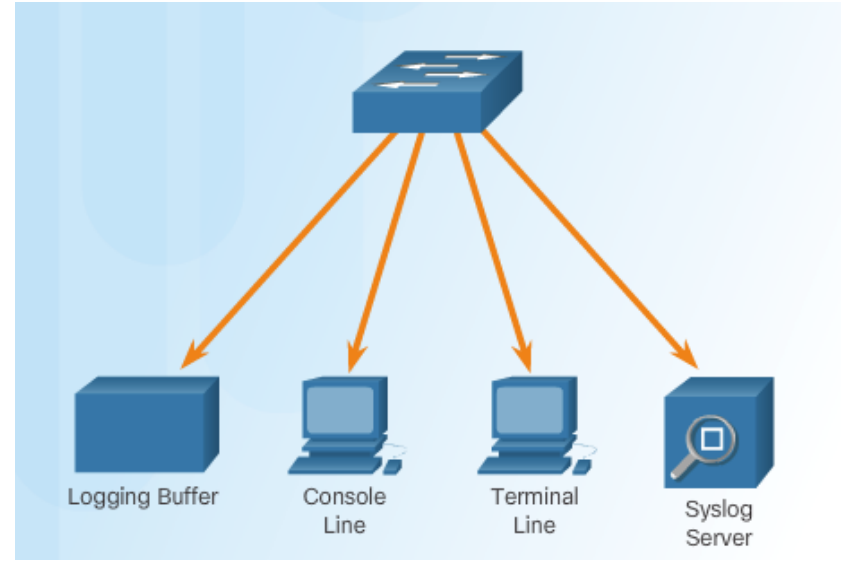


### ▪ Syslog logging service provides three primary functions:

- 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

- 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 (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.

# 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.

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

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

Field	Explanation
seq no	Stamps log messages with a sequence number only if the <code>service sequence-numbers</code> global configuration command is configured.
timestamp	Date and time of the message or event, which appears only if the <code>service timestamps</code> 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.

# 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 down
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)#
```

# 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
```

17:46:01.619

IFMGR

No entry listed

7

NO\_IFINDEX\_FILE

June 12 17:46:01.619

ifIndex-table

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.

22:06:49.642

CHANGED

Interface Loopback0,  
changed state to  
administratively down.

5

LINK

Jun 12 22:06:49.642

LINK-5

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

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

# 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.

No entry listed

SYS-5

000011

5

CONFIG\_I

IFMGR-7

SYS

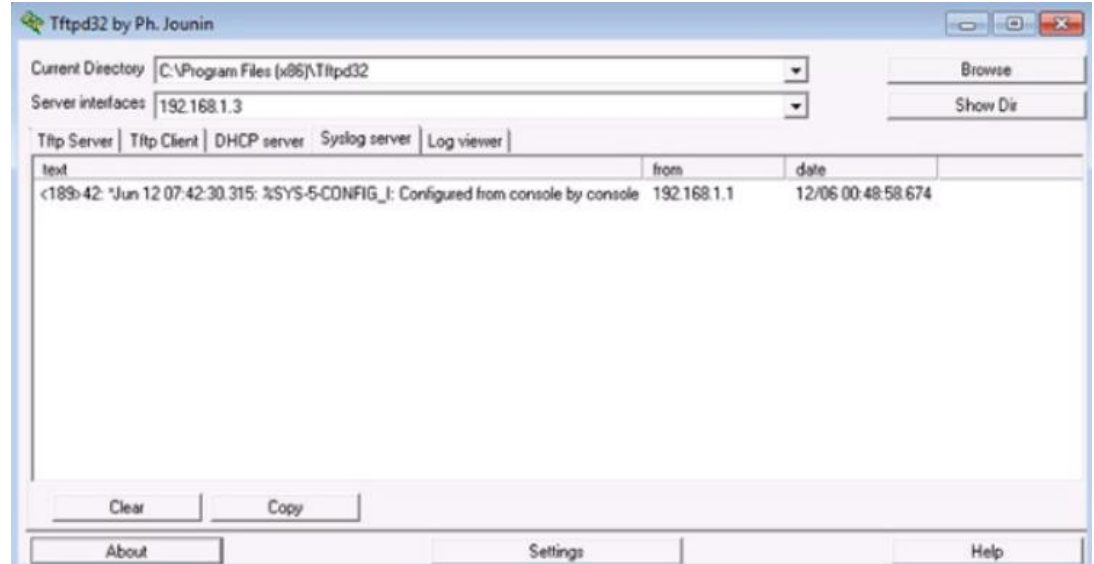
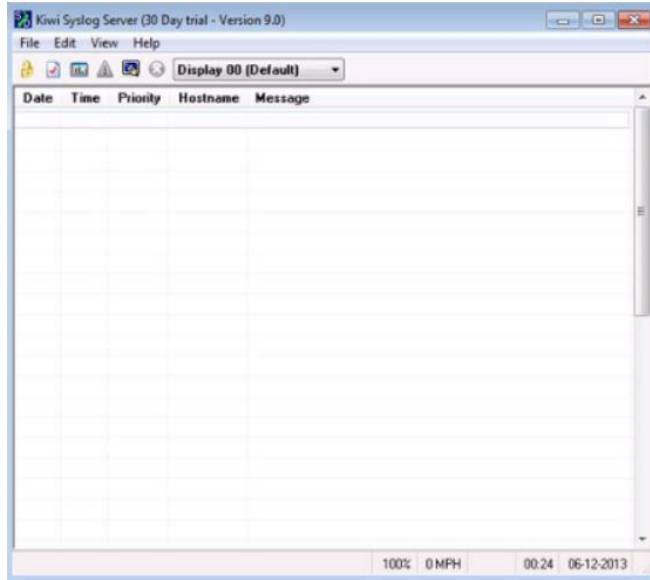
```
*000011: $SYS-5-CONFIG_I: Configured from console by console.
```

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



# 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

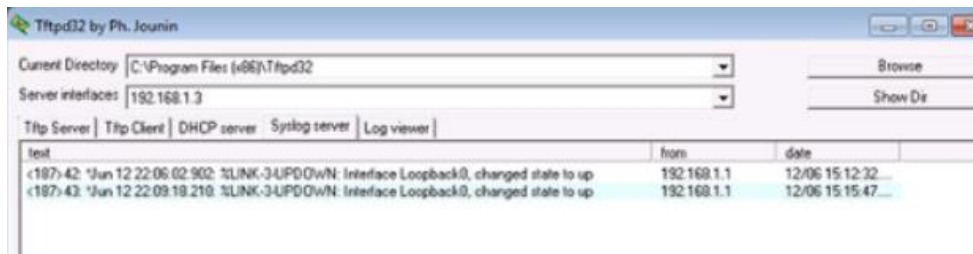
<output omitted>
```

- 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.

# 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



The screenshot shows the Tftpd32 application window with the 'Log viewer' tab selected. It displays two log entries from a syslog server at 192.168.1.3. The first entry is at 12:06:15:12:32 and the second is at 12:06:15:15:47. Both entries report that Interface Loopback0 has changed state to up.

test	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...

# 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#
```

# Chapter Summary

# 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.



# New Terms and Commands

<ul style="list-style-type: none"><li>• Cisco Discovery Protocol (CDP)</li></ul>	<ul style="list-style-type: none"><li>• Link Layer Discovery Protocol (LLDP)</li></ul>
--	--

# New Terms and Commands

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>• Syslog</li><li>• Network Time Protocol (NTP)</li><li>• NTP client</li><li>• NTP server</li><li>• software clock</li></ul> | <ul style="list-style-type: none"><li>• stratum</li><li>• authoritative time source</li><li>• severity level</li><li>• facility</li></ul> |
|---|---|

# New Terms and Commands

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• ROMMON mode</li><li>• configuration register</li><li>• Services on Demand</li><li>• Product Activation Key (PAK)</li><li>• Cisco IOS Software Activation</li><li>• technology package licenses</li><li>• permanent licenses</li></ul> | <ul style="list-style-type: none"><li>• evaluation license</li><li>• End User License Agreement (EULA)</li><li>• Cisco License Manager (CLM)</li><li>• Cisco License Registration Portal</li><li>• Unique Device Identifier (UDI)</li><li>• Evaluation Right-To-Use licenses (RTU)</li></ul> |
|---|--|