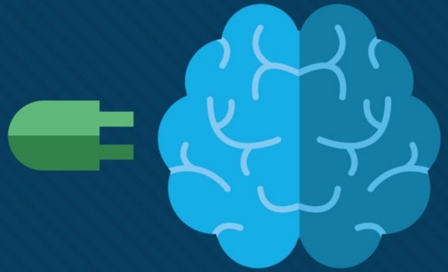


Chapter 10: Device Discovery, Management, and Maintenance

Instructor Materials

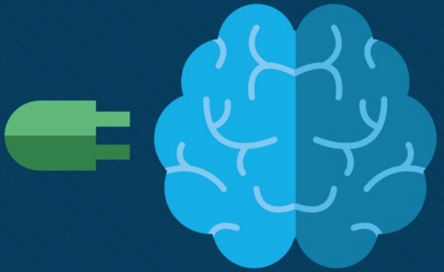
CCNA Routing and Switching

Routing and Switching Essentials v6.0

Chapter 10: Device Discovery, Management, and Maintenance

Routing and Switching Essentials 6.0
Planning Guide

Chapter 10: Device Discovery, Management, and Maintenance



CCNA Routing and Switching

Routing and Switching Essentials v6.0

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.

Chapter 10 - Sections & Objectives (Cont.)

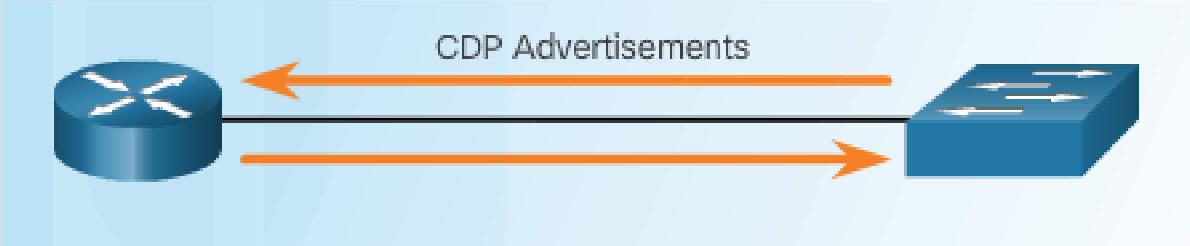
- 10.3 Device Maintenance
  - Maintain router and switch configuration and IOS files.
    - Use commands to back up and restore an IOS configuration file.
    - Explain the IOS image naming conventions implemented by Cisco.
    - Upgrade an IOS system image.
    - Explain the licensing process for Cisco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

10.1 Device Discovery

Device Discovery with CDP

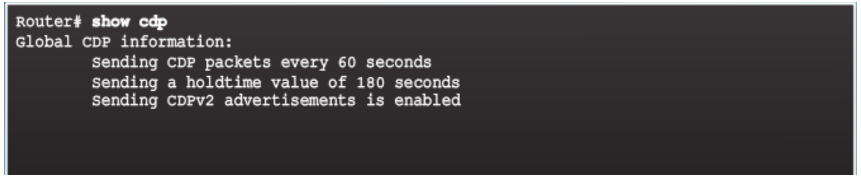
CDP Overview

- 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



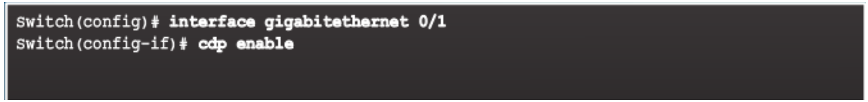
Device Discovery with CDP

Configure and Verify CDP



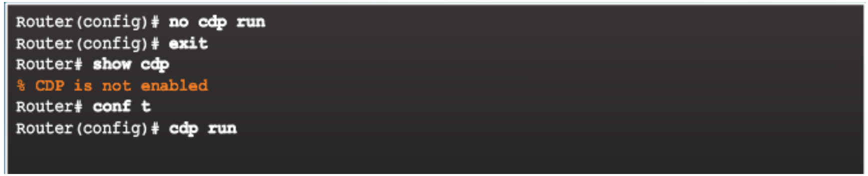
```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

Verify status and display information



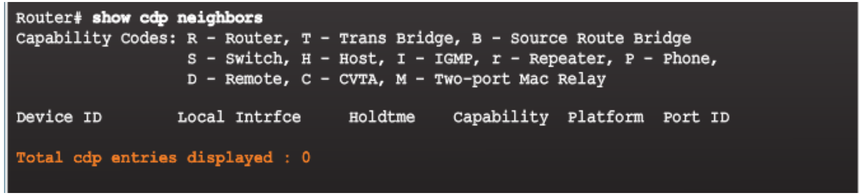
```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# cdp enable
```

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



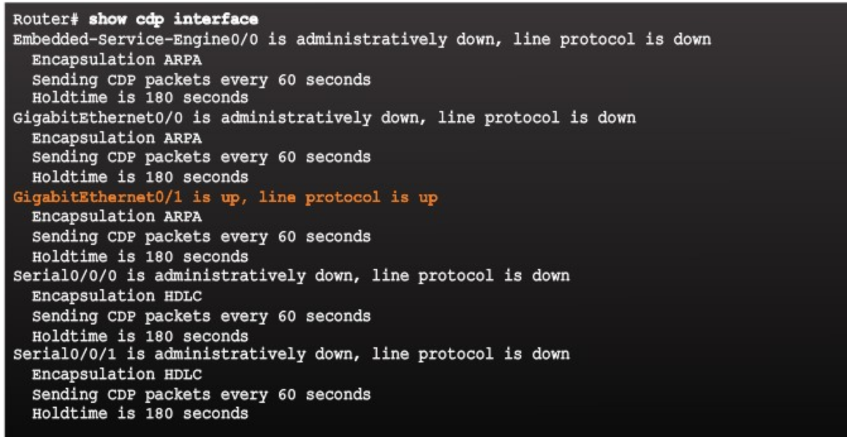
```
Router(config)# no cdp run
Router(config)# exit
Router# show cdp
% CDP is not enabled
Router# conf t
Router(config)# cdp run
```

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
```

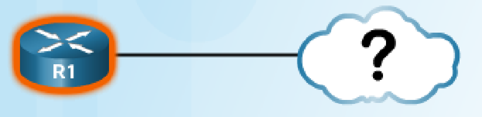
No neighbors detected

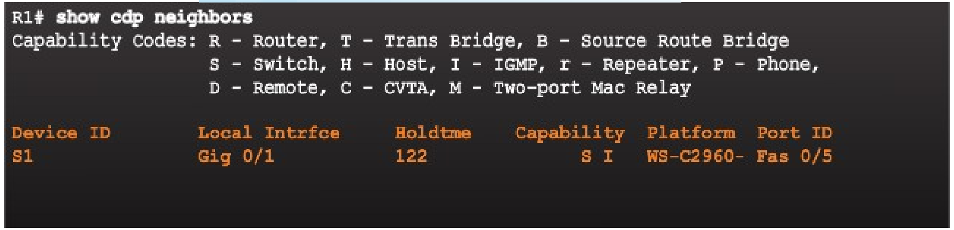


```
Router# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets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

Discover Devices Using CDP

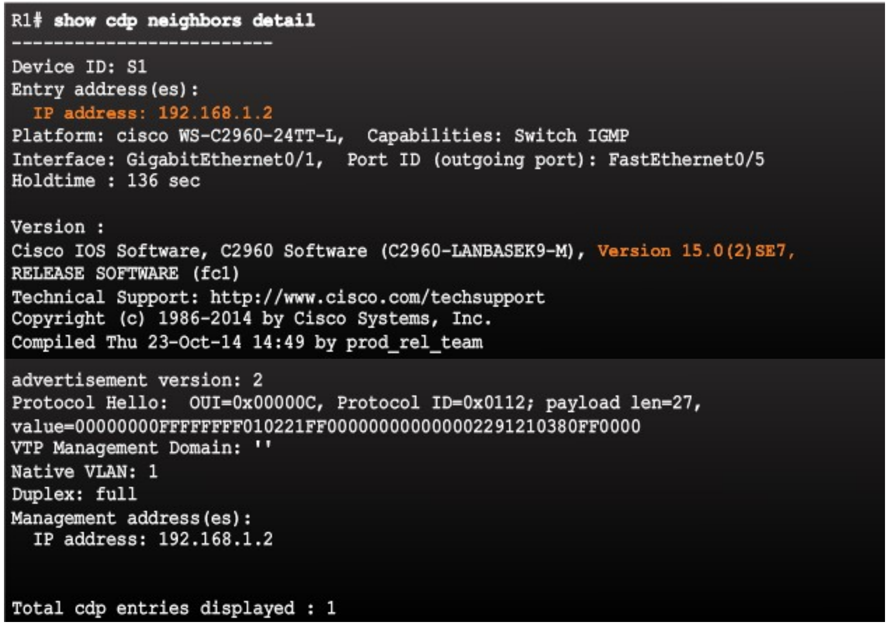




```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

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)



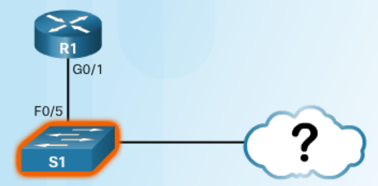
```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

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
```

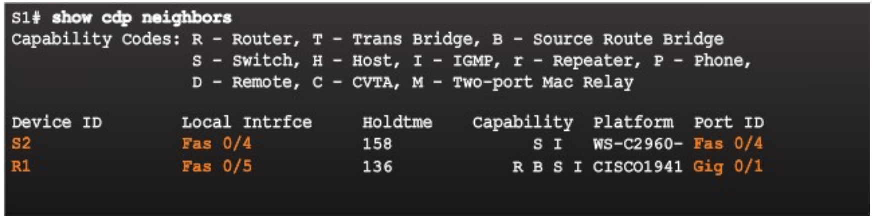
show cdp neighbors detail command provides additional information:

- IPv4 address
- IOS version

Device Discovery with CDP

Discover Devices Using CDP (Cont.)

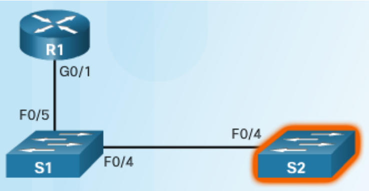


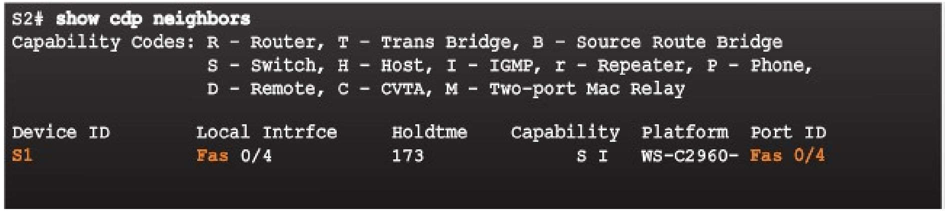


```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

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!



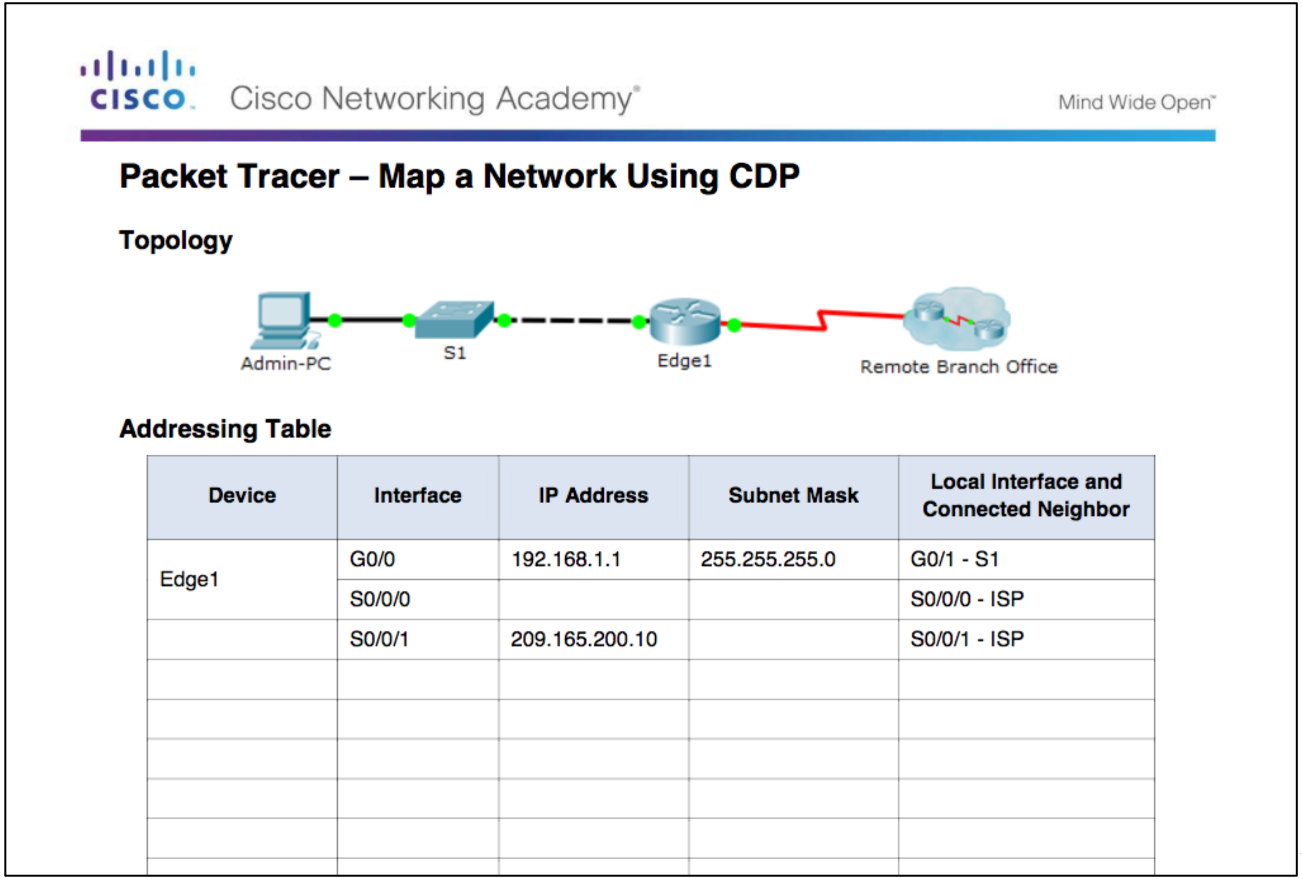


```
S2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

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 CDP

Packet Tracer – Map a Network Using CDP



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Map a Network Using CDP

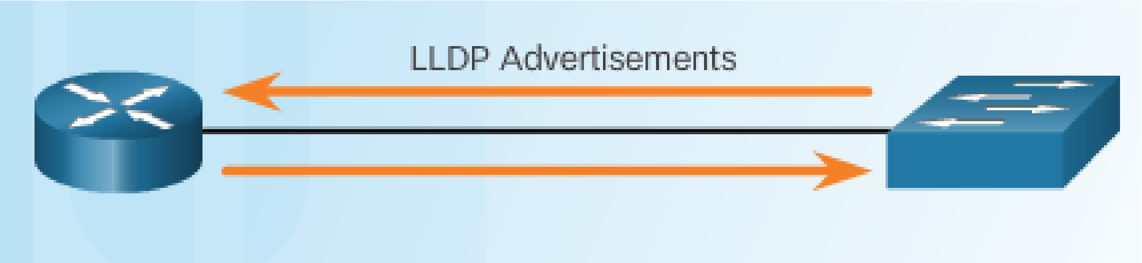
Topology

Addressing Table

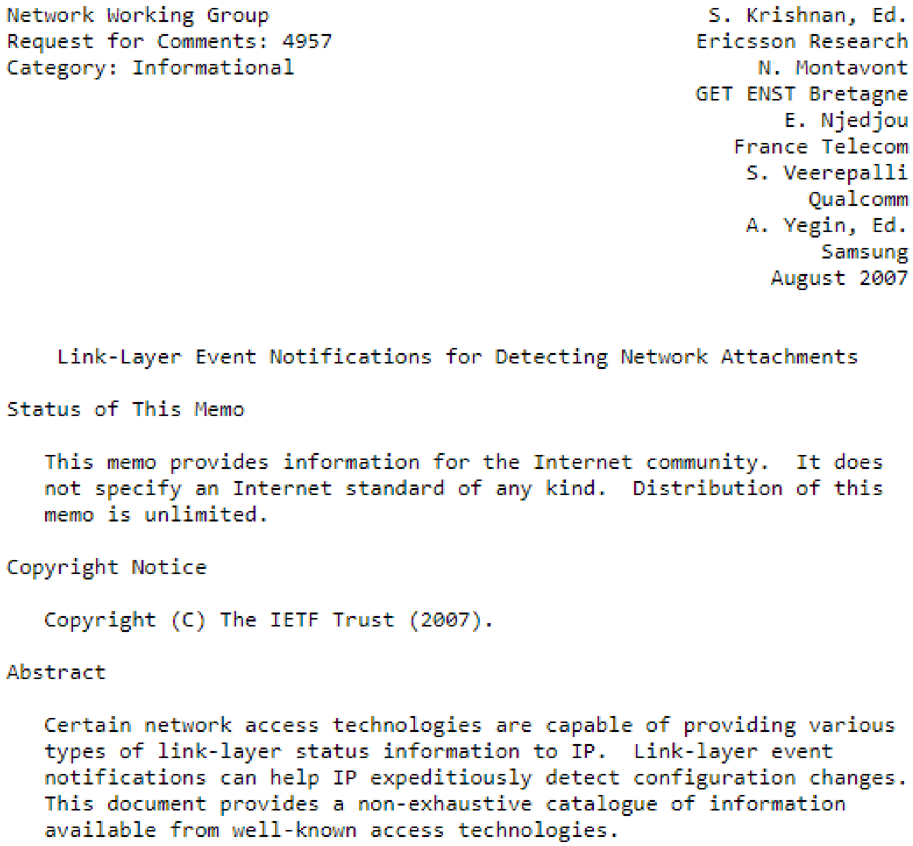
Device	Interface	IP Address	Subnet Mask	Local Interface and Connected Neighbor
Edge1	G0/0	192.168.1.1	255.255.255.0	G0/1 - S1
	S0/0/0			S0/0/0 - ISP
	S0/0/1	209.165.200.10		S0/0/1 - ISP

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



IEEE 802.1AB and IEEE 802.3-2012 section 6 clause 79, i RFC



Network Working Group
Request for Comments: 4957
Category: Informational

S. Krishnan, Ed.
Ericsson Research
N. Montavont
GET ENST Bretagne
E. Njedjou
France Telecom
S. Veerepalli
Qualcomm
A. Yegin, Ed.
Samsung
August 2007

Link-Layer Event Notifications for Detecting Network Attachments

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

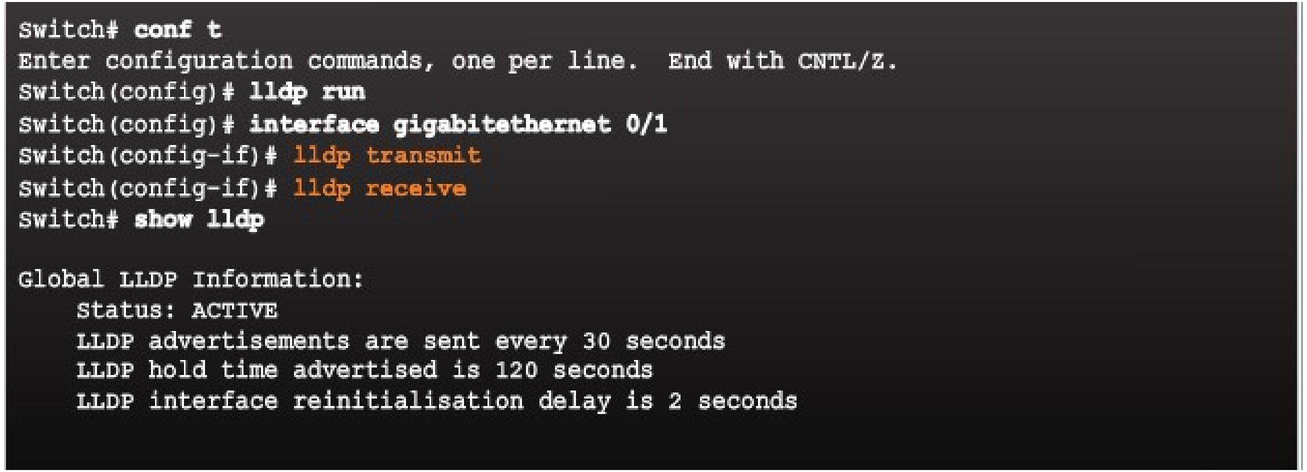
Copyright Notice

Abstract

Certain network access technologies are capable of providing various types of link-layer status information to IP. Link-layer event notifications can help IP expeditiously detect configuration changes. This document provides a non-exhaustive catalogue of information available from well-known access technologies.

Device Discovery with LLDP

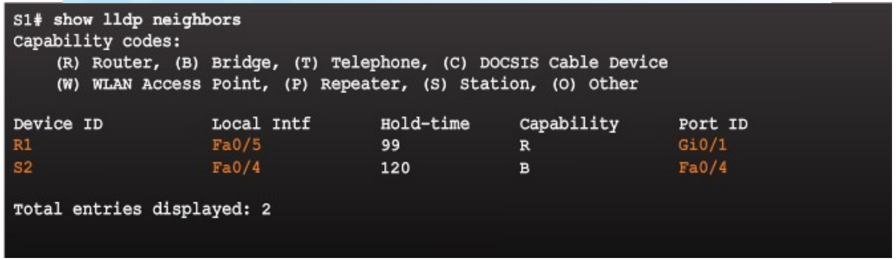
Configure and Verify LLDP



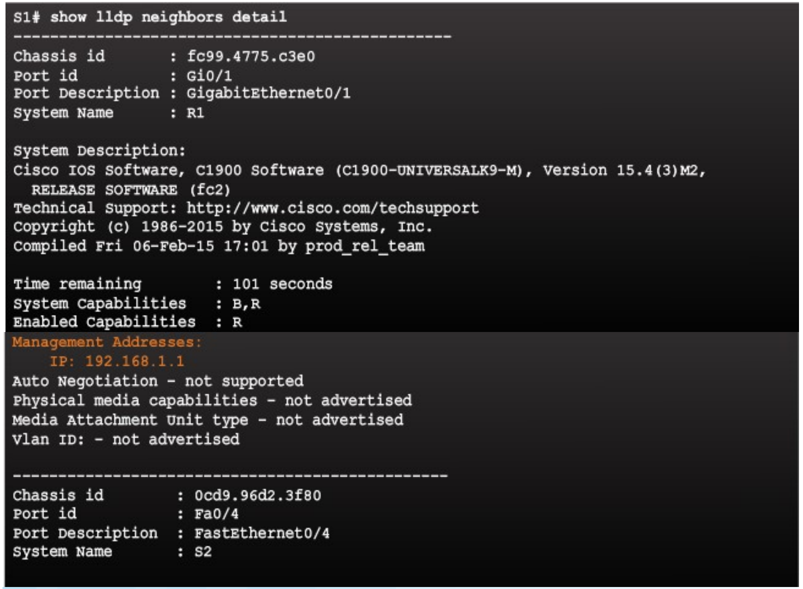
```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp

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**

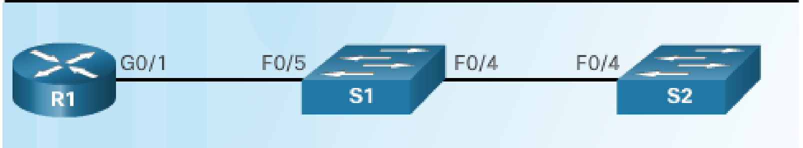
Discover Devices Using LLDP



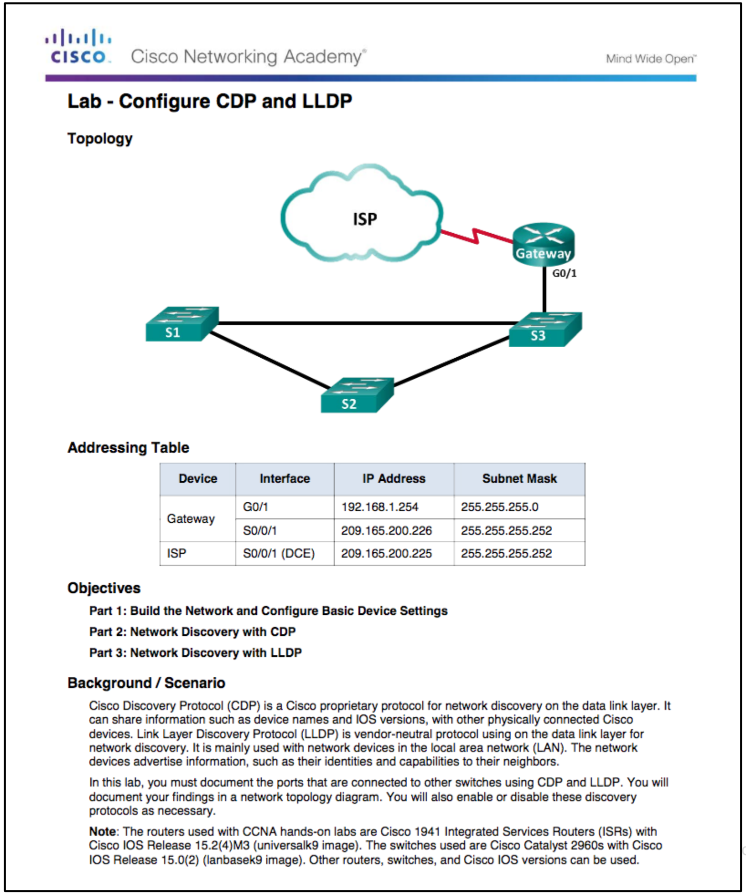
```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

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
```



Lab – Configure CDP and LLDP



Cisco Networking Academy® Mind Wide Open™

Lab - Configure CDP and LLDP

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask
Gateway	G0/1	192.168.1.254	255.255.255.0
	S0/0/1	209.165.200.226	255.255.255.252
ISP	S0/0/1 (DCE)	209.165.200.225	255.255.255.252

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Network Discovery with CDP

Part 3: Network Discovery with LLDP

Background / Scenario

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol for network discovery on the data link layer. It can share information such as device names and IOS versions, with other physically connected Cisco devices. Link Layer Discovery Protocol (LLDP) is vendor-neutral protocol using on the data link layer for network discovery. It is mainly used with network devices in the local area network (LAN). The network devices advertise information, such as their identities and capabilities to their neighbors.

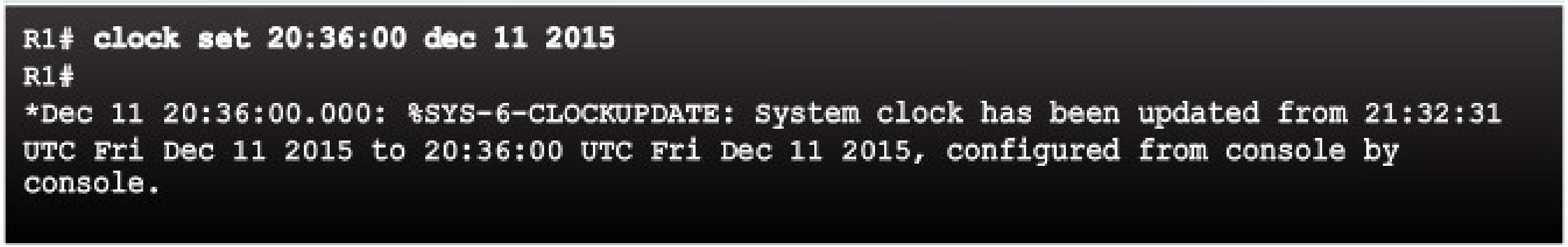
In this lab, you must document the ports that are connected to other switches using CDP and LLDP. You will document your findings in a network topology diagram. You will also enable or disable these discovery protocols as necessary.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used.

10.2 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.
```

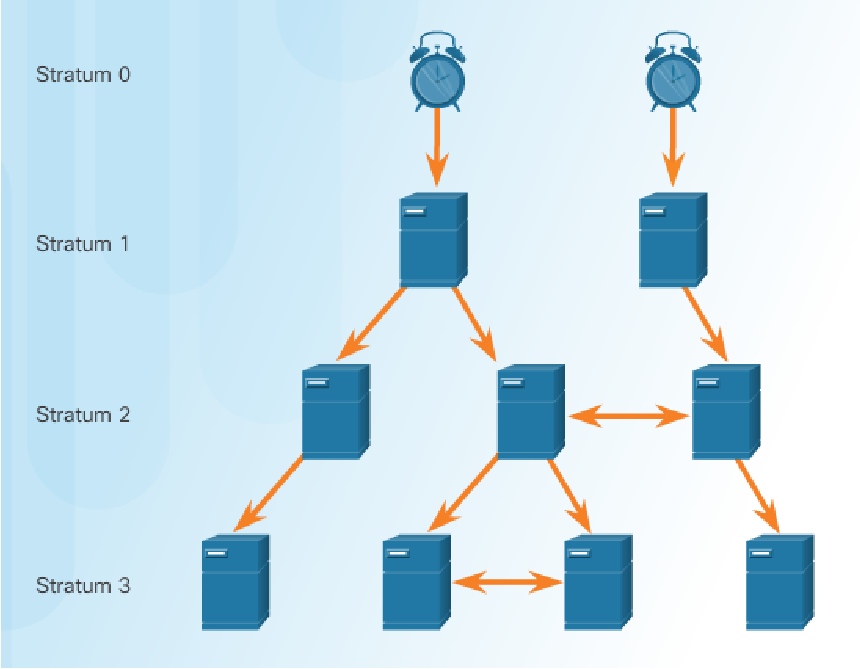
Managing, securing, troubleshooting, and planning networks requires accurate timestamping

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

NTP Operation

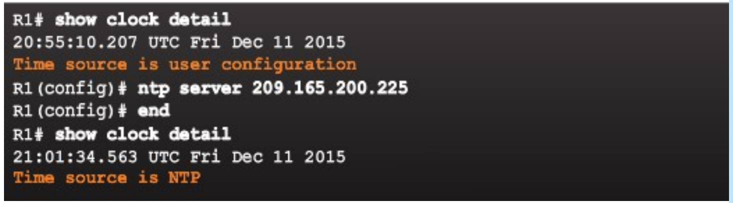
- Stratum 0 – top level of hierarchical system, authoritative time sources, assumed to be accurate
- Stratum 1 – directly connected to authoritative sources and act as primary network time standard
- Stratum 2 and Lower – connected to stratum 1 devices via network connections, act as servers for stratum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



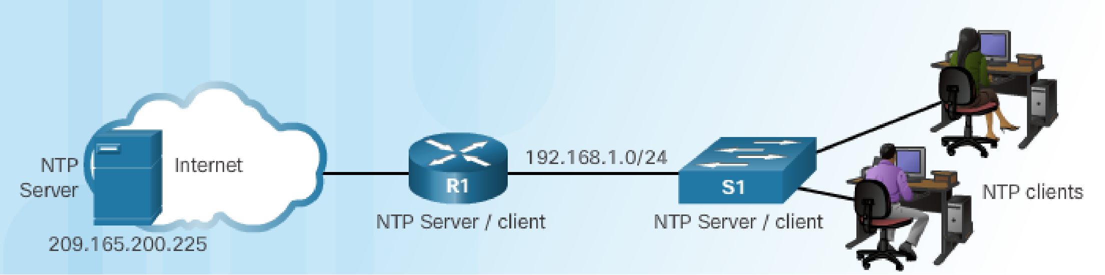
NTP

Configure and Verify NTP

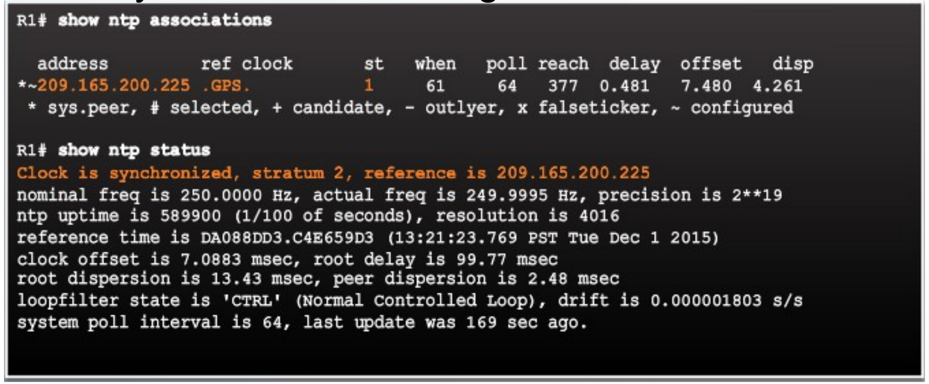
- Configure Stratum 2 NTP Server



```
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



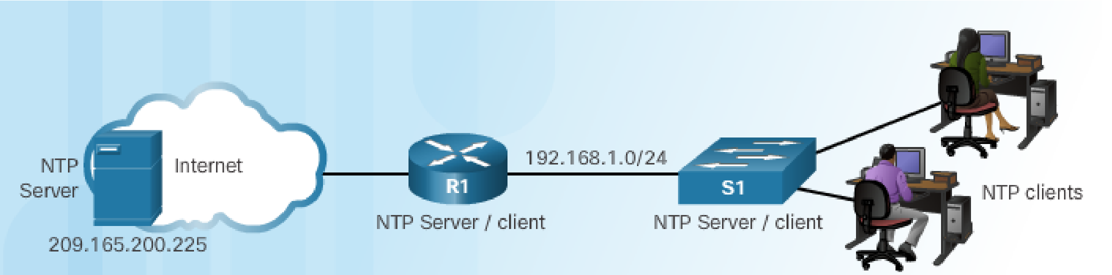
```
R1# show ntp associations

  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.
```

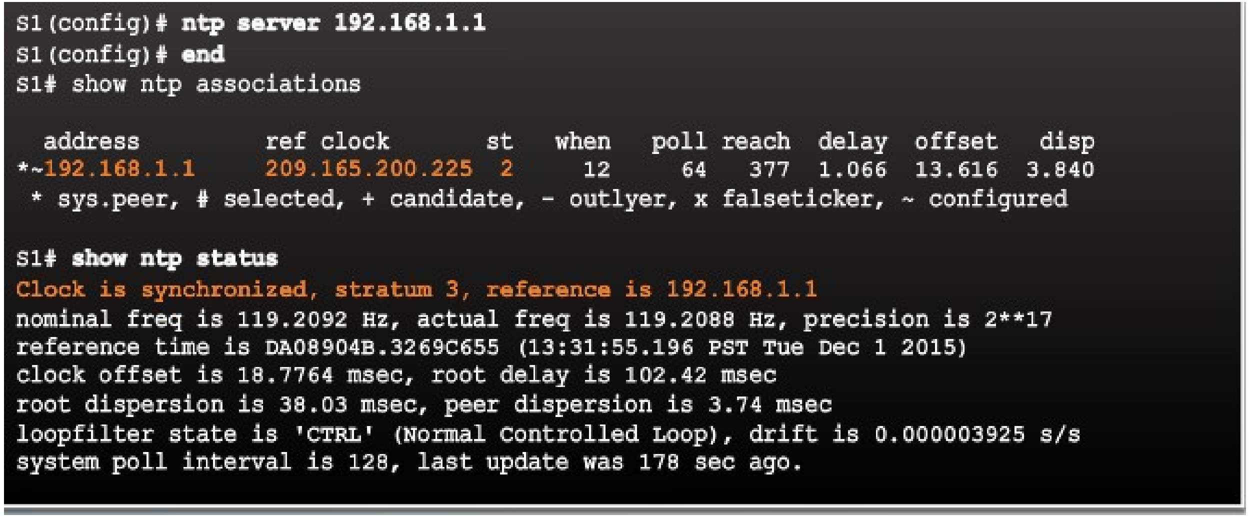
- R1 is synchronized with a stratum 1 NTP server at 209.165.200.225 which is synchronized with a GPS clock

NTP

Configure and Verify NTP (Cont.)

- Configure Stratum 3 NTP Server



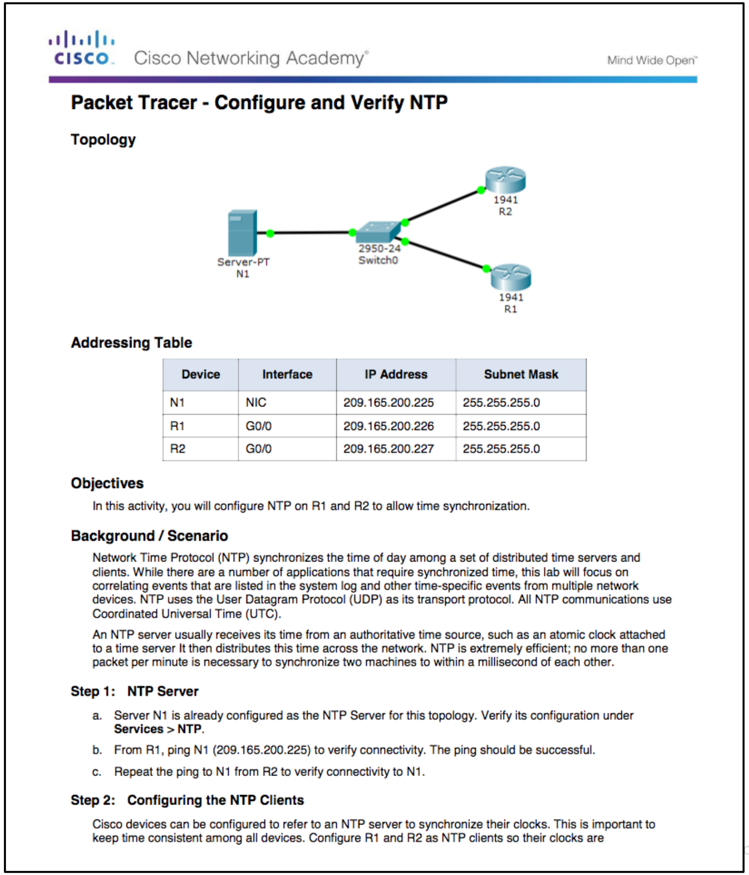


```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations

  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

NTP

Packet Tracer - Configure and Verify NTP



Cisco Networking Academy® Mind Wide Open®

Packet Tracer - Configure and Verify NTP

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask
N1	NIC	209.165.200.225	255.255.255.0
R1	G0/0	209.165.200.226	255.255.255.0
R2	G0/0	209.165.200.227	255.255.255.0

Objectives

In this activity, you will configure NTP on R1 and R2 to allow time synchronization.

Background / Scenario

Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients. While there are a number of applications that require synchronized time, this lab will focus on correlating events that are listed in the system log and other time-specific events from multiple network devices. NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC).

An NTP server usually receives its time from an authoritative time source, such as an atomic clock attached to a time server It then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

Step 1: NTP Server

a. Server N1 is already configured as the NTP Server for this topology. Verify its configuration under **Services** > **NTP**.

b. From R1, ping N1 (209.165.200.225) to verify connectivity. The ping should be successful.

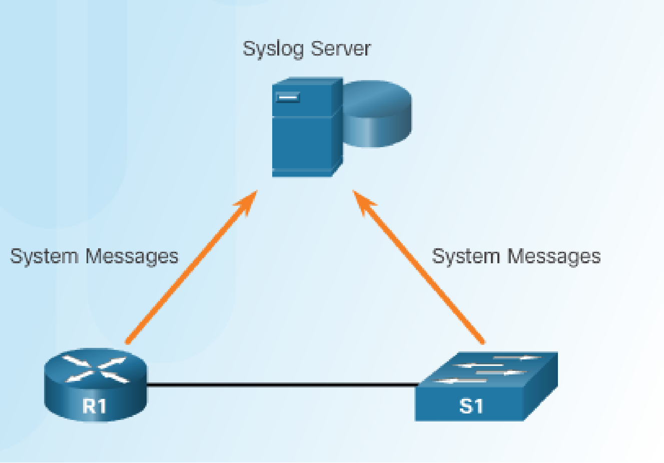
c. Repeat the ping to N1 from R2 to verify connectivity to N1.

Step 2: Configuring the NTP Clients

Cisco devices can be configured to refer to an NTP server to synchronize their clocks. This is important to keep time consistent among all devices. Configure R1 and R2 as NTP clients so their clocks are

Introduction to Syslog

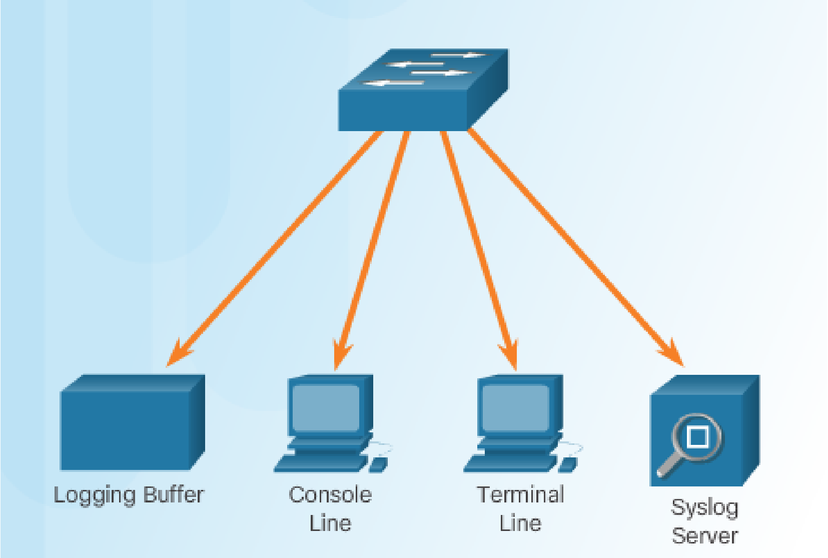
- Syslog
  - Describes a standard and protocol
  - Uses UDP port 514
  - Send event notification messages across IP networks to event message collectors
  - Routers, switches, servers, firewalls support syslog



- 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.

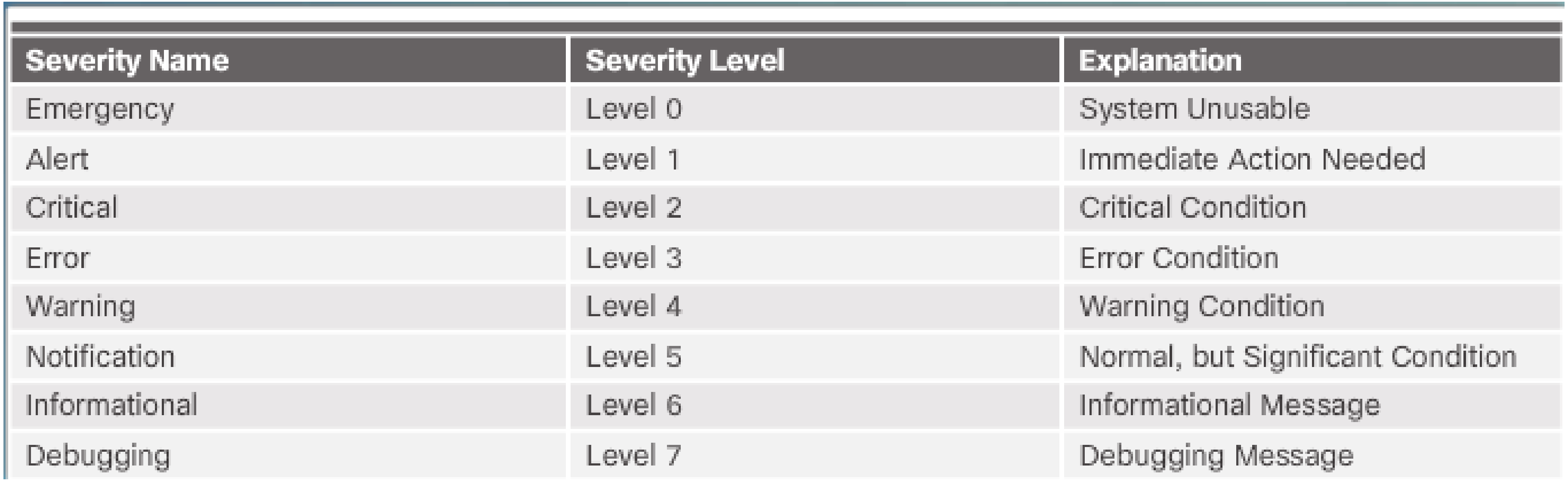


- Destinations for syslog messages include:
  - Logging buffer (RAM inside a router or switch)
  - Console line
  - Terminal line
  - Syslog server

Syslog Operation

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

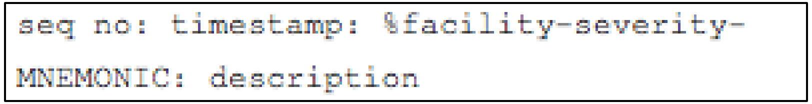
Syslog Message Format (Cont.)

- 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 Operation

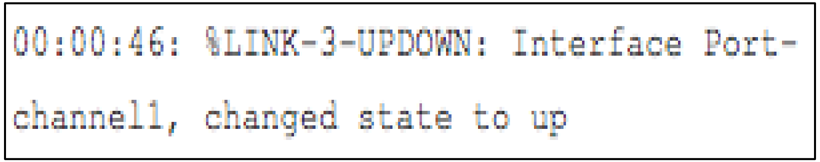
Syslog Message Format (Cont.)

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



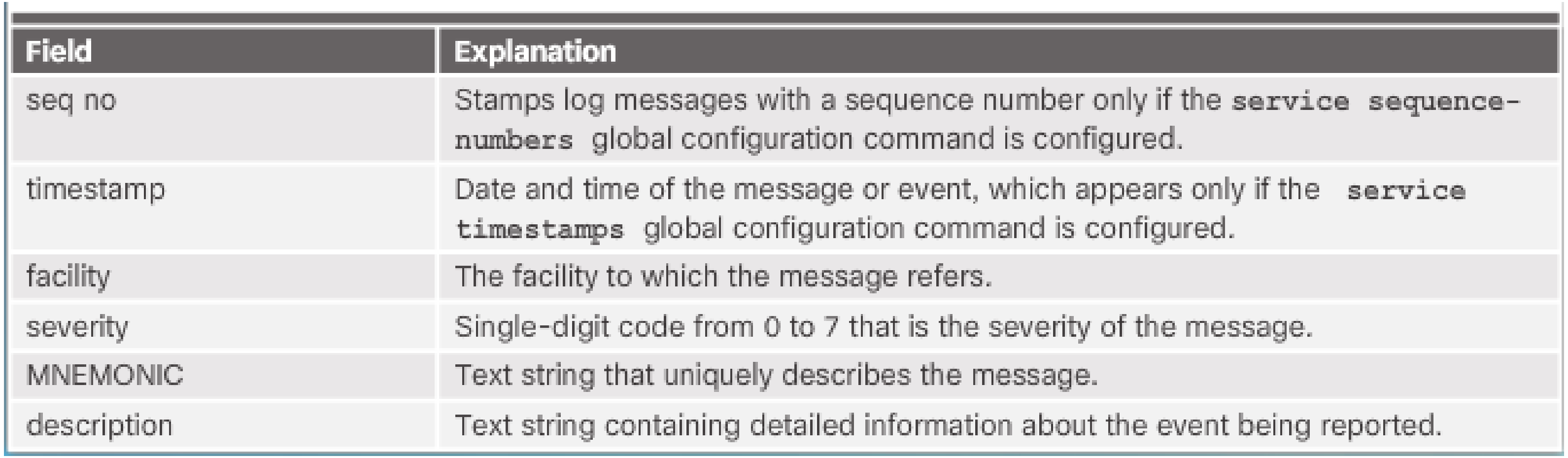
```
seq no: timestamp: %facility-severity-
MNEMONIC: description
```

- 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.

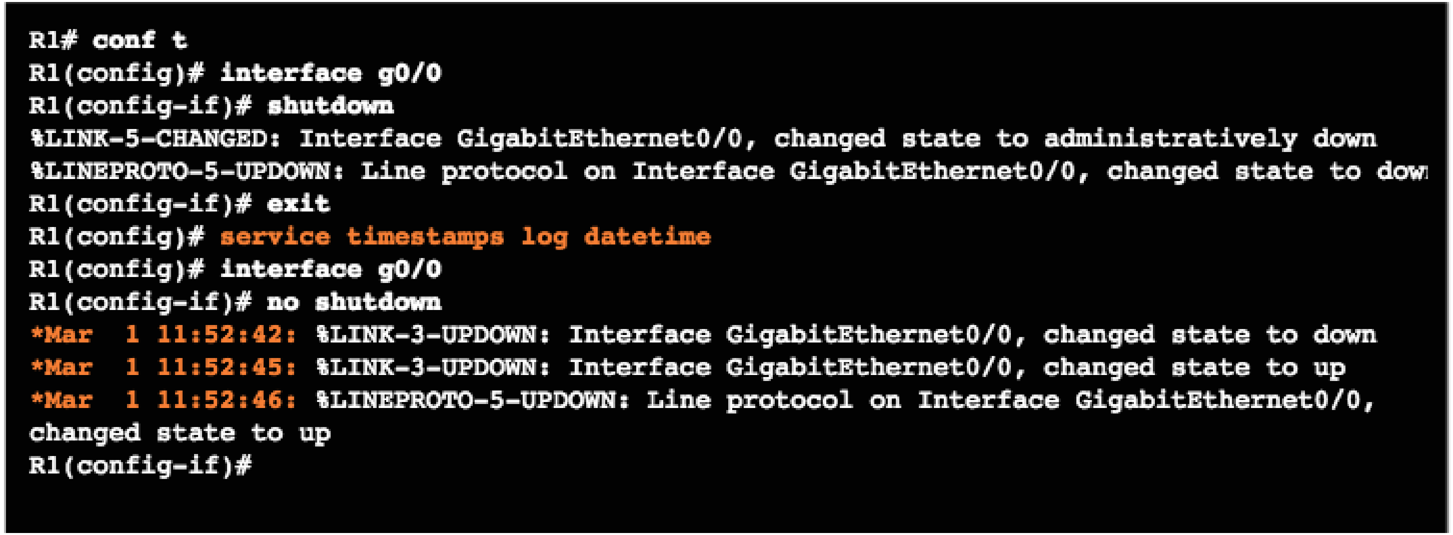


Field	Explanation
seq no	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured.
timestamp	Date and time of the message or event, which appears only if the **service timestamps** global configuration command is configured.
facility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

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

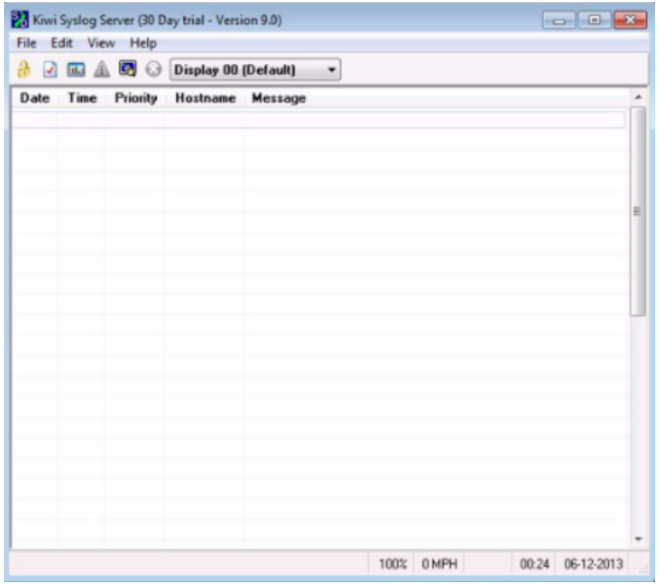


```
R1# conf t
R1(config)# interface g0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to dow
R1(config-if)# exit
R1(config)# service timestamps log datetime
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)#
```

Syslog Configuration

Syslog Server

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

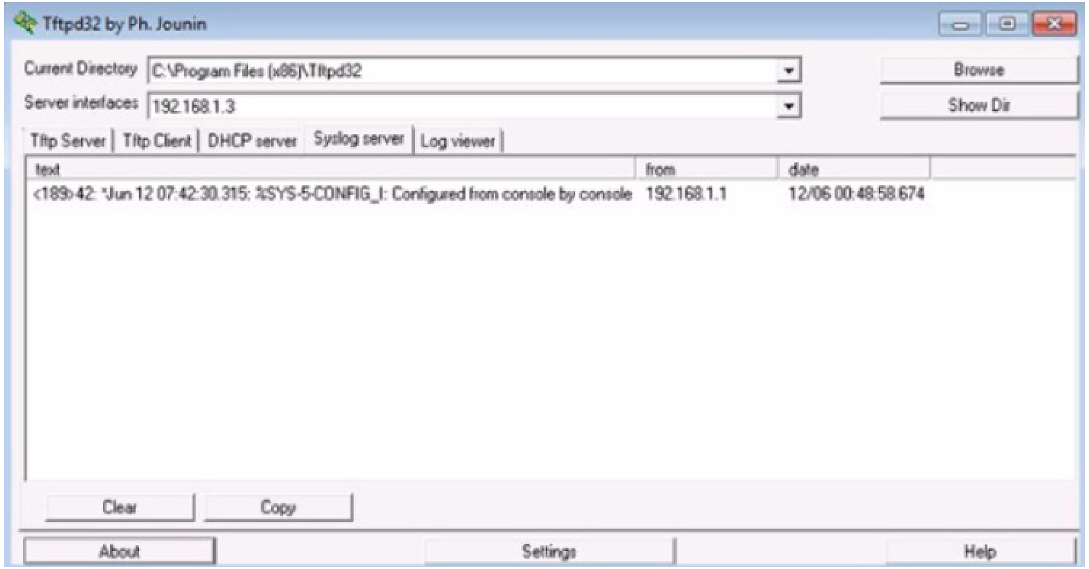


Kiwi Syslog Server (30 Day trial - Version 9.0)

Display 00 (Default)

Date	Time	Priority	Hostname	Message

100% 0 MPH 00:24 06-12-2013



Tftpd32 by Ph. Jounin

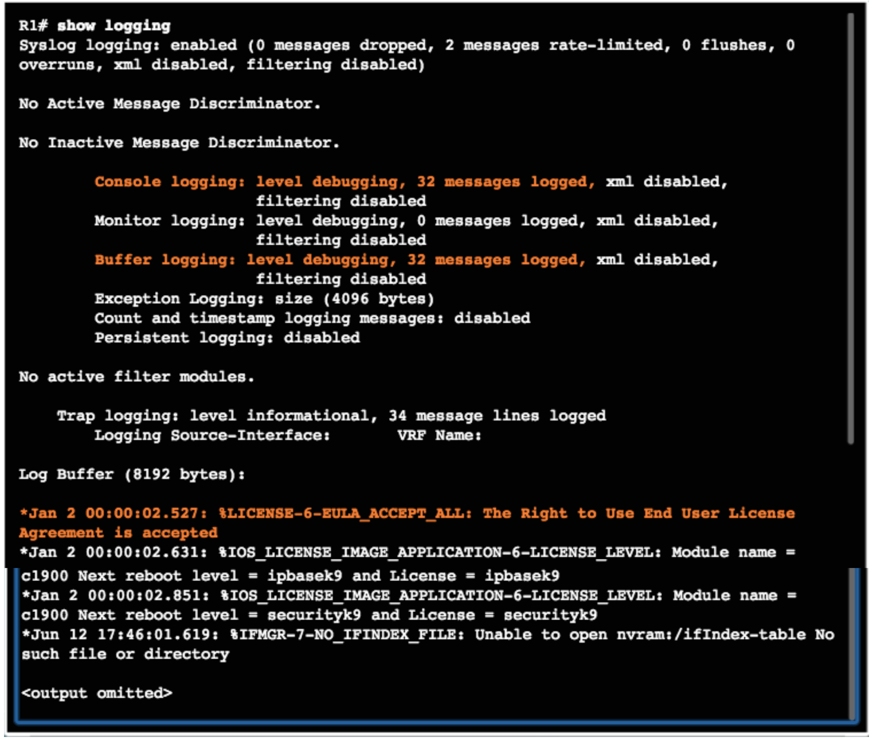
Current Directory: C:\Program Files (x86)\Tftpd32

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 Configuration

Default Logging

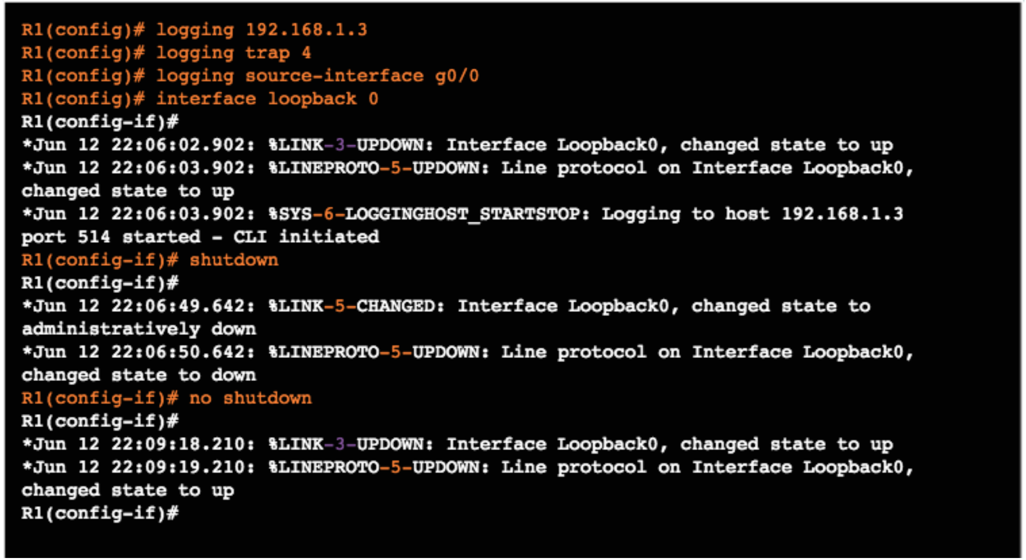


```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

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 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.

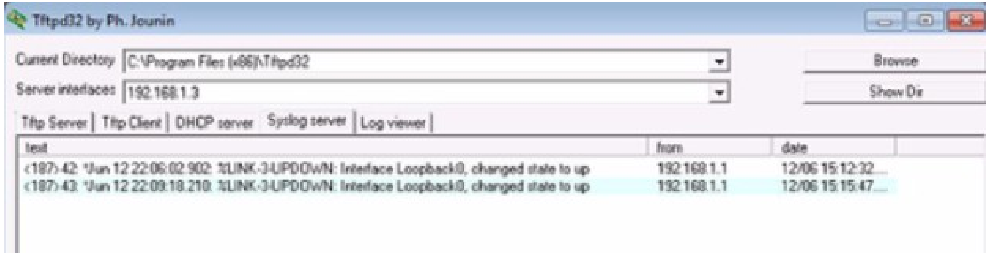
Syslog Configuration

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



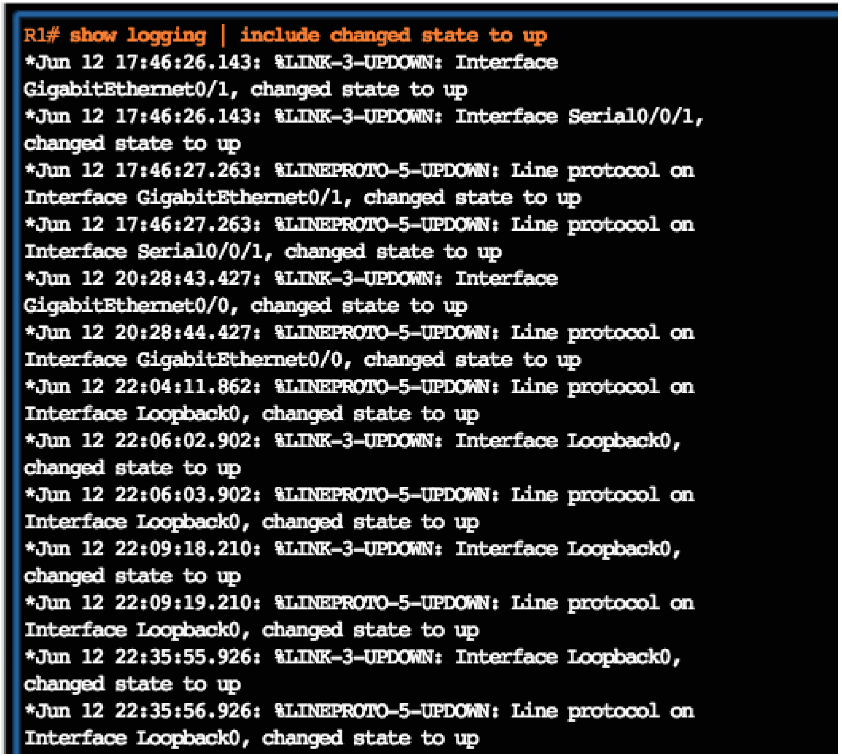
Current Directory: C:\Program Files (x86)\Tftpd32

Server interfaces: 192.168.1.3

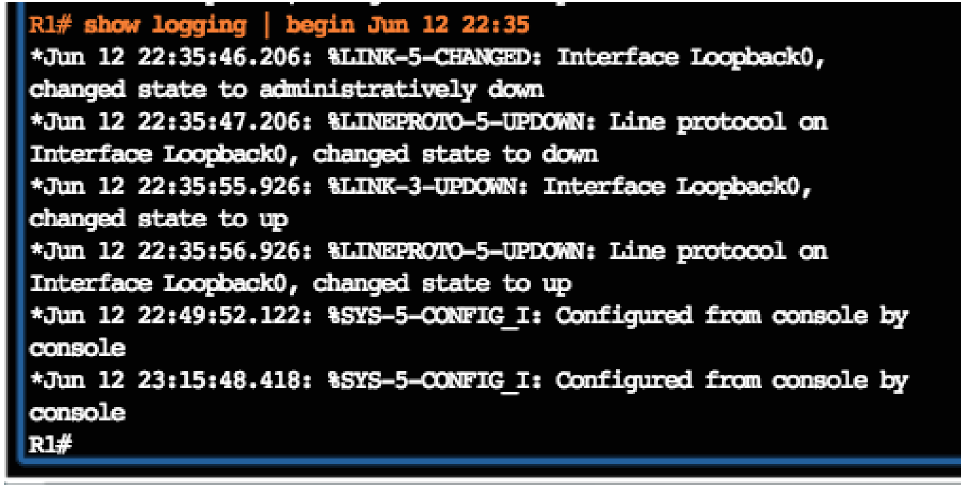
text	from	date
<187>42: *Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0, changed state to up	192.168.1.1	12/06 15:12:32...
<187>43: *Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0, changed state to up	192.168.1.1	12/06 15:15:47...

Syslog Configuration

Verifying Syslog



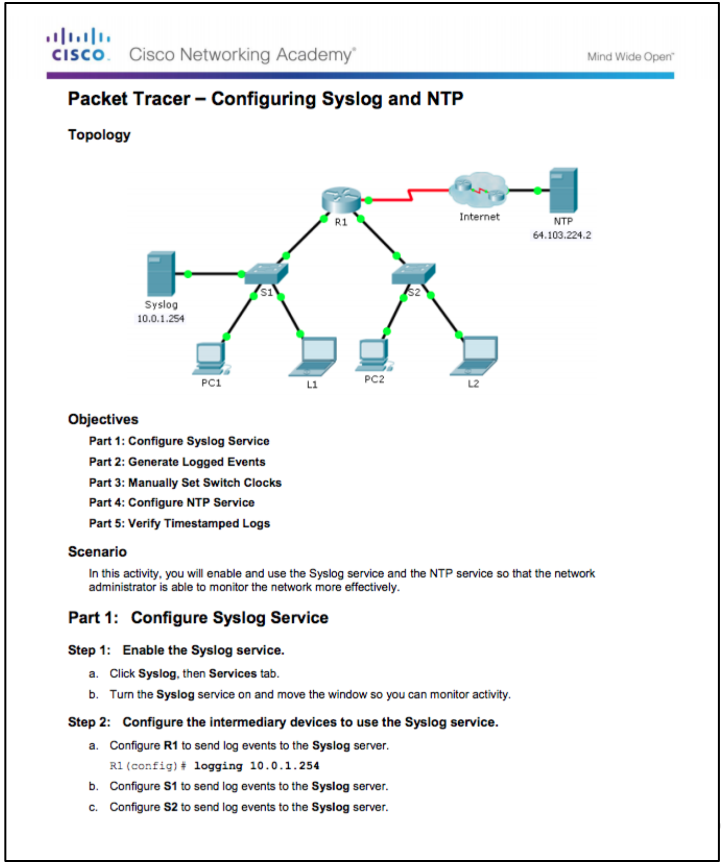
```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, 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#
```

Syslog Configuration

Packet Tracer – Configuring Syslog and NTP



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Configuring Syslog and NTP

Topology

Objectives

Part 1: Configure Syslog Service

Part 2: Generate Logged Events

Part 3: Manually Set Switch Clocks

Part 4: Configure NTP Service

Part 5: Verify Timestamped Logs

Scenario

In this activity, you will enable and use the Syslog service and the NTP service so that the network administrator is able to monitor the network more effectively.

Part 1: Configure Syslog Service

Step 1: Enable the Syslog service.

a. Click **Syslog**, then **Services** tab.

b. Turn the **Syslog** service on and move the window so you can monitor activity.

Step 2: Configure the intermediary devices to use the Syslog service.

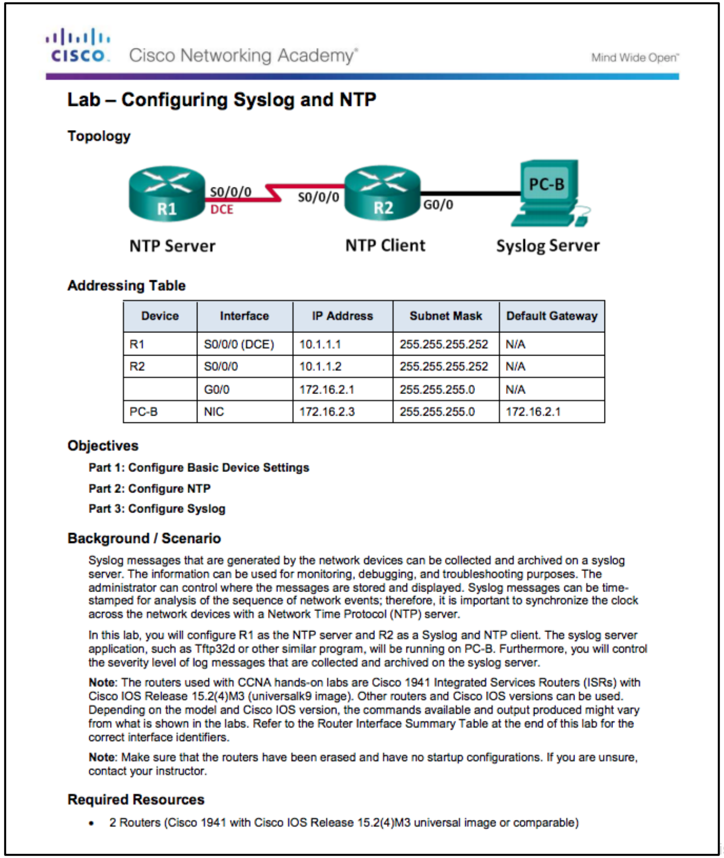
a. Configure **R1** to send log events to the **Syslog** server.

```
R1(config)# logging 10.0.1.254
```

b. Configure **S1** to send log events to the **Syslog** server.

c. Configure **S2** to send log events to the **Syslog** server.

Lab – Configuring Syslog and NTP



Cisco Networking Academy® Mind Wide Open™

Lab – Configuring Syslog and NTP

Topology

S0/0/0
DCE
R1
S0/0/0
R2
G0/0
PC-B
NTP Server
NTP Client
Syslog Server

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	G0/0	172.16.2.1	255.255.255.0	N/A
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure NTP

Part 3: Configure Syslog

Background / Scenario

Syslog messages that are generated by the network devices can be collected and archived on a syslog server. The information can be used for monitoring, debugging, and troubleshooting purposes. The administrator can control where the messages are stored and displayed. Syslog messages can be time-stamped for analysis of the sequence of network events; therefore, it is important to synchronize the clock across the network devices with a Network Time Protocol (NTP) server.

In this lab, you will configure R1 as the NTP server and R2 as a Syslog and NTP client. The syslog server application, such as Tftp32d or other similar program, will be running on PC-B. Furthermore, you will control the severity level of log messages that are collected and archived on the syslog server.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)

SIEM

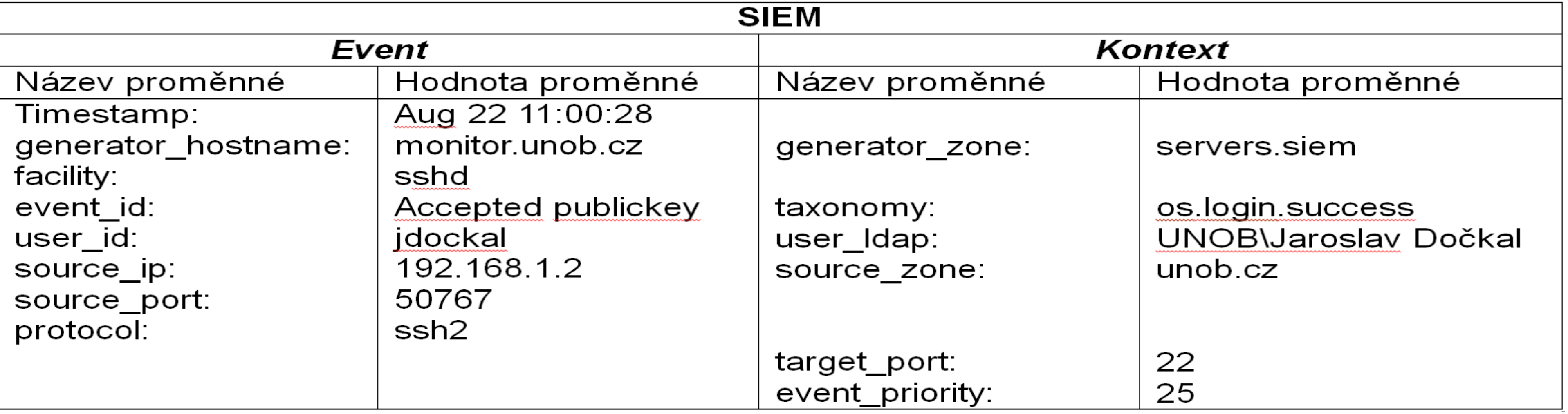
- *agregace dat* z různých zdrojů – síťových monitorů, přepínačů, firewallů, serverů, počítačových stanic, databází, detektorů průniku, aplikací atd.
- *korelace* – nalézání vzájemných vztahů událostí, např. monitorování činnosti konkrétního uživatele, pohled na určité události v nějakém časovém intervalu atp.
- *varování* (alerting)
- *informační panely, přehledové sestavy* (dashboards)
- *reportování shod* (compliance)
- *logování* (ukládání historických dat)

Parsing jako součást Event managementu

Event management	
Název proměnné	**Hodnota proměnné**
Timestamp:	Aug 22 11:00:28
generator_hostname:	monitor.unob.cz
facility:	sshd
event_id:	Accepted publickey
user_id:	jdockal
source_ip:	192.168.1.2
source_port:	50767
protocol:	ssh2

- Nalezení hodnoty a její přiřazení k příslušné proměnné je označováno jako **parsing**, který je součástí procesu Event management.
- Jednotlivé Event management nástroje mají postup parsingu víceméně shodný,

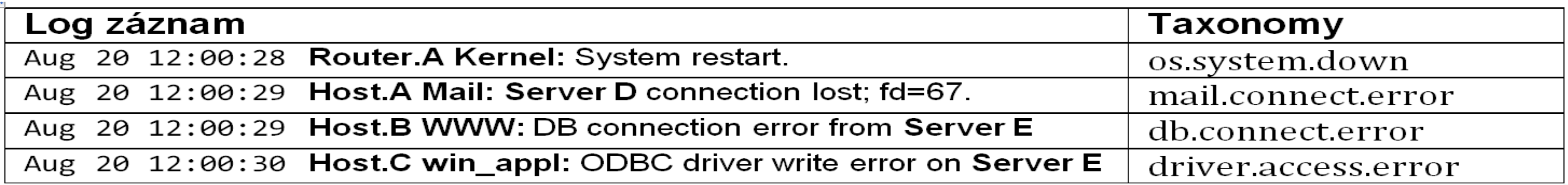
Doplňující kontextové údaje
(pro zpřesnění děje, identifikace komponenty, uživatele, atp.)



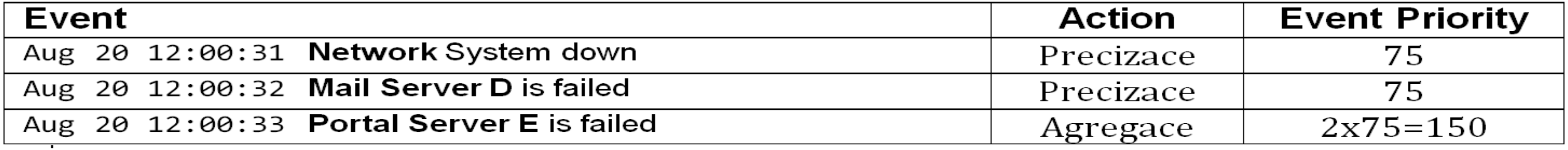
SIEM			
Event		*Kontext*	
Název proměnné	Hodnota proměnné	Název proměnné	Hodnota proměnné
Timestamp:	Aug 22 11:00:28		
generator_hostname:	monitor.unob.cz	generator_zone:	servers.siem
facility:	sshd		
event_id:	Accepted publickey	taxonomy:	os.login.success
user_id:	jdockal	user_ldap:	UNOB\Jaroslav Dočkal
source_ip:	192.168.1.2	source_zone:	unob.cz
source_port:	50767		
protocol:	ssh2		
		target_port:	22
		event_priority:	25

Účelem kontextových dat je popsat analytikovi detailněji zdroj, cíl a děj analyzované události ve smyslu – typ zařízení, lokalita, procesní příslušnost, kategorie děje, atp.

Ze zápisu logů do zápisu událostí



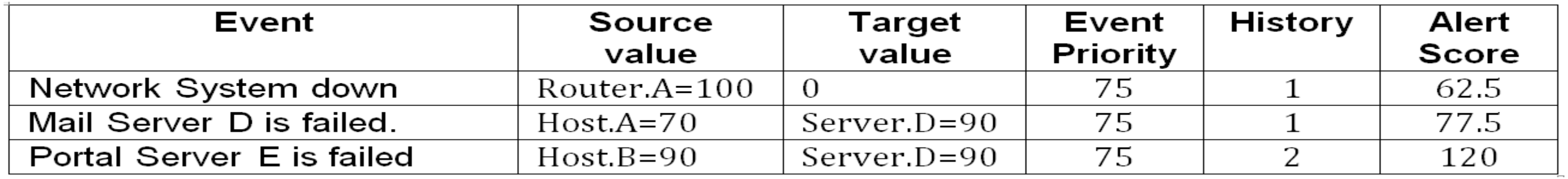
Log záznam	Taxonomy
Aug 20 12:00:28 **Router.A Kernel:** System restart.	os.system.down
Aug 20 12:00:29 **Host.A Mail: Server D** connection lost; fd=67.	mail.connect.error
Aug 20 12:00:29 **Host.B WWW:** DB connection error from **Server E**	db.connect.error
Aug 20 12:00:30 **Host.C win_appl:** ODBC driver write error on **Server E**	driver.access.error



Event	Action	Event Priority
Aug 20 12:00:31 **Network** System down	Precizace	75
Aug 20 12:00:32 **Mail Server D** is failed	Precizace	75
Aug 20 12:00:33 **Portal Server E** is failed	Agregace	2x75=150

- **Precizace** probíhají pomocí substitucí: Router.A=Network, Host.A=Mail, Host.B/Host.C=Portal. a přidáním bezpečnostní hodnoty události (Event Priority).
- **Agregace** může být v SIEM volitelně provedena nejen nad událostmi, ale i nad „vytěženou informací“, jako např. na *source_hostname*, *source_ip*, *target_hostname*, *target_ip*, atp.

Alert

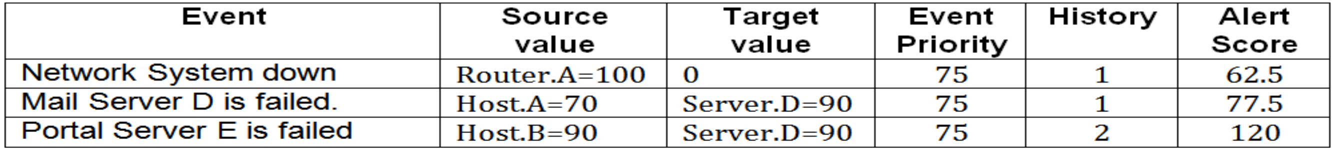


Event	Source value	Target value	Event Priority	History	Alert Score
Network System down	Router.A=100	0	75	1	62.5
Mail Server D is failed.	Host.A=70	Server.D=90	75	1	77.5
Portal Server E is failed	Host.B=90	Server.D=90	75	2	120

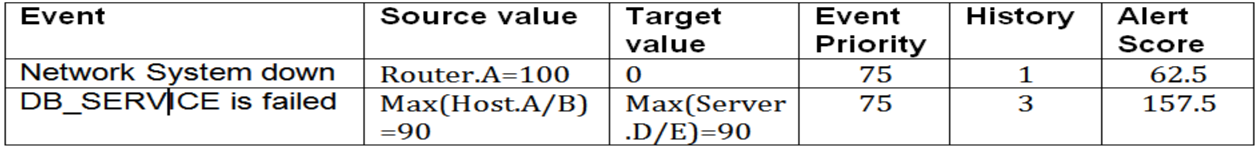
Např.

$$Score_{Alert} := 0{,}25 \times Source_{value} + 0{,}25 \times Target_{value} + 0{,}5 \times History \times Event_{priority}$$

Precizace eventů díky kontextové vazbě

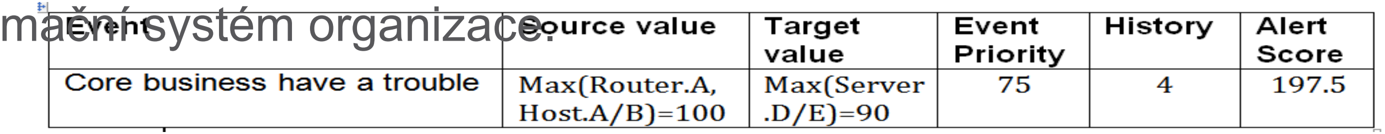


Event	Source value	Target value	Event Priority	History	Alert Score
Network System down	Router.A=100	0	75	1	62.5
Mail Server D is failed.	Host.A=70	Server.D=90	75	1	77.5
Portal Server E is failed	Host.B=90	Server.D=90	75	2	120



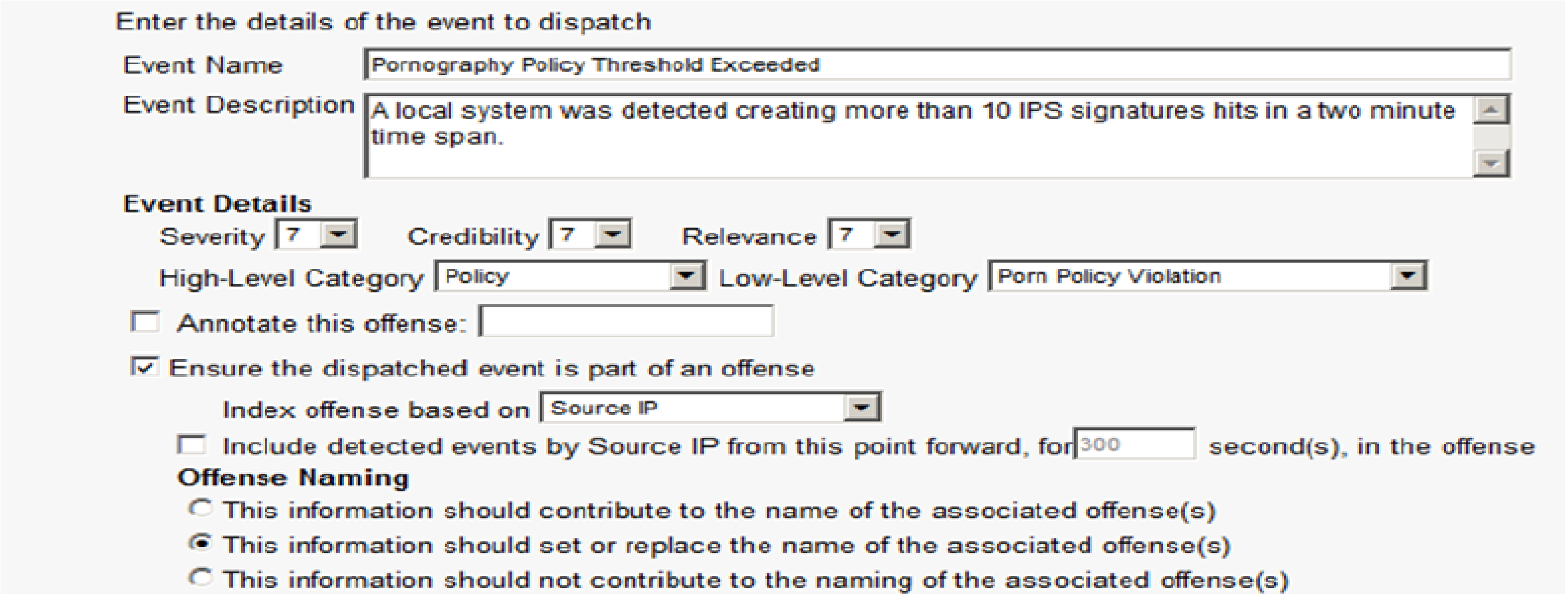
Event	Source value	Target value	Event Priority	History	Alert Score
Network System down	Router.A=100	0	75	1	62.5
DB_SERVICE is failed	Max(Host.A/B) =90	Max(Server .D/E)=90	75	3	157.5

…a pomocí konfigurační databáze , což je evidence veškerých ICT komponent, včetně vzájemných vazeb a SLA, které tvoří provozovaný informační systém organizace.



Event	Source value	Target value	Event Priority	History	Alert Score
Core business have a trouble	Max(Router.A, Host.A/B)=100	Max(Server .D/E)=90	75	4	197.5

Způsob sestavování pravidel na našem systému



Enter the details of the event to dispatch

Event Name: Pornography Policy Threshold Exceeded

Event Description: A local system was detected creating more than 10 IPS signatures hits in a two minute time span.

Event Details

Severity: 7 Credibility: 7 Relevance: 7

High-Level Category: Policy Low-Level Category: Porn Policy Violation

☐ Annotate this offense:

☑ Ensure the dispatched event is part of an offense

Index offense based on: Source IP

☐ Include detected events by Source IP from this point forward, for 300 second(s), in the offense

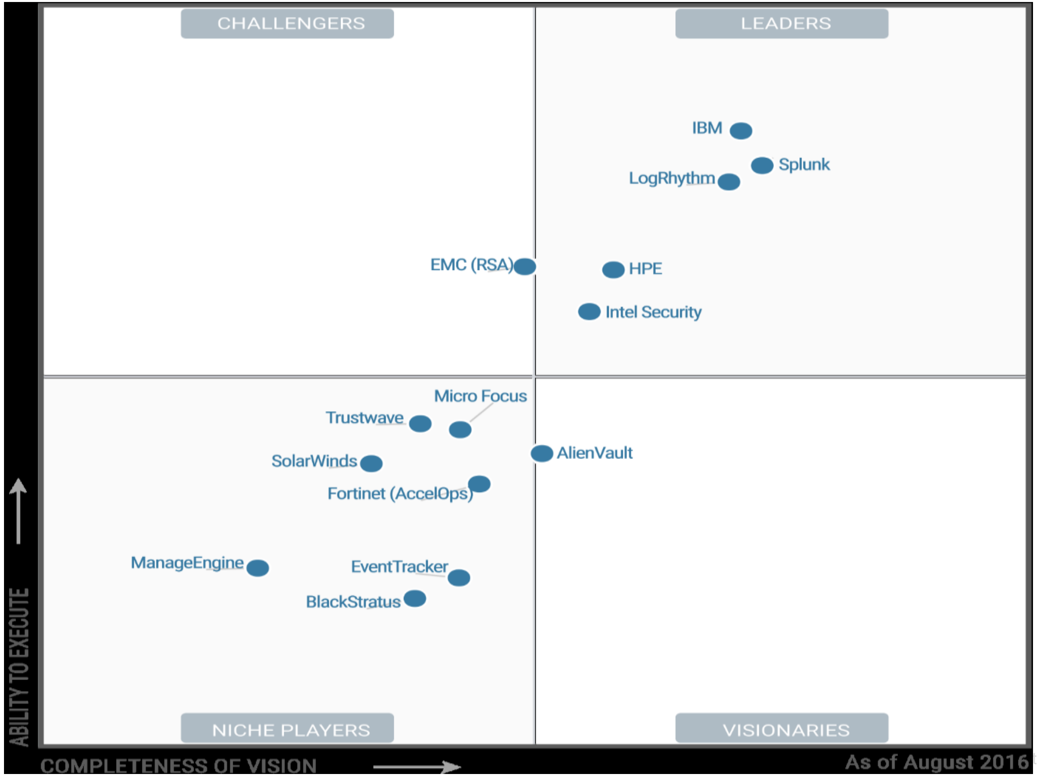
Offense Naming

○ This information should contribute to the name of the associated offense(s)

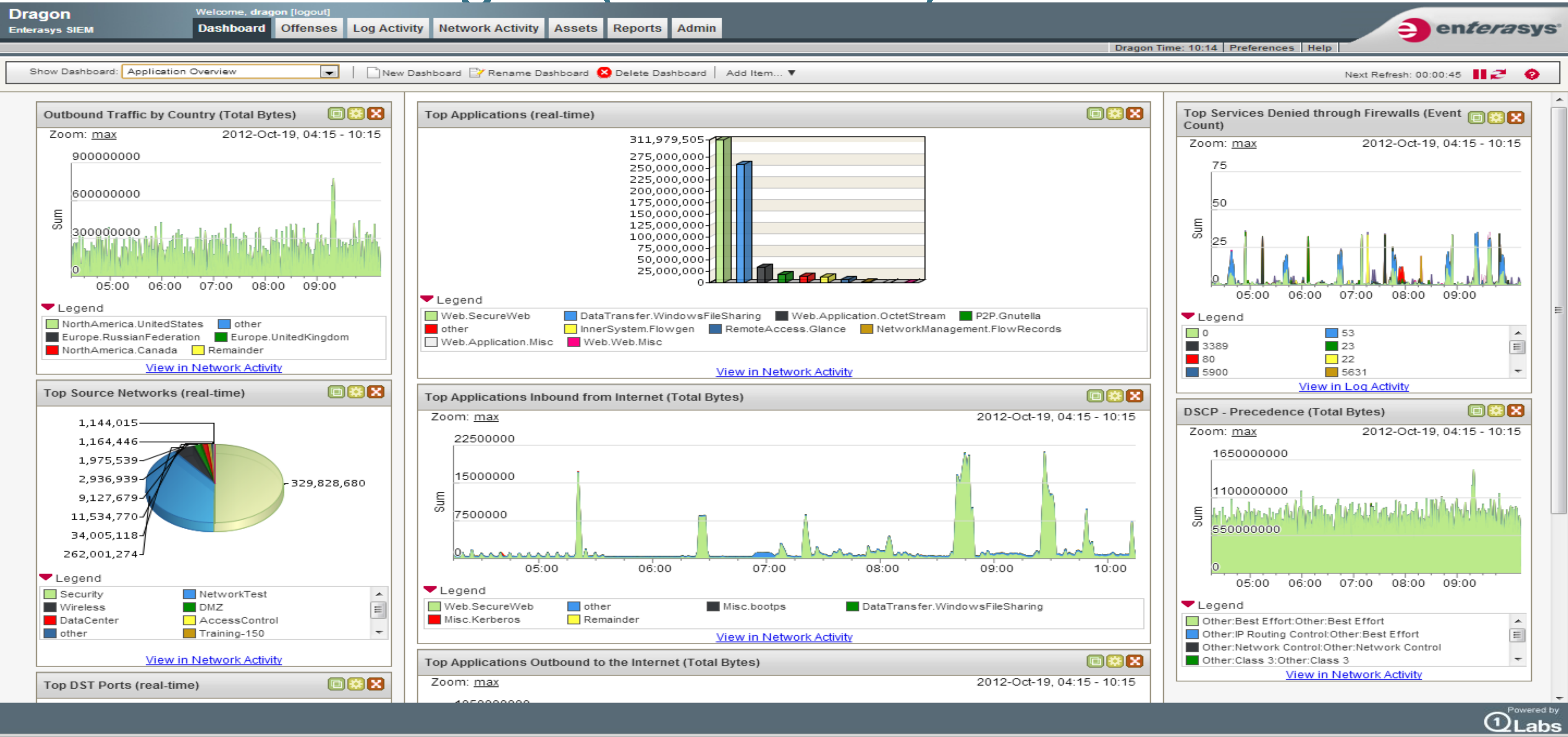
● This information should set or replace the name of the associated offense(s)

○ This information should not contribute to the naming of the associated offense(s)

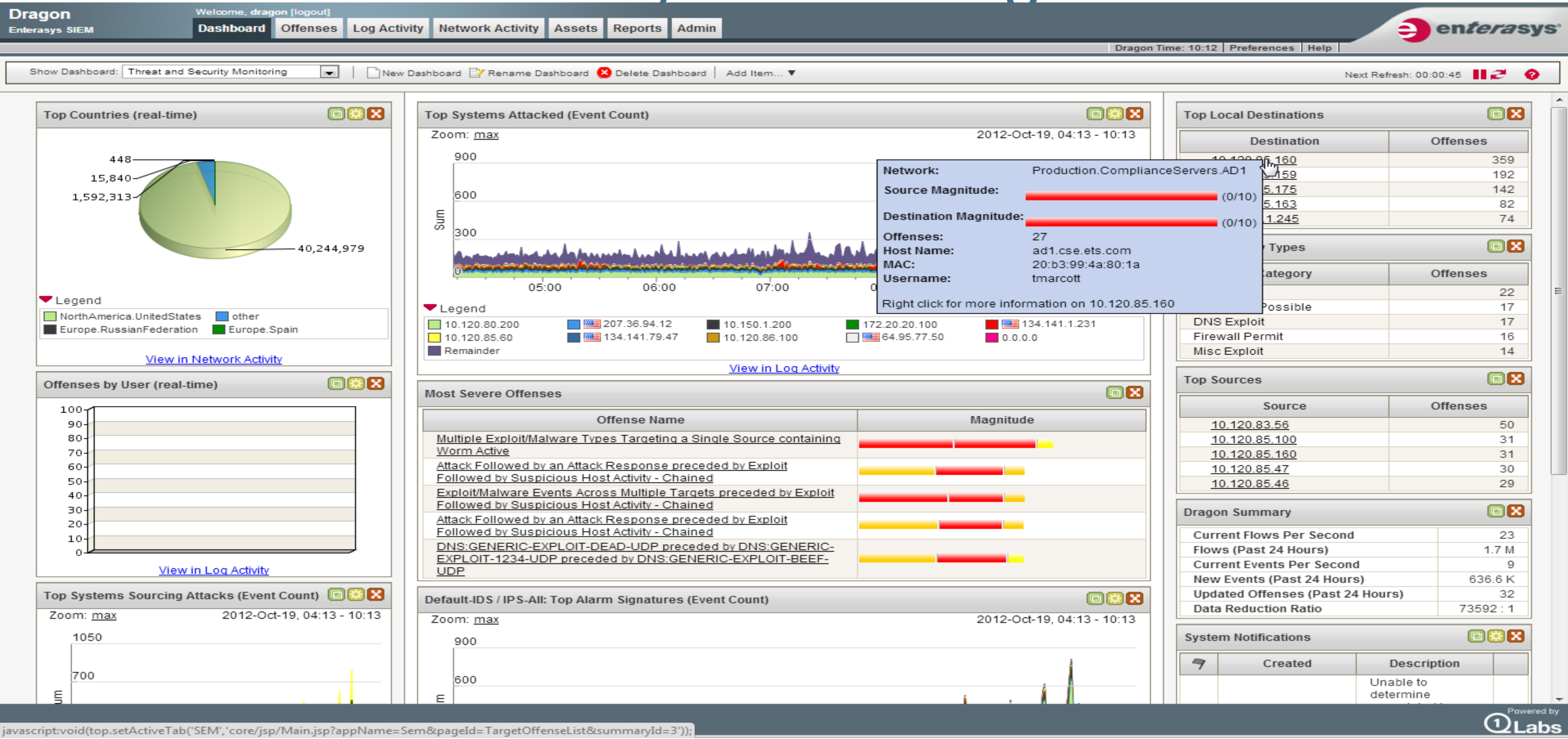
Který SIEM byl nejlepší – 2016



Příklad: Dragon (OEM IBM) - dashboard



Náhled na detail systému Dragon



Top Countries (real-time)

Legend

- 🟩 NorthAmerica.UnitedStates
- 🟦 other
- ■ Europe.RussianFederation
- 🟩 Europe.Spain

View in Network Activity

Offenses by User (real-time)

View in Log Activity

Top Systems Sourcing Attacks (Event Count)

Zoom: max 2012-Oct-19, 04:13 - 10:13

Top Systems Attacked (Event Count)

Zoom: max 2012-Oct-19, 04:13 - 10:13

Network:	Production.ComplianceServers.AD1
Source Magnitude:	(0/10)
Destination Magnitude:	(0/10)
Offenses:	27
Host Name:	ad1.cse.ets.com
MAC:	20:b3:99:4a:80:1a
Username:	tmarcott

Right click for more information on 10.120.85.160

Legend

- 10.120.80.200
- 207.36.94.12
- 10.150.1.200
- 172.20.20.100
- 134.141.1.231
- 10.120.85.60
- 134.141.79.47
- 10.120.86.100
- 64.95.77.50
- 0.0.0.0
- Remainder

View in Log Activity

Most Severe Offenses

Offense Name	Magnitude
Multiple Exploit/Malware Types Targeting a Single Source containing Worm Active	
Attack Followed by an Attack Response preceded by Exploit Followed by Suspicious Host Activity - Chained	
Exploit/Malware Events Across Multiple Targets preceded by Exploit Followed by Suspicious Host Activity - Chained	
Attack Followed by an Attack Response preceded by Exploit Followed by Suspicious Host Activity - Chained	
DNS:GENERIC-EXPLOIT-DEAD-UDP preceded by DNS:GENERIC-EXPLOIT-1234-UDP preceded by DNS:GENERIC-EXPLOIT-BEEF-UDP	

Default-IDS / IPS-All: Top Alarm Signatures (Event Count)

Zoom: max 2012-Oct-19, 04:13 - 10:13

Top Local Destinations

Destination	Offenses
10.120.9_.160	359
.159	192
5.175	142
5.163	82
1.245	74

Types

ategory	Offenses
	22
Possible	17
DNS Exploit	17
Firewall Permit	16
Misc Exploit	14

Top Sources

Source	Offenses
10.120.83.56	50
10.120.85.100	31
10.120.85.160	31
10.120.85.47	30
10.120.85.46	29

Dragon Summary

Current Flows Per Second	23
Flows (Past 24 Hours)	1.7 M
Current Events Per Second	9
New Events (Past 24 Hours)	636.6 K
Updated Offenses (Past 24 Hours)	32
Data Reduction Ratio	73592 : 1

System Notifications

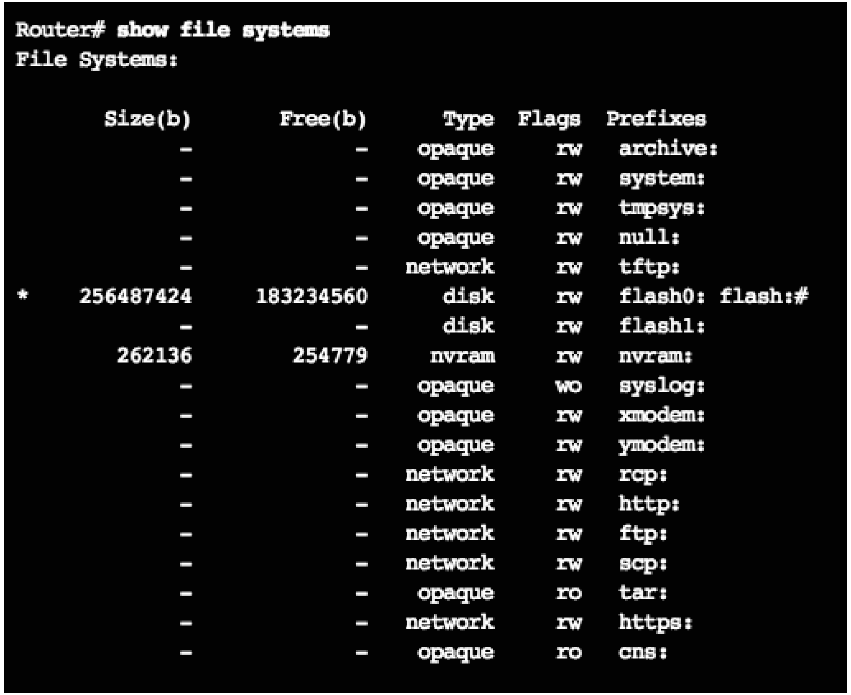
	Created	Description
		Unable to determine

javascript:void(top.setActiveTab('SEM','core/jsp/Main.jsp?appName=Sem&pageId=TargetOffenseList&summaryId=3'));

10.3 Device Maintenance

Router and Switch File Maintenance

Router File Systems

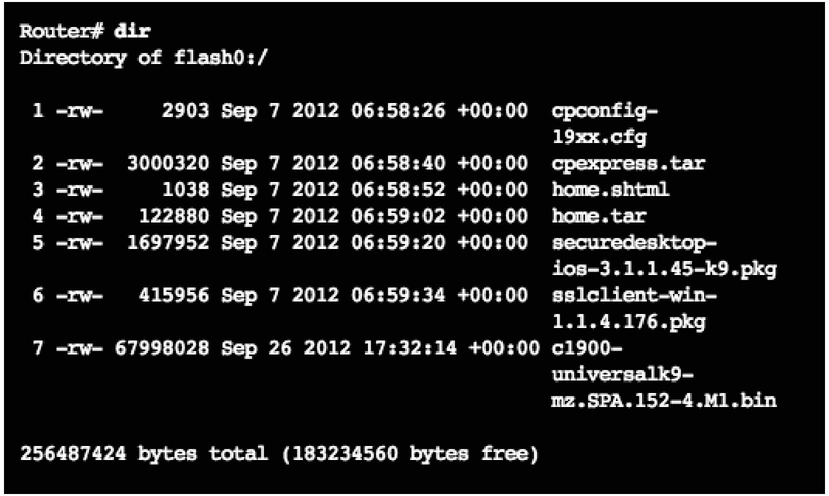


```
Router# show file systems
File Systems:

       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 *

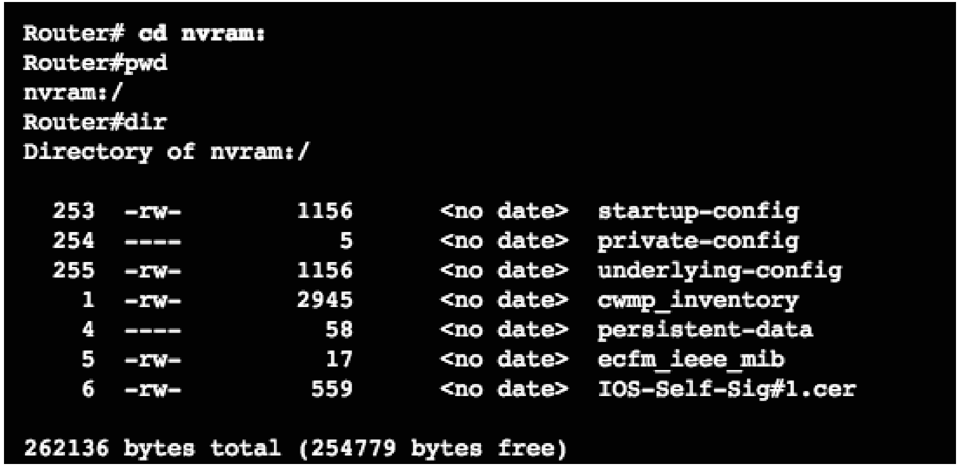
Router and Switch File Maintenance

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)
```

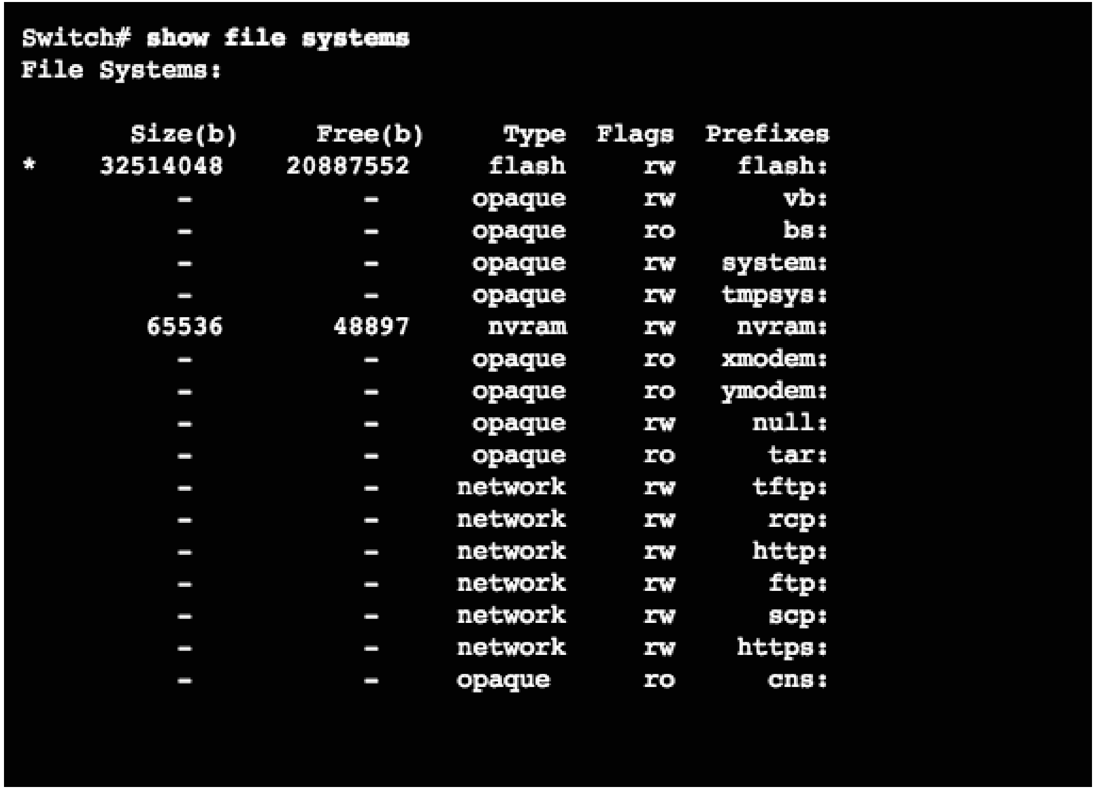
- **dir** lists the contents of flash
- Last listing is the name of the current Cisco IOS file that is running in RAM



```
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

Switch File Systems

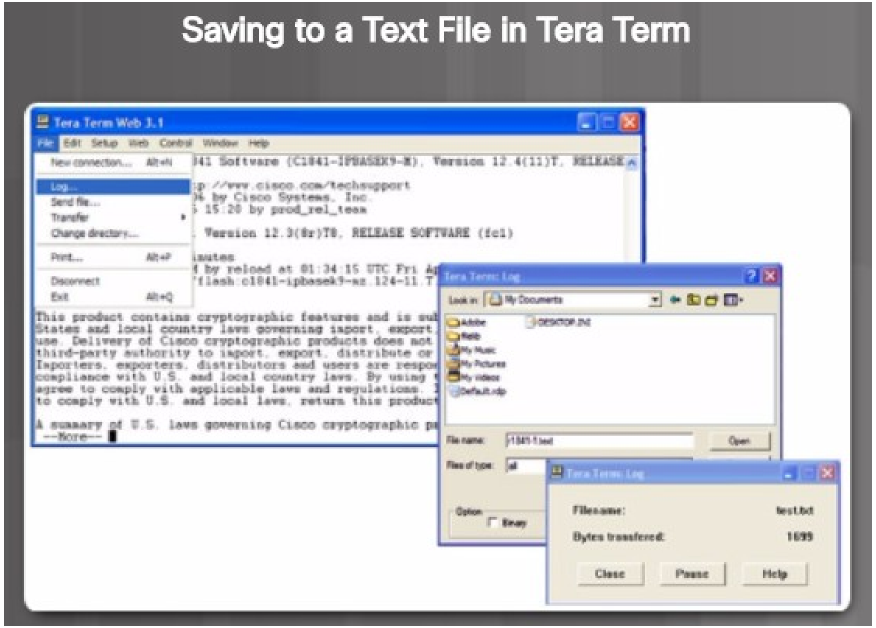


```
Switch# show file systems
File Systems:

       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!

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
:p://www.cisco.com/techsupport
)6 by Cisco Systems, Inc.
5 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 respon
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: 1841-1.txt

Files of type: all

Filename: test.txt

Bytes transfered: 1699

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.

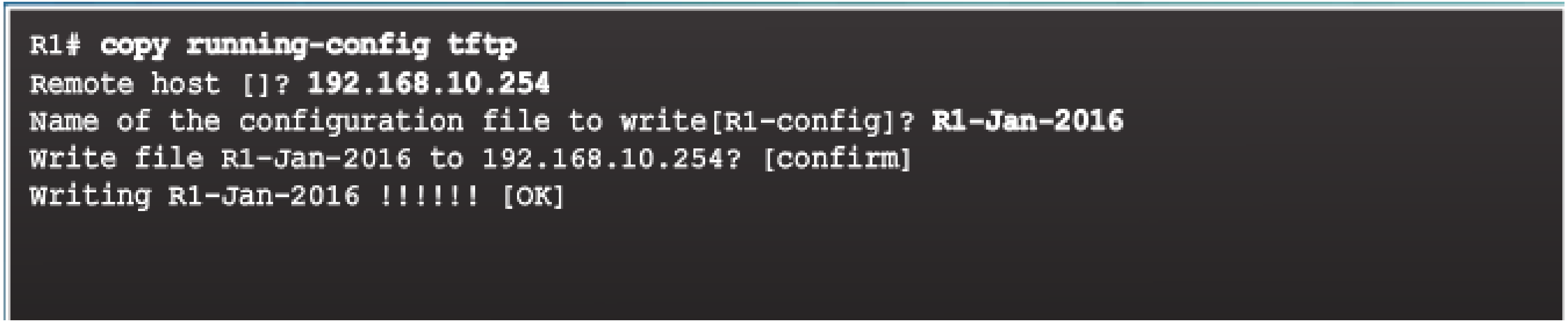
When using Tera Term, the steps are:

- 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.

Router and Switch File Maintenance

Backing up and Restoring using TFTP

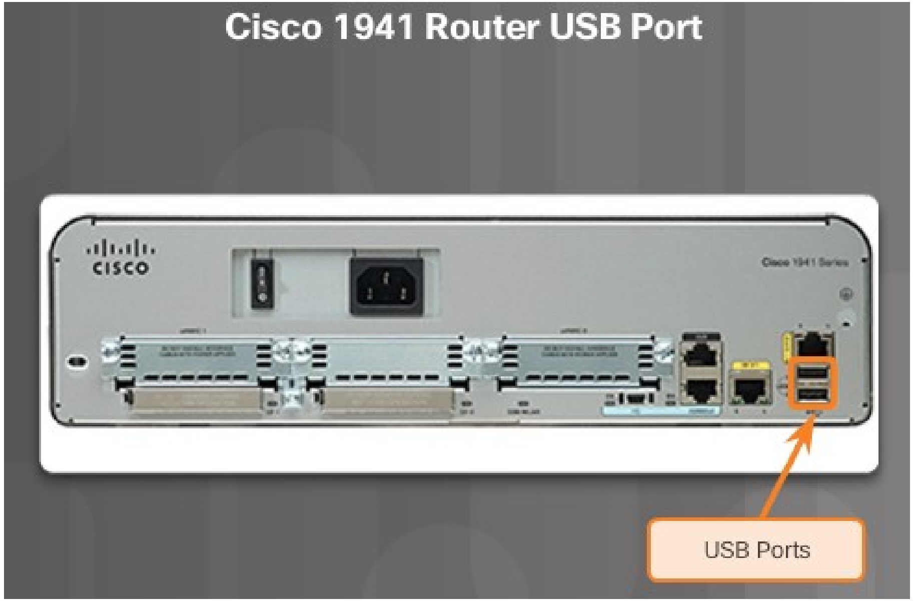
- Configuration files should be backed up and included in network documentation
- Commands - **copy running-config tftp** (see figure) or **copy startup-config tftp**
- To restore the running configuration or the startup configuration from a TFTP server, use **copy tftp running-config** or **copy tftp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

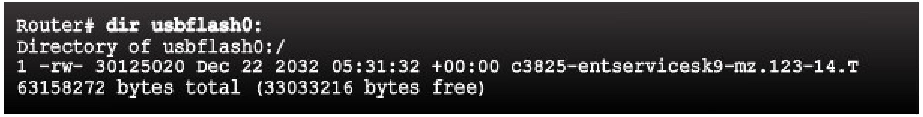


```
R1# copy running-config tftp
Remote host []? 192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2016
Write file R1-Jan-2016 to 192.168.10.254? [confirm]
Writing R1-Jan-2016 !!!!!! [OK]
```

Router and Switch File Maintenance

Using USB Ports on a Cisco Router



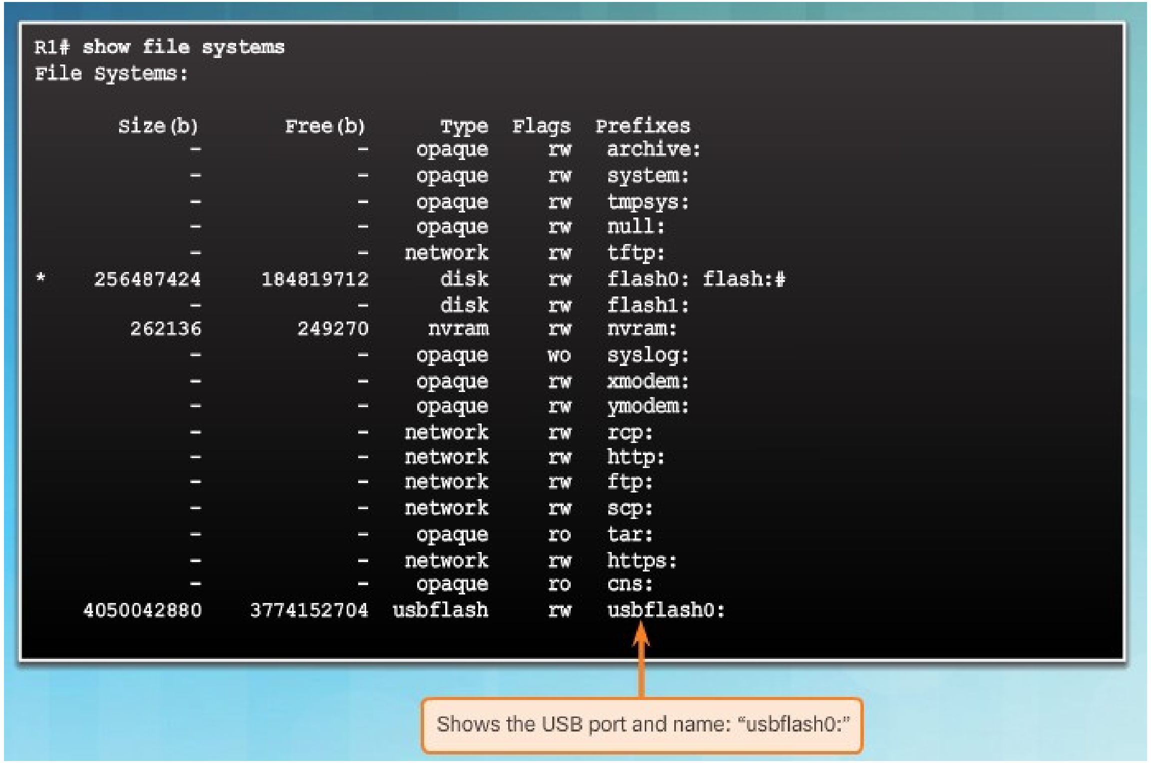


```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

- 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.

Router and Switch File Maintenance

Backing up and Restoring Using USB



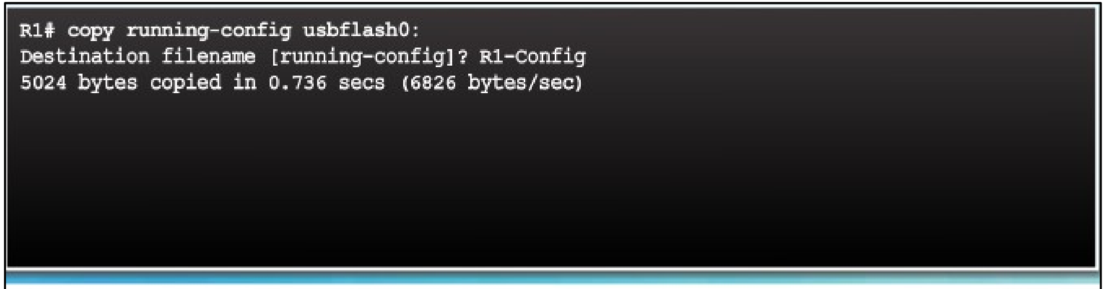
```
R1# show file systems
File Systems:

       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

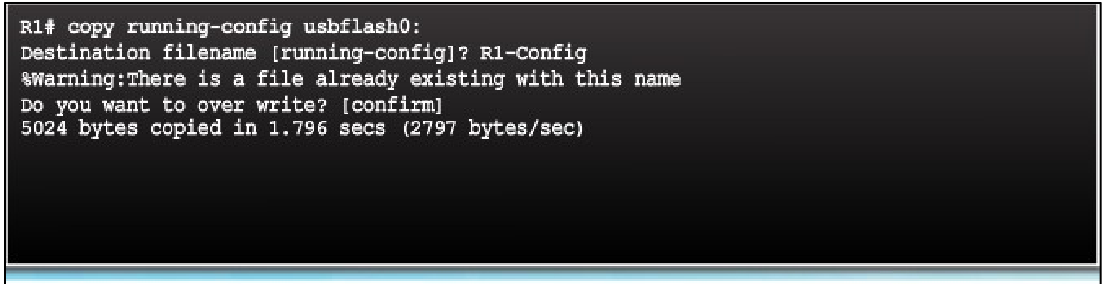
Router and Switch File Maintenance

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.



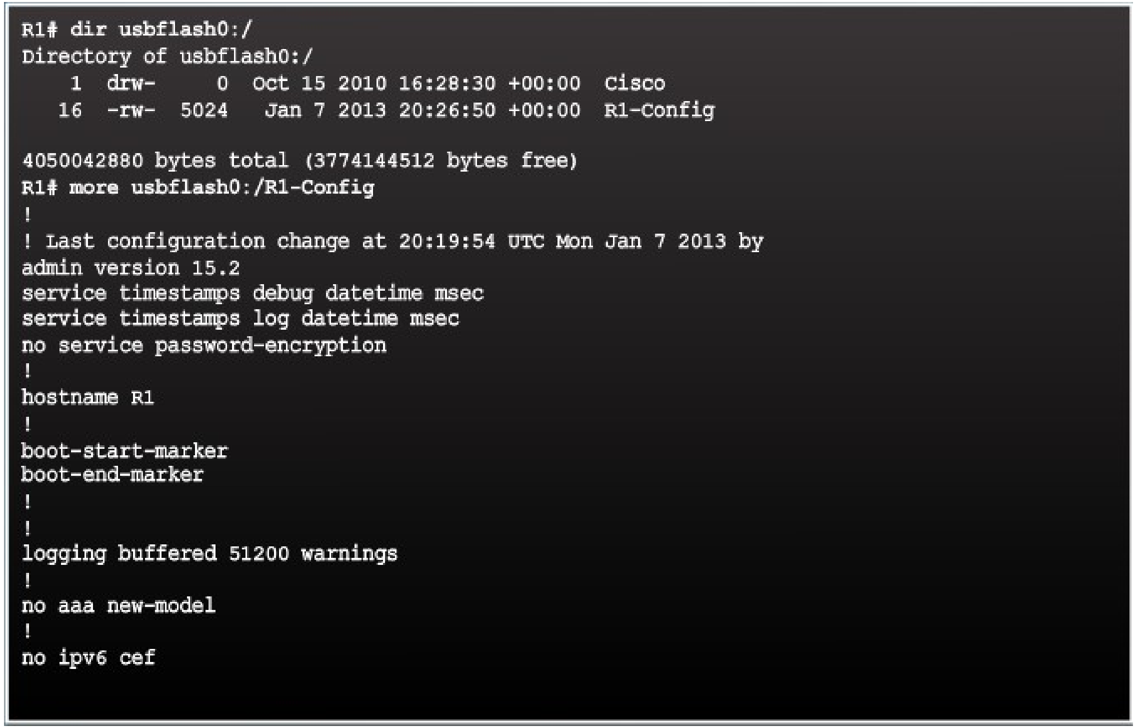
```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

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

Router and Switch File Maintenance

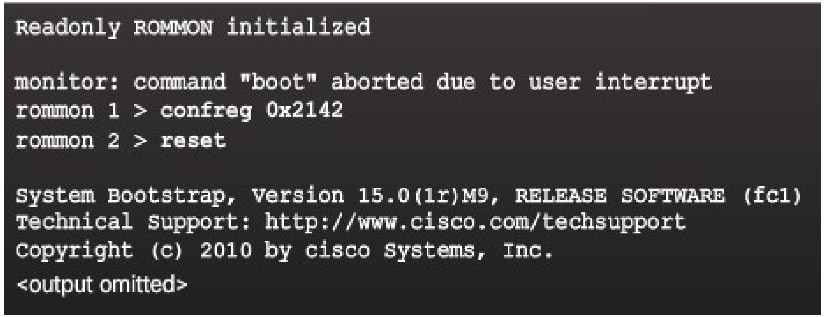
Backing up and Restoring Using USB (Cont.)



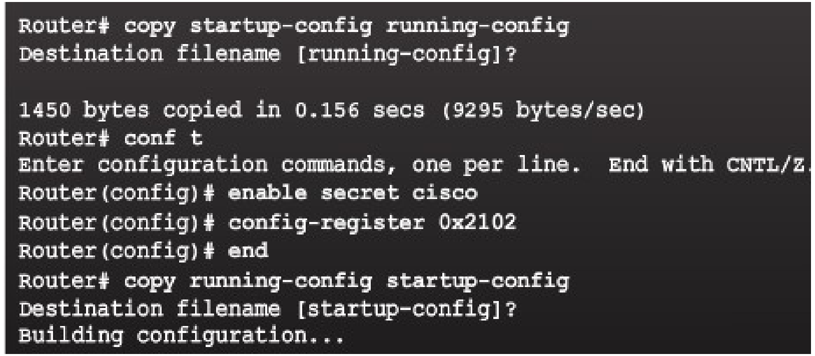
```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config

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

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

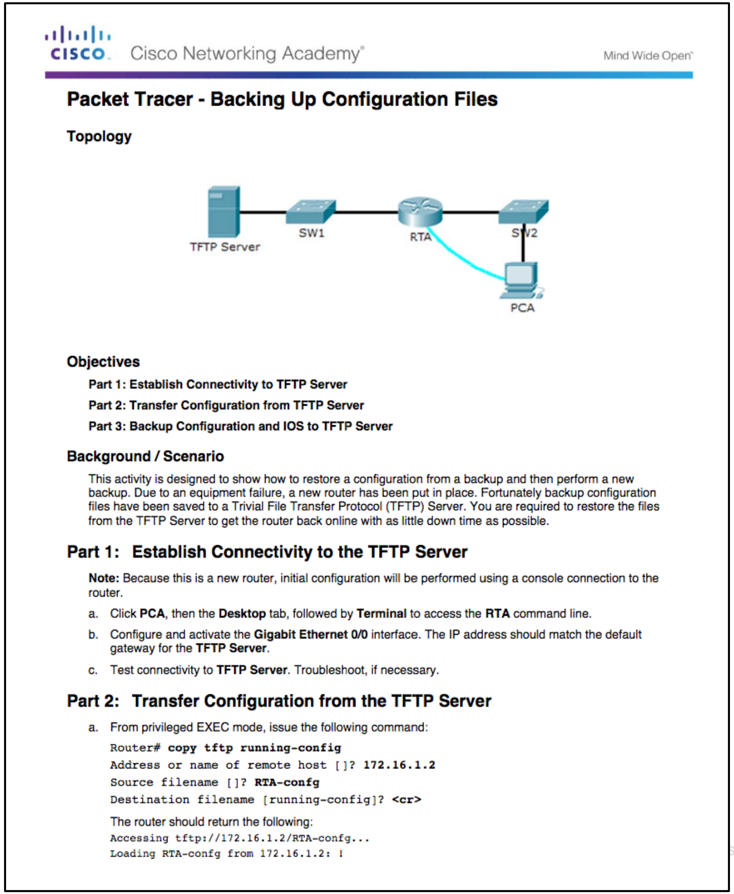
Step 3. Make necessary changes to the original startup config file.

- 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.

Router and Switch File Maintenance

Packet Tracer – Backing Up Configuration Files



Cisco Networking Academy®   Mind Wide Open™

Packet Tracer - Backing Up Configuration Files

Topology

Objectives

Part 1: Establish Connectivity to TFTP Server

Part 2: Transfer Configuration from TFTP Server

Part 3: Backup Configuration and IOS to TFTP Server

Background / Scenario

This activity is designed to show how to restore a configuration from a backup and then perform a new backup. Due to an equipment failure, a new router has been put in place. Fortunately backup configuration files have been saved to a Trivial File Transfer Protocol (TFTP) Server. You are required to restore the files from the TFTP Server to get the router back online with as little down time as possible.

Part 1: Establish Connectivity to the TFTP Server

Note: Because this is a new router, initial configuration will be performed using a console connection to the router.

a. Click **PCA**, then the **Desktop** tab, followed by **Terminal** to access the **RTA** command line.

b. Configure and activate the **Gigabit Ethernet 0/0** interface. The IP address should match the default gateway for the **TFTP Server**.

c. Test connectivity to **TFTP Server**. Troubleshoot, if necessary.

Part 2: Transfer Configuration from the TFTP Server

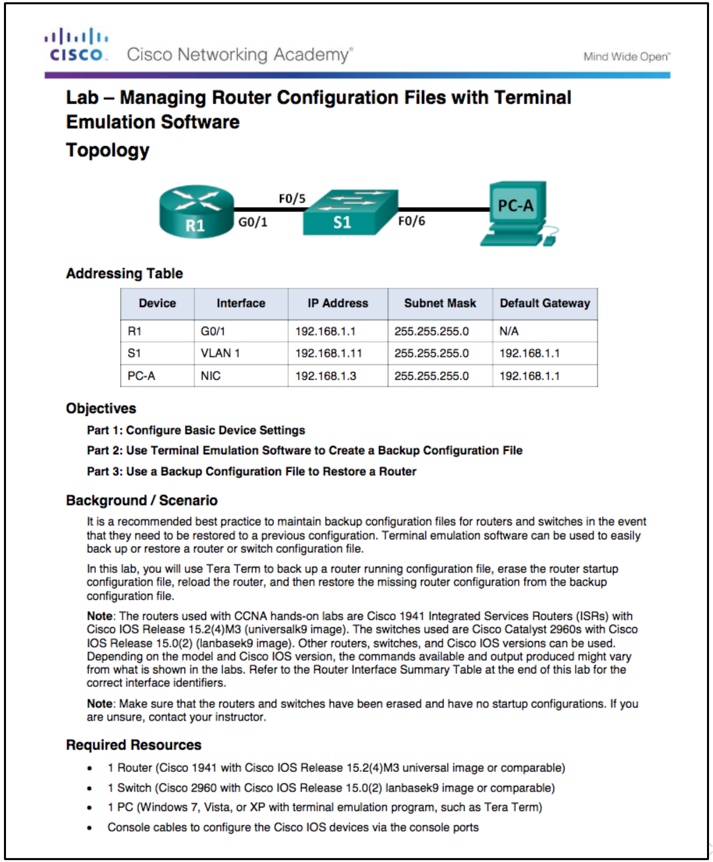
a. From privileged EXEC mode, issue the following command:

```
Router# copy tftp running-config
Address or name of remote host []? 172.16.1.2
Source filename []? RTA-confg
Destination filename [running-config]? <cr>
```

The router should return the following:

```
Accessing tftp://172.16.1.2/RTA-confg...
Loading RTA-confg from 172.16.1.2: !
```

Lab – Managing Router Configuration Files with Tera Term



Cisco Networking Academy® Mind Wide Open™

Lab – Managing Router Configuration Files with Terminal Emulation Software

Topology

R1
G0/1
F0/5
S1
F0/6
PC-A

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

Part 3: Use a Backup Configuration File to Restore a Router

Background / Scenario

It is a recommended best practice to maintain backup configuration files for routers and switches in the event that they need to be restored to a previous configuration. Terminal emulation software can be used to easily back up or restore a router or switch configuration file.

In this lab, you will use Tera Term to back up a router running configuration file, erase the router startup configuration file, reload the router, and then restore the missing router configuration from the backup configuration file.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

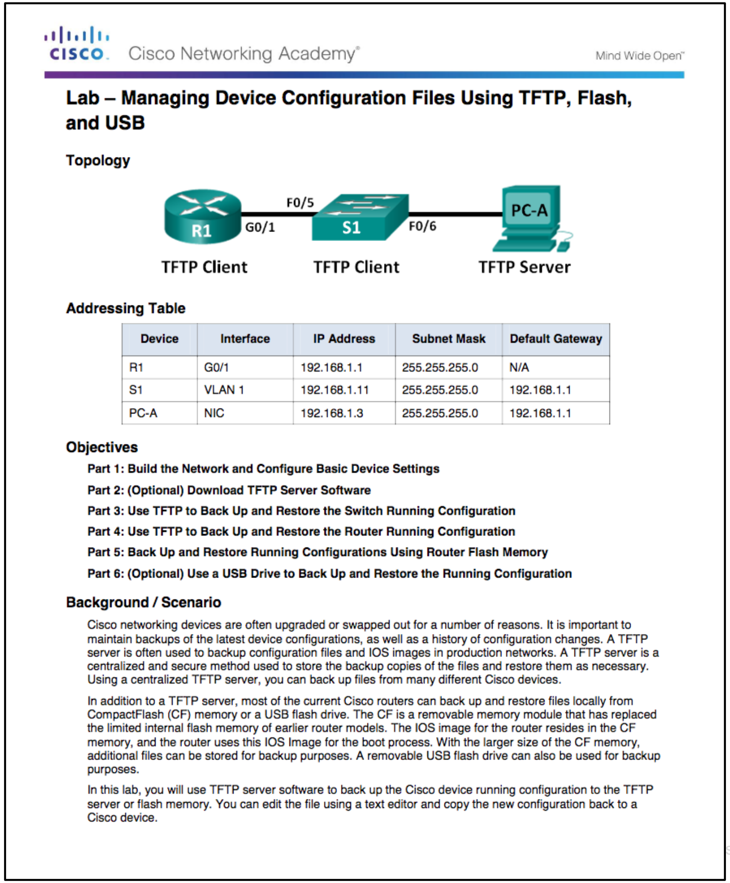
Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

Router and Switch File Maintenance

Lab – Managing Device Configuration Files Using TFTP, Flash, and USB



Cisco Networking Academy® Mind Wide Open™

Lab – Managing Device Configuration Files Using TFTP, Flash, and USB

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: (Optional) Download TFTP Server Software

Part 3: Use TFTP to Back Up and Restore the Switch Running Configuration

Part 4: Use TFTP to Back Up and Restore the Router Running Configuration

Part 5: Back Up and Restore Running Configurations Using Router Flash Memory

Part 6: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

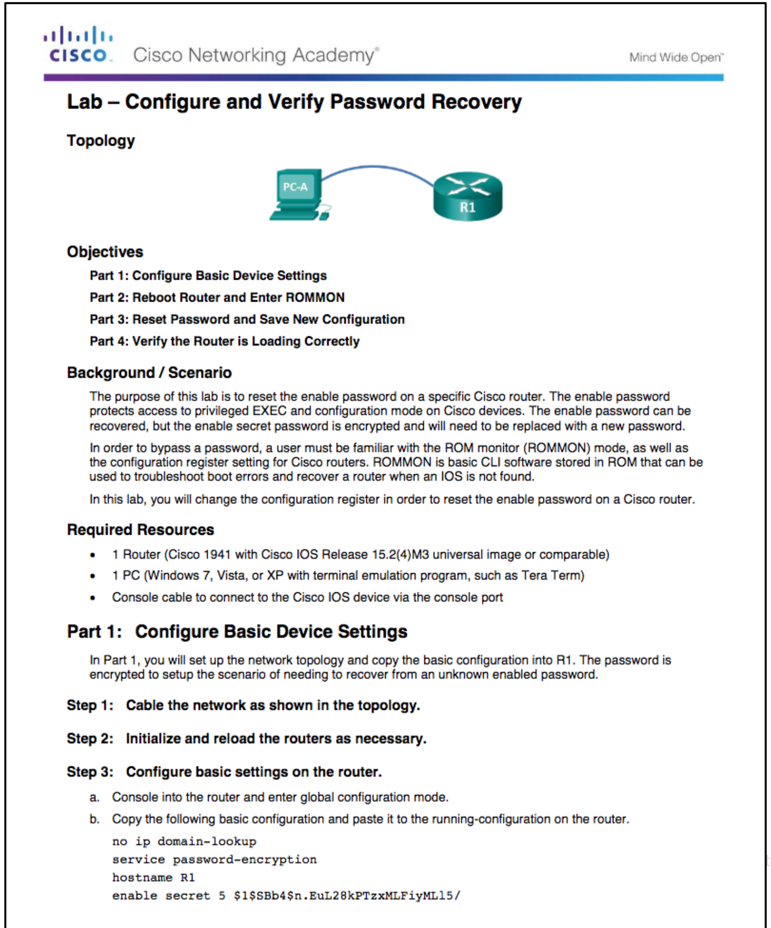
Background / Scenario

Cisco networking devices are often upgraded or swapped out for a number of reasons. It is important to maintain backups of the latest device configurations, as well as a history of configuration changes. A TFTP server is often used to backup configuration files and IOS images in production networks. A TFTP server is a centralized and secure method used to store the backup copies of the files and restore them as necessary. Using a centralized TFTP server, you can back up files from many different Cisco devices.

In addition to a TFTP server, most of the current Cisco routers can back up and restore files locally from CompactFlash (CF) memory or a USB flash drive. The CF is a removable memory module that has replaced the limited internal flash memory of earlier router models. The IOS image for the router resides in the CF memory, and the router uses this IOS Image for the boot process. With the larger size of the CF memory, additional files can be stored for backup purposes. A removable USB flash drive can also be used for backup purposes.

In this lab, you will use TFTP server software to back up the Cisco device running configuration to the TFTP server or flash memory. You can edit the file using a text editor and copy the new configuration back to a Cisco device.

Lab – Researching Password Recovery Procedures



Cisco Networking Academy®

Mind Wide Open™

Lab – Configure and Verify Password Recovery

Topology

Objectives

Part 1: Configure Basic Device Settings

Part 2: Reboot Router and Enter ROMMON

Part 3: Reset Password and Save New Configuration

Part 4: Verify the Router is Loading Correctly

Background / Scenario

The purpose of this lab is to reset the enable password on a specific Cisco router. The enable password protects access to privileged EXEC and configuration mode on Cisco devices. The enable password can be recovered, but the enable secret password is encrypted and will need to be replaced with a new password.

In order to bypass a password, a user must be familiar with the ROM monitor (ROMMON) mode, as well as the configuration register setting for Cisco routers. ROMMON is basic CLI software stored in ROM that can be used to troubleshoot boot errors and recover a router when an IOS is not found.

In this lab, you will change the configuration register in order to reset the enable password on a Cisco router.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to connect to the Cisco IOS device via the console port

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and copy the basic configuration into R1. The password is encrypted to setup the scenario of needing to recover from an unknown enabled password.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings on the router.

a. Console into the router and enter global configuration mode.

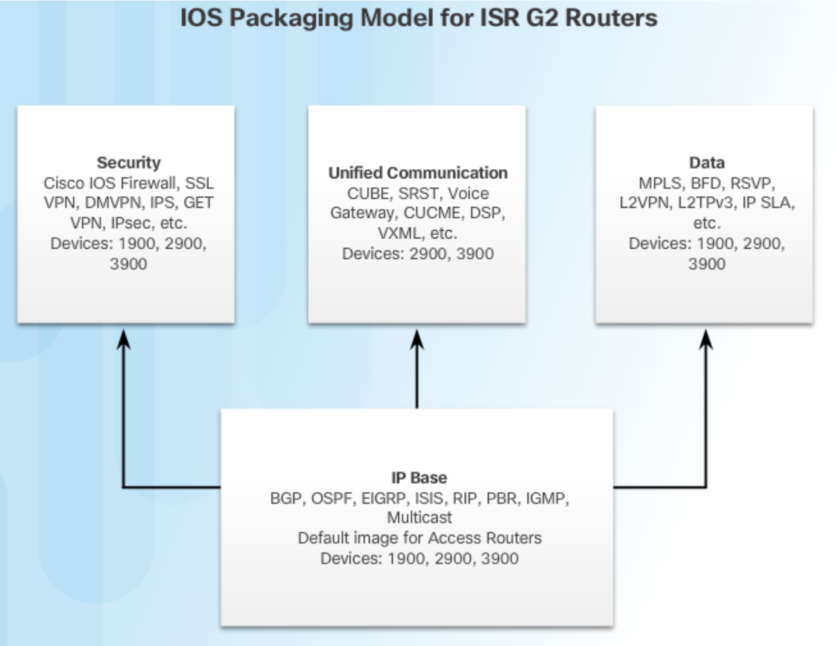
b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
hostname R1
enable secret 5 $1$SBb4$n.EuL28kPTzxMLFiyML15/
```

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

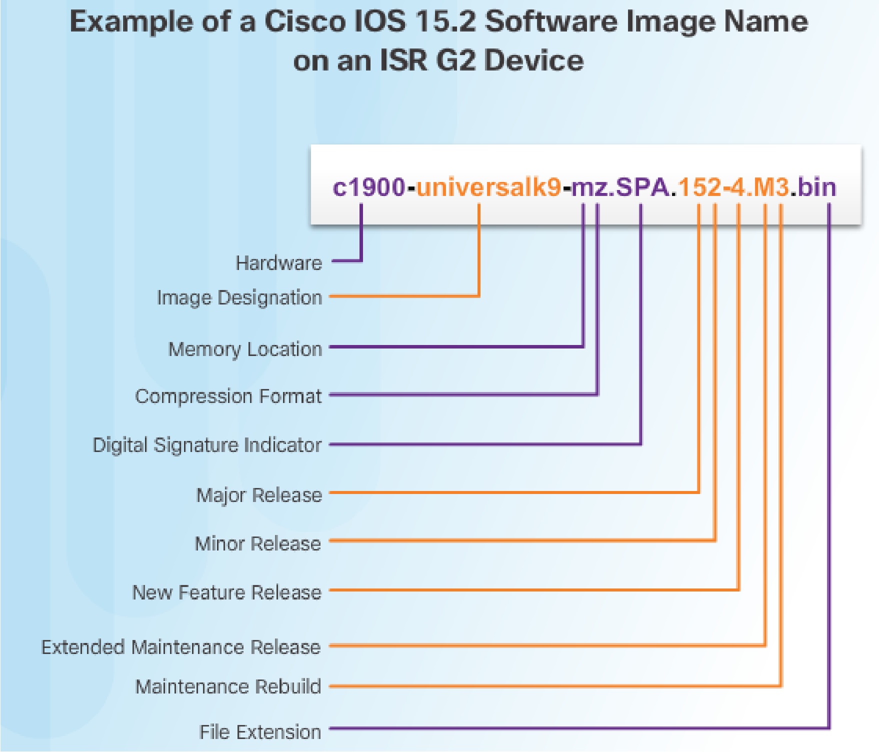
Data
MPLS, BFD, RSVP, L2VPN, L2TPv3, IP SLA, etc.
Devices: 1900, 2900, 3900

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

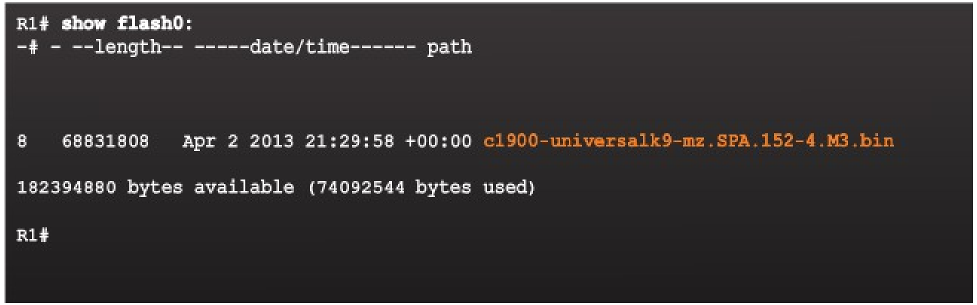
- Each router ships with one of two types of universal images in ISR G2:
  - **“universalk9"** – offers all of the Cisco IOS software features, including strong payload cryptography features, such as IPsec VPN, SSL VPN, and Secure Unified Communications
  - **“universalk9_npe”** – some countries have 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 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



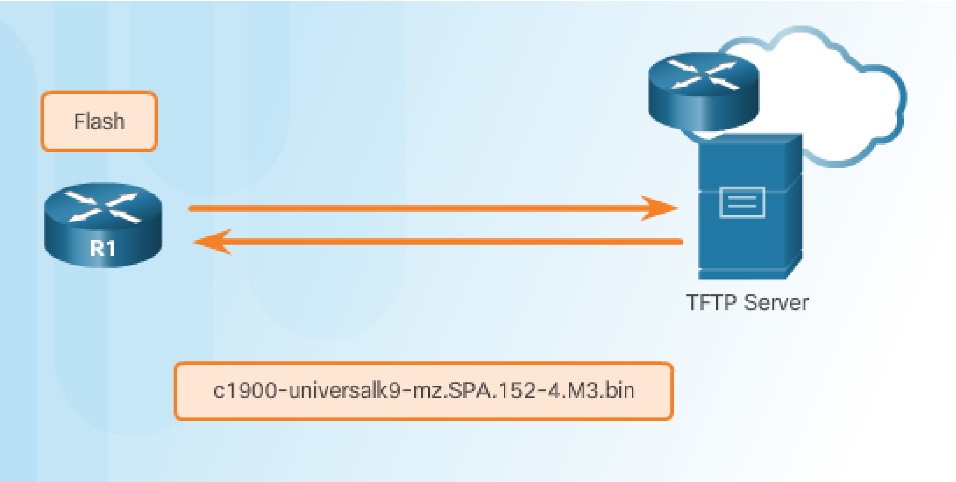
```
R1# show flash0:
-# - --length-- -----date/time------ path


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 Management

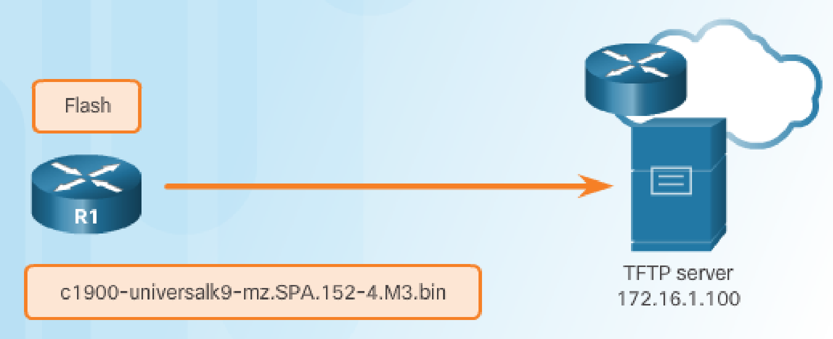
TFTP Servers as a Backup Location

- 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.

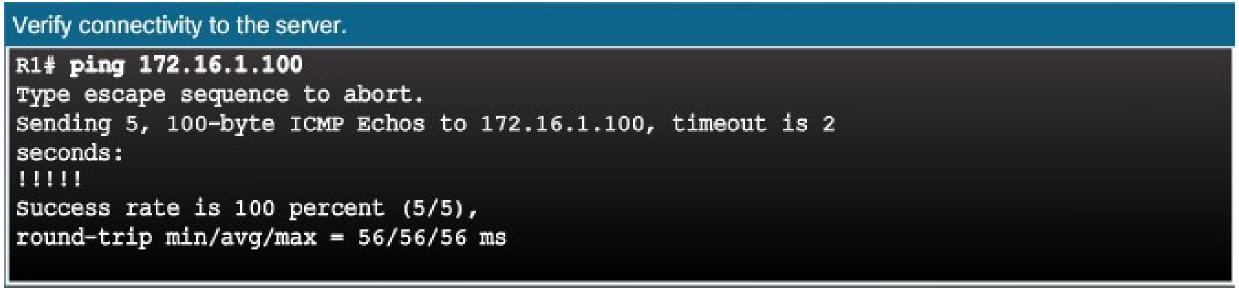


IOS Image Management

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.

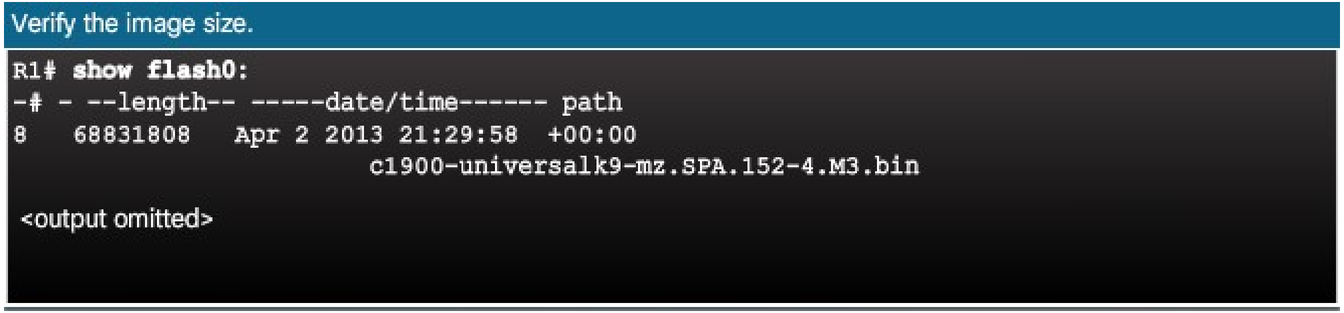


Verify connectivity to the server.

```
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
```

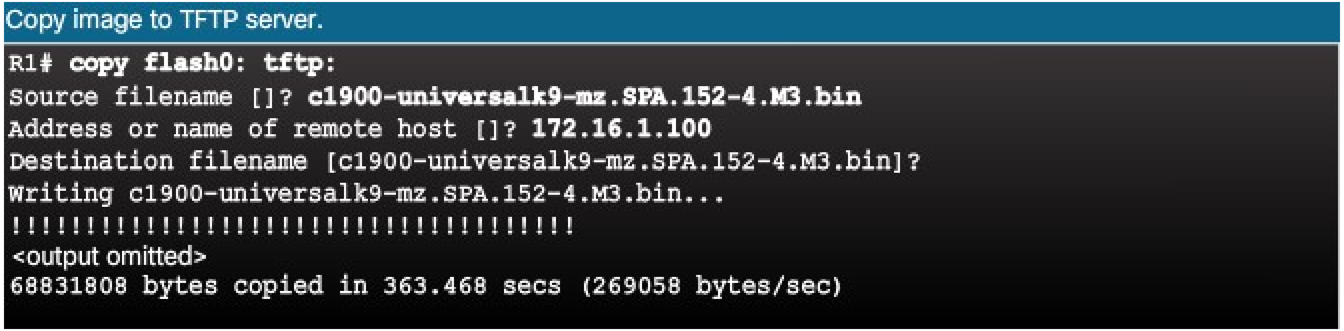
IOS Image Management

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



Verify the image size.

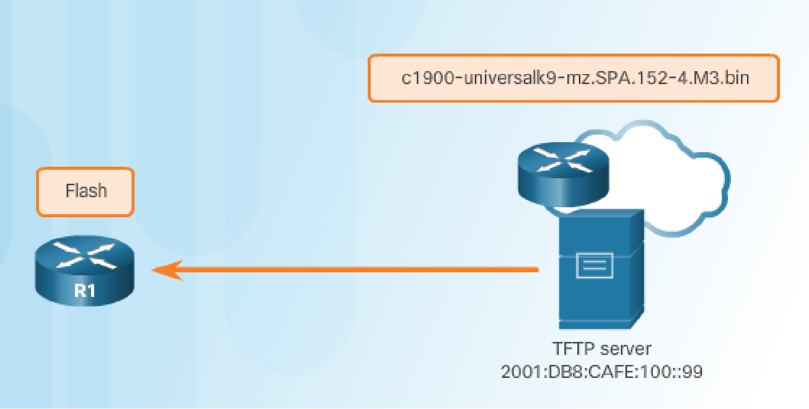
```
R1# show flash0:
-# - --length-- -----date/time------ path
8    68831808   Apr 2 2013 21:29:58  +00:00
                        c1900-universalk9-mz.SPA.152-4.M3.bin

 <output omitted>
```



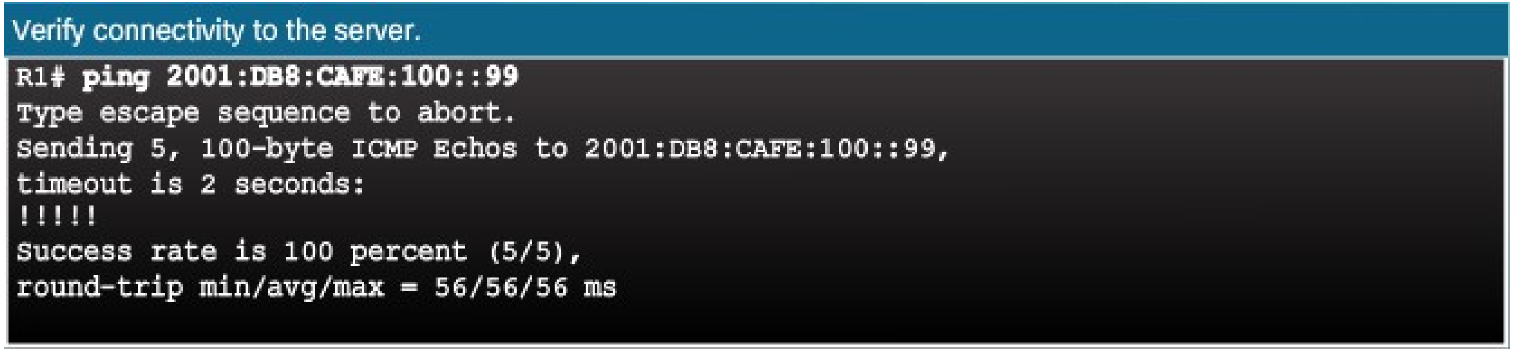
Copy image to TFTP server.

```
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



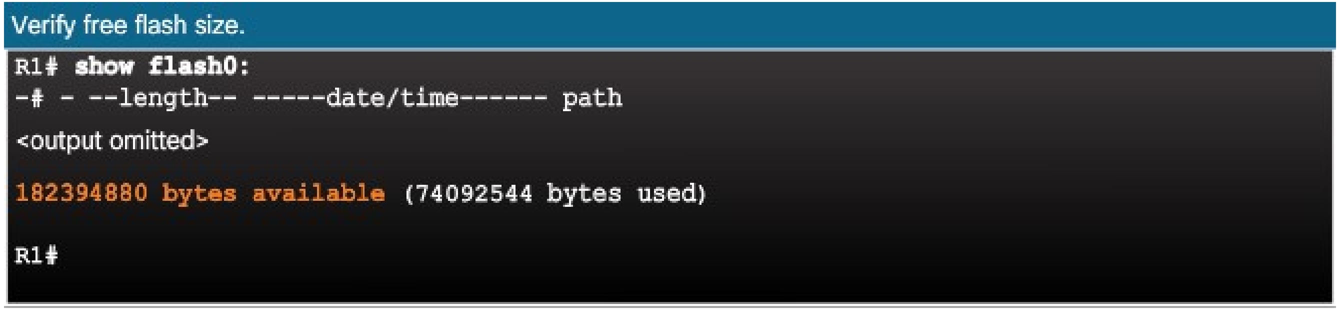
- A new image file (c1900-universalk9-mz.SPA.152-4.M3.bin) will be copied from the TFTP server at 2001:DB8:CAFE:100::99 to the router.



Verify connectivity to the server.

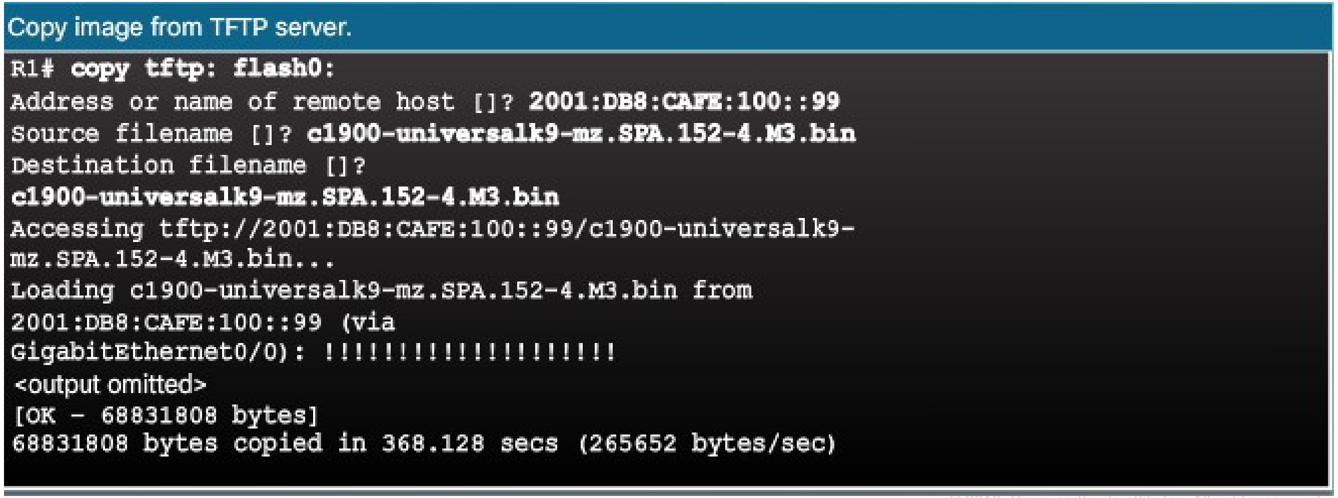
```
R1# ping 2001:DB8:CAFE:100::99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:100::99,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

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



Verify free flash size.

```
R1# show flash0:
-# - --length-- -----date/time------ path
<output omitted>

182394880 bytes available (74092544 bytes used)

R1#
```

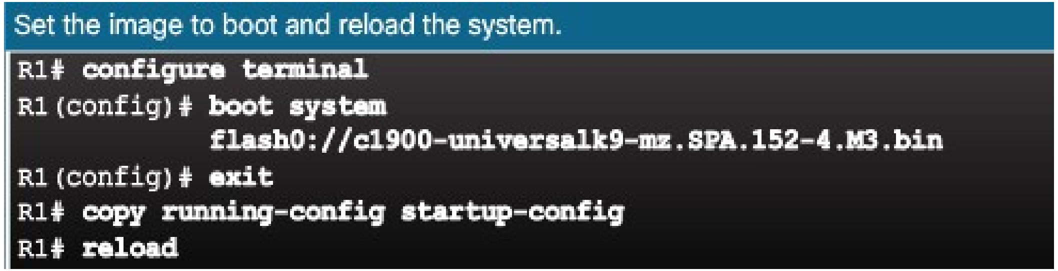


Copy image from TFTP server.

```
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)
```

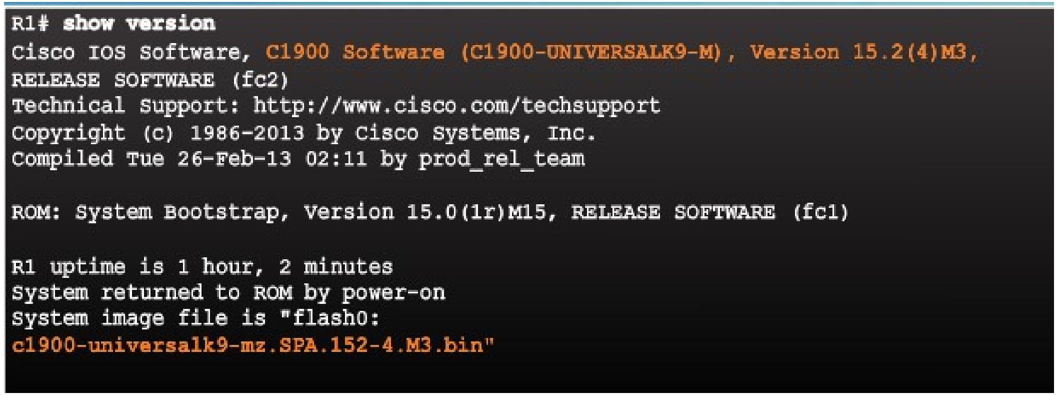
The boot system Command

- 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.

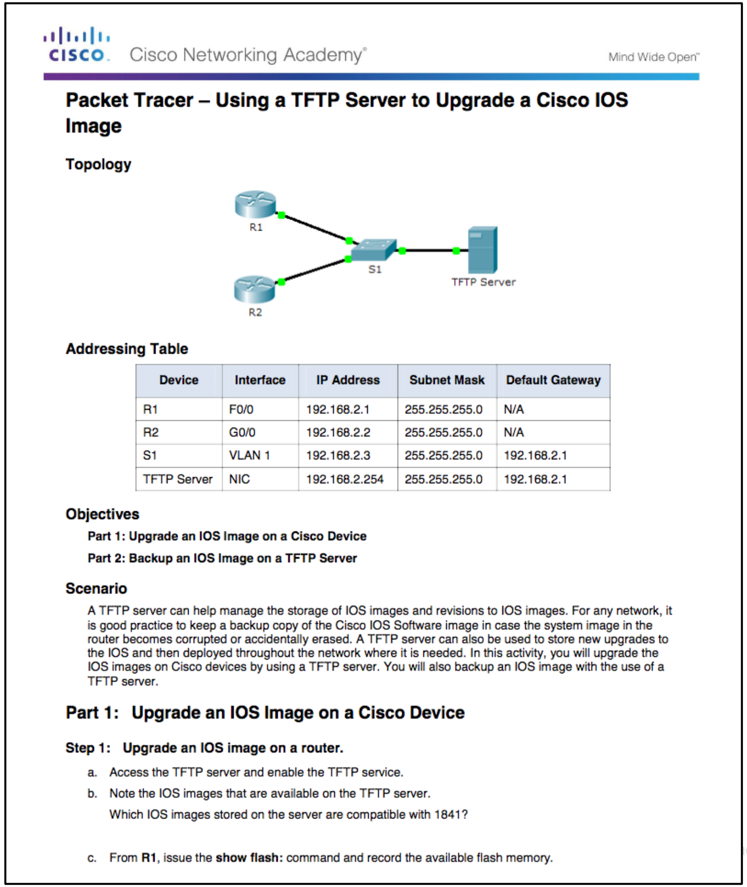
```
R1# configure terminal
R1(config)# boot system
            flash0://c1900-universalk9-mz.SPA.152-4.M3.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```



```
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.

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



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.

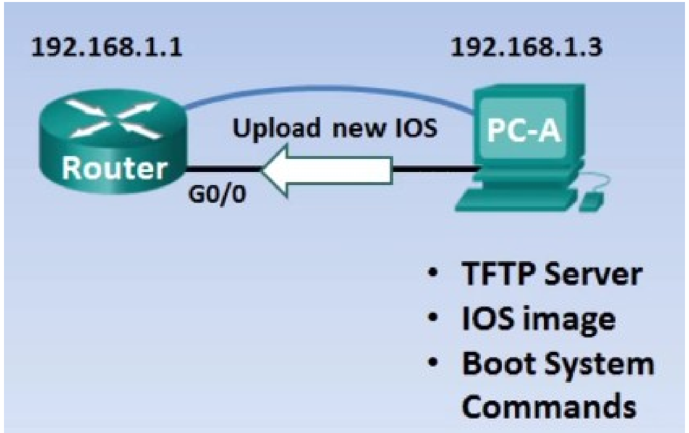
Which IOS images stored on the server are compatible with 1841?

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

Video Demonstration - Managing Cisco IOS Images

Objective:

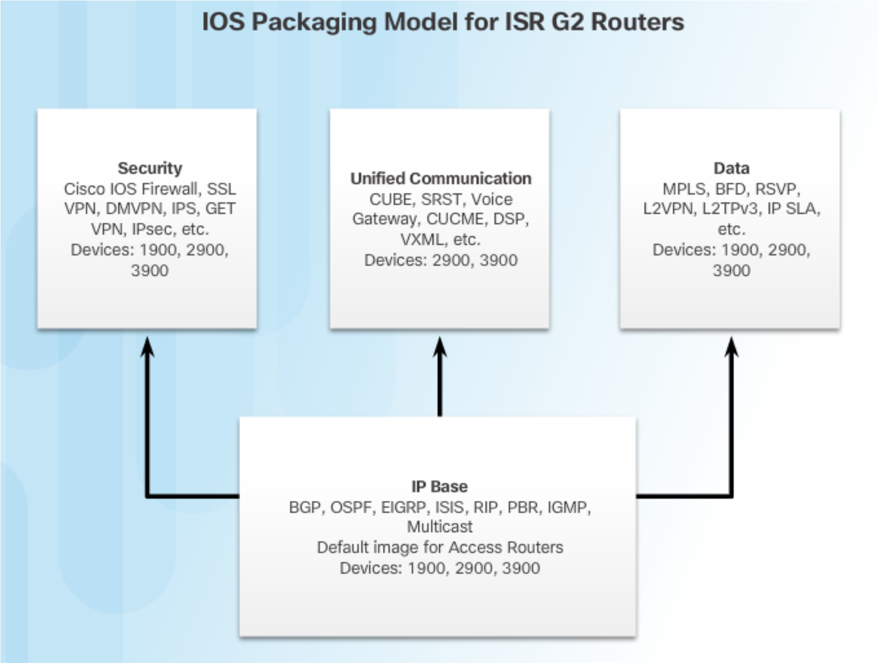
- Use a TFTP server to upload an updated IOS image file to a Cisco Router.
- Use the boot system command to boot the router to the new IOS image file.
- Reload the router and successfully boot to the new IOS image file.



- TFTP Server
- IOS image
- Boot System Commands

Software Licensing

Licensing Overview

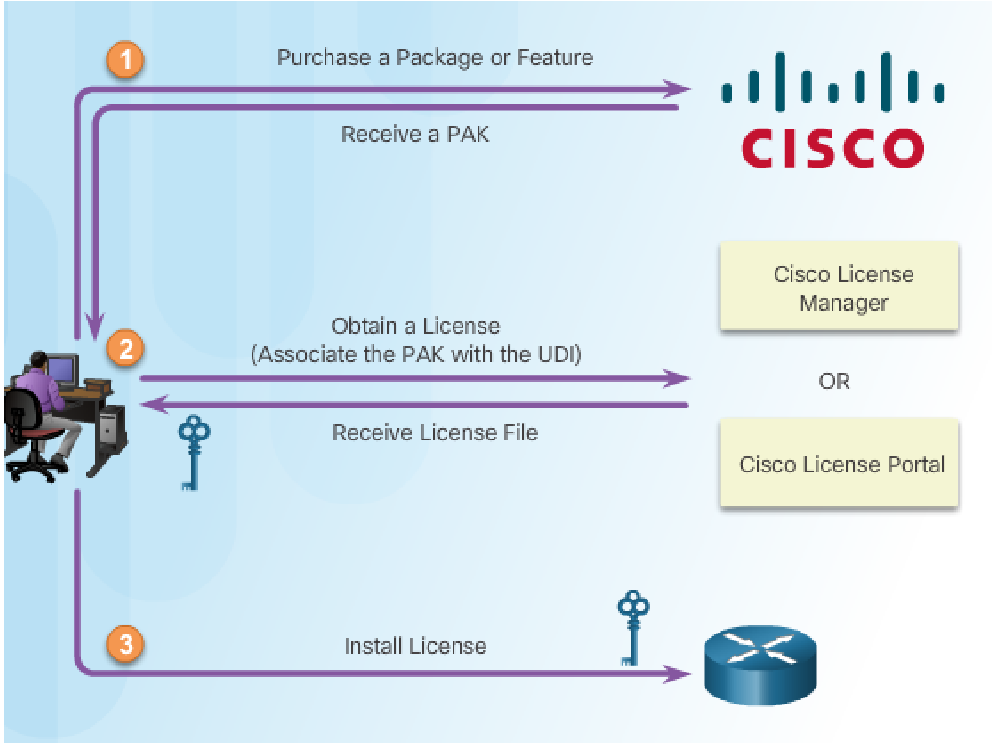


IOS Packaging Model for ISR G2 Routers

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

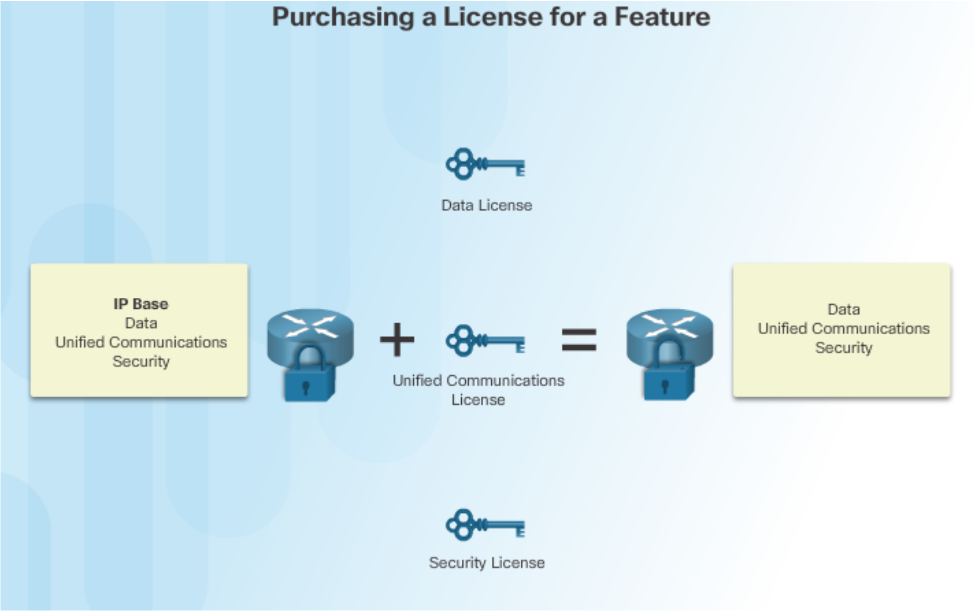
- Each device ships with the same universal image.
- Technology packages are enabled in the universal image via Cisco Software Activation licensing keys.
- The Cisco IOS Software Activation feature allows the user to enable licensed features and register licenses.
- Technology packages that are available: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

Licensing Process



- 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

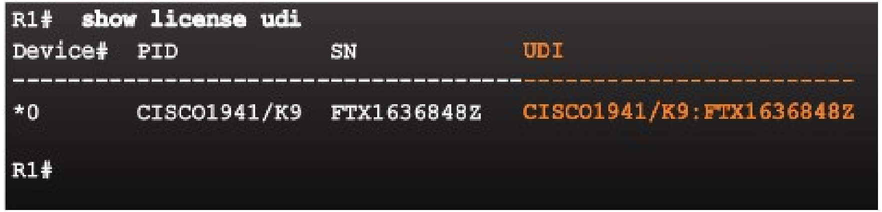


- Customers receive a PAK with purchase that serves as a receipt and is used to obtain a license.
- A PAK is an 11 digit alpha numeric key created by Cisco manufacturing. It defines the Feature Set associated with the PAK.
- As shown in the figure, a separate license is required for each package, IP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

Step 2. Obtain a License

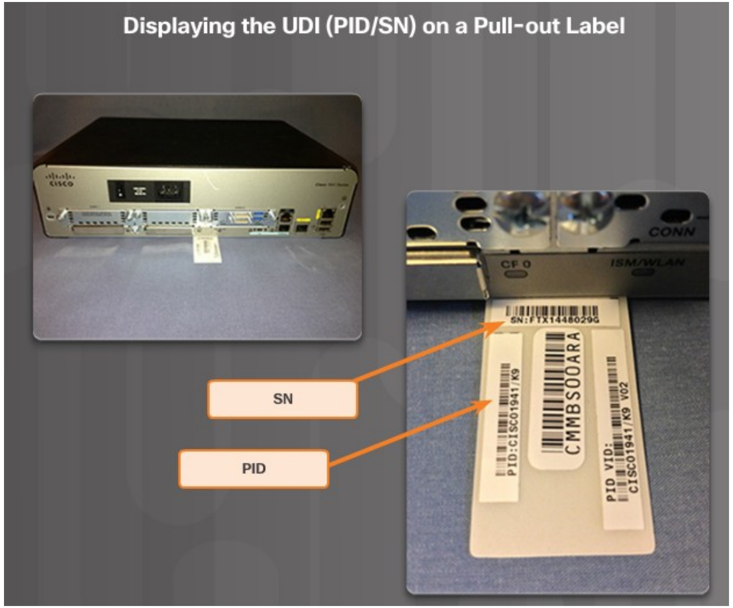
- The UDI is a combination of the Product ID (PID), the Serial Number (SN), and the hardware version. The SN is an 11 digit number which uniquely identifies a device. The PID identifies the type of device. Only the PID and SN are used for license creation.

- 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#
```

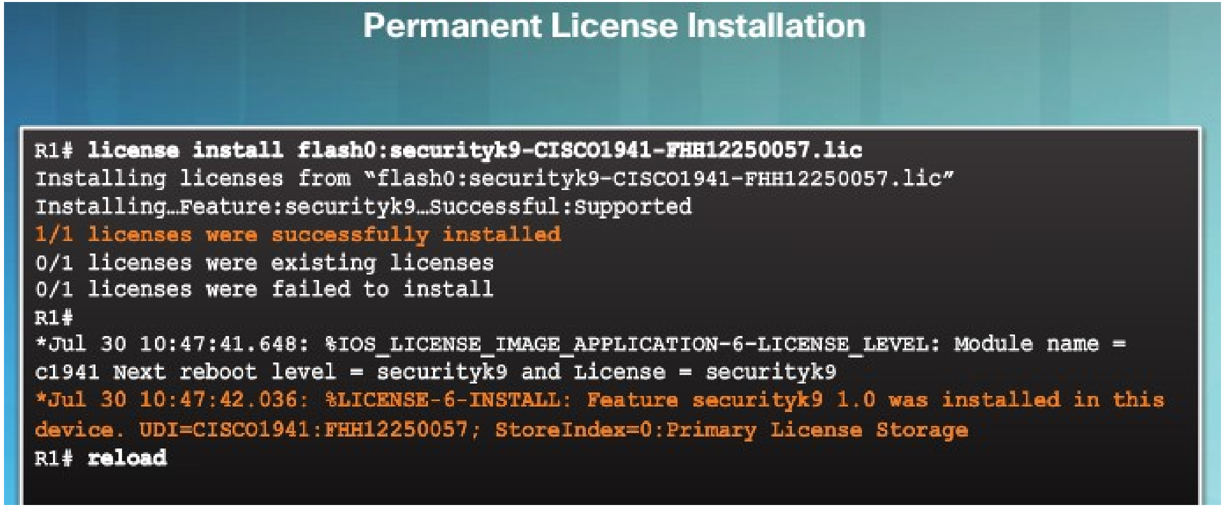
K9 silné crypto
K8 slabé crypto



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

Software Licensing

Step 3. Install the License

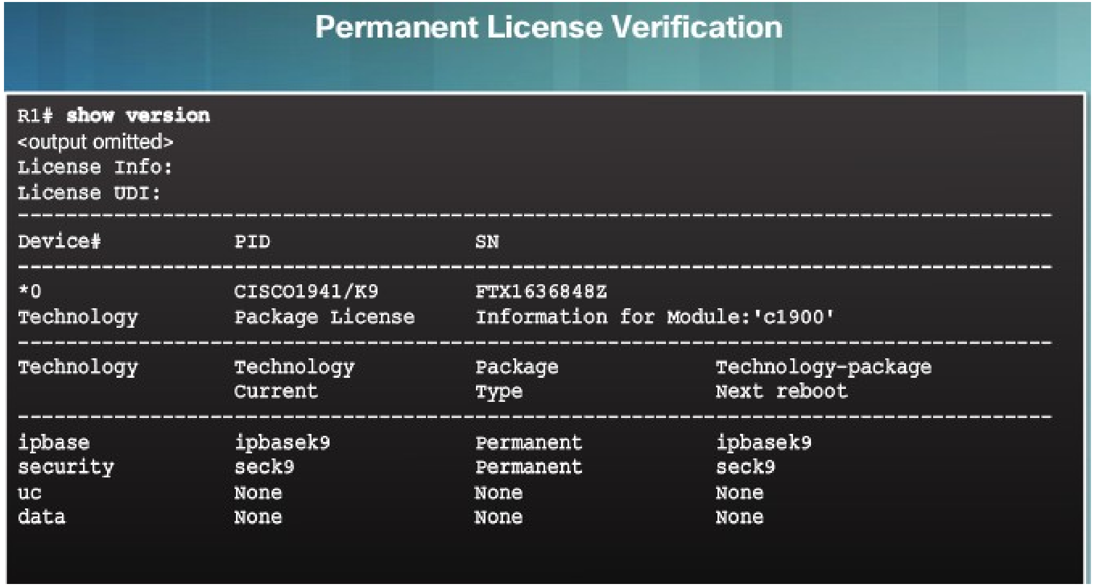


Permanent License Installation

```
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
```

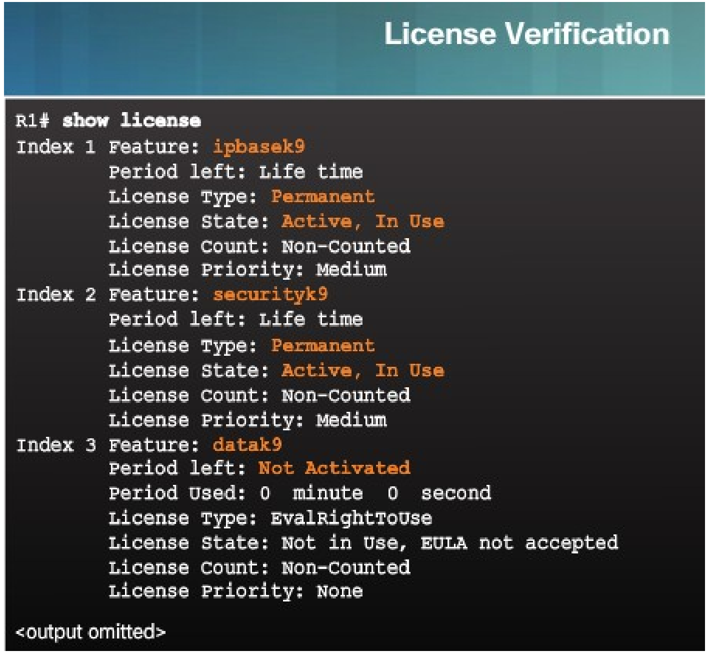
- A permanent license is a license that never expires. After a permanent license is installed on a router, it is good for that particular feature set for the life of the router, even across IOS versions.

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
```

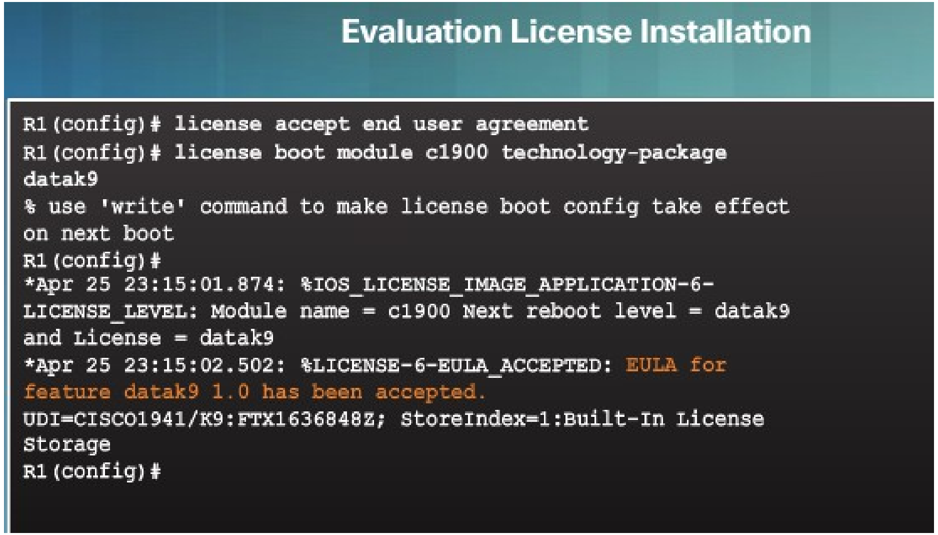


License Verification

```
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>
```

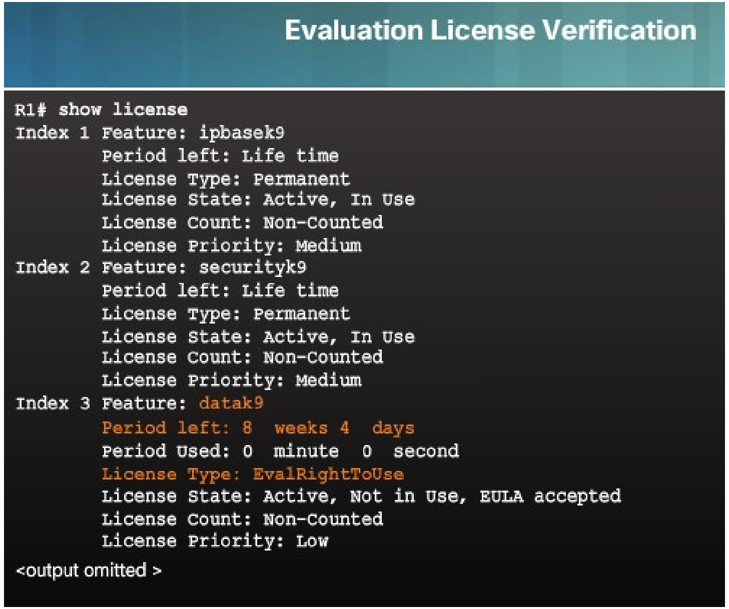
License Verification and Management

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)#
```

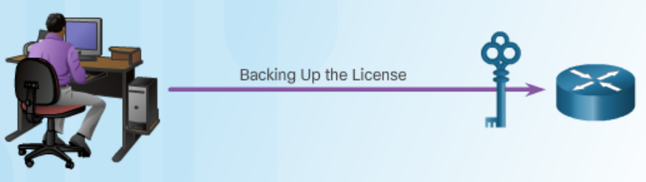


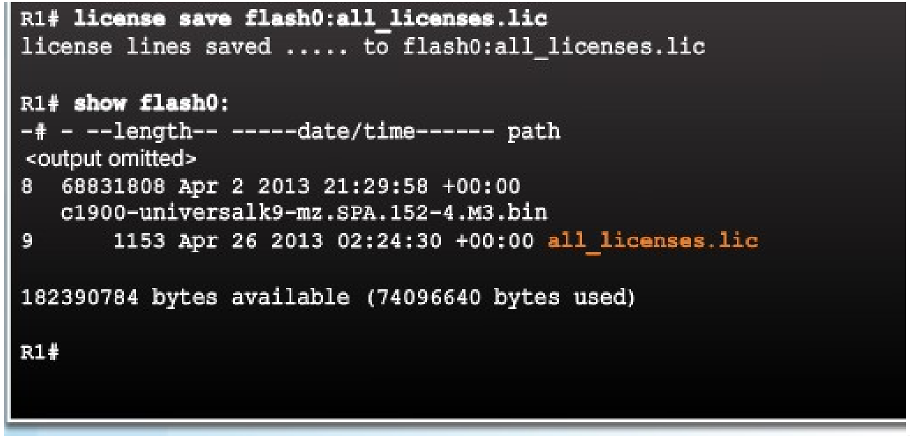
Evaluation License Verification

```
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 >
```

Back up the License

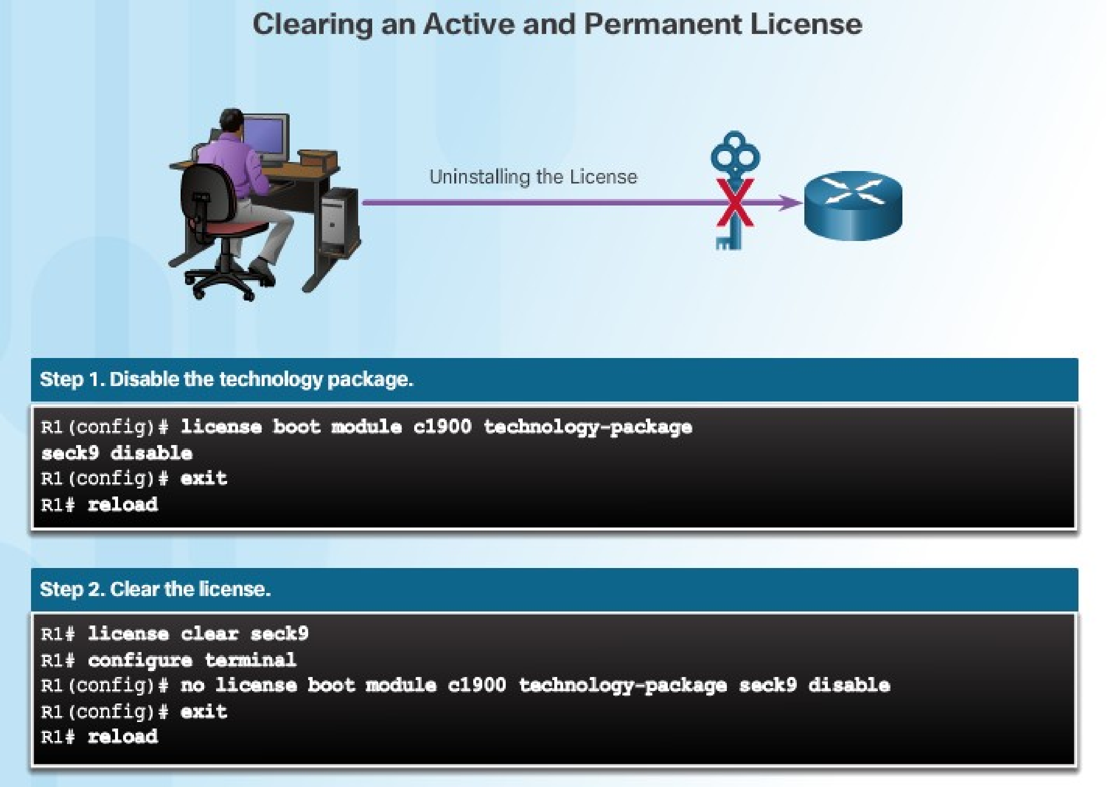
- The **license save** command is used to copy all licenses in a device and store them.
- Saved licenses are restored by using the **license install** command.
- The command to back up a copy of the licenses on a device is:
  - Router# **license save** *file-sys://lic-location*
- Use the show flash0: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

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.

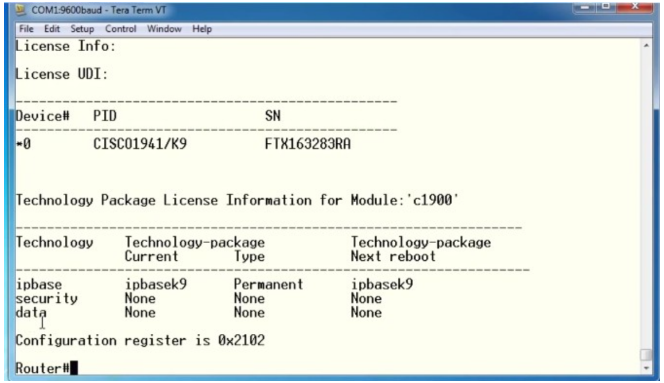
```
R1# license clear seck9
R1# configure terminal
R1(config)# no license boot module c1900 technology-package seck9 disable
R1(config)# exit
R1# reload
```

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

Video 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


COM1:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX163283RA


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      None          None           None
data          None          None           None

Configuration register is 0x2102

Router#
```

10.4 Chapter Summary

Conclusion

Packet Tracer – Skills Integration Challenge

Conclusion

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.

cisco