Cisco IOS Management

NETWORK ADMINISTRATION

Songyut Phoemphon

Email: songyut@sut.ac.th

Device Discovery

Use discovery protocols to map a network topology.

- Use CDP to map a network topology.
- Use LLDP to map a network topology.

Device 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
  - Determin l topology when documen

Device Discovery

Device Discovery with CDP

Configure and Verify CDP

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

Verify status and display information

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

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

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

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

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

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Total cdp entries displayed : 0
```

No neighbors detected

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

Indicates the interfaces with CDP enabled

Device Discovery

Device Discovery with CDP

Discover Devices Using CDP


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

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

show cdp neighbors discovers:

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

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

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010221FF0000000000000000229121038OFF0000
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

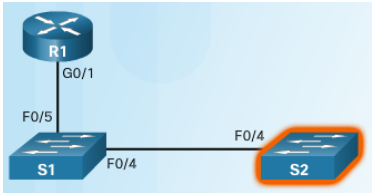
Device Discovery

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

Device Discovery with LLDP

LLDP Overview

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

Device Discovery

Device Discovery with LLDP

Configure and Verify LLDP

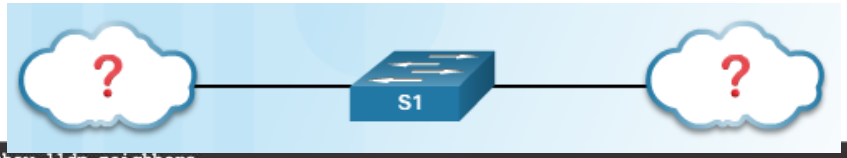
```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp

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**

Device Discovery

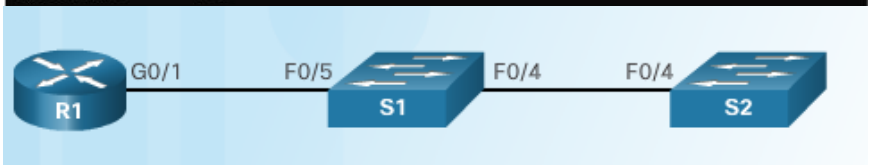
Device Discovery with LLDP

Discover Devices Using LLDP




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

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

Total entries displayed: 2
```

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

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

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

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



Device Management

Configure NTP and Syslog in a small to medium-sized business network.

- Implement NTP between a NTP client and NTP server.

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:

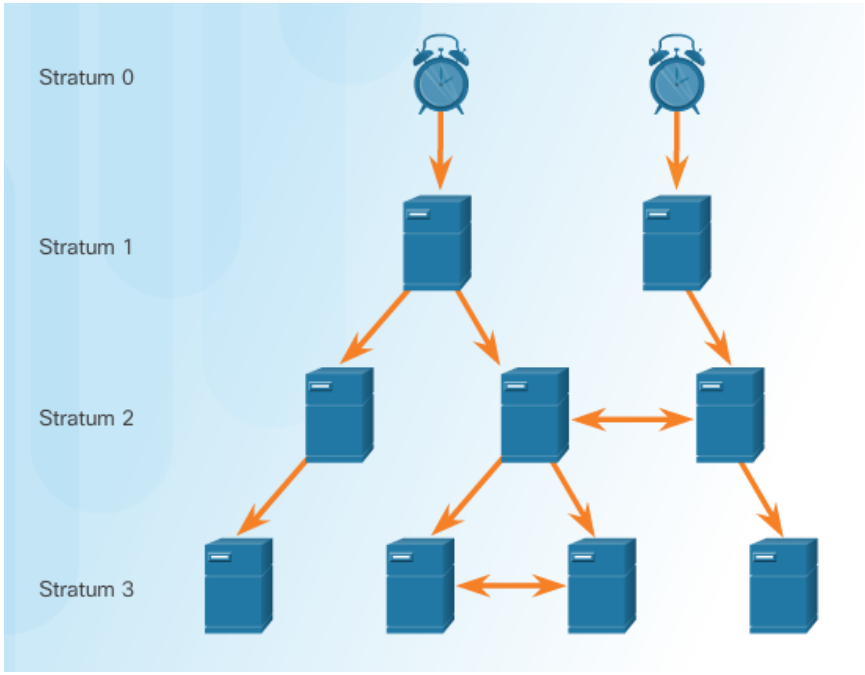
- Manually configure the date and time, as shown in the figure
- Configure the Network Time Protocol (NTP)
  - NTP uses UDP port 123
  - NTP clients obtain time and date from a single source

Device Management

NTP

NTP Operation

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



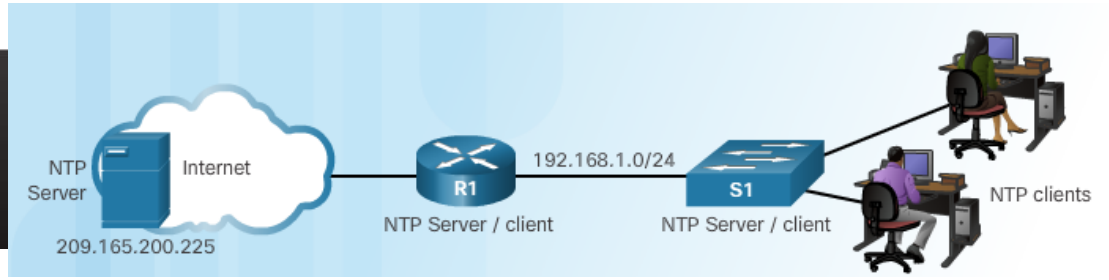
Device Management

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

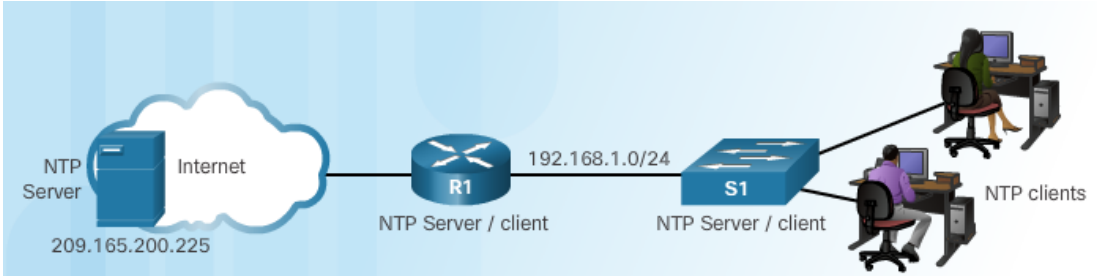
```
R1# show ntp associations

  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

Device Management

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

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.

Device Maintenance

Router and Switch File Maintenance

Backing up and Restoring using TFTP

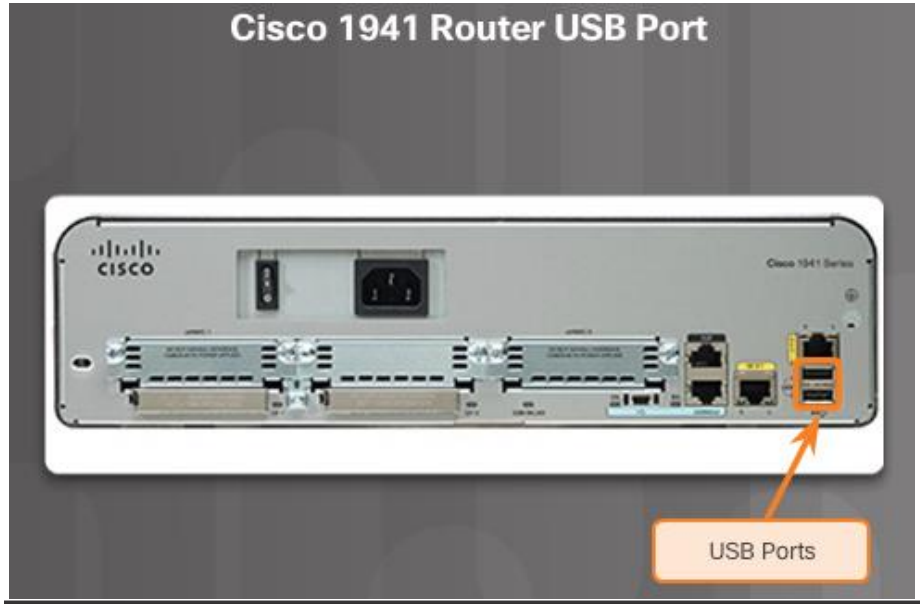
- Configuration files should be backed up and included in network documentation
- Commands - **copy running-config tftp** (see figure) or **copy startup-config tftp**

```
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]
```

Device Maintenance

Router and Switch File Maintenance

Using USB Ports on a Cisco Router



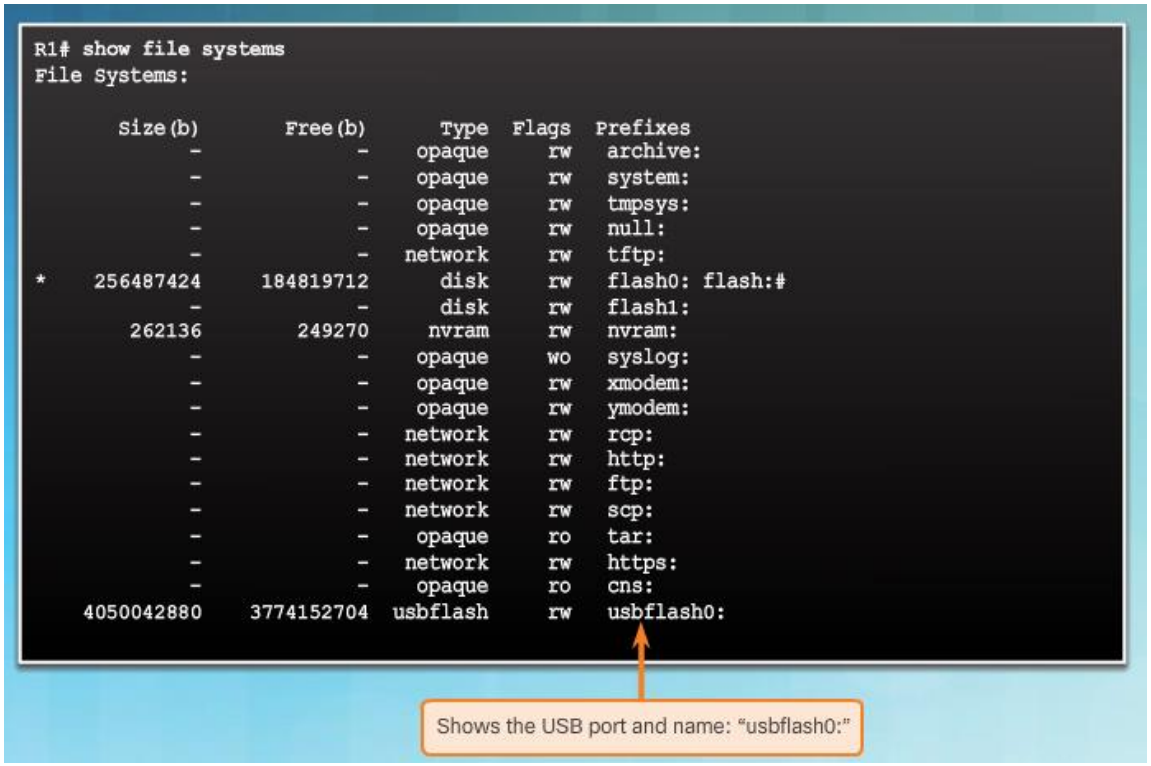

```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

- 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.

Device Maintenance

Router and Switch File Maintenance

Backing up and Restoring Using USB



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

Device Maintenance

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

Device Maintenance

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

Device Maintenance

Router and Switch File Maintenance
Password Recovery

```
Readonly ROMMON initialized

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

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

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

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

Step 1. Enter the ROMMON mode.

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

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

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

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

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

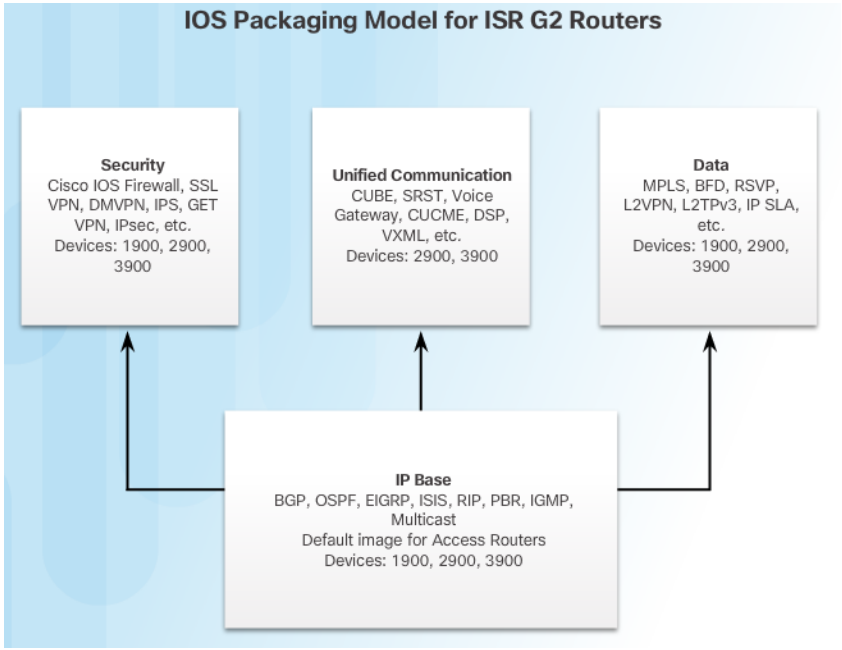
Step 4. Save the new configuration.

Device Maintenance

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.

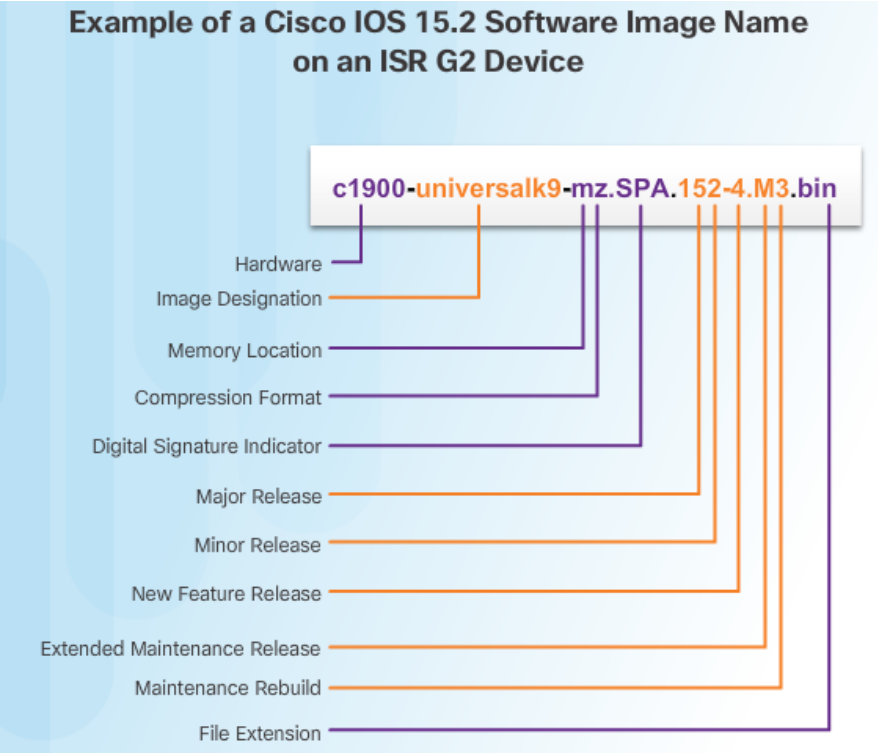


- Each router ships with one of two types of universal images in ISR G2:
  - **"universalk9"** – offers all of the Cisco IOS software features, including strong payload cryptography features, such as IPsec VPN, SSL VPN, and Secure Unified Communications
  - **"universalk9_npe"** – some countries have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

Device Maintenance

IOS System Files

IOS Image Filenames



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#
```

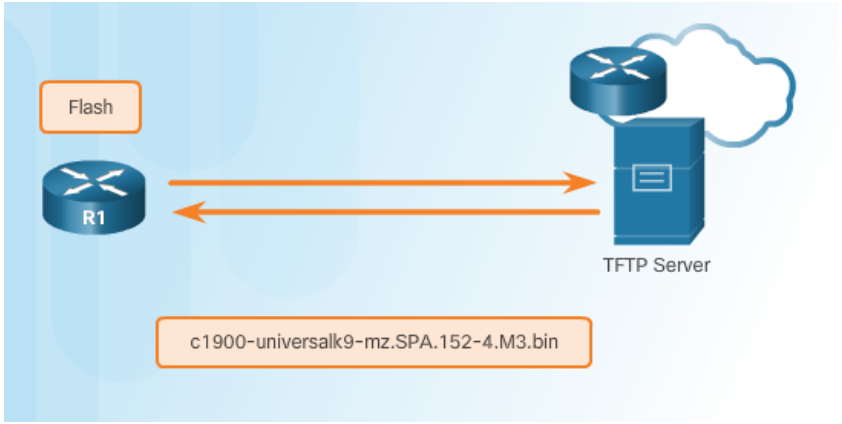
- The most common designation for memory location and compression format is mz. The first letter indicates the location where the image is executed on the router. The locations can include:
  - f - flash
  - m - RAM
  - r - ROM
  - l - relocatable
- The compression format can be z for zip or x for mzip.

Device Maintenance

IOS Image Management

TFTP Servers as a Backup Location

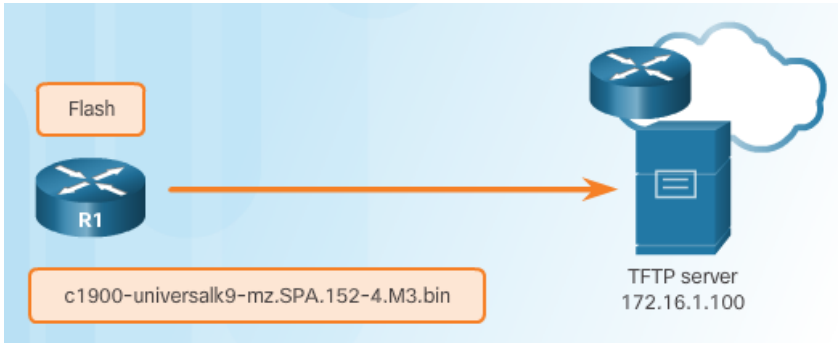
- Cisco IOS Software images and configuration files can be stored on a central TFTP server.
- It is good practice to keep a backup copy of the Cisco IOS Software image in case the system image in the router becomes corrupted or accidentally erased.
- Using a network TFTP server allows image and configuration uploads and downloads over the network. The network TFTP server can be another router, a workstation, or a host system.



Device Maintenance

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
```

Device Maintenance

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>
```

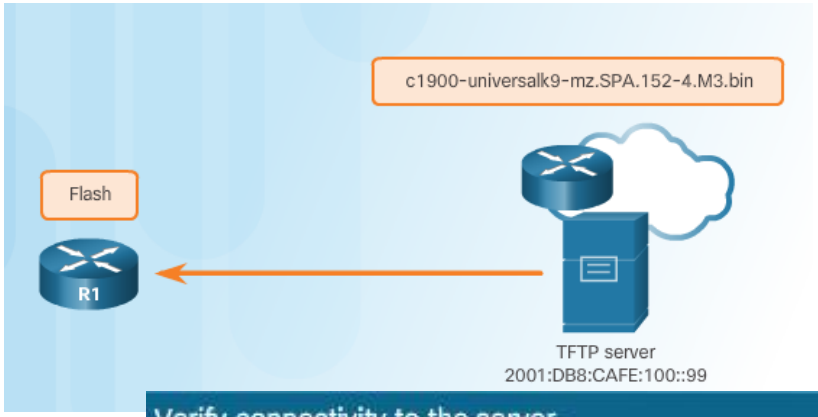
Copy image to TFTP server.

```
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)
```

Device Maintenance

IOS Image Management

Steps to Copy an IOS Image to a Device



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

Verify connectivity to the server.

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

Device Maintenance

IOS Image Management

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

Verify free flash size.

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

182394880 bytes available (74092544 bytes used)

R1#
```

Copy image from TFTP server.

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

Device Maintenance

IOS Image Management

The boot system Command

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

Set the image to boot and reload the system.

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

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

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

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

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

Operating Cisco IOS Software

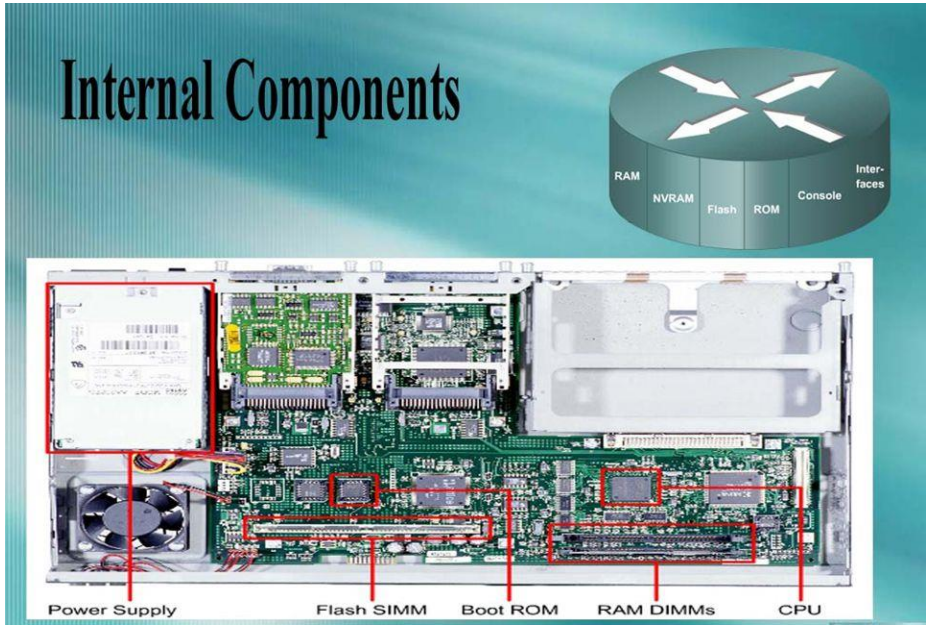
Cisco IOS

Memory

- RAM (RW, Volatile=Temporary)
  - Operating System (IOS), Current Configuration, Table, Buffer
- NVRAM (RW, Non-Volatile) keep backup config
- FLASH (RO) keep OS
- ROM (RO) keep bootstrap

Interface

- LAN (ethernet, fastethernet, gigabitethernet)
- WAN (serial, hssi)
- Console /AUX

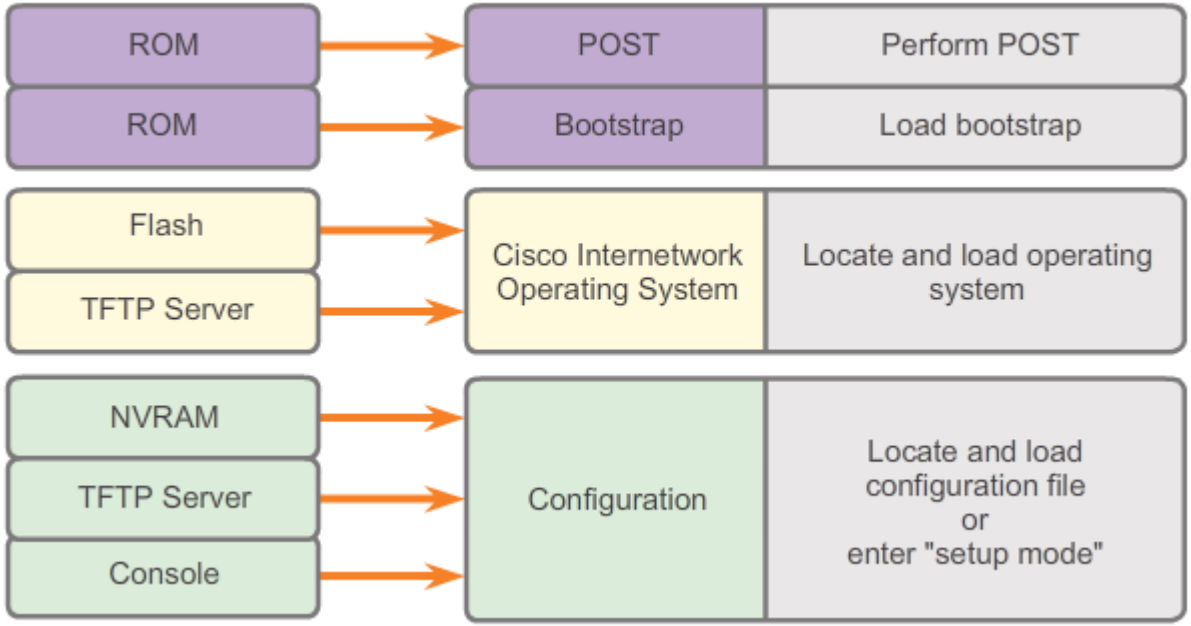


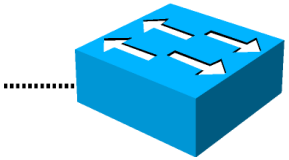
Operating Cisco IOS Software

Cisco IOS

An Overview of Cisco Device Startup

1. Find and check device hardware.
2. Find and load Cisco IOS software image.
3. Find and apply device configurations.





Operating Cisco IOS Software

Cisco IOS
Configuration Register

- 16-bit register written in NVRAM
  - Bit 15 to 0 (left to right)
  - Default: 0x2102

Bit value on	Hexa Decimal value	Description
0 to 3	0000 to 000F	These value define the Boot field as shown in previous image.
5, 11 and 12	0800-1000	Denotes the console line speed
6	0040	This value ignore the contents of NVRAM
7	0080	This value enable the OEM function
8	0101	This value do disable the break function
10	0400	This will broadcast the IP with all values 0
13	0200	Router boot from default ROM
14	4000	IP broadcast
15	8000	This will enable diagnostic message. NVRAM content do not participate any more

Configuration Register	Router Behavior
0x2102	Ignores break Boots into ROM if initial boot fails 9600 console baud rate default value for most platforms
0x2142	Ignores break Boots into ROM if initial boot fails 9600 console baud rate Ignores the contents of Non-Volatile RAM (NVRAM) (ignores configuration)

Operating Cisco IOS Software

Cisco IOS
Configuration Register

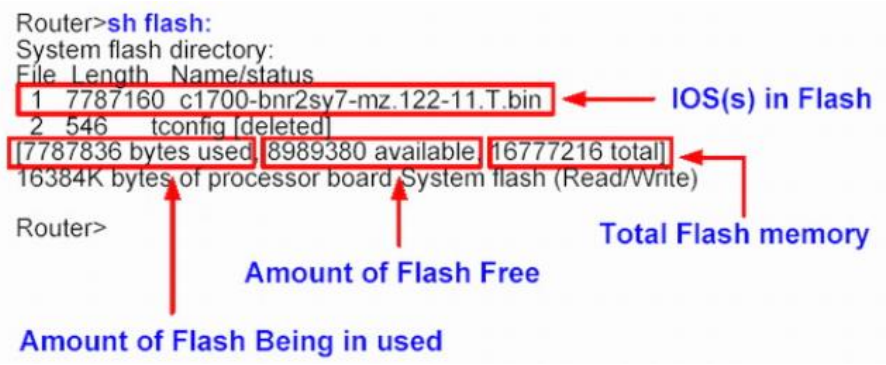
- Boot via ROM monitor
- Select a file to boot
- Enable / disable Break
- Setting console terminal baud rate
- Load IOS from ROM
- Boot from TFTP server

Operating Cisco IOS Software

Cisco IOS

Checking / Changing Register Values

- Router#show version
- Router(config)#config-register 0x0101



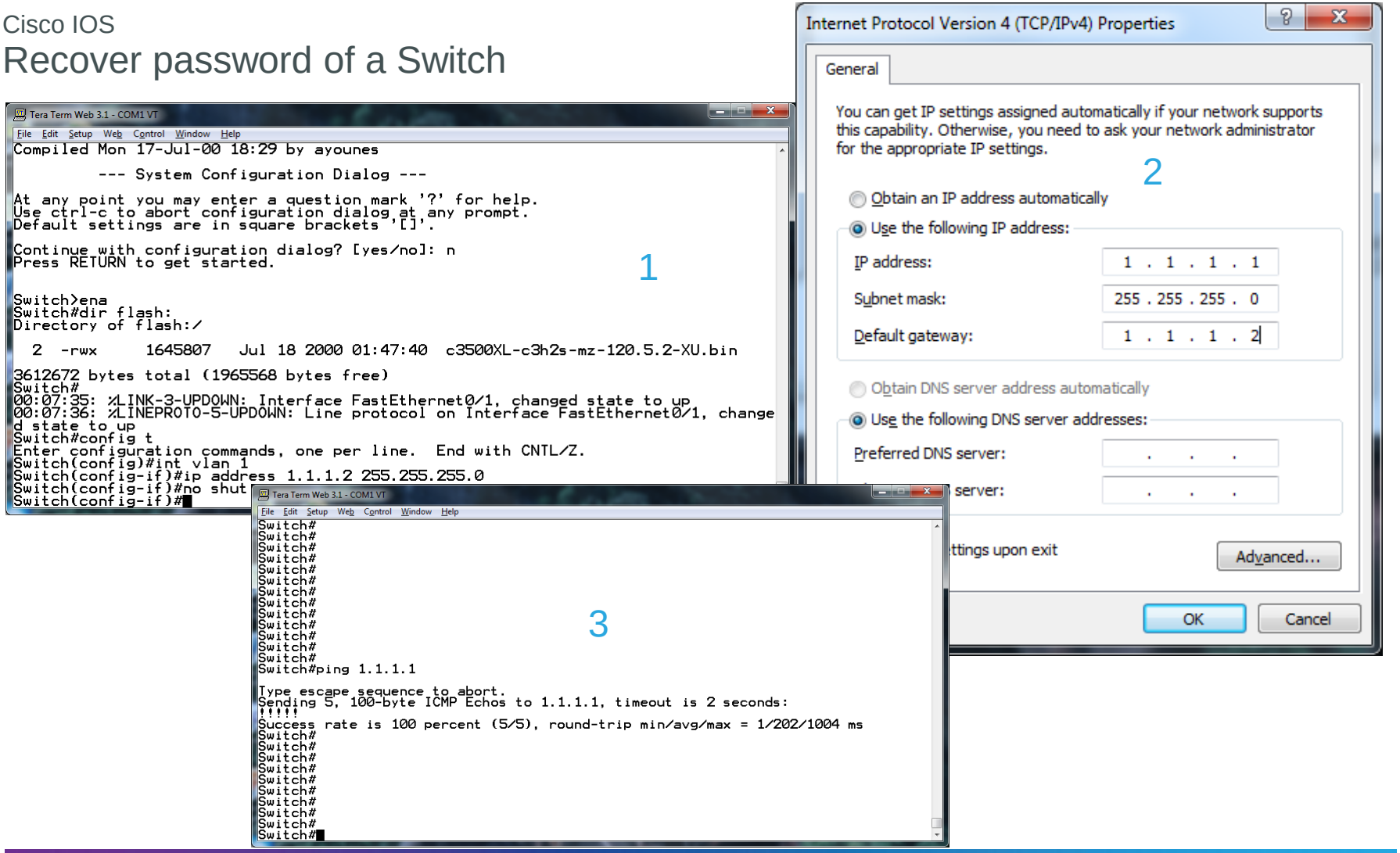
Recover password of a Router

- Press Ctrl+Break while booting
- rommon> 0x2142 /* change Register to set bit 6 */
- rommon> reset /* reload router */
- Router asks “Would you like to enter basic … setup?” (Ans= No)
- Router> enable /* login to Privilege mode */
- Router# copy startup-config running-config
- Router(config)# enable secret <password> /* change password */
- Router(config)# config-register 0x2102 /* unset bit 6 (original) */
- Reload router

Operating Cisco IOS Software

Cisco IOS

Recover password of a Switch



Operating Cisco IOS Software

Cisco IOS

Recover password of a Switch

```
S1#copy tftp flash
Address or name of remote host []? 192.168.1.1
Source filename []? c2960-lanbasek9-mz.122-55.SE.bin
Destination filename [c2960-lanbasek9-mz.122-55.SE.bin]?
Accessing tftp://192.168.1.1/c2960-lanbasek9-mz.122-55.SE.bin...
Loading c2960-lanbasek9-mz.122-55.SE.bin from 192.168.1.1 (via Vlan1): !!!!
```

3

```
Directory of flash:/

    2  -rwx  1919      <date>          private-config.text
    3  -rwx  7075041   <date>          c2960-lanbasek9-mz.122-44.SE6.bin
    6  -rwx  9771520   <date>          c2960-lanbasek9-mz.122-55.SE.bin
    4  -rwx  1572      <date>          config.text
    5  -rwx  3096      <date>          multiple-fs

11004928 bytes available (16993280 bytes used)
```

4

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#boot system flash:/c2960-lanbasek9-mz.122-55.SE.bin
S1(config)#
S1(config)#
```

5

Tera Term Web 3.1 - COM1 VT

File Edit Setup Web Control Window Help

```
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#format flash:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "flash:".  Continue? [confirm]
flashfs[1]: 0 files, 1 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 3612672
flashfs[1]: Bytes used: 1024
flashfs[1]: Bytes available: 3611648
flashfs[1]: flashfs fsck took 3 seconds.
Format of flash: complete
Switch#
```

1

Tera Term Web 3.1 - COM1 VT

File Edit Setup Web Control Window Help

```
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#format flash:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "flash:".  Continue? [confirm]
flashfs[1]: 0 files, 1 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 3612672
flashfs[1]: Bytes used: 1024
flashfs[1]: Bytes available: 3611648
flashfs[1]: flashfs fsck took 3 seconds.
Format of flash: complete
Switch#
Switch#
Switch#
Switch#dir flash:
Directory of flash:/

No files in directory

3612672 bytes total (3611648 bytes free)
Switch#
```

2

Operating Cisco IOS Software

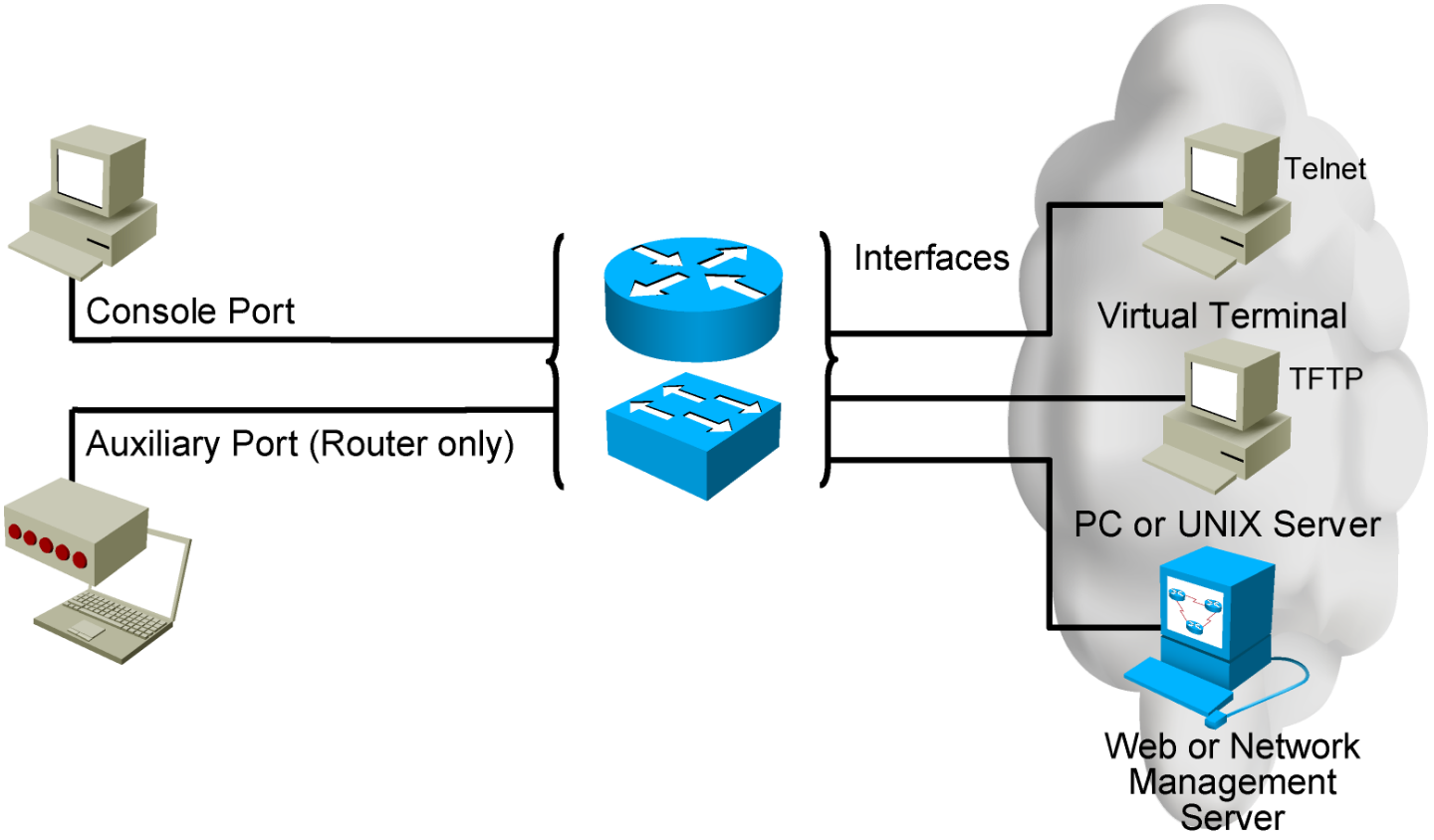
Cisco IOS
Configuration Register

- Boot via ROM monitor
- Select a file to boot
- Enable / disable Break
- Setting console terminal baud rate
- Load IOS from ROM
- Boot from TFTP server

Operating Cisco IOS Software

Cisco IOS

External Configuration Sources



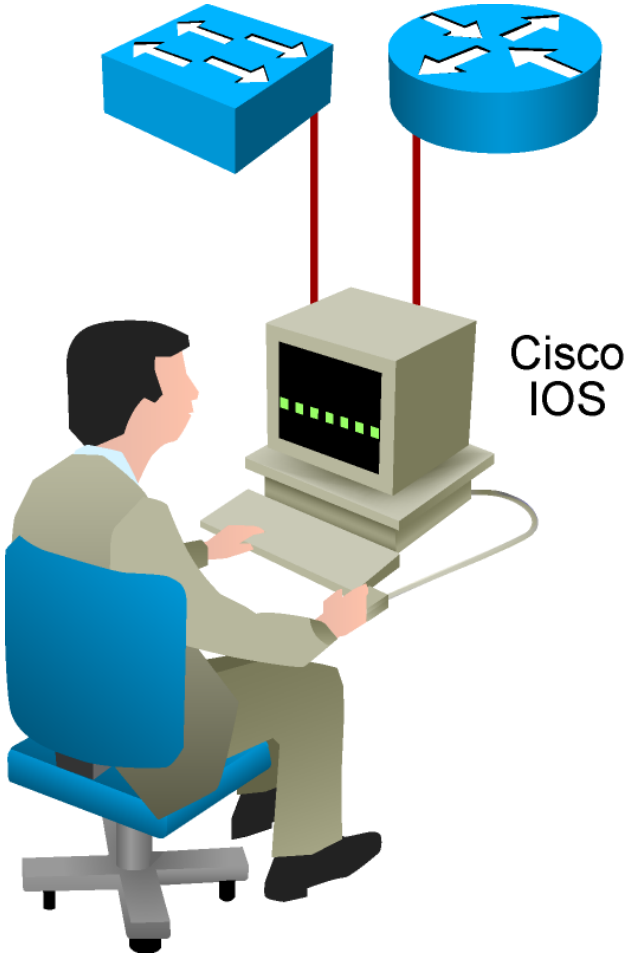
- Configurations can come from many sources.
- Configurations will act in device memory.

Operating Cisco IOS Software

Cisco IOS

Cisco IOS User Interface Functions

- CLI is used to enter commands.
- Operations vary on different internetworking devices.
- Users type or paste entries in the console command modes.
- Command modes have distinctive prompts.
- Enter key instructs device to parse and execute the command.
- Two primary EXEC modes are user mode and privileged mode.



Operating Cisco IOS Software

Cisco IOS

Cisco IOS Software EXEC Mode (User)

There are two main EXEC modes for entering commands.

First Mode

User Mode

- Limited examination of switch or router
- Command prompt: hostname>

Operating Cisco IOS Software

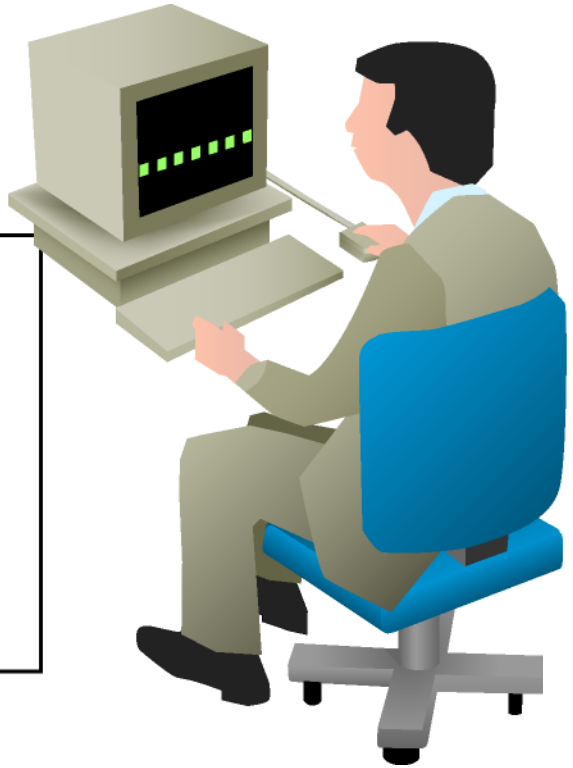
Cisco IOS

Cisco IOS Software EXEC Mode (Privileged)

Second Mode (and Most Commonly Used)

Privileged (aka Enabled) Mode

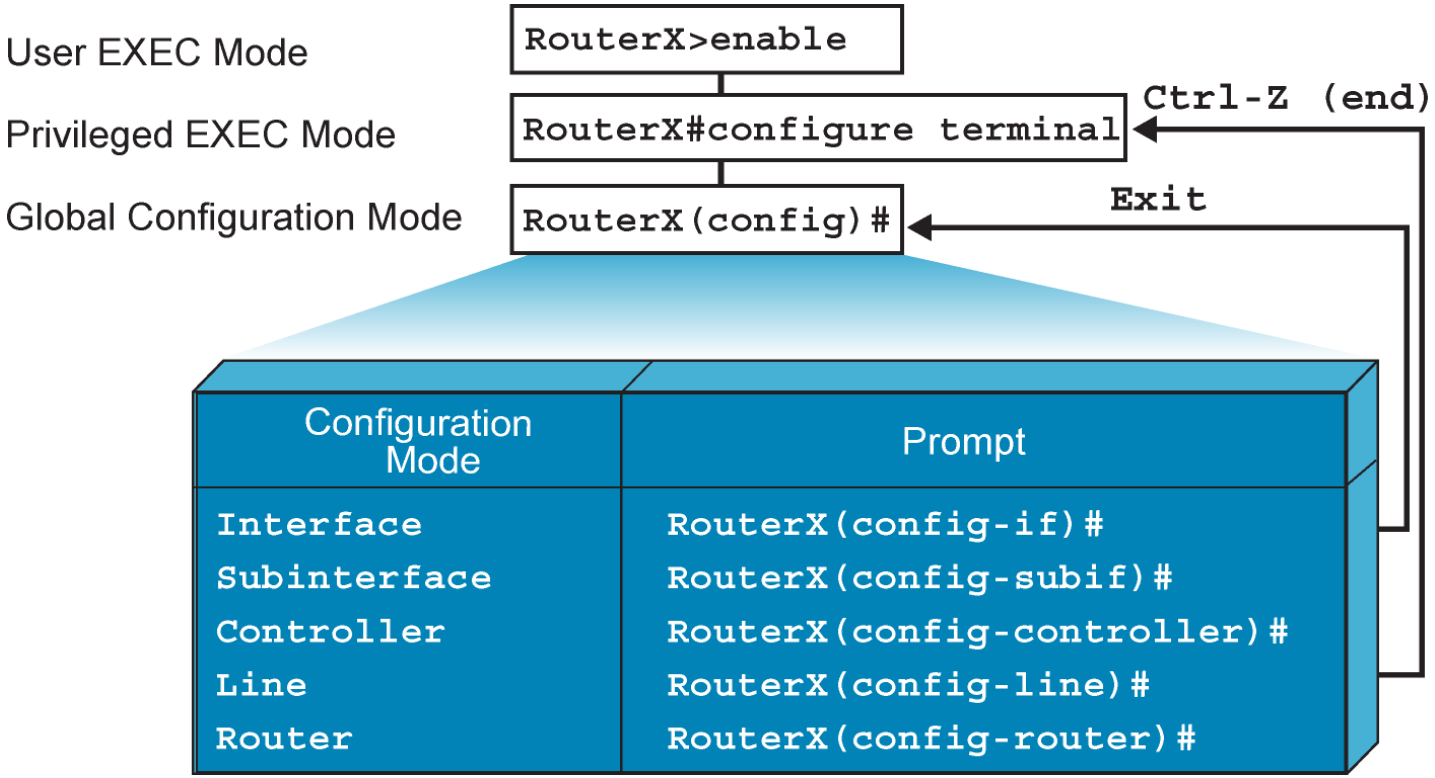
- Detailed examination of switch or router
- Enables configuration and debugging
- Prerequisite for other configuration modes
- Command prompt: hostname#



Operating Cisco IOS Software

Cisco IOS

Overview of Cisco IOS Configuration Modes



Operating Cisco IOS Software

Cisco IOS
Switch Command-Line Help Facilities

Context-Sensitive Help

Provides a list of commands and the arguments associated with a specific command.

Console Error Messages

Identifies problems with any switch commands that are incorrectly entered so that they can be altered or corrected.

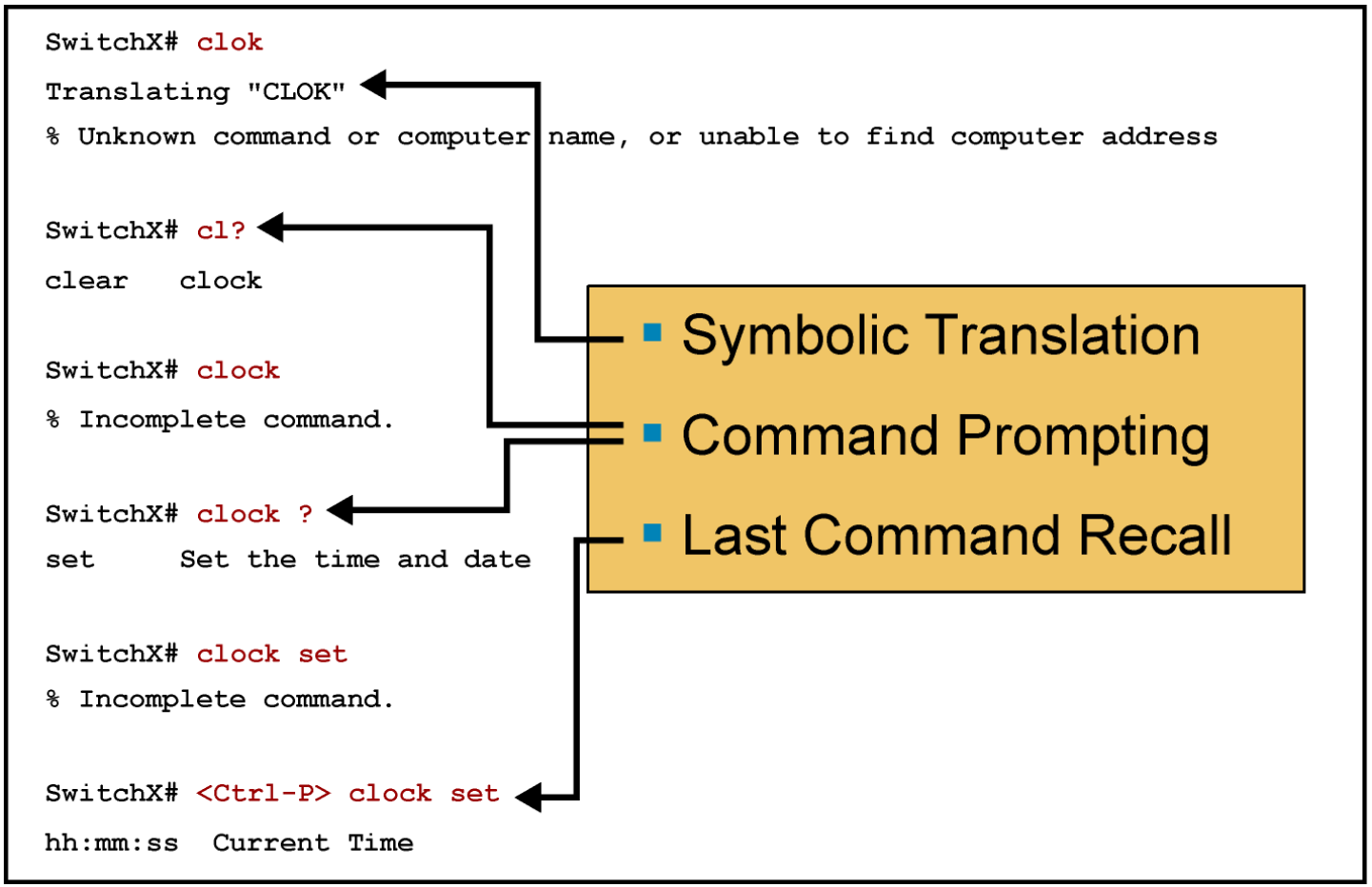
Command History Buffer

Allows recall of long or complex commands or entries for re-entry, review, or correction.

Operating Cisco IOS Software

Cisco IOS

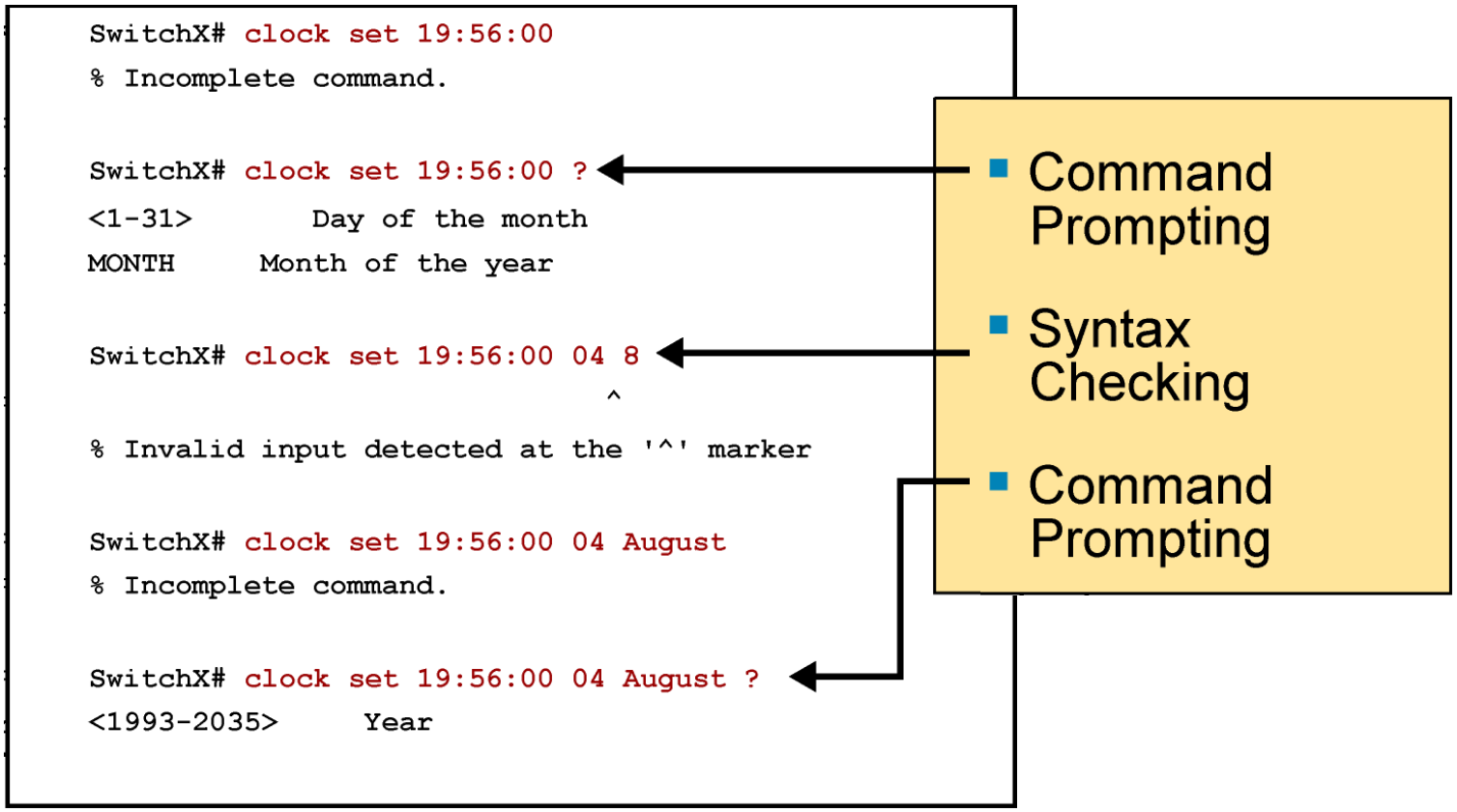
Context-Sensitive Help



Operating Cisco IOS Software

Cisco IOS

Context-Sensitive Help (Cont.)



Operating Cisco IOS Software

Cisco IOS

Enhanced Editing Commands

	(Automatic scrolling of long lines)
Ctrl-A	Move to the beginning of the command line.
Ctrl-E	Move to the end of the command line.
Esc-B	Move back one word.
Esc-F	Move forward one word.
Ctrl-B	Move back one character.
Ctrl-F	Move forward one character.
Ctrl-D	Delete a single character.

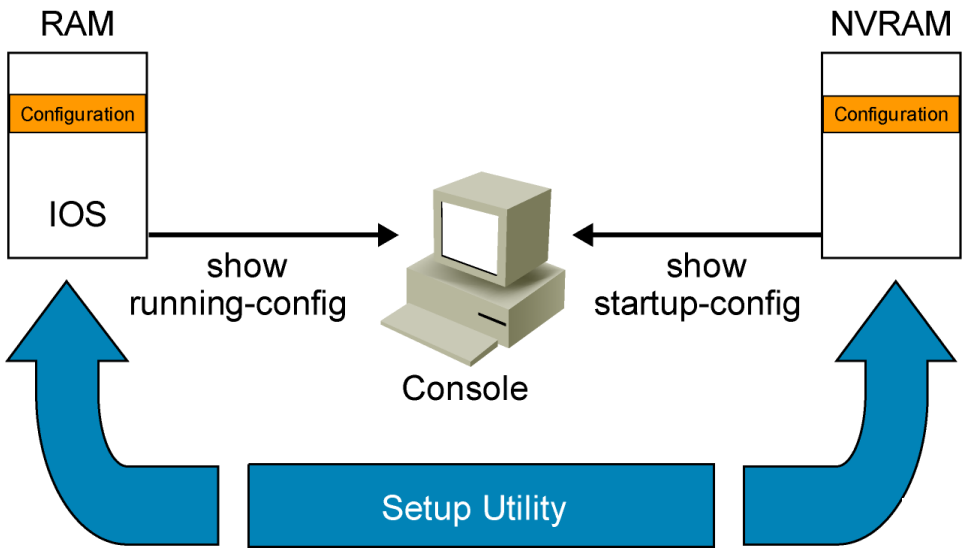
Router Command History

Ctrl-P or Up Arrow	**Recalls last (previous) commands.**
Ctrl-N or Down Arrow	**Recalls more recent commands.**
`show history`	**Shows command buffer contents.**
`terminal history size` *`lines`*	**Sets session command buffer size.**

Operating Cisco IOS Software

Cisco IOS

Viewing the Configuration



show running-config and show startup-config Commands

In RAM

```
SwitchX#show running-config
Building configuration...??
Current configuration:?
!?
version 12.0
!
 -- More --
```

In NVRAM

```
SwitchX#show startup-config
Using 1359 out of 32762 bytes
!
version 12.0
!
 -- More --
```

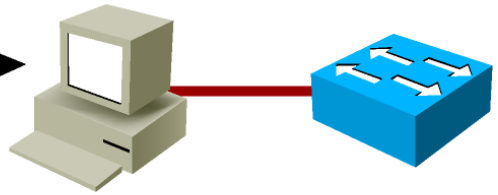
Operating Cisco IOS Software

Cisco IOS

Configuring a Switch Password

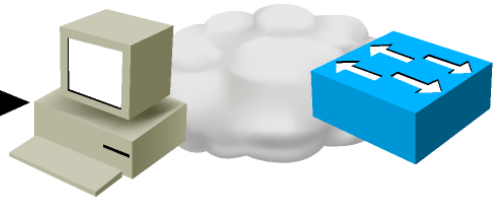
Console Password

```
SwitchX(config)#line console 0
SwitchX(config-line)#login
SwitchX(config-line)#password cisco
```



Virtual Terminal Password

```
SwitchX(config)#line vty 0 4
SwitchX(config-line)#login
SwitchX(config-line)#password sanjose
```



Enable Password

```
SwitchX(config)#enable password cisco
```

Secret Password

```
SwitchX(config)#enable secret sanfran
```

Service Password-Encryption Commands

```
SwitchX(config)#service password-encryption
SwitchX(config)#no service password-encryption
```

Operating Cisco IOS Software

Cisco IOS

Telnet vs. SSH Access

- Telnet
  - Most common access method
  - Insecure
- SSH-encrypted

```
!- The username command create the username and password for the SSH session
Username cisco password  cisco

ip domain-name mydomain.com

crypto key generate rsa

ip ssh version 2

line vty 0 4
   login local
   transport input ssh
```

Summary

Conclusion

Managing Cisco IOS

- CDP
- LLDP
- NTP
- Component of Cisco Router
- Boot procedure of Cisco Router
- Switch
- Router
- Virtual terminal

Thank you.

Songyut Phoemphon

Email: songyut@sut.ac.th