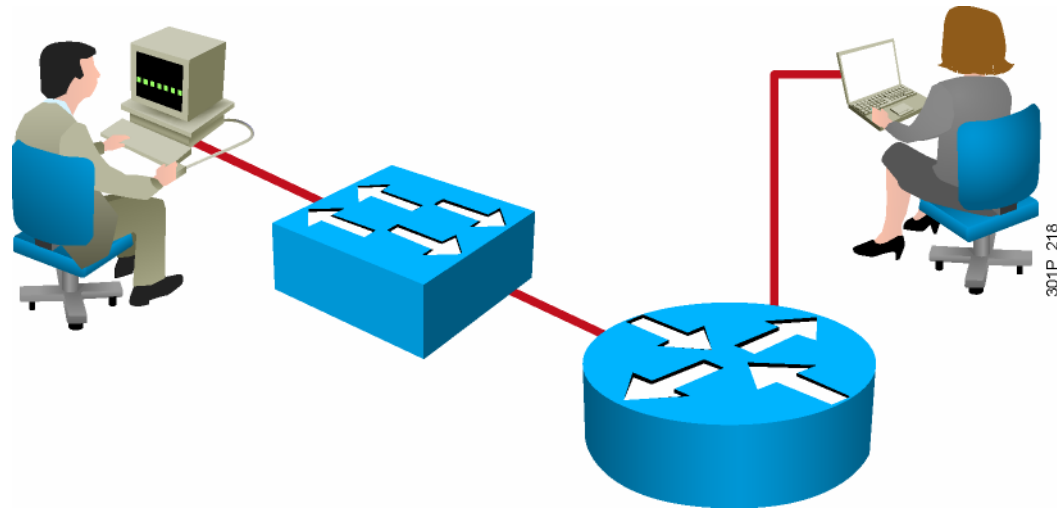# Operating Cisco IOS Software

Ethernet LANs

Cisco IOS Software

- Features to carry the chosen network protocols and functions
- Connectivity for high-speed traffic between devices
- Security to control access and prohibit unauthorized network use
- Scalability to add interfaces and capability as needed for network growth
- Reliability to ensure dependable access to networked resources

Configuring Network Devices

- Initial default settings are sufficient for the switch to operate at Layer 2 as a switch.

- A Cisco device will prompt for initial configuration if there is no configuration in memory.

- Additional configuration tasks set up the device with the following:

  - Protocol addressing and parameter settings
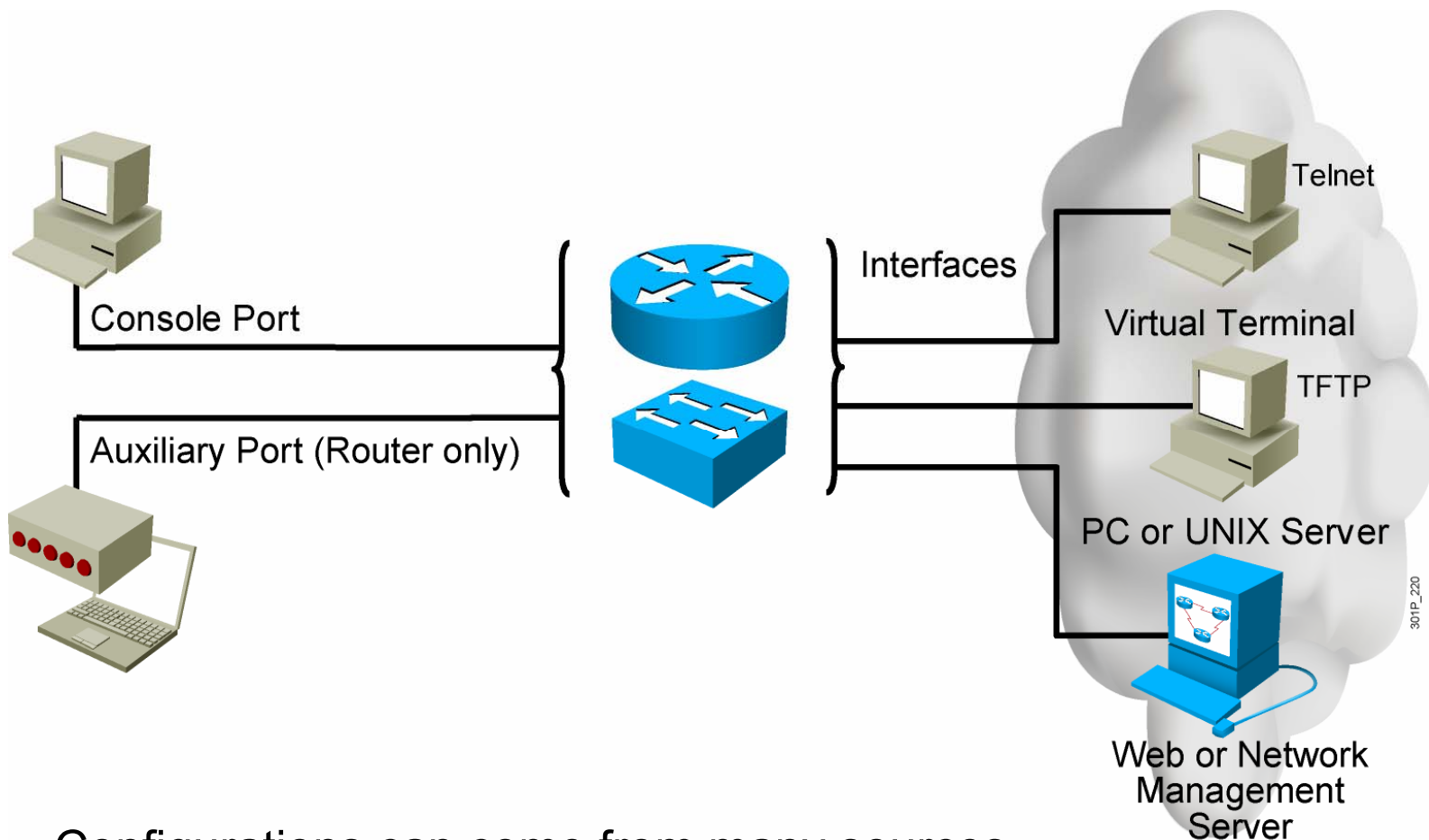
  - Options for administration and management

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.
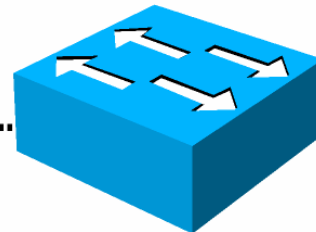
301P_219

External Configuration Sources

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

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.
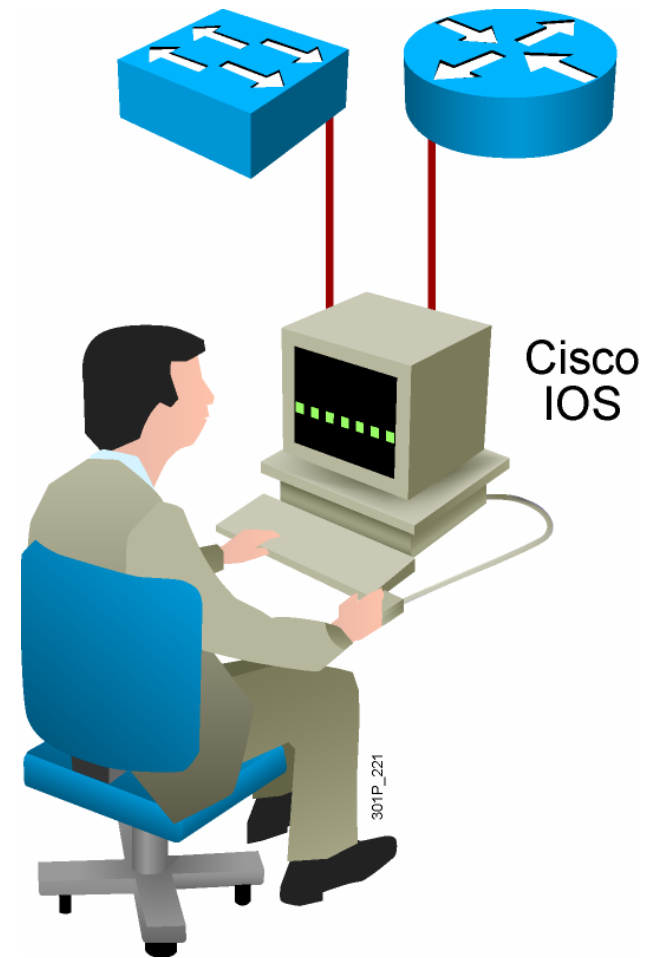
Cisco IOS

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
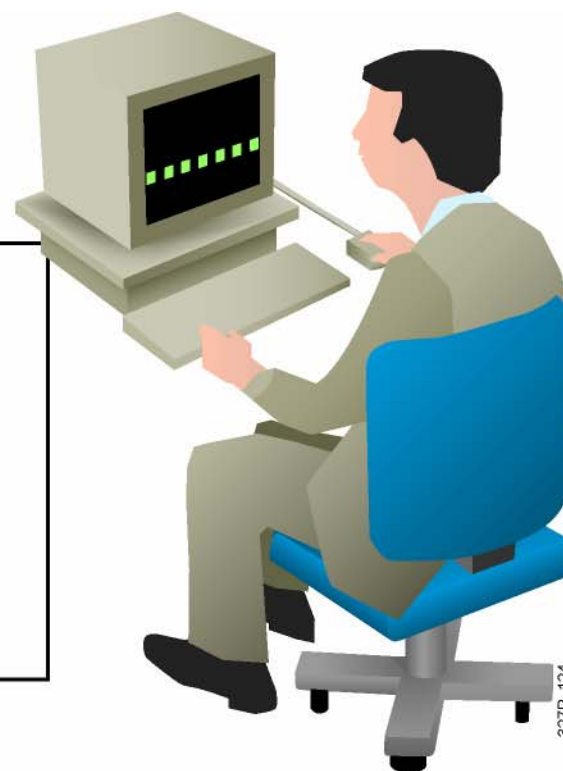- Command prompt: hostname>

301P_222

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#

327P_124

Switch Command-Line Help Facilities

Context-Sensitive Help

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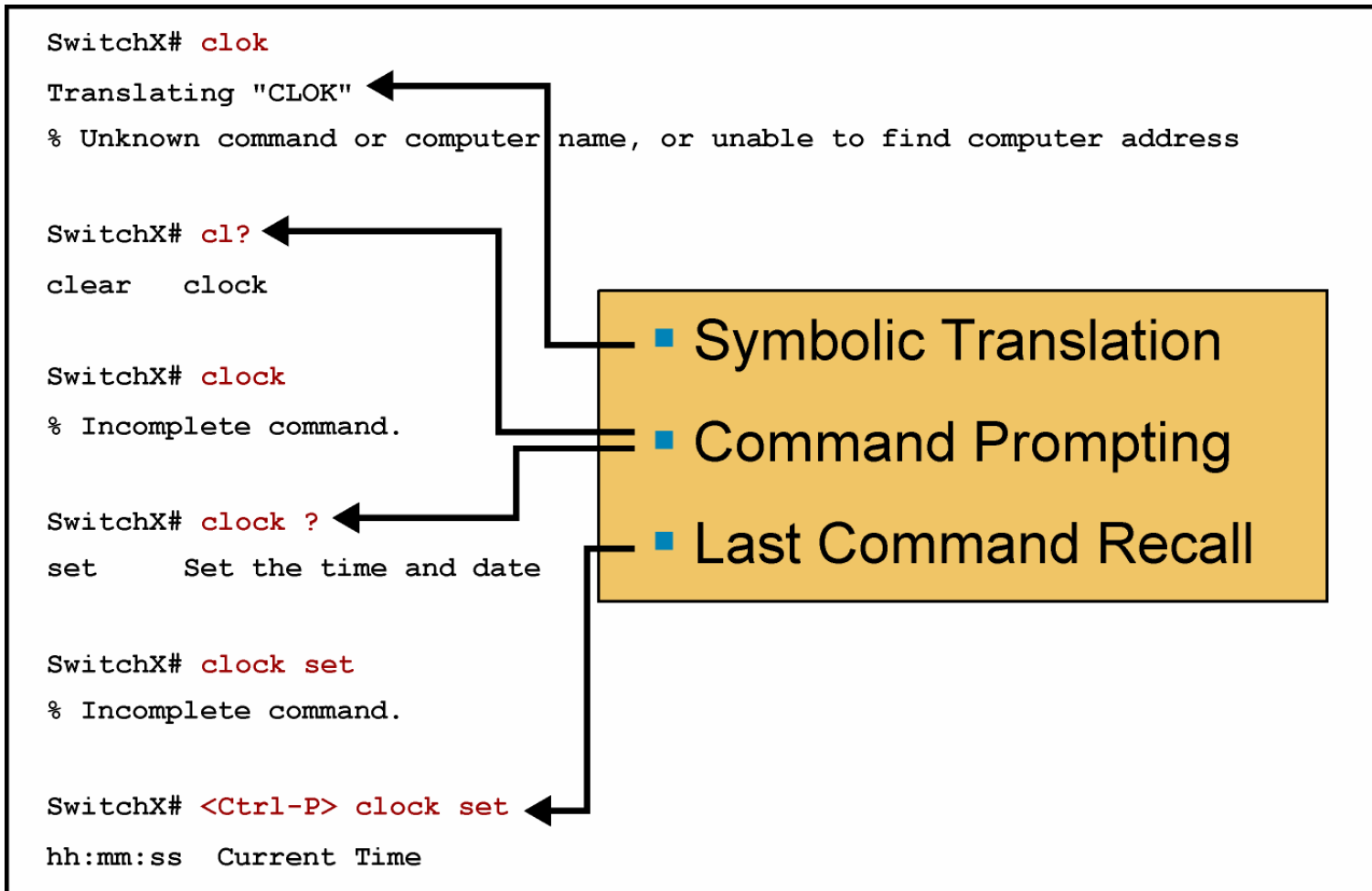
Console Error Messages

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.

301P_949

Context-Sensitive Help

```
SwitchX# clok

Translating "CLOK"

% Unknown command or computer name, or unable to find computer address


SwitchX# cl?

clear    clock


SwitchX# clock

% Incomplete command.


SwitchX# clock ?

set      Set the time and date


SwitchX# clock set

% Incomplete command.


SwitchX# <Ctrl-P> clock set

hh:mm:ss  Current Time
```

- ▪ Symbolic Translation
- ▪ Command Prompting
- ▪ Last Command Recall

301P_992

ICND1 v1.0—2-10

Context-Sensitive Help (Cont.)

```
SwitchX# clok

Translating "CLOK"

% Unk
           SwitchX# clock set 19:56:00

Switc       % Incomplete command.

clear       SwitchX# clock set 19:56:00 ?              ◄──────  ■ Command
            <1-31>        Day of the month                       Prompting
Switc       MONTH       Month of the year
% Inc
            SwitchX# clock set 19:56:00 04 8           ◄──────  ■ Syntax
Switc                              ^                              Checking
set         % Invalid input detected at the '^' marker

Switc       SwitchX# clock set 19:56:00 04 August      ┌──────  ■ Command
% Inc       % Incomplete command.                      │         Prompting

Switc       SwitchX# clock set 19:56:00 04 August ?    ◄─┘
hh:m        <1993-2035>    Year
```

Enhanced Editing Commands

```
SwitchX>Shape the future of internetworking by creating unpreced
```

Shape the future of internetworking by creating unprecedented value for customers, employees, and partners.

Enhanced Editing Commands (Cont.)

```
SwitchX>$ value for customers, employees, and partners.
```

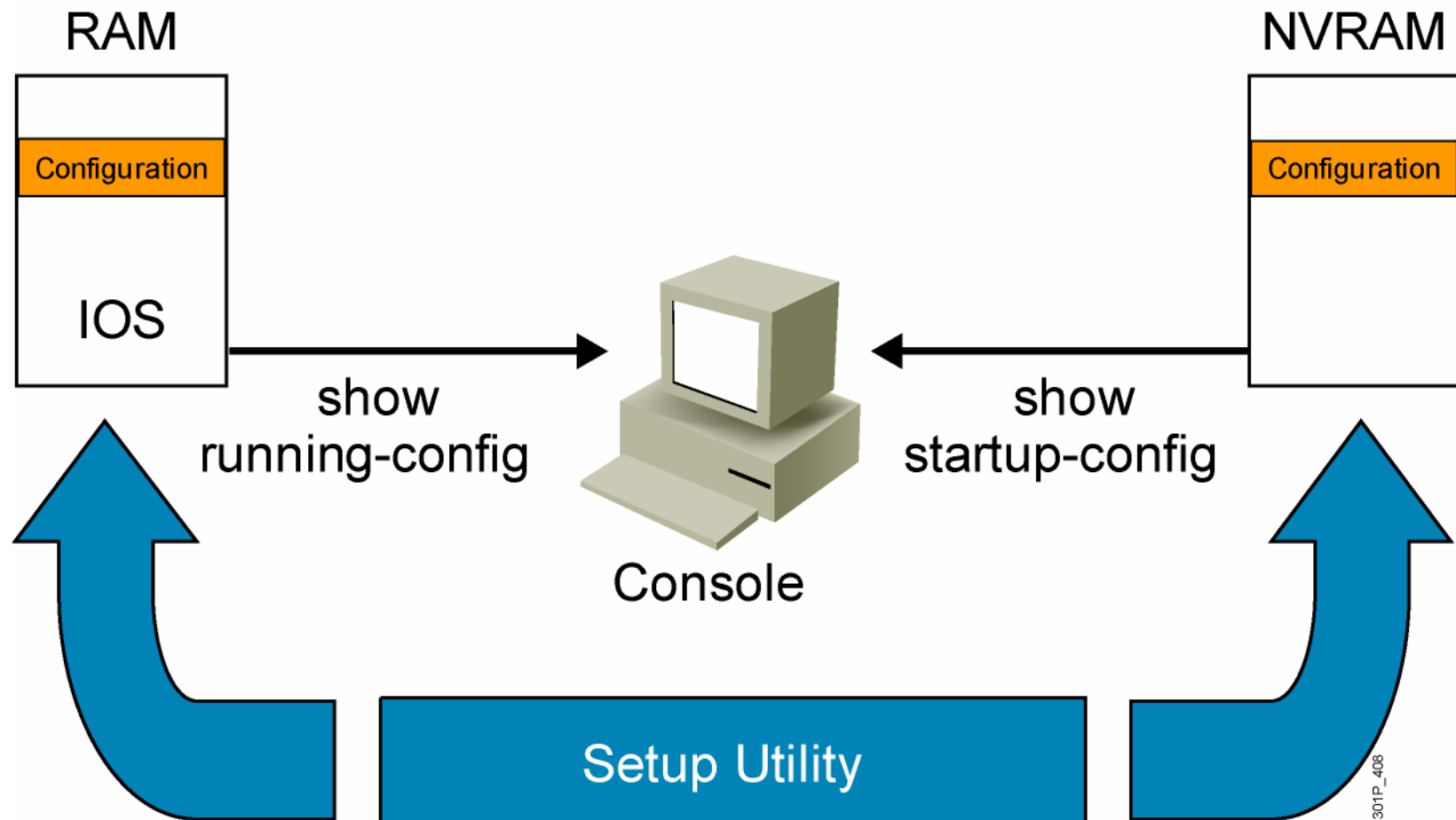|	(Automatic scrolling of long lines)
Ctrl-A	Move to the beginning of the command line.
Ctrl-E	Move to the end of the command line.
Esc-B	Move back one word.
Esc-F	Move forward one word.
Ctrl-B	Move back one character.
Ctrl-F	Move forward one character.
Ctrl-D	Delete a single character.

301P_990

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.**

022P_249

Viewing the Configuration

RAM

Configuration

IOS

NVRAM

Configuration

show
running-config

show
startup-config

Console

Setup Utility

301P_408

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 --
```

Displays the current and saved configuration

301P_987

Summary

- Cisco IOS software is the embedded software architecture in all Cisco IOS devices and is also the operating system of Catalyst switches. Its functions include carrying the chosen network protocols, connectivity, security, scalability, and reliability.

- A switch or IOS device can be configured from a local terminal connected to the console port or from a remote terminal connected via a modem connection to the auxiliary port.

- The CLI is used by network administrators to monitor and configure various Cisco IOS devices. CLI also offers a help facility to aid network administrators with the verification and configuration commands.

Summary (Cont.)

- The CLI supports two EXEC modes: user and privileged. The privileged EXEC mode provides more functionality than the user EXEC mode.

- The Cisco IOS devices uses Cisco IOS software with extensive command-line input help facilities, including context-sensitive help.

- The Cisco IOS CLI includes an enhanced editing mode that provides a set of editing key functions.

- The Cisco IOS devices CLI provides a history or record of commands that have been entered. This feature, called the command history, is particularly useful to help recall long or complex commands or entries.

Starting a Switch

Ethernet LANs

Initial Startup of the Catalyst Switch

- System startup routines initiate switch software.
- Initial startup uses default configuration parameters.

1. Before you start the switch, verify the cabling and console connection.
2. Attach the power cable plug to the switch power supply socket.
3. Observe the boot sequence:
   - LEDs on the switch chassis
   - Cisco IOS software output text

301P_224
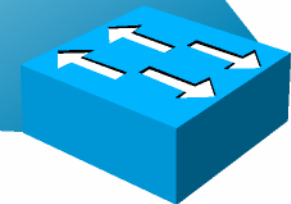
Catalyst 2960 Switch LED Indicators
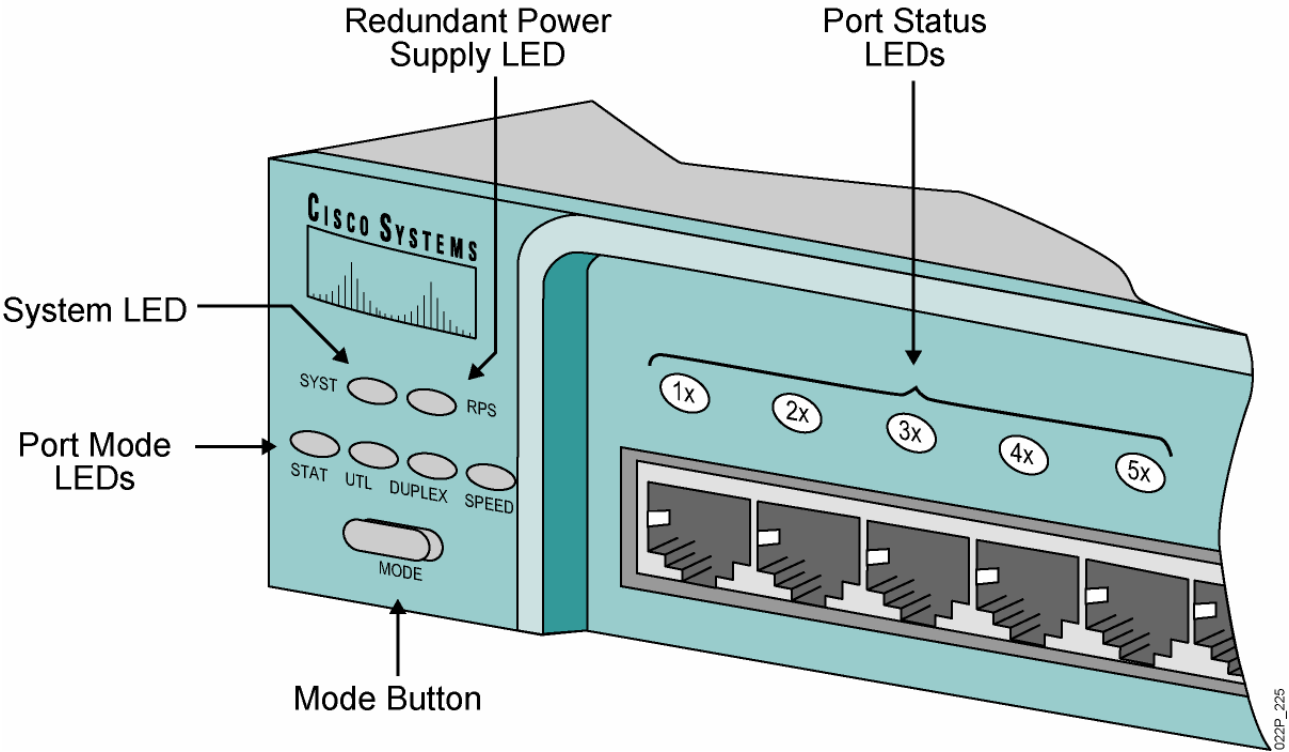
Initial Bootup Output from the Catalyst 2960 Switch

```
Base ethernet MAC Address: 00:19:30:38:bd:00
Xmodem file system is available.
The password-recovery mechanism is enabled.
Initializing Flash...
flashfs[0]: 598 files, 19 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 8210432
flashfs[0]: Bytes available: 24303616
flashfs[0]: flashfs fsck took 9 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
done.
Loading "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9
-mz.122-25.SEE2.bin"...@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@
File "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.
122-25.SEE2.bin" uncompressed and installed, entry point: 0x3000
executing...

!Rest of startup text omitted
```

Console Connection

301P_226
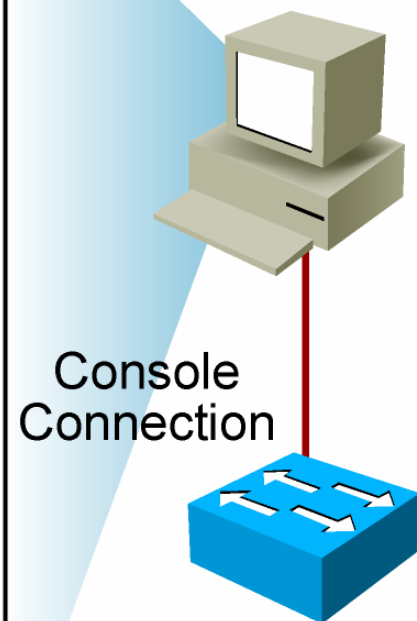
Initial Configuration of the Catalyst 2960 Switch Using Setup

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: no
First, would you like to see the current interface summary? [yes]:
no
Configuring global parameters:
..
..text omitted ..
..
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this
configuration.
```
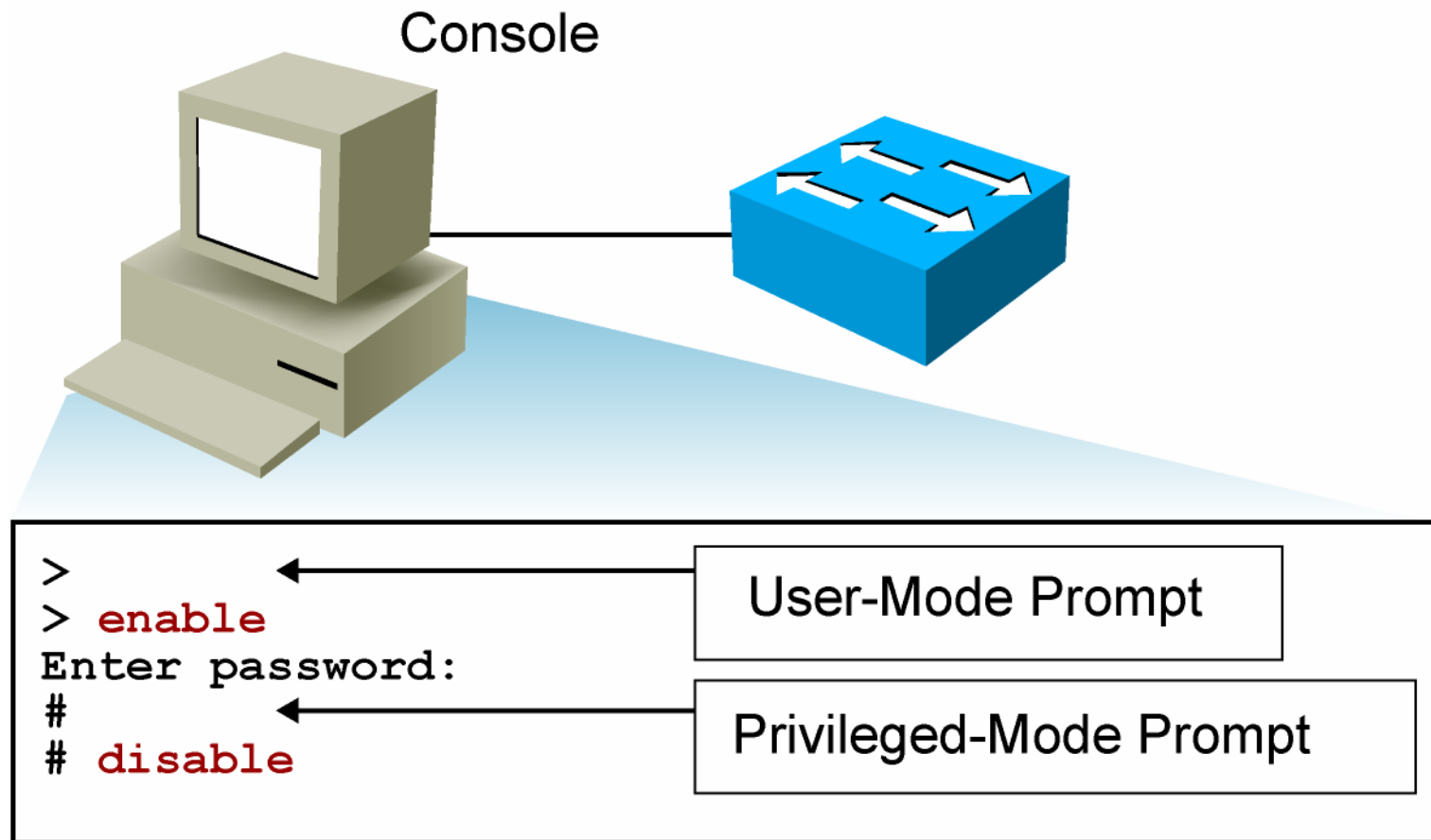
022P_227

Logging In to the Switch and Entering the Privileged EXEC Mode

Console

```
>
> enable
Enter password:
#
# disable
```

User-Mode Prompt

Privileged-Mode Prompt

301P_228

Configuring the Switch

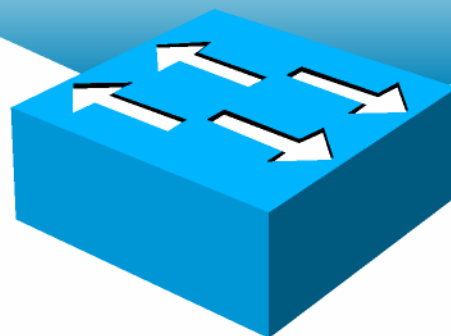

Configuration modes:

- Global configuration mode
  - `SwitchX#configure terminal`
  - `SwitchX(config)#`
- Interface configuration mode
  - `SwitchX(config)#interface fa0/1`
  - `SwitchX(config-if)#`

Configuring Switch Identification

Switch Name

```
(config)#hostname SwitchX
SwitchX(config)#
```

Sets the local identity for the switch

Configuring the Switch IP Address

```
SwitchX(config)#interface vlan 1
SwitchX(config-if)#ip address {ip address} {mask}
```

Example:

```
SwitchX(config)#interface vlan 1
SwitchX(config-if)#ip address 10.5.5.11 255.255.255.0
SwitchX(config-if)#no shutdown
```

Note: It is necessary to use the **no shutdown** command to make the interface operational.

Configuring the Switch Default Gateway

fa 0/1 172.20.137.1

Default Gateway

301P_948

```
SwitchX(config)#ip default-gateway {ip address}
```

Example:

```
SwitchX(config)#ip default-gateway 172.20.137.1
```

Saving Configurations

```
SwitchX

SwitchX copy running-config startup-config

Destination filename [startup-config]?

Building configuration…


SwitchX
```

Copies the current configuration to NVRAM

Showing Switch Initial Startup Status

```
SwitchX#show version
```

- Displays the configuration of the system hardware, software version, names and sources of configuration files, and boot images

```
SwitchX#show running-config
```

- Displays the current active configuration file of the switch

```
SwitchX#show interfaces
```

- Displays statistics for all interfaces configured on the switch

Switch show version Command

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE

SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh
Image text-base: 0x00003000, data-base: 0x00BB7944

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE SOFTWARE (fc1)

Switch uptime is 24 minutes

System returned to ROM by power-on
System image file is "flash:c2960-lanbasek9-mz.122-25.SEE2/c2960-lanbasek9-mz.122-
25.SEE2.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 61440K/4088K bytes of
memory.

Processor board ID FOC1052W3XC
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

! Text omitted

Switch#
```

Switch show interfaces Command

```
SwitchX#show interfaces FastEthernet0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0008.a445.ce82 (bia 0008.a445.ce82)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 4w6d, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     182979 packets input, 16802150 bytes, 0 no buffer
     Received 49954 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 8 ignored
     0 watchdog, 20115 multicast, 0 pause input
     0 input packets with dribble condition detected
     3747473 packets output, 353656347 bytes, 0 underruns
  --More--
```

Managing the MAC Address Table

Catalyst 2960 Series

```
SwitchX#show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type        Ports
----      -----------         --------    -----
 All      0008.a445.9b40      STATIC      CPU
 All      0100.0ccc.cccc      STATIC      CPU
 All      0100.0ccc.cccd      STATIC      CPU
 All      0100.0cdd.dddd      STATIC      CPU
   1      0008.e3e8.0440      DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 5
SwitchX#
```

Summary

- The startup of a Cisco IOS switch requires verifying the physical installation, powering up the switch, and viewing the Cisco IOS software output on the console.

- Cisco IOS switches have several status LEDs that are generally green when the switch is functioning normally but turn amber when there is a malfunction.

- The Cisco Catalyst POST is executed only when the switch is powered up.

- During initial startup, if POST test failures are detected, they are reported to the console. If POST completes successfully, the switch can be configured.

Summary (Cont.)

- When starting any mode on a Cisco IOS switch, begin in user EXEC mode. To change modes, a password must be entered.

- The Catalyst IOS switches can be configured using the global and other configuration modes, similar to the routers.

- Configure a Cisco IOS switch from the command line to add the host name and IP addressing.

- After logging into a Catalyst switch, the switch software and hardware status can be verified using **show version**, **show running-config**, and **show interfaces** commands.
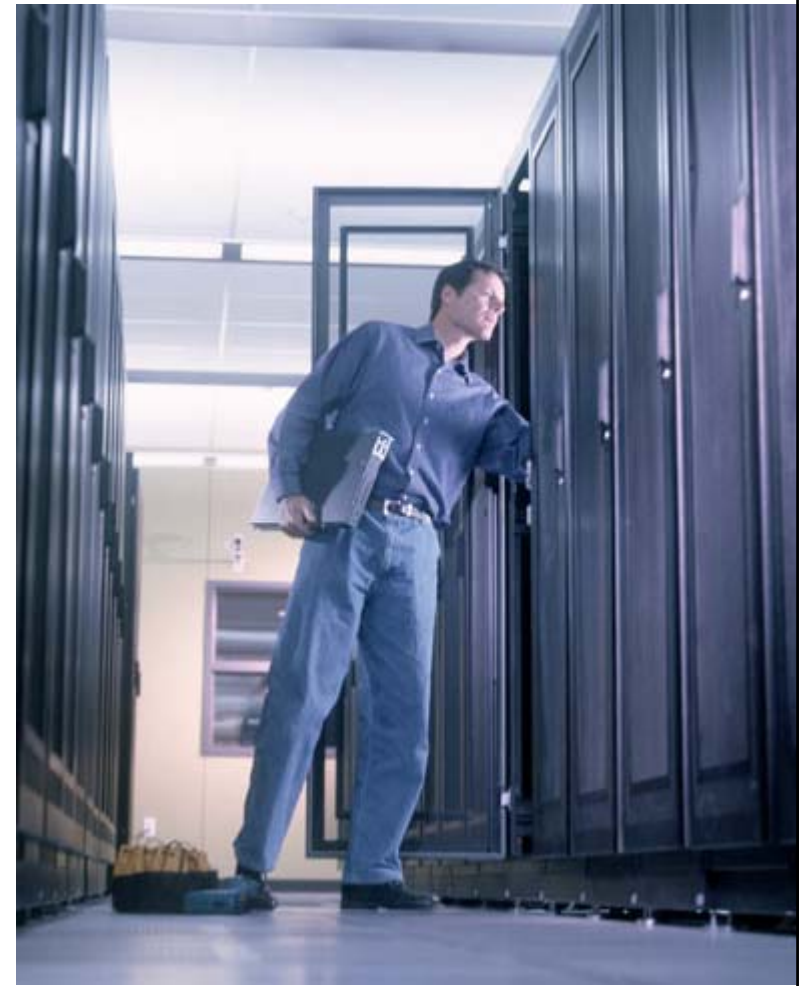
Understanding Switch Security

Ethernet LANs

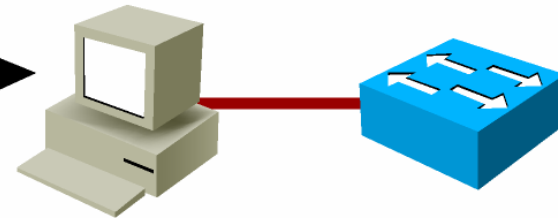# Common Threats to Physical Installations

- Hardware threats

- Environmental threats

- Electrical threats

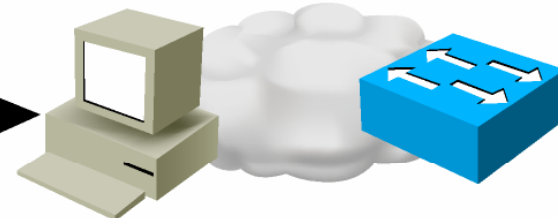- Maintenance threats

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
```

301P_256

Configuring the Login Banner

- Defines and enables a customized banner to be displayed before the username and password login prompts.

```
SwitchX# banner login " Access for authorized users only. Please enter your username and password. "
```
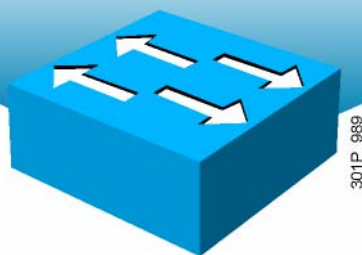
Telnet vs. SSH Access

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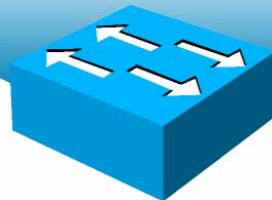 - Insecure
- SSH-encrypted

```
!- 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
```

Configuring Port Security

Cisco Catalyst 2960 Series

```
SwitchX(config-if)#switchport port-security [  mac-address
mac-address | mac-address sticky [mac-address] | maximum
value | violation {restrict | shutdown}]
```

```
SwitchX(config)#interface fa0/5
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport port-security
SwitchX(config-if)#switchport port-security maximum 1
SwitchX(config-if)#switchport port-security mac-address sticky
SwitchX(config-if)#switchport port-security violation shutdown
```

Verifying Port Security on the Catalyst 2960 Series

```
SwitchX#show port-security [interface interface-id] [address] [ |
{begin | exclude | include} expression]
```

```
SwitchX#show port-security interface fastethernet 0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 20 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address        : 0000.0000.0000
Security Violation Count   : 0
```

Verifying Port Security on the Catalyst 2960 Series (Cont.)

```
SwitchX#sh port-security address
        Secure Mac Address Table
-------------------------------------------------------------------
Vlan      Mac Address       Type                    Ports   Remaining Age
                                                            (mins)

----      ----------        ----                    -----   ------------
 1        0008.dddd.eeee    SecureConfigured        Fa0/5        -
-------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
SwitchX#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)        (Count)        (Count)
-----------------------------------------------------------------------
      Fa0/5       1              1               0            Shutdown
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Securing Unused Ports

- Unsecured ports can create a security hole.

- A switch plugged into an unused port will be added to the network.

- Secure unused ports by disabling interfaces (ports).

Disabling an Interface (Port)

```
SwitchX(config-int)#
```

```
shutdown
```

- To disable an interface, use the **shutdown** command in interface configuration mode.
- To restart a disabled interface, use the **no** form of this command.

Summary

- The first level of security is physical.

- Passwords can be used to limit access to users that have been given the password.

- The login banner can be used to display a message before the user is prompted for a username.

- Telnet sends session traffic in cleartext; SSH encrypts the session traffic.

- Port security can be used to limit MAC addresses to a port.
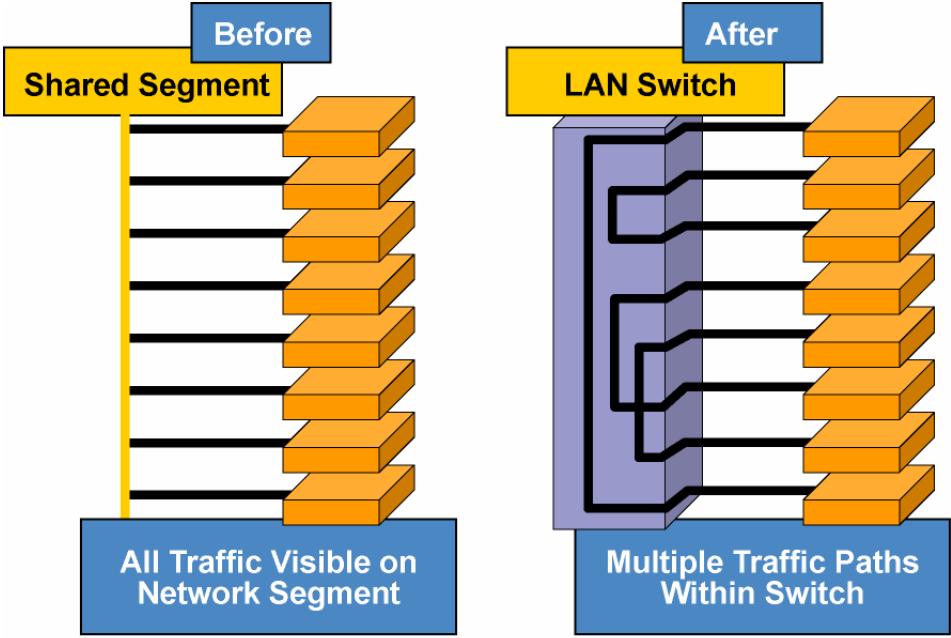
- Unused ports should be shut down.

Maximizing the Benefits of Switching

Ethernet LANs

Microsegmentation

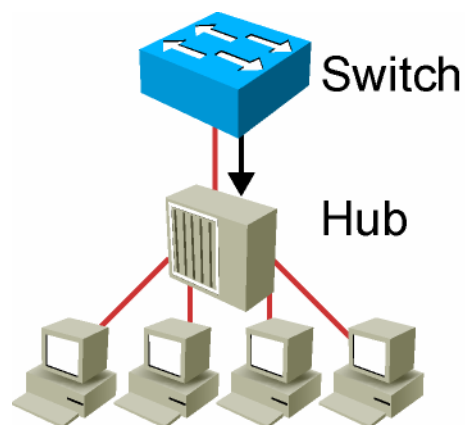## Microsegmentation of the Network

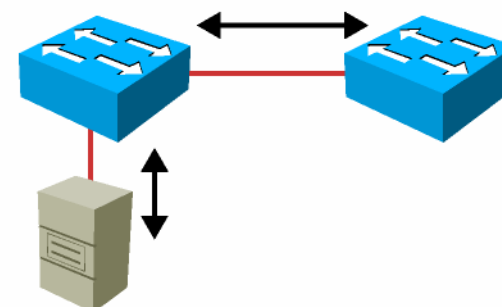Dedicated paths between sender and receiver hosts

Duplex Overview

Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity

Full Duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled

301P_126

Setting Duplex and Speed Options

Cisco Catalyst 2960 Series

```
SwitchX(config)#interface fa0/1
SwitchX(config-if)#duplex {auto | full | half}
```

Cisco Catalyst 2960 Series

```
SwitchX(config)#interface fa0/1
SwitchX(config-if)#speed {10 | 100 | 1000 | auto}
```
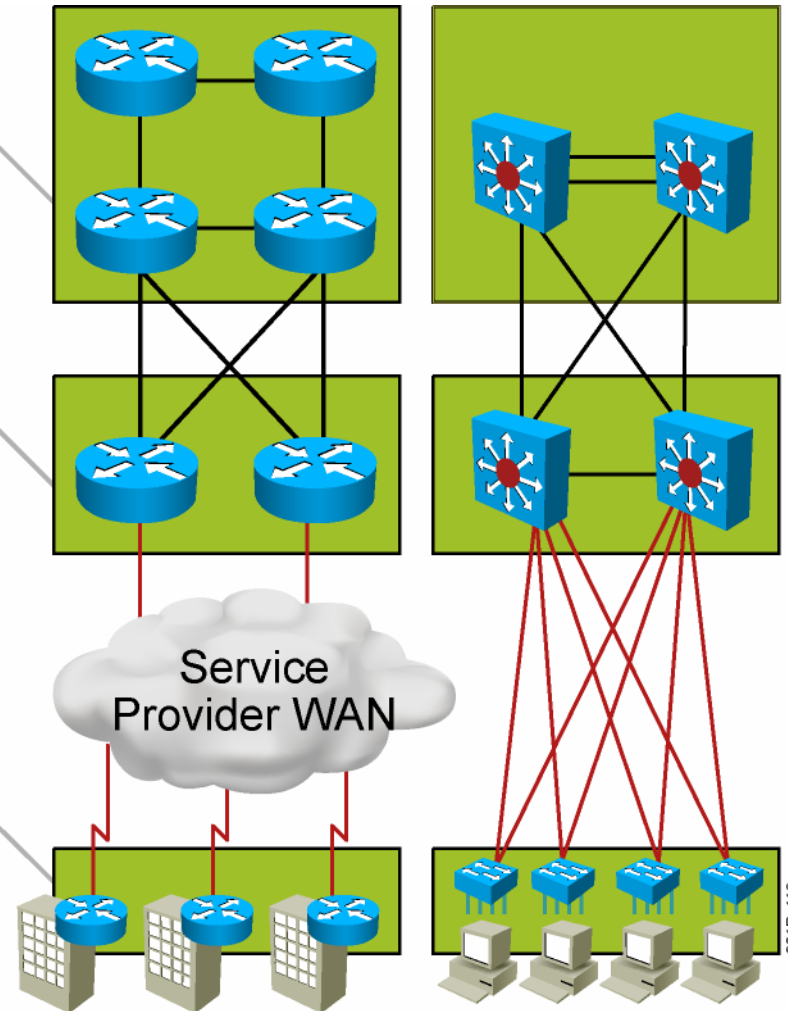
Showing Duplex Options

```
SwitchX#show interfaces fastethernet0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0008.a445.9b42 (bia 0008.a445.9b42)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:57, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     323479 packets input, 44931071 bytes, 0 no buffer
     Received 98960 broadcasts (0 multicast)
     1 runts, 0 giants, 0 throttles
     1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 36374 multicast, 0 pause input
     0 input packets with dribble condition detected
     1284934 packets output, 103121707 bytes, 0 underruns
     0 output errors, 2 collisions, 6 interface resets
     0 babbles, 0 late collision, 29 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```
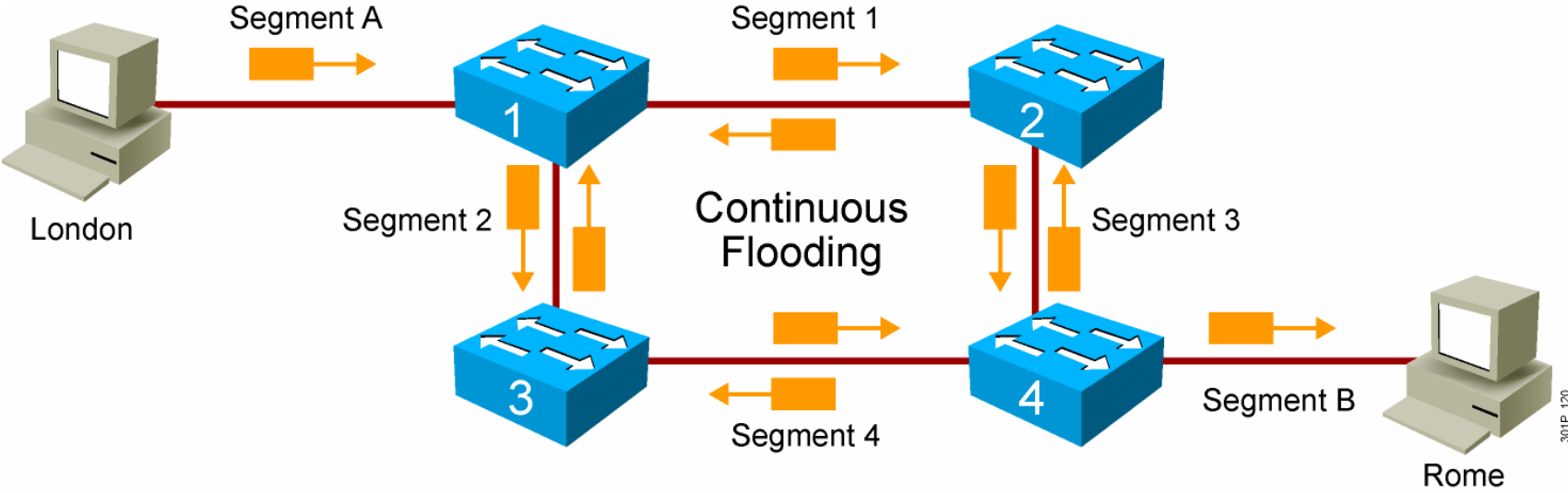
The Hierarchy of Connectivity

Core layer: Provides optimal transport between core routers and distribution sites

Distribution layer: Provides policy-based connectivity, ? peer reduction, and aggregation

Access layer: Provides common group access to the internetworking environment

Service Provider WAN

ICND1 v1.0—2-6

301P_118

Loops

Spanning Tree Protocol

One switch is elected the root based on lowest bridge ID (priority and MAC address concatenated).

A tree-like, loop-free topology is established.

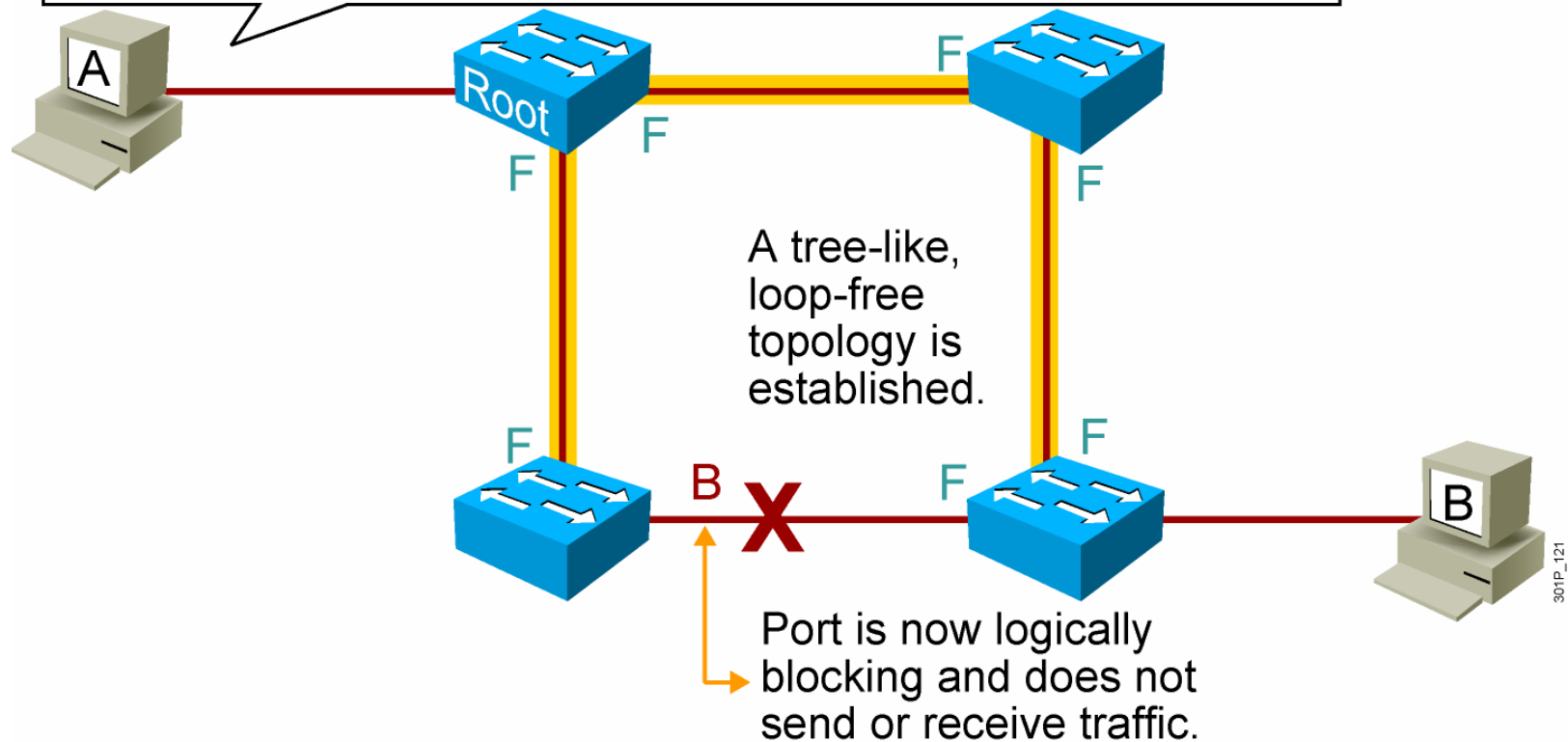Port is now logically blocking and does not send or receive traffic.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual self-study.

Summary

- Switched LANs provide microsegmentation, which means that each device on a network segment is connected directly to a switch port and receives its own bandwidth; each device does not have to contend for bandwidth with any other device on the network.

- Half-duplex communication in an Ethernet LAN allows data transmission in only one direction at a time (either sending or receiving); full-duplex communication allows both sending and receiving of data simultaneously. Switches provide full-duplex communication capability.

- Employing a hierarchy of Ethernet connectivity is usually the most efficient way to provide speed where it will be most effective in a campus network, implementing Fast Ethernet and Gigabit Ethernet primarily in workgroup and backbone connections.

Summary (Cont.)

- Loops result when switches connected to the same segment transmit the same data. The data frames circulate between the two paths without being removed from the network and may cause inaccurate data in the MAC address tables.

- The solution to loops is STP, which manages the paths to given network segments. STP provides path redundancy in an Ethernet LAN while preventing undesirable active loops in the network.