Chapter 2: Configure a Network Operating System
Chapter Outline

2.0 Introduction
2.1 IOS Bootcamp
2.2 Basic Device Configuration
2.3 Address Schemes
2.4 Summary
Section 2.1: IOS Bootcamp

Upon completion of this section, you should be able to:

• Explain the purpose of Cisco IOS.
• Explain how to access a Cisco IOS device for configuration purposes.
• Explain how to navigate Cisco IOS to configure network devices.
• Describe the command structure of Cisco IOS software.
Topic 2.1.1: Cisco IOS
Operating Systems

Shell: The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.

Kernel: Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.

Hardware: The physical part of a computer including underlying electronics.
Purpose of OS

• PC operating systems enable a user to:
  • Use a mouse to make selections and run programs.
  • Enter text and text-based commands.
  • View output on a monitor.

• Cisco IOS enables a network technician to:
  • Use a keyboard to run CLI-based network programs.
  • Use a keyboard to enter text and text-based commands.
  • View output on a monitor.

• All networking devices come with a default IOS.

• It is possible to upgrade the IOS version or feature set.
Topic 2.1.2: Cisco IOS Access
Access Methods

Console

The advantage of using a console port is that the device is accessible even if no networking services have been configured, such as when performing an initial configuration of the networking device. When performing an initial configuration, a computer running terminal emulation software is connected to the console port of the device using a special cable. Configuration commands for setting up the switch or router can be entered on the connected computer.

Telnet

Best practice dictates to use SSH instead of Telnet for remote management CLI connections. Cisco IOS includes a Telnet server and a Telnet client that can be used to establish Telnet sessions with other devices.

SSH

SSH is the recommended method for remote management because it provides a secure connection. SSH provides encrypted password authentication and transport of session data. This keeps the user ID, password, and the details of the management session private. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.
Terminal Emulation Programs

PuTTY
Terminal Emulation Programs (cont.)

Tera Term
Terminal Emulation Programs (cont.)

SecureCRT

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>1K-blocks</th>
<th>Used</th>
<th>Available</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sda6</td>
<td>505605</td>
<td>171696</td>
<td>307805</td>
<td>36%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/sda2</td>
<td>77772</td>
<td>25621</td>
<td>48135</td>
<td>35%</td>
<td>/boot</td>
</tr>
<tr>
<td>/dev/sda9</td>
<td>30115460</td>
<td>23596276</td>
<td>4998936</td>
<td>83%</td>
<td>/home</td>
</tr>
<tr>
<td>none</td>
<td>1032324</td>
<td>0</td>
<td>1032324</td>
<td>0%</td>
<td>/dev/shm</td>
</tr>
<tr>
<td>/dev/sda5</td>
<td>256667</td>
<td>9122</td>
<td>234293</td>
<td>4%</td>
<td>/tmp</td>
</tr>
<tr>
<td>/dev/sda8</td>
<td>3099260</td>
<td>2838228</td>
<td>103608</td>
<td>97%</td>
<td>/usr</td>
</tr>
<tr>
<td>/dev/sda3</td>
<td>381121</td>
<td>99109</td>
<td>262333</td>
<td>28%</td>
<td>/var</td>
</tr>
</tbody>
</table>
Topic 2.1.3: Navigate the IOS
Cisco IOS Modes of Operation

- A console connection must be established before initial configuration of a Cisco device.
- After being consoled in, the network technician will have to navigate through various command modes of the IOS CLI.
- The Cisco IOS modes use a hierarchical structure and are quite similar for both switches and routers.
- Video Available
Primary Command Modes

**User EXEC Mode**
Limited examination of router. Remote access.

Switch>
Router>

The **User EXEC** mode allows only a limited number of basic monitoring commands and is often referred to as view-only mode.

**Privileged EXEC Mode**
The **Privileged EXEC** mode, by default, allows all monitoring commands, as well as execution of configuration and management commands.


Switch#
Router#
Configuration Command Modes

Global Configuration Mode

- To configure the device must enter this mode with **configure terminal** command
- Example: `Switch(config)#`
- CLI configuration changes are made that affect the operation of the device as a whole
- From this mode, the user can enter different sub-configuration modes

Two common sub-configuration modes include:

- **Line Configuration Mode** - Used to configure console, SSH, Telnet, or AUX access. Example: `Switch(config-line)#`
- **Interface Configuration Mode** - Used to configure a switch port or router network interface. Example: `Switch(config-if)#`

- Video Available
Navigate Between IOS Modes

Router con0 is now available.
Press RETURN to get started.

User Access Verification
Password:
Router> enable
Password:
Router# disable
Router> exit

Comparator:
Switch
Router
Navigate Between IOS Modes (cont.)

Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# exit
Switch(config)# exit
Switch#

Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# vlan 1
Switch(config-vlan)# end
Switch#

Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
Topic 2.1.4: The Command Structure
Basic IOS Command Structure

Switch>show ip protocols

Prompt  Command  Space  Keyword or Argument

Switch>ping 192.168.10.5
# IOS Command Syntax

When describing the use of commands, we generally use these conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface text indicates commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>italics</em></td>
<td>Italic text indicates arguments for which you supply values.</td>
</tr>
<tr>
<td><code>[x]</code></td>
<td>Square brackets indicate an optional element (keyword or argument).</td>
</tr>
<tr>
<td><code>{x}</code></td>
<td>Braces indicate a required element (keyword or argument).</td>
</tr>
<tr>
<td>`[x {y</td>
<td>z}]`</td>
</tr>
</tbody>
</table>
**IOS Help Features**

**Context-Sensitive Help**

Switch\#cl?
clear clock

Command options - display a list of commands or keywords that start with the characters cl

Switch\#clock set ?
   hh:mm:ss  Current Time

Command explanation - the IOS displays what command arguments or variables can be next, and provides an explanation of each

Switch\#clock set 19:50:00 ?
   <1-31>  Day of the month
   MONTH   Month of the year

Command explanation with more than one argument or variable option

Switch\#clock set 19:50:00 25 June 2012
Switch#
IOS Help Features (cont.)

Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.

The IOS returns a help message indicating that required keywords or arguments were left off the end of the command.

Switch#c
% Ambiguous command:'c'

The IOS returns a help message to indicate that there were not enough characters entered for the command interpreter to recognize the command.

Switch#clock set 19:50:00 25 6
^%
Invalid input detected at '^'
marker.

The IOS returns a "^" to indicate where the command interpreter can not decipher the command.

Video Available
Hotkeys and Shortcuts

- **Tab** – Completes the remainder of a partially typed command or keyword
- **Ctrl-R** – Redisplays a line
- **Ctrl-A** – Moves cursor to the beginning of the line
- **Ctrl-Z** – Exits configuration mode and returns to user EXEC
- **Down Arrow** – Allows the user to scroll forward through former commands
- **Up Arrow** – Allows the user to scroll backward through former commands
- **Ctrl-Shift-6** – Allows the user to interrupt an IOS process such as ping or traceroute.
- **Ctrl-C** – Aborts the current command and exits the configuration mode
Section 2.2: Basic Device Configuration

Upon completion of this section, you should be able to:

- Configure hostnames on a Cisco IOS device using the CLI.
- Use Cisco IOS commands to limit access to device configurations.
- Use IOS commands to save the running configuration.
Topic 2.2.1: Hostnames
Device Names

Guidelines to Choose a Hostname

Hostnames should:
- Start with a letter
- Contain no spaces
- End with a letter or digit
- Use only letters, digits, and dashes
- Be less than 64 characters in length

Configuring Device Names

Hostnames allow devices to be identified by network administrators over a network or the Internet.
Configure Hostnames

Switch# configure terminal
Switch(config)# hostname SW-Floor-1
Sw-Floor-1(config)#

Syntax Checker Available
Topic 2.2.2: Limit Access to Device Configurations
Secure Device Access

Securing Administrative Access
- Secure privileged EXEC access with a password
- Secure user EXEC access with a password
- Secure remote Telnet access with a password

Other tasks
- Encrypt all passwords
- Provide legal notification

When Choosing Passwords:
- Use passwords that are more than 8 characters in length.
- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
- Avoid using the same password for all devices.
- Don’t use common words because these are easily guessed.
Configure Passwords

Privileged EXEC Password Example

Sw-Floor-1> enable
Sw-Floor-1#
Sw-Floor-1# conf terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
Sw-Floor-1# disable
Sw-Floor-1> enable
Password: 
Sw-Floor-1#

User EXEC Password Example

Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# exit
Sw-Floor-1(config)#

VTY Line Password Example

Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)#
Configure Passwords (cont.)

- Use the **enable secret** command, not the older **enable** password command.
- The **enable secret** command provides greater security because the password is encrypted.
Configure Passwords (cont.)

Console port must be secured.

- Reduces the chance of unauthorized personnel physically plugging a cable into the device and gaining device access.

VTY lines allow access to a Cisco device via Telnet.

- The number of VTY lines supported varies with the type of device and the IOS version.
Encrypt Passwords

service password-encryption

• Prevents passwords from showing up as plain text when viewing the configuration.

• Purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file.

• After this command is applied, removing the encryption service does not reverse the encryption.
Banner Messages

- These are an important part of the legal process in the event that someone is prosecuted for breaking into a device.
- Wording that implies that a login is "welcome" or "invited" is not appropriate.
- Often used for legal notification because it is displayed to all connected terminals.
- Video Available
Topic 2.2.3: Save Configurations
Save the Running Configuration File

- **Startup configuration** – File stored in NVRAM that contains all of the commands that will be used upon startup or reboot. NVRAM does not lose its contents when the device is powered off.

- **Running configuration** – File stored in RAM that reflects the current configuration, modifying affects the operation of a Cisco device immediately. RAM loses all of its content when the device is powered off or restarted.

```
Switch#show running-config
Building configuration...
Current configuration : 2904 bytes
!
! Last configuration change at 00:02:32
UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
<output omitted>
!
```

```
Switch#copy running-config startup-config
```
Alter the Running Configuration

• Restore the device to its previous configuration by removing the changed commands individually.

• Copy the startup configuration file to the running configuration with the `copy startup-config running-config` privileged EXEC mode command.

• Reload the device with the `reload` command from privileged EXEC mode.

• **Switch# reload**
  
  System configuration has been modified. Save? [yes/no]: n
  
  Proceed with reload? [confirm]

• Video Available
Capture Configuration to a Text File
Using PuTTY to Capture Console Session
Capture Configuration to a Text File (cont.)

Enabling Session Logging in PuTTY

- All session output will be captured to the file specified, MySwitchLogs.
- Execute the show running-config or show startup-config command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.
Capture Configuration to a Text File (cont.)
Disabling Session Logging in PuTTY
Chapter Objectives:

- Explain how devices communicate across network media.
- Configure a host device with an IP address.
- Verify connectivity between two end devices.
Topic 2.3.1: Ports and Addresses
IP Addresses

Connecting End Devices

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Smart phones
- Mobile handheld devices (such as wireless barcode scanners)

Configuring a Static IP Address on a Host

![Internet Protocol Version 4 (TCP/IPv4) Properties](image)
Interfaces and Ports

• Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.

• Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.

• Different types of network media have different features and benefits.

• Ethernet is the most common local area network (LAN) technology.

• Ethernet ports are found on end user devices, switch devices, and other networking devices.

• Cisco IOS switches have physical ports for devices to connect to, but they also have one or more switch virtual interfaces (SVIs). No physical hardware on the device is associated with it. It is created in software.

• SVI provides a means to remotely manage a switch over a network.
Topic 2.3.2: Configure IP Addressing
Manual IP Address Configuration for End Devices

Ethernet Adapter Properties

Manually Assigning IPv4 Address Information

![Ethernet Adapter Properties](image1.png)

![Manually Assigning IPv4 Address Information](image2.png)
Automatic IP Address Configuration for End Devices
Assigning Dynamic Addresses

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- Obtain an IP address automatically
- Use the following IP address:
  - IP address:
  - Subnet mask:
  - Default gateway:

- Obtain DNS server address automatically
- Use the following DNS server addresses:
  - Preferred DNS server:
  - Alternate DNS server:

Validate settings upon exit
Automatic IP Address Configuration for End Devices (cont.)

Verifying Windows PC IP Configuration

Enter the command to display the IP configuration on a Windows PC.

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : cisco.com
Link-local IPv6 Address . . . . . . : fe80::b0ef:ca42:af2c:c6c7%16
IPv4 Address . . . . . . . . . . . : 10.82.240.197
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.82.240.198

You successfully displayed the IP configuration on a Windows PC.
Switch Virtual Interface Configuration

```
Switch(config)#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface VLAN 1
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#no shutdown
```

- **IP address** - Together with subnet mask, uniquely identifies end device on internetwork
- **Subnet mask** - Determines which part of a larger network is used by an IP address
- **interface VLAN 1** - Interface configuration mode
- **ip address 192.168.10.2 255.255.255.0** - Configures the IP address and subnet mask for the switch
- **no shutdown** - Administratively enables the interface
- Switch still needs to have physical ports configured and VTY lines to enable remote management
Topic 2.3.3: Verifying Connectivity
## Interface Addressing Verification

### S1
```
show ip interface brief
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES</td>
<td>manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/2</td>
<td>unassigned</td>
<td>YES</td>
<td>manual</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

---

### S2
```
show ip interface brief
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES</td>
<td>manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/2</td>
<td>unassigned</td>
<td>YES</td>
<td>manual</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

---

`<output omitted>`

### VLAN

#### VLAN1
- **S1**: 192.168.10.2
- **S2**: 192.168.10.3

---

**Video Available**
End-to-End Connectivity Test

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
      Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.11:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
      Minimum = 820ms, Maximum = 883ms, Average = 842ms
```
Section 2.4: Summary

Chapter Objectives:

• Explain the features and functions of Cisco IOS Software.

• Configure initial settings on a network device using the Cisco IOS software.

• Given an IP addressing scheme, configure IP address parameters on end devices to provide end-to-end connectivity in a small to medium-sized business network.
Topic 2.4.1: Conclusion
Thank you.