

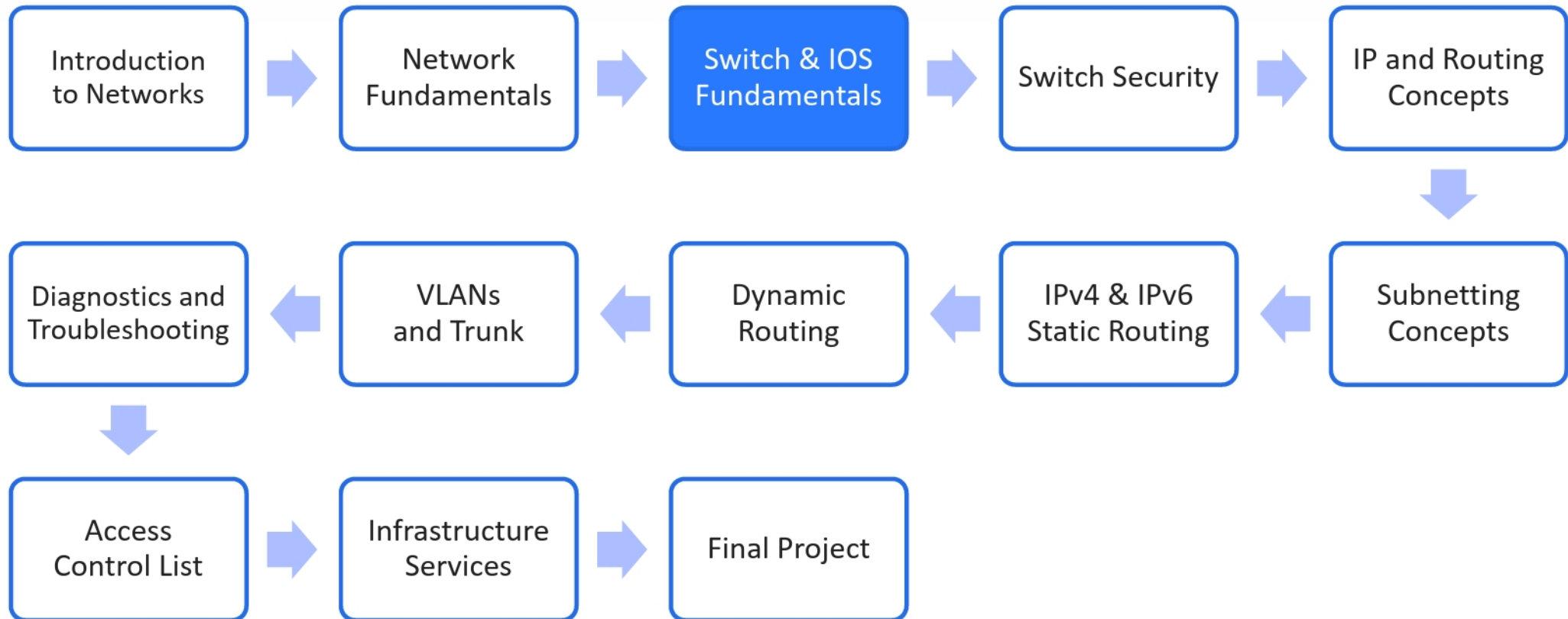


Cybersecurity Professional Program

Switch & IOS Fundamentals

Computer Networking

Computer Networking Course Path



Overview

Lesson Objective

The objective of this lesson is to learn more about the network switch and how it operates.

It also covers Cisco's operating system and configuration settings for Cisco and other platform devices.



Switch Fundamentals

The Cisco IOS

Initial Device Configuration

Managing IOS & System Files

Switch & IOS Fundamentals

SWITCH FUNDAMENTALS

The Switch

Overview



Switches are smart Layer 2 devices with many ports designed to forward frames from source to destination, according to specific MAC addresses in the frame (Data-Link Layer).

They include multiple technologies providing various capabilities.

Switches were developed to forward frames in accordance with their destination addresses and MAC tables using a MAC learning process known as *forwarding decision*.



MAC Tables

The command used to display the MAC address table is ***show mac address-table***

MAC address tables include the following columns:

- VLAN
- MAC address
- Dynamic or static
- Associated physical ports

DYNAMIC refers to a frame with a source MAC that arrives at a switch and updates the table with the MAC address for that port.

STATIC indicates a manually configured MAC address on a switch.

MAC Table

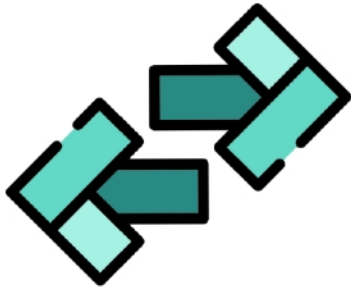
```
Switch#show mac address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
1	0001.97d7.45c3	DYNAMIC	Fa0/5
1	0004.9a3d.bbc6	DYNAMIC	Fa0/4
1	000c.8500.13bb	DYNAMIC	Fa0/3
1	00d0.978c.5690	DYNAMIC	Fa0/2



Switching Methods

Switching Methods



Switches have different methods of receiving and transmitting frames on the LAN.

The following switching methods are used:

- Store-and-forward
- Cut-through
- Fragment-free



Store-and-Forward Switching

Store-and-Forward Switching



- A switch using the store-and-forward method buffers the entire frame upon receipt. This enables the switch to support various port speeds. For example, a frame received on a 100 Mbps ingress port can be transmitted via a 1 Gbps egress port.
- Another advantage of this method is error checking, which can be done once the entire frame is buffered. The switch can easily detect frame errors using the FCS field.
- Although store-and-forward is relatively slow, it does provide error checking and support for different speeds across multiple ports.



Cut-through Switching

Cut-through Switching



- Cut-through switching is a much faster method than store-and-forward. In this method, only the first 6 bytes of the incoming frame are buffered, meaning the switch only regards the destination MAC address of the frame.
- The switch forwards the frame immediately, even before the entire frame is received, and no error checking is done.
 - **Note:** Modern switches can buffer up to 14 bytes of the beginning of a frame, before deciding what to do with it.
- Although the advantage of cut-through switching is its speed, a significant disadvantage is that most frames that reach the destination host are corrupted due to lack of error checking.



Fragment-Free Switching

Fragment-Free Switching

- Fragment-free switching is a more advanced method.
- This method buffers the first 64 bytes of the frame, including MAC address data and the frame's payload. The technique provides faster switching than the store-and-forward method while also performing partial error checking to make sure there is no fragmentation on the first 64 bytes of the frame.
- Fragment-free switching is therefore a better choice, as it is faster than store-and-forward switching and provides partial error checking, unlike the cut-through method.



Duplex Operation

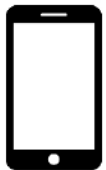
Half-Duplex



A connection for which the communication is restricted to exchanging data in one direction at a time. For example, a walkie-talkie is a half-duplex device because only one person at a time can talk.



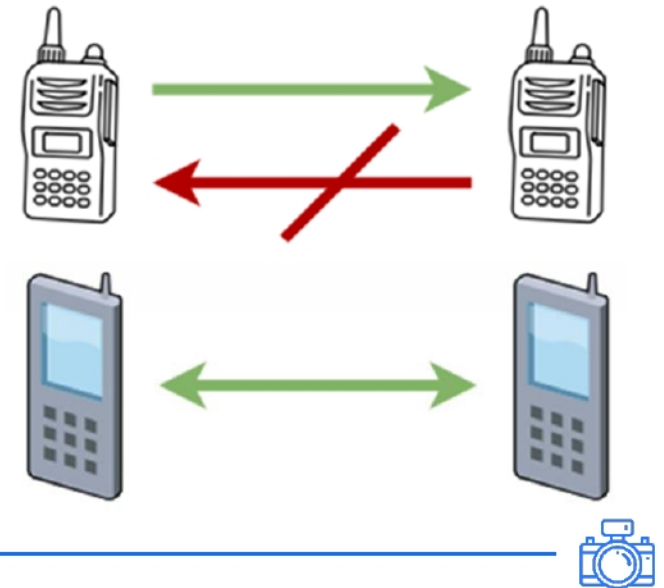
Full-Duplex



Full-duplex means that data can be transmitted in both directions, on a signal carrier, at the same time. For example, a telephone is a full-duplex device because both users can talk at once.



Communication



Port Speed

Switch Ports



Switch ports can transfer traffic at speeds of 10 Mbps, 100 Mbps, or 1000 Mbps.

The default is for the switch port to auto-configure its speed based on signaling between the port and the connected device.



There are switches that can transfer traffic at 10 Gbps or even 40 Gbps.

Auto-Negotiation

Auto-Negotiation



Auto-negotiation tells connected devices to announce their capabilities, and then, based on the settings of the interconnected device at the other end, chooses the optimal speed and duplex mode.



If one of the devices is configured with a different mode, a duplex mismatch will occur.

Switch & IOS Fundamentals

THE CISCO IOS

The Cisco IOS

The Cisco IOS

Overview



Every network device, such as a switch or router, has an operating system that tells it how to forward packets and execute network operations.

An operating system for a device is known as a Network Operating System (NOS).

An NOS does not operate in the same way as PC and server operating systems.

An Internetwork Operating System (IOS) is a CLI-based system, and users interface with it using text-based Cisco commands.



The Cisco IOS

The Cisco IOS

Overview



Most Cisco devices, regardless of their size or type, run the IOS, which is an advantage due its singularity and familiarity.

While all devices come with a default IOS and feature set, it is possible to upgrade the IOS version or feature set to obtain additional capabilities.

This course focuses on versions 12 and 15.



The versions of the IOS may be different, depending on the device hardware.

The Cisco IOS

The Cisco IOS

IOS or iOS

IOS

vs.

iOS



Internetwork **O**perating **S**ystem



It is interesting to note that the rights to the IOS name at first belonged only to Cisco.

IOS Interface Features

Command Line



IOS uses a command line interface (CLI) to enable administrators and technicians to interact with the system via special Cisco commands.



CLI



CLI is a means of interacting with programs by entering commands on a command line. Using a CLI-based system has many advantages, such as minimum resource usage, faster ability to operate on the system, and others.



Terminal Emulation



Many network devices are configured and managed using Terminal Emulation (TE) software, such as PuTTY. TE programs enable configuration of local devices using a serial cable or a remote management protocol, such as SSH.



The Cisco IOS

Terminal Software

PuTTY



PuTTY is a versatile tool for remote access to another computer. It is often used by people who want secure remote shell access to a UNIX or Linux system, though that is only one of its many uses.



Tera Term



Tera Term is an open-source, free, software-based terminal emulator (communication) program. It emulates different types of computer terminals, from DEC VT100 to DEC VT382, and supports Telnet, SSH 1 and 2, and serial port connections.



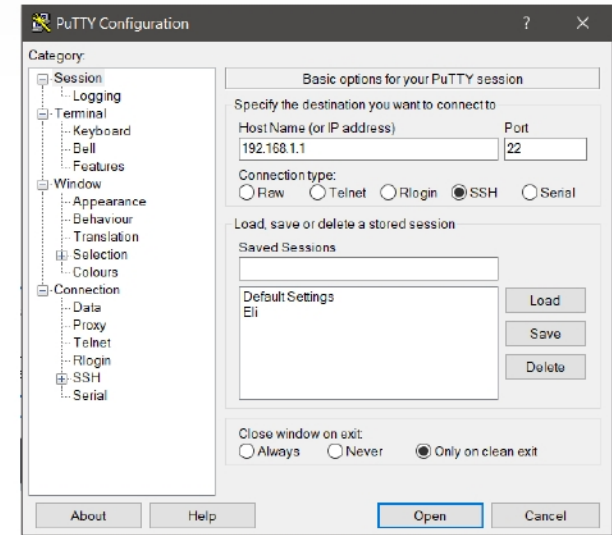
SecureCRT



SecureCRT is a commercial SSH and Telnet client and terminal emulator by VanDyke Software. Originally a Windows product, VanDyke recently added Mac OS X and Linux versions.



PuTTY



The Cisco IOS

Cisco Packet Tracer

Overview



Cisco Packet Tracer allows the user to map a network. Packet Tracer enables the testing of network configurations, trains users to work with network configuration, helps them understand how a network operates, and provides them with network deployment experience.



Lab NET-03-L1

Packet Tracer Installation
30–60 Min.



Mission

Create a Cisco account and download Packet Tracer to explore the features it provides.

Steps

- Register the account.
- Download Packet Tracer.
- Install Packet Tracer.

Environment & Tools

- Web Browser

Related Files

- Lab document

Access Methods

Out-of-Band



This method uses a dedicated management console cable that must be physically connected to the device. Initial configuration is usually done using this method.



In-Band



This method uses management protocols, such as SSH or Telnet, which access the device remotely over the network.



Console Cable



Out-of-Band Management

How Local Configuration Works



Out-of-Band management requires two main items:

- PC with terminal software
- Console cable



Terminal



A network device is like a PC, but without a mouse, keyboard, and screen. A PC with a terminal provides a way to input commands and view output from the device.



Console Cable



A console cable or management cable is like a bridge between the PC and the device. Almost every device has a designated console cable for this purpose. Older cables use an RS-232 connector; modern ones use USB.



IOS Modes

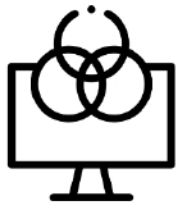
Permissions



IOS can operate in one of three work modes, each with different capabilities and permissions. For example, one mode may have a lower level of privileges compared with another mode.



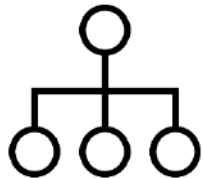
Modes



The division of modes is meant to separate the management levels and increase the efficiency of network device security and configuration.



Structure



Cisco IOS modes have a hierarchical structure and are similar among switches and routers.



IOS Modes

User EXEC Mode



This mode has low-level capabilities but is useful for basic operations. It has a limited number of monitoring commands and does not allow device configuration changes.



Privileged EXEC Mode



This mode has a large number of monitoring commands and device configuration viewing commands (show commands). It also enables file management operations, such as device configuration backups and IOS upgrades.



The Cisco IOS

IOS Modes

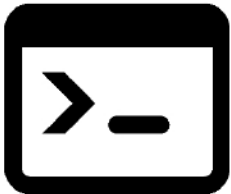
Global Configuration Mode

(config)#

Global configuration is the only mode that allows administrators to change device configuration. This mode is only accessible from the privileged EXEC mode.



Interface Configuration Mode



The interface mode allows you to change specific parameters within a switch or router.



The Cisco IOS

Navigating IOS Modes



Navigating the system and understanding the difference between the modes is very important when working in the system.

The default display name of a device appears before the prompt. In the example at right, the name is *Switch*.

The **enable** command moves the user from user mode to privileged mode.

The **configure terminal** command moves the user from user mode to global configuration mode.

The **exit** command takes the user one mode back.

IOS Modes

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#exit
Switch#exit
Switch>
```



IOS Error Messages

Incomplete Command



The command is correct but not complete.



Ambiguous Command



Not enough characters were entered for the command to be recognized. Or, more than one command exists with the same name.



Invalid Input



The command was entered incorrectly (i.e., typo) or inserted in the wrong mode.



Example

```
Switch>di
% Ambiguous command: "di"

Switch#show
%Incomplete Command.

Switch(config)#hostname S1
                        ^
% Invalid input detected at '^'
marker.
```



The Cisco IOS

Hotkeys and Shortcuts

TAB

Completes partial entry.

Break sequence used to abort DNS lookups, traceroutes, pings, etc.

CTRL+SHIFT+6

CTRL + D

Erases the character at the cursor.

Erases the word to the left of the cursor.

CTRL + W

CTRL + K

Erases all characters from the cursor to the end of the command line.

Recalls a command from the history buffer.

CTRL + P

ESC + D

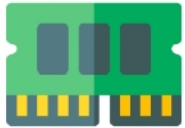
Erases all characters from the cursor to the end of the word.

Ends configuration mode and returns to privileged EXEC mode.

CTRL + Z

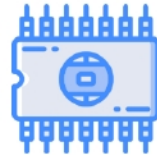
Cisco Device Components

RAM



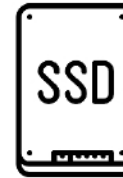
Volatile memory that stores the system configuration (running-config) and tables (such as the MAC table).

ROM



Non-volatile memory responsible for the Power-On Self-Test (POST) process and bootstrap, which is the initial program responsible for booting the IOS.

FLASH



Non-volatile memory that stores the operating system itself (IOS).

NVRAM



Non-volatile memory that stores the startup config file.

Device Boot Process

POST

POST and bootstrap program load: This part of the sequence checks the CPU, RAM, and NVRAM. When done, the device copies the bootstrap program from the ROM to the RAM.

1

Load IOS

Load IOS: After copying the bootstrap program from the ROM to the RAM, the IOS (which is still stored in flash memory) is copied to the RAM for execution.

2

Load Configuration

Load configuration: The bootstrap program now copies the startup configuration file from the NVRAM to the RAM.

3

Switch & IOS Fundamentals

INITIAL DEVICE CONFIGURATION

Device Name

Command

```
hostname <device name>
```



Set Device Name

```
Switch(config)#hostname S1-Floor1  
S1-Floor1(config)#
```



Sets the local network device name; for example, S-Floor1

Create User Account

Command

```
username <user-name> password <password>
```



Create Account

```
Switch(config)#username Admin password p@nd@  
Switch(config)#username Peter password Spiderm@n
```



Creates a local user account on the device

Initial Device Configuration

Secure Privileged Mode

Command

```
enable password <password>
```



Set Password

```
Switch(config)#enable password c!sc0
```



Enables password authentication when accessing the privileged EXEC mode

Security Message

Command

```
banner motd #security-message#
```



Set Message

```
Switch(config)#banner motd #Access to this device is for authorized personnel only#
```

```
Press RETURN to get started!
```

```
Access to this device is for authorized personnel only
```

```
User Access Verification
```

```
Password:
```



Displays a security message each time a user logs into the system

Encrypt Passwords

Command

```
service password-encryption
```



Encrypt Passwords

```
Switch(config)#service password-encryption
```



Configured passwords appear in plain text in the configuration file.
This command encrypts all plain-text passwords using the Cisco Type 7 method.

Save Device Configuration

Command

```
copy running-config startup-config
```



Save Configuration

```
Switch#copy running-config startup-config
```



Copies the device configuration from the RAM to the NVRAM (non-volatile memory)
If the configuration isn't saved to the NVRAM, all configurations that were performed will be lost.

Secure Console Access

Command

```
line console 0 & login local
```



Two steps are performed to enable local credential (username and password) authentication on the console port.

1. Enter the console port config mode (line mode).
2. Enter the local login and exit.

Note: Besides the local login command, there is a login command that enables only password checking.

Secure Console Port

```
Switch(config)#line console 0  
Switch(config-line)#login local  
Switch(config-line)#exit
```



Verify Configuration

All configuration changes are immediately saved in the *running-config* file.

To display them, run the *show running-config* or *show run* command.

Note: The example on the right is a brief glimpse of the actual file.

Verify Settings

```
S1-Floor1#show running-config
Building configuration...
Current configuration : 1234 bytes
!
version 12.2
service password-encryption
!
hostname S1-Floor1
!
enable password 7 08220D5D0A49
!
username Admin privilege 1 password 7 08316C400D39
!
banner motd #Access to this device is for authorized personnel only!#
!
line con 0
line aux 0
Line vty 0 4
  login
```



Lab NET-03-L2

Initial Cisco
Device Configuration
30–60 Min.



Mission

Learn how to set basic configurations on a switch using Cisco IOS commands.

Steps

- Access the device.
- Navigate the IOS.
- Configure initial and security settings.
- Alternate PKA opening

Environment & Tools

- Cisco Packet Tracer 7.2.2 or later

Related Files

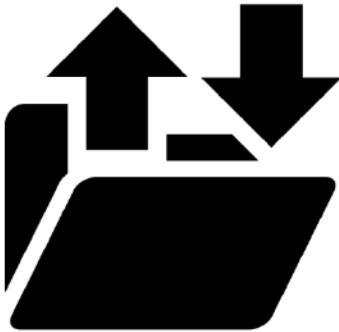
- Lab document
- NET-03-L2.pka

Switch & IOS Fundamentals

MANAGE IOS & SYSTEM FILES

TFTP

TFTP



Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol that allows clients to retrieve files from a remote host or transfer files to a remote host.

TFTP can also be used to remotely start a computer, back up network or router configuration files, and upgrade a device's IOS.



TFTP relies on UDP to transport data and uses port number 69.

Backup Device Configuration

Command

```
copy running-config tftp
```



Save Configuration

```
Switch#copy running-config tftp:
```



Copies the *running-configuration* file to a remote TFTP server
This is very useful for when a disaster occurs and a quick restoration of settings is required.

Backup Using TFTP

Note: First save the configuration locally using: *copy running-config startup-config*

Step 1: Copy the file to the server.

Step 2: Enter the TFTP server IP address.

Step 3: Select the name of the file saved on the server.

Backing up the IOS file is almost the same. You only need to replace the source location of the file, meaning *flash:* instead of *running-config*

Backup Example

```
R1#copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [R1-config]? R1-config-backup20.9

Writing running-config....!!
[OK - 1362 bytes]
```



IOS Upgrade

Step 1: The command **copy tftp: flash:** is used to copy the new IOS file from a TFTP server to the flash memory.

Step 2: Upgrading the device can be performed after copying the new IOS to the device using the **boot system** command. This command tells the device which IOS file to load on the next startup.

Step 3: The command **copy running-config startup-config** is used to save the current configuration to the startup configuration and reload the device for the new IOS to load.

Upgrading the IOS

```
R1#copy tftp: flash:
Address or name of remote host []? 192.168.1.3
Source filename []? c1901-imoversa;l9.mz.SPA.152-4.M3.bin
Destination filename [c1901-imoversa;l9.mz.SPA.152-4.M3.bin]?

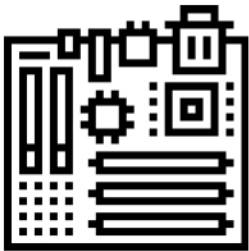
Accessing tftp://192.168.1.3/ c1901-imoversa;l9.mz.SPA.152-4.M3.bin...
Loading c1901-imoversa;l9.mz.SPA.152-4.M3.bin from 192.168.1.3:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4670455 bytes]

R1# Configuration terminal
R1(config)#boot system flash0://c1901-imoversa;l9.mz.SPA.152-4.M3.bin
R1(config)# exit
R1#copy running-config startup-config
R1#reload
```



ROMmon

What Does ROMmon Do?



The purpose of the Read-Only Memory MONitor (ROMmon) configuration register is to change the router's behavior in several ways:

- Determine how the router will boot.
- Apply options while booting (such as ignore configuration).
- Set the console speed and baud rate for terminal emulation sessions.



Configure Register Value

In the configuration terminal mode, we can change the register value, which will affect the next boot process.

In the example on the right, we change the register value to the default 0x2102, and save the configuration in startup config, which will set default factory settings.

Set Register Value

```
Router(config)# config-register 0x2102
Router(config)# end
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration
[OK]
Router# Reload
```



ROMmon Register Values

The default configuration register is 0x2102. We can verify this using the ***show version*** command. Using the command ***configreg***, we can change the register value and the router's behavior.

Common Settings

Register Value	Device Behavior
0x102	• Ignores break key • 9600 console baud rate (maximum transfer rate of the console port in bits per second; in this case, 9600)
0x1202	• 1200 baud rate
0x2101	• Boots into bootstrap • Ignores break key • Boots into ROM if initial boot fails • 9600 console baud rate
0x2102	• Default register value • Boots into ROM if initial boot fails • 9600 console baud rate default value for most platforms



Verifying Configured Register Value

By entering the command **show version** we can verify the configured register value.

We can also display additional information, such as the software type and version.

Show Version

```
Router#show version
<output omitted>
Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version 12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbasek9-mz.124-12.bin"

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```



Lab NET-03-L3

Backing up Config Files
and Managing the IOS
30–60 Min.



Mission

Use a TFTP server to back up and roll out switch configurations.

Steps

- Back up configuration files.
- Back up and upgrade the device IOS.

Environment & Tools

- Cisco Packet Tracer 7.2.2 or higher

Related Files

- Lab document
- NET-03-L3.pka

An overhead photograph of three people sitting around a wooden table, working on laptops. The scene is dimly lit with a blue tint. One person is pointing at a laptop screen with a blue pen. There are papers, a smartphone, and coffee cups on the table. The word "QUESTIONS?" is overlaid in white text.

QUESTIONS?



THANK YOU
