Module III

Basics of Router Configuration

Syllabus

Introduction to Routers. Router Hardware-Memory on Routers- 'Talking to Router' (Through the Console).- Router IOS- Configuring Router with <copy> and TFTP-Basic Router Configuration-Disaster Recovery-Setting the Bootstrap Behavior-Configuration Register Settings-t upgrading Router's IOS- Configuring the Router's Clock-IOS Message Logging.-Setting Up Buffered Logging-Setting Up Trap Logging-IOS Authentication and Accounting.

Introduction to Routers

- A router is a device that forwards data packets along networks.
- A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.
- Routers are located at gateways, the places where two or more networks connect.
- Routers use headers and forwarding tables to determine the best path for forwarding the packets.

Router Hardware

- In 1984 Cisco Systems began as a small startup.
- At first, the founders devised a "gateway server" to connect computers from different departments.
- Cisco Systems' first generation of products were known as gateway servers, and the product line had four iterations:
    - Advanced Gateway Server (AGS)
    - Mid-Range Gateway Server (MGS)
    - Integrated Gateway Server (IGS)
    - Advanced Gateway Server Plus (AGS+)
- These servers provided basic LAN-to-WAN and LAN-to-LAN routing.
- Today Cisco's router provides routing solutions for every application.

Entry Level	Mid Range	High End
Cisco 16xx	Cisco 26xx	Cisco 7xxx
Cisco 25xx	Cisco 36xx	Cisco 4xxx

Memory on Routers

Memory is used to boot the router, store its operating system, perform the routing process, and store the router's configuration information. To perform these tasks, four types of memory are used:

- Read-only memory (ROM)
- Flash memory
- Non-volatile random access memory (NVRAM)
- Dynamic random access memory (DRAM)

- **ROM**—Contains the power-on self test and the bootstrap program for the router. The ROM chips also contain either a subset or the complete router IOS (for example, the ROM on the 2505 router contains only a subset of the IOS, whereas the 7000 series contains the full IOS). The ROM chips on Cisco routers are removable and can be upgraded or replaced.
- **NVRAM (nonvolatile RAM)**—Stores the startup configuration file for the router. NVRAM can be erased, and you can copy the running configuration on the router to NVRAM. The great thing about NVRAM is that it retains the information it holds even if the router is not powered.
- **Flash RAM**—Flash is a special kind of ROM that you can actually erase and reprogram. It is used to store the Cisco IOS that runs on your router. You also can store alternative versions of the Cisco IOS on the Flash.
- **DRAM**—Similar to the dynamic memory you use on your PC, RAM provides the temporary storage of information and holds information such as the current routing table. RAM also holds the currently running router configuration (changes that you make to the configuration are kept in RAM until you save them to NVRAM).

Talking to Router' (Through the Console)

Access to the router's console (in most cases) is required for access to the operating system for initial setup and configuration. After the router is online, Telnet can be used to access a virtual router terminal port. After the router is online, Simple Network Management Protocol (SNMP) can be an alternative to the router's Command-Line Interface (CLI) to make changes and gather information about the router. Like Telnet, SNMP is dependent on TCP/IP for transport. Therefore, it requires TCP/IP to be enabled, in addition to its own protocol configuration. Once SNMP is configured and running on the router, an SNMP manager is used to send and receive commands.

Every **Cisco router/network switch** has a console port on its back. It is there to provide a way to hookup a terminal to the router in order to work on it. The console port (sometimes called the management port) is used by administrators to log into a router directly — that is, without a network connection. The console must be used to install routers onto networks because, of course, at that point there is no network connection to work through.

Making the physical connection

Follow these steps to connect the Router/Switch to a terminal or PC running terminal emulation software:

Step 1 Locate the console port on the back of the Router/Switch.

Step 2 Connect the console (or rollover) cable to the console port on the **Router/Switch**.

Step 3 Use the correct adapter to connect the other end of the cable to your terminal or PC.

Step 4 If your terminal or PC has a console port that does not fit one of the adapters, you must provide the correct adapter for that port.

Connecting using HyperTerminal

Click on the HyperTerminal icon below to launch a pre-configured HyperTerminal connection. This connection is configured for use with all Cisco Router/Switches. (The Router/Switch should be connected to your laptop at this time.)

Depending on your browser settings, you may initially see a message asking whether you want to open the file or save it to disk. To launch the connection now, select the "open" option. To save the connection to your local hard-drive for future use, select the "save" option.

If you selected the "open" option, you should now be communicating with the **Router/Switch**. If you are experiencing problems, make sure the

Router/Switch is powered on; you are attached to the proper Com Port and verify your cabling.

Router IOS

- Cisco IOS is the standard operating system for all Cisco routers.
- Cisco IOS is the standard by which other routing implementations are measured in terms of protocol implementation stability, IEEE, and ANSI hardware and software standards implementations.
- Following are the four types of internetwork services:-
    1. ***Reliable Adaptive Routing Services***
    - The Cisco IOS has reliable adaptive routing capabilities
    - It finds optimal paths on any network failures.
    - Reliable adaptive routing also reduces costs by efficiently using network bandwidth and resources.
    - Policy-based IOS features (such as route filtering) save network resources. It prevents data from being unnecessarily broadcast to nodes that do not require it.
    2. ***WAN Optimization Services***
    - It increases network throughput while reducing delay time.
    - It also minimizes ownership costs by eliminating unnecessary traffic and intelligently selecting the most economical WAN links available.
    3. ***Management and Security Services***
    - The Cisco IOS provides network management and security capabilities designed to meet the needs of today's large, complex internetworks.
    - Integrated management simplifies administrative procedures and shortens the time required to diagnose and fix problems.
    - Automated operations reduce hands-on tasks and make it possible to manage large, geographically dispersed internetworks with a small staff of experts located at a central site.
    4. ***Scalability Services***
    - Scalability services provide a high degree of flexibility.

- The IOS's scalable routing protocols help avoid congestion, overcoming protocol limitations, and solve problems related to geographical dispersion of an internetwork.
- The IOS also helps to cut costs by reducing network bandwidth and processing overhead,and easing system configuration tasks.

Configuring Your Router with <copy> and TFTP

Configuration EXEC mode is fine for simple adds and changes. The <copy> command is used to copy files on and off the router's NVRAM, DRAM, and flash "file systems".

Using <copy> to Erase File Systems

- The <copy /erase> command is introduced in IOS version 12.x, and when used with the [null] file system will erase a memory partition.
- For example, to erase NVRAM, the command <write erase> would be used.

Using <copy> with TFTP

- TFTP is the standard used for offloading and uploading IOS images and configuration files.
- It provides a file transfer mechanism for loading OS and configuration information for disk less workstations.
- TFTP has no security, and files can be copied back and forth with no authentication.
- It uses IP's UDP port (69) for transport.

Three types of files:-

- User EXEC - The user EXEC mode is basically a user shell.
- Privileged EXEC - The privileged EXEC mode enables complete control over the router.
- Configuration EXEC - Configuration EXEC mode is only for creating and modifying the router's configuration files.

Basic Router Configuration

To configure the router, perform one or more of these tasks:

- Configure Global Parameters
- Configure Fast Ethernet LAN Interfaces
- Configuring a Loopback Interface
- Configuring Command-Line Access to the Router

Configure Global Parameters

Perform these steps to configure selected global parameters for your router:

	Command	**Purpose**

Step 1	**configure terminal** Example: Router> enable Router# configure terminal Router(config)#	Enters global configuration mode, when using the console port. If you are connecting to the router using a remote terminal, use the following: telnet router name or address Login: login id Password: ********* Router> enable
Step 2	**hostname** *name* Example: Router(config)# hostname Router Router(config)#	Specifies the name for the router.
Step 3	**enable secret** *password* Example: Router(config)# enable secret cr1ny5ho Router(config)#	Specifies an encrypted password to prevent unauthorized access to the router.
Step 4	**no ip domain-lookup** Example: Router(config)# no ip domain-lookup Router(config)#	Disables the router from translating unfamiliar words (typos) into IP addresses.

Configure Fast Ethernet LAN Interfaces

The Fast Ethernet LAN interfaces on your router are automatically configured as part of the default VLAN and as such, they are not configured with individual addresses.

Perform these steps to configure a loopback interface:

Command

Step 1

interface *type number*

Example:

Router(config)# interface Loopback 0
Router(config-int)#

Purpose:- Enters interface configuration mode.

Step 2

ip address *ip-address mask*

Example:

Router(config-int)# ip address 10.108.1.1 255.255.255.0
Router(config-int)#

Purpose:- Sets the IP address and subnet mask for the loopback interface.

Step 3

exit

Example:

Router(config-int)# exit
Router(config)#

Purpose:- Exits configuration mode for the loopback interface and returns to global configuration mode.

Configuring Command-Line Access to the Router

Perform these steps to configure parameters to control access to the router, beginning in global configuration mode:

	Command	**Purpose**
Step 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number* Example: Router(config)# line console 0 Router(config)#	Enters line configuration mode, and specifies the type of line. This example specifies a console terminal for access.
Step 2	**password** *password* Example: Router(config)# password 5dr4Hepw3 Router(config)#	Specifies a unique password for the console terminal line.
Step 3	**login** Example: Router(config)# login Router(config)#	Enables password checking at terminal session login.

Step 4 **end**

Example:

Router(config)# end
Router#

Purpose:- Exits line configuration mode, and returns to privileged EXEC mode.

Disaster Recovery

Disaster Recovery involves a set of policies, tools and procedures to enable the recovery from a disaster of router such as the enable password is lost, or a sudden flow of power destroys the router and the IOS image is corrupted.

RTO refers to how much time an application can be down without causing significant damage to the data. Some applications can be down for days without significant consequences.

The Recovery Time Objective (RTO) is the duration of time within which a process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

Setting the Bootstrap Behavior

A Cisco router's bootstrap behavior is set using the configuration register(conf-reg).
Olden Cisco routers (such as AGS), the conf-reg was set with jumpers on the router's system board.
On the later Cisco models (Cisco 1000 and up), the conf-reg can be set in global configuration mode using the config-register command.
If access to global configuration mode is unavailable, the ROM Monitor (rommon), which is similar in function to a PC's BIOS mode, can be used.
Disaster recovery on Cisco routers using rommon and conf-reg settings is simple because all Cisco routers use the same basic boot sequence:
1. The router is powered up.
2. It checks its conf-reg settings.
3. It checks the NVRAM for boot loader information.
4. It loads the IOS.
5. It loads the NVRAM config.

Configuration Register Settings
Following are the most common conf-reg settings and their effects on the router.

- Register setting 0x2010—Configures the router to check NVRAM and boot directly into the ROM monitor.
- Register setting 0x8000—Configures the router (2500,4000,7x00) and loads the router into diagnostic mode.
- Register setting 0x2101—Loads the IOS from ROM, and the NVRAM configuration is loaded into RAM as the running configuration.
- Register setting 0x2102—The router loads the IOS from flash or the boot system source specified in NVRAM.
- Register setting 0x2141—Tells the router to load the IOS from ROM and ignore the configuration in NVRAM.
- Register setting 0x2142—The router loads the IOS from flash and ignores the NVRAM.

Upgrading Router's IOS

TFTP is the easiest way to upgrade your router's IOS. It is recommended that you have the **TFTP** server on the same local segment, if possible. On RFF routers (1600, 2500 series), the router boots with the flash in read-only mode, and because it reads data structures from the IOS stored in flash, it cannot be altered while the router is using them. To perform an IOS upgrade, you need to configure the router to load its IOS off the TFTP server instead of using the flash stored image.
On RFR routers (1600-R, 2600, 36x0, 4x00, and 7x00 series), the router's flash is in read/write mode all the time because the IOS is loaded into DRAM at boot. IOS can be upgraded while the router is in operation.

RFF - Run from flash
RFR - Run from RAM

Configuring the Router's Clock
Cisco routers, like all computers, keep track of time.When you configure your router, you need to set its clock, either manually each time the router reboots, or by using the Network Time Protocol (NTP).

To set your time zone, use the global configuration command <clock timezone>.
Router(config)#clock timezone EST -5

To set the router's system clock, use the privileged EXEC command <clock set>. The convention is hour:min:second day month year:
Router#clock set 12:00:15 14 June 1999

The router's clock must be set every time the router boots (or reboots). Because this can be inconvenient, IOS supports NTP to perform this function. In many cases, a site's ISP will provide access to a timeserver for its customers. If this service is unavailable, there are several public Time servers available over the Internet.
IOS provides the facility for the router to act as an NTP client, an NTP server, or an NTP peer. As an NTP client, the router contacts the defined NTP server, then verifies and synchronizes its system clock. As an NTP server, the router can be used by other systems on the network as their NTP server. In a peer scenario, the router and the NTP source exchange time synchronization information.

IOS Message Logging
log information is status data, such as changes in the router's interface status, modifications to running configuration, and debugging output.
The IOS provides four methods for viewing logging information:

- Console—The router's console port
- Monitor—The router's system monitor
- Trap— log output to a remote syslog server
- Buffer—A place to store a list of logging events in the router's DRAM

By default, all console and monitor methods are enabled, buffer and trap are disabled. The trap method is more useful for logging because the messages are stored on a remote server. The buffer approach stores the messages in DRAM, which is lost when the router is shut down or rebooted.

Setting Up Buffered Logging

To set up buffered logging, you first need to enable it. Then the local DRAM allocation and logging event history needs to be set. All logging parameters are set in global configuration Mode:
local-AS(config)#logging on
local-AS(config)#logging buffered 64000
local-AS(config)#logging history size 250

In the example above, all logging has been enabled, a local buffer of 64K has been allocated, and up to 250 logging messages will be stored in the buffer (the maximum is 500). The buffer logfile is a rotating one, so once the message count has reached its limit, it starts to overwrite itself, deleting the last message in the file as new messages are added.

Cisco uses the syslog level classification to define the severity of logging messages:

Message	Severity Level	Meaning Explanation
0	Emergencies	System is unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages
7	Debugging	Debugging messages

Each level sends messages recursively. If the warning's level is set, all message levels below. It is sent as well, so the message level defines what classes of messages will be sent. The default logging configuration has all router event messages logged. This is achieved with the logging level set to debugging.

Setting Up Trap Logging

Sending router messages to a remote host running syslog is more useful than local logging methods, but it requires a little more work. In addition to configuring the router, you must set up a host to process the syslog messages.

Here is an IOS trap logging configuration example:

local-AS(config)#logging trap informational

IOS Authentication and Accounting

IOS supports two modes of system authentication: old-mode and new-mode. Old-mode uses a static, locally stored user table or Terminal Access Controller Access Control System (TACACS) for user authentication. TACACS (introduced in IOS version 10.0) is a security software suite that provides a configurable modular system for providing authentication, accounting, and authorization.The server stores the user authentication and authorization data, and logs user and system accounting events.

There are three versions of TACACS supported by IOS:

- TACACS
- Extended TACACS
- TACACS+

New-mode is also referred to as AAA (authentication, accounting and authorization). In addition to user authentication, AAA provides facilities for system and IOS command accounting and authorization.

AAA also provides the capability to use Remote Authentication Dial-In User Service (RADIUS) and Kerberos V5 as an alternative to TACACS.

RADIUS (introduced in IOS version 11.2) is an open protocol security authentication and accounting system.

Kerberos (introduced in IOS version 11.2) is a trusted third-party authentication system. On the system side, authentication information is exchanged using a key called a servtab to encrypt messages between the system and the KDC. On the client side (which, from the Kerberos perspective, is the unsecured element), however, authentication is a little more complicated.

A simple view of the Kerberos user authentication process looks like this:

1. A user logs in, and a request is sent to the KDC, where the user's access rights are verified.
2. If the user is valid, a ticket-granting ticket (TGT) and a session key (SK) (which is used as a one-time password [OTP] to decrypt the TGT) are sent back in encrypted form, using the user's password as the source of the encryption key. The user is now authenticated locally. To access other systems that are part of the realm, another ticket is needed.
3. To get a ticket (which has a limited life span), the user generates a ticket request for the remote host it wants to access. The TGT and an authenticator are sent to the Ticket Granting Server (TGS). The request is verified, and a ticket and session key (an OTP to decrypt the ticket) for the requested system are returned.
4. After the ticket is acquired, the user logs in to the system. The system then verifies that the ticket and authenticator match, and if so, access is permitted.