UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Securizarea Calculatoarelor și a Rețelelor

6. Securizarea accesului la routere și switchuri

1 Router Architecture

Cisco routers have many similarities with personal computers. After all, most operating systems offer basic routing features to any PC with at least two network cards. The advantages of routers over personal computers lie in their dedicated hardware, specialized in routing functions, as well as in their operating system. This is why the performance of a router with a CPU 20-times slower than the one of a PC is still above the PC's performance when it comes down to routing packets.

Routers also have the common memory types that can be found in a PC, too:

- ROM – used at boot up, for hardware tests and initialization; it also retains a minimal operating system that allows the administrator to perform an OS update or a password recovery. It's quite small.
- RAM – loses its contents when the router is powered off or rebooted. It loads the operating system, stores all the running configuration, statistics, the routing table and a fraction of it is used for packet buffers. Varies is size; it can have tens or hundreds of MB.
- Flash – permanent memory, similar to a computer's HDD. It stores the operating system's image file and any other types of files. It is usually smaller than the RAM (tens of MB).
- NVRAM – this small non-volatile memory permanently retains the router's configuration. It can be around 32 KB.

A router also has a CPU that does all the arithmetical and logical work. The lookup in the routing table and the routing process are done in software. Layer 3 switches have dedicated circuits that accelerate the routing table lookup, making them faster than routers.

A router also has different types of interfaces that allow it to communicate with the outside world. All interfaces are indexed starting from 0 (zero):

- Network interfaces are meant for packet routing. Each interface must be configured with a layer 3 address (IP) before it will be able to route packets. You will encounter interfaces like Ethernet, FastEthernet or Serial. Each interface is numbered according to its index and the module it belongs to. For example, Serial 1/2 indicates the third serial interface from the second module.
- Administrative interfaces are considered „out-of-band", meaning that data transferred through these interfaces is not routed data. They are used for management purposes and require the administrator to be in the proximity of the router (or to have some other mean to overcome this). Each router has a console interface (Console 0) used to connect a PC's serial port to the router. Some routers also have an AUX interface, which connects to a PC's modem.
- Virtual interfaces. Some more advanced configuration topics require virtual interfaces, which are defined in software and have no hardware counterpart. These include loopback interfaces, tunnel interfaces and virtual terminals. If these sound strange to you, don't worry, you'll get to know them better later on!

A router does much more than "simple" routing functions. It can run a lot of services and provide many features to the networks it connects to. For example, it can also function as a firewall or some other security device. All these features are provided by the operating system, Cisco IOS (Internetwork Operating System).

2 Cisco IOS Fundamentals

The Cisco IOS command-line interface (CLI) is the primary user interface used for configuring, monitoring, and maintaining Cisco devices. This user interface allows you to directly and simply execute Cisco IOS commands, whether using a router console or terminal, or using remote access methods.

To aid in the configuration of Cisco devices, the Cisco IOS command-line interface is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of router and network operations. The commands available to you at any given time depend on the mode you are in. Entering a question mark (**?**) at the system prompt (router prompt) allows you to obtain a list of commands available for each command mode.

The use of specific commands allows you to navigate from one command mode to another. The standard order that a user would access the modes is as follows: user EXEC mode; privileged EXEC mode; global configuration mode; specific configuration modes; configuration submodes (and several other configuration sub-sub-...-submodes).

When you start a session on a router, you generally begin in *user EXEC mode*, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in user EXEC mode. This level of access is reserved for tasks that do not change the configuration of the router, such as determining the router status.

In order to have access to all commands, you must enter *privileged EXEC mode*, which is the second level of access for the EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. In privileged EXEC mode, you can enter any EXEC command, as the privileged EXEC mode is a superset of the user EXEC mode commands.

From privileged EXEC mode, you can enter *global configuration mode*. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots.

3 Basic Configuration Examples

Throughout these labs, you will be using Cisco Packet Tracer, a network simulator from Cisco. It simulates several network devices (routers, switches, access points) along with the connections between them. PT can save the topology, together with the configuration for all the devices involved, in a .pkt file.

Remember that PT is only a simulator. It does not offer all the functionality of a real router IOS and you might encounter some bugs from time to time. Still, you will be able to solve all the tasks in these labs using Packet Tracer.

To enter a router's CLI, click once on a router in PT and go the CLI tab. This is where all your configuration will take place.

3.1 Modes

After a router boots up, you get an output that look like this:

```
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)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

The output summarizes the router's hardware configuration. After you type no you get to the `Router>` prompt. At this prompt you can type show version again to display a summary of the router's hardware configuration.

```
Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>
```

This is the user EXEC mode. Press ? to get a list of available commands:

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
```

To turn on privileged commands, type enable. The prompt changes to indicate the privileged EXEC mode. Type disable to go back to user EXEC:

```
Router>enable
Router#disable
Router>
```

A router maintains a configuration file in RAM (active or „running" configuration) and a permanent configuration file in NVRAM. To enter the configuration mode, type `configure terminal` in the privileged EXEC mode. The prompt changes:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

The `(config)` indicates the configuration mode the router is currently in. Right now, this is the „root" of the configuration mode. All other sub-modes will be accessed from here. You can list the available commands using „`?`" in every mode.

To go „back" one level in the configuration hierarchy, type `exit`. To go back to the `Router#` prompt and completely exit all configuration modes, use `end` or press CTRL-Z.

3.2 *Interfaces*

Interface configuration is done in interface configuration mode. For example, to configure a FastEthernet interface with an IP address and a network maks and to turn it on, type the following commands:

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
```

Use the `show interfaces` and `show ip interfaces` commands to view the full configuration of all network interfaces. To quicky view the state of each interface and the IP configuration, use the `show ip interface brief` command:

```
Router#show ip interface brief
Interface        IP-Address      OK? Method Status                Protocol
Serial1/0        10.0.0.1        YES manual up                    down
Serial1/1        192.168.0.1     YES manual up                    up
Serial1/2        unassigned      YES unset  administratively down down
Serial1/3        unassigned      YES unset  administratively down down
Loopback0        200.100.0.1     YES manual up                    up
```

The status of the interface can be `up` (layer 1 OK), `down` (layer 1 error) or `administratively down`, if the administrator specifically shut down the interface or was never brought up. All interfaces on a router are `administratively down`, by default.

The „protocol" field indicates the layer 2 protocol status (Ethernet, PPP and others). For example, the first serial interface has been brought up but the cable hasn't been connected on the other end, so the layer 2 protocol cannot function between the two interfaces.

3.3 „Lines”

A line is a special kind of interface and they are used for administrative purposes. The lines exist only in software but some of them can have a hardware counterpart. For example, when you connect to the console, the IOS „sees” you on the „console 0” line. The same goes for telnet connections: each time a user connects via Telnet to the router, the user communicates with the IOS through a Virtual TeletYpes (VTY) interface that allow the user to connect to the listening telnet daemon. Each user „occupies” one vty, even if multiple users connect through the same physical interface.

To enter line configuration mode, use the same syntax as you did when you entered interface configuration mode and substitute the word `interface` with the word `line`:

```
Router(config)#line console 0
Router(config-line)#exit
Router(config)#line vty 0
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#
```

Commands similar to `line vty 0 4` can be used to select multiple vty lines. The configuration made in the `(config-line)` mode will then apply to all the lines that were selected.

4 Tasks

Open the `Labweek2_Topology.pkt` file. To solve the following tasks, DO NOT configure anything on the switch.

Important! „?" and „tab":

- Remember to type „`?`" in all configuration modes to list the commands available to you. The „`?`" can be used to list all the forms of a certain command, too. Simply type „`?`" after the first word in the command and you will get a list of parameters that you can use to continue the command. For example, typing `configure ?` will return a list in which you will find `terminal` as an option.
- The „tab" key autocompletes the words that make up commands, as long as there is no confusion. For example, pressing „tab" after typing `c` will not give you `configure`, but pressing „tab" after `conf` will.

Important! Writing answers:

- Whenever you are asked to answer a question, type the answer in a notepad window and keep it until the lab assistant checks that task.

1. [0.5p] Log in to router Mickey. List the commands available in user exec mode and then in privileged exec mode. Find the command that reboots the router and reboot it.

2. [+1.0 = 1.5p] Find out and write down the amount of memory for each memory type: RAM, flash, NVRAM.
   Hint: All routers have the same hardware configuration, you only need to query one.

3. [+0.5 = 2.0p] Configure the hostnames on each router. Your prompt will change when you change the hostname (name) of each router.

4. [+1.0 = 3.0p] Configure a clear-text enable password. Then, configure an md5-hashed enable password. „Hide" using a weak encryption algoritm the clear-text enable password.
   Hint: See page 288 from the ICND1 documentation.

5. [+0.5 = 3.5p] Configure a message-of-the-day banner on router Mickey with the message „This router is <your name here>'s property! Unauthorized access will be punished with no mercy!". Test this banner.
   Hint: the banner will show up when you log into the router. Find the command to exit user exec mode.

6. [+0.5 = 4.0p] Set the clock on router Pluto to the current time and date. Use „`?`" to find out the syntax and verify it with `show clock`.

7. [+1.0 = 5.0p] List the available interfaces on each router. Determine which interfaces have cables in them. For each used interface, insert a description that says „Interface to router X" or „interface to switch X".

   Hint: Hover your mouse cursor over a cable to display the interfaces on both ends. Use the interface configuration mode.

8. [+0.5 = 5.5p] Show the running configuration. Show the startup configuration. What are the differences between these two? Copy the running configuration over the startup configuration.

9. [+1 = 6.5p] Configure the serial interfaces between Mickey and Minnie with IP addresses from the network 172.16.150.0/24. Serial interfaces need a clock rate to be configured equally on both ends. Ping from one router to the other to test your connection.

   Hint: You can use any IP addresses in the given address space.

10. [+1 = 7.5p] Configure the FastEthernet interfaces between all three routers (the network with the switch in the center) using IP addreses from the 192.168.1.0/24 address space. Do not configure anything on the switch. Test using ping.

    Hint: All three interfaces connecting to the switch are in the same network. Also, same hint as above.

11. [+0.5 = 8.0p] Write down the routing tables for each router. Does each router see exactly two networks?

12. [+0.5 = 8.5p] Add a loopback interface for each router. Use the address 200.100.X.1/24, where X is 1, 2 or 3 for Mickey, Minnie and Pluto. List your interfaces to check this task.

13. [+0.5 = 9.0p] Write down the MAC addresses of each FastEthernet interface on each router. Also, write down the ARP tables for each of the above interfaces.

14. [+0.5 = 9.5p] Write down the routing tables for each router. Does each router know about all the loopback addresses you assigned? Explain why (write a single sentence).

    Hint: Determine what kind of routes are in each router's routing table.

15. [+0.5 = 10.0p] CDP is protocol used for Cisco network device discovery. Find the command to view each router's neighbors using CDP.

    Hint: CDP is enabled by default. You don't have to start the protocol; just show the neighbors.

---

16. [BONUS +1 = 11p] Manually configure the missing routes on each router, so that every loopback can be pinged from any router.