Cisco 2600 Router
Configuration
PartA
30 min
Static Routing
PartB
20 min
Dynamic Routing
PartC
0 min
Access Control Lists
PartD
30 min
Explore!

Components used:
2 computers with Microsoft Windows 2000
1 Cisco Systems Catalyst 2900 Series Switch
1 Cisco 2600 Router

Required Reading:
Study this handout carefully before you come to the lab.

Required PreLab:
When you come to the lab, bring this handout and submit the pre-lab to the proctor.

Submission of your lab work:
Submit the lab at the end of your session.

Part A: Cisco Router Configuration
Time 30 min

Introduction: Cisco routers are powered by the Cisco Internetwork Operating System (IOS) which allows the routers to be configured to perform specific tasks. Before you start configuration of a Cisco Router, you must understand the two EXEC modes available on a router: user EXEC mode and privileged EXEC mode. User mode allows you to perform basic trouble shooting tests, telnet to remote hosts, and list router system information. You know that the router is in this mode if the prompt is the router name followed by the greater than sign "RouterName>". Privileged mode, sometimes called enable mode, allows for full router configuration and advanced troubleshooting. "RouterName#" is an example of the privileged mode prompt. If you log into a router via a console or telnet connection, you enter user mode. Privileged mode requires that you issue the enable command.

Before you actually configure a Cisco router, you must understand the two main configuration modes: global configuration mode and interface configuration mode. You
use global configuration mode to configure router settings that affect overall router operations. This is accomplished by the command `configure` after you are in the privileged mode. If you wish to configure a particular interface, you must use interface configuration mode. To enter this mode, you need to be in the global configuration mode. You then enter the `interface` command followed by the name and number of the interface you wish to enter. If the router is in global configuration mode, the prompt will be "RouterName(config)#" while in interface configuration mode it will be "RouterName(config-if)#".

In this lab for each group of 2 students, there will be one designated router, one switch, 2 PCs running Windows, and several Ethernet (straight and crossover) cables. It is the goal of this lab to accustom you to the basic set up of a router. Most of the tasks require only one person typing; let one person do the typing for one section and let the other person do so for the next section.

You will configure the router to obtain the topology in the following diagram.

![Network Topology Diagram](image_url)

**Figure showing the network topology being used for this lab.**

**Lab Setup**

1. Make sure one PC per group is connected through the serial port to the router. That is, one end of the light blue serial cable will be plugged into the console port of the router and the other will be connected to the COM1 port of the PC.
2. Make sure each group has a switch and a router along with cables (one cable for each machine to connect it to the switch, one for connecting the switch to the
Task 0 - Statically configure an IP address and subnet mask for each computer.

1. Looking at the desktop window, find the icon labeled "My Network Places". Right click on this icon and select "Properties".

2. A window named “Network and Dial-up Connections” will appear with an icon named "Local Area Connection". Right click on this icon and again select "Properties".

3. Another window called "Local Area Connection Properties" will appear that has a white area with three items listed. One of these should be "Internet Protocol (TCP/IP)". Verify that this item is checked. If it is not, please do so.

4. Double click "Internet Protocol (TCP/IP)". Select “Use the following IP address”.

5. Input to the fields the IP address, subnet mask and gateway address according to the following table. Then click “OK” button in “Internet protocol (TCP/IP) Properties” window and “Local Area Connection Properties” window. You do not need to care about the DNS setting.

<table>
<thead>
<tr>
<th>Group A</th>
<th>IP Address</th>
<th>Subnet Mask Address</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer1</td>
<td>192.168.0.2</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>Computer2</td>
<td>192.168.0.3</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group B</th>
<th>IP Address</th>
<th>Subnet Mask Address</th>
<th>Gateway:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer1</td>
<td>192.168.50.2</td>
<td>255.255.255.0</td>
<td>192.168.50.1</td>
</tr>
<tr>
<td>Computer2</td>
<td>192.168.50.3</td>
<td>255.255.255.0</td>
<td>192.168.50.1</td>
</tr>
</tbody>
</table>

6. Verify that the IP Address for the computer has indeed changed. To do this, click on the "Start" button at the lower left of the computer screen and select "Run...". In the field, type cmd. This will allow for a command prompt window to appear. Type in ipconfig /all and press the Enter key. The windows may need to restart if you changed the IP address setting. From your host, ping the other host on your network. The ping should succeed.

NOTE: In order to see the IP address information shown by the ipconfig /all command, you should have connected the two computers in your group through the switch.
Task 1 - Use the program HyperTerminal to log on to the router.

Do the following operations on the machine that is connected to the console port of the router.

1. Verify the router is turned off.
2. Launch "HyperTerminal" at "Start", "Programs", "Accessories", "Communication", "HyperTerminal". You will now need to configure HyperTerminal so that it communicates with the router out of COM1.
3. Type `router` for the "Name" field in the "Connection Description" window, and click “OK”.
4. In the "Connect To" window, the fourth field is titled "Connect Using:" Scroll down to select COM1, and then click OK.
5. Confirm and change if necessary the following settings in the COM1 "Properties" window that pops up.

<table>
<thead>
<tr>
<th>Bits Per Second:</th>
<th>9600</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Bits:</td>
<td>8</td>
</tr>
<tr>
<td>Parity:</td>
<td>None</td>
</tr>
<tr>
<td>Stop Bits:</td>
<td>1</td>
</tr>
<tr>
<td>Flow Control:</td>
<td>Xon/Xoff</td>
</tr>
</tbody>
</table>

6. Click OK. At the bottom left of the window, it should say "Connected" with a running count of the time for which the connection has been active.
7. Turn on the router. Observe the boot-up procedure displayed in HyperTerminal. This lists information about the hardware, as well as the initial configuration. We will modify this configuration. (*Explore!*)

   NOTE: During the router boot-up, it may prompt if you want to enter the initial configuration dialog. Just ignore this prompt or type `NO`. And then press Return key when it prompts “…Line Protocol on Interface FastEthernet 0/0, changed state to down”.

8. Note that there are two Ethernet interfaces at the back of the router. Each of these interfaces should already be currently assigned an IP address. Type `show interfaces` to see their current state.

9. Record the MAC address (Hardware address), the speed of the interface (BW), and the Maximum Transfer Unit (MTU) for each interface in the table below. This information is the details about each interface.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Speed</th>
<th>MTU</th>
</tr>
</thead>
</table>
10. When the router boots up initially, it is in the User EXEC mode. This has limited capabilities. The commands that can be used in this mode can be viewed with the "?" command. Type ?, and carefully read the descriptions for the following command Enable, Show, Traceroute, Ping, and other commands shown.

You can type the ? command at any time to receive context sensitive help.

Task 2 – Reset router configuration

Because we are unsure of the validity of the current configuration, we need to erase it and configure it by ourselves. To erase the current configuration, we must be in Privileged Mode.

11. Type enable to enter Privileged Mode. If you are required to type password, type the password given on the chalkboard and press enter. The prompt should now end with #.
12. Type erase startup-config to clear the current configuration that resides on the router. (Note: Wait, it takes some time)
13. Confirm that you wish to erase nvram file system by press Enter, and wait till it completes
14. Type reload and confirm by pressing Enter. This reboots the router and allows the changes to take effect. (Note: Wait, this also takes some time)
15. If you are asked whether you want to save changes, type no.

Task 3 – Configure the router

Once the router has finished booting up, you will be in the System Configuration Dialog.

16. Type yes to enter.
17. Type no to skip the basic management setup.
18. Type yes to see the current interface summary.
19. Type in the name of your group for the host name (GroupA or GroupB)
20. Type in the password given on the chalkboard for the enable secret.
21. Type in the same password for the enable password. It will tell you not to use the same password, but it is okay, just type it in again.
22. Type in the same password for the virtual terminal password.
23. Type no to skip configuring the SNMP Network Management.
24. Type yes to configure IP.
25. Type no to IGRP and RIP routing, and bridging and configuring Async lines.
26. Type yes to configure the FastEthernet0/0 interface
27. Type yes to use the RJ-45 connector.
28. Type yes to full duplex mode.
29. Type yes to configure IP on the interface.
30. Use the following table to answer the next prompts.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group A</th>
<th>Group B</th>
<th>Subnet Mask Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEtherernet0/0</td>
<td>192.168.0.1</td>
<td>192.168.50.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>192.168.100.1</td>
<td>192.168.100.2</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

31. If you are asked whether to configure the Serial0/0 interface, type **no**.
32. Similarly configure the FastEtherenet0/1 interface (do it yourself). Then press Enter to save the newly created configuration to nvrarn.
33. Type **show interfaces**.
34. Verify that the IP addresses were correctly assigned. (do it yourself)

   NOTE: Make sure that you have connected the host machines to the switch and connected the switch to the FastEtherenet 0/0 interface of the router using Ethernet cables.

   One of the nice things about the Cisco IOS is that it does auto complete of commands, if you type a significant part of the command and press tab, the rest of the command will be added automatically. Another feature is the ability to abbreviate commands. Yet another and most useful feature is the ability to query for command syntax. For example if you don’t know what arguments are accepted for the show command, type **show ?** and a list of possible arguments is printed. (*Explore!*)

**Part B: Static Routing**

**Time 20 min**

The remaining part of this lab is to connect the two routers of Groups A and B together so that Group A and B can communicate with each other. The remainder of router configuration will be done via the Ethernet interface of each host.

1. Wait for the other team to finish Part A. Connect the FastEtherenet 0/1 interfaces of both the routers using the crossover cable.
2. Telnet (at “Start”->”…run” ) to the router interface that is connected to your switch. (do it yourself)
3. Type the password given on the board when prompted.

We will now set up a static routing table in each of the two routers. The idea is for the table to indicate that the other group's network can be reached via the 0/1 interfaces of both routers. To create a static entry in the routing table of the router, you must be in Configuration Mode.

4. Enter privileged mode and type **config terminal**. (do it yourself)
5. Using the command **ip route**, set up the static routing table. (do it yourself). The parameters that ip route takes are:
   a. Destination network(subnet) number (*the other group’s subnet*),
   b. Its subnet mask, (*the other group’s subnet mask*) and
   c. The IP address of the next hop that can reach the destination network (*the other group’s FastEthernet 0/1 router address*). (Question to think about: How would Group A setup an entry in the routing table so that machines in LAN1 can access machines in LAN2?)

6. By pinging a host from a host of the other group, verify that the static routing table has been created, and hosts from both groups should be able to communicate with each other.

7. To view the routing table, type **show ip route**. (Does this command work in the mode that you are in? Find that out by typing ‘show ?’. If the command is not available, change modes by typing ‘exit’.)

8. Gaining information about the topology of our network: Type **tracert** (in the Windows command window) on a host within your group's network; record the information that was returned. Now execute a tracert command on a host in the other group.

**Exercise1: list the entries in the routing table.**

<table>
<thead>
<tr>
<th>Entry 1</th>
<th>Entry 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Exercise2: record the output of the trace routes.**

---

**Part C: Dynamic Routing using RIP**

**Time: 0 min**
I. Introduction: The access list is one of the most important control mechanisms to control access to both the internal and external network. Access lists consist of *permit* or *deny* statements that filter traffic based on the source address/port, destination address/port, and protocol type of the packet. In this lab, you have a chance to setup a Cisco router access list from scratch.

**Access-list format**

Standard IP access lists

```
access-list [list #] [permit | deny] [source address] [source wildcard mask]
```

where

- `[list #]`: Standard IP access-lists are represented by a number in range 1-99
- `[permit | deny]`: Either allow or deny access to certain source
- `[source address]`: The IP address of the source
- `[source wildcard mask]`: A wildcard mask, or inverse mask, applied to determine which bits of the source are significant.

Unlike subnet masks, 0’s are placed in bit positions deemed significant, and 1’s are placed in positions that are not significant.

**Table**  Wildcard mask examples.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.22.5.2</td>
<td>0.0.0.0</td>
<td>All bit positions must match exactly. Access list will be applied only to the host 172.22.5.2</td>
</tr>
<tr>
<td>172.22.5.0</td>
<td>0.0.0.255</td>
<td>Bit positions in the first three octets must match exactly, but the last octet can be any valid number. The access list will apply to all hosts in the 172.22.5.0 subnet.</td>
</tr>
</tbody>
</table>

One of the most common problems with access list is lacking of planning. Since, access-list is accessed from top to bottom, therefore configuration and order of each entry must be very precise to work correctly.

Ex: The following access list is not correctly configured.

```
Access-list 1 deny any
Access-list 1 permit 168.243.32.0 0.0.0.255
Access-list 1 permit any
```

According to the access-list above, none of the computers on the network will be able to get access to the router because when a condition is satisfied by a rule in access-list, Router will NOT continue to check all remaining rules. Therefore, access list rules must appear in a logical order.

Extended IP access lists: Standard IP access lists are limited to filtering by source IP address only. Extended IP access lists, on the other hand, can filter by source IP address, destination IP address, protocol type, and application port number.
access-list [list #] [permit| deny] [protocol] [source IP address] [source wildcard mask] [destination IP address] [destination wildcard mask] [operator] [port] [log]

[list#]: Extended IP access-lists are represented by a number in range 100-199
[protocol]: The protocols to be filtered can be IP, TCP, UDP, ICMP etc.
[operator]: Can contain lt(less than), gt(greater than), eq(equal to), or neq(not equal to).
It is used if an extended list filters by a specific port number.
[port]: if necessary, the port number of the protocol to be filtered. (actually the format
allows you to specify the source port and the destination port)

Example:
Access-list 100 deny tcp host 172.22.5.2 host 172.22.2.2 eq 21
Access-list 100 permit ip any any

Once an access list is created, it must be applied to an interface. (You have a choice of
applying it to the 0/0 interface or the 0/1 interface, and for each interface if you apply it
to ‘out’, then all outgoing packets are examined and if you apply it to ‘in’, then all
incoming packets through that interface are examined.) With standard access lists, since
they examine the source address only, it must be placed as close to the destination as
possible to avoid blocking traffic bound for another interface. On the other hand,
extended access lists are able to filter based on source and destination. Therefore they are
placed as close to the source as possible.

Task 1 – Reset Access List
1. Make sure you are in privileged mode.
2. Verify that there are no access lists using show access-lists. If there are any
existing access lists, write down their access list number (e.g. the access list
number for “Standard IP access list 1” is 1.).
3. Type configure terminal.
4. Type no access-list followed by the access list number you recorded to delete the
pre-existing access list. For example, no access-list 1.
5. Verify that the router is able to communicate with both computers by using the
ping command with the ip address of a machine in your group and one in the
other group.

Task 2 – Create new Access List
Here you are going to configure the router so that one of the machines from the other
group can talk with you, while the other cannot.
6. Verify that there are no access lists using show access-lists
7. If you are GroupA, type access-list 1 deny 192.168.50.3; if you are GroupB, type
access-list 1 deny 192.168.0.3.
8. Group A type access-list 1 permit 192.168.50.2; GroupB type access-list 1
permit 192.168.0.2.
Task 3 – Applying Access List to Interfaces

9. Enter the interface configuration mode to configure the 0/0 interface. Type `interface FastEthernet 0/0`.
10. Apply the above list (list 1) to the out side of the interface by typing `ip access-group 1 out`.
11. Press control+z to quit the interface configuration mode.
12. Verify that the list has been entered; this time use the command `show run`.
13. And verify that the router correctly filters packets. Use `ping` from both host to verify.

Exercise 5: Fill in the IP addresses in the space provided with success of failure of the pings

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Your Group Computer 1</th>
<th>Your Group Computer 2</th>
<th>Other Group Computer 1</th>
<th>Other Group Computer 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your Group Computer 1</td>
<td>(</td>
<td>)</td>
<td>)</td>
<td>)</td>
<td>)</td>
</tr>
<tr>
<td>Your Group Computer 2</td>
<td>(</td>
<td>)</td>
<td>)</td>
<td>)</td>
<td>)</td>
</tr>
</tbody>
</table>

Ideas to explore if time permits:

A) Implement the Pre-Lab Question 4 problem: Implement and accesss list rule that disallows users on a PC in your group to browse web servers outside of your LAN. Make sure that that PC can still perform other tasks (such as PING) outside of your LAN.

B) Explore the possible commands on the router using ‘?’.