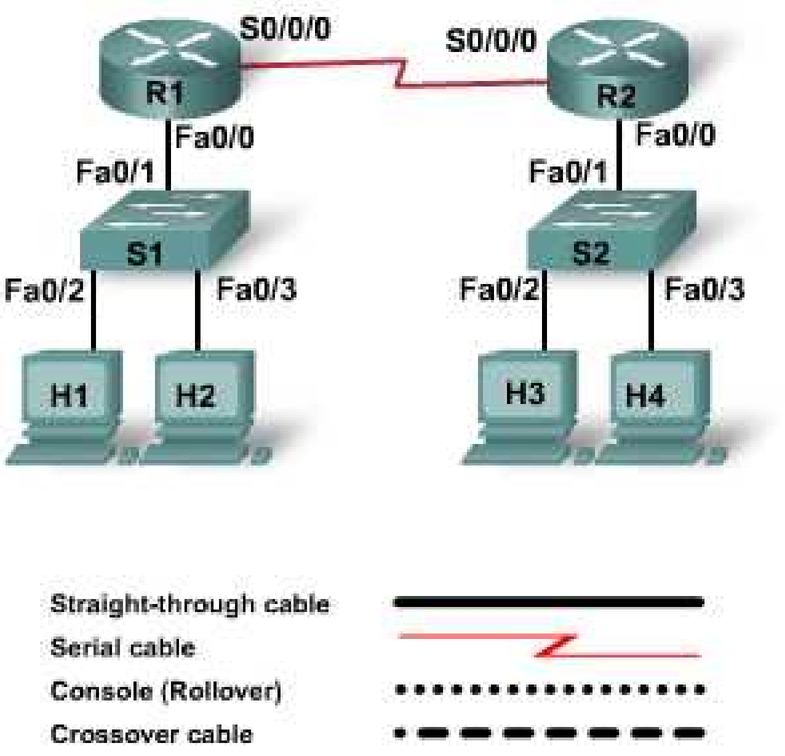
Lab 8.3.6 Configuring and Verifying VTY Restrictions



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.15.1/24	192.168.16.1/24	DTE		class	cisco
Router 2	R2	192.168.17.1/24	192.168.16.2/24	DCE		class	cisco
Switch 1	S1					class	cisco
Switch 2	S2					class	cisco
Host 1	H1	192.168.15.2/24			192.168.15.1		
Host 2	H2	192.168.15.3/24			192.168.15.1		
Host 3	H3	192.168.17.2/24			192.168.17.1		
Host 4	H4	192.168.17.3/24			192.168.17.1		

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Objectives

- Use access-class and line commands to control Telnet access to a router.
- Test the ACLs to determine whether they achieve the desired results.

Background / Preparation

In this lab you will work with vty ACLs to restrict Telnet access to a router. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Two Cisco 2960 switches or other comparable switches
- Two Cisco 1841 or comparable routers, each with a Serial connection and an Ethernet interface
- Four Windows-based PCs, both with a terminal emulation program, and both set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Six straight-through Ethernet cables
- One 2-part (DTE/DCE) serial crossover cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the S0/0/0 interface of Router 1 to the S0/0/0 interface of Router 2 using a serial cable as shown in the diagram and addressing table.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

c. Connect Host 1 to the Fa0/2 port of Switch 1 using a straight-through cable, and connect Host 2 to the Fa0/3 port of Switch 1 using a straight-through cable.

d. Connect Host 3 to the Fa0/2 port of Switch 2 using a straight-through cable, and connect Host 4 to the Fa0/3 port of Switch 2 using a straight-through cable.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Router 1, configure the hostname, interfaces, passwords and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram. Save the configuration.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Step 3: Perform basic configuration on Router 2

Step 4: Perform basic configuration on Switch 1 and Switch 2

Step 5: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure the hosts IP address, subnet mask, and default gateway according to the table and the topology diagram.

b. Each workstation should be able to ping the attached router. If the pings were not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure dynamic routing on the routers

a. Configure RIP routing on R1. Advertise the appropriate networks.

b. Configure RIP routing on R2. Advertise the appropriate networks.

Step 7: Verify connectivity

a. If the network has converged, list four destinations that H1 should be able to ping:

____

b. Test connectivity by pinging all the destinations. If any pings fail, troubleshoot the configurations on the routers and host PCs.

c. Check the routing table on R1.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.15.0/24 is directly connected, FastEthernet0/0
R    192.168.17.0/24 [120/1] via 192.168.16.2, 00:00:09, Serial0/0/0
C    192.168.16.0/24 is directly connected, Serial0/0/0
```

How many routes should appear? __________

d. Verify that all routes appear in the routing table. If a route is missing, troubleshoot the router configuration.

e. Telnet from the hosts to both routers. All hosts should be able to Telnet to both routers. If Telnet fails, troubleshoot the router and host configurations.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Step 8: Configure and test an ACL that will limit Telnet access

a. Create a standard ACL that represents the LAN attached to R1.

```
R1(config)#access-list 1 permit 192.168.15.0 0.0.0.255
```

b. Now that you have defined the LAN traffic, you must apply it to the vty lines. This allows users from this LAN to Telnet to this router, but will block users from other LANs from accessing Telnet on this router.

```
R1(config)#line vty 0 4
R1(config-line)#access-class 1 in
R1(config-line)#end
```

Which PCs should be able to Telnet to R1 and which should not?

____

c. Test the restriction.

Step 9: Create vty restrictions for R2

a. Create a Standard ACL that will not allow hosts on the R1 LAN to Telnet to R2 but will allow hosts on the R2 LAN to Telnet to their attached router.

```
R2(config)#access-list 2 permit 192.168.17.0 0.0.0.255
R2(config)#line vty 0 4
R2(config-line)#access-class 2 in
R2(config-line)#end
```

b. Conduct the tests to verify that this ACL achieves its goals. If it does not, troubleshoot by viewing the output of a **`show running-config`** command to verify that the ACL is present and applied correctly.

Step 10: Reflection

Why is the vty restriction ACL a good practice when configuring a router?

____

____

____

____

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.