1.9 – ENSA – Training - PacketKnows – Configuring an IPv4 ACL on VTY Lines

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router1	F0/0	10.0.0.254	255.0.0.0	N/A
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
Router2	F0/0	10.0.0.2	255.0.0.0	N/A
S1	VLAN 1	10.0.0.3	255.0.0.0	N/A

Objectives

- **Part 1: Configure and Apply an ACL to VTY Lines**
- **Part 2: Verify the ACL Implementation**

NOTE

- **Power all the devices first by clicking the triangle button on the upper navbar.**
- **Right click the device then click the web console first to configure on the device**

- **Always type “save” when configuring IP addresses of PC’s**

Background

As network administrator, you must have remote access to your router. This access should not be available to other users of the network. Therefore, you will configure and apply an access control list (ACL) that allows PC access to the Telnet lines, but denies all other source IP addresses.

Part 1: Configure and Apply an ACL to VTY Lines

Step 1: Verify Telnet access before the ACL is configured.

Both Router2 and S1 should be able to Telnet to the **Router**. The password is **cisco**.

Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on **Router1**.

Route1(config)# access-list 99 permit host 10.0.0.2

Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.

Step 3: Place a named standard ACL on the router.

Access to the **Router1** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 15. From the configuration prompt of **Router1**, enter line configuration mode for lines 0 – 15 and use the **accessclass** command to apply the ACL to all the VTY lines:

Router1(config)# line vty 0 15

Router1(config-line)# access-class 99 in

Part 2: Verify the ACL Implementation

Step 1: Verify the ACL configuration and application to the VTY lines.

Use the **show access-lists** to verify the ACL configuration. Use the **show run** command to verify the ACL is applied to the VTY lines.

Step 2: Verify that the ACL is working properly.

Both S1 and Router 2 should be able to ping the **Router**, but only **Router2** should be able to Telnet to it.