## Lab 23: Explore a Simple Network

### Case Study

SkyNet Systems, a growing IT services and infrastructure solutions provider, offers network deployment, support, and security services to a wide range of clients. As the company scaled its services, the complexity of managing client and internal networks increased. Relying on traditional manual methods for device configuration became inefficient and error-prone. To improve operational efficiency, SkyNet Systems adopted simulation-based training using Packet Tracer to help its technical team explore practical skills in network management, connectivity validation, internal service hosting, and access control configuration.

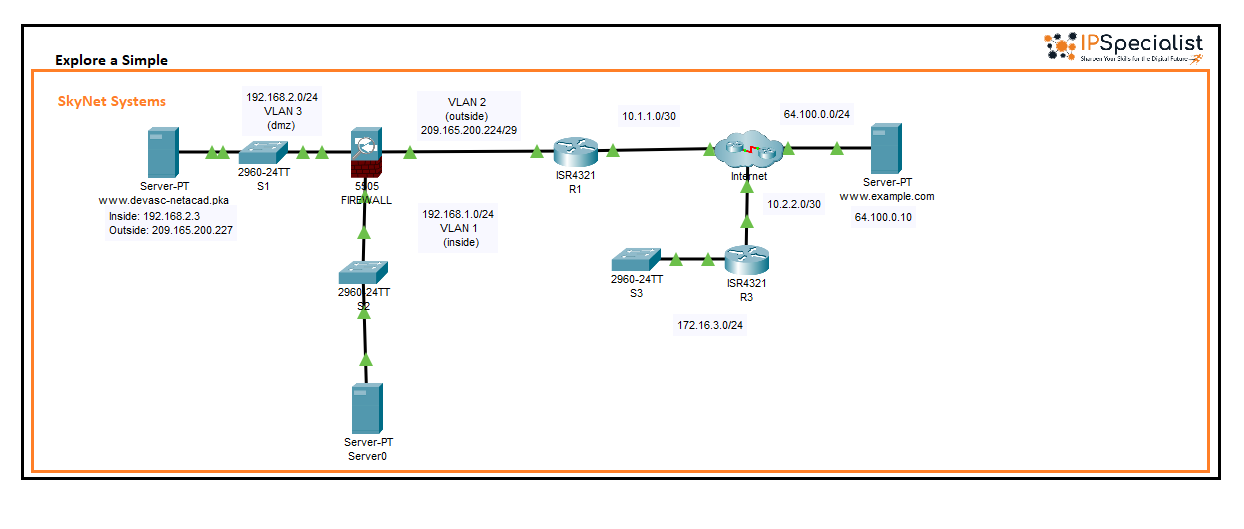
### Business Challenge

SkyNet Systems faced several operational challenges as it expanded. The team was spending too much time manually configuring devices, leading to inconsistent setups and delays in project completion. Troubleshooting was inefficient due to the absence of centralized visibility into network activity. There was also a lack of standard access control enforcement, exposing networks to potential security vulnerabilities. Moreover, regular connectivity and availability tests were not streamlined, making it difficult to detect and address issues before they impacted service delivery proactively.

### Solution

To resolve these issues, SkyNet Systems implemented a structured lab exercise using Packet Tracer, broken into four hands-on sections. These sections focused on adding new devices to the network, verifying connectivity paths, hosting a simple web application internally, and reviewing firewall policies. This practical simulation enabled SkyNet’s technical team to replicate real-world scenarios, test solutions in a safe environment, and develop consistent procedures for efficiently managing and securing networks.

1. Add PCs to the Topology
2. Test Connectivity Across the Network
3. Create a Web Page and View it
4. Examine the FIREWALL Access Lists



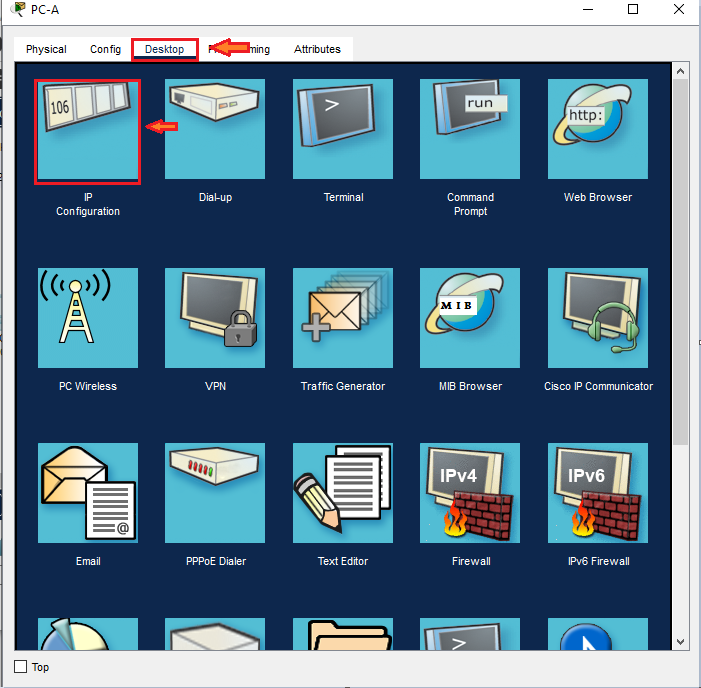
*Figure 23-01: Lab Topology*

**//Add PCs to the Topology**

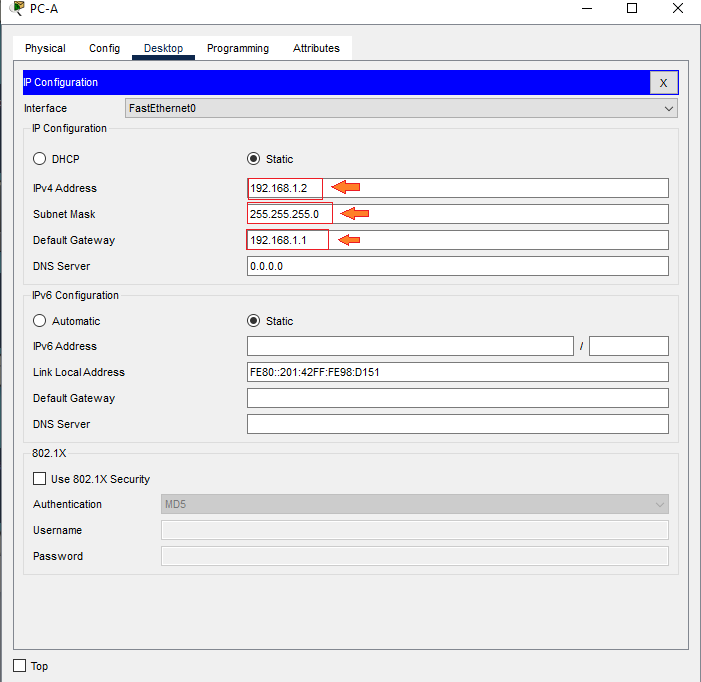
1. In this part, you will add PCs to the network topology and configure them with IPv4 addresses. Start by placing a PC in the workspace near switch S2. Make sure to use the correct device names, as they are case-sensitive; any variation in naming may affect your score. After placing the PC, rename it to **PC-A** to match the required naming convention. Once the PC is correctly named and positioned, it will be ready for further configuration and network connectivity.

2.Drag a PC to the work area and place it near S3, and rename the PC as**PC-B.** Connect a **Copper Straight-Through** cable from the **FastEthernet0** port a PC-A to any available FastEthernet port on S2. Connect a **Copper Straight-Through** cable from the **FastEthernet0** port of a **PC-B** to any available FastEthernet port on **S3**.

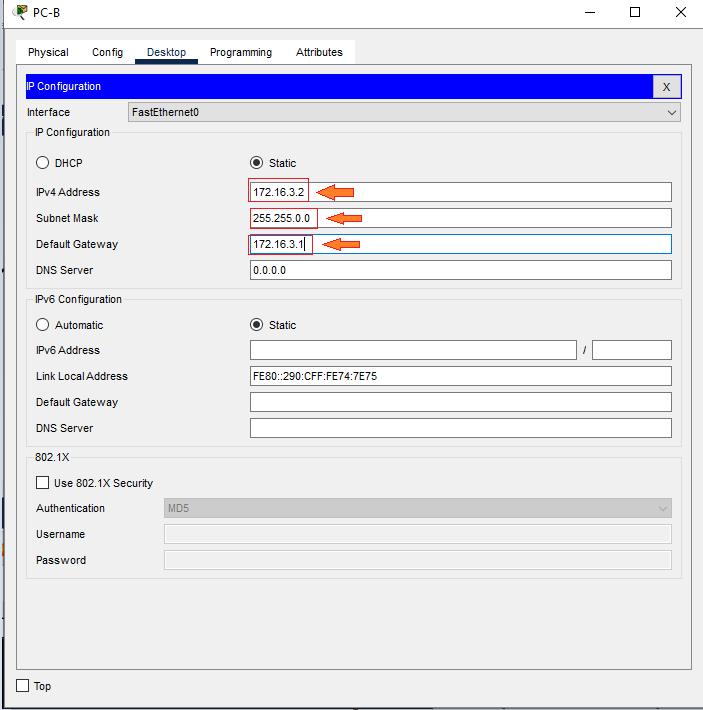
3. Click on **PC-A** to open its configuration window. Then, navigate to the **Desktop** tab to access desktop-related settings. From there, click on **IP Configuration** to begin assigning the IPv4 address and other network settings to the PC.



4. After accessing the IP Configuration window on PC-A through the Desktop tab, assign the necessary IPv4 addressing information. Enter **192.168.1.2** as the IPv4 address, **255.255.255.0** as the subnet mask, and **192.168.1.1** as the default gateway. Make sure all values are entered correctly to ensure PC-A can communicate effectively within the network.

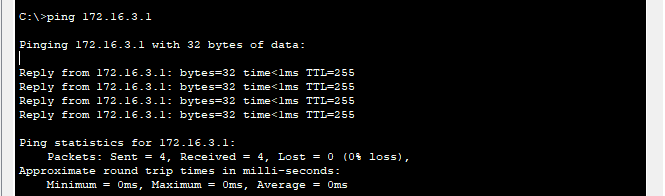


5. Repeat the same steps for **PC-B** by first placing it in the workspace near its designated switch, then renaming it to PC-B. Click on PC-B, go to the Desktop tab, and open the IP Configuration window. Assign the following IPv4 addressing details: set the IPv4Address to **172.16.3.2**, the Subnet Mask to **255.255.255.0**, and the Default Gateway to **172.16.3.1**. Ensure that all information is entered accurately to enable proper network connectivity for PC-B.

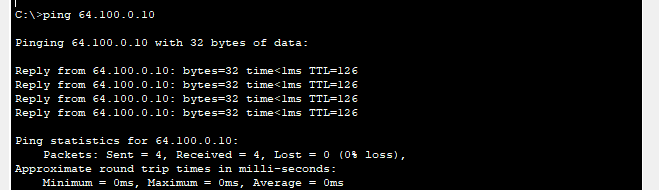


**//Test Connectivity Across the Network**

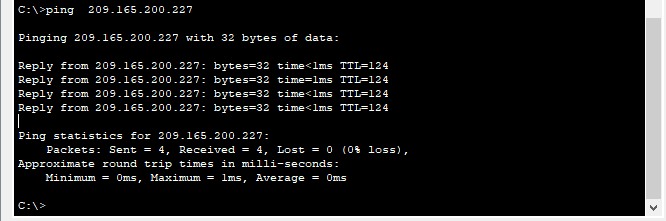
1. Click on PC-B to open its configuration window. Then, navigate to the Desktop tab and select **Command Prompt**. In the command prompt, type **ping 172.16.3.1** to test connectivity to the default gateway, which is router **R3**. You may need to run the ping command more than once as the network may take a moment to converge; eventually, you should begin receiving replies from the router.



2. Verify internet connectivity by pinging the **Example Server** at IP address **64.100.0.10**. Again, if the initial attempts fail, repeat the command until successful replies are received.



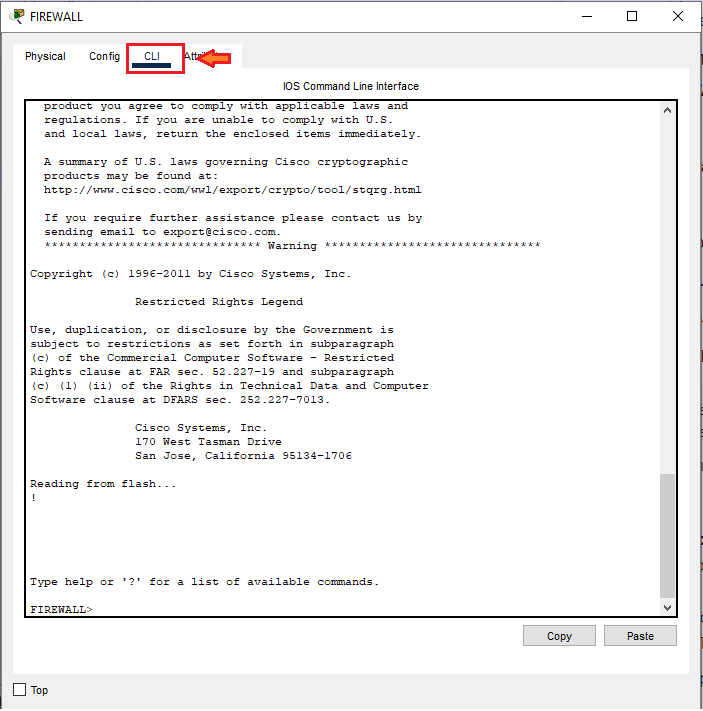
3. Test end-to-end connectivity by pinging the **DEVASC Server** at **209.165.200.227**. If you encounter any delays or timeouts, reissue the ping command until consistent replies confirm full network reachability.



|  |  |
| --- | --- |
| **//Create a Web Page and View it**  1. Click on **Services** in the PC or server window. By default, the **HTTP** service will be selected. Within the HTTP settings, click on **New File** to begin creating a new web page or file for the HTTP server. This allows you to host and test web content within the network environment     |  | | --- | | <html>  <center><font size='+2' color='blue'>DevNet Associate</font></center>  <hr>Welcome to the NetAcad DEVASC course! |   2. Name the new file **html** in the file name field. In the content area below, enter the following basic HTML code, which Packet Tracer can interpret for displaying a simple web page. If you are familiar with HTML, you can also customize this content to suit your preferences. Click **Save** and then click **Yes** to the warning.    3. Click on **PC-B** to open its configuration window. Navigate to the **Desktop** tab, and if the Command Prompt window is still open, close it. Then, click on **Web Browser** to open the web interface, which allows you to access web pages hosted on servers within the network.    4. In the **Web Browser** window on **PC-B**, enter the following URL into the address bar: **http://209.165.200.227**. Press **Enter** to load the page. If the web page does not display, double-check your IP configuration settings, default gateway, and ensure that the server is running the HTTP service correctly. Try refreshing or re-entering the address if needed, as the network may still be converging. |

**//Modify the Firewall Access List**

1. To Examine the access list on the Firewall device.Click on**Firewall** and thenclick on the **CLI.**



2. Press **Enter** a few times in the terminal window until the command prompt appears. Then, type **en** and press **Enter** to enter privileged EXEC mode. Since no password is configured, simply press **Enter** again when prompted. Next, type **show run** and hit **Enter** to display the router’s running configuration. Use the **space bar** to scroll through the output and review the configuration details. As you go through the configuration, take note of the Access Control List (ACL) entries, which specify the traffic filtering rules that help manage and secure network access.

**access-list OUTSIDE-DMZ extended permit icmp any host 192.168.2.3**

**access-list OUTSIDE-DMZ extended permit tcp any host 192.168.2.3 eq www**



3. Typically, it is best practice to prevent external users from pinging internal servers for security reasons. To enforce this, you need to remove the access-list statement that explicitly allows ICMP (ping) access. Start by entering **global configuration mode** using the command configure terminal at the firewall prompt:

**FIREWALL#**

**FIREWALL#configure terminal**

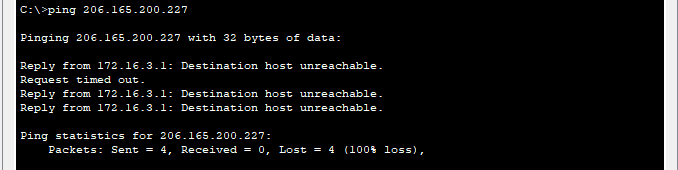


4. Once in configuration mode, remove the access-list rule that permits ping by entering the following command. Although it might wrap in the terminal, it's a single command line:

**FIREWALL(config)# no access-list OUTSIDE-DMZ extended permit icmp any host 192.168.2.3**



5. From the **Command Prompt** on **PC-B**, ping the **DEVASC Server** outside IPv4 address using command **ping 206.165.200.227**. The ping should now fail.



6.  From the **Web Browser** on **PC-B**, access the **DEVASC Server** web page at **http://209.165.200.227**. You should still see the web page, as you did not remove this **access-list** statement that allows HTTP access.

