Packet Tracer - Explorar una red simple

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Puerta de enlace predeterminada
R1	G0/0/0	209.165.200.225	255.255.255.248	N/D
	G0/0/1	10.1.1.2	255.255.255.252	
R3	G0/0/0	10.2.2.2	255.255.255.252	N/D
	G0/0/1	172.16.3.1	255.255.255.0	
FIREWALL	VLAN1	192.168.1.1	255.255.255.0	N/A
	VLAN2	209.165.200.226	255.255.255.248	
	VLAN3	192.168.2.1	255.255.255.0	
Servidor DEVASC	NIC	IN: 192.168.2.3	255.255.255.0	192.168.1.1
	VLAN1	OUT: 209.165.200.227	255.255.255.248	209.165.200.225
Servidor de ejemplo	NIC	64.100.0.10	255.255.255.0	64.100.0.1
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-B	NIC	172.16.3.2	255.255.255.0	172.16.3.1

Nota: Añadirá PC-A y PC-B a la topología en el paso 1.

Objetivos

Parte 1: Agregar equipos a la topología

Parte 2: Pruebe la conectividad a través de la red

Parte 3: Crear una página Web y verla

Parte 4: Examinar las listas de acceso del firewall

Aspectos básicos/Situación

Packet Tracer es una gran herramienta para construir y probar redes y equipos de red. Como desarrollador, es importante que esté familiarizado con los dispositivos de red y cómo se comunican entre sí. La red sencilla de esta actividad de Packet Tracer está preconfigurada para darle la oportunidad de explorar los dispositivos.

Nota: En esta actividad, los dos servidores web se denominan **Servidor DEVASC** y **Servidor de ejemplo**. En la topología, se nombran con su URL: **www.devasc-netacad.pka** y **www.example.com**.

Instrucciones

Parte 1: Agregar equipos a la topología

En esta parte, agregará equipos a la topología y los configurará con direcciones IPv4.

Paso 1: Coloque los equipos y conéctelos a la red.

Nota: Los nombres de los dispositivos distinguen entre mayúsculas y minúsculas. Si usa un nombre diferente, su puntuación se verá afectada.

a. Arrastre un PC al área de trabajo y colóquelo cerca de S2.

b. Cambie el nombre del PC como **PC-A**.

c. Arrastre un PC al área de trabajo y colóquelo cerca de S3.

d. Cambie el nombre del PC como **PC-B**.

e. Conecte un cable **recto de cobre** desde el puerto **FastEthernet0** de PC-A a cualquier puerto FastEthernet disponible en S2.

f. Conecte un cable **recto de cobre** desde el puerto **FastEthernet0** de PC-B a cualquier puerto FastEthernet disponible en S3.

Paso 2: Configure el direccionamiento IPv4 para los equipos.

a. Haga clic en **PC-A**.

b. Haga clic en **Desktop(Escritorio)**

c. Haga clic en **IP Configuration** (Configuración de IP).

d. Asigne la siguiente información de direccionamiento IPv4:

Dirección IPv4: 192.168.1.2

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1

e. Repita esto para PC-B, pero utilice la siguiente información de direccionamiento IPv4:

Dirección IPv4:172.16.3.2

Máscara de subred: 255.255.255.0

Gateway predeterminado: 172.16.3.1

f. En la ventana Instrucciones para esta actividad, el porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Check Results** (Verificar resultados) para saber cuáles son los componentes requeridos que aún no se completaron. El resto de esta actividad no se puntúa.

Parte 2: Prueba de conectividad a través de una red.

a. Haga clic en **PC-B**.

b. Haga clic en **Símbolo del sistema (command prompt)**.

c. Hacer ping a R3. Escriba **ping 172.16.3.1** (su puerta gateway predeterminado).

Es posible que tenga que emitir el comando un par de veces, pero debe comenzar a recibir respuestas del router.

d. Hacer ping al **servidor de ejemplo** en la dirección 64.100.0.10.

Es posible que tenga problemas inicialmente a medida que converja la red. Repita el ping si es necesario. Ahora se sabe que hay conectividad a través de Internet.

e. Hacer ping al **servidor DEVASC** en la dirección 209.165.200.227.

Es posible que tenga problemas inicialmente a medida que converja la red. Repita el ping si es necesario. Ahora sabe que tiene conectividad de extremo a extremo en toda la topología de red.

Parte 3: Crear una página Web y verla

En esta parte, creará una página web sencilla en el servidor DEVASC y, a continuación, verificará que PC-B pueda acceder a la página web.

Paso 1: Crear una página web.

a. Haga clic en el **servidor PT www.devasc-netacad.pka**.

b. Haga clic en **Servicios (Services)**.

c. En **Servicios**, el valor predeterminado es el primer servicio, que es HTTP. Haga clic en **Nuevo archivo (New file)**.

d. Asigne un nombre al archivo **index.html**.

e. Packet Tracer entiende el lenguaje de marcado de hipertexto básico (Hypertext Markup Language, HTML). Coloque el siguiente código html en el cuadro debajo del nombre del archivo. Si conoce HTML, no dude en personalizar el código.

```
<html>
<center><font size='+2' color='blue'>DevNet Associate</font></center>
<hr>¡Bienvenido al curso de NetAcad DEVASC!
```

f. Haga clic en **Guardar**. Haga clic en **Sí** a la advertencia.

Paso 2: Ver la página web.

a. Haga Clic en **PC-B**

b. Haga Clic en **Desktop(Escritorio)** Si es necesario, cierre la ventana **Command Prompt**.

c. Haga clic en **Web Browser (Navegador web)**.

d. Coloque la siguiente dirección en el cuadro URL: **http://209.165.200.227**.

Debería mostrarse su página web. Si no es así, verifique sus configuraciones y vuelva a intentarlo.

Parte 4: Modificar la lista de acceso de Firewall

En esta parte, examinaremos la lista de acceso del dispositivo firewall, editaremos la lista de acceso y comprobaremos que el firewall deniega ahora el acceso a ping.

Paso 1: Examine la lista de acceso en el dispositivo Firewall.

a. Haga clic en **Firewall**

b. Haga click en **CLI**.

c. Presione **Enter** un par de veces para obtener una línea de comandos.

d. Escriba **en** y presione **Enter**.

e. No hay contraseña. Vuelva a presionar la tecla **Enter**.

f. Escriba **show run** y presione **Enter**.

g. Presione la **barra espaciadora** para desplazarse por la configuración en ejecución.

h. Observe la siguiente lista de acceso:

```
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
```

El host 192.168.2.3 es la direeción ipv4 interna del servidor DEVASC en el DMZ.

- La primera instrucción **de lista de acceso** permite a cualquier dispositivo acceder al servidor mediante el Protocolo de mensajes de control de Internet (ICMP), que es el protocolo utilizado por el comando **ping**.
- La segunda instrucción de **lista de acceso permite que cualquier dispositivo acceda** al servidor mediante el Protocolo de transferencia de hipertexto (HTTP), que es el protocolo utilizado por los navegadores web.

i. Si es necesario, presione la **barra espaciadora** hasta que esté en el símbolo del sistema.

```
FIREWALL#
```

Paso 2: Modificar y probar la eficacia de la lista de acceso.

Normalmente, no desea que el mundo exterior pueda hacer ping a sus servidores internos. Por lo tanto, debe eliminar la instrucción de **lista de acceso** que permite explícitamente el acceso ping.

a. Ingrese al modo de configuración global con el **comando configure terminal.**

```
FIREWALL# configure terminal
```

b. Elimine la instrucción **access-list** que permite el ping con el siguiente comando y presione **Enter**.

Nota: El comando está en una línea aunque pueda verse ajustado en el terminal

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

c. Desde el **símbolo del sistema** en **PC-B**, haga ping al **servidor DEVASC** fuera de la dirección IPv4. El ping ahora debería fallar.

d. Desde el **Navegador Web** en **PC-B**, acceda a la página web del **servidor DEVASC** en **http://209.165.200.227**. Aún debería ver la página web, ya que no eliminó esta instrucción de **lista de acceso** que permite el acceso HTTP.