Aquí tienes el Laboratorio #20 sobre la configuración básica de routers y switches, diseñado para ser implementado en Cisco Packet Tracer.

Sesión #20: Configuración Básica de Routers y Switches

Duración: 2 Horas

Objetivos del Laboratorio:

En este taller, los participantes aprenderán a:

- Comprender los conceptos básicos de routers y switches.
- Configurar un router y un switch.
- Implementar medidas de seguridad básicas mediante ACLs.
- Asegurarse de que todos los componentes de la red están correctamente integrados y funcionando.

Materiales Necesarios:

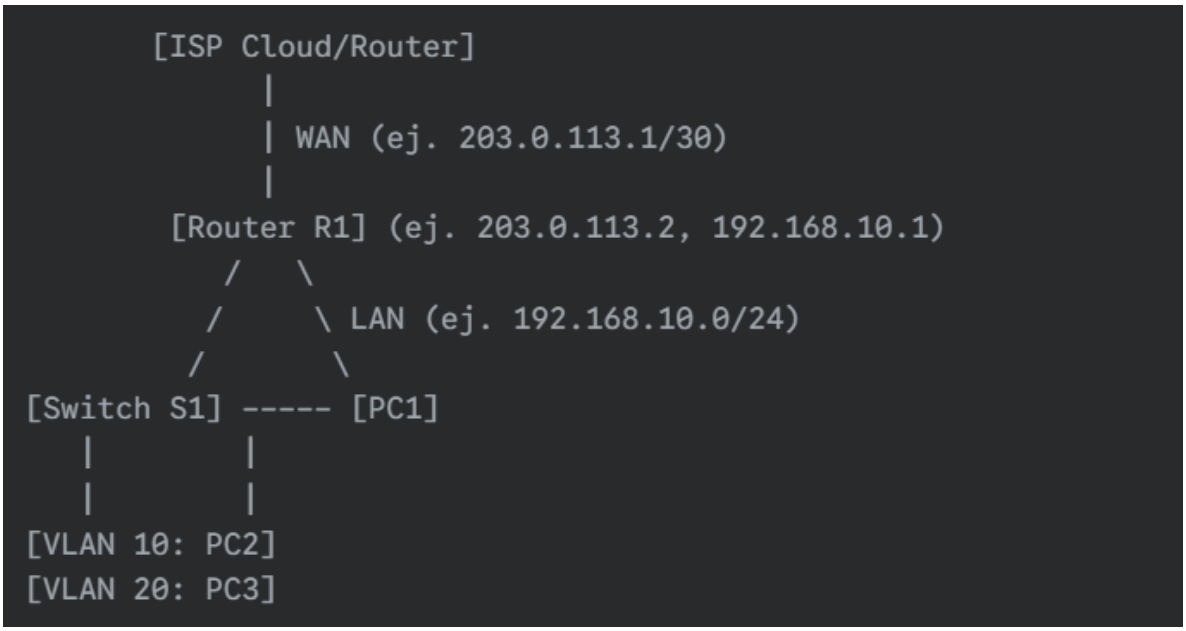
- Computador con acceso a internet.
- Cisco Packet Tracer instalado.
- Academia Cisco (Netacad.com): Para la actividad complementaria (aunque no se especifica una actividad complementaria para esta sesión, se incluye como un material general).
- GitHub: Para el repositorio (opcional, pero recomendado para la gestión de laboratorios).
- Manual del usuario: Este documento con instrucciones detalladas para cada paso del taller.

Estructura del Laboratorio:

Laboratorio 1:

Diagrama de Red a Implementar:

Para este laboratorio, crearemos una topología sencilla que simule una red interna conectada a una "Internet" simulada.



Esquema de Direccionamiento:

- **Red WAN (Simulada):**
  - Router R1 (interfaz externa): 203.0.113.2/30
  - Cloud/ISP: 203.0.113.1/30
- **Red LAN Interna:** 192.168.10.0/24
  - Router R1 (interfaz interna): 192.168.10.1/24
  - Switch S1 (VLAN de gestión): 192.168.10.2/24 (si se configura)
  - **VLAN 10 (Datos):** 192.168.10.0/24 (PCs en esta VLAN)
    - PC2: IP asignada por DHCP
    - PC3: IP asignada por DHCP
    - PC1: IP estática 192.168.10.10
  - Servidor Web (opcional para ACL): 192.168.10.50

Pasos del Taller:

• Introducción:

1. **Explicar los conceptos básicos de routers y switches:**
    - **Router:** Dispositivo de Capa 3 (red) que conecta diferentes redes y enruta el tráfico entre ellas basándose en direcciones IP. Toma decisiones de reenvío utilizando tablas de enrutamiento.
    - **Switch:** Dispositivo de Capa 2 (enlace de datos) que conecta dispositivos dentro de la misma red (LAN) y reenvía el tráfico basándose en direcciones MAC. Crea dominios de colisión separados para cada puerto.
2. **Presentar el diagrama de red que se implementará en el taller:** (El diagrama de arriba).
3. **Revisar los comandos básicos de configuración:**
    - enable: Pasa al modo privilegiado.
    - configure terminal: Pasa al modo de configuración global.
    - interface <tipo/numero>: Entra al modo de configuración de interfaz.
    - ip address <ip> <máscara>: Asigna una dirección IP a una interfaz.
    - no shutdown: Activa una interfaz.
    - exit: Sale del modo actual.
    - end: Sale al modo privilegiado.
    - show running-config: Muestra la configuración actual en la RAM.
    - copy running-config startup-config: Guarda la configuración en la NVRAM.

• Configuración del Router (R1):

1. **Montar el hardware en Packet Tracer:**
    - Arrastra un **Router (ej., 1941)**.
    - Arrastra un **Switch (ej., 2960)**.
    - Arrastra **tres PCs** (PC1, PC2, PC3).

- Arrastra una **Cloud (Nube)** y un **Cable Modem** para simular la conexión a Internet. Conecta el Cable Modem a la Cloud (puerto Coaxial) y luego al Router (puerto GigabitEthernet).
- Conecta el Router (GigabitEthernet0/0) al Switch (FastEthernet0/1).
- Conecta PC1, PC2, PC3 al Switch.
- (Opcional) Agrega un **Servidor HTTP** para probar la ACL más adelante. Conéctalo al Switch.

2. **Acceso al modo de configuración:**
    - **Conectar una computadora al puerto de consola del router:** En Packet Tracer, arrastra una **PC** y conéctala al **puerto de consola (Console)** del router usando un **cable de consola** (Console Cable - el cable azul).
    - **Utilizar un software de terminal para establecer una conexión:** En la PC, ve a **Desktop > Terminal**. Deja la configuración por defecto y haz clic en **OK**.
    - **Ingresar el modo de usuario y luego el modo de configuración global:**
    - Router> enable
    - Router# configure terminal
    - Router(config)# hostname R1
    - R1(config)#
3. **Asignación de direcciones IP:**
    - **Configurar la interfaz del router conectada a la LAN:**
    - R1(config)# interface GigabitEthernet0/0
    - R1(config-if)# ip address 192.168.10.1 255.255.255.0
    - R1(config-if)# no shutdown
    - R1(config-if)# description LAN_Interface
    - R1(config-if)# exit

- **Configurar la interfaz del router conectada a la "Internet" (simulada por la Nube/Cable Modem):**
    - Conecta el **Cable Modem** a la **Nube** (puerto Coaxial) y el **Cable Modem** al router (por ejemplo, GigabitEthernet0/1).
    - Configura la **Nube** para que el puerto Coaxial7 esté mapeado a un puerto Ethernet (ej. Ethernet6) que será donde se conectará el Cable Modem.
    - En el **Cable Modem**, no necesitas mucha configuración IP manual; obtendrá su IP de la "Nube".
    - **En el Router R1, configura la interfaz WAN:**
    - R1(config)# interface GigabitEthernet0/1
    - R1(config-if)# ip address 203.0.113.2 255.255.255.252 (Usando una /30 para la WAN)
    - R1(config-if)# no shutdown
    - R1(config-if)# description WAN_to_ISP
    - R1(config-if)# exit

Asegúrate de que el Cable Modem obtiene su IP (puede que necesites ir a la pestaña GUI del Cable Modem y verificar el estado).

4. **Configuración de DHCP en R1:**
    - **Configurar el servidor DHCP para asignar direcciones IP a los dispositivos conectados a la red LAN (VLAN 10 en este caso).**
    - R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.99 (Excluir IPs para dispositivos estáticos o de gestión)
    - R1(config)# ip dhcp pool LAN_POOL
    - R1(dhcp-config)# network 192.168.10.0 255.255.255.0
    - R1(dhcp-config)# default-router 192.168.10.1
    - R1(dhcp-config)# dns-server 8.8.8.8 (DNS público de Google)
    - R1(dhcp-config)# exit

- Configura PC2 y PC3 (y el servidor web si lo agregaste) para obtener IP por DHCP (en la pestaña Desktop -> IP Configuration -> DHCP).

5. **Configuración de NAT (Network Address Translation):**
    - **(Opcional) Configurar NAT para permitir que los dispositivos de la red interna accedan a Internet.**
    - R1(config)# ip access-list standard NAT_ACL
    - R1(config-std-nacl)# permit 192.168.10.0 0.0.0.255
    - R1(config-std-nacl)# exit
    -
    - R1(config)# interface GigabitEthernet0/0 (Interfaz interna)
    - R1(config-if)# ip nat inside
    - R1(config-if)# exit
    -
    - R1(config)# interface GigabitEthernet0/1 (Interfaz externa)
    - R1(config-if)# ip nat outside
    - R1(config-if)# exit
    -
    - R1(config)# ip nat inside source list NAT_ACL interface GigabitEthernet0/1 overload
    - R1(config)#

• Configuración del Switch (S1):

1. **Acceso al modo de configuración:**
    - **Conectar una computadora al puerto de consola del switch:** Similar al router, usa una PC y un cable de consola al puerto **Console** del Switch S1.
    - **Utilizar un software de terminal para establecer una conexión:** En la PC, ve a **Desktop > Terminal**.

- **Ingresar el modo de configuración global:**
- Switch> enable
- Switch# configure terminal
- Switch(config)# hostname S1
- S1(config)#

2. **Creación de VLANs:**
    - **Crear varias VLANs y asignarles nombres descriptivos.**
    - S1(config)# vlan 10
    - S1(config-vlan)# name DATA_VLAN
    - S1(config-vlan)# exit
    -
    - S1(config)# vlan 20
    - S1(config-vlan)# name VOICE_VLAN (Aunque no la usaremos, es para la práctica)
    - S1(config-vlan)# exit
    - **Asignar puertos a las VLANs creadas.**
        - Conecta PC2 a FastEthernet0/2 y PC3 a FastEthernet0/3. PC1 (estática) se queda en la VLAN por defecto (VLAN 1) o la asignas explícitamente a VLAN 10.
    - S1(config)# interface FastEthernet0/2
    - S1(config-if)# switchport mode access
    - S1(config-if)# switchport access vlan 10
    - S1(config-if)# exit
    -
    - S1(config)# interface FastEthernet0/3
    - S1(config-if)# switchport mode access
    - S1(config-if)# switchport access vlan 10

- S1(config-if)# exit

Para PC1 (192.168.10.10, estática), si no se asigna a VLAN 10, estará en la VLAN 1 (por defecto). Asegúrate de que los dispositivos en VLAN 10 obtienen IP del servidor DHCP.

3. **Configuración de trunking:**
    - **(Opcional) Configurar puertos de trunk para conectar el switch al router.**
        - Conecta el puerto FastEthernet0/1 del Switch S1 al GigabitEthernet0/0 del Router R1. Este puerto debe ser un trunk para llevar el tráfico de múltiples VLANs al router.
    - S1(config)# interface FastEthernet0/1
    - S1(config-if)# switchport mode trunk
    - S1(config-if)# switchport trunk encapsulation dot1q (Solo si el switch es de Capa 3 o modelos antiguos)
    - S1(config-if)# exit
    - **Configurar subinterfaces en el Router (Router-on-a-Stick):**
        - Esto permite al router enrutar entre VLANs.
    - R1(config)# interface GigabitEthernet0/0.10 (Subinterfaz para VLAN 10)
    - R1(config-subif)# encapsulation dot1Q 10
    - R1(config-subif)# ip address 192.168.10.1 255.255.255.0
    - R1(config-subif)# exit

(Nota: Si no se crearan más VLANs en el switch, no sería estrictamente necesario crear subinterfaces ni trunking en este escenario simple, ya que la VLAN 10 sería la única VLAN que contendría los hosts.) Para este laboratorio, con solo una VLAN en uso (VLAN 10 para DHCP), la configuración de subinterfaz en el router se aplica a la IP de la puerta de enlace por defecto para esa VLAN. La configuración del puerto troncal en el switch es necesaria para que el router reciba el tráfico etiquetado de la VLAN 10.

• Implementación de una ACL (Access Control List):

1. **Crear una ACL simple para restringir el acceso a un determinado servicio (por ejemplo, bloquear el acceso a un servidor web específico).**
    - **Agrega un Servidor HTTP** a tu red (ej. 192.168.10.50). Configúralo con el servicio HTTP activado.
    - La ACL bloqueará el acceso a este servidor desde PC2.
2. R1(config)# access-list 101 deny tcp host 192.168.10.20 host 192.168.10.50 eq 80 (Asumiendo PC2 obtiene IP 192.168.10.20)
3. R1(config)# access-list 101 permit ip any any
    - *Nota: La IP de PC2 será asignada por DHCP. Necesitarás verificar la IP real de PC2 (ipconfig en la PC) para que la ACL sea precisa, o usar el rango DHCP si quieres bloquear a todos en el rango.* Para simplicidad, asume que PC2 obtiene 192.168.10.100 (primera IP del DHCP pool).
4. R1(config)# access-list 101 deny tcp host 192.168.10.100 host 192.168.10.50 eq 80
5. R1(config)# access-list 101 permit ip any any
6. **Aplicar la ACL a una interfaz del router.**
    - La ACL debe aplicarse a la interfaz donde el tráfico que quieres filtrar entra o sale. Para bloquear PC2 de acceder al servidor, aplica la ACL in en la interfaz LAN.
7. R1(config)# interface GigabitEthernet0/0.10 (o GigabitEthernet0/0 si no usas subinterfaces)
8. R1(config-subif)# ip access-group 101 in
9. R1(config-subif)# exit

• Verificación de la Configuración:

1. **Utilizar los comandos show para verificar la configuración de los dispositivos.**
    - **En el Router (R1):**
    - R1# show ip interface brief

- R1# show ip dhcp pool
- R1# show ip nat translations
- R1# show access-lists
- **En el Switch (S1):**
- S1# show vlan brief
- S1# show interface trunk
- S1# show interface FastEthernet0/2 switchport

2. **Realizar pruebas de ping y traceroute para verificar la conectividad entre los dispositivos.**
    - Desde PC1 (estática) a PC2 (DHCP).
    - Desde PC2 a PC3.
    - Desde cualquier PC interna a la interfaz LAN del router (192.168.10.1).
    - Desde cualquier PC interna al Servidor Web (192.168.10.50).
    - Desde PC1/PC2/PC3 a 203.0.113.1 (ISP Cloud/Router). Esto debería funcionar gracias al NAT.
    - Realiza un traceroute desde una PC interna a una dirección IP externa (ej. 8.8.8.8) para ver la ruta.
3. **Verificar el funcionamiento de la ACL.**
    - Desde PC2 (la IP bloqueada por la ACL), intenta acceder al Servidor Web (192.168.10.50) usando el navegador web en la PC. Debería fallar.
    - Desde PC1 (la IP no bloqueada por la ACL), intenta acceder al Servidor Web. Debería tener éxito.
    - En el Router R1, ejecuta show access-lists 101 para ver los "matches" (coincidencias) de la ACL, lo que indicaría que el tráfico fue denegado.