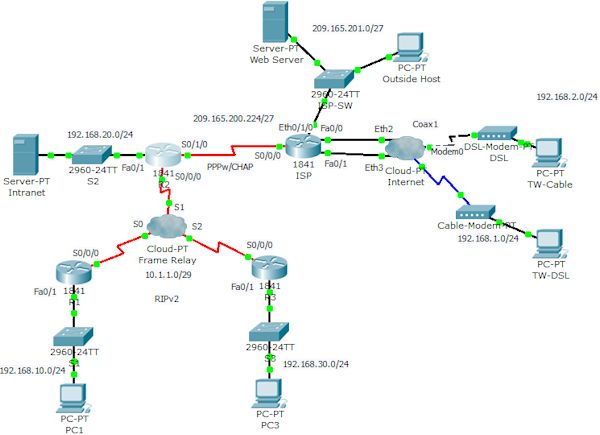
**Practica: Packet Tracer 6.4.1 Desafío de Integración de Habilidades**



**Tarea 1: Aplicar configuraciones básicas del Router**

**Tarea 2: Configurar el enrutamiento dinámico y predeterminado**  **Paso 1. Configurar el enrutamiento por defecto.**   
R2 necesita una ruta predeterminada. Utilizar el argumento de interfaz de salida en la configuración de ruta por defecto.

R2 (config) # ip ruta 0.0.0.0 0.0.0.0 S0 / 1/0

**Paso 2. Configurar el enrutamiento dinámico.**   
Configurar RIPv2 en R1, R2 y R3 para todas las redes disponibles. R2 tiene que pasar su configuración de red por defecto para los otros Routers. También, asegúrese de utilizar el comando passive-interface en todas las interfaces activas que no se utilizan para el enrutamiento.

R1(config)#router rip   
R1(config-router)#version 2   
R1(config-router)#network 10.1.1.0   
R1(config-router)#network 192.168.10.0   
R1(config-router)#passive-interface f0/1   
R1(config-router)#no auto-summary   
R1(config-router)#exit

R2(config)#router rip   
R2(config-router)#version 2   
R2(config-router)#network 10.1.1.0   
R2(config-router)#network 192.168.20.0   
R2(config-router)#default-information originate   
R2(config-router)#passive-interface s0/1/0   
R2(config-router)#passive-interface f0/1   
R2(config-router)#no auto-summary   
R2(config-router)#exit

R3(config)#router rip   
R3(config-router)#version 2   
R3(config-router)#network 10.1.1.0   
R3(config-router)#network 192.168.30.0   
R3(config-router)#passive-interface f0/1   
R3(config-router)#no auto-summary   
R3(config-router)#exit

**Tarea 5: Aplicar políticas de ACL**

**Paso 1. Crear y aplicar seguridad 1 número de póliza.**   
Aplicar las siguientes reglas ACL ACL utilizando el número 101: Permitir que los hosts de la red 192.168.30.0/24 acceso a la Web a cualquier destino. Permitir que los hosts de la red 192.168.30.0/24 ping de acceso a cualquier destino. Negar cualquier otro acceso de origen de la red.

R3(config)#access-list 101 permit tcp 192.168.30.0 0.0.0.255 any eq www   
R3(config)#access-list 101 permit icmp 192.168.30.0 0.0.0.255 any   
R3(config)#access-list 101 deny ip any any   
R3(config)#int fa0/1   
R3(config-if)#ip access-group 101 in   
R3(config-if)#exit

**Paso 2. Crear y aplicar seguridad 2 número de póliza.**   
Debido ISP representa la conectividad a Internet, configurar una ACL llamada CORTAFUEGOS llamado en el siguiente orden: Permitir TW-DSL acceso web al servidor de Intranet. Permitir TW-TV por cable Servicio Web al servidor de Intranet. Permitir que sólo se entrante de estas respuestas de los ISP y más allá de cualquier fuente ISP. Permitir sesiones TCP sólo se establece a partir de cualquier fuente de ISP y más allá de ISP. Explícitamente bloquear todos los demás accesos entrantes de ISP y más allá de cualquier fuente ISP.

R2(config)#ip access-list extended FIREWALL   
R2(config-ext-nacl)#permit tcp host 192.168.1.10 host 192.168.20.254 eq www   
R2(config-ext-nacl)#permit tcp host 192.168.2.10 host 192.168.20.254 eq www   
R2(config-ext-nacl)#permit icmp any any echo-reply   
R2(config-ext-nacl)#permit tcp any any established   
R2(config-ext-nacl)#deny ip any any   
R2(config-ext-nacl)#int s0/1/0   
R2(config-if)#ip access-group FIREWALL in   
R2(config-if)#exit

**Conclusiones**

En esta práctica se puede concluir que el uso de ACLs extendidas es muy útil para administración de redes pues nos permite tener un control total sobre la misma, esto es importante en cualquier empresa u organización pues la seguridad en las redes en un punto muy importante.