Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

ACL, DHCP, NAT, PAT

Módulo 9: **Mantenimiento de redes de acceso y banda ancha.**

Telecomunicaciones

Perfil de Egreso - Objetivos de Aprendizaje de la Especialdad

Módulo 1

OA1 Leer y utilizar esquemas, proyectos y en general todo el lenguaje simbólico asociado a las operaciones de montaje y mantenimiento de redes de telecomunicaciones.

Módulo 2

OA6 Realizar mantenimiento y reparaciones menores en equipos ysistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.

OA7 Aplicar la normativa y los implementos de seguridad y protección relativos almontaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.

Módulo 3

OA2 Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción, y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.

OA10 Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo a los requerimientos de los usuarios.

Módulo 4

OA9 Detectar y corregir fallas en circuitos de corriente continua de acuerdo a los requerimientos técnicos y de seguridad establecidos.

Módulo 5

OA2 Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.

OA4 Realizar medidas y pruebas de conexión y de continuidad de señal eléctrica, de voz, imagen y datos- en equipos, sistemas y de redes de telecomunicaciones, utilizando instrumentos de medición y certificación de calidad de la señal autorizada por la normativa vigente.

Módulo 6

OA8 Instalar y configurar una red inálambrica según tecnologías y protocolos establecidos.

OA7 Aplicar la normativa y los implementos de seguridad y protección relativos al montaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.

Módulo 7

OA5 Instalar y configurar una red de telefonía (tradicional o IP) en una organización según los parámetros técnicos establecidos.

Módulo 8

OA3 Instalar y/o configurar sistemas operativos en computadores o servidores con el fin de incorporarlos a una red laN, cumpliendo con los estándares de calidad y seguridad establecidos.

Módulo 9

OA10 Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo, a los requerimientos de los usuarios.

OA6 Realizar el mantenimiento y reparaciones menores en equipos y sistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.

Módulo 10

No está asociado a Objetivos de Aprendizaje de la Especialidad (AOE), sino a genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.	**B-** Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.	**C-** Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.
D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.	**E-** Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.	**F-** Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.
G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.	**H-** Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.	**I-** Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.
J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.	**K-** Prevenir situaciones de riesgo y enfermedades ocupasionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.	**L-** Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.

Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información
1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.
2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas
1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o funcion.
2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.
3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos
1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.
2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.
3. Identifica y aplica procedimientos y técnicas específicas de una función de acuedo a parámetros establecidos.

4. Comunicación
4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros
1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía
1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.
2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.
3. Evalua el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.
4. Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad
1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.
2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.
3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.
4. Actúa acorde al marco de sus conocimientos. experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos
1. Demuestra conocimientos especificos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.

Metodología seleccionada

Aprendizaje Basado en Problemas (ABP)

- Esta presentación les ayudará a poder comprender los conceptos necesarios para el desarrollo de su actividad

Aprendizaje Esperado

- **AE4.** Resuelve problemáticas de funcionamiento de conectividad entre redes ejecutando las tareas de detectar, mantener y administrar los equipos, según parámetros de calidad y seguridad, cumpliendo con los estándares de la industria y los protocolos de seguridad establecidos (según ANSI/TIA o ETSI, etc.).

¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

Configurar listas de control de acceso para la seguridad perimetral en una red, configurar servicio DHCP para obtener direccionamiento IPv4 e IPv6 automático en los hosts de la red y establecer mecanismos de traducción de direcciones IP (NAT y PAT).

Contenidos

01 Listas de control de acceso (ACL)

- ¿Qué son las listas de control de acceso?
- Wildcard.
- Calcular wildcard.
- Comodín host y any.
- Tipos de ACLS.
- Aplicación de las ACL.
- Topología ejemplo.
- ACL estándar numerada.
- Ejemplo de ACL estándar numerada.
- ACL estándar nombrada.
- Ejemplo de ACL estándar nombrada.
- Verificar las ACLS aplicadas.
- Editar las ACL.
- Restringir acceso remoto en la VTY.

Contenidos

02 DHCPv4 y v6 «

- ¿Qué es DHCP?
- Funcionamiento de DHCP.
- Configuración de cliente DHCP.
- Retransmisión DHCPv4 y v6.
- Configuración de DHCPv6.
- Retransmisión DHCPv6.

Contenidos

03 NAT (Traducción de direcciones de red) y PAT (Traducción de Direcciones de Puertos)

- ¿Qué es NAT?
- Tipos de NAT
- NAT estático.
- NAT dinámico.
- ¿Qué es PAT?
- Asignación de direcciones IP desde el ISP.
- PAT con una dirección IPv4 publica.
- Revisar PAT.
- PAT con múltiples direcciones IPv4 publicas.
- Revisar PAT.

Te has preguntado alguna vez:

¿Por qué debemos dar seguridad a una red de equipos?

¿Qué tendríamos que hacer para dar una mayor seguridad?

Listas de control de acceso (ACL)

¿Qué son las listas de control de acceso?

- Las listas de control de acceso (ACL) son una serie de comandos que nos ayudarán a filtrar (permitir o denegar) paquetes que circula por un router. Cabe destacar que las ACLS no vienen configuradas de forma predeterminada en los router, sino que hay que configurar y aplicar según los requerimientos de seguridad que se necesiten en la red.

Wildcard

01 Para el uso de ACL se utilizan las máscaras wildcard, que se conoce como máscara inversa o máscara comodín, cuando el valor de la máscara comodín se transforma a binario, sus resultados determinarán cuales son los bits de las direcciones que se deben considerar para el procesamiento del tráfico. Donde los ceros indican los bits que se deben considerar y los unos, los que se deben descartar:

02

		OCTETO1	OCTETO2	OCTETO3	OCTETO4
IP	192.168.1.0	11000000	10100000	00000001	00000000
MASCARA	255.255.255.0	11111111	11111111	11111111	00000000
WC	0.0.0.255	00000000	00000000	00000000	11111111

03 Esto significa que la máscara coincide con 192.168.1 y las última parte se descarta, por lo tanto, podemos decir que las direcciones IPS que se procesaran son 192.168.1.0 a 192.168.1.255

Wildcard

- Un método abreviado para calcular las wildcard es restar la máscara de red a 255.255.255.255.

255.255.255.255 255.255.255.0
0 .0 .0 .255

255.255.255.255 255.255.255.252
0 .0 .0 . 3

255.255.255.255 255.255.255.240
0 .0 .0 . 15

Comodín host y any

- **Permitir o denegar un IP específico:** **172.16.0.1 0.0.0.0.** Se puede abreviar como **host 172.16.0.1.**

- **Permitir o denegar a cualquiera:** **0.0.0.0 255.255.255.255.** Se puede abreviar como **any.**

Tipos de ACL

Existen dos tipos de ACL:

1. *ACL estándar.*
2. *ACL extendida.*

En esta actividad conoceremos y aplicaremos las ACL estándar, para luego utilizarlas con otros tipos de servicios que lo requieran.

Dentro de las ACL estándar existen dos tipos:

1. *ACL estándar numerada.*
2. *ACL estándar nombrada.*

Ambas las revisaremos en detalle para poder realizar correctamente nuestras actividades prácticas, filtrando información en el router.

ACL estándar numerada

- **Sintaxis de la ACL numerada:**

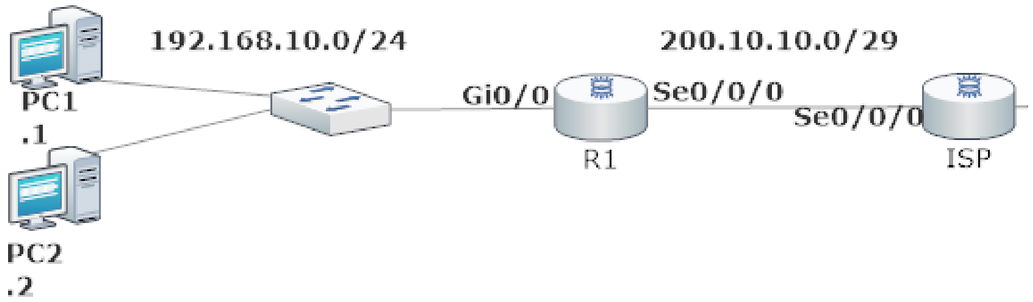
Para poder crear una ACL debemos utilizar el comando access-list.

Router(config)#access-list NúmeroDeACL {permit | deny | remark texto} origen [Wilcard de origen] [log]

- **Numero de ACL:** el rango utilizado para las ACL estándar es de 1 a 199.
- **Permit:** permite acceso si hay coincidencias con las ACL.
- **Deny:** deniega el acceso si hay coincidencias con la ACL.
- **Remark:** ingreso de información para poder documentar.
- **Origen:** identifica la IP de un host o la IP de una red que debemos filtrar.
- **Wildcard:** mascara wildcard para aplicar al origen.
- **Log:** envía un mensaje cuando hay coincidencia en las ACLS.

Ejemplo ACL estándar numerada

- Como ejemplo, denegaremos el PC2 pueda salir hacia internet y los demás hosts de la red puedan salir sin problemas. Realizaremos el ejercicio tanto para ACL estándar numerada como nombrada para que verifiquen la forma la cual se aplican.



- **10.0.0.0/24**

Ejemplo ACL estándar numerada

- A continuación, podemos observar que se acaba de denegar el acceso a un host de la red 192.168.10.0/24 y para que estas ACLS funcionen, necesitamos ingresar a la interfaz y aplicamos nuestra ACL del grupo 1 con filtro en la salida de esa interfaz.

Para verificar nuestra ACL utilizaremos el comando show **access-list.**

```
Router(config)#access-list 1 remark RESTRINGIR EL ACCESO AL HOST 192.168.10.2
Router(config)#access-list 1 deny host 192.168.10.2
Router(config)#access-list 1 permit 192.168.10.0 0.0.0.255
Router(config)#interface se0/0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Standard IP access list 1
    10 deny host 192.168.10.2
    20 permit 192.168.10.0 0.0.0.255

Router#
```

ACLS

Aplicación de las ACL

Verificación

ACL estándar nombrada

- **Sintaxis de la ACL nombrada:**

1. *Router(config)#ip access-list {estándar | extendida} nombre.*

2. *Router(config-std-nacl)#{permit | deny | remark} origen.*

Ejemplo de ACL estándar nombrada

- Realizamos el mismo ejercicio para denegar un host de la red 192.168.10.0/24 donde utilizamos una ACL nombrada DENEGAR_HOST y luego aplicamos la ACL en la interfaz serial como filtro de paquetes de salida.

  Finalmente, utilizamos el comando para verificar las ACL ingresadas.

```
Router(config)#ip access-list standard DENEGAR_HOST
Router(config-std-nacl)#deny host 192.168.10.2
Router(config-std-nacl)#permit 192.168.10.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#interface se0/0/0
Router(config-if)#ip access-group DENEGAR_HOST out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Standard IP access list DENEGAR_HOST
    10 deny host 192.168.10.2
    20 permit 192.168.10.0 0.0.0.255

Router#
```

ACL

Aplicación

Verificación

Ejemplo de ACL estándar nombrada

- En el host que denegamos el acceso para salir de la red, intentamos salir a una red remota que está en otro router y nos indicó que el destino era inaccesible. Por lo tanto la ACL fue correctamente aplicada. Por otra parte, revisando las ACLS en el router, nos indica que tuvieron coincidencias, tanto con el bloqueo del host, como con los permiso de los demás hosts de la red a otros destinos.

```
   IPv4 Address. . . . . . . . . . . : 192.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : ::
                                       192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : ::
   IPv6 Address. . . . . . . . . . . : ::
   IPv4 Address. . . . . . . . . . . : 0.0.0.0
   Subnet Mask . . . . . . . . . . . : 0.0.0.0
   Default Gateway . . . . . . . . . : ::
                                       0.0.0.0

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
```

```
Router#show access-list
Standard IP access list DENEGAR_HOST
    10 deny host 192.168.10.2 (16 match(es)) ←
    20 permit 192.168.10.0 0.0.0.255 (4 match(es)) ←

Router#
```

Editar las ACL

- Para poder editar veremos algunas alternativas que nos podrían ayudar:

1. **Utilizando un editor de texto**

Copie las ACLS creadas en el sistema y llévelas a un editor de texto. Luego elimine las ACLS con el comando no acces-list NumSecuencia, edite las ACL en el editor. Finalmente las copia y las pega en la consola en configuración global.

```
Router#show running-config | section access-list
access-list 1 deny host 192.168.10.2
access-list 1 permit 192.168.10.0 0.0.0.255
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Router(config)#no access-list 1
Router(config)#access-list 1 deny host 192.168.10.3
Router(config)#access-list 1 permit 192.168.10.0 0.0.0.255
Router(config)#
```

Copiar las ACL

Eliminar las acl

Pegar las ACLS editadas

Editar las ACLS

2. **Utilizando el número de secuencia.**

Revisaremos las ACLS creadas, luego entraremos a nuestra lista de acceso estándar y luego eliminaremos la línea que necesitamos modificar, para finalmente ingresar el número de secuencia con el nuevo cambio.

```
Router#show access-list
Standard IP access list 1
    10 deny host 192.168.10.2
    20 permit 192.168.10.0 0.0.0.255

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list standard 1
Router(config-std-nacl)#no 10
Router(config-std-nacl)#10 deny host 192.168.10.3
Router(config-std-nacl)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Standard IP access list 1
    10 deny host 192.168.10.3
    20 permit 192.168.10.0 0.0.0.255

Router#
```

ACLS en el sistema

Eliminar las acl

Revisar los nuevos cambios

Restringir el acceso remoto en la VTY

- Para restringir el acceso a las conexiones remotas, realizamos nuestras ACLS que nos permitirán definir quienes podrán ingresar a la VTY, luego las aplicamos con access-class más el numero de ACLS de entrada al dispositivo.

```
R1(config)#access-list 1 permit host 192.168.10.3
R1(config)#access-list 1 deny any
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#access-class 1 in
R1(config-line)#exit
```

ACLS

Aplicamos la ACL

```
   IPv4 Address.....................: 192.168.10.3
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: ::
                                      192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway..................: ::
                                      0.0.0.0

C:\>ssh -l ADMIN 192.168.10.1

Password:



R1#
```

- Ahora estamos en condiciones de poder aplicar las ACLS estándar numeradas, nombradas y dar seguridad de acceso a nuestras conexiones remotas.

- En esta ocasión restringimos el acceso a través de SSH hacia nuestro router para obtener acceso remoto desde algún equipo específico.

Reflexionemos

A partir de estos conocimientos, ¿Cómo podrías dar mayor seguridad a la red de tu casa o la red de la empresa de un amigo o amiga?

Configuración de servicio DHCP.

¿Qué es DHCP?

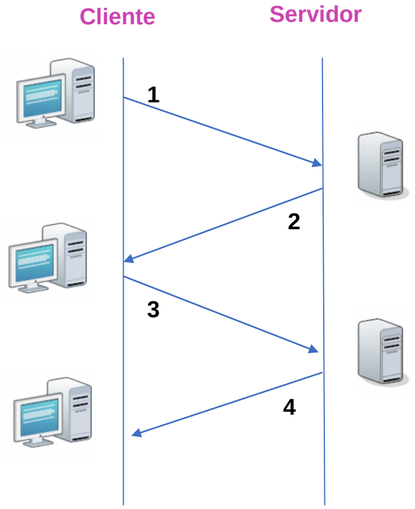
- DHCP significa protocolo de configuración de host dinámico y es utilizado para poder asignar direccionamiento IP de forma automática a los hosts de una red, simplificando la administración de direccionamiento IP en las redes.

Los datos asignados a un host pueden ser lo siguientes:

- **Dirección IP y máscara de subred.**
- **Dirección IP de Servidor DNS.**
- **Dirección IP de puerta de enlace.**
- **Nombre de un dominio.**

Funcionamiento DHCPv4

1. El cliente hace un broadcast de un mensaje de descubrimiento solicitando una IP.
2. El servidor manda un broadcast con un mensaje de oferta de un a dirección IP.
3. El cliente responde con un mensaje de aceptando la dirección IP.
4. El servidor hace acuse de recibo de la aceptación de la dirección IP del cliente.



Configuración de DHCPv4

- Podemos excluir direcciones que no se necesite asignar a los hosts y estarán reservadas.

  Asignaremos un nombre al pool de direcciones que se asignan a los dispositivos de la red.

```
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
Router(config)#ip dhcp excluded-address 192.168.10.254
Router(config)#ip dhcp pool NOMBRE-POOL
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 192.168.10.10
Router(dhcp-config)#domain-name dominio.cl
Router(dhcp-config)#exit
Router(config)#
```

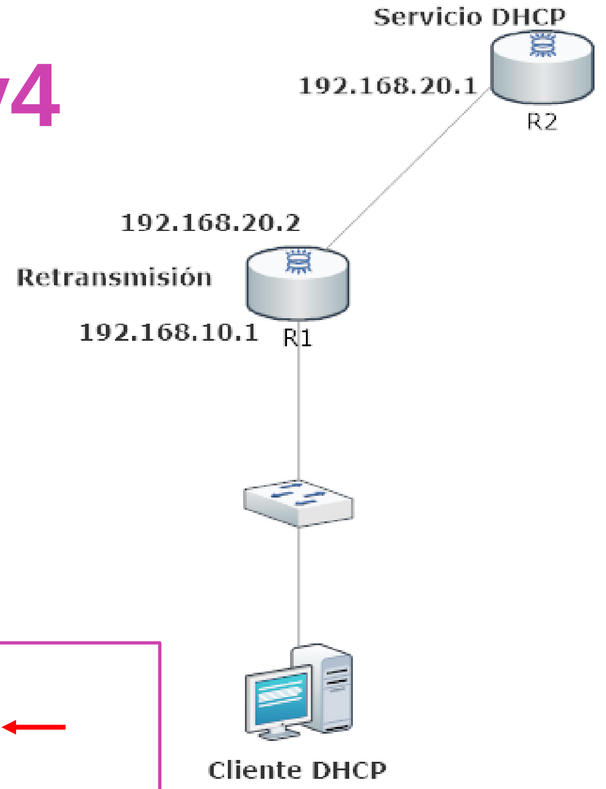
Configuración de cliente DHCPv4

- Debemos entrar a la interfaz que necesitamos que adquiera dirección IP por dhcp e ingresamos **IP address dhcp**, habilitamos la interfaz y debería asignar la dirección como se observa en la imagen.


```
Router(config)#interface gi0/1
Router(config-if)#ip address dhcp
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/1 assigned DHCP address 200.0.0.2, mask
255.255.255.252, hostname Router0


Router(config-if)#do show ip interface gi0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 200.0.0.2/30
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  MTU is 1500 bytes
```

Retransmisión de DHCPv4

- Reenvía difusiones de DHCPv4 a un servidor con DHCPv4, para que puedan obtener direccionamiento IP los clientes locales. Para habilitarlo, debemos ingresar a la interfaz, la cual tiene a dirección de Gateway de la red que necesita dhcp y digitamos el comando **ip helper-address IP_SERVIDOR_DHCP**.




```
Router(config)#interface gi0/0
Router(config-if)#ip helper-address 192.168.20.1
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip interface gi0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.20.1
  Directed broadcast forwarding is disabled
```

Configuración de DHCPv6 con estado

El servicio DHCPv6 con estado funciona muy similar al de IPv4, el cual asignará direccionamiento IP a nuestros clientes de la red.

Habilitamos el servicio routing para IPv6 y realizamos nuestro Pool DHCPv6. Para finalizar habilitamos el servicio en la interfaz, la cual está conectada a los clientes que necesiten IP por DHCPv6.

```
Router(config)#Ipv6 unicast-routing
Router(config)#ipv6 dhcp pool POOL-IPV6
Router(config-dhcpv6)#address prefix 2001:1234:ABCD:1::/64
Router(config-dhcpv6)#dns-server 2001:1234:ABCD:2::10
Router(config-dhcpv6)#domain-name dominio.cl
Router(config-dhcpv6)#exit
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#ipv6 address 2001:1234:ABCD:1::1/64
Router(config-subif)#ipv6 nd managed-config-flag
Router(config-subif)#ipv6 dhcp server POOL-IPV6
Router(config-subif)#
```

Configuración de cliente DHCPv6

- Para configurar una interfaz de un router para que pueda recibir parámetros de red, debemos habilitar ipv6 en la interfaz y configurar la IP con dhcp.


```
Router(config)#interface gi0/1
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address dhcp
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ipv6 interface gi0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::201:63FF:FE15:3A02
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:AAA:2222:2:70A2:621F:621F:621F, subnet is 2001:AAA:2222:2::/64
  Joined group address(es):
```

Retransmisión de DHCPv6

- Reenvía difusiones de DHCPv6 a un servidor con DHCPv6, para que puedan obtener direccionamiento IP los clientes locales. Para habilitarlo debemos digitar el comando **ipv6 dhcp server NOMBRE_POOL_SERVER.**

  En el caso de dispositivos físicos, digitar **ipv6 dhcp relay destination DIR_IPV6_SERVER**

```
Router(config)#interface gi0/0
Router(config-if)#ipv6 dhcp server POOL
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ipv6 dhcp interface
GigabitEthernet0/0 is in server mode
  Using pool: POOL
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit: disabled
Router#
```

Reflexionemos

¿En qué ocasiones se necesita retransmitir el servicio DHCP? ¿Por qué?

NAT(Traducción de direcciones de red) y PAT (Traducción de Direcciones de Puertos)

¿Conoces los conceptos de NAT y PAT?

¿Te imaginas para qué podrían servir?

¿Qué es NAT?

NAT (Network Address Translation) es traducción de direcciones de red. Conserva las direcciones IPv4 públicas. Esto se logra al permitir que las redes utilicen direcciones IPv4 privadas en nuestra LAN y proporciona la traducción a una dirección pública para salir a internet. También podemos decir que NAT nos puede proporcionar seguridad y privacidad al ocultar las direcciones IP internas de las externas.

Tipos de NAT

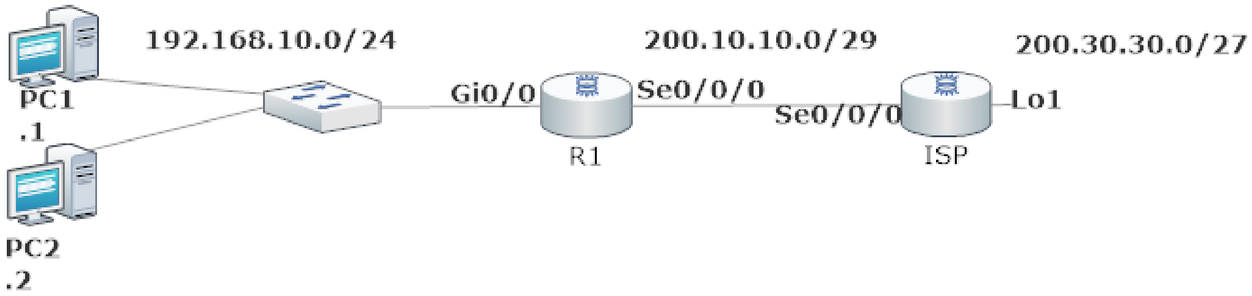
- **NAT estático:** permite que una dirección IP privada se traduzca a una dirección IP pública. Este modo de funcionamiento permite a un host de la red LAN poder ser visible de una conexión externa desde internet.

- **NAT dinámico:** permite a un router que pueda tener múltiples direcciones IP públicas, de esta manera cada dirección IP privada utilizará una dirección IP pública disponible por el router.

- **PAT:** conocido como NAT con sobrecarga, también traduce las direcciones privadas a direcciones públicas, asignando puertos de conexión al salir a internet.

NAT estático

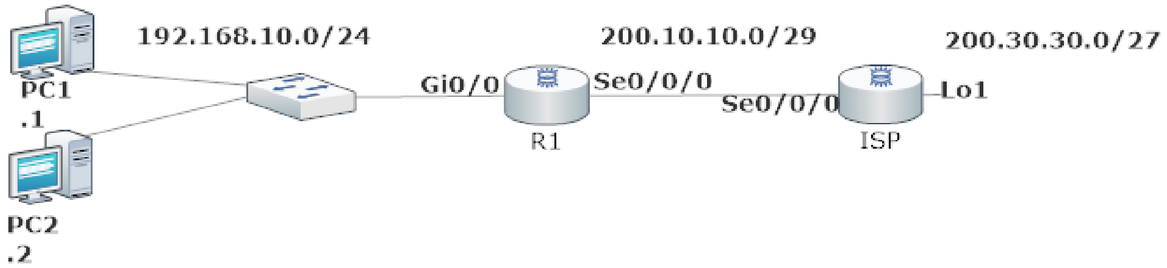
- Podremos indicar estáticamente que un equipo pueda salir a internet a través de una dirección IPv4 pública.




```
Router(config)#ip nat inside source static 192.168.10.2 200.10.10.1
Router(config)#interface gi0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se0/0/0
Router(config-if)#ip nat outside
Router(config-if)#
```

NAT dinámico

- Podemos indicar que la red 192.168.10.0/24 podrá tender permisos para salir a internet, utilizando diferentes direcciones IP públicas indicados por el NAT dinámico.




```
Router(config)#ip nat pool RANGO_PUBLICO 200.10.10.2 200.10.10.4 netmask 255.255.255.248
Router(config)#access-list 1 permit 192.168.10.0 0.0.0.255
Router(config)#ip nat inside source list 1 pool RANGO_PUBLICO
Router(config)#interface gi0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

¿Qué es PAT?

- **PAT** (**Port Address Translation**) Traducción de Direcciones de Puertos, es conocido como NAT con sobrecarga, nos permite que se pueda utilizar una dirección IPv4 pública para múltiples direcciones IP privadas internas.

  Cuando se utiliza este tipo de traducción, el router mantiene bastante información de los números de puertos TCP o UDP, que asignará a medida que soliciten salir a internet con una dirección IP pública, asignando a cada conexión un puerto asociado al servicio el cual quieran alcanzar.

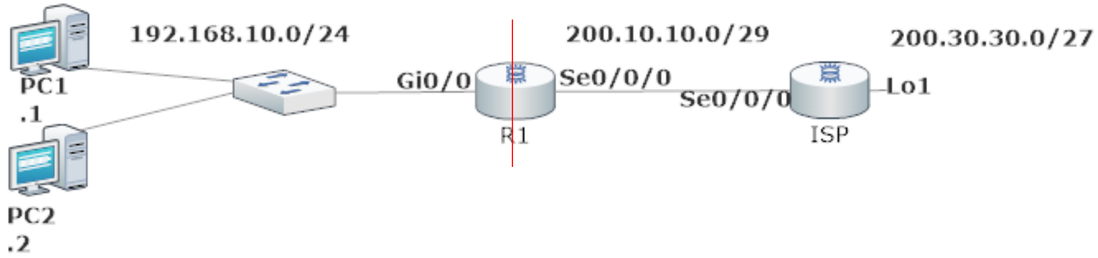
Asignación de direcciones IP desde el ISP

Existen dos formas de configurar PAT, dependiendo de cómo los ISP asignen las direcciones IP públicas a sus clientes:

- Asignar una única dirección IP pública.
- Asignar múltiples direcciones IP públicas.

PAT con una dirección IPv4 pública

- Todos los host de la red 192.168.10.0/24 podrán enviar su trafico de red a través de la interfaz se0/0/0 que tiene la IP publica 200.10.10.1/29 y el trafico se identificara a través de un número de puerto asignado habilitado por el comando **overload.**




```
R1(config)#ip nat inside source list 1 interface se0/0/0 overload
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface gi0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface se0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
```

Asignación de interfaz de entrada y salida para el NAT con sobrecarga

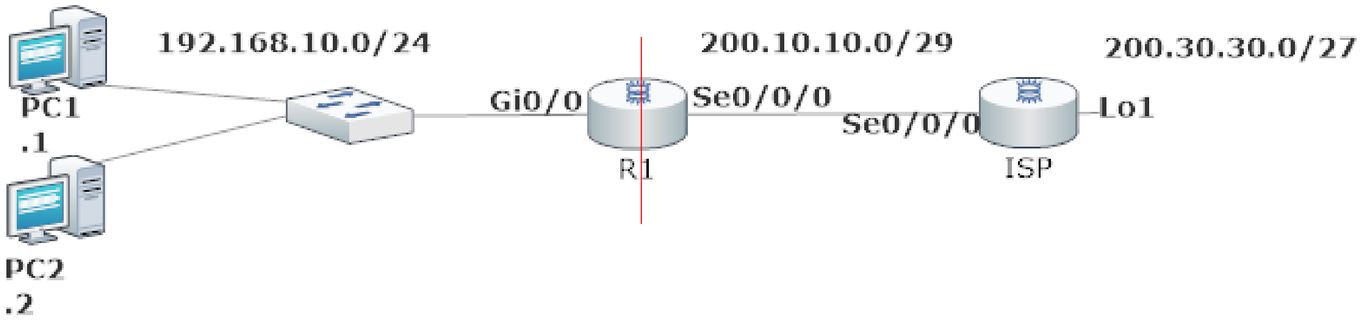
Revisar PAT

- Para poder revisar la configuración debemos digitar el comando **show ip nat translation.** Donde a través de un ping hacia una IP que simula la conexión a internet al momento de salir de nuestro router, comenzó a asignarle un puerto a nuestra dirección IP pública asignada por el ISP.

```
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.10.10.1:1     192.168.10.2:1     200.30.30.1:1      200.30.30.1:1
icmp 200.10.10.1:2     192.168.10.2:2     200.30.30.1:2      200.30.30.1:2
icmp 200.10.10.1:3     192.168.10.2:3     200.30.30.1:3      200.30.30.1:3
icmp 200.10.10.1:4     192.168.10.2:4     200.30.30.1:4      200.30.30.1:4

R1#
```

PAT con multiples direcciones IPv4 públicas

- El POOLNAT permitirá que la red 192.168.10.0/24 pueda realizar la traducción de direcciones IP con el rango dado por el ISP y el tráfico se identificará a través de un número de puerto asignado, habilitado por el comando **overload.**




```
R1(config)#ip nat pool POOLNAT 200.10.10.5 200.10.10.10 netmask 255.255.255.224
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#ip nat inside source list 1 pool POOLNAT overload
R1(config)#interface gi0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interfac se0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
```

Asignación de interfaz de entrada y salida para el NAT con sobrecarga

Revisar PAT

- Al realizar un ping desde dos PCS hacia una IP que simula la conexión a internet, al momento de salir de nuestro router, comenzó a asignar un puerto a una de las direcciones IP asignada en el rango entregado por ISP.

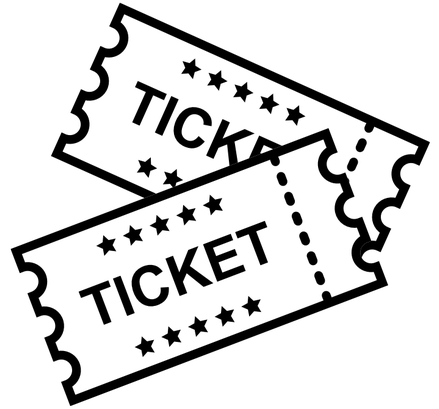
```
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.10.10.5:10    192.168.10.2:10    200.30.30.1:10     200.30.30.1:10
icmp 200.10.10.5:11    192.168.10.2:11    200.30.30.1:11     200.30.30.1:11
icmp 200.10.10.5:12    192.168.10.2:12    200.30.30.1:12     200.30.30.1:12
icmp 200.10.10.5:1     192.168.10.3:1     200.30.30.1:1      200.30.30.1:1
icmp 200.10.10.5:2     192.168.10.3:2     200.30.30.1:2      200.30.30.1:2
icmp 200.10.10.5:3     192.168.10.3:3     200.30.30.1:3      200.30.30.1:3
icmp 200.10.10.5:4     192.168.10.3:4     200.30.30.1:4      200.30.30.1:4
icmp 200.10.10.5:9     192.168.10.2:9     200.30.30.1:9      200.30.30.1:9

R1#
```

Reflexionemos

¿Cuál es la diferencia de NAT y PAT en la aplicación de un router?

¿Alguna duda que aclarar?

Ticket de salida



01

¿Qué son, para qué sirven y cómo se configuran las listas de control de acceso?

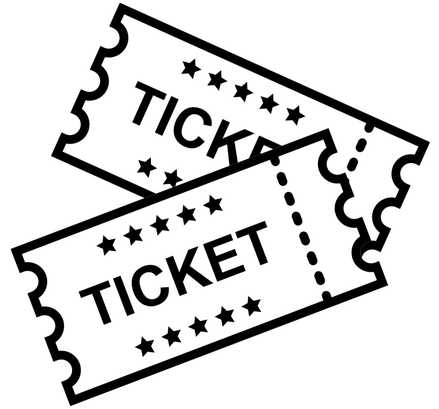
02

¿Podrías aplicar los conocimientos de servicios de DHCP en los dispositivos de red en una situación práctica?

03

¿Cuáles son los pasos para aplicar NAT y PAT en los routers? ¿Qué problemas se podrían presentar en este contexto? ¿Qué solución aplicarías?

Ticket de salida



04

¿Qué contenido fue el que más te costó entender? ¿Qué harías para tener una mejor comprensión de ese contenido?

05

¿Qué debilidades percibiste en tu desempeño durante el desarrollo de la actividad?

¿Cómo puedes trabajarlas para convertirlas en fortalezas?

Referencias

- https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html
- https://study-ccna.com/configure-cisco-router-as-dhcp-server/
- https://ccnadesdecero.es/configuracion-dhcpv6-con-estado/
- https://ccnadesdecero.es/configuracion-pat-nat-sobrecarga/
- https://www.netacad.com/
- **Libro Cisco CCNA ICND2 200-105**

Referencias de imágenes por orden de aparición en el PPT

- **Las imágenes son de autoría personal.**