Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

Listas de control de acceso y conceptos de PAT

Módulo 4: **Configuración y puesta en servicio de aplicaciones en redes de área local.**

Conectividad y Redes

Objetivos de Aprendizaje de la Especialidad

Módulo 1	**OA1** Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI. **OA3** Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes. **OA7** Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.
Módulo 2	**OA2** Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos. **OA11** Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.
Módulo 3	**OA8** Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.
Módulo 4	**OA4** Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.
Módulo 5	**OA5** Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.
Módulo 6	**OA9** Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de adcuerdo a las especificaciones técnicas del equipo.
Módulo 7	**OA10** Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.
Módulo 8	**OA6** Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.
Módulo 9	No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), 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

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

.

Aprendizaje Esperado

- **AE5:** Resuelve problemas de funcionamiento de conectividad entre redes, administrando equipamientos de acuerdo a su mantenimiento y detección de fallas, según protocolos de fabricantes.

¿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 e implementar mecanismos de traducción de direcciones IP (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.

02 PAT (Traducción de Direcciones de Puertos)

- ¿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 mayor seguridad a la red de equipos de una casa?

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 viene configuradas de forma predeterminada en los routers, sino que hay que configurar y aplicar según los requerimientos de seguridad que se necesiten en la red.

Wildcard

- Para el uso de **ACLS** 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 cuáles 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.

		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

Fuente propia

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

Calcular 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**

Fuente propia

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:

- **ACL estándar.**
- **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:

- **ACL estándar numerada.**
- **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.

Aplicación de las ACL

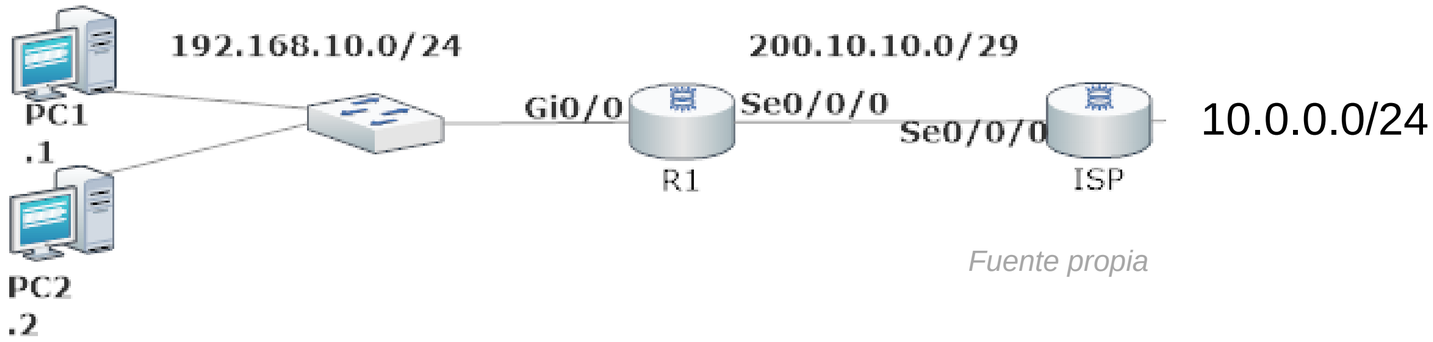
- Para poder aplicar una ACL, debemos ingresar a la interfaz que necesitamos ocupar e ingresar los siguientes comandos:

  Router(config)#interface se0/0/0
  Router(config-if)#ip Access-gropup **NumeroDeGrupo {**in | out**}**

- El número de grupo es el numero de la ACL que necesitamos aplicar y la interfaz se puede aplicar filtrando los paquetes de entrada o salida en un router**.**

Topología para los ejemplos

- Como ejemplo denegaremos el PC2 pueda salir hacia internet y los demás host 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.



Fuente propia

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

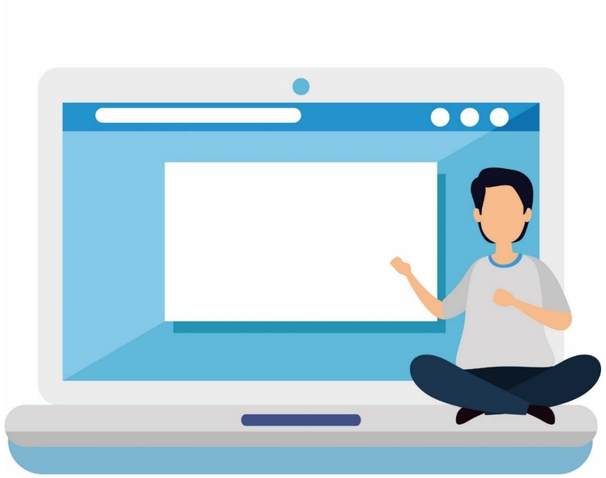
Verificación

Fuente propia

ACL estándar nombrada

- **Sintaxis de la ACL nombrada:**

Router(config)#ip access-list {estándar | extendida} nombre
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 con el nombre 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#
```

Fuente propia

Verificar las ACLS aplicadas

En el host que denegamos el acceso para salir de la red, intentamos salir a un 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 host 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#
```

Fuente propia

Editar las ACLS

Para poder editar veremos algunas alternativas que nos podrían ayudar:

01 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

Fuente propia

Editar las ACL

02 **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 ACL

Revisar los nuevos cambios

Fuente propia

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

Fuente propia

```
   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 casa de un amigo?

PAT (Traducción de Direcciones de Puertos).

¿Conoces los conceptos de PAT?

¿Te imaginas para qué podrían servir?

¿Qué es PAT?

PAT (**Port Address Translation**)

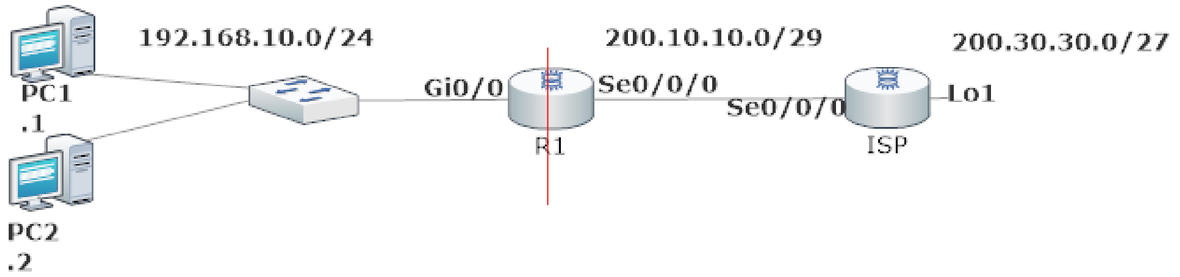
Traducción de Direcciones de Puertos, es conocido como NAT con sobrecarga, nos permite que se pueda utilizar una dirección IPv4 pública para múltiples direcciones IP privadas internas. Cuando se utiliza este tipo de traducción, el router mantiene bastante información de los números de puertos TCP o UDP, que asignará a medida que soliciten salir a internet con una dirección IP pública, asignando a cada conexión un puerto asociado a el servicio el cual quieran alcanzar.

Asignación de direcciones IP desde el ISP

Existen dos formas de configurar PAT, dependiendo de como 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 pública 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.

Fuente propia

Revisar PAT

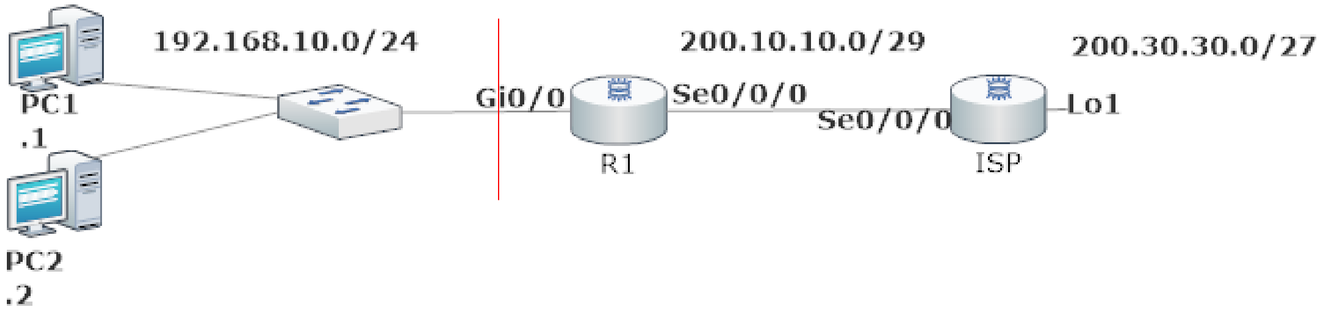
- Para poder revisar la configuración debemos digitar el comando **show ip nat translation.** Donde a través de un ping hacia una IP que simula la conexión a internet al momento de salir de nuestro router, comenzó a asignarle un puerto a nuestra dirección IP pública asignada por el ISP.

```
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#
```

Fuente propia

PAT con múltiples 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.

Fuente propia

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#
```

Fuente propia

Reflexionemos

¿Cuál es la importancia de poder utilizar PAT en los router de la red?

¿Tienes preguntas de lo trabajado hasta aquí?

Referencias de contenido:

https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

https://ccnadesdecero.es/configuracion-pat-nat-sobrecarga/

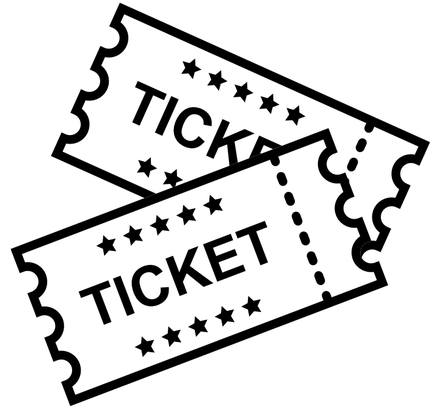
https://www.netacad.com/

Libro Cisco CCNA ICND2 200-105

Referencias de imágenes por orden de aparición en el ppt:

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

Ticket de salida



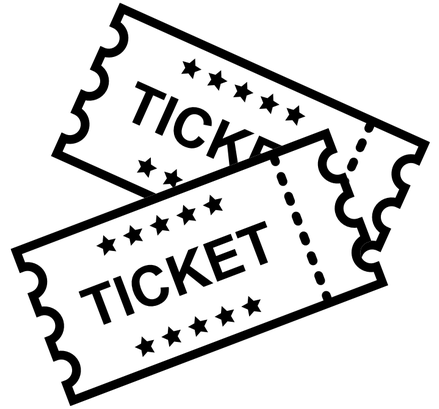
01

¿Cómo le explicarías a un compañero o compañera que le cuesta entender estos contenidos, qué son, para qué sirven y cómo se configuran las listas de control de acceso?

02

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

Ticket de salida



03

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

04

¿Qué debilidades percibiste en tu desempeño durante el desarrollo de la actividad? ¿Cómo puedes trabajarlas para convertirlas en fortalezas?