Salvavidas ASR

INFORMATIK

NAT

¿Cuándo traducir?

El router hace una traducción (agrega una entrada a su tabla de traducciones) cuando se realiza una comunicación entre ordenadores/servidores que estén, uno en una red pública y otra privada, o viceversa.

Si la comunicación es entre dos que estén en una red pública o los dos están en la misma privada no se hace traducción.

Tabla de traducciones

Protocolo	Socket destino	Socket Origen traducido	Socket Origen sin traducir

Si la conexión va de privada a pública, la tabla de traducciones del router que realiza la traducción sería:

PO → Puerto Origen

PD → Puerto Destino

Protocolo	Socket destino	Socket Origen traducido	Socket Origen sin traducir
TCP	IPDestino:PD	InterfazRouterPorLaQueSale:PO	IPOrigen:PO

Tabla NAPT dinámica --> Protocolo, Socket Destino, Socket Origen ST, Socket Origen Traducido

Tabla NAPT estática --> Protocolo, Socket Local, Socket Remoto

Remoto → Ip privada

Local → Ip interfaz de salida del router que te asigna la red

Abajo ejemplo

Cuando un ordenador se quiere conectar a un servidor web de su misma red, la IP_Destino es la interfaz de salida del router, pero la MAC_Destino es la interfaz de entrada a la red.

Para poner un servidor web a una red, hay que añadir una entrada estática al router.

HairPinning

Si el PC y el servidor están en la misma subred, pero consulta a Internet, entonces la IP_ORIGEN del PC será IP_PC y la IP_DESTINO IP_ROUTER_Interfaz, mientras que en el servidor será ORIGEN: IP_ROUTER_MismaInterfazQueArriba y la IP_DESTINO será IP_PC.

SOLO PARA UDP. AL USAR TCP NO SE TIENE EN CUENTA EL FILTRADO

5

Filtering → Dirección sin traducir

Mapping → Dirección traducida

Traducción y filtrado:

RFC 3489:

- Full Cone: Siempre se traduce de la misma forma, no hay filtrado en entrada (siempre que el socket de destino se corresponda con algo ya existente).
  - Traduce el puerto de entrada por uno de salida independientemente de la dirección IP.
- Restricted cone: Siempre se traduce de la misma forma, en entrada debe coincidir la IP origen (no importa el puerto) con algo ya existente.
  - Si el mensaje de entrada al router no coincide con ninguna IP que tiene el PC, no lo deja pasar.
- Port-restricted cone: Siempre se traduce de la misma forma, en entrada debe coincidir la IP origen y el puerto origen con algo ya existente.
- Symmetric: La traducción no siempre es la misma.

Esta clasificación no modela bien el comportamiento dispar de los NAT.
El RFC 3489 está obsoleto.

RFC 4787

- Comportamiento en la traducción:
  - EndPoint-Independent mapping: Se reutiliza el mismo mapeo si el socket origen (de la red interna) es el mismo, independientemente del destino (exterior).
  - Address-Dependent mapping: Se reutiliza el mismo mapeo si el socket origen (red interna) es el mismo y la dirección IP destino (exterior) es la misma, independientemente del puerto.
  - Address and Port-Dependent mapping: Idém, pero el puerto e IP destino tienen que ser el mismo.
- Comportamiento en el filtrado:
  - Endpoint-Independent filtering: El router NAT no tiene en cuenta ni la dirección IP origen ni el puerto (EXTERNOS), solo comprueba que la IP y el puerto de destino se corresponda con algo que se conectó previamente (desde dentro).
  - Address-Dependent filtering: Idem pero ahora fuerza a que al menos la IP origen coincida, aunque no el puerto origen.
  - Address and Port-Dependent filtering: Idem pero debe corresponder exactamente con la misma IP origen y puerto.

DHCPINFORM → Si el cliente obtuvo la IP por otros medios (asignación manual), puede pedir el resto de los parámetros a un servidor DHCP. La petición será broadcast si no conoce al servidor.

2) Para transformarlo, se pasa a la forma → ::FFFF:wxyz donde w.x.y.z es la IPv4 pero en hexadecimal.

::FFFF:A9FE:C

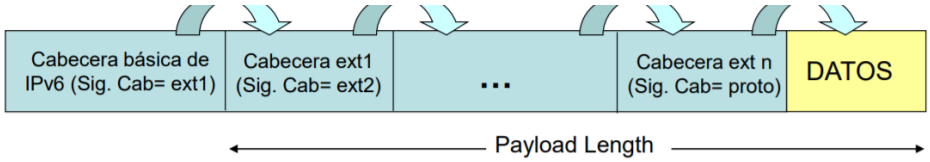
Se pone ":" porque "y" es 0

169.254.0.12

Si no se usa DHCP, se usa ICMPv6, asignando estas IP para router solicitation y advertisement

Averiguar sin una IPV6 es válida → https://isc.sans.edu/tools/ipv6.html#form

c. Una IPv6_PDU tiene 40 bytes de cabecera básica, 20 bytes de cabecera de encaminamiento, 20 bytes de cabecera TCP y 512 bytes de TCP_UD. Indique el valor del campo Payload Length



Justificación

Una IPv6 es válida si tiene el prefijo binario 001.

La dirección origen para enviar router_solicitation es FE80::/10

La dirección destino para enviar router_solicitation es FF02::/2

La dirección destino para enviar router_advertisement es FE02::/1

FF02::2 es la dirección multicast all-routers.

¿Como te puedes conectar a una red oculta?

Solo se puede conectar a esa red si se escribe anualmente la SSID y se envía un Probe request. El punto de acceso mandaría BSSID en el Probe response y ya se podrían conectar mediante Association request y response.

TTL negativo → Tiempo durante el cual el host debe esperar debido a una respuesta negativa. Esta respuesta negativa es debida a que el servidor secundario no tiene la información que tú quieres recibir. Se debe almacenar en la caché de cualquier otro servidor DNS una respuesta. (es el que se pone junto a serial, refresh…)

Si un servidor tiene caché de una zona, quiere decir que no es un servidor autoritativo de esa zona.

Hay dos tipos de consultas DNS: recursivas e iterativas.

Poniendo como ejemplo que me conecto desde mi ordenador a mi DNS para preguntar por una página web.

Habría una consulta recursiva, que sería de mi ordenador a mi DNS, y una consulta iterativa por cada servidor de dominio que tenga que atravesar.

Ejemplo: www.wgrp.es → 3 consultas iterativas, a la raíz, a .es y a wgrp.es

135.232.111.161.in-addr.arpa. IN PTR asr.example.com.

¿Durante cuánto tiempo puede seguir accediendo a una página un PC con DNS autoritativo y otro no autoritativo?

Si la consulta es autoritativa y es al servidor secundario, será Refresh.

Si la consulta no es autoritativa, tendrá caché, por lo que será TTl si se conecta al servidor primario y TTL+Refresh si se conecta al secundario

¿Se puede realizar una consulta DNS sobre un DNS que no está en caché si se apagan todos los DNS se esa zona?

Si no hay entrada en la caché, habrá que irse a la jerarquía DNS; si no están las entradas NS, entonces irse al nodo raíz. Si el servidor está apagado, no podrá resolver la consulta.

Seguridad

Definiciones Integridad, confidencialidad y no-repudio.

Integridad → Aseguramiento de que el mensaje no ha sido cambiado, es decir, que la información de un extremo no ha sido modificada de camino al otro extremo.

Confidencialidad → Garantía de que ningún medio externo accede a la comunicación.

No repudio → Garantía de que la comunicación que llega a un extremo es la generada por el otro extremo.

Cifrado Asimétrico

3 pasos

1) El mensaje se hashea mediante una función hash, que será un resumen del mensaje y que formará parte de esta. Antes de formar parte del mensaje, se encriptará con la clave primaria de A.
2) Se vuelve a encriptar con la clave pública del extremo B.
3) El extremo B desencriptará el mensaje con la clave privada de B. por un lado tendrá la función hash para obtener el resumen del mensaje, y, por otro, desencriptará el mensaje con la clave pública de A. Entonces, si ambos mensajes coinciden, se habrá cumplido el no repudio.

Definición hash

Resumen del mensaje, que tendrá un tamaño determinado y que formará parte del mensaje. El receptor calcula el resumen en la misma función hash y, si el recibido y el calculado son el mismo, entonces se habrá garantizado la integridad.

¿Para qué necesita el servidor web mandar las certificaciones intermedias, junto con la suya?

Para comprobar la ruta de autenticación (Path Validation).