Salvavidas-ASR.pdf

Informatik

Arquitectura y Servicios de Redes

3º Grado en Ingeniería Informática - Ingeniería del Software

Escuela Técnica Superior de Ingeniería Informática
Universidad de Sevilla

Coucke's English Academy

BY SARAH COUCKE, TEACHING SINCE 2005

Exámenes oficiales

de Inglés

Seas o no alumno de la academia,
¡ahora puedes matricularte en los exámenes oficiales a través nuestra!

Y nosotros nos encargamos de todo 😉

Cambridge English
Exam Preparation Centre

TRINITY COLLEGE LONDON
Registered Examination Centre 54473

BRITISH COUNCIL Aptis
Forward thinking English testing
Network

www.couckesacademy.es/examenes

Nervión
Avenida San Francisco Javier 24,
Planta Baja, Módulo 12C
954 65 98 99 - 605 54 50 19
nervion@couckesacademy.es

Macarena
Calle Don Fadrique 19
954 38 51 02 - 636 64 90 58
macarena@couckesacademy.es

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

Entrada estática NAPT R1

Protocolo	Socket Local	Socket Remoto
TCP	80.10.20.2:80	10.1.1.30:80

Estática

Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. (Ver imagen anterior)

Dinámica

El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública.

Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando.

Cuando te preguntan si se puede meter un servidor web, en el caso de que se pueda, tienes que añadir al router una entrada NAPT estática. Siempre se puede añadir, a menos que haya un conflicto en ese mismo puerto con otro servidor que estuviera de antes, si son servidores que usan puertos distintos, por ejemplo, correo (puerto 25) y web (puerto 80), no habría problema.

Fijarse si una TCP_PDU va al puerto 80, dentro de la red privada, porque entonces habrá un servidor web, y por tanto habrá que añadir una entrada estática.

Entrada estática --> PC a servidor web o viceversa

Entrada dinámica --> PC a PC

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

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.

DHCP

- MAC_PDUs de gestión:
  - Sirven para gestionar el enlace inalámbrico.
    - Beacon. La envía subnivel MAC periódicamente para informar de la existencia de una red inalámbrica.
      - Intervalo es un parámetro configurable
    - Probe request. Sirve para que el subnivel MAC escanee un área en buscando redes inalámbricas.
      - Se informa de las velocidades soportadas.
    - Probe response. Enviado por el subnivel MAC en respuesta a un Probe request.
    - Association request. Sirve para que el subnivel MAC solicite "conectarse" a una red inalámbrica.
    - Association response. Confirmación de la "conexión" a una red inalámbrica.
    - Otras…

DHCPDISCOVER → Sirve para que el cliente "pida" una dirección IP. Es un broadcast, debe incluirse la MAC del cliente (chaddr), el cliente puede sugerir tanto opciones adicionales como su propia IP.

DHCPOFFER → Cada servidor DHCP envía una "oferta" de dirección (yiaddr) y opciones adicionales de configuración (DNS, gateway, etc). Los servidores comprobarán (ej: PING) que la dirección que ofrecen no está en uso.

DHCPREQUEST → El cliente elige una de las ofertas y responde con una IP_PDU de broadcast en la que indica la IP que le ofrecían. Debe enviar además en las opciones el identificador del servidor, de esta forma todos los demás servidores saben que el cliente no usará la dirección que le ofrecieron.

DHCPPACK → Se confirma finalmente la asignación de esa IP. El servidor DHCP marcará la IP como "en uso" y el cliente tiene que, en ese momento, comprobar que la IP no esté en uso (por ejemplo, con ARP) y rechazar esa IP si está en uso (DHCPDECLINE).

DHCPRELEASE → En caso de parada ordenada de un ordenador, este puede liberar la IP asignada.

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

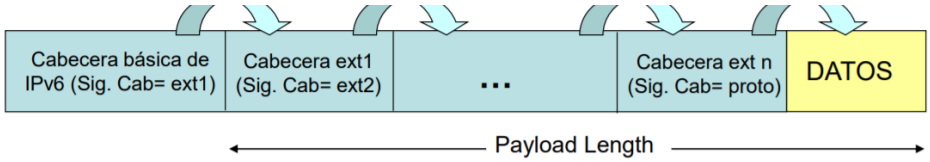
Se pone ":" porque "y" es 0

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.

c) Describa cómo funciona el mecanismo de reserva del medio previsto en IEEE802.11

Para reservar el medio, un cliente debe enviar una MAC_PDU de control llamada RTS, de esta forma evitará que otros clientes colisionen con él. También se especificará la duración de la reserva. El punto de acceso de su BSS responderá con una MAC_PDU de control llamada CTS, indicando qué puede enviar y la duración de la reserva.

La IP de autoconfiguración es cualquiera del tipo 169.254.X.X

HolePunching

Consiste en el establecimiento de comunicaciones entre dos partes en organizaciones separadas que están deras de firewalls. Se utiliza para aplicaciones como juegos, P2P y VoIP.

Para que sea una dirección IPV6 pública, debe empezar por 001 de izquierda a derecha.

Si no se fragmenta el mensaje, no hace falta usar el protocolo ARP.

DNS

Para saber el FQDN del servidor principal de una zona, hay que fijarse en los NS que tengamos en la caché. Si tenemos más de uno, no podemos saber cuál es el principal ya que eso viene en el SOA, y no ahí; sin embargo, si tenemos un solo NS, quiere decir que ese es el principal.

TTL SOA → TTL para las entradas de los servidores.

TTL/entrada→ Nos indica el tiempo de vida durante el cual esa entrada puede ser considerada válida, entrada tipo A.

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.

Correo

MIME

Caracteres extendidos en cabeceras

- Las cabeceras, a no ser que el MTA soporte 8bits, siguen transmitiéndose con 7bits. ¿Qué ocurre con los caracteres ASCII extendidos en las cabeceras?
- Puede ser necesario que en el asunto, el From o el To aparezcan estos caracteres.
- SOLUCIÓN. Se codifican, si es necesario, determinadas partes de las cabeceras con este esquema:
  - encoded-word = "=?" charset "?" encoding "?" encoded-text "?="
  - charset es el juego de caracteres, encoding: q=quoted-printable, b=Base64.
  - Los espacios se sustituyen por "_", los "_" por su codificación. Restricciones con otros.

Subject: Elaboración de guías ECTS
Subject: =?iso-8859-1?Q?Elaboraci=F3n_de_gu=EDas_ECTS?=

Subject: Abierto el plazo de petición de libros
Subject: Abierto el plazo de =?ISO-8859-1?Q?petici=F3n_de_libros?=

Subject: Este_es_un_texto_extraño
Subject: =?ISO-8859-1?Q?Este=5Fes=5Fun=5Ftexto=5Fextra=F1o?=

Subject: No_necesariamente_se_codifica.
Subject: No_necesariamente_se_codifica.

Q → quoted printable

B → Base64

f) Con los datos que se muestran, ¿es posible saber si se han usado caracteres ASCII extendidos en el cuerpo del correo?

Content-Transfer-Encoding: 7bit
Subject: =?iso-8859-1?**B**?UmVwb3J0

El Subject nos dice que tiene iso-8859-1 y que tiene de enconding base 64 (la B, quoted-printable es Q). Base 64 permite caracteres de la "A" a la "Z", de la "a" a la "z", del "0" al "9" y "+" y "/", así pues **NO permite caracteres extendidos, puesto que no se pueden poner acentos, ni la ñ.** Si tuviera Q sí que permitiría caracteres extendidos.

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).

Ataques man in the middle

1. El atacante captura la conexión.

2. El atacante envía su clave pública (que él ha generado) y negocia una conexión segura.

3. El atacante se conecta al servidor real, negociando una conexión segura.

4. El atacante gestiona esas dos conexiones y, por tanto, tiene acceso a los datos de la conexión.

Para que todo funcione bien, es necesario garantizar la propiedad de la clave pública (garantizar que es de quien dice ser), la manera que te preguntarán en el examen es mediante certificados, aunque también podría ser de manera offline.

CRL Distribution Point: Lista de certificados revocados.