

T1 - Latencia

1) ¿Qué es la latencia? ¿Cuáles son sus componentes? ¿Qué componente tiene mayor incidencia en el cálculo de la latencia?

Latencia es el retardo entre un estímulo y su respuesta.

- **Tiempo de inserción:** El tiempo en insertar el paquete en el medio a ser transmitido

Formula: L/R , con L largo del paquete y r ancho de banda/velocidad de serialización.



- **Tiempo de propagación:** es el tiempo en propagar un bit a través de un medio.

Formula: d/c , con d distancia entre extremos del enlace y c velocidad del medio.



- **Tiempo de encolado:** el tiempo que espera un paquete en la cola de router para ser forwardado

Es el tiempo desde que arriba hasta que es finalmente transmitido, y depende del tráfico de la red (ocupación del router, tamaño de la cola)

- **Tiempo de procesamiento:** el tiempo que tarda el router en procesar datos del paquete

Causas: leer el header y tomar la decisión de por cual enlace se debe enviar. Es despreciable.

No hay un tiempo que tenga mayor incidencia siempre. Depende de la topología y Estado de red (aunque dadas determinadas condiciones si se puede saber cual es el predominante).

Por ejemplo:

- si hay mucha congestión el tiempo encolado será grande
- si la distancia es mucha entonces el tiempo de propagación será grande -
- si la señalización es baja el tiempo de inserción será grande

Métrica: Se usa como métrica para latencia el **RTT Round Trip Time** Tiempo que tarda un paquete de datos enviado desde un emisor en volver al mismo emisor habiendo pasado por el receptor de destino.

¿Cuál es el componente con mayor incidencia si la red se encuentra congestionada en cada punto del camino que recorre el paquete?

El componente con más incidencia en este caso es el tiempo de encolado.

¿Qué es la asimetría de caminos y cómo afecta el cálculo de la latencia?

La asimetría de caminos se da cuando un paquete toma un camino de vuelta distinto al camino de ida. Esto afecta la latencia ya que al estar eligiendo otro camino puede darse un cambio en el tráfico de la red afectando así el tiempo de encolado por la disminución de la congestión y tiempo de propagación

Responde verdadero o falso

A. una cdn propone manejar los protocolos de ruteo y el procesamiento de paquetes control Plain desde una unidad central controller y separar dichas funciones de aquellas netamente relacionadas con el envío de paquetes

falso ese comportamiento corresponde al sdn

cdn (content delivery network): grupo de servidores distribuidos en diferentes ubicaciones geográficas de todo el mundo para permitir la entrega rápida del contenido de un sitio web

sdn(Software-Defined Networking): utilizan controladores basados en software o interfaces de programación de aplicaciones (API) para dirigir el tráfico en la red y comunicarse con la infraestructura de hardware subyacente

B. La latencia puede ser reducida por medio de una cdn

verdadero se puede reducir la latencia que se produce en comunicarse con algo lejano si se reduce el tiempo de propagación colocando algún punto intermedio cercano

c la cdn ayuda a maximizar el throughput

verdadero Esto es así ya que al alcanzar un contenido tiene que pasar por menos routers siendo menos afectada por factores que pueden alterar el throughput en el camino.

Baja la congestión de la red y por eso aporta a maximizar el throughput..

Aunque una CDN no aumenta el throughput de la red en su conjunto, sí puede mejorar la velocidad y la eficiencia en la entrega de contenido al usuario final al minimizar la latencia y reducir la carga en los servidores originales, lo que puede percibirse como una mejora en el rendimiento.

throughput: amount of data or traffic that **can be successfully** transmitted through the network

D. La ubicación geográfica de los clientes es un factor determinante para la performance de una cdn

verdadero. una cdn gestiona servidores situados en múltiples ubicaciones geográficamente distribuidas almacena copias en sus contenidos en sus servidores y trata de dirigir cada solicitud de usuario a una ubicación de la cdn que proporcione la mejor experiencia de usuario posible

F. La simetría de caminos siempre impacta negativamente en el cálculo de rtt.

Falso **No necesariamente** el camino de vuelta al ser distinto el camino de ida genera un mayor valor de rtt Por ejemplo si el camino de ida se congestiona es mejor que se elija otro camino de vuelta con menor tráfico y disminuye así el rtt

G. El tiempo encolado es un componente despreciable respecto a la suma del resto de los componentes de la latencia

falso, depende. **Varia con el tráfico**

h. TCP Splitting es una técnica que reduce latencia

Verdadero. TCP splitting es una técnica que divide una conexión TCP en dos conexiones separadas, a menudo para aplicar controles, reglas o políticas específicas, mejorar el rendimiento, o permitir la manipulación de datos en el flujo de comunicación

T6 - ICMP

Responda Verdadero o Falso. Justifique la respuesta.

- a. **La herramienta ping utiliza UDP en su implementación.** Falso. Utiliza ICMP
segun [links](#): falso

- b. **ICMP es un protocolo de transporte.** Falso. Es un protocolo auxiliar de IP (Internet Control Message Protocol) - pertenece a la capa de red
- c. **ICMP se elimina en IPv6** Falso. Sí se utiliza ipv6.
- d. **El tráfico ICMP no se puede filtrar debido a que ICMP es un protocolo de diagnóstico y reporte de errores.** Falso, si se pueden filtrar mensajes ICMP

T2 - Capa de Transporte

¿Es posible para una aplicación tener transmisión de datos confiable aún cuando la aplicación utilice UDP?. ¿Cómo?

Si, es posible. Si bien UDP no garantiza una entrega confiable, para lograrlo se debe implementar un protocolo de transferencia de datos fiable a nivel de aplicación que funcione sobre UDP.

¿Qué significa que un protocolo de transporte implemente un servicio de entrega confiable? Dé un ejemplo.

Transferencia de datos confiable (reliable data transfer): Se dice que es confiable cuando puede garantizar que no se pierdan o corrompan paquetes de datos.

Significa que el protocolo garantiza que el flujo de datos que un proceso extrae de un buffer de recepción no está corrompido, no tiene huecos, ni duplicados y está en orden.

Responder Verdadero o Falso. Justificar la respuesta.

1. **Los routers implementan todas las capas del modelo TCP/IP excepto la capa de aplicación.**

Falso. No implementan la capa de transporte ya que eso está implementado en cada host

2. **El protocolo de la capa de red proporciona una comunicación lógica entre procesos que se ejecutan en diferentes hosts mientras que un protocolo de capa de transporte proporciona comunicación lógica entre hosts**

Falso. Es al revés: el protocolo de la capa de red proporciona una comunicación lógica entre hosts mientras que el protocolo de la capa de transporte proporciona comunicación lógica entre procesos.

3. **Un protocolo de capa de transporte puede ofrecer un servicio de entrega confiable aún cuando el protocolo de red subyacente no lo proporcione a nivel de capa de red.**

Verdadero. De hecho, el protocolo TCP de la capa de transporte ofrece un servicio de entrega confiable sobre la capa no confiable de la red.

4. **Un protocolo de capa de transporte puede ofrecer garantías de delay aún cuando el protocolo de red subyacente no lo proporcione a nivel de capa de red.**

Verdadero porque tcp incluye mecanismos de control de flujo y de congestión

La afirmación original es cierta. Es posible que un protocolo de capa de transporte, como el TCP, ofrezca garantías de retardo (delay) a pesar de que el protocolo de red subyacente no proporcione garantías a nivel de capa de red. El TCP incluye mecanismos de control de flujo y gestión de la congestión que pueden influir en el retardo experimentado por los datos, aunque la capa de red no ofrezca garantías específicas de retardo.

Segun gente: falso, por mas que un protocolo de transporte pueda ofrecer control de congestion como TCP, nunca podria asegurar que un paquete llegue antes de los 30ms por ejemplo, si el protocolo de red no lo garantiza.

T2 - TCP

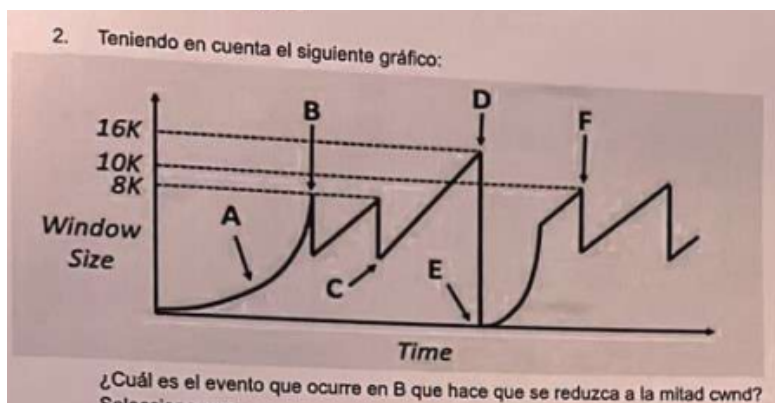
Responder Verdadero o Falso. *Justificar la respuesta.*

1. **TCP implementa el pipeline con el protocolo Go-Back-N.** Falso.
Lo que implementa solo tiene similitudes con este (rwnd == pipeline)
2. **TCP implementa el pipeline con protocolo Selective Repeat.** Falso
Las dos anteriores son falsas porque implementa un híbrido de ambos
3. **TCP es full duplex**
verdadero. Incluso cada emisor tiene una ventana de recepción de diferente tamaño.
full duplex: debe establecerse la comunicacion en ambos sentidos
half duplex: primero habla uno y luego habla el otro
simplex: solo uno puede hablar y el otro debe escuchar
4. **Udp implementa un servicio Full dúplex.**
Falso. UDP no está orientado a la conexión con lo cual no se genera una conexión con otro cliente para mandar y recibir mensajes.
5. **Un socket es la interfaz entre la capa de transporte y la capa de red.**
Falso. es la interfaz entre la capa de aplicación y de transporte.

Responder:

¿Cuál es la diferencia entre TCP Tahoe y TCP Reno?

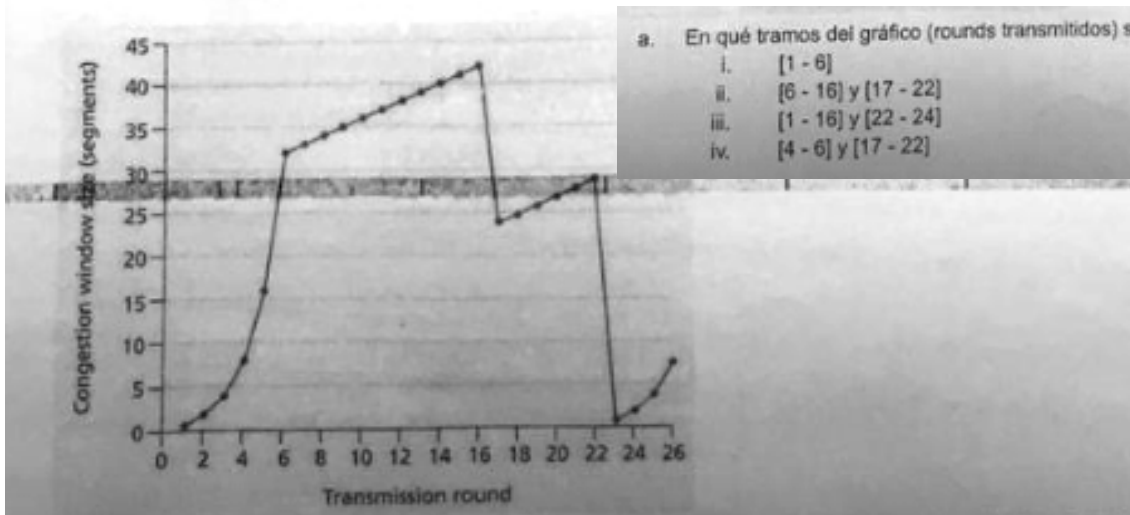
La diferencia entre TCP tahoe y TCP reno está en cómo se comportan cuando se pierde un paquete. En el caso de **tahoe**, se retransmite el segmento perdido y luego se retoma el envío de paquetes comenzando con slow start. En cambio, cuando se pierde un paquete en **reno** lo que ocurre es que se reenvía el paquete perdido y luego se retoma entrando en la etapa conocida como fast recovery y luego continua con Congestion Avoidance



Triple ACK duplicado. Dentro de los dos implementaciones de tcp estudiados en la materia tcp reno es el único que reduce el cwnd a la mitad ~~y se hace luego de un triple ACK duplicado.~~ Tanto tahoe como reno se hacen luego de recibir 3 acks duplicados.

2. Seleccionar la respuesta correcta:

Considerando que el siguiente gráfico es una captura de TCP Reno



- a. En qué tramos del gráfico (rounds transmitidos) se encuentra la etapa de Slow Start?
- [1 - 6]
 - [6 - 16] y [17 - 22]
 - [1 - 16] y [22 - 24]
 - [4 - 6] y [17 - 22]

- b. ¿Qué evento produce el descenso en el gráfico luego de la transmisión número 16?
- Timeout
 - Congestion Avoidance
 - Fast Retransmit
 - Fast Recovery
 - Triple ACK duplicado
 - Ninguna de las anteriores

- c. ¿Qué evento produce el descenso en el gráfico luego de la transmisión número 22?
- Timeout
 - Congestion Avoidance
 - Fast Retransmit
 - Fast Recovery
 - Triple ACK duplicado
 - Ninguna de las anteriores

- d. ¿Cuál es el valor del *ssthresh* en la transmisión número 18?
- 1
 - 15
 - 21
 - 32
 - 42

- e. Asumiendo que una pérdida de paquete con una detección de triple ACK duplicados es detectado luego de la transmisión número 26, ¿cuáles son los valores de la ventana de congestión y del *ssthresh*?
- cwnd = 1, ssthresh = 8
 - cwnd = 8, ssthresh = 8
 - cwnd = 4, ssthresh = 2
 - cwnd = 6, ssthresh = 4
 - Ninguna de las anteriores

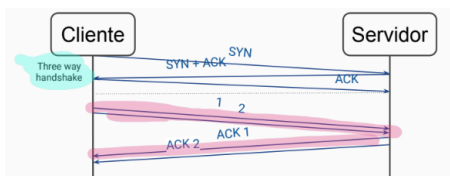
c. timeout.

d. entre 8 y 16 => 15 (porque la vieja estaba entre 16 y 32)

e. 3ack es perdida de un paquete, cwnd es 4. pero ssthresh debería ser 7. entonces no es ninguna de las anteriores.

En TCP ¿si el valor ack recibido es 200 cuánto bytes han sido recibidos exitosamente? justificar.

199 porque el ack nos da el siguiente byte que estamos esperando en este caso 200



-> práctica

1. Responder Verdadero o Falso. Justificar la respuesta.

a. Los routers implementan todas las capas del modelo TCP/IP excepto la capa de aplicación.

Falso. No implementan la capa de transporte ya que eso está implementado en cada host ni las de aplicación.

ROUTER SOLO RED, ENLACE Y FISICO

d. Luego de detectar la pérdida de un paquete por un time out, TCP reduce su ventana de congestión a la mitad como respuesta ante dicha situación de congestión.

Falso. Por time out la cwind se resetea a 1. Y se reduce SST a Cwnd/2

2. Elija la respuesta correcta:

a. Suponiendo que dos hosts utilizan una conexión TCP para transmitir un archivo grande. ¿Cual/es de las siguientes afirmaciones es/son falsas?

1. Si el número de secuencia de un segmento es x , entonces el número de secuencia del siguiente segmento es siempre $x+1$.
2. Si el tiempo estimado de un round trip en cualquier momento de la conexión es t segundos, el tiempo de retransmisión de timeout siempre es mayor o igual a t segundos.
3. El tamaño de la ventana de congestión nunca se modifica durante una conexión TCP.
4. El número de bytes sin acknowledge en el emisor siempre es menor o igual a la ventana de congestión.

i. 1 y 4

ii. 1 y 3 *

iii. 4

iv. 3

v. Ninguna es falsa.

1. El NRO DE SECUENCIA no arranca siempre en 0 y es tipo circular.
2. V
3. F
4. V

b. ¿Para qué sirve el campo rwnd en el header de los segmentos de TCP?

i. Determina la cantidad de datos que son posibles de enviar a la red antes de recibir un ACK.

ii. Determina la cantidad de paquetes ACK que el host emisor recibió durante la conexión.

iii. Determina la cantidad de paquetes que el host destino puede recibir sin descartar ningún paquete de su buffer.

VERDADERO

iv. Ninguna de las anteriores

c. ¿Cómo se identifican los sockets en UDP?

i. (source_ip, destination_ip)

ii. (source_ip, source_port, destination_ip)

iii. (source_ip, source_port, destination_ip, destination_port)

ASI ES EN TCP

iv. Ninguna de las anteriores

verdadero. Se necesita Puerto de destino e IP destino.

d. ¿Qué evento, en TCP Reno, produce que la ventana de congestión se reduzca a la mitad?

i. Timeout

ii. Congestion Avoidance

iii. Fast Retransmit

iv. Fast Recovery

ESTO ES UNA ETAPA, no un evento.

v. Triple ACK duplicado

VERDADERO

vi. Ninguna de las anteriores

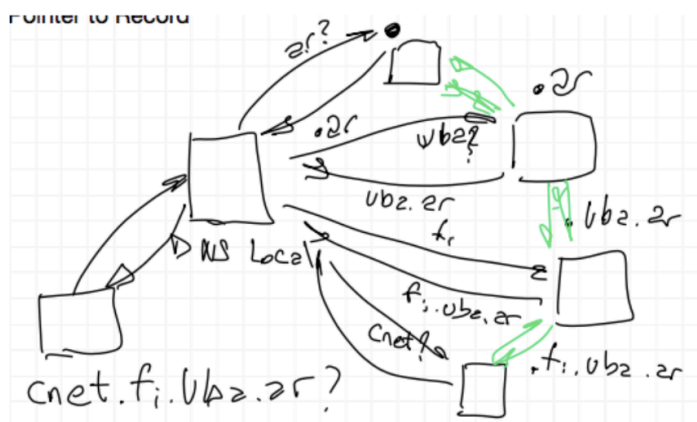
T5. DNS

Explicar la función del protocolo DNS y Describir detalladamente el proceso de resolución de una consulta ¿qué protocolo de transporte utiliza? ¿Por qué se utiliza este protocolo?

El dns es un protocolo de capa de aplicacion que se encarga de realizar la traducción de los nombres de Host a su dirección IP además probé load balancing, host aliasing y email server aliasing (Load balancing: distribuir la carga tráfico de red de un servicio en más de un servidor). Típicamente usa el puerto UDP porque es connectionless y asi es mas rapido el proceso.

Ej:

- Ponemos drive.google.com en nuestro browser
- El browser busca la URL en la(s) cachés de DNS: Primero, checkea su propia caché. Si no lo encuentra, system call para chequear caché del SO
- Si no se tiene, se escala al DNS resolver que tengamos configurad por ej, 8.8.8.8 (DNS de google) también puede ser el default gateway
- Si el resolver no lo tiene cacheado, comienza proceso iterativo para averiguar la IP del dominio:
 - Se lanza la query al root server; responde con info del TLD .com
 - Se lanza la query al TLD .com; responde con info del SA google.com
 - Se lanza la query al SA google.com; responde la IP de drive.google.com
- Resolver cachea la respuesta, y se la redirige al browser (que tambien la cachea).
- El browser ahora puede realizar la request HTTP



El DNS local hace preguntar iterativas porque itera desde el root a .ar, luego de .ar a .uba.ar y de .uba.ar a .fi.uba.ar.

Responder: ¿De qué forma una CDN puede utilizar DNS para acercar el contenido a los usuarios?

La idea es que haya múltiples servidores CDN distribuidos por el mundo y que dependiendo la ubicación de los request de los usuarios DNS devuelve la IP del CDN más cercano del usuario, de esta forma beneficiando al usuario de tener menos latencia y acceso al contenido más rápido y también como un beneficio global la red se ve menos saturada ya que los paquetes deben hacer un recorrido menor.

Una CDN tiene múltiples servidores distribuidos por todo el mundo, tal que intenta redirigir las solicitudes de cada cliente al CDN que le provea la mejor experiencia.

Muchas CDNs aprovechan DNS para redirigir solicitudes. Por ejemplo: un proveedor NetCinema distribuye sus videos mediante KingCDN, en el sitio de NetCinema las urls tienen la forma `http://video.netcinema.com/6Y7B23V`. Lo que sucede:

1. El usuario ingresa a la url y el host envia la solicitud DNS para `video.netcinema.com`
2. El DNS local del usuario envía la solicitud al servidor de mayor jerarquía de NetCinema. Este último, en vez de devolver la IP, devuelve otro hostname del dominio de KingCDN, podría ser por ej. `a1105.kingcdn.com`
3. Ahora el DNS local envía una segunda query pero esta vez al servidor DNS de KingCDN y este sí devuelve la IP.

Cuáles serían los pasos al ejecutar una consulta dns?

Local resolver. Root DNS. TDL dns. Authoritative DNS

T3- Routing

¿Qué es una máscara de red? ¿Cómo y dónde se utiliza? ¿Cómo se codifica la máscara de red en el datagrama IP?

Una máscara define qué bits nos interesan de un espacio de direcciones y es una secuencia de bits de izquierda a derecha que contiene unos. Se utilizan para determinar A qué interfaz mandar el paquete haciendo una AND entre la dirección IP y la máscara

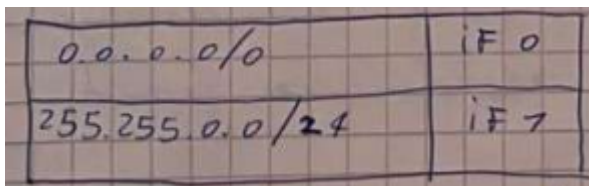
La máscara no se codifica en el datagrama IP.

<red><host>

¿Qué es una tabla de ruteo? Qué papel desempeña en el proceso de enrutamiento de un paquete dar un ejemplo

Es la tabla que determina por cual interfaz se hace el forwarding para cada paquete. La tabla se arma durante el proceso de routing.

Ejemplo: hacer el forwarding de esta dir IP = 255. 255.1.0



0.0.0.0/0	iF 0
255.255.0.0/24	iF 7

En este caso solo hace match con el default get away entonces saldrá por la interfaz 0

Verdadero o falso

Cuando un Host envía un paquete la cantidad de bytes transferidos en la red es la misma sin importar si hubo un proceso de fragmentación en el medio es por esto que decimos que la fragmentación es transparente para el Host.

Falso. Cuando un Host Envía un paquete este puede ser fragmentado y en cada fragmentación se agrega headers y metadata a este fragmento y por ende la cantidad de transferidos en la red no es la misma que el paquete original

T3 - IP Routing

Dada una tabla de ruteo, se busca optimizar la configuración de las entradas. Explicar y dar un ejemplo de los siguientes casos:

a. La tabla de ruteo contiene 3 entradas que se pueden agregar en una única entrada.

Por un lado tenemos dos entradas que pueden agregarse entre si

160.200.3.0 /24 | if2 160.200.00000011|.0

160.200.2.0 /24 | if2 160.200.00000010|.0

Ambas direcciones difieren en el ultimo bit, Tiene la misma máscara y tienen el mismo puerto de salida.

se agregan de la siguiente manera

160.200.2.0 /23 | if2

Ahora tendríamos una tercera que difiere en el último bit con la anterior y tiene el mismo puerto de salida:

160.200.0.0 /23 | if2

ya que

160.200.00000000|.0

160.200.00000001|.0

Se agregan de la siguiente manera:

160.200.0.0 /22 | if2

b. La tabla de ruteo contiene una entrada ya contenida en otra entrada.

Esto sucede cuando dos entradas tienen distinta máscara pero coinciden bit a bit hasta el prefijo de menor máscara

Por ejemplo 127.80.192.0/18 y 127.80.224.0/23

127.80.11 000000

127.80.11 1000000

c. La tabla de ruteo contiene una entrada mal configurada, donde el prefijo es más específico de lo que la máscara permite.

Una entrada mal configurada sucede cuando tenemos un prefijo más específico que la máscara esto quiere decir que tiene bits en uno a la derecha de la máscara cuando aplicamos la máscara debido al and lógico que realiza esos bits se convierten en cero y quedan redundantes

8.8.8.8/24 porque el último octeto no va a matchear con nada

Pregunta. Si tenemos el siguiente prefijo: 182.64.46.0/x.

¿Cuál es el mínimo valor que puede tomar x?. Justificar.

182.64.00100110.00000000

El mínimo valor que puede tomar x es $32 - 9 = 23$.

Pregunta. Si tenemos el siguiente prefijo: 172.128.6.0/x.

¿Cuál es el mínimo valor que puede tomar x?. Justificar.

172.128.00000110.00000000

el mínimo valor de x es $32 - 9 = 23$

T4 - IPv4

Responder: ¿Qué es NAT y cómo funciona? ¿Qué problema busca resolver?

NAT es Networking Address Translation y lo que hace es traducir las direcciones privadas a públicas.

El problema que busca resolver es otorgar más ips de las que ofrecia ipv4

El mecanismo que utiliza es mapear cada una de los pares ip/puerto que salen de la red privada a la pública a un puerto en particular, cambiando la ip de origen por la de la WAN y el puerto por uno libre del nat. De esta manera, cuando el servidor responde con una ip y puerto de destino puede revisar esta tabla para cambiarlas por las direcciones privadas correspondientes,

Explicar por qué diferentes host pueden compartir la misma IP privada siendo la IP un identificador unívoco. Cómo es el procedimiento para comunicarse con un host fuera de la red privada a la que pertenece.

Diferentes hosts pueden compartir la misma IP privada ya que sus routers están configurados para usar NAT. Estos routers tienen lo que se conoce como la tabla de traducciones NAT cuyas entradas incluyen numeros de puerto junto con las direcciones ip.

El procedimiento es el siguiente:

Cuando un host quiere comunicarse con alguien que está fuera de la red privada, crea el datagrama con la direccion destino y puerto destino a la LAN. Dicho datagrama es recibido por el router NAT, y este genera un nuevo puerto origen para el datagrama y sustituye la direccion origen por su propia direccion origen (la del router NAT). El nuevo puerto origen que selecciona el NAT es un número que aun no este en la tabla. El router NAT finalmente agrega una entrada en su tabla con este puerto origen nuevo y la direccion del host que envio el datagrama. Cuando el host que está fuera de la red envía su respuesta, el puerto al que se dirige el datagrama es el que creo el router NAT. Así, finalmente para que el host de la red privada reciba el datagrama de respuesta, el router NAT indexa su tabla con el puerto de origen que creó.

Rangos de Bien conocidos: 0-1023

Rango servicios definidos: 1024 en adelante hasta 49751

Rangos de puertos privados:65000

puerto HTTP: 80 y 8080

-> puedo usar desde el 1024 al 65mil

T5 - Fragmentación

2) Un paquete P es fragmentado en N paquetes Fi al atravesar una red IPv4 antes de llegar al host destino. En el camino, uno de los paquetes Fi se pierde en el camino. ¿Qué

consecuencia tiene la pérdida del paquete F_i sabiendo que el protocolo de la capa de transporte utilizado es TCP?

Al perderse uno de los fragmentos se descarta la secuencia completa. Como se está utilizando TCP el paquete completo será posteriormente reenviado ya sea porque se produce un timeout del lado del emisor o porque el emisor recibe una serie de ACK repetidos.

Un paquete P es fragmentado en n paquetes F_i al atravesar una red IPv4 antes de llegar al host destino. En el camino, uno de los paquetes F_i se pierde en el camino.

¿Qué consecuencia tiene la pérdida del paquete F_i sabiendo que el protocolo de la capa de transporte utilizado es UDP?

El paquete es descartado y se da como perdido en este caso al usar udp el paquete va a ser descartado ya que no es de entrega confiable.

Un paquete P es fragmentado en n paquetes F_i al atravesar una red IPv4 antes de llegar al host destino. En el camino, uno de los paquetes F_i se pierde en el camino.

¿Qué consecuencia tiene la pérdida del paquete F_i sabiendo que el protocolo de la capa de aplicación implementa un servicio de entrega confiable similar a TCP, utilizando UDP como protocolo de transporte?

El paquete es descartado y se da como perdido en este caso al utilizar un servicio de entrega confiable todo el paquete va a ser reenviado.

Verdadero o Falso. Justificar en caso de que la afirmación sea falsa.

a. Sólo los routers pueden fragmentar paquetes en una red IPv4

Falso. No prohíbe que un Host pueda fragmentar el paquete antes de mandar el primer router si el mtu del medio no es suficiente

b. El ensamblado de los fragmentos se realiza en el último router, antes de llegar al host receptor.

Falso el ensamblado se realiza en el Host destino. ROUTER NUNCA ENSAMBLA.

c. Para mejorar la eficiencia de la red IPv4 al utilizar TCP, cuando se fragmenta un paquete y uno de los paquetes fragmento se pierde, el host emisor sólo retransmite el paquete fragmento, en vez de retransmitir el paquete original.

Falso si se pierde un fragmento tcp envía todo el paquete de nuevo

d. El mecanismo de fragmentación de IPv4 no introduce una vulnerabilidad en el protocolo.

Falso. fragmentar consume mucha cpu del router y enviando paquetes grandes podrias hacerlo colapsar. También se podría enviar un fragmento solo, simulando que luego se van a enviar muchos más y hacer que el receptor reserve espacio para almacenarlos y agotar sus recursos

Otra vulnerabilidad es realizar un ataque dos enviando muchos paquetes con el flag de “more fragments” en true. Esto haría que un host receptor sin ningún mecanismo de protección reserve memoria esperando completar el paquete.

Dado dos Host separados por un único router por medio de enlaces de mtu 600 el Host A Envía un paquete cuya IP destino corresponde al hospe Cuántos fragmentos llegan al host B si se tiene en cuenta los siguientes datos:

Header Size	Datagram Length	Do Not Fragment
20 Bytes	1400 Bytes	1

Ninguno ya que el datalen es mayor al mtu y además está activado el flag que no se puede fragmentar Por ende no se transmite nada

Si solo me dan lo que llega al dst host (y hay fragmentos perdidos):

2. ¿Puedo determinar la cantidad de fragmentos que se generaron en el camino? Calcule el valor en caso de ser posible.
3. Determine la cantidad de fragmentos que se generaron en el camino? Calcule el valor en caso de ser posible.

No. porque no sabes que camino toman los fragmentos y quizás tomaron unos que necesitaban mayor fragmentación y por ahí son los que se perdieron

T4 - Subnetting

Responder Verdadero o Falso. Justificar

- a. Dada las subredes: A (100 hosts), B (100 hosts), C (80 hosts), todas conectadas a un mismo router. Es posible subnetear la configuración utilizando el prefijo 200.128.64.0/24.**

falso.

para A se necesita un bloque de 128
para B se necesita un bloque de 128
para C se necesita un bloque de 128

Se necesita por lo menos un espacio de 512 direcciones. Osea, 2^9 .

Con 200.128.64.0/24 tenemos uno de 256 direcciones, por lo tanto no alcanza.

- b. Dada las subredes: A (100 hosts), B (80 hosts), C (10 hosts), todas conectadas a un mismo router. Es posible subnetear la configuración utilizando el prefijo 200.128.64.0/24 dado que tengo 256 direcciones posibles.**

falso.

para A se necesita un bloque de 128
para B se necesita un bloque de 128
para C se necesita un bloque de 16

Se necesita por lo menos un espacio de 512 direcciones. Osea, 2^9 . No alcanza
200.128.64.0/24.

- c. Dada las subredes: A (100 hosts), B (60 hosts), C (60 hosts), todas conectadas a un mismo router. Es posible subnetear la configuración utilizando el prefijo 200.128.64.0/24 dado que tengo 256 direcciones posibles.**

verdadero.

para A se necesita un bloque de 128

para B se necesita un bloque de 64
para C se necesita un bloque de 64

Se necesita por lo menos un espacio de 256B. Osea, 2^8 . Alcanza 200.128.64.0/24.

- d. **Dada las subred: A (300 hosts), B (60 hosts), C (60 hosts), todas conectadas a un mismo router. Es posible subnetear la configuración utilizando el prefijo 200.128.128.0/23 dado que tengo 512 direcciones posibles.**

falso

para A se necesita un bloque de 512
para B se necesita un bloque de 64
para C se necesita un bloque de 64

Se necesita por lo menos un espacio de 1024. Osea, 2^{10} . No alcanza 200.128.128.0/23.

Responda Verdadero o Falso. Justifique en caso de que la afirmación sea falsa.

Aclaración: Se debe responder correctamente TODOS los ítems del ejercicio.

1. **Classful routing es el mecanismo por el cual se particionan las redes debido a que aprovecha mejor el espacio de direcciones.**

FALSO, se pierden muchas direcciones porque si tienes una ip de mas tienes que consumir el doble de hosts

Classful avanza de a octetos !=\Classless: avanza de a bits

2. **Al subnetear un espacio de direcciones de clase C, un host puede tener asignada cualquiera de las 256 direcciones posibles.**

C es /24. Falso porque hay 2 reservadas.

B es /16 puedo usar 2 a las 16-2

3. **Con classful routing las clases de red se pueden identificar sin necesidad de conocer la máscara.**

Verdadero porque hay una asignación según rangos a cada clase

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

4. **Todas las direcciones asignadas a un mismo dispositivo deben pertenecer a la misma subred.**

FALSO. porque cada router está en más de una subnet y tienen una ip diferente por cada red en la que están

Supongamos que tengo #Host= 253 y +2 +1router = 256.... que bloque asigno? 256

DEALBREAKERS

forwarding vs routing

Forwarding: cuando un paquete llega al enlace de entrada de un router, el router debe mover el paquete al enlace de salida apropiado. Toma muy poco tiempo, típicamente en la medida de nanosegundos. Se suele implementar en hardware. Viene un paquete, miro su red con máscara y miro la tabla (lookup) para ver donde salir

Routing: se debe determinar la ruta o el camino tomados por los paquetes a medida que viajan del emisor al receptor. Toma un poco más de tiempo, en la medida de los segundos. Se suele implementar en software.

Routing es planear todo el camino desde el sender al receiver.

Forwarding es dentro de un router determinar cuál va a ser la salida.

control plane vs data plane

Data plane hace Forwarding (mirar la tabla)

Control plane hace routing (armar la tabla)

The control plane decides how data is managed, routed, and processed, while the data plane is responsible for the actual moving of data. For example, the control plane decides how packets should be routed, and the data plane carries out those instructions by forwarding the packets

¿QUÉ ES SDN? Software Defined Network

¿Qué hace? Controla las tablas de ruteo

Las redes definidas por software utilizan soluciones de software para definir la topología de la red. Todo esto se consigue mediante la separación del plano de control del plano de datos.

maneja los protocolos de ruteo y el procesamiento de paquetes control Plane desde una unidad central controller y separar dichas funciones de aquellas netamente relacionadas con el envío de paquetes

QUE ES ICMP? es un complemento de ip, esta en la capa de red

Que es ping? Herramienta de software de administración de redes que se utiliza para probar la accesibilidad de un host en una red IP.

control de flujo vs control de congestión

Flujo: el receptor te dice a través de la RWND cuántos bytes puede seguir recibiendo según la capacidad de su buffer

Congestión: vas cambiando la CWND para limitar la cantidad de paquetes que mandas según la congestión (se detecta con RTTs/acks duplicados) La congestión es producto de múltiples flujos TCP en simultáneo sobre la misma red

Que es DNS.

Es un protocolo de la capa de aplicación que traduce ips <-> hosts . Este utiliza UDP ya que es connectionless y así no agrega tanto delay en la consulta.

provee:

- load balancing
- host aliasing
- mail aliasing

Características UDP? y TCP?

udp: Es connectionless - ofrece mux/demux - no confiable - provee control de integridad (checksum)
tcp: Orientado a la conexión (handshake) - confiable (rdt) - control de congestión - control de flujo - mux y demux - checksum, full duplex - bidireccional

¿Qué es RDT?

En orden, lleguen todos y servicio de integridad o sea que no estén corruptos, rotos, vacíos, etc.

Syn flood y cookies?

ataque Dos que manda muchos Syn y el servidor reserva espacio y cuando llega el verdadero cliente no lo puede atender porque te tiro abajo todo.

Crea un número de secuencia tcp inicial que es una función Hash de las direcciones ip de origen y de destino y los nros de puerto del segmento SYN

Cookies: EL servidor en vez de reservar memoria y un puerto al recibir el primer paquete de un handshake, el SYN, lo codifica dentro de el valor de ACK que responde al cliente. Luego, si el cliente responde con el tercer paquete del handshake, el ACK, puede reconstruir la información restando uno a el sequence number de dicho paquete. De esta forma evita reservar recursos al recibir muchos paquetes SYN y solo lo realiza en caso de finalizar el handshake.

Que es multiplexar y Demux

Multiplexar es divide el mensaje de App en segmentos Se agrega el header con sus identificadores Se lo pasa a la capa de red

Demultiplexar es agarrar todos los paquetes y darselos al socket que corresponde

Objetivo de la capa de transporte: Comunicar procesos (apps!) corriendo en diferentes hosts