apunteParcial2

FedericoPolidoro

Contents

TCP

Es un protocolo muy utilizado por distintos motivos uno de los cuales es que asume muy poco de la red en la que esta funcionando por lo que puede tanto funcionar en redes ethernet simples como en otras más complejas. Ademas es preferido en situaciones donde se envian grandes volumenes de datos y un protocolo sin coneccion ni deteccion de errores no es lo más optimo porque obliga al ingeniero a programar esto manualmente en la aplicacion en la capa 8 (OSI).

Caracteristicas

1. Oritentacion de flujo,

Cuando dos programas de aplciacion transfieren grandes volumenes de datos, pensamos en los datos como un flujo de bits, divididos en octetos de 8 bits. El servicio de entrega en la maquina destino pasa al receptos la misma secuencia de octetos que los emitidos.

1. Conexion de circuito virtual,

La transferencia de flujo es analoga a realizar una llamada telefonica. Conceptualmente las computadoras realizan llamadas las cuales las receptoras tienen que aceptar para empezar la comunicacion.

1. Transferencia con memoria intermedia,

Las aplicaciones envian un flujo de datos a través del circuito virtual pasando repetidamente octetos de datos al software de protocolo. Cuando transfieren datos la aplicacion usa piezas de memoria del tamaño que encuentre adecuado. En el extremo receptor se entrega a la aplicacion los octetos en el orden en el cual fueron enviados

De forma independiente de cuantos bytes llegen en cada x tiempo. El receptos va a acumular los bytes recibidos hasta hacer un datagrama lo suficientemente grande antes de entregarlo a la aplicacion del receptor. De la misma forma si

se envia un datagrama muy grande el **SO** receptor puede separar los datos en datagramas más pequeños.

En caso de que no se llegue a llenar la memoria intermedia donde se almacena el datagrama antes de darlo a la aplicacion existe un mecanismo de (push) el cual se utiliza para forzar la transferencia. sin esperar a que esa memoria se llene. Esto puede dividir los datos transferidos de formas innesperadas por lo que no es un recomendable.

1. flujo no estructurado,

Es importante entender que el servicio TCP/IP no esta obligando a formar flujos estructurados. Osea no se pueden poner en comunicacion entre el emisor y receptor para definir el formato que se va a utilizar antes de iniciar la conexión.

1. Conexión full-duplex,

Las conecciones con TCP proveen una coneccion en ambas direcciones

Confiabilidad

Si bien el protocolo IP solo soporta la entrega no confiable de paquetes, TCP solo soporta la entrega confiable de paquetes esto realizado gracias a que utiliza un sistema el cual solo envia el siguiente paquete cuando recive un ACK si recive NAK o se termina el tiempo reenvia el paquete que no recibio afirmacion.

Puertos y conexiones

Al igual que UDP, TCP recide sobre IP, Al igual que UDP utiliza numeros para especificar puertos.

cuando hablamos de UDP pensamos en que cada puerto como una cola de salida en la que el software del protocolo coloca los datagramas entrantes. PERO en TCP no es así, ya que para tcp un puerto no es un solo objeto, TCP esta diseñado con el concepto de abstraccion de conexion por lo que se identifica es en realidad un cirtuito virtual, esto es necesario de entender para poder explicar que significan los numeros de puertos en TCP.

Es Visualizable si pensamos en como identifica el emisor TCP, Este ubica 2 direcciones IP (Emisor)(Receptor) pensemoslo como (181.245.21.244) que supongamos corresponde a mi casa y (136.134.65.33) que corresponde supuestamente a la de la pagina de la uai. por lo que si hubiera una conexion entre los dos puntos se definiria como

(181.245.21.244, 666)(136.134.65.33, 22).

y si hubiera otro servidor en la otra sede de la uai que este conectada con la anterior podria representarse comom

(233.25.1.44, 1234)(136.134.65.33, 22).

Pero que esta pasando porque hay dos conecciones contra el puerto 22 de la primera sede de la uai.
Como TCP identifica las cionecciones con un par de puntos extremos varias conecciones en la mismsa maquina pueden compartir el mismo numero de puerto tcp.

Conexiones Pasivas

TCP al ser orientado a la conexion requiere que ambos puntos esten de acuerdo en participar. Esto antes de que el trafico TCP pueda pasar a través de una red de redes, los programas de aplicacion en ambos extremos. estos deben de estar de acuerdo en que desean la conexión.

Formato Paquetes TCP

Estos estan formados por dos partes: header y payload. En el header se guardan los datos de la identificacion y la informacion de control. Los datos de Src Port y Dest Port tienen los numeros de los puertos tcp que identifican a los programas de aplicacion en los extremos de la conexión.

Hlen tiene el numero que especifica la longitud del header en multiplos de 32bit porque el campo options puede variar en longitud.

El campo CODE puede tener los siquientes datos

CODE	que es
URG	campo urgente es valido
ACK	El campo acuse es valido
PSH	se solicita un push
RST	se inicia la comunicacion
SYN	sincroniza numeros de secuencia
FIN	el emisor llego al final de su flujo de datos

Un header TCP tiene una longitud de 20 bytes.

Suma de Verificacion

El campo CHECKSUM en él encabezado TCP contiene una suma de verificación de números enteros y los bits que se utiliza para verificar la integridad de los datos junto al encabezado TCP.

Respuesta al congestionamiento

Es una condicion de retraso severo Tcp reduce su velocidad de transmision. Los ruteadores verifican la longitud de las colas de salida y en base a eso utilizan

ICMP para informar a los anfitriones que hay un congestionamiento. Aunque hay otra forma de reducir el congestionamiento y viene ya implementada en TCP que es limitar la velocidad de trasmision de forma automatica utilizando 2 tecnicas:

- Arranque lento.
- Disminucion multiplicativa.

En una coneccion no consgestionada la ventana será del mismo tamaño que la anterior, pero una reduccion en el tamaño de la ventana tambien reducirá la cantidad de informacion que TCP inyectará en la red. Para reducir el tamaño de la ventana se toma por hecho que la perdida de datagramas proviene del congestionamiento de la red por lo que al tener una perdida reduce la ventana a la mitad y aumentan el temporizador de forma exponencial para la retrasmisión.

Pero como se recupera TCP de estas reducciones? en esto toma protagonismo el arranque lento que de forma aditiva aumenta la cantidad de datagramas enviados de a 1 por cada ACK recivido. Esto aunque pueda parecer lento no lo es para nada. por lo que TCP tiene una segunda restriccion al momento de incrementar la cantidad de datagramas enviados. Esta consiste en que cuando una ventana llega a la mitad de su tamaño este entra en un modo de prevencion del congestionamiento donde hace aun más lento el aumento de datagramas enviados. donde para que aumente la cantidad de segmentos por ventana enviados se necesita que todos den ACK.

Estableciendo una coneccion

Se utiliza un saludo de 3 etapas las cuales son:

1. Envio de un Syn.
2. Devolucion Syn + Ack.
3. Envio Ack.

Terminacion Conexion TCP

Las conversaciones TCP se pueden cerrar cortesmente con una operacion close. Como las conexiones son full duplex si un lado envia un close solo se cierra la coneccion en una direccion y la otra tiene que enviar un close tambien cuando termine de trasmitir datos. Utiliza una modificacion del handshake donde en vez de un Syn envia un Fin

1. Envio de un Fin.
2. Devolucion Fin + Ack.
3. Envio Ack.

Restablecimiento

En algunas ocaciones las conexiones son expuestas a condiciones anormales por lo que es necesario interrumpir la conexion. por lo que existe el reset.

Para iniciar una conexión, un lado inicia la interrupción enviando un: segmento con el bit RST activado en el campo CODE. Esto genera una desconeccion inmediata.

https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fimage.slidesharecdn.com%2Ft3tcp-150414054318-conversion-gate01%2F95%2Fprotocolo-tcp-38-638.jpg%3Fcb%3D1428990267&f=1&nofb=1&ipt=ceb4ca3dff72adec5c9f367c9fe38720a30871c99d66ccfa0a3daa00c0f8debd&ipo=images

Puertos Reservados

Los primeros 1024 puertos son los que se utilizan para aplicaciones determinadas, lo que es más algunos sistemas operativos requieren que estes en un modo de privilegios asendido para poder bindear a esos puertos. Los de 1025 inclusive para arriba se pueden usar libremente.

Tablas de Ruteo

Estas son tablas que se generan en el router para que el mismo no este pidiendo todo el tiempo todas las direcciones ip con cada intento de coneccion.

Tabla Vector-Distancia

Es cuando un router genera una tabla de todas las rutas conocidas y las mide segun la cantidad de saltos que tenga que realizar para poder alcanzar dicha red.

Protocolos SPF

Conocido como ruteo enlace estado, Estos requieren que todos los ruteadores participes tengan conocimiento sobre la topologia de la red, es decir, que tengan un mapa con todos los ruteadores a las que esta conectado. Spf es el acronimo de Shortest Path First.

Exterior Gateway Protocol

Se utilizan los routers que dan contra la frontera de la red para difundir informacion sobre la accesibilidad.
Los tipos de mensajes que puede enviar EGP son:

Tipo Mensaje	Desc
Request	Solicitud de que un router se identifique como vecino
Confirm	Confirma soluciud de adquisicion
Refuse	Rechasa la solicitud
Cease Req	Solicita finalizar la relacion vecino
Cease Conf	Confirma la finalizacion de la relacion

Tipo Mensaje	Desc
Hello	Basicamente un ping
I Heard You	la respuesta del ping
Poll Req	Solicitud de actualizar el ruteo de red
Routing update	Informacion de accesiblidad de red
Error	Respuesta mensaje incorrecto

Sistemas autonomos

Estas son conjuntos de redes las cuales estan bajo control de una sola entidad administrativa, Esta teniendo conocimiento de todas las redes que conforma independientemente de que sean ocultas o no

Ruteo dentro de un sistema autonomo

Definidos como IGP son los protocolos que los sistemas autonomos utilizan para poder hacer llegar los datos entre los routers internos.

RIP

Es un protocolo que funciona gracias a que los routers mantienen una tabla de ruteo con la cantidad de hops de una red a otra limitando esta en que no puede tener más de 15 saltos. Además las tablas son eliminadas cada 30s. Es el protocolo más utilizado para las redes autonomas.

Cada cierto tiempo los routers anuncian su tabla de ruteo a los routers vecinos. Estos reciben los datos y los comparan con los suyos si una ruta recibida es más corta que una ya definida esta pasa a ocupar el espacio de la ruta menos optima.

Tiene un problema de consumo de ancho de banda y por eso existen protocolos que solo pasan los cambios en vez de la tabla entera.

OSPF

En un protocolo usado en redes grandes que usa el algoritmo de dijkstra. Sus caracteristicas son:

- Rapida Convergencia,
  `Osea en caso de un error recalcula rapido`
- Costo de enlase,
  `Como con un grafo ponderado utiliza una nocion de costo con las conecciones y elija la de menos costo`

Cliente-Servidor

Es un modelo en el cual un programa servidor ofrese un servicio y un programa cliente consume dicho servicio

Socket

Consiste de un descriptor que referencia uno de los extremos de una conexion.

BOOTP y DHCP

creados como una alternativa al protocolo RARP. **BOOTP** es un protocolo UDP el cual usa puertos 67 y 68 para en base a una direccion mac dada dar la direccion ip configurada.

Mientras que DHCP utiliza un Protocolo algo más complejo con leasing por tiempo de direcciones donde un cliente pide una direccion ip al servidor y el servidor le entrega una direccion por una x cantidad de tiempo. Tambien usa los puertos 67 y 68 udp porque es retrocompatible con BOOTP.

Ambos protocolos tienen agentes de retrasmision en caso de haber vlans para que el servidor no necesite estar presente en todas las redes virtuales para poder darles servicio.

Doy lista de codigos DHCP:

code	desc
Discover	Descubre servidores dhcp
Offer	Respuesta del servidor al cliente
Request	el cliente pide una ip
Decline	el servidor declina la request
Ack	respuesta del servidor al request para que se pueda usar la ip priv
Nack	Respuesta negativa del servidor a la request
Release	cliente suelta ip asignada

Telnet

Es un protocolo para acceder a servidores de forma remota, ya no tan utilizado, tiene reservado el puerto 23/tcp. No es cifrado

Rlogin

Es como Telnet pero no es necesario ingresar contraseña cada vez que te logeas. sino que si estas en una lista de hosts confiables podes entrar sin necesitar

credenciales. Tampoco casi no se usa. Es inseguro.

Ftp

Es un protocolo con autentificacion para trasferir archivos en redes. No tiene Cifrado y es ampliamente reemplazado por SFTP. usa tcp 21

TFTP

Es un protoco muy simple si autentificacion para transferencia de archivos en redes locales. Es común verlo utilizado para la carga de archivos de configuracion para los routers.

NFS

es un sistema de archivos compartidos en la red para sistemas unix (tambien usado para el networkbooting). Permite la lectura de archivos y puede incluir auth.

SMTP

Es el protocolo que es utilizado para enviar emails a través de la red. Comunmente usa los puertos 25(servidor-Servidor), 587 o 465 para cliente a servidor.

POP3 / Imap

Ambos son protocolos que se encargan de leer emails de un servidor y mostrarlos en un cliente para lectura de emails (como thunderbird, windows emails, etc).

- POP3,
  `Todos los emails se envian a un solo dispositivo con almacenamiento y tiene sincronizacion minima`
- IMAP,
  `Los emails son almacenados en servidor para siempre y tiene implementado sincronizacion entre muchos dispositivos en paralelo`.

SNMP

Es un protocolo de capa de aplicacion utilizado para intercambiar informacion entre dispositivos de red