TCP/IP

INTRODUCCIÒN

A finales de los años 60 y principios de los 70, las redes no estaban diseñadas de forma que fuera posible compartir recursos entre redes diferentes. Por su parte, los administradores de las redes eran reacios a permitir que los usuarios invadieran sus recursos por motivos de seguridad. Además, experimentaban una utilización excesiva de los recursos de las redes. Como resultado, era difícil que los usuarios extendieran el uso de sus sistemas de información a otros usuarios en redes diferentes. O bien las redes eran incompatibles entre sí, o no podían comunicarse debido a problemas de administración.

Desde entonces se ha hecho cada vez más patente la necesidad de que las aplicaciones de usuario compartan recursos. Pero para que puedan hacerlo, los administradores de las redes deben acordar primero un conjunto de tecnologías y normas comunes para que las redes puedan comunicarse. De ahí se sigue que las aplicaciones como la transferencia de archivos y el correo electrónico se deberían estandarizar también, para permitir la interconexión entre aplicaciones de usuario (no sólo la conexión de las redes). El Protocolo de Control de Transmisión y el Protocolo Internet (TCP/P) se desarrollaron con esos objetivos. En este capítulo se analizarán protocolos.

TCP/IP Y COMUNICACIONES ENTRE REDES

Con objeto de comprender la forma de funcionar de TCP/IP, hay que presentar previamente algunos términos y conceptos. En la figura 10-1 se utilizan los términos pasarela (gateway) y sistema de encaminamiento (router) para denominar a las máquinas que realizan las retransmisión entre redes. En la figura 10-1 se muestra una pasarela situada entre las redes A, B y C.

Las redes A, B y C se denominan comúnmente subredes. Esta denominación no quiere decir que realicen menos funciones que las redes convencionales, sino que las tres redes forman un única red lógica y las subredes contribuyen en las operaciones globales de interconexión. Dicho de otro modo, las tres subredes forman un interred (Internet).

Las pasarelas entre redes se diseñan de forma que sean transparentes a las aplicaciones de los usuarios finales. De hecho, las aplicaciones de usuarios residen en computadoras conectados a las redes. Es raro que las pasarelas tengan aplicaciones de usuario. Este esquema resulta atractivo desde de diversos puntos de vista. En primer lugar, la pasarela no necesita cargarse con los protocolos del nivel de aplicación. Como no son invocados por la pasarela, ésta se puede dedicar a otras tareas, como la gestión del tráfico entre las redes. No se ocupa de funciones del nivel de aplicación como acceso a bases de datos, correo electrónico y gestión de archivos.

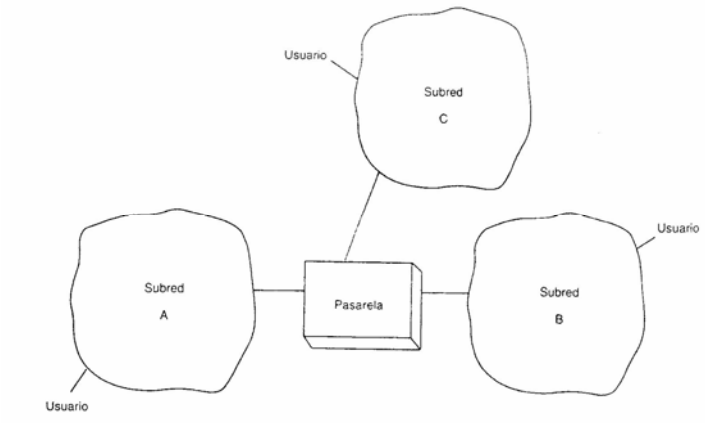

Figura 10-1. Subredes y pasarelas

En segundo lugar, este esquema permite que la pasarela dé soporte a cualquier tipo de aplicación, ya que considera que el mensaje de la aplicación no es más que una unidad de datos de protocolo transparente (PDU).

Además de la transparencia para el nivel de aplicación, la mayoría de los diseñadores intentan que las pasarelas sean transparentes a las subredes, y viceversa. Es decir, a la pasarela no le importa el tipo de red que se conecta con ella. El propósito principal de la pasarela es recibir una PDU que contenga información de direccionamiento suficiente para que se pueda encaminar hacia su destino final o hasta la pasarela siguiente. Esta característica es muy atractiva, ya que convierte a la pasarela en algo modular, que se puede utilizar con diferentes tipos de redes.

Hay que escribir software que permitan la comunicación entre el protocolo de la subrede y la pasarela. Estos módulos son característicos de cada esquema completo y las normas no describen el interfaz entre la subred y la pasarela. Hay una excepción, que es la publicación de definiciones de servicio Internet, ISA e IEEE, que describen procedimientos entre los protocolos de los computadores principales y de las pasarelas (niveles).

EJEMPLO DE LAS OPERACIONES DE TCP/IP

La figura 10-2 muestra la relación entre las subredes y las pasarelas y los protocolos de niveles. Se supone que la aplicación de usuario del computador A envía una PDU de aplicación al protocolo del nivel de aplicación del computador B, como en un sistema de transferencia de archivos. El software de transferencia de archivos realiza unas determinadas funciones y añade una cabecera de transferencia de archivos a los datos de usuario.

Como indican las flechas que apuntan hacia abajo en los niveles del computador A, esta unidad se pasa a TCP, que es un protocolo de nivel de transporte. TCP realiza varias funciones (que veremos enseguida) y añade una cabecera a la PDU que se le transfiere. La unidad de datos se denomina ahorra segmento. Las PDU de los niveles superiores son consideradas por TCP como datos.

Después, el TCP pasa el segmento al nivel de red. Que trabaja con IP, IP realiza de nuevo unos determinados servicios y añade otra cabecera. La unidad resultante (denominada datagrama en la terminología de TCP/IP) se pasa a los niveles inferiores. El nivel de enlace de datos añade una cabecera y una cola, y la unidad de datos (que ahora se denomina trama) se envía a la red a través del nivel físico. Si el computador B enviara datos al computador A, el proceso se invertiría y, por supuesto, la dirección de las flechas cambiaria.

TCP/IP no tiene conocimiento de lo que realmente circula por la red. El gestor de la red es libre de manejar la PDU de cualquier forma que considere necesaria. Sin embargo, en la mayoría de los ejemplos, la PDU Internet (datos y cabeceras) no cambian mientras se transmite por la subred. En la figura 10-2 vemos el papel de la pasarela, donde la unidad de datos atraviesa los niveles inferiores hasta llegar al nivel IP (de red). En ese nivel se toman las decisiones de encaminamiento bajándose en la información de direccionamiento proporcionada por el computador principal.

Después de tomar las decisiones de encaminamiento, el datagrama se envía el enlace de comunicaciones conectado con la subred apropiada (que consta de los niveles inferiores). El datagrama es reencapsulado para formar una PDU (denominada trama) en el nivel de enlace de datos y se pasa la subred siguiente. Como antes, esta unidad se mueve por la red de forma transparente (habitualmente) hasta que llega finalmente al computador destinado.

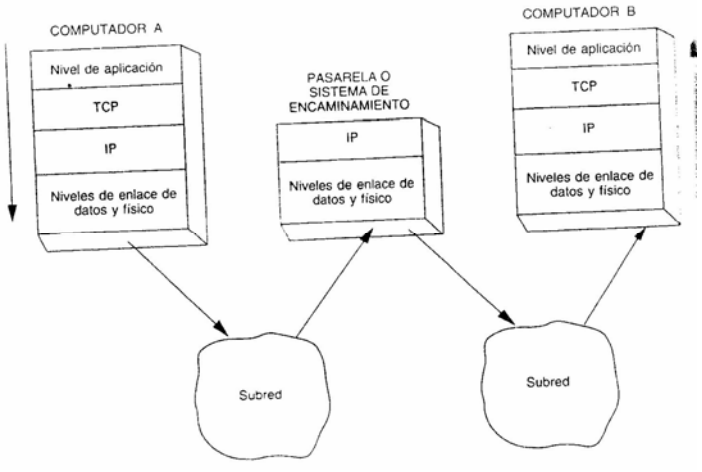

Figura 10-2 Ejemplo de operaciones de TCP/IP

El computador destinado (computador B) recibe el tráfico a través de los niveles inferiores e invierte el proceso que se realizó en el computador A. Es decir, realiza el desencapsulado retirando las cabeceras en el nivel apropiado. Cada cabecera es utilizada por el nivel apropiado para decidir las acciones a realizar. Es decir, la cabecera correspondiente gobierna las operaciones que se realizan en cada nivel.

La PDU creada por la aplicación de transferencia de archivos se pasa a la aplicación de transferencia de archivos que reside en el computador B. Si los computadores A y B fueran grandes computadores (mainframes), esta aplicación sería seguramente un duplicado exacto del software del computador transmisor. Sin embargo, la aplicación puede llevar a cabo diversas funciones, dependiendo de la cabecera que reciba. Por ejemplo, los datos podrían pasarse a otra aplicación del computador B. No obstante, en muchos casos el usuario del computador A sólo desea obtener los servicios de un protocolo servidor, como, por ejemplo, un sistema de transferencia de archivos o un servidor de correo electrónico. Si ese fuera el caso, no sería necesario invocar ningún proceso de usuario final en el computador B.

Para devolver los datos del servidor en el computador B al cliente en el computador A, los datos descienden por los niveles del computador B, pasan por la red, viajan de una pasarela a otra y ascienden por los niveles de A hasta el usuario final.

PROTOCOLOS RELACIONADOS

TCP/IP puede funcionar conjuntamente con una amplia variedad de protocolos. Los protocolos que se apoyan en TCP son ejemplos de protocolos de nivel de aplicación, que suministran servicios como transferencia de archivos, correo electrónico, servicios de terminales, etc. Los dos niveles inferiores representan los niveles físico y de enlace de datos y, como muestra la figura 10-2, se realizan con una amplia variedad de normas y protocolos. Existen otros protocolos que realizan la búsqueda de ruta y que permiten construir las tablas de encaminamiento que utiliza IP para transmitir el tráfico por una interred.

PUERTOS Y “SOCKETS”

Todos los procesos de nivel de aplicación que utilicen protocolos TCP/IP se deben identificar mediante un número de puerto. Este número se utiliza por los dos computadores para identificar qué programa de aplicación va a recibir el tráfico entrante.

El uso de números de puerto proporciona capacidades de múltiplexación, ya que varios programas de usuario se pueden comunicar de forma concurrente con un programa de

aplicación, como TCP. Los números de puerto sirven para identificar a cada aplicación. Este concepto es muy semejante al del punto de aplicación de servicio (SAP) en el modelo ISA.

Además del uso de puertos, los protocolos basados en TCP/IP pueden utilizar también un identificador abstracto denominado socket. El concepto de socket procede de las operaciones de entrada/salida en redes en el sistema Unix BSD 4.3. Es muy similar a los procedimientos de acceso a archivos en UNIX, en el sentido de que se identifica un proceso de comunicaciones entre dos puntos terminales. En TCP/IP, un socket consiste en la concatenación de un número de puerto y la dirección de red (la dirección IP, de la que hablamos posteriormente) del computador que da soporte al servicio de puertos.

En la Internet, algunos números de puerto están ya preasignados. Se denominan puertos bien conocidos (en ingles, well-known ports), y se utilizan para identificar aplicaciones muy comunes que se denominan servicios bien conocidos tienen valores de 0 a 255. Las organizaciones y empresas no deben utilizar números en ese rango, ya que están reservados.

LA ESTRUCTURA DE DIRECCIONES IP

Las redes TCP/IP identifican los computadores y las redes a las que están conectados utilizando direcciones de 32 bits. La figura 10-3 muestra la estructura de una dirección IP. Su formato es DIRECCIÒN IP = DIRECCIÒN DE RED + DIRECCIÒN DE COMPUTADOR.

La dirección IP no identifica por sí misma a un computador, sino más bien la conexión de un computador con su red. En consecuencia, si una máquina se traslada a otra red, su espacio de direcciones deberá ser modificado.

Las direcciones IP se clasifican por sus formatos. Está, permitidos cuatro formatos: clase A, clase B, clase C o clase D. Como muestra la figura 10-3, los primeros bits de la dirección especifican el formato del resto del campo de direcciones en relación con los subcampos de red y computador. La dirección de computador se denomina también dirección local (o campo REST).

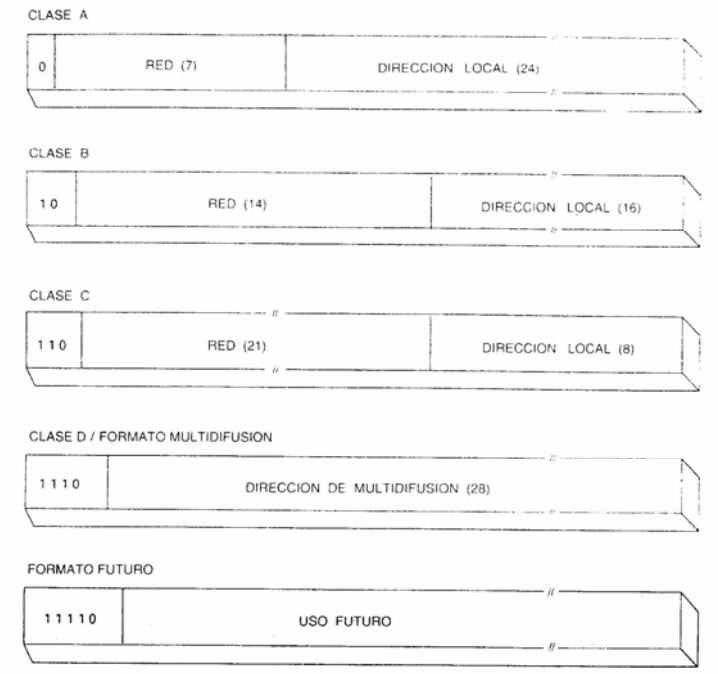

Figura 10-3 Formatos de direcciones IP

Las direcciones clase A se utilizan para redes con un gran número de ordenadores conectados. El campo identificado de ordenador tiene 24 bits. Se podrían identificar, por tanto, hasta 224

ordenadores. El identificar de red ocupa siete bits, con lo que se podrían identificar hasta 127 redes (con los valores de 1 a 127).

Las direcciones de clases B se utilizan para redes de tamaño intermedio. El identificador de red utiliza 14 bits y el identificador de ordenador 16 bits. Las redes de clase C contienen menos de 256 ordenadores (28). El identificador de red utiliza 21 bits. Finalmente, las direcciones de clase D se reservan para multidifusiòn que es una forma de difusión en u área limitada.

PRINCIPALES CARACTERISTICAS DE IP

IP es muy similar a la especificación ISO 8473 (el Protocolo de Redes No Orientadas a Conexión, o CLNP) que se explica en la última sección de esta capítulo. Muchas ideas de ISO 8473 proceden de IP.

IP es un ejemplo de servicio no orientado a conexión. Permite, sin establecimiento de llamada previo, el intercambio de datos entre dos computadores (sin embargo, los dos computadores generalmente comparten un protocolo común de transporte orientado a conexiona). Como IP no es orientado a conexión, se pueden perder datagramas entre las dos estaciones de usuario. Por ejemplo, las pasarelas IP utilizan un tamaño máximo de cola, y si se sobrepasa, los buffers se desbordarán. En esta situación se descartarán datagramas en la red. Por esta razón es fundamental un protocolo de transporte de nivel superior (como TCP) que solucione esos problemas.

IP oculta la subred que hay debajo a los usuarios finales. Crea para ellos una red virtual. Este aspecto de IP es muy atractivo, ya que permite que diferentes redes se conecten a una pasarela IP. Como resultado, IP es razonablemente simple de instalar y, debido a su diseño no orientado a conexión, es muy versátil.

Dado que IP es un protocolo de tipo datagrama, no dispone de mecanismos para proporcionar fiabilidad. No proporciona procedimientos de recuperación de errores en las redes subyacentes ni mecanismos de control de flujo. Los datos de usuario (datagramas) se pueden perder, duplicar o incluso llegar desordenados. No es trabajo de IP ocuparse de esos problemas. Como veremos posteriormente, la mayoría de esos problemas se pasan al nivel superior, TCP.

IP soporta operaciones de fragmentación. La fragmentación es una operación por la que una unidad de datos de protocolo (PDU) se divide y segmenta en unidades más pequeñas. Es una característica que puede ser muy útil, ya que no todas las redes utilizan PDU del mismo tamaño. Por ejemplo, las redes de cobertura amplia (WAN) basadas en X.25 utilizan típicamente PDU (denominados paquetes en el contexto de X.25) con un campo de datos de 128 octetos. Algunas redes permiten negociar tamaños de PDU mayores o menores. El estándar Ethernet limita el tamaño de una PDU a 1500 octetos. En cambio, proNET-10 especifica una PDU de 2000 octetos.

Sin el uso de fragmentación, las pasarelas emplearían recursos para intentar resolver incompatibilidades de los tamaños de las PDU de las diferentes redes. IP resuelve el problema establecimiento unas reglas de fragmentación en la pasarela, y de reconstrucción en el computador receptor.

El datagrama de IP

Una perspectiva muy útil en el análisis de IP consiste en examinar los campos del datagrama de IP (PDU) que se muestra en la figura 10-4.

El campo de versión identifica la versión de IP en uso. La mayoría de los protocolos tienen este campo debido a que algunos nodos pueden no utilizar la última versión del protocolo disponible. La versión actual de IP es la 4.

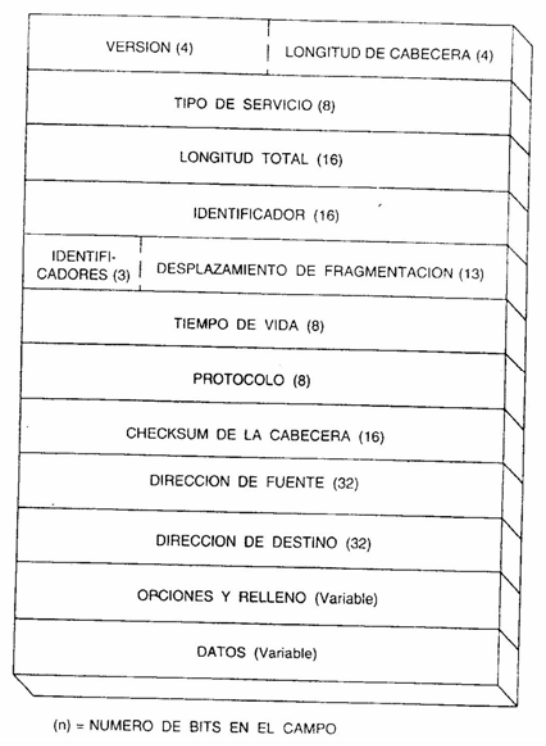

Figura 10-4. El datagrama de IP

El campo de longitud de cabecera contiene cuatro bits con el valor de la longitud de la cabecera del datagrama. La longitud se mide en palabras de 32 bits. Típicamente una cabecera con opciones QQS contiene 20 octetos. Por lo tanto, el valor del campo de longitud habitualmente es de 5.

El campo de tipo de servicio (TOS) se puede utilizar para identificar varias funciones QQS de Internet. El retardo de tránsito, el caudal efectivo, la procedencia y la fiabilidad se pueden solicitar utilizando este campo.

Los siguientes tres bits se utilizan para otros servicios que ase describen a continuación: El bit 3 es el bit de retardo (bit D). Cuando vale 1 este TOS solicita un retardo pequeño por la interred. El aspecto del retardo no esta definido en el estándar, y se deja a criterio del vendedor la posibilidad de utilizar este servicio. El siguiente bits es el bit de caudal efectivo (bit T). Se pone a 1 para solicitar de la interred un alto caudal efectivo. De nuevo, depende de cada sistema y no esta definido en el estándar. El ultimo bit utilizando es el bit de fiabilidad (bit R), que permite que los usuarios soliciten alta fiabilidad para sus datagramas. Los siguientes dos bits (6 y 7) no se utilizan por ahora.

El campo de longitud total especifica la longitud total del datagrama de IP. Se mide en octetos e incluye la longitud de la cabecera y de los datos. IP resta el valor del campo de longitud de cabecera del valor del campo de longitud total para obtener el tamaño del campo de datos. La longitud máxima de un datagrama de es 65 535 octetos (216). Las pasarelas que dan servicio a datagramas de IP deben aceptar cualquier datagrama que soporte el tamaño máximo de las PDU de las redes conectadas. Adicionalmente, todas las pasarelas deben aceptar datagramas de 576 octetos de longitud total.

El protocolo IP utiliza tres campos de datos en la cabecera que sirven para controlar la fragmentación y ensamblando del datagrama. Son el identificador, los indicadores y el desplazamiento de fragmentación. El campo de identificador se utiliza para identificar

unívocamente todos los fragmentos de un datagrama original. Se utiliza junto con la dirección de fuente del computador receptor para identificar el fragmento. El campo de identificadores contiene bits que indican si el datagrama se puede fragmentar y, si se puede fragmentar, uno de los bits se puede poner a 1 para indicar el último fragmento del datagrama original. El campo de desplazamiento de fragmentación contiene un valor que especifica la posición relativa del fragmentación en el datagrama original. El campo de desplazamiento de fragmentación contiene un valor que especifica la posición relativa del fragmento en el datagrama original. Su valor se inicializa a cero y se va poniendo al valor apropiado a medida que la pasarela fragmenta los datos. El valor se mide en unidades de 8 octetos. Dedicaremos una sección especial de este capitulo a la fragmentación y ensamblado con el uso de esos tres campos.

El parámetro de tiempo de vida (TTL) se utiliza para medir el tiempo que un datagrama lleva en la interred. Es muy similar al campo de tiempo de vida de los protocolos de redes no orientadas a conexión. Todas las pasarelas de la interred deben observar este campo y destacarlo si el valor es cero. Las pasarelas deben también decrementar el valor de ese campo en todos los datagramas que procesan. En esquemas reales, el valor del TTL es una medida del "numero de saltos". Por lo tanto, cuando un datagrama pasa por una pasarela ("salta") el valor de ese campo se decrementa en una unidad. Algunas realizaciones de IP utilizan un contador de tiempo para este campo y decrementan su valor en unidades de 1 segundo.

El campo TTL no solo se utiliza para que la pasarela evite bueles sin fin, sino también para que los computadores limiten el tiempo de vida de los segmentos que pasan por la interred. Si hay un computador que actúa como una pasarela, debe tratar los campos TTL con las reglas de las pasarelas. Hay que consultar al fabricante para saber si el computador descarta los datagramas utilizando el valor del campo TTL. Idealmente, los valores del campo TTL se pueden configurar, asignándose su valor en función de las prestaciones observadas de la red. Además, los protocolos de información de gestión de la red, como los que residen en SNMP, podrían desear utilizar el valor del campo TTL para operaciones de diagnostico. Finalmente, si nuestro suministrador utiliza un valor fijo que no se puede reconfigurar, hay que asegurarse de que se fija inicialmente permitiéndose el crecimiento de la interred.

E l campo de protocolo se utiliza para identificar el siguiente protocolo en la estructura de niveles por encima de IP que va a recibir el datagrama en el computador de destino. Es muy similar al campo de tipo presente en la trama Ethernet. Los grupos de normalización Internet han ideado un sistema de numeración que identifica a los protocolos de nivel superior mas ampliamente utilizados. Por ejemplo, el numero 6 identifica a TCP, y el numero 20 identifica al nivel de transporte de ISA (clase 4).

El checksum de la cabecera se utiliza para detectar distorsiones en la cabecera. No se realiza comprobaciones en la cadena de datos de usuario. Algunos sectores críticos a IP indican que si se detectaran errores en los datos de usuario, las pasarelas podrían al menos notificar al computador remitente que hay problemas. En cualquier caso, la solución adoptada en IP hace que algoritmo de comprobación sea muy simple. No tiene que operar con muchos octetos, pero exige que un protocolo de nivel superior en el computador sea el que realice algún tipo de comprobación de errores para velar por la integridad de los datos.

El datagrama de IP lleva dos direcciones. Se denominan dirección de fuente y de destino y no se modifican durante toda la vida del datagrama. Esos campos contienen las direcciones de IP examinadas anteriormente en este capítulo.

El campo de opciones se emplea para identificar diversos servició adicionales, que se trataran en breve. El campo de opciones no se utiliza en todos los datagramas. La mayoría de los esquemas utilizan este campo para gestión de la red y diagnósticos.

El campo de relleno se puede utilizar para asegurarse de que la cabecera del datagrama se alinea exactamente con una división de intervalo de 32 bits.

Finalmente, el campo de datos contiene los datos de usuario. IP estipula que la combinación de los campos de cabecera y de datos no puede sobrepasar 65 535 octetos.

PRINCIPALES SERVICIOS DE IP

Esta sección proporciona una panorámica general de los principales servicios de IP. Los fabricantes suministran diferentes productos para IP, y puede que algunos no soporten todas las características que se describen en esta sección.

Encaminamiento de fuente de IP

IP utiliza como parte de su algoritmo de encaminamiento un mecanismo denominado encaminamiento de fuente. El encaminamiento de fuente permite que un protocolo de nivel superior (ULP) determine la forma en que las pasarelas IP encaminan el datagrama. El ULP tiene la opción de pasar una lista de direcciones interred al modulo de IP. Esta lista contiene los nodos IP intermedios que se van a atravesar durante el encaminamiento del datagrama hasta su destino final. La última dirección de la lista es el destino final de un nodo intermedio.

Cuando IP recibe un datagrama, utiliza la dirección del campo de encaminamiento de fuente para determinar el siguiente salto intermedio. IP utiliza un campo puntero para averiguar la siguiente dirección IP. Si La comprobación del puntero y de los campos de longitud indica que la lista se ha completado, el campo de dirección IP de destino se utiliza para encaminamiento.

El modulo de IP reemplaza entonces el valor de la lista de encaminamiento de fuente con su propia dirección. Por supuesto, hay que incrementar el puntero en el valor de una dirección (4 bytes) para que en el siguiente salto se pueda recuperar la siguiente dirección de IP de la ruta. Con esta solución, el datagrama sigue la lista de fuente dictada por el ULP y almacena también la ruta durante el camino.

Operaciones de encaminamiento. La pasarela de IP toma decisiones e encaminamiento basándose en la lista de encaminamiento. Si el computador de destino reside en otra red, la pasarela debe decidir la ruta de encaminamiento hacia la otra red. Realmente, si el proceso de comunicación involucra varios saltos, hay que atravesar cada pasarela, y las pasarelas deben tomar decisiones sobre el encaminamiento.

En cada pasarela se mantiene una tabla de rutas que contienen la siguiente pasarela a atravesar en el camino hacia la red de destino. Dicha tabla contiene una entrada por cada red alcanzable. Dichas tablas pueden ser estáticas o dinámicas, aunque lo más normal es que sean dinámicas. El modulo de IP realiza las decisiones de encaminamiento de todos los datagramas que recibe.

La tabla de rutas contiene una dirección de IP por cada red alcanzable y la dirección de una pasarela vecina (es decir, una pasarela directamente conectada a esta red). La pasarela vecina es la ruta mas corta hacia la red de destino. En otro caso, la lógica de la pasarela de IP establece que la pasarela esta directamente conectada a esta red.

El encaminamiento de IP se basa en un concepto denominado métrica de distancia. Este valor generalmente no es nada más que el número mínimo de saltos entre la pasarela y el destino final. La pasarela consulta su tabla de encaminamiento e intenta encontrar una dirección de red de destino (contenida en la cabecera) igual a una entrada de red contenida en la tabla de encaminamiento. Si no se encuentra, se descarta al datagrama y se forma un mensaje de error que se devuelve a al fuente de IP (lo que hace un protocolo adjunta a IP, denominado Protocolo de Mensajes de Control de Internet ICMP). El mensaje contiene un código de “destino inalcanzable”. Si se encuentra una dirección igual en la tabla de encaminamiento, la pasarela lo utiliza para determinar el puerto de salida.

Encaminamiento relajado y estricto. IP proporciona dos opciones para el encaminamiento de los datagramas hasta su destino final. El encaminamiento relajado de fuente deja a los módulos de IP libertad para escoger los saltos intermedios que se deben realizar para alcanzar las direcciones obtenidas en la lista de fuentes. En cambio, el encaminamiento estricto de fuente exige que los datagramas viajen solo por las redes cuyas direcciones están indicadas en la lista de fuentes. Si no se puede seguir una ruta estricta de fuentes, el IP del computador original recibe un mensaje de error. Ambos tipos de encaminamiento requieren que exista la característica de grabación de ruta, de la que hablaremos seguidamente.

Opción de grabación de ruta

La opción de grabación de ruta funciona de la misma forma que el encaminamiento de fuente con la característica de grabación que acabamos de discutir. Esto quiere decir que cualquier modulo de IP que reciba un datagrama debe añadir su dirección a una lista de grabación de ruta. Para que se lleve a cabo la operación de grabación de ruta, el modulo de IP receptor utiliza los campos de longitud y de puntero para determinar si hay espacio suficiente para grabar la ruta. Si la lista de grabación de ruta estuviera llena, el modulo de IP simplemente envía el datagrama sin insertar su dirección. Si no estuviera llena, el puntero se utiliza para encontrar el primer intervalo de octeto libre. Se inserta la dirección y el modulo de IP incrementa el puntero hasta el siguiente intervalo de IP.

Opción de marca temporal

Otra opción muy útil de IP es la posibilidad de incluir marcas temporales en los datagramas cuando atraviesan cada modulo de IP de la interred. De esta forma, el gestor de red no solo puede determinar la ruta del datagrama, sino también el instante en el que cada modulo de IP proceso el datagrama. Esto es muy útil para comprobar la eficacia de las pasarelas y de los algoritmos de encaminamiento.

La marca temporal se basa en milisegundos (ms) de la hora universal (la hora de Greenwich). Lógicamente, el uso de la hora universal no garantiza absolutamente que las marcas temporales sean completamente exactas, ya que los relojes de cada maquina pueden diferir ligeramente. No obstante, en la mayoría de las redes, el uso de la hora universal en milisegundos proporciona un grado de precisión razonable.

ICMP

El Protocolo Internet (IP) es un protocolo no orientado a la conexión, y, por tanto, no proporciona mecanismos de corrección ni de información de errores. Se basa en un modulo denominado protocolo de mensajes de control interred (ICMP) para: (a) informar de los errores ocurridos en el procesamiento de los datagramas y (b) proporcionar algunos mensajes de administración y de estatus.

ICMP reside en computadoras o pasarelas y acompañan a IP. Se utiliza en tres computadores y pasarelas por diversas razones, entre ellas: (1) cuando no se puedan enviar los datagramas; (2) cuando las pasarelas encaminan el trafico por rutas mas cortas, o (3) cuando una pasarela no dispone de suficiente capacidad de almacenamiento (buffer) para retener y enviar unidades de datos de protocolo.

ICMP notificara al computador si el destinado no se puede alcanzar. Es también responsabilidad de ICMP gestionar o crear un mensaje de tiempo sobrepasado en el caso de que expire el periodo de vida de un datagrama. ICMP realiza también ciertas funciones de edición para determinar si la cabecera de IP es errónea o ininteligible.

Formato de mensaje de ICMP

La figura 10-5 muestra el formato de los mensajes de ICMP. Esos mensajes se sitúan en la parte de usuario del datagrama de IP. El campo de protocolo de la cabecera de IP se pone a 1 indicar que se esta utilizando ICMP. Todos los mensajes de ICMP contienen tres campos: (a) el campo de tipo define el tipo de mensaje, (b) el campo de código describe el tipo de error o información de estatus y (c) un campo de checksum para calcular un complemento de unos de 16 bits del mensaje de ICMP. El mensaje de errores de ICMP lleva también la cabecera de interred y los primeros 64 bits del campo de datos de usuario. Esos bits son muy útiles en el análisis y resolución de problemas.

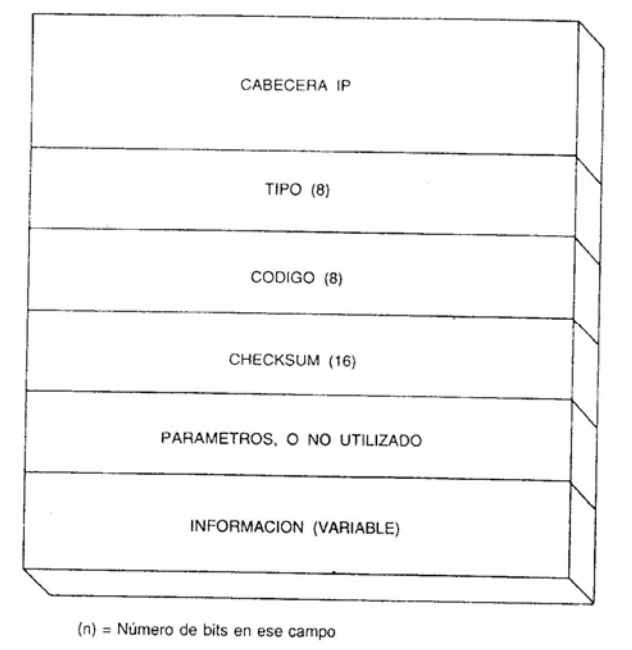

Figura 10-5 El formato de mensajes de IP

Procedimientos de información de errores y estatus

Los servicios de información de errores y status tal como indica ICMP se resumen a continuación:

· Exceso de tiempo de vida del datagrama: servicio ejecutado por una pasarela en el caso de que el tiempo de vida del datagrama de IP haya expirado (el valor del campo correspondiente es cero) y la pasarela descarta el datagrama.

· Parámetro no comprensible: El computador o pasarela de servicio invoca, este servicio si encuentra problemas al procesar cualquier parte de una cabecera IP. Típicamente, esto ocurre cuando un campo no es comprensible y por tanto no se puede procesar al datagrama.

· Destino inalcanzable: Este servicio es utilizado por una pasarela o por el computador de destino. Una pasarela lo invoca si encuentra problemas para alcanzar la red de destino especificada en la dirección de destino de IP. También lo puede utilizar un computador de destino si no puede identificar un protocolo de alto nivel disponible, o si un puerto especificado no esta disponible (inactivo).

· Congelación de fuente: Este servicio es una forma de control de flujo para evitar congestiones. Este servicio es invocado por una maquina cuando no tiene suficiente espacio de almacenamiento para poner en cola los datagramas que van llegando. Si un datagrama se descarta, el sistema de encaminamiento puede enviar este mensaje al computador origen del datagrama.

· Eco y respuesta de eco: La solicitud y respuesta de eco son muy útiles para determinar el estado de la interred. El eco se puede enviar a cualquier dirección de IP, como, por ejemplo, una pasarela. La pasarela debe devolver una respuesta de eco al solicitante. De esta forma los administradores de las redes pueden saber cual es el estado de los recursos de la red. Si no se recibe respuesta, es indicativo de problemas.

· Redirección: Este servicio sirve para suministrar al computador información de gestión de encaminamiento y es invocado por una pasarela. Se envía un mensaje ICMP al computador fuente. La redirección del mensaje indica que hay disponible una ruta mejor. Esto quiere decir que el computador debería enviar su tráfico a otra pasarela. La mayoría de las veces, la pasarela genera este mensaje de redirección si su tabla de rutas indica que el siguiente salto (el computador destino u otra pasarela) esta en la misma red que la red contenida en la dirección de fuente de la cabecera IP.

· Marca temporal y respuesta de marca temporal: Este servicio es utilizado por las pasarelas y computadores para determinar el retardo empleado en el envió de trafico por la redes. La unidad de datos de ICMP contiene tres valores de marcas temporales:

· Marca temporal de origen, La hora en que el remitente proceso por última vez el mensaje antes de enviarlo (se rellena inmediatamente antes del envió).

· Marca temporal de recepción. Instante en que el sistema que envía el eco proceso el mensaje por primera vez tras recibirlo (se rellena inmediatamente antes de enviar la respuesta).

· Solicitud de información o respuesta de información: Este servicio es utilizado por los computadores para determinar la red a la que esta unido. Los computadores envían este mensaje ICMP con los campos de direcciones fuente y destino de las cabeceras de IP acero, que significa “esta red”. Un modulo de IP de respuesta (designado como servidor y autorizado para llevar a cabo esta tarea) devolverá una respuesta con la dirección completamente especificada tanto en el campo de fuente como en el campo de cabecera de IP.

· Solicitud y respuesta de mascara de direcciones: El uso de la mascara de direcciones permite dividir la parte de “computador” de la dirección de IP una dirección de subred y una dirección de computador. Esta técnica permite al administrador de la red dividir la dirección de red en subredes menores y más manejables. Este servicio se utiliza por los computadores para obtener la mascara de red utilizada en la red donde reside el computador. El computador solicitante puede enviar la dirección directamente a la pasarela de IP o puede difundirla.

VALOR DE NIVEL DE TRANSPORTE

Anteriormente hicimos hincapié en que el Protocolo Internet (IP) no esta diseñado para solucionar problemas ni garantiza el envió de trafico. IP esta diseñado para destacar los datagramas obsoletos o que han sobrepasado el numero de saltos entre redes permitidos.

Ciertas aplicaciones de usuario requieren asegurarse de que todos los datagramas han llegado correctamente a su destino. Es más, el usuario transmisor puede necesitar asegurarse de que el tráfico se ha enviado al computador receptor. Los mecanismos para realizar esos importantes servicios reside en TCP (UDP es no orientado a conexión y no proporciona esos servicios).

El trabajo de TCP puede ser muy complejo. Debe ser capaz de satisfacer un amplio rango de requerimientos de las aplicaciones e, igualmente importante, debe ser capaz de adaptarse a un entorno dinámico en la interred. Debe ser capaz de establecer y gestionar sesiones (conexiones lógicas) entre los usuarios locales y los remotos. Esto significa que TCP debe tener conocimiento de las actividades de los usuarios para dar soporte a la transferencia de sus datos por la interred. En el siguiente capitulo volveremos de nuevo sobre estos temas.

TCP

Como muestra la figura 10-6, YCP reside en el nivel de transporte del modelo de niveles convencional. Esta situado entre IP y los niveles superiores. La figura ilustra también que TCP no esta cargado en las pasarelas. Esta diseñado para residir en los computadores o en las maquinas que se ocupan de conservar la integridad de la transferencia de datos entre extremos. Lo más común es que YCP resida en los computadores de usuario.

Como IP es una red no orientada a conexión, es TCP quien se debe encargar de las tareas de fiabilidad, control de flujo, secuenciamiento, aperturas y cierres. Aunque TCP e IP estén relacionados que incluso se les denomine juntos “TCP/IP”, TCP puede soportar otros protocolos. Por ejemplo, otro protocolo no orientado a conexión como el ISO 8473 (Protocolo de Redes No Orientadas a Conexión o CNLP) podrían funcionar con TCP (sise realizan algunos ajustes de los interfaces entre módulos). Además, los protocolos de aplicación, como el Protocolo de Transferencia de Archivos (de siglas en ingles FTP) y el Protocolo de Transferencia de Correo Simple (de siglas en ingles, SMTP se apoyan en muchos servicios que proporciona TCP.

Principales características de TCP

TCP suministra una serie de servicios a los niveles superiores. Esta sección presenta brevemente esos servicios.

TCP es un protocolo orientado a conexión. Esto quiere decir que TCP mantiene información del estado de cada cadena de datos de usuario que circula por el. E l término utilizado en este contexto significa también que TCP es responsable de la transferencia de datos entre extremos por la red o redes hasta la aplicaron de usuario receptora (o el protocolo de nivel superior). Refiriéndonos de nuevo a la figura 10-2, TCP debe asegurarse que los datos se transmitan y se reciben correctamente por los computadores atravesando las correspondientes redes.

Como TCP es un protocolo orientado a conexión, es responsable de la transferencia fiable de cada uno de los caracteres (bytes u octetos) que reciben del nivel superior correspondiente. En consecuencia, utiliza números de secuencia y aceptaciones/rechazos.

El término asociado con estos aspectos de los protocolos orientados a conexión es el circuito virtual.

Cada octeto transmitido lleva un número de secuencia. El modulo TCP receptor utiliza una rutina de cheksum para comprobar la posible existencia de daños en los datos producidos en el proceso de transmisión. Si los datos son aceptables, TCP envía una aceptación positiva (ACK) al modulo TCP remite. Si los datos han resultado dañados, el TCP receptor los descarta u utiliza un número de secuencia para informar al TCP remitente del problema. Como muchos otros protocolo orientados a conexión, TCP emplea temporizadores para garantizar que no transcurre un lapso de tiempo demasiado grande antes de la transmisión de aceptaciones desde el nodo receptor y/o de la transmisión de datos desde el nodo transmisor.

TCP recibe datos de un protocolo de nivel superior de forma orientada a cadenas. Esto es diferente a muchos otros protocolos empleados en la industria. Los protocolos orientados a cadenas se diseñan para enviar caracteres separados y no bloques, tramas, datagramas, etc. Los

datos son enviados por un protocolo de nivel superior en forma de cadena, byte a byte. Cuando llegan al nivel TCO, los bytes son agrupados para formar segmentos TCP. Dichos segmentos se transfieren a IP (o a otro protocolo de nivel inferior) para su transmisión al siguiente destino. La longitud de los segmentos la determina TCP, aunque el realizador de un determinado sistema puede determinar la forma en que TCP toma decisión.

Los realizadores de TCP que han trabajado con sistemas orientados a bloques, como los sistemas operativos de IBM, puede que tengan que modificar ligeramente su forma de pensar acerca de las prestaciones de TCP. TCP admiten el uso de segmentos de longitud variable, debido a su diseño orientado a cadenas. Por tanto, las aplicaciones que trabajan normalmente con bloques de datos de longitud fija (una aplicación de gestión de personal que envíe registros de empleados de longitud fija o una aplicación de gestión de nóminas con registros de pago también de longitud fija) no pueden utilizar TCP para transmitir bloques fijos al receptor. El nivel de aplicación debe ocuparse de configurar los bloques dentro de las cadenas de TCP.

TCP comprueba también la duplicación de los datos. En el caso de que el TCP remitente decida retransmitir los datos, el TCP descarta los datos redundantes. Estos datos redundantes podrían aparecer en la interred, por ejemplo cuando el TCP receptor no acepta el tráfico de manera temporizada, en cuyo caso el TCP remitente decidiría retransmitir los datos.

Además de la capacidad de transmisión de cadenas, TCP soporta también el concepto de función push. Esta función se utiliza cuando una aplicación desea asegurarse de que todos los datos que han pasado al nivel inferior se han transmitido. Para hacer eso, gobierna la gestión del buffer de TCP. Para obtener esta función, el protocolo de nivel superior envía una orden a TCP con un indicador de parámetro de push a 1. Esta operación implica que TCP envía todo el tráfico almacenado en forma de segmento o segmentos hacia su destino.

Además de utilizar los números de secuencia para las aceptaciones, TCP los utiliza para la reordenación de los segmentos que llegan a su destino fuera de orden. Como TCP descansa sobre un protocolo no orientado a conexión, es bastante posible que en la interred se creen datagramas duplicados. TCP también elimina los segmentos duplicados.

TCP emplea un esquema de aceptación inclusiva. El numero de aceptación acepta todos los octetos hasta (e incluyendo) el del numero de aceptación menos uno. Este esquema es un método muy sencillo y eficiente de aceptar tráfico, pero presenta una desventaja. Por ejemplo, supongamos que se han transmitida diez segmentos y debido a las operaciones realizadas durante el proceso de encaminamiento llegan desordenados. TCP esta obligado a aceptar solo el mayor numero de bytes contiguos recibidos sin error. No esta permitido aceptar el byte de mayor numero recibido hasta que hayan llegado todos los bytes intermedios. Por tanto, como en cualquier otro protocolo orientado a conexión, podría transcurrir el periodo de temporizacion de aceptaciones y TCP transmisora retransmitiría el tráfico no aceptado todavía. Esas retransmisiones podrían introducir una considerable sobrecarga en la red.

El modulo TCP receptor se ocupa también de controlar el flujo de los datos del transmisor, lo que es muy útil para evitar el desbordamiento de los dispositivos de almacenamiento y la saturación de la maquina receptora. La idea que utiliza TCP es algo poco usual en protocolos de comunicaciones. Se basa en enviar al dispositivo transmisor un valor de “ventana”. Se permite que el transmisor envié un numero máximo de bytes igual al valor de su ventana. Cuando se ha llegado a ese valor, la ventana se cierra y el transmisor debe interrumpir el envió de datos.

Además, TCP posee una facilidad muy útil que permite multiplexar varias sesiones de usuario en un mismo computador. Esta operación se realiza definiendo algunos convenciones para combatir puertos y sockets entre usuarios.

TCP proporciona transmisión en modo duplex integral entre las entidades que se comunican. De esta forma, la transmisión se puede efectuar en ambos sentidos sin necesidad de esperar a la señal de indicación de cambio de sentido, necesaria en las transmisiones semiduplex. Además, TCP permite a los usuarios especificar niveles de seguridad y prioridades de las conexiones. Aunque esas opciones no están incluidas en todos los productos TCP, están definidas en el estándar TCP.

TCP proporciona el cierre seguro de los circuitos virtuales (la conexión lógica entre dos usuarios). El cierre seguro se ocupa de que todo el tráfico sea reconocido antes de la desactivación del circuito virtual.

Aperturas activa y pasiva

Los puertos TCP pueden establecer dos tipos de conexiones. El modo de apertura pasiva permite que el protocolo de nivel superior (por ejemplo, un servidor) indique al TCP y al sistema operativo del computador que va a esperar la llegada de solicitudes de conexión procedentes del sistema remoto, en lugar de enviar una apertura activa. Tras recibir esta solicitud, el sistema operativo asigna un número de puerto a este extremo. Esta utilidad se puede usar para realizar comunicaciones con usuarios remotos sin tener el retardo de la apertura activa.

Los procesos de aplicaciones que solicitan la apertura pasiva pueden aceptar una solicitud de cualquier usuario. (supuesto que se cumplen algunos requisitos de compatibilidad, que se comentaran en breve). Si se puede aceptar cualquier llamada (sin requisitos de compatibilidad) el número de socket exterior se pone a ceros. Los números de socket exterior no especificados solo se permiten en aperturas pasivas.

La segunda forma de establecimiento de conexión es el modo de apertura activa. En esta situación, el protocolo de nivel superior designa específicamente otro socket por el que establecer la conexión. Típicamente, se envía la apertura activa a un puerto con apertura pasiva para establecer un circuito virtual.

TCP admite un escenario en el que se envían dos aperturas activas de un sistema a otro a la vez. TCP realizara la conexión. Esta característica permite que las aplicaciones envíen una apertura en cualquier momento, sin preocuparse de si la otra aplicación ha enviado otra apertura o no.

TCP establece convenciones estrictas sobre como se deben utilizar conjuntamente las aperturas activas y pasivas. En primer lugar, una apertura activa identifica un socket específico, así como sus niveles de prioridad y de seguridad. TCP garantiza una apertura si el socket remoto tiene una apertura pasiva compatible, o si ha enviado una apertura activa compatible.

El Bloque de Control de Transmisión (TCB)

Como TCP debe recordar varias cosas de cada conexión virtual, almacena esa información en un Bloque de Control de Transmisión (TCB). Entre la información que se almacena en la TCB destacamos los números de socket local y remoto, los punteros a los buffers de transmisión y recepción, los punteros a la cola de retransmisión, los valores de seguridad y prioridad de la conexión y el segmento en curso. La TCB también contiene varias variables asociadas a los números de secuencia de envió y recepción.

EL SEGMENTO TCP

Las PDU que se intercambian entre dos módulos TCP se denominan segmentos. En la figura 10-6 se muestra el formato de un segmento. En esta sección examinaremos cada uno de los campos de un segmento.

El segmento se divide en dos partes, la parte de cabecera y la parte de datos. La parte de datos sigue a la parte de cabecera. Los primeros dos campos del segmento se denominan puerto de fuente y puerto de destino. Esos campos de 16 bits identifican a los programas de aplicación de nivel superior que utilizan la conexión TCP.

El siguiente campo se denomina número de secuencia. Este campo contiene el número de secuencia del primer octeto del campo de datos de usuario. Su valor especifica la posición de la cadena de bits del modulo transmisor. Dentro del segmento especifica el primer octeto de datos de usuario.

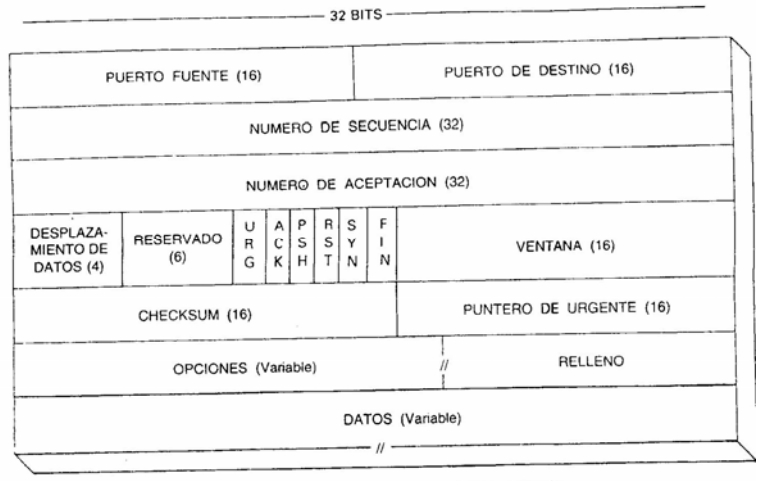

Figura 10-6 El segmento TCP (PDU)

El número de secuencia se utiliza también durante la operación de gestión de la conexión. Si dos entidades TCP utilizan el segmento de solicitud de conexión, entonces el número de secuencia especifica el numero de secuencia de envió inicial (ISS) que se utilizara para la numeración subsiguientes de los datos de usuario.

El valor del número de aceptación permite aceptar los datos previamente recibidos. Este campo contiene el valor del número de secuencia del siguiente octeto que espera recibir del transmisor. Con esa definición permite la aceptación inclusiva, en el sentido de que permite la aceptación de todos los octetos hasta, e incluyendo, el valor de este numero menos 1.

El campo de desplazamiento de datos especifica el número de palabras alineadas de 32 bits de que consta la cabecera de TCP. Este campo se utiliza para determinar donde comienza el campo de datos.

Como puede esperarse, el campo reservado esta reservado. Consta de 6 bits que deben valer cero. Estos bits reservados para usos futuros.

Los seis bits siguientes se denominan indicadores (flags). Son bits de control de TCP y se utilizan para especificar ciertos servicios o utilidades que se pueden emplear durante la sesión. El valor de algunos de esos bits indica como interpretar otros campos de la cabecera. Los seis bits mencionados llevan la siguiente información:

· URG indica que el campo de puntero de urgencia es significativo.
· ACK indica si el campo de aceptación es significativo.
· PSH significa que el modulo va a utilizar la función push.
· RST indica que la conexión se va a inicializar.

· SYN indica que se va a sincronizar los números de secuencia; se utiliza en los segmentos de establecimiento de conexión como indicación de que se va a realizar algunas operaciones de preparación.
· FIN indica que el remitente no tiene más datos para enviar. Es comparable a la señal de fin de transmisión (EOT) en otros protocolos.

El campo siguiente, denominado ventana, se pone a un valor que indica cuantos octetos desea aceptar el receptor. Este valor se establece teniendo en cuenta el valor del campo de aceptación (numero de aceptación). La ventana se establece sumando los valores del campo de ventana y del campo de número de aceptación.

El campo de checksum contiene el complemento a 1 de 16 bits del complemento a 1 de la suma de todas las palabras de 16 bits del segmento, incluyendo la cabecera y el texto. El propósito de este cálculo es determinar si el segmento procedente del transmisor ha llegado libre de errores.

El siguiente campo del segmento, denominado puntero de urgente, se utiliza solo si el indicador de URG esta a 1. E l objeto de este puntero es identificar el octeto de datos al que siguen datos urgentes. Los datos urgentes se denominan datos fuera de banda. TCP no dice lo que hay que hacer con los daros urgentes. Depende de la implementación. Dicho de otro modo, solo se indica el lugar donde empiezan los datos urgentes, no lo que hay que hacer con ellos. El valor de este campo es un desplazamiento del número de secuencia y apuntar al octeto a partir de cual siguen los datos urgentes.

El campo de opciones esta concebido para posibilitar futuras mejoras de TCP. Esta diseñado de forma semejante al campo de opción de los datagramas de IP, en el sentido de que cada opción se especifica mediante un byte que especifica el número de opción, un campo que contiene la longitud de la opción, y finalmente, los valores de la opción propiamente dichos.

Actualmente el campo de opción tiene un uso bastante limitado, y el estándar TCP solo especifica tres opciones:

0: fin de listas de opciones
1: no operación
2: tamaño máximo de segmento

Finalmente, el campo de relleno asegura que la cabecera TCP ocupa un múltiplo par de 32 bits. Finalmente, como muestra la figura, siguen los datos de usuario.

PROTOCOLOS DE DATAGRAMAS DE USUARIO (UDP)

Recordaremos que los protocolos no orientados a conexión no proporcionan fiabilidad ni mecanismos de control de flujo. No proporcionan procedimientos de recuperación de errores. UDP es un protocolo no orientado a conexión. Se utiliza a veces como sustituto de TCP cuando no hay que utilizar los servicios de este. Por ejemplo, varios del nivel de aplicación, como el Protocolo de Transferencia de Archivos Trivial (TFTP) y la Llamada de Procedimiento Remoto (RPC) utilizan UDP.

UDP sirve como interfaz de aplicación simple para IP. Como no incluye mecanismos de fiabilidad, control de flujo ni medidas de recuperación de errores, sirve únicamente como multiplexor/demultiplexor del envió y recepción del tráfico de IP.

UDP hace uso del concepto de puerto para dirigir los datagramas hacia las aplicaciones de nivel superior apropiadas. El datagrama de UDP contiene un número de puerto de destino y un número de puerto de fuente. El número de destino es utilizado por el modulo de UDP para enviar el trafico al receptor adecuado.

Formato del mensaje UDP

Quizá la mejor forma de explicar este protocolo sea examinar el mensaje y los campos que lo componen. Como muestra la figura 10-7, el formato es muy simple e incluye los siguientes campos:

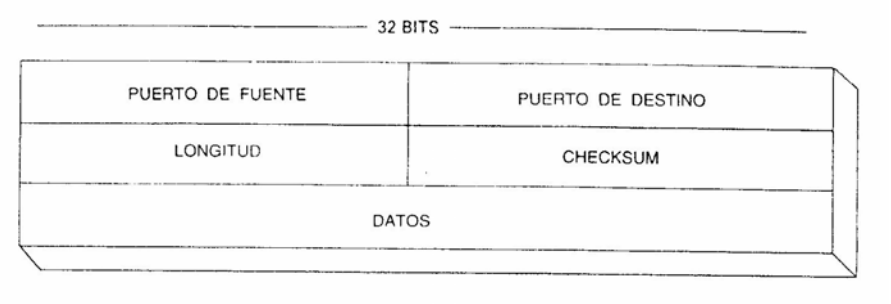

Figura 10-7. Formato de UDP

Puerto de fuente: Este valor identifica el puerto del proceso de aplicación remitente. Este campo es opcional. Si no se utiliza, se pone a 0.

Puerto de destino: Este valor identifica el proceso de recepción en el computador de destino.

Longitud: Este valor indica la longitud del datagrama de usuario, incluyendo la cabecera y los datos. La longitud mínima es de 8 octetos.

Checksum: Este valor contiene el valor del complemento a 1 en 16 bits del complemento a 1 de la suma de la seudocabecera de IP, la cabecera de UDP y los datos. Se realiza también el checkcum de los campos de relleno (si es necesario que el mensaje contenga un número de octetos que sean un múltiplo de dos).

Poco más después se puede decir de UDP. Representa el nivel de servicio mínimo que utiliza mochos sistemas de aplicación basados en transacciones. Es, sin embargo, muy útil en los casos en los que no son necesarios los servicios de TCP.

PROTOCOLOS DE BUSQUEDA DE RUTA

La comunicación entre redes, las pasarelas y los sistemas de encaminamiento tienen un papel muy importante en las redes basadas en TCP/IP. De hecho, el protocolo IP esta diseñado basándose en el concepto de intercomunicación entre redes de computadores con pasarelas y sistemas de encaminamiento. IP no es un protocolo de búsqueda de ruta. Hace uso de tablas de ruta que son rellenadas por los protocolos que se indican en esta sección.

Cada red esta conectada con un computador que actúa como conmutador entre redes. Las operaciones de conmutador están programadas para encaminar el tráfico hacia la red apropiada examinando la dirección de destino y buscándola en las direcciones almacenadas en una tabla de rutas. Las entradas de la tabla de rutas indican la ruta mejor hacia la siguiente red o parársela.

Incluso cuando hay redes administradas por autoridades locales, es práctica común que un grupo de redes sea administrado globalmente. Desde la perspectiva de intercedes, este grupo de redes se denomina sistema autónomo y es administrado por una autoridad. Ejemplos de sistemas autónomos pueden ser redes de campus universitarios, de complejos hospitalarios e instalaciones militares. Las diversas redes localizadas en esos lugares se conectan mediante

pasarelas. Como esas pasarelas operan dentro de un sistema autónomo, poseen a menudo sus propios mecanismos de encaminamiento de los datos.

Los sistemas autónomos se identifican con un número. La forma de realizar la identificación depende de los administradores, pero la idea es identificar los sistemas autónomos particulares con números diferentes. Este esquema de numeración es útil el gestor de la red desea encaminar el tráfico por un sistema autónomo administrado por un competidor, aunque este conectado con el suyo, que no tenga servicios de seguridad apropiados. Con el uso de protocolos de encaminamiento y de números de identificación de sistemas autónomos, las pasarelas pueden determinar como comunicarse e intercambiar información de encaminamiento.

Las pasarelas solo tienen responsabilidades sobre una parte de la interred. Es decir, una pasarela no tiene que saber nada de las otras pasarelas de la interred, pero puede basarse en pasarelas vecinas y/o de otros sistemas autónomos para obtener la información de encaminamiento. Si no disponen de la información suficiente como pata tomar una decisión sobre la ruta, simplemente escogen una ruta por defecto. En la figura 10-8 se muestra la relación entre los protocolos de las pasarelas internas y externas. Un conjunto de redes de conmutación de paquetes denominado sistema autónomo A se conecta con otro conjunto de redes de paquetes denominado sistema autónomo B. La pasarela 1 (G1) y la pasarela 2 (G2) utilizan un protocolo de pasarela externa (EGP) para el intercambio de información de control y de datos. Las dos intercedes utilizan sus propios protocolos de pasarela interna (IGP) para realizar la gestión del encaminamiento dentro de cada sistema autónomo. Por lo tanto, no es raro que una pasarela soporte dos (o más) protocolos de búsqueda de ruta, dependiendo del lugar de destino del tráfico. Esas pasarelas utilizan un IGP dentro de cada sistema autónomo y un EGP entre sistemas autónomos.

Los sistemas EGP e IGP deben encontrar la mejor ruta y construir una tabla de rutas. IP utiliza esta tabla para enviar el datagrama por la red, entre redes o entre sistemas autónomos.

Las tablas de ruta son cambiadas por una pasarela cuando otra pasarela descubre algo de lo siguiente:

· Se encuentra una nueva red.
· Se encuentra un camino mejor hacia una red determinada.
· Un camino “mejor” puede resultar degradado.

¿Qué es un camino “mejor”? Depende de la selección del administrador de la red. En la mayoría de los casos es simplemente el que presenta el menor número de saltos entre el transmisor y el receptor. Puede basarse también en una variedad de criterios que se denominan de forma general como encaminamiento de mínimo coste o métricas de coste mínimo. El nombre no significa que el encaminamiento este basado solo en la ruta de coste mínimo en el sentido lineal. Hay otros factores que se tienen en cuenta en el algoritmo de encaminamiento por las redes:

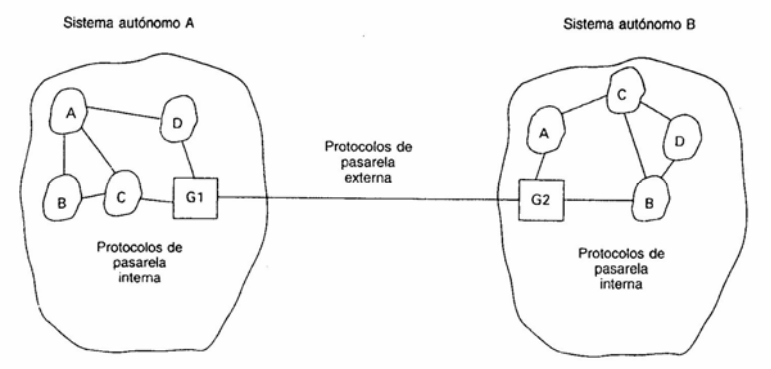

Figura 10-8. Protocolos de pasarela

· Capacidad de los enlaces.
· Requerimientos de retardo y de caudal efectivo.
· Número de datagramas que esperan transmisión por el enlace.
· Equilibrado de la carga por la red.
· Requerimientos de seguridad del enlace.
· Tipo de tráfico respecto al tipo de enlace.
· Número de enlaces intermedios, de redes y de pasarelas entre los computadores transmisor y receptor.
· Capacidad de alcanzar (conectarse con) los nodos intermedios y, por supuesto, con el computador receptor final.

Ejemplos de protocolos de búsqueda de ruta

El protocolo de pasarela externa (EGP) se utiliza para proporcionar información de accesibilidad de redes entre pasarelas vecinas. Aunque en el nombre del protocolo se incluye el término “externo”, esas pasarelas pueden pertenecer a distintos sistemas autónomos o a sistemas autónomos distintos. Sin embargo, el esquema más común es utilizar el EGP entre pasarelas que no pertenecen al mismo sistema autónomo.

EGP contiene procedimientos para: (a) adquirir vecinos, (b) intercambiar información entre vecinos y (c) controla la accesibilidad de las redes. EGP utilizan procedimientos de sondeo que las pasarelas se controlen entre si e intercambiar mensajes de actualización de encaminamiento.

EGP está restringido a anunciar la accesibilidad de aquellas redes completamente incluidas dentro del sistema autónomo de las pasarelas. Por lo tanto, una pasarela con EGP tiene autoridad restringida. Uno de sus valores es evitar un excesivo trasiego de información por la red. Los mensajes de EGP sirven de aviso a muchas pasarelas. Una pasarela con EGP puede enviar secuencias de bloques con información de accesibilidad relativas a una red específica.

EGP no realiza cálculos utilizando los valores del mensaje de actualización de ruta. El software esta diseñado solo para establecer la forma en que EGP puede indicar que hay un camino disponible. EGP se utiliza para anunciar la información de accesibilidad y no funciona con topologías elaboradas que incluyen pasarelas en bucle.

El protocolo de Información de Encaminamiento (RIP) se desarrolla basándose en investigaciones realizadas por el Centro de Investigación de Seros en Palo Alto (PARC) y en los protocolos PUP y XNS de Xerox. Como RIP fue diseñado para LAN, se basa en tecnologías de difusión; las pasarelas difunden periódicamente su tabla de rutas a sus vecinos. El aspecto de difusión de RIP ha suscitado quejas sobre su ineficiencia.

RIP esta clasificado como un protocolo de algoritmo de encaminamiento basado en vectores de distancia. Las decisiones de encaminamiento que toma RIP se basan en el número de “saltos” que se deben producir para alcanzar el destino final. RIP informa solo de direcciones de redes y distancias (medidas, generalmente, en numero de saltos). Utiliza el número de saltos para calcular el coste de la ruta, pero utiliza un valor máximo de 16 para indicar que la red no es alcanzable. La cuenta de saltos es una medida del “coste” de la ruta. Se pueden utilizar otras métricas, basadas en el retardo, la seguridad, el ancho de banda, etc., pero la mayoría de los sistemas utilizan simplemente la cuenta de los saltos. Además, RIP necesita información de todas las redes del sistema autónomo e intercambiar información solo con sus vecinos.

Las maquinas que participan en las operaciones de RIP pueden ser dispositivos activos o pasivos. Las maquinas activas (habitualmente, pasarelas), informan de las rutas a otras maquinas. Las maquinas pasivas (habitualmente, computadores) no informan de las rutas, pero reciben mensajes y actualizan sus tablas de rutas.

RIP utilizan el protocolo de datagrama de usuario (UDP). El numero de puerto 520 de UDP es utilizado por las maquinas RIP para enviar y recibir mensajes RIP.

El protocolo denominado Primar Camino más Corto Abierto (OSPF) esta diseñado para las necesidades de las pasarelas de alta velocidad. El propósito de un protocolo de pasarela es distribuir la información de ruta entre los sistemas de encaminamiento de una red o entre redes. El objetivo de esta operación es proporcionar a los usuarios de la red rutas fiables y eficientes a través de una red o por diversas redes. El resultado final, si se realiza adecuadamente, es un uso eficiente de la red, deforma que los usuarios experimenten pocos retardos y un caudal efectivo de datos altos con un coste razonable.

OSPF esta clasificado como un protocolo dinámico y adaptativo en el sentido de que se ajusta automáticamente (sin intervención humana) a los problemas de l red (o sistema autónomo) y consigue tiempos de convergencia pequeños en la estabilización de las rutas. Además, esta diseñado para evitar que el trafico realice bucles; esto es importante en redes en malla o en LAN, en donde puede haber múltiples sistemas de encaminamiento que interconectan LAN distintas.

Los bucles ocurren cuando un computador o red recibe el tráfico que emite. Este problema crea en la red problemas de caudal efectivo, retardos y congestión. En la figura 10-9, el tráfico que se envía desde la red 3 al sistema de encaminamiento 3 vuelve a la red 3 pasando por los sistemas de encaminamiento 3, 6, 5 y 4.

OSPF evita la aparición de bucles bloqueando las vías de comunicación que pueden causar ese problema. Por ejemplo, el trafico que procedente de la red 3 envía al sistema de encaminamiento 4 podría no enviarse al sistema d encaminamiento5. Asimismo, el tráfico que, procedente de la red 3 se envía al sistema de encaminamiento 3, no tendría porque pasar del sistema de encaminamiento 5 al sistema de encaminamiento4. A pesar de esas limitaciones, todas las redes y sistemas de encaminamiento mantienen una conectividad completa. En otras palabras, todas las redes y sistemas de encaminamiento pueden enviar y recibir tráfico. El árbol de operaron de OSPF resulta así “podado”, con las ramas (enlace de comunicaciones) que pueden causar lazos cortadas.

Como ya hemos dicho, un conjunto de redes, sistemas de encaminamiento y computadores se pueden organizar en forma de sistema autónomo. Un sistema autónomo es aquel en el que un grupo de sistemas de encaminamiento utilizan un protocolo común ce ruta, como OSPF, para intercambiar la

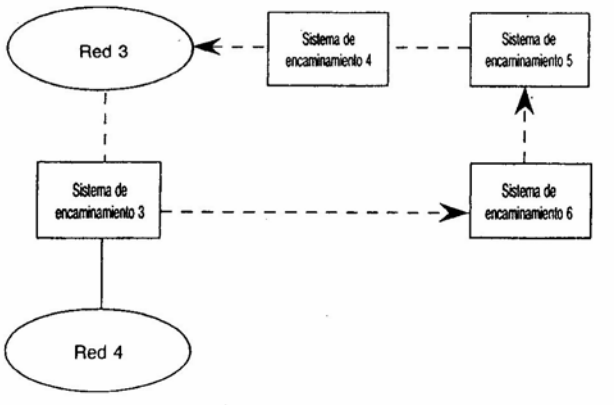

Figura 10-9. Bucles

información de encaminamiento. OSPF se clasifica como un protocolo de pasarela interna (IGP) debido a que solo admite encaminamiento dentro de un mismo sistema autónomo. El intercambio de información de encaminamiento entre sistemas autónomos es responsabilidad de otro protocolo: el protocolo de pasarela externa, o EGP.

Cada sistema de encaminamiento contiene un directorio de rutas (que en OSPF se denomina base de daros de rutas). Esta base de datos contiene información sobre los interfaces de enlaces del sistema de encaminamiento que están operativos, además de información de estatus de los vecinos del sistema de encaminamiento. La base de datos es la misma para todos los sistemas de encaminamiento de una misma área.

La información de la base de datos de encaminamiento presente la topología de la red como si fuera un grafo dirigido. Los sistemas de encaminamiento y las redes forman los vértices del grafo. Esta información se difunde de forma periódica a todos los sistemas de encaminamiento pertenecientes al sistema autónomo. Cada sistema de encaminamiento OSPF calcula el camino mas corto gasta los otros sistemas de encaminamiento pertenecientes al sistema autónomo, considerándose a si mismo el nodo de trabajo (que en este protocolo se denomina raíz). Seguidamente realiza la “poda” de todas las vías, excepto el “camino mas corto” a cada sistema de encaminamiento.

Un aspecto muy flexible y potente de este protocolo es que diferentes tipos de servicio (TOS) pueden trabajar con métricas diferentes, como las basadas en el retardo, el caudal efectivo, o la prioridad del datagrama. Si los cálculos indicaran que dos caminos son del mismo valor, OSPF distribuirá el tráfico por los dos caminos a partes iguales.

OSPF puede trabajar con una red o con muchas redes. Las redes pertenecientes a un sistema se pueden agrupar formando áreas. El diseño del protocolo permite aislar las áreas entre si. Es mas, un área puede quedar aislada del sistema autónomo completo. Además, debido a la creciente preocupación por la seguridad, OSPF incluye procedimientos de autorización. Los sistemas de encaminamiento pueden utilizar procedimientos sencillos para autorizar al tráfico que intercambian.

El método para determinar la información de encaminamiento fuera del sistema autónomo se denomina encaminamiento externo. La información de ruta necesaria en este caso se obtiene típicamente de OSPF, así como de otros protocolos como EGP. Alternativamente, podría establecerse también utilizando rutas estáticas entre los sistemas autónomos. El encaminamiento podría llevarse entonces a cabo utilizando rutas por defecto. Esta información también es difundida por el sistema autónomo.

Cada área utiliza su propio algoritmo de encaminamiento. Tiene también su propia base de datos de topología distinta que las otras áreas. El objetivo de las áreas es dividir y aislar partes del sistema autónomo y reducir la cantidad de información que los sistemas de encaminamiento deben mantener sobre el sistema completo. Además, la sobrecarga de información que se transmite entre los sistemas de encaminamiento para mantener las tablas de ruta de OSPF se ve considerablemente reducida.

OSPF utiliza el término columna vertebral para referirse a la parte del sistema autónomo que transporta los paquetes entre áreas. El camino completo de un paquete es como sigue : (1) un camino dentro del área hasta llegar al sistema de encaminamiento conectado con la columna vertebral; (2) un camino por la columna vertebral hasta llegar al sistema de encaminamiento del área de destino, y (3) otro camino dentro de un área hasta la red destino.

OSPF utiliza protocolo “Hola” para comunicar la información de estado entre vecinos. Los paquetes “Hola” se utilizan para confirmar acuerdos entre sistemas de encaminamiento de una red común acerca de operaciones y ciertos temporizadores. Es decir, se emplea para asegurase de que las relaciones entre vecinos tiene sentido.

El objetivo de OSPF es permitir que los sistemas de encaminamiento se informen entre si de las rutas interred mediante aviso. Estos avisos se envían a cada sistema de encaminamiento mediante paquetes de actualización. Se emplean cuatro tipos de avisos:

· Avisos de enlace de sistema de encaminamiento. Contiene información sobre los interfaces de un sistema de encaminamiento concreto de esa área. Es utilizado por todos los sistemas de encaminamiento y difundido por un área.

· Aviso de enlace de redes. Contiene la lista de sistemas de encaminamiento conectados a una red. Es utilizado por las redes de difusión y se difunde por un área.

· Resumen de avisos de enlaces. Contiene información de las rutas fuera de un área. Es utilizada por los sistemas de encaminamiento de las fronteras y se difunde a las áreas de los sistemas de encaminamiento de las fronteras (pero dentro del sistema autónomo).

· Aviso de enlaces extendidos de sistemas autónomos (AS). Contiene información de las rutas de otros sistemas autónomos. Es utilizado por un sistema de encaminamiento de la frontera y se difunde por todo el sistema autónomo.

Los protocolos del nivel de aplicación

Los protocolos del nivel de aplicación de la colección de TCP/IP se encuentran entre los más utilizados por parte de la industria. Algunos de esos protocolos son muy ricos en funciones y una explicación detallada de sus posibilidades seria excesivamente extensa. Como este libro es un libro de comunicaciones, no se derriben. Los principales protocolos de nivel de aplicación son:

· TELNET para servicios de terminales.
· Protocolo Trivial de Transferencia de Archivos (TFTP) para servicios simples de transferencia de archivos.
· Protocolo de Transferencia de Archivos (TFP) para servicios de transferencia de archivos más elaborados.
· Protocolo Simple de Transferencia de Correo (SMTP) para servicios de transferencia de mensajes (correo electrónico).

RESUMEN

Los protocolos Internet se han convertido en una de las familias de protocolos mas ampliamente utilizada en el mundo. Están diseñados para facilitar la intercomunicación de redes de computadores. Aunque se conocen con el nombre genérico de TCP/IP, los protocolos Internet consta de muchos protocolos diseñados para dar soporte a las operaciones de comunicaron entre redes. Varios protocolos de esta familia reciben el nombre de protocolos de pasarela (más exactamente, de protocolos de búsqueda de ruta) y son protocolos ampliamente utilizados, como los protocolos de pasarela externa (EGP), el protocolo de información de encaminamiento (RIP) y el camino abierto mas corto primero (OSPF). Además, los protocolos interred contienen una gran cantidad de protocolos de nivel de aplicación, como TELNET, el protocolo de transferencia de archivos (FTP) y el protocolo simple de transferencia de correo (SMTP).

Bibliografía:

Black Uyless
Redes de Computadores. Protocolos, Normas e Interfaces. 2ª Edición.
Alfaomega. 1977. México.
ISBN 970-15-0329-5