FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

A LOS ASISTENTES A LOS CURSOS

Las autoridades de la Facultad de Ingeniería, por conducto del jefe de la División de Educación Continua, otorgan una constancia de asistencia a quienes cumplan con los requisitos establecidos para cada curso.

El control de asistencia se llevará a cabo a través de la persona que le entregó las notas. Las inasistencias serán computadas por las autoridades de la División, con el fin de entregarle constancia solamente a los alumnos que tengan un mínimo de 80% de asistencias.

Pedimos a los asistentes recoger su constancia el día de la clausura. Estas se retendrán por el periodo de un año, pasado este tiempo la DECFI no se hará responsable de este documento.

Se recomienda a los asistentes participar activamente con sus ideas y experiencias, pues los cursos que ofrece la División están planeados para que los profesores expongan una tesis, pero sobre todo, para que coordinen las opiniones de todos los interesados, constituyendo verdaderos seminarios.

Es muy importante que todos los asistentes llenen y entreguen su hoja de inscripción al inicio del curso, información que servirá para integrar un directorio de asistentes, que se entregará oportunamente.

Con el objeto de mejorar los servicios que la División de Educación Continua ofrece, al final del curso deberán entregar la evaluación a través de un cuestionario diseñado para emitir juicios anónimos.

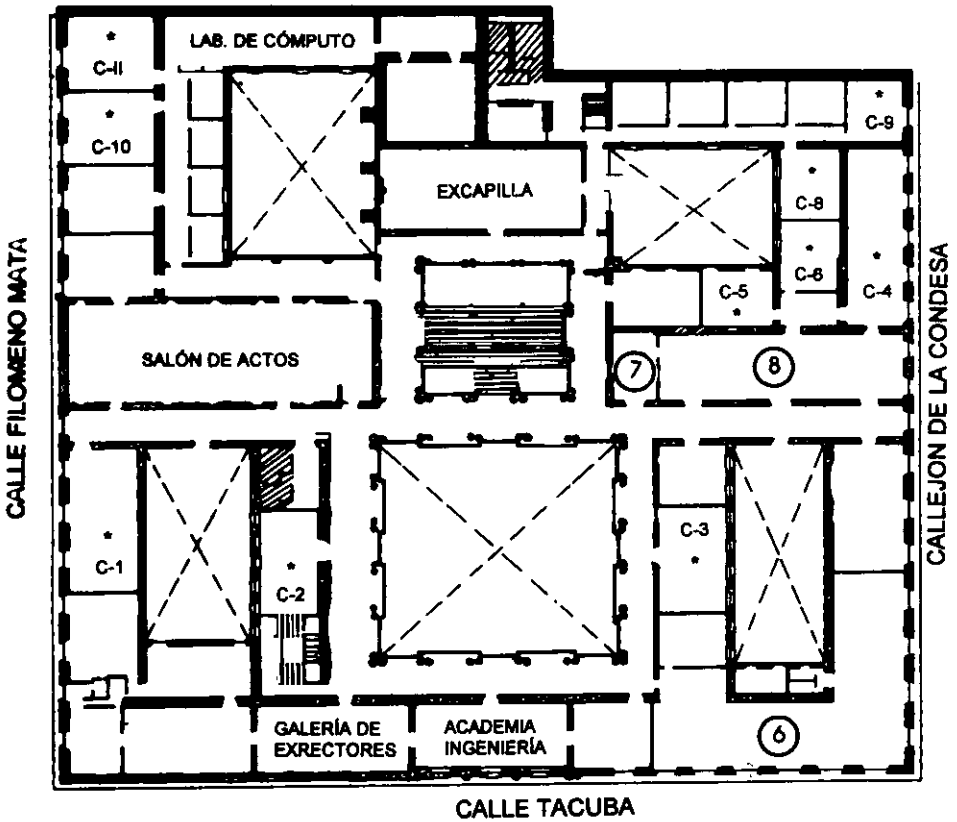
Se recomienda llenar dicha evaluación conforme los profesores impartan sus clases, a efecto de no llenar en la última sesión las evaluaciones y con esto sean más fehacientes sus apreciaciones.

Atentamente

División de Educación Continua.

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

PALACIO DE MINERIA



1er. PISO

GUÍA DE LOCALIZACIÓN

1. ACCESO
2. BIBLIOTECA HISTÓRICA
3. LIBRERÍA UNAM
4. CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN "ING. BRUNO MASCANZONI"
5. PROGRAMA DE APOYO A LA TITULACIÓN
6. OFICINAS GENERALES
7. ENTREGA DE MATERIAL Y CONTROL DE ASISTENCIA
8. SALA DE DESCANSO

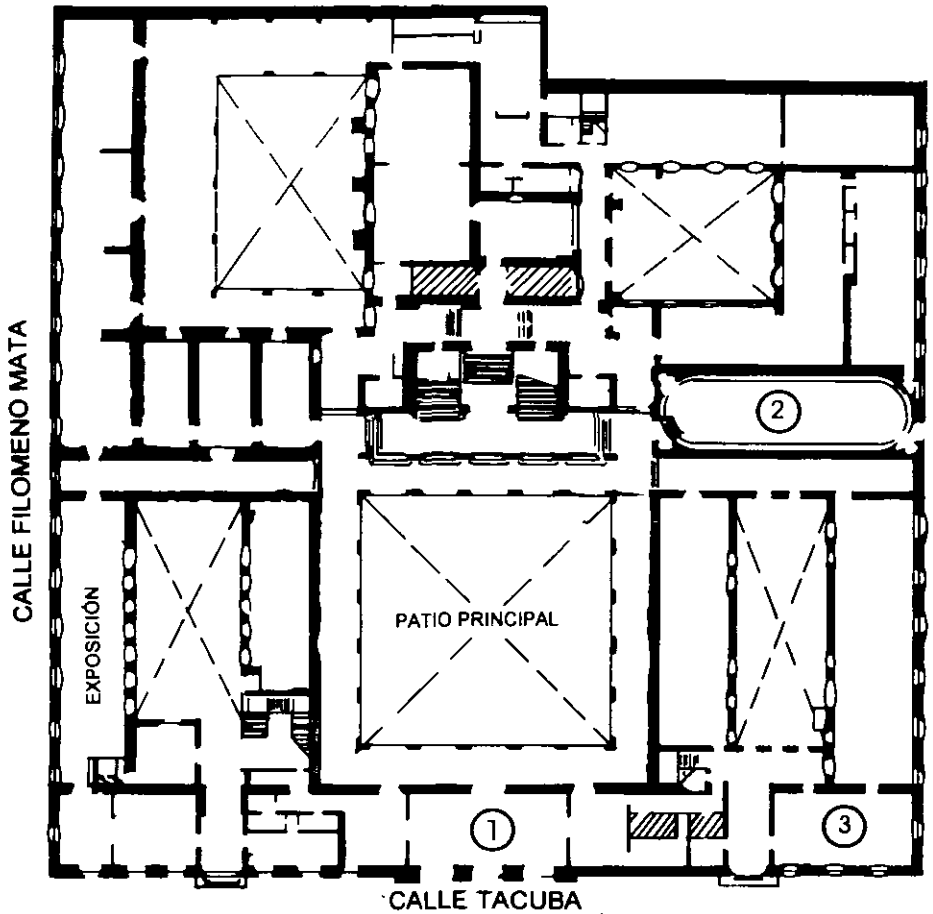
SANITARIOS

* AULAS

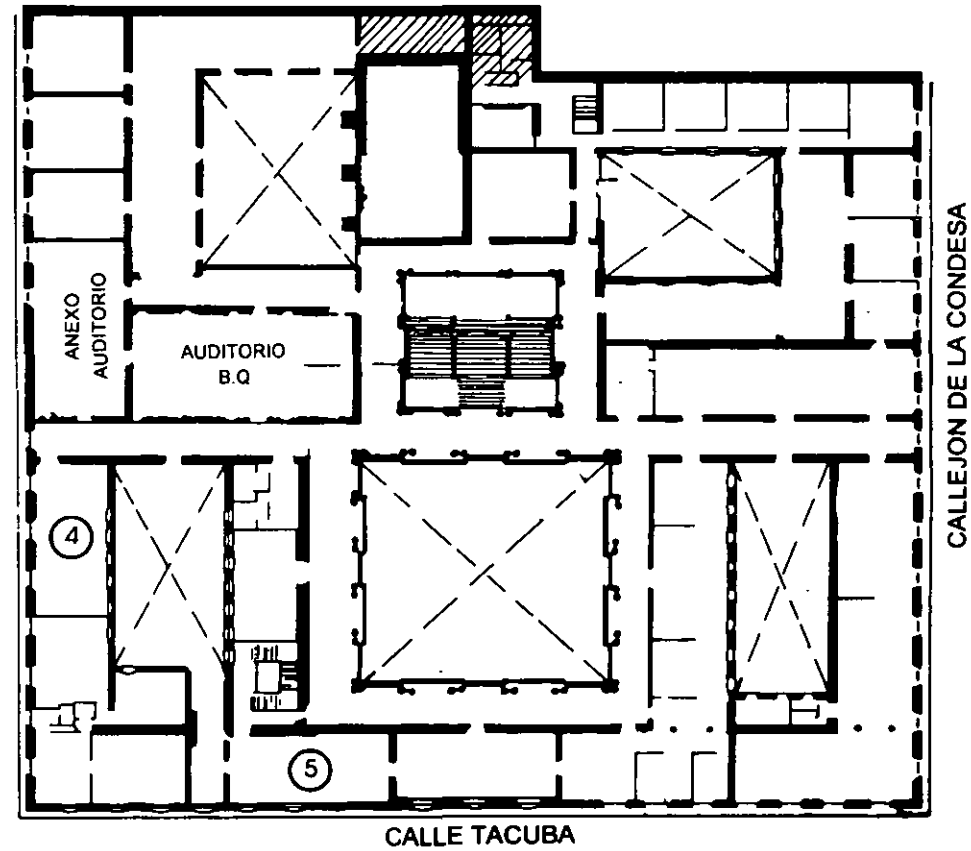
DIVISIÓN DE EDUCACIÓN CONTINUA
FACULTAD DE INGENIERÍA U.N.A.M.
CURSOS ABIERTOS

DIVISIÓN DE EDUCACIÓN CONTINUA
DEC

PALACIO DE MINERIA



PLANTA BAJA



MEZZANINNE

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

DIPLOMADO EN REDES WAN

MODULO V

CONFIGURACION DE RUTEADORES Y ENRUTAMIENTO
(CA135)

NOTAS DEL CURSO

OCTUBRE 1998

EXPOSITOR:
ARTURO LEV SERVIN NIEMBRO

Palacio de Mineria Calle de Tacuba 5 Primer piso Deleg Cuauhtemoc 06000 México, D F APDO. Postal M-2285
Telefonos 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

Enrutamiento

Profesor: Ing. Arturo Lev Servín Niembro

Introducción

En 1980, el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) emprendió la tarea de definir estándares de LAN. El interés principal fue asegurar el bajo costo y la interoperabilidad en la interfaz de red para redes de área local.

Proyecto 802

Después de iniciar el proyecto, el IEEE determinó que un estándar de LAN no podría satisfacer a todas las partes y decidió crear varios estándares. Finalmente, en 1985 el Proyecto 802 del Comité de la Sociedad de Computación del IEBE publicó cuatro estándares por separado, los cuales se mencionan a continuación:

- IEEE 802.2 Provee control de enlace lógico
- IEEE 802.3 Define una red CSMA/CD
- IEEE 802.4 Define una red lineal utilizando acceso *tóken pass ¡ng*
- IEEE 802.5 Define una red en anillo usando acceso *token passing*

Estos estándares fueron adoptados por el ANSI (American National Standard Institute) en 1985 y han sido revisados y reexpedidos por la Organización Internacional de Estándares (ISO: International Standards Organizatión), formando parte de su proyecto de protocolos ISO 8802.

Ethernet

Es un recurso para conectar una computadora a una red por medio de un cable y así permitir que la información sea transmitida entre computadoras que estén en la misma red. Ethernet permite la transmisión de datos a una velocidad de 10 Mbps (megabits por segundo).

Ethernet se desarrolló por la compañía Xerox. La tecnología del primer modelo fue refinada y una segunda generación llamada Ethernet salió al mercado. A partir de ese momento Ethernet se conoció como DIX, debido a sus patrocinadores: Digital, Intel y Xerox. Después de registrar la marca, Xerox estableció y publicó los estándares.

Acceso y colisiones

Ethernet utiliza un protocolo llamado CSMAICD, del inglés Carrier Sense, Multiple Access, Collision Detect. La parte *Multiple Access* significa que cada estación está conectada a un solo cable de cobre (o a un conjunto de cables que están conectados para formar una ruta de datos única). La parte *Carrier Sense* indica que antes de transmitir datos la estación o host verifica el cable para percatarse si alguna otra estación está transmitiendo algo Si la LAN está desocupada, entonces la estación puede empezar a enviar datos. *Collision Detect* significa que dos estaciones pueden comenzar a enviar datos al mismo tiempo por lo que sus señales serán inentendibles. Cuando esto ocurre, las dos

estaciones paran la transmisión y, después de un periodo de espera aleatorio, tratan de transmitir nuevamente.

Token Ring

Token Ring significa red LAN tipo Token Passing (paso de fichas) con topología en anillo. Es un método de acceso en el cual los dispositivos de la red acceden al medio físico en un orden definido por la posesión de una pequeña trama (frame) llamada token (ficha).

El principio de control de Token Ring para LAN se desarrolló alrededor de 1972 por Von Willemjin (IBM). Tomó más de una década a IBM preparar esta red para su producción. IBM introdujo la red Token Ring IBM al final de 1985. El objetivo del desarrollo de esta red fue producir la red de transmisión de datos más económica y veloz. La red IBM Token Ring corresponde a la ECMA (Asociación Europea de Fabricantes de Computadoras), al IEEE y a la Normas Internacionales para LAN Token Ring (IBEE 802.2 y 802.5). Es una red abierta que permite acceder desde dispositivos IBM y No-BM.

El acceso al anillo compartido es controlado por el procedimiento normalizado de Token Ring. Los datos se transmiten en una sola dirección dentro del anillo. Hay un único símbolo en el anillo en cualquier tiempo determinado. Cada una de las terminales conectadas al anillo regeneran la señal entrante y retransmiten los datos a la próxima estación.

Existen estándares de Token Ring para trabajar a velocidades de transmisión de datos de 4 y 16 Mbps. La distancia máxima entre una estación de la red Token Ring y otra varía según la línea de transmisión. Para una línea de transmisión a 4 hilos, la distancia varía entre 300 y 750 metros. En cambio, si la línea es de fibra óptica, teóricamente la distancia no es una restricción.

FDDI

FDDI (Fiber Distributed Data Interface) es un estándar de red basado en fibra óptica del ANSI, escrito en 1990.

Una red con FDDI consiste en un número de estaciones serialmente unidas por un cable de transmisión *(fibra* óptica) para formar un lazo cerrado. Una estación activa transmite información secuencialmente como una "corriente" de símbolos hacia la otra estación activa del círculo. Como cada estación activa recibe dichos símbolos de datos, ésta los regenera y repite para la siguiente estación del círculo.

La red con FDDI opera a 100 Mbps. Puede operar a distancias de 200 kilómetros o más. Tiene una conecfividad con otras LAN corno Ethernet y Token Ring o a través de dispositivos de puenteo (bridging).

Enrutamiento

Se conece por enrutamiento al movimiento de información a través de redes interconectadas (internets). El enrutamiento implica dos actividades básicas: la determinación de la mejor ruta y el transpone de los paquetes de información a través de la internet (conmutación).

El enrutador opera en la capa 3 del modelo OSI o en la capa de internet del modelo TCP/IP, a diferencia del puenteo (bridging) que opera en la capa 2 de OSI o de red de TCP/IP.

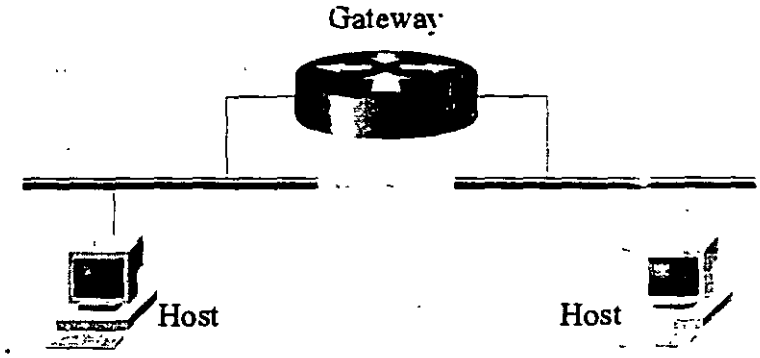
Enrutamiento directo e indirecto

De manera informal se pueden distinguir dos formas de enrutamiento: directo e indirecto El primero se refiere a la transmisión directa de un datagrama de una máquina a otra, siempre y cuando ambas pertenezcan al mismo segmento lógico (y, por lo tanto, al mismo segmento físico). Para realizar esta transferencia, la máquina origen encapsula el datagrama en una trama física, mapea la dirección IP a la dirección física (probablemente a través de ARP) y la entrega a la capa de red para su envío. La máquina origen sabe que la transmisión de datos puede ser directa gracias a la estructura de cualquier dirección IP. el anfitrión (host) origen extrae el identificador de red (netid) de la dirección del anfitrión destino y lo compara con su identificador; si son iguales, el datagrama puede ser enviado directamente Lo mismo se aplica para la transferencia entre anfitriones de redes segmentadas (fragmentadas en sub redes), con la única diferencia de que para la comparación, el anfitrión origen toma además el identificador de segmento (subnetid).

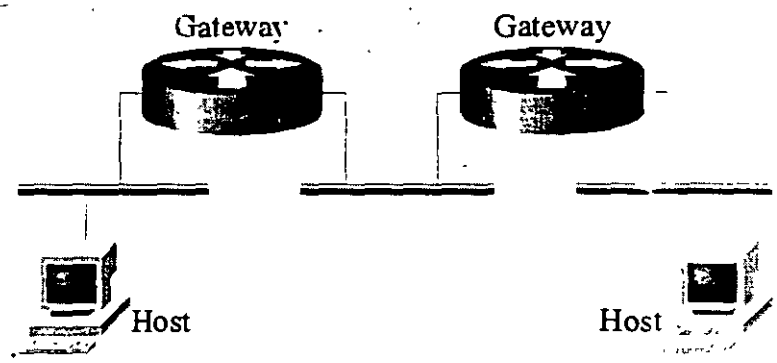
El enrutamiento indirecto se presenta cuando las máquinas que se comunican no están en la misma red (física y lógica), lo cual se traduce en la necesidad de utilizar un gateway (compuerta) que se encargue de comunicar as redes destino y origen. A ésta se le deberán enviar los datagramas para que continúen con su trayecto.

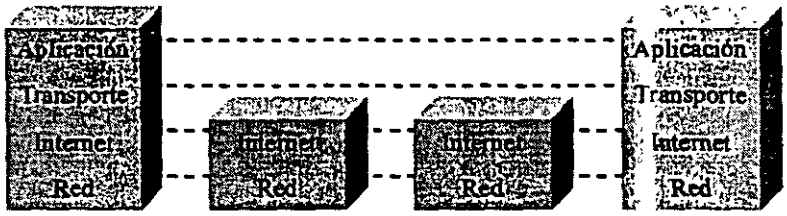
Ejemplo

Imagine una internet que contiene muchas redes, todas ellas conectadas entre sí por medio de compuertas pero con sólc dos anfitriones en sus extremos. Cuando uno de éstos quiere comunicarse con el otro, encapsula los datagramas y los envía al gateway más cercano (ambos están en los mismos segmentos físicos y lógicos. por lo que es posible un enrutamiento directo).



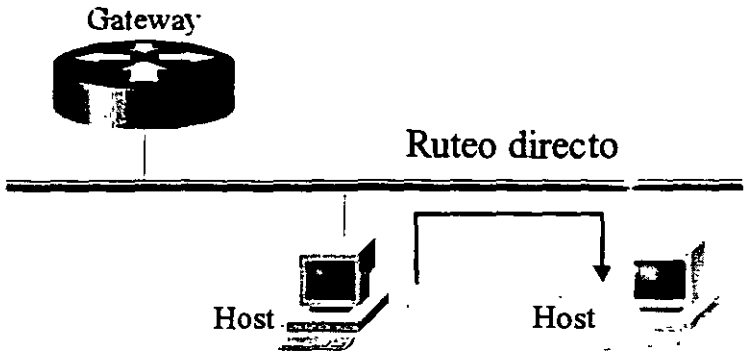
El software de la compuerta extrae la dirección IP destino del datagrama y la entrega a las rutinas de enrutamiento de IP para que seleccionen la siguiente compuerta que continuará la transferencia. Este proceso se repite hasta que el datagrama llega a la última compuerta (la cual está directamente conectada con la red destino), quien entregará al anfitrión destino enrutándolo directamente.

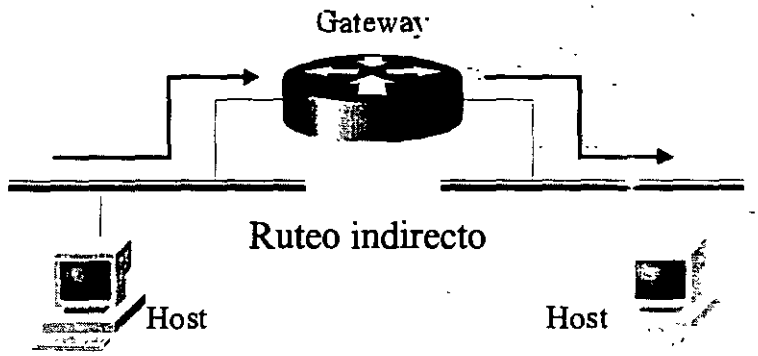




Tipos de enrutamiento

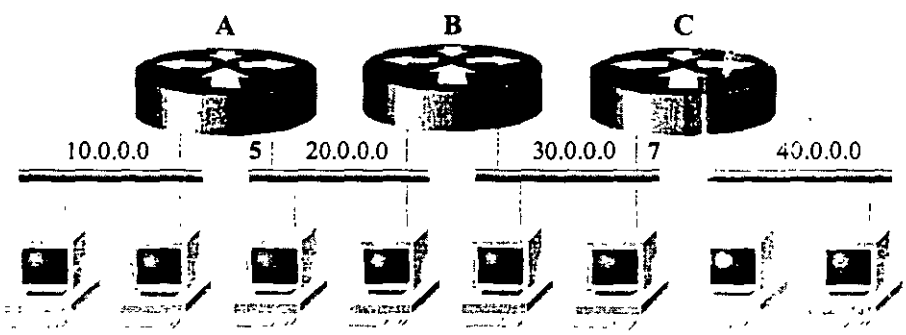
Los algoritmos de enrutamiento emplean comúnmente una tabla de enrutamiento en la que almacenan *información* referente a los posibles destinos y cómo llegar a ellos. Tanto anfitrionescomo compuertas tienen esta tabla, a la que consultan para enviar a la red todo datagrama que generen, pero la idea es que sólo las compuertas tomen las decisiones de enrutamiento; los anfitriones deberán confiar en ellas para acceder a destinos fuera de sus redes locales. Con el fin de agilizar la consulta a las tablas y de mantenerlas lo más pequeñas posibles, las entradas que conforman las tablas hacen referencia exclusivamente a redes o segmentos de redes; sólo en casos muy particulares una tabla de enrutamiento contendrá entradas para anfitriones específicos (host-specific-routes).

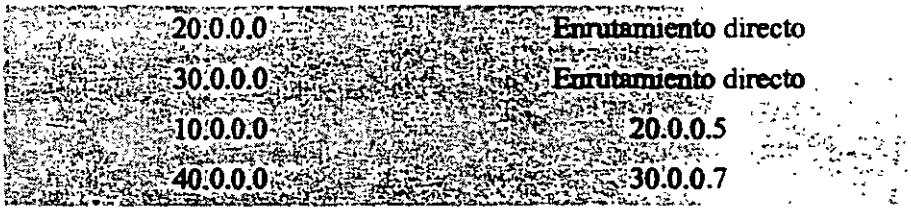




Las entradas de las tablas de enrutamiento contienen parejas de datos (N,G), donde N es la dirección IP de la red destino y G es la dirección IP de la compuerta "siguiente" en el camino a dicho destino; debido a esto las tablas de enrutamiento son llamadas en ocasiones tablas destino siguiente salto. Por tanto, la compuerta sólo conoce parte de la ruta final para llegar a cualquier destino a este proceso se le conoce como enrutamiento con información parcial. La tabla de enrutamiento siempre se dirige a compuertas que se hallan en la misma red, por lo que la comunicación entre compuertas siempre será a través de un enrutamiento directo.

Ejemplo





Cuando un destino en particular no aparece en la tabla de enrutamiento de la compuerta, éste envía los datagramas a una gateway de default (compuerta predeterminada). Este enrutamiento predeterminado es muy usado en aquellas redes que sólo tienen una conexión a la internet. Por ejemplo, las compuertas predeterminadas son usadas por todos los anfitriones de una red local para transferir información fuera de ella.

Se puede resumir el proceso de enrutamiento como sigue: el anfitrión origen determina si el destino se halla en la misma red (al comparar los netid y subnetid contra los del destino); de ser así, el anfitrión origen envía directamente los datagramas por la red física (previo mapeo de direcciones IP a físicas y encapsulamiento de las tramas respectivas); si los netid y subnetid son distintos, el anfitrión origen consulta la tabla de enrutamiento que apunta al gateway de default, la cual está encargada de toda transferencia a anfitriones fuera de la misma red.

Hasta aquí se ha explicado el proceso de enrutamiento con base en la consulta de las tablas, pero ¿de dónde se obtiene la información contenida en ellas? Las tablas de enrutamiento se generan a partir de dos procesos: la inicialización del proceso de enrutamiento y el intercambio de tablas con otras compuertas.

Toda compuerta comienza su operación con una tabla mínima, en ocasiones manualmente configurada por el operador o generada a partir de algoritmos de auto descubrimiento. Esta etapa de inicialización depende enteramente del sistema operativo de la compuerta. Una vez que las tablas están listas para ser consultadas, es necesario que se actualicen con cierta frecuencia, de tal manera que reflejen los cambios que se dan en la topología de la red. En redes pequeñas estos cambios pueden ser incorporados por el administrador local, pero en una internet grande es imprescindible automatizar la actualización, pues la intervención humana sería demasiado lenta. Estos mecanismos automáticos de actualización, conocidos como algoritmos de enrutamiento, permiten además el intercambio de información entre compuertas vecinas.

A continuación se presenta un extracto del RFC 1058:

Routing is *the task offinding a path from a sender to a desired destination. In the IP "catenel model" this reduces primarily for a matter of finding gateways between networks. As long as a message remains on a single network or subnet, any routing problems are solved by technology that is specific to the network. For example, the Ethernet and the ARPANET each define a way in which any sender can talk to any specifled destination within that one network. IP routing comes in primarly when messages must go from a sender on one such network to a destination on a different one. In that case, the message must pass through gateways connecting the networks. If the networks are not adjacent, the*

message may pass through several intervening networks, and the gateways connecting them. Once the message gets to a gateway thtat is on the same network as the destination, that network's own technology is used to get to the destination.

Throughout this section, the term "network" is used generically to cover a single broadcast network (e.g. an Ethernet), a point to point line, or the ARPANET The critical point is that a network is treated as a single entity by IP. Either no routing is necessary (as with a poini to point line). or that routing is done in a manner that is transparent to IP; allowing IP to treat the entire network as a single fully-connected system (as with an Ethernet or the ARPANET). Note that the term "network" is used in a somewhat different way in discussions of IP addressing. A single IP network number may be assigned to a collection of networks, with "subnet" addressing being used to describe the individual networks. in effect, we are using the term "network" here to refer to subnets in cases where subnet addressing is in use.

Algoritmos de enrutamiento

Los enrutadores se comunican entre sí con el objeto de intercambiar tablas de enrutamiento, información de control y diversos mensajes. La actualización de las tablas de enrutamiento, se lleva a cabo a través de mensajes de actualización (updates) que contienen toda la tabla de enrutamiento o sólo una porción de la misma. Al analizar las tablas de sus vecinos, un enrutador puede construir una réplica exacta de la topología de la red. Los avisos de estado de los enlaces (link-state advertisement) informan a los vecinos del enrutador origen el estado de los enlaces que éste mantiene con sus redes y otros enrutadores. Esta información también puede servir para construir una imagen fiel de la topología de la red.

Los algoritmos de enrutamiento se diseñan generalmente para satisfacer uno o varios de los requisitos que se mencionan a continuación:

- Optimización
- Simplicidad / bajo overhead
- Robustez / estabilidad
- Convergencia rápida
- Flexibilidad

Optimización

Se refiere a la capacidad que tiene el enrutador de seleccionar Ja mejor ruta. Ésta depende de los parámetros que elige para determinaría. Por ejemplo, un algoritmo puede utilizar el número de saltos y el retardo, pero este último puede influir más en el resultado final (es decir, tiene más importancia que el otro parámetro).

Simplicidad / bajo overhead

Los algoritmos son diseñados para ser lo más simples posibles, es decir, para que requieran el mínimo procesamiento del enrutador, no lo ocupen demasiado y no se convierta en una carga pesada para la carga general de la red. Esta característica permite al algoritmo operar con redes de ancho de banda pequeño y en máquinas con escasos recursos.

Robustez / estabilidad

Los algoritmos de enrutamiento deben operar correctamente bajo casi cualquier circunstancia, tal como fallas del hardware, alta carga en la red, implementación incorrecta, etcétera. Este es un punto crucial en su diseño, pues los enrutadores representan no dos que interconectan redes diferentes y cualquier falla que presenten afectará seriamente la comunicación entre las redes.

Convergencia rápida

Se llama convergencia al proceso mediante el cual los enrutadores determinan las mejores rutas. Cuando en la internet se dan situaciones que cambian su topología (alguna red se cayó, otra acaba de ser dada de alta, etcétera), los enrutadores intercambian entre sí actualizaciones de enrutamiento que utilizan para calcular nuevas rutas y eventualmente llegar a un acuerdo sobre la jerarquía de selección de las rutas para todos los destinos posibles.

Flexibilidad

Los protocolos de enrutamiento deben ser capaces de adaptarse a una amplia variedad de circunstancias. Por ejemplo, suponga que una red se cayó, los enrutadores que se han enterado cambiarán las rutas que cruzaban por esa red por la siguiente mejor opción contenida en las tablas de enrutamiento. La mayoría de los enrutadores pueden ser programados para adaptarse a cambios en anchos de banda, retardos en la red y otros parámetros.

Clasificación de los algoritmos de enrutamiento

Los algoritmos de enrutamiento pueden ser clasificados por su tipo en:

- Estático o dinámico
- Single-path o multi-path
- Plano o jerárquico
- De anfitrión inteligente o enrutador inteligente
- Intradominio o interdominio
- Estado de enlace (Link state) o vector-distancia (distance-vector)

Estático o dinámico

Estrictamente hablando, el enrutamiento estático no es un algoritmo automatizado sino un mapeo establecido manualmente por el administrador, al principio del proceso de enrutamiento. Este tipo de enrutamiento únicamente cambia si el administrador lo desea, por lo que sólo es recomendable en una

internet pequeña, estable y de tráfico relativamente predecible. Los algoritmos dinámicos, en cambio, se ajustan en tiempo real a las circunstancias cambiantes de la internet gracias al análisis que desarrollan sobre todo mensaje de enrutamiento. Si el mensaje indica que se ha producido un cambio en la red, el software del enrutador calcula nuevamente sus rutas, actualiza sus tablas y envía a sus vecinos actualizaciones de enrutamiento, estimulándolos a calcular de nuevo sus rutas. Sin embargo, bajo ciertos ambientes es posible que los algoritmos dinámicos se complementen con rutas estáticas.

Single-path o multi-path

Se refiere a la capacidad que tiene el enrutador de balancear tráfico multicanalizador sobre enlaces paralelos, característica que se traduce en mayor confiabilidad y eficiencia; o en su caso, conmutar el tráfico a un solo canal en caso de que fallen los otros.

Plano o jerárquico

En un sistema plano de enrutamiento todos los enrutadores son pareja de los demás (pairs). En un Sistema jerárquico algunos enrutadores forman parte de la columna vertebral o backbone de enrutamiento de la red interna. Los paquetes de enrutadores que no pertenecen a la columna vertebral son enviados a ésta y circulan en ella basta que llegan al enrutador de acceso/salida en el área general de destino. Éste entrega el paquete al primer enrutador fuera de la columna vertebral que lo llevará hasta su destino. Las columnas vertebrales de enrutamiento son conocidas como dominios, sistemas autónomos o áreas. En los sistemas jerárquicos sólo algunos enrutadores pueden establecer comunicación con enrutadores de dominios distintos al propio, aunque por lo general la comunicación entre enrutadores de un mismo dominio puede ser limitada. En internets grandes pueden existir múltiples niveles de jerarquía. La principal ventaja de los protocolos jerárquicos es que por su funcionamiento se adaptan fácilmente a la organización de muchas compañías. La mayor parte de la comunicación ocurre dentro de pequeños grupos (dominios), por lo que los enrutadores de intradominio sólo necesitan intercambiar información con sus vecinos de dominio, lo que simplifica enormemente el diseño de los algoritmos y el tráfico en la red.

De anfitrión inteligente o enrutador inteligente

Algunos algoritmos de enrutamiento asumen que el anfitrión origen determinará la ruta a seguir hasta alcanzar al destino. A esto se le conoce como enrutamiento origen/fuente. En los sistemas de enrutamiento origen (o anfitrión inteligente) los enrutadores actúan como equipos de "almacenamiento" y "envío" (store and forward) exclusivamente; no participan en la toma de decisiones. Otros algoritmos (enrutador inteligente) no conceden al anfitrión ni voz ni voto para el proceso de enrutamiento; sólo los enrutadores pueden determinar las rutas con base en sus cálculos. Los sistemas de anfitrión inteligente con frecuencia escogen las mejores rutas, pues descubren todas las rutas posibles antes de enviar los datos, lo que implica un incremento sustancial de tiempo de procesamiento y tráfico de autodescubrimiento.

Intradominio o interdominio

Algunos algoritmos de enrutamiento sólo pueden operar dentro de un mismo dominio (sistema autónomo), otros en cambio están diseñados para operar dentro y entre sistemas autónomos.

Estado de enlace (Link state) o vector-distancia (distance-vector)

Los algoritmos de estado de enlace (también conocidos como "primero abrir la ruta más corta") llevan la información de enrutamiento a todos los nodos de la Internet. Sin embargo, todo enrutador envía exclusivamente aquella porción de su tabla de enrutamiento que describe el estado de sus propios enlaces. Los algoritmos de vector-distancia (también conocidos como **Bellman-Ford**) obligan a todo enrutador a intercambiar sus tablas de enrutamiento (o parte de ellas) solamente con sus vecinos. Básicamente los algoritmos de estado de enlace envían pequeñas actualizaciones por toda la Internet, mientras que los de vector-distancia envían actualizaciones más grandes sólo a sus vecinos. Los algoritmos de estado de enlace convergen más rápidamente y por lo tanto es más difícil que caigan en lazos de enrutamiento; por otro lado, requieren mayor poder de procesamiento y memoria que los algoritmos de vector-distancia.

En el extracto del RFC 1058 que se presenta a continuación, se describe brevemente el algoritmo final de enrutamiento para los protocolos de la familia vector-distancia:

To sumarize, here is the basic distance-vector algorithm as it has been developed so far the following procedure is carried out by every entity that participates in the routing protocol. This must include all of the gateways in the system. Hosts that are not gateways may participate as wel.

Keep a table with an entry for every possible destination in the system. The entry contains the distance D to the destination, and the first gateway G on the route to that network. Conceptually, there should be an entry for the entity itself, with metric 0, but this is not actually included.

Periodically, send a routing update to every neighbor. The update is a set of messages that contain all of the information from the routing table. It contains an entry for each destination, with the distance shown to that destination.

When a routing update arrives from a neighbor G', add the cost associated with the neighbor that is shared with G' (this should be the network over which the update arrived). Call the resultance distance D'. Compare the resulting distances with the current routing table entries. If the new distance D' for N is smaller than the existing value D, adopt the new route. That is, change the table entry for N to have metric D' and gateway G'. If G' is the gateway from which the existing route carne, i.e. G' = G, then use the new metric even if it is larger than the old one.

Métricas

Se ha mencionado que las tablas de enrutamiento contienen la información

necesaria para determinar la mejor ruta a cualquier red pero, ¿Cómo se define y cuál es la mejor ruta?, ¿Qué parámetros o combinación de éstos son empleados?

Diversas métricas (valores obtenidos de cálculos hechos sobre variables particulares, tales como la longitud de la ruta, el retraso para cruzaría, etc.) o combinaciones de ellas han sido utilizadas en los algoritmos de enrutamiento. Los más sofisticados de ellos basan sus decisiones de enrutamiento en múltiples métricas, combinándolas en una sola métrica híbrida. Las métricas más empleadas actualmente son:

- Longitud de la ruta
- Confiabilidad
- Retardo
- Ancho de banda
- Carga
- Costo de la comunicación

Longitud de ruta

Es la métrica más comúnmente empleada. Algunos protocolos de enrutamiento permiten al administrador que designe en forma arbitraria costos a cada enlace de la red. En este caso, la longitud de la ruta es la suma de los costos asociados con cada enlace atravesado. Otros protocolos de enrutamiento definen una cuenta de saltos (hop count) como él número de enrutadores que un paquete debe cruzar para llegar a su destino.

Confiabilidad

Se refiere a la confiabilidad de cada enlace de red. Algunos enlaces se caen con más frecuencia que otros. Ya fuera de servicio, toma más tiempo poner a trabajar de nuevo a unos que a otros. Cualquier factor de confiabilidad puede ser tomado en cuenta en la asignación de los factores de confiabilidad. Éstos son por lo general valores numéricos arbitrarios.

Retardo

Se refiere al tiempo empleado para mover un paquete desde su origen hasta su destino a través de una internet. El retardo depende de muchos factores, entre ellos el ancho de banda de enlaces intermedios, tráfico en la red, la distancia física entre los extremos, etc. Como métrica que refleja distintas variables, el retardo es muy útil.

Ancho de banda

Se refiere a la capacidad del canal para manejar tráfico. Aunque refleja la máxima capacidad del medio, no implica que éste sea mejor ruta que aquellos canales con anchos de banda menores. Por ejemplo, un canal de 10 Mbps puede estar muy saturado de tráfico, por lo que el tiempo que le requeriría a un datagrama llegar a su destino a través de él, sería mayor que si empleara otro

canal alterno con ancho de banda y tráfico menores.

Carga

Se refiere a qué tan ocupado está un dispositivo de red, el enrutador, por ejemplo. La carga puede ser calculada de diversas formas, entre ellas la utilización del CPU y el número de paquetes procesados por segundo.

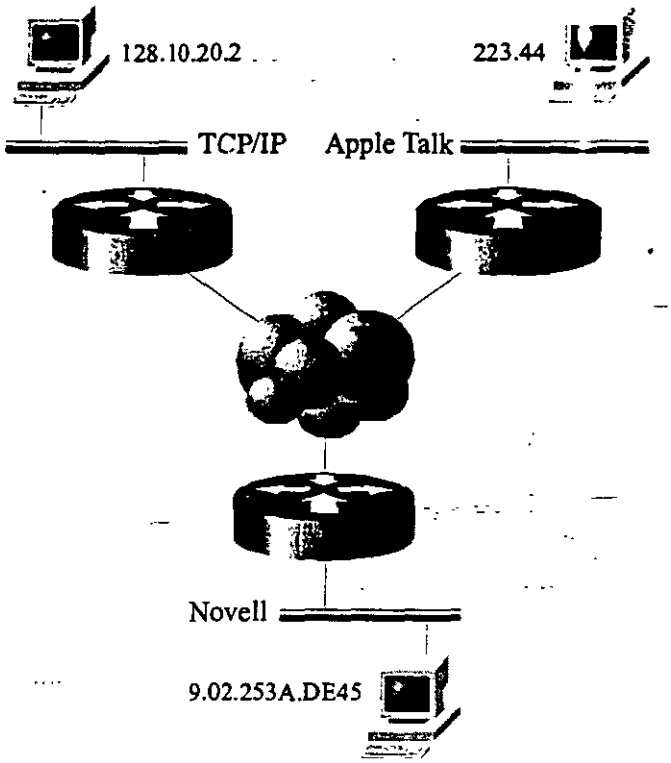
Costo de la comunicación

Algunas compañías se preocupan más por el costo económico de la operación de su red que por su desempeño. Esta métrica ayuda a forzar la circulación de la información a través de los enlaces de la compañía en lugar de los servicios públicos.

La parte del RFC 1058 que se incluye enseguida define someramente las métricas:

As we mentioned above, the purpose of routing is £0 find a way to get datagrans to the ir ultimate destinations. Distance-vector algorithms are based on a table giving the best route for every destination in the system. Of course, in order to define which route is the best, we have to some way of measuring goodness. This is referred to as the "metric".

In simple networks, It is common to use a metric that simply counts how many gateways a message must go through. In more complex networks, a metric is chosen to represent a total amount of delay that the message suffres, the cost of sending it, or some other quantity which may be minimized. The main requirement is that it must be possible to represent the metric as a sum of "costs" for individual hops.



Los enrutadores mantienen tablas separadas para cada protocolo de la capa de red.

Los diferentes protocolos de enrutamiento no se conocen entre sí.

Protocolos de enrutamiento

Un protocolo es una descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en la que los dispositivos de una red intercambian información.

Protocolo de información de enrutamiento: RIP

Este protocolo pertenece a una serie de protocolos de enrutamiento basados en el algoritmo de Bellman-Ford, también conocido como algoritmo de vector-distancia. Este algoritmo ha sido usado para enrutamiento en redes de computadoras desde los primeros días de ARPANET. RIP (Routing Information Protocol) está incluido en la distribución de UNIX de Berkeley, por lo que se ha convertido en un estándar para intercambio de información de enrutamiento por medio de compuertas y anfitriones. Ha sido implementado para este propósito por la mayoría de los vendedores comerciales de compuertas IP.

RIP es usado como un «protocolo de compuerta interno» (IGP). También fue diseñado para trabajar con redes de un tamaño moderado usando tecnología homogénea. Por eso, está situado como un IGP para campus y redes regionales que utilizan líneas seriales, donde sus velocidades no son muy variadas. No se tiene la intención de usar RIP en ambientes más complejos.

RIP está dispuesto para ser usado dentro del protocolo IP basado en Internet. Internet está organizada en un número de redes conectadas por compuertas. Las redes pueden ser punto a punto o más complejas como Ethernet o Token Ring. Los anfitriones o compuertas son representados por datagramas IP direccionados a un anfitrión. Enrutar es el método por el cual el anfitrión o compuerta decide a dónde enviar el datagrama. Es posible enviar el datagrama a su destino en forma directa, si el destino se encuentra en una de las redes que están conectadas directamente al anfitrión o compuerta. Sin embargo, lo interesante es cuando el destino no se alcanza directamente. En este caso, la compuerta o anfitrión intenta enviar el datagrama a una compuerta cercana al destino. La meta de un protocolo de enrutamiento es muy simple: sustituir la información que se necesita para realizar el enrutamiento.

Limitaciones de RIP

RIP no resuelve todos los posibles problemas de enrutamiento. Como ya se mencionó anteriormente está diseñado para trabajar como un protocolo IGP en redes homogéneas y de tamaño moderado, por lo cual se mencionarán algunas limitaciones:

El protocolo está limitado a redes en las cuales la ruta más grande contiene 15 saltos. De esta manera se configura RIP si el administrador de sistema escoge más de 15 saltos podría ocurrir un problema fácilmente.

El protocolo utiliza "métricas" fijas para comparar rutas alternativas. Esto no es apropiado para situaciones donde las rutas necesitan escoger parámetros de tiempo real tales como un retardo, fiabilidad o carga. La extensión obvia para permitir métricas de este tipo implica inestabilidad que este protocolo no puede manejar.

Especificaciones para el protocolo

RIP está desarrollado para permitir que anfitriones y compuertas intercambien información para calcular rutas a través de redes IP. RIP es un protocolo de vector-distancia, que puede ser implementado por anfitriones y compuertas. Se utiliza para llevar información de enrutamiento al destino, el cual puede ser anfitriones individuales, redes o destinos especiales usados para llevar una ruta predeterminada. RIP mantiene sólo la mejor ruta hacia un destino.

Se puede asumir que cualquier anfitrión que utilice RIP tiene una interfaz para una o más redes; es decir, redes de conexiones directas. El protocolo proporciona cierta información acerca de cada una de estas redes.

Cada anfitrión que implementa RIP contiene una tabla de enrutamiento. Esta tabla tiene una entrada para cada uno de los destinos que es alcanzable a través del sistema descrito por RIP. Cada entrada contiene al menos la siguiente información:

- La dirección IP del destino.
- Una métrica, la cual representa el costo total de obtener un datagrama del anfitrión al destino. Esta métrica es la suma del costo asociado con las redes por las cuales pasará para corregir el destino.
- La dirección IP de la siguiente compuerta de la ruta al destino. Si el destino es uno de los que están conectados directamente, esta información no es necesaria.
- Una banden que indica que la información acerca de la ruta se ha modificado recientemente. Ésta será referida como «bandera de enrutamiento modificada».
- Varios timen asociados con la ruta.

Red A	Enrutador 1	3	t1;t2,t3	x,y
Red B	Enrutador 2	5	t1,t2,t3	x,y
Red C	Enrutador 3	2	t1,t2,t3	x,y

Las entradas para redes conectadas directamente son dadas por el anfitrión, usando información que no se encuentra especificada en este protocolo. La métrica para una red conectada directamente está dada por el costo de esa red. En implementaciones existentes de RIP el coto se reduce a una Simple cuenta de saltos. Las métricas más complejas deben ser usadas cuando se desea tener referencia de otras redes, por ejemplo debido a diferencias de ancho de banda o fiabilidad.

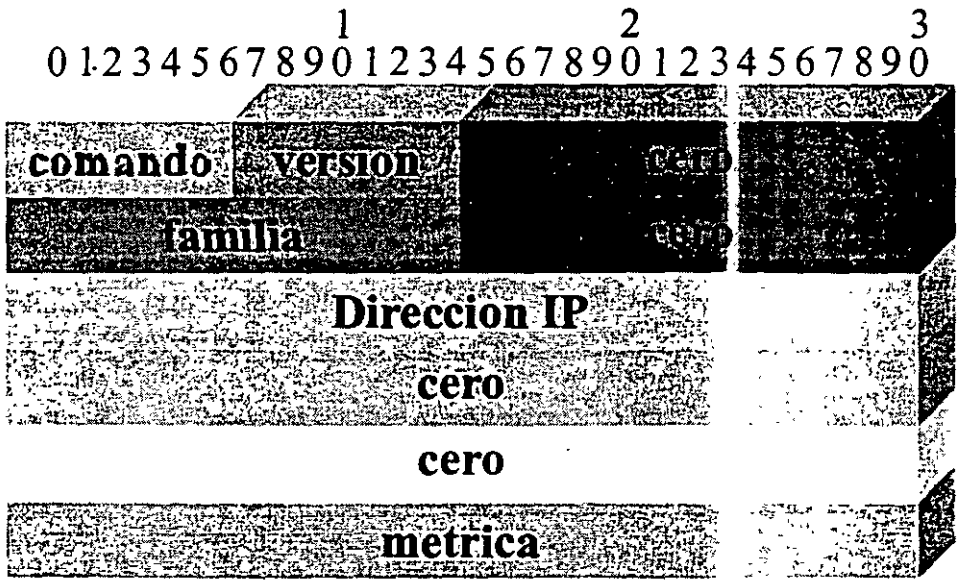
Para proveer el protocolo de información de enrutamiento, cada compuerta en el sistema debe participar. Los anfitriones que no son compuertas no necesitan participar, pero muchas implementaciones hacen provisiones para ello y así los anfitriones pueden tener la información para mantenerlas en su tabla de enrutamiento.

Formatos de mensajes

RIP es un protocolo basado en UDP. Cada anfitrión que utiliza este protocolo tiene un proceso de enrutamiento que envía y recibe datagramas en el puerto UDP 520.

Hay estipulaciones en el protocolo para permitir procedimientos RIP «silenciosos». Un proceso silencioso es aquel que normalmente no manda ningún mensaje. Sin embargo, escucha los mensajes enviados por otros. Un RIP silencioso debe ser usado por anfitriones que no actúan como compuertas, pero que desean escuchar los enrutamientos a manera de compuertas locales y guardar sus tablas de enrutamiento interno.

La siguiente figura muestra el formato del paquete:



El formato de los datagramas condene información de la red. El tamaño de los campos está dado en octetos. A menos que se especifique otra cosa, los campos condenen enteros binarios, con el octeto más significativo primero. Cada marca representa un bit.

La dirección IP usualmente es el octeto 4 del paquete RIP la dirección de Internet. Cada datagrama contiene un comando, un número de versión y posibles argumentos. El campo del comando se utiliza para especificar el propósito de este datagrama. El máximo tamaño del datagrama es de *512* octetos. No incluye el encabezado IP o UDP.

Consideraciones de direcciones

Un enrutamiento de vector-distancia puede ser usado para describir rutas para un anfitrión individual o una red. El protocolo RIP permite las dos posibilidades. El formato del paquete MP no distingue entre varios tipos de direcciones. Los campos que están etiquetados como «address» pueden contener cualquiera de la siguiente información:

- Dirección de anfitrión
- Número de una subred
- Número de una red
- 0, indica una ruta predeterminada (por default)

Las entidades que utilizan RIP emplean la información más específica disponible cuando se enruta un datagrama, su dirección de destino debe ser verificada primeramente para ver si concuerda con alguna subred o números de redes conocidos. Finalmente, si ninguno de éstos concuerda entonces se utiliza la ruta predeterminada (default).

Cuando un anfitrión evalúa la información que recibe vía RIP la interpretación de la dirección depende de si se conoce la máscara de la subred que se aplica a la red. Si esto se cumple, entonces es posible determinar el significado de la dirección. Sin embargo, si el anfitrión no conoce la máscara de la subred la evaluación de la dirección puede ser ambigua. Si no existe un cero en la parte del anfitrión, no se puede determinar el camino para determinar qué es lo que la dirección representa, si es un número de subred o es una dirección de anfitrión.

La dirección especial 0.0.0.0 se utiliza para saber una ruta predeterminada. Una ruta predeterminada se usa cuando no es conveniente listar todas las redes de RIP y cuando una o más compuertas cercanas en el sistema están preparadas para manejar tráfico a las redes que no están especificadas explícitamente.

Estas compuertas deben crear entradas RIP para la dirección 0.0.0.0 como si

hubiera una red a la cual estuvieran conectadas, Si existe más de una compuerta predeterminada será posible preferir una sobre otra. Las entradas 0.0.0.0 son manejadas por RIP como si fueran redes con sus direcciones. Sin embargo, la entrada es usada para enrutar cualquier datagrama cuya dirección de destino no concuerde con otra en la tabla.

Timers

Cada 30 segundos, el proceso de salida está capacitado para generar una actualización completa hacia todas las compuertas cercanas. Cuando existen varias compuertas en una sola red, se tiende a sincronizarías unas con otras, de tal manera que todas sus emisiones ocurran al mismo tiempo. Esto puede suceder siempre y cuando los 30 segundos sean afectados por el procesamiento cargado en el sistema.

Existen dos timers asociados con cada ruta, un «tiempo de expiración» y un «tiempo de colecta de basura o de 'flushing' ». Cuando un tiempo de expiración se cumple la ruta ya no es valida.

Sin embargo, permanece en la tabla por un tiempo, dando lugar a que las compuertas cercanas se den cuenta de que la ruta ya no es válida. Cuando expira el timer de colecta de basura, la ruta se elimina de la tabla.

El tiempo de expiración es inicializado cuando se establece la ruta, y a cualquier tiempo se reciben mensajes para la ruta. Si pasan 180 segundos después de la inicialización del tiempo agotado se considera que la ruta ha expirado y enseguida comienza el proceso de desecho (tiempo de colecta de basura).

Protocolo de enrutamiento de compuerta interna: IGRP

IGRP (Internal Gateway Routing Protocol) es un protocolo que permite que las compuertas coordinen sus rutas. Sus objetivos son:

- Establecer enrutamiento en una cierta topología de red.
- Dar una respuesta a cierta topología de red.
- Dividir el tráfico entre varias rutas paralelas.
- Manipular múltiples servicios con un conjunto simple de información.

Los protocolos como IGRP son llamados "protocolos de compuerta interna" (IGP). Este tipo de protocolos, se utiliza dentro de un conjunto de redes simples, conectadas por "protocolos de compuerta externa" (EGP).

En algunas situaciones el protocolo de enrutamiento de compuerta interna, IGRP, puede ser utilizado como un EGP. IGRP tiene algunas similitudes con

los protocolos de enrutamiento de Xerox y RIP de Berkeley, pero difiere en que IGRP fue implementado para grandes redes de computadoras.

El protocolo IGRP está destinado para uso de compuertas que conecten varias redes. Cuando un sistema conectado a una red quiere enviar un paquete a otro sistema en otra red, el paquete se envía directamente, en cambio si el destino está más lejos la compuerta busca en su tabla de enrutamiento la compuerta que está más cercana al destino.

Timers

IGRP mantiene un número de timers e intervalos de tiempo de contacto. Esto incluye un dato de tiempo actualizador de timer, un timer inválido, un periodo de retención de timer y un timer de desecho. El timer de actualización actualiza el mensaje antes de que sea enviado. El timer de invalidación especifica cuánto tiempo debe esperar un enrutador, en la ausencia de mensajes de enrutamiento actualizados acerca de una ruta específica, declarando antes la ruta inválida. El IGRP define esta variable como 3 veces el periodo de actualización del timer. Y la variable del periodo de retención especifica el periodo de mantenerse sujeto (IGRP por omisión es igual a 3 veces el periodo de actualización del timer más 10 segundos). Finalmente, el timer de desecho indica cuánto tiempo pasará antes de que una ruta sea desechada de la tabla de enrutamiento. IGRP por omisión lo define igual a 7 veces el periodo de actualización de enrutamiento.

Resumen

El protocolo IGRP permite a las compuertas construir y mantener tablas de enrutamiento para intercambiar información con otras compuertas. Una compuerta hace su tabla para poder comunicarse con las redes que están directamente conectadas a ella.

En un caso simple una compuerta encontrará una ruta que represente el mejor camino para alcanzar otra red o una ruta caracterizada por la próxima compuerta, para que los paquetes puedan ser enviados. Periódicamente una compuerta realiza una broadcast (difusión) en su tabla de enrutamiento, cuando una compuerta recibe un broadcast (difusión) de otra compuerta, la compara con la tabla existente para buscar otras rutas mejores y poder sustituirla. Todos los protocolos de vector-distancia utilizan este procedimiento, al cual se le conoce como algoritmo de Bellman-Ford.

Protocolo de compuerta exterior: EGP

El protocolo EGP (Exterior Gateway Protocol) es más utilizado en compuertas externas vecinas y entre internets, en las cuales los sistemas autónomos hacen uso del EGP para divulgar las rutas del sistema central.

El protocolo EGP se ha especificado para permitir desarrollos autónomos de sistemas de compuerta mientras se mantiene una distribución global de la información de enrutamiento en redes interconectadas. EGP provee un significado para sistemas de compuerta autónomos para intercambiar información acerca de redes que son alcanzadas por ellos.

EGP generalmente se conduce por medio de compuertas en diferentes sistemas autónomos que comparten una red en común, es decir, compuertas vecinas.

Características

A continuación se mencionan las principales características del protocolo EGP:

Soporte de mensajes de adquisición de vecino

Una compuerta envía un mensaje de adquisición de vecino para establecer comunicación EGP con otra compuerta.

Antes de iniciar la propagación de rutas una compuerta solicita y espera un permiso para enviar información. Un mensaje de adquisición contiene campos con valores iniciales para dos intervalos de tiempo:

Hello	Usado para ver si la compuerta vecina está "viva".
Polling	Controla la frecuencia máxima de actualización de rutas.

Verificación continua del funcionamiento de vecinos

El protocolo EGP permite dos formas de verificar si la compuerta vecina está "viva": por medio del modo activo y por el modo pasivo.

En el modo activo las compuertas prueban periódicamente un vecino, enviando mensajes Hello y un mensaje Polling, y esperan una respuesta.

En el modo pasivo, la compuerta depende de su vecino para enviar mensajes tipo Hello o Polling.

Divulgación de información

La compuerta que ejecuta EGP periódicamente divulga mensajes que listan las rutas para las redes o sistemas autónomos que toman accesos públicos. Estos mensajes también listan cuál es la distancia y el número de compuertas. Estos sistemas deben ser divulgados para redes que pertenezcan a un sistema autónomo, facilitando así el control de la información y evitando el tráfico de información redundante.

Tipos de mensaje

Para ilustrar las características citadas anteriormente, el protocolo define dos tipos de mensajes:

- Adquisición de vecino
- Establecimiento de contacto con el vecino
- "Polling" (determinar si una red es o no alcanzable)
- "Update", que indica actualización (preveer actualización de enrutamiento)
- Error, que indica condiciones de error
- Solicitud de adquisición
- Compuerta que solicita ser vecino

Tablas de enrutamiento

Una ruta consiste en un numero de red destino, la dirección de la próxima compuerta que se pueda usar de manera directa para conectarse a una red y una métrica que proporciona la distancia de los saltos hacia la red destino.

Existen dos tipos de tablas de enrutamiento, las tablas kernel (para envíos de paquetes) y el proceso de tablas EGP. Las tablas kernel contienen tablas separadas para destinos de anfitrión y de redes. El proceso EGP sólo mantiene las tablas de enrutamiento de red.

La implementación del EGP está diseñada para correr en una compuerta que también es un anfitrión.

El proceso EGP de tablas de enrutamiento se mantiene como dos tablas separadas, una para rutas exteriores (vía diferentes compuertas del mismo sistema autónomo) y la otra para rutas interiores (vía compuertas de sistemas autónomos).

Tener tablas separadas para enrutamientos interiores y exteriores facilita la separación de mensajes de salida, los cuales sólo contienen información de enrutamiento interno. También permite guardar rutas externas alternativas como un respaldo por si alguna ruta interna fracasa.

Restricciones del protocolo EGP

El protocolo EGP también tiene algunas restricciones técnicas:

- Limita las compuertas.
- Permite que propaguen sólo aquellas redes totalmente dentro de dos sistemas autónomos.
- Limita la topología.

- Limita la topología de cualquier red interna que use EGfl debido a que se propaga información de alcanzabilidad.

Protocolo de compuerta frontera: BGP

BGP (Border Gateway Protocol) es un protocolo de enrutamiento de sistemas interautónomos. Fue construido con base en la experiencia obtenida con el protocolo EGP (protocolo de compuerta externa).

La función primaria de un sistema BGP es intercambiar información de comunicación de red con otros sistemas BGP. Esta información de comunicación de red incluye la lista de los sistemas autónomos involucrados. Esta información es suficiente para construir un diagrama de la conectividad de los sistemas autónomos desde los cuales se deben probar los ciclos de enrutamiento.

Version: 8 bits

El campo Versión es de 8 bits del número de versión del protocolo. Si se encuentra un número de versión equivocada, un mensaje de notificación con el código 8 (número de versión equivocada) debe ser enviado y la conexión BGP se debe cerrar. El número de versión equivocada debe ser incluido en un byte de dato de notificación.

Type: 8 bits

El campo Type es de 8 bits. Los mensajes de tipo de códigos que se encuentran definidos son:

- OPEN
- UPDATE
- NOTIFICATION
- "KEEP ALIVE"
- OPEN CONFIRM

Si se encuentra un valor de tipo no conocido, se debe enviar un mensaje de notificación con código 7 (tipo de código equivocado) y el dato consiste de un byte del campo type, y se debe cerrar la conexión BOR

Holder timer: 16 bits

Este campo contiene el número de segundos que pueden transcurrir desde que se recibe el mensaje "Keep Alive" o "Update" desde el par BGP, antes de que se declare un error y se cierre la conexión BGP.

Descripción de la operación

Dos sistemas forman una conexión de protocolo de transpone entre uno y otro. Ambos intercambian mensajes para abrir y confirmar la conexión de parámetros. El dato inicial aparece en la entrada BGP de la tabla de enrutamiento. BGP no necesita refrescar periódicamente la tabla de enrutamiento, por lo tanto, "el que habla" (speaker) BGP debe retener la versión actual de la entrada BGP de la tabla de enrutamiento de todos sus pares durante la conexión. Mensajes "Keep Alive" se envían periódicamente para asegurarse de que la conexión está "viva". Se envían mensajes de notificación en respuesta a errores de condiciones especiales. Si una conexión encuentra una condición de error, un mensaje de notificación es enviado y se cierra la conexión.

Los anfitriones que ejecutan no necesariamente tienen que ser enrutadores. Un anfitrión no enrutador puede intercambiar información de enrutamiento con otros enrutadores vía EGP (Protocolo de compuerta externa) o también mediante un protocolo de enrutamiento interno. Así, el anfitrión no enrutador puede intercambiar información de enrutamiento con un enrutador de frontera (border) en otro sistema autónomo.

Si un sistema autónomo particular tiene múltiples speakers BGP y provee servicio de tránsito a otros sistemas autónomos, entonces se debe hacer una revisión consistente del enrutamiento dentro del sistema autónomo. Una revisión consistente de las rutas interiores del sistema autónomo es provista por el protocolo de enrutamiento interno. Una revisión consistente de las rutas exteriores del sistema autónomo puede ser provista al tener todos los speakers BGP dentro del sistema autónomo, manteniendo una conexión directa con cada una.

Conexiones con speakers BGP de diferentes sistemas autónomos son referidas como enlaces "externos". Conexiones BGP entre speakers BGP dentro del mismo sistema autónomo son referidas como enlaces "internos". De manera súnilar, un par en un sistema autónomo diferente es conocido como un par externo, mientras que a un par en el mismo sistema autónomo se le llama par interno.

Formatos de mensajes

Los mensajes son enviados dentro de una conexión de un protocolo de transporte. Un mensaje es procesado después de que es enteramente recibido. El tamaño máximo del mensaje es de 1024 bytes. El mensaje más pequeño que puede ser enviado consiste de un encabezado (header) BGP sin la parte de datos u 8 bytes.

Formato del mensaje de encabezado

Cada mensaje tiene un tamaño de encabezado fijo. Puede o no existir una porción de datos después del encabezado, dependiendo del tipo de mensaje. La siguiente figura muestra el formato de encabezado:

Marker: 16 bits

El campo Marker es de 16 bits, todos números 1. Este campo es usado para marcar el inicio del mensaje. Silos dos primeros bytes del mensaje no son todos números 1, entonces se tiene un error de sincronización y la conexión BGP debe ser cerrada después de enviar un mensaje de notificación con el código 5 (conexión no síncrona). La notificación de no datos es enviada.

Length: 16 bits

El campo Length es de 16 bits. Es la longitud total del mensaje, incluyendo el encabezado en bytes. Si se encuentra una longitud ilegal (más de 1024 bytes o menos de 8 bytes), se debe enviar un mensaje de notificación con el código 6 (mensaje de longitud errónea) y dos bytes de datos de la longitud errónea, y la conexión BGP se debe cerrar.

A continuación se ofrecen extractos del RFC 1267 que describen a BGP 3:

The primary function of a BGP speaker system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the full path of Autonomous Systems (ASs) that traffic must transit to reach these networks. This information is sufficient to construct a graph of AS connectivity from which routing loops may be pruned and some policy decisions at the AS level may be enforced.

To characterize the set policy decisions that can be enforced using BGP, one must focus on the rule than a AS advertise to t oits neighbor ASs only those routes that it itself uses. This rule reflects the "hop-by-hop" routing paradigm generally used throughout the current Internet. Note that some policies cannot be supported by the "hop-by-hop" routing paradigm and thus requires techniques such as source routing to enforce. For example, BGP does not enable one AS to send traffic to a neighbor AS intending that that traffic tale a different route from that taken by traffic originating in the neighbor AS. On the other hand, BGP can support any policy conforming to the "hop-by-hop" routing paradigm. Since the current Internet uses only the "hop-by-hop" routing paradigm and since BGP can support any policy that conforms to that paradigm, BGP is highly applicable as an Inter-AS routing protocol for the current Internet.

BGP runs over a reliable transpot protocol. This eliminates the need to implement explicit update fragmentation, retransmission, ackowledgement, and

sequencing. Any authentication scheme used by the transport protocol rnay be used in adition to BGP's own authentication mechanisms. The error notification mechanism used in BGP assumes that the transport protocol supports a "graceful" close, i.e., that all outstanding data will be delivered before the connection is closed.

BGP uses TCP (4) as its transport protocol. TCP meets BGP's transport requirements and is present in virtually all commercial routers and hosts.

BGP Timers.

BGP emplea tres timers: ConnectRetry, HoldTime y KeepAlive.
Loas valores

Suggested value for the ConnectRetry timer is 120 seconcis.
Suggested value for the Ho íd flme timer is 90 seconds.
Suggested value for the KeepAlive timer is 30 seconds.
An implementation of BGP shall allow any of these timers to be configurable.
OSPF
OSPF (Open Shortest Pat First) es clasificado como un protocolo IGP ~rotocolo de compuerta interna). Esto significa que se dedica a distribuir información entre enrutadores de sistemas autónomos simples. El~protocolo OSPF está basado en la tecnología Link State.

OSPF fue modelado para internets, incluyendo soporte explicito para subredes IR También provee autenticidad de mensajes de actualización de enrutamiento y utiliza IP multicast cuando recibe o envía actualizaciones.
Generalidades
OSPF es un protocolo de enrutamiento dinámico. que enruta paquetes básicos. El protocolo detecta rápidamente fallas fuera del sistema autónomo y calcula nuevas rutas, libres de ciclos.

En un protocolo de enrutamiento basado en SPF (Shortest Pat First) cada enrutador mantiene una base de datos que describe la topologia del sistema autónomo. Cada enrutador participan-te posee una base idéntica. Y cada parte individual de esta base de datos~es un estado particular del enrutador local.

OSPF calcula separadamente rutas para cada tipo de servicios (TOS). Cuando varias rutas de costos iguales existen para un destino, el tráfico es distribuido sobre ellas. El costo de una ruta es descrito por una métrica.

Además OSPF permite que conjuntos de redes sean agrupados en áreas. Una topología de área no es vista por el resto del sistema autónomo. Esta información oculta permite una reducción significativa del tráfico de enrutamiento. De la misma forma, el enrutamiento de un área es determinado por la topología del área.

El protocolo OSPF permite una configuración flexible de subredes IP. Cada ruta distribuida OSPF posee un destino y una máscara. Dos subredes de un mismo número de IP de red pueden tener diferentes tamaños (máscaras), a 10 cual se conoce como tamaño variable de subredes. Un paquete es enrutado por la mejor combinación.

Datos externos de enrutamiento (originales de EGP) son pasados en forma transparente del sistema autónomo. Estos datos se conservan de forma separada de los datos del estado de enlace OSPE Cada ruta externa puede ser etiquetada pór el enrutador que está anunciado, permitiendo un paso de información adicional entre enrutadores de fronteras de un sistema autónomo.

OSPF soporta los siguientes tipos de redes:

Punto a punto Una red que posee un par de enrutadores.

Broadcast Redes que soportan más de un enrutador, los cuales poseen la capacidad de enviar un mensaje a todos los otros enrutadores (broadcast).

No-bmadcast Redes que poseen varios enrutadores, pero no poseen la capacidad de broadcast. Por ejemplo, la red pública ~25.

Funcionalidades

En cada área se encuentra una copia del algoritmo básico de OSPE Los enrutadores que poseen una interfaz~para varias áreas tienen múltiples copias del algoritmo.

Un enrutador se inicializa como una estructura de datos del protocolo. Utiliza el protocolo Hello para conocer lós enrutadores vecinos que envían paquetes de Hello.

Los enrutadores informan periódicamente su estado, al que también se conoce como estado de enlace (lirik state). El estado de enlace a su vez es informado cuando un enrutador no tiene un buen funcionamiento.

A continuación se présentan extractos del RFC 1247 que describen a OSPF 2:

1.1 Pmtocol overview

OSPF mutes packets based soley on the destination IP address and IP Type ofServicefound in the IPpacket header IPpackets are routed as is~-they are nol encapsulated in anyfrrther proto col headers as they transit the Autonomous System. OSPE is dynamicmuting pro tocol It quickly detecis topological chan ges in the AS (such as rauter interjáce failures) and calcula ies new loop-free mutes after a period of convergence. 'his period of convergence is short and invo ¿ves a minimum of routing traffic.

In an SPF-based mutingpmtoco¿ each mu ter maintains a dala base describing ihe Autonomous System '5 topology.. Each participating muter has identical database. Each individual piece of this database is aparticular roater 's local state (e. g.; ihe muter 's usable inteifaces aH reachable neighbors). The muter distributes jIs local siate thmughout the Autonomaus System byfolding.

Al! muters run lhe exacl same algorithm, in parallet Fmm ihe topological database, each muter construcis a tree ofshortestpaths with itselfas mot 'his shortest-path tree gives the mute to each destination in the Autonomous System.

Externally derived routing information appears on the tree as ¡caves.

OSPF calculates sepa rate mutes for each Type of Service (TOS). When several equal-cost mutes to a destination exist, trafflc is distributed equally among them. 'he cost of a mute is described by a single dimensionless metric.

OSPF allows sets of networks to be gmuped together Such a groupi~g is called an area. The topology of an area is hidden 'mm the rcst of the Autonomous System. Ibis information hiding enables a signzficant reduction trafflc. Also, muting within the area ¿5 determined only by the area 5 own topology, lending the area pmtection 'mm bat muting data. An area is generalization of an IP subnetted network.

OSPF enables the flexible configuration of IP subnets. Iach mute distribute by OSPF has a destination aH mask Two drfferent subnets of the sarne IP network number may have dzfferent sizes (e. g.; dzfferent masks). Ibis is commonly referred to as variable len gth subnets. A packet ¡5 muter to the best (Le.; Ion gs or most speczflc) match. Host mutes are considered to be subnets whose masks are 'afl ones~ (O~.

Aif OSPF pmtocol exchan ges are authenticated. Ibis means that only trusted mutes can participate in the Autonomous System'8 routing. A variety of authentication schemes can bë used; a sin gled authentication scheme is configuredfor each area. Ibis enables sorne arcas to use much stricter authentication than others.

flmers

Two differenr kind of times are required. 'he first kind, caller singles shon time rs, fire once aH cause. a pmtocol event to be pmcessed. 'he second kind, called interval timers, fire at continuous intervais. 'hese are used for the sending of packets at regular intervais. A good example of this is the regitiar bmadcast of Helio packets (on bmadcast networks). 'he granularity of both kinds of timers ¡5 one secorid.

Interval time rs should be implemented to avoid dnft. In sorne mutered implernentations, packet pmcessing can affect timer execution. When multiple mutes are anached. to a single network, alf doing bmakasts, this can lead to the synchmnization ofmutingpackets (wh ¿ch shoud be avoided). ff timers cannot be imp lemented to avoid drrfi, srnall random arnounts shoud be acicied tol subtracted 'mm the timer interval at eachfiring.

OSPF

A continuación se mencionan algunas de las características de OSPF:

- Especificado en los RFC 1131 y 1247
- Es un protocolo de estado de línea
- Utiliza el costo como métrica
- Se utiliza en un solo AS

Arcas én OSPF

Son una o más redes contiguas. Cada área corre su propia copia de algoritmo .SPF. El enrutamiento corre:

Backbone de OSPF

Todos IOS dominios de enrutamiento de OSPF tienen una sola área de backbone que se define como área 0. El backbone debe ser contiguo. El enrutamiento de interárea utiliza el backbone como un área de tránsito. Todas las áreas deben estar conectadas al área O (backbone).

LSA ~ink State Annoúncements)

Un LSA es un paquete que contiene información acerca de las lineas directamente conectadas al original del LSA. Se generan cuando hay un cambio en la línea o cada 30 minutos.

Protocolo Helio

El protocolo Hello establece y mantiene las relaciones de vecinos. Los enrutadores vecinos forman adyacencias, las cuales se utilizan para elegir enrutadores designados o redes de multiacceso.

Ennitadores designados (13R) de OSPF

Isis DR generan el LSA de la finca de la red. Al usar un DR se limita el número de enrutadores adyacentes necesarios, reduciendo el tráfico de los protocolos de enrutamiento y el tamaño de la base de datos topológica.

Métrica de OSPF

La métrica selecciona una ruta basada en el menor costo. El costo de un valor arbitrario se asigna por el administrador de la red. Casi todos los equipos tienen valores predeterminados.

Protocolos de enrutamiento

OSPF puede tener máscaras variables, TUS basado en enrutamiento y autentificación de paquetes.