**RESUMEN**

**Encaminamiento**

Es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por mejor ruta y en consecuencia cuál es la métrica que se

debe utilizar para medirla.

**Métrica de la red**

La métrica simplemente es un valor que toman los diferentes protocolos de enrutamiento para poder determinar cuál es la mejor ruta hacia una red de destino. No es difícil encontrarse con situaciones donde un router tenga más de un único camino hacia una red de destino y, por lo tanto, deberá emplear algún método para determinar cuál de esos caminos le conviene más.

En algunos casos el router determinará que el mejor camino es aquel cuya distancia es menor o en otros casos determinará que la mejor ruta es aquella que tiene mejor ancho de banda. Esto va a depender de cual sea el protocolo de enrutamiento que se esté utilizando, el número de saltos necesarios para ir de un nodo a otro. Aunque ésta no es una métrica óptima ya que supone “1” para todos los enlaces, es sencilla y suele ofrecer buenos resultados.

Otro tipo de métrica es la medición del retardo de tránsito entre nodos vecinos, en la que la métrica se expresa en unidades de tiempo y sus valores no son constantes, sino que dependen del tráfico de la red.

**Mejor Ruta**

Consigue mantener acotado el retardo entre pares de nodos de la red.

Consigue ofrecer altas cadencias efectivas independientemente del retardo medio de tránsito

Permite ofrecer el menor costo.

**Adaptativos o dinámicos**

El encaminamiento dinámico o adaptativo se puede clasificar a su vez en tres categorías, dependiendo de donde se tomen las decisiones y del origen de la información intercambiada:

Adaptativo centralizado. Todos los nodos de la red son iguales excepto un nodo central que es quien recoge la información de control y los datos de los demás nodos para calcular con ellos la tabla de encaminamiento. Este método tiene el inconveniente de que consume abundantes recursos de la propia red.

**Adaptativo distribuido**

Este tipo de encaminamiento se caracteriza porque el algoritmo correspondiente se ejecuta por igual en todos los nodos de la subred. Cada nodo recalcula continuamente la tabla de encaminamiento a partir de dicha información y de la que contiene en su propia base de datos. A este tipo pertenecen dos de los más utilizados en Internet que son los algoritmos por vector de distancias y los de estado de enlace.

**Adaptativo aislado**

Se caracterizan por la sencillez del método que utilizan para adaptarse al estado cambiante de la red. Su respuesta a los cambios de tráfico o de topología se obtiene a partir de la información propia y local de cada nodo.

Un caso típico es el encaminamiento “por inundación” cuyo mecanismo consiste en reenviar cada paquete recibido con destino a otros nodos, por todos los enlaces excepto por el que llegó.

**Datagrama**

Un datagrama es un fragmento de paquete que es enviado con la suficiente información como

para que la red pueda simplemente encaminar el fragmento hacia el Equipo Terminal de Datos

(ETD) receptor, de manera independiente a los fragmentos restantes. Esto no garantiza que los

paquetes lleguen en el orden adecuado o que todos lleguen a destino.

Los datagramas IP son las unidades principales de información de Internet. Los términos trama, mensaje, paquete de red y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

La estructura de un datagrama es cabecera y datos.

Un datagrama tiene una cabecera de IP que contiene información de direcciones de la capa 3. Los

encaminadores examinan la dirección de destino de la cabecera de IP, para dirigir los datagramas

al destino.

**Trama**

En redes una trama es una unidad de envío de datos. Viene a ser el equivalente de paquete de

datos o Paquete de red.

Para delimitar una trama se pueden emplear cuatro métodos

1. **Por conteo de caracteres**:

Al principio de la trama se pone el número de bytes que la componen, este método presenta un posible problema de sincronización.

1. **Por caracteres de principio y fin**:

En comunicaciones orientadas a caracteres se puede emplear un código de control para representar el principio y fin de las tramas. Habitualmente se emplean STX para empezar y ETX para terminar. Si se quieren transmitir datos arbitrarios se recurre a secuencias de escape para distinguir los datos de los caracteres de control.

1. **Por secuencias de bits**:

En comunicaciones orientadas a bit, se puede emplear una secuencia de bits para indicar el principio y fin de una trama. Se suele emplear el "guión", 01111110, en transmisión siempre que aparezcan cinco unos seguidos se rellena con un cero; en recepción siempre que tras cinco unos aparezca un cero se elimina.

1. **Por violación del nivel físico**:

Se trata de introducir una señal, o nivel de señal, que no se corresponda ni con un uno ni con un cero.

**Paquete de redes**

Reciben este nombre cada uno de los bloques en que se divide, en el nivel de Red, la información

a enviar. En todo sistema de comunicaciones resulta interesante dividir la información a enviar en bloques de un tamaño máximo conocido. Esto simplifica el control de la comunicación, las

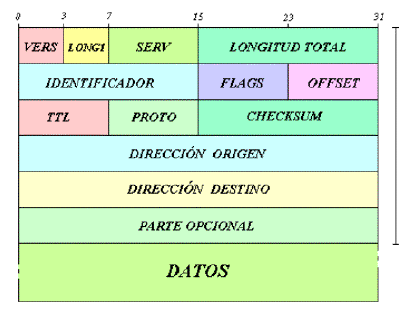
comprobaciones de errores, la gestión de los equipos de encaminamiento.

**Estructura**

Al igual que las tramas, los paquetes pueden estar formados por una cabecera, una parte de

datos y una cola.

**Datagrama IP**



**Versión:**

Los protocolos evolucionan y cambian con el tiempo. Por esto, es conveniente saber con qué versión se ha generado un datagrama.

**Longitud:**

Es la longitud de la cabecera medida en palabras de 32 bits. Puesto que este campo tiene 4 bits la longitud máxima de la cabecera es de 64 octetos.

**Servicio:**

Lo rellena quien envía el datagrama. Su utilidad actual es muy escasa, pero irá aumentando en la medida en que se empleen diferentes tipos de tráfico.

**Longitud total:**

Es la longitud total del mensaje en octetos incluida la cabecera. Por ser un campo de 16 bits permite una longitud de hasta 65535 octetos.

**Identificador:**

número de secuencia. Es el mismo para todos los datagramas generados al segmentar e igual al del datagrama original.

**Offset:**

Posición de los datos del datagrama segmentado en el original.

**Flags:**

El único que nos va a interesar es MF. Éste se pone a ´0´ si el datagrama es el último fragmento de una segmentación. En caso contrario estará a ´1´

**TTL: o *T*ime *T*o *L*ife.**

Limita el tiempo que un datagrama puede pasar en la red. TTL se decrementa en una unidad cada vez que pasa por un router si todo va bien, o en una unidad por segundo en el router si hay congestión. Al llegar a cero el datagrama es descartado.

**Checksum:**

Es el resultado de aplicar un código de protección de errores a la cabecera con los bits del campo

checksum puestos a cero.

**Opciones:**

En este campo se especifican algunas opciones de las que se puede hacer uso. Por ejemplo, una de ellas es la denominada registro de ruta. Si se emplea esta opción todos los Routers por los que pase el datagrama copiarían en su campo de opciones su dirección

**Ipv6**

El Internet Protocol version es una versión del protocoloInternet Protocol, diseñadapara reemplazar a Internet Protocol version 4, que actualmente está implementado en la granmayoría de dispositivos que acceden a Internet.el desarrollo e introducción de IPv6no estuvo exenta de controversia. El diseño fue duramentecriticado por la falta de interoperabilidad con IPv4 y otrosaspectos por ingeniero D. J. Bernstein

Se espera ampliamente que IPv6 sea soportado en conjunto con IPv4 en el futuro cercano. Los nodos solo-IPv4 no son capaces de comunicarse directamente con los nodos IPv6, y necesitarán ayuda de un intermediario.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes.

Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables.

Algunos de los cambios de IPv4 a IPv6 más relevantes

Son:

* Capacidad extendida de direccionamiento
* Autoconfiguración de direcciones libres de estado (SLAAC)
* Multicast
* Seguridad de Nivel de Red obligatoria
* Procesamiento simplificado en los routers
* Movilidad
* Soporte mejorado para las extensiones y opciones
* Jumbogramas

**Paquete IPv6**

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera y la carga útil (los datos).

**Carga útil**

La carga útil del paquete puede tener un tamaño de hasta 64 KB en modo estándar, o mayor con una opción de carga jumbo en el encabezado opcional Hop-By-Hop.

La fragmentación es manejada solamente en el host que envía la información en IPv6: los routers nunca fragmentan un paquete y los hosts se espera que utilicen el *Path* *MTU discovery*.

**El protocolo UDP**

UDP es un protocolo no orientado a conexión. Es decir, cuando una maquina A envía paquetes a

una maquina B, el flujo es unidireccional. La transferencia de datos es realizada sin haber

realizado previamente una conexión con la máquina de destino (maquina B), y el destinatario

recibirá los datos sin enviar una confirmación al emisor (la maquina A). Esto es debido a que la

encapsulación de datos enviada por el protocolo UDP no permite transmitir la información

relacionada al emisor. Por ello el destinatario no conocerá al emisor de los datos excepto su IP.

**El protocolo TCP**

Contrariamente a UDP, el protocolo TCP está orientado a conexión. Cuando una máquina A envía

datos a una máquina B, la máquina B es informada de la llegada de datos, y confirma su buena

recepción. Aquí interviene el control CRC de datos que se basa en una ecuación matemática que

permite verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son

corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que vuelvan a enviar

los datos corruptos.

**ARP**

En red de computadoras, el protocolo de resolución de direcciones es un protocolo de comunicaciones de la capa de enlace de datos, responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP.

Para ello se envía un paquete (ARP request) a la dirección de difusión de la que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina responda con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga.

ARP se utiliza en cuatro casos referentes a la comunicación entre dos hosts:

1. Cuando dos hosts están en la misma red y uno quiere enviar un paquete a otro.
2. Cuando dos hosts están sobre redes diferentes y deben usar un gateway o router para alcanzar otro host.
3. Cuando un router necesita enviar un paquete a un host a través de otro router.
4. Cuando un router necesita enviar un paquete a un host de la misma red.

**ARP Proxy**

La técnica ARP Proxy consiste en que un host, generalmente un router, responde a peticiones ARP destinadas a un host que se encuentra fuera de la red local.

**Generación del paquete ARP**

Si una aplicación desea enviar datos a una determinada dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un “router”) y el dispositivo hardware al que se debería enviar

**Estructura del paquete**

El ARP utiliza un formato de mensaje simple que contiene una solicitud de resolución de dirección o respuesta.

El tamaño del mensaje ARP depende de la capa superior y menor tamaño de dirección de capa, que se da por el tipo de protocolo de red

**Recepción del paquete ARP**

Cuando un host recibe un paquete ARP, el dispositivo receptor le pasa el paquete al módulo ARP.