

iloveCARLOS_merged (2).pdf



Nerdy



Interconexión de Redes



3º Grado en Ingeniería Informática



**Escuela Superior de Ingeniería
Universidad de Cádiz**

quieres trabajar
en Wuolah??

TE BUSCAMOS

TEMA 2

INTRODUCCIÓN

→ El protocolo IP realiza un servicio de entrega de datagramas no orientado a conexión.

→ Al proceso de selección del camino por el que se mandarán los datagramas se le llama enrutamiento.

→ Sus funciones principales son:

Selecciones de la mejor ruta

Reenvío de paquetes al destino

La entrega de datagramas puede ser:

→ Directa:

Datagrama se entrega en la misma red de origen

Se realiza cuando NETID de origen y destino son los mismos.

No requiere de routers

→ Indirecta:

NETID de origen y destino distintos.

Intervienen uno o más routers para pasar el datagrama por las redes.

Routers analizan el NETID de destino para determinar el siguiente router al que pasar el datagrama.

El datagrama va pasando de router a router hasta que se puede enviar de forma directa.

ENRUTAMIENTO ESTÁTICO

Una única ruta permanente se configura para cada par de redes de origen-destino:

→ Las rutas son fijas.

→ Sólo cambian cuando hay un cambio en la topología y se hace manualmente.

→ Los costes de enlace no pueden estar basados en datos dinámicos.

→ Pueden estar basados en volúmenes estimados de tráfico o en la capacidad de cada enlace.

Implementación de enrutamiento fijo en los routers:

→ Se necesita una tabla de encaminamiento por cada router.

→ La tabla contendrá una entrada por cada red de destino (de manera general):

No es necesario tener una entrada para cada destino.

El encaminamiento sólo necesita la IP de red.

→ Cada entrada muestra el siguiente nodo en la ruta:

No es necesario almacenar la ruta

Implementación de enrutamiento fijo en los host:

→ Todos los hosts también tienen tabla de enrutamiento

Si hay varios routers directamente conectados al host, la tabla del host indicará qué router utilizar en cada momento.

Si un host está unido a un solo router, entonces la tabla se configura automáticamente al llenar la "Puerta de Enlace". Así todo el tráfico que no sea de la red a la que pertenece el host se dirigirá hacia este router.

sin ánimo
de lucro,
chequea esto:



tú puedes
ayudarnos a
llevar
WUOLAH
al siguiente
nivel
(o alguien que
conozcas)

ENRUTAMIENTO DINÁMICO

- El objetivo de un protocolo de enrutamiento es el de obtener las mejores rutas hasta las redes remotas.
- Dichas rutas se almacenan en la tabla de enrutamiento.
- En el momento que hay un cambio en la red, los routers intercambian información para recalcularlas de nuevo.
- Se dice entonces que los routers de la red entran en proceso de convergencia.
- Una red ha convergido, en el momento de que todos los routers han creado de nuevo su tabla de enrutamiento.
- El tiempo de convergencia debe ser el min. posible. Éste depende:
 - Del algoritmo empleado en el protocolo
 - De los temporizadores característicos del protocolo
 - Del uso o no de la summarización de rutas.
- La summarización consiste en apiñar varias subredes en una sola con objeto de disminuir el tamaño de la tabla de rutas y por tanto, el tiempo de convergencia.
- La escalabilidad es la capacidad que tiene un protocolo en soportar redes que crecen.
 - Los factores que influyen en ella son: n.º de rutas, n.º de vecinos adyacentes, nº de routers de la red, diseño de red, frecuencia de los cambios, cantidad de recursos disponibles (CPU y memoria).
 - Se adapta a las condiciones de la red variando la ruta en función de dichas condiciones.
 - Las condiciones que influyen son:
 - Fallo de un router: excluyéndose de las rutas
 - Congestión: rodeando la zona congestionada
- Ventajas
 - El usuario de la red percibe que las prestaciones mejoran.
 - Puede ayudar en el control de la congestión.
- La consecución de estos beneficios dependen de la solidez del diseño y de la carga de las redes.
 - El enrutamiento dinámico es una tarea muy compleja que hace que haya una evolución continua de los protocolos.
- Desventajas:
 - Las decisiones de enrutamiento son complejas: aumenta el procesamiento en los routers.
 - Depende de la información obtenida en una parte, pero que es utilizada en otra.
 - Un intercambio mayor de información mejora las decisiones de encaminamiento, pero aumenta la carga.
 - Puede reaccionar demasiado rápidamente, provocando congestión y produciendo oscilaciones.
 - Puede reaccionar de forma demasiado lenta, resultando irrelevante.
- Patologías:
 - Agitación:
 - Oscilaciones rápidas en el enrutamiento.
 - Pueden ser causadas por intentos del encaminador de hacer reparto o equilibrado de cargas:
 - Problemas: Dificultad al estimar el tiempo de ida y vuelta, los paquetes TCP llegan fuera de orden.

saboteas a tu propia persona?
cómo?? escríbelo **aquí** y táchalo

manual de instrucciones: escribe sin filtros

y una vez acabes, táchalo (si lo compartes en redes mencionándonos, te llevas 10 coins por tu cara bonita)

DESFÓGATE CON WUOLAH

Formacion de Bucles: Aunque los algoritmos están diseñados para impedir la formación de bucles, se pueden producir cuando los cambios en la conectividad no se propagan inmediatamente a los demás routers.

→ Clasificación en función de la fuente de la cual obtienen información:

Local:

--Por ejemplo, encaminar cada datagrama a la red con la cola de menor longitud y así equilibrar las cargas en las redes.

--Son raramente utilizados.

Nodos adyacentes: Algoritmos de vector distancia y de vector camino.

Todos los nodos: Algoritmos de estado del enlace.

→ Clasificación en función de tener o no clase:

Protocolos de enrutamiento con clase (classful):

--NO envían la máscara de subred durante las actualizaciones de enrutamiento

Protocolos de enrutamiento sin clase (classless):

--Envían la máscara de subred durante las actualizaciones de enrutamiento

→ Clasificación en función del ámbito de trabajo del router:

IGP: protocolo común utilizado en todos los routers de dentro de un AS (sistema Autónomo).

EGP: establece rutas entre AS.

PROTOCOLOS:

→ IGP:

Protocolo de 1º el camino más corto disponible (OSPF): basado en algoritmos de Estado Enlace.

Protocolo de Información de Enrutamiento (RIP): basado en algoritmos de Vector Distancia

Protocolo de enrutamiento de Gateway interior (IGRP): basado en algoritmo de Vector Distancia

IGRP Mejorado (EIGRP): basado en algoritmos de Vector Distancia.

→ EGP:

Protocolo de pasarela (BGP): basado en algoritmos de Vector Camino

→ Elección del protocolo:

Tamaño de la red.

Soporte Multi-proveedor.

Curva de aprendizaje del protocolo.

Tipo de algoritmo del protocolo.

Velocidad de convergencia del algoritmo.

Escalabilidad.

→ AS=Conjunto de redes y routers controlados por una sola autoridad administrativa. Ej.: Red de la UCA

→ Dentro de él se utiliza un protocolo de enrutamiento común.

→ A éste tipo de protocolo que se utiliza dentro de un Sistema Autónomo se le llama Protocolo de Pasarela Interior o IGP (Interior Gateway Protocol)

- Es habitual que este Sistema Autónomo necesite transferir información a otros sistemas autónomos, para ello se usan un Protocolo de Pasarela Exterior o EGP (Exterior Gateway Protocol)
- Un EGP sólo necesita determinar la ruta para alcanzar el sistema autónomo objetivo, una vez alcanzado el IGP se encarga de entregar los paquetes a la máquina destinataria.
- Un EGP no tiene información de las rutas internas de un sistema autónomo, sólo de las rutas entre sistemas autónomos.

TABLAS DE RUTAS

- Los routers deciden por donde envían los paquetes en base a una tabla que poseen en memoria, y lo hacen de manera independiente a otros routers.
- Ésta relaciona las posibles redes de destino con el siguiente router por el que deben pasar los paquetes hasta llegar a dichas redes.
- También contiene el costo de uso de una ruta (métrica) para determinar si conviene utilizarla o no (el camino con menor coste es el mejor).
- A veces el costo no es más que el número de saltos para alcanzar una red, pero en otras ocasiones se tiene en cuenta otros parámetros (ancho de banda, carga, retraso, confiabilidad, etc...)
- Cada registro de la tabla apunta a un router alcanzable de manera directa.
- Los routers trabajan con las Direcciones de Red.
- Una tabla de enrutamiento debe contener la mínima información posible para no sobrecargar al router cuando la consulta.
- Una tabla de enrutamiento tiene información sobre cómo llegar a un destino, pero no sobre cómo regresar
- Información que puede contener una ruta de la tabla de enrutamiento:

Información de si la red está conectada directamente o indirectamente
La fuente de la información
Dirección de red
La máscara de subred
La dirección IP del router de siguiente salto

- En IPv6 se recomienda el uso de un prefijo de tamaño /64
- Un router puede tener en una interfaz varias direcciones unicast globales, pero sólo una de enlace local
- Distintas interfaces de un router pueden tener la misma dirección de enlace local

Las rutas pueden ser:

- Directamente conectadas (C): ruta estática que se añade automáticamente al levantar una interfaz.
- Locales (L): dirección de la propia interfaz.
- Estáticas (S): introducidas a mano por el administrador de la red.
- Dinámicas: son rutas que se actualizan automáticamente y que son generadas por los protocolos de enrutamiento.
- Por defecto u omisión: es una ruta estática por la que se enviarán los datagramas en caso de la red de destino no aparecer en ninguna otra ruta.

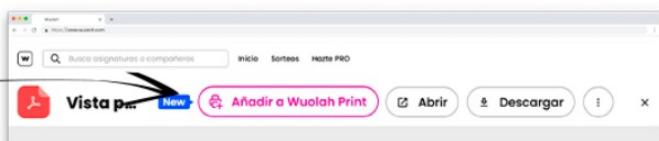
Métrica:

- Valor que se asigna a un enlace entre routers para que los protocolos de enrutamiento averigüen cual es la mejor ruta.
- Puede ser: Ancho de banda, Costo, Retraso, Conteo de saltos, Carga, Confidencialidad.

**ahora en Wuolah,
imprimimos apuntes a 0,02€**

**WUOLAH
print**

IMPRIME AQUÍ



Te lo llevamos
(casi siempre)
donde quieras



El mejor precio
por copia que
hay (en serio)



Lo imprimimos
sin nada de
publi, claro



Y siquieres
recógelo
cerquita



imprime

→ Cada protocolo de enrutamiento usa una Métrica en particular:

RIP: conteo de saltos

IGRP y EIGRP: ancho de banda (usado por defecto), retraso (usado por defecto), carga, confiabilidad

IS-IS y OSPF: costo, ancho de banda (implementación de Cisco)

→ Distancia Administrativa:

Valor numérico calculado en función del protocolo de enrutamiento utilizado, que se emplea para saber cual es la mejor ruta.

→ Balanceo de carga: Capacidad de un router de distribuir paquetes entre varias rutas de igual costo.

→ Estructura jerárquica de la tabla para acelerar los procesos de búsqueda:

Rutas de nivel 1:

Tienen una máscara de subred igual o menor que la máscara classful de la dir. de red:

--Pueden funcionar como: Ruta por defecto, Ruta de superred, Ruta de red

--El final de la ruta incluye: la dirección del siguiente salto o la interfaz de salida.

También son las rutas primarias (se producen cuando se agrega una subred a la tabla)

Rutas de Nivel 2:

Son las rutas secundarias o finales

Hacen referencia a las subredes

Contienen la dirección del siguiente salto o la interfaz de salida de la subred.

→ Búsqueda de la ruta:

Examinar las rutas de nivel 1: Si hay una coincidencia con una ruta final de nivel 1 y no es una ruta principal, esta ruta se utiliza para reenviar el paquete

El router examina las rutas de nivel 2 (secundarias):

Si hay una coincidencia con la ruta secundaria de nivel 2, esa subred se utiliza para reenviar el paquete.

Si no hay coincidencia, se determina el tipo de comportamiento de enrutamiento

El router determina si el comportamiento de enrutamiento es classful o classless

Si es classful, el paquete se descarta

Si es classless, el router busca la superred de nivel 1 y las rutas por defecto

--Si hay una coincidencia de superred de nivel 1 o de ruta por defecto, el paquete se reenvía. De lo contrario, se descarta el paquete.

El examen busca la ruta preferida: ruta que tiene la IP a la cual le coinciden más bits por la izquierda con la IP de destino del paquete.

→ En tablas IPv6 no existen jerarquías.

→ Cada ruta es independiente del resto.

TEMA 3: RIP

PROTOCOLO VECTOR DISTANCIA:

Introducción:

Clasificación de los protocolos de enrutamiento en función de la fuente de la cual obtienen información:

→Local: Por ejemplo, encaminar cada datagrama a la red con la cola de menor longitud y así equilibrar las cargas en las redes.

Son raramente utilizados.

→Nodos adyacentes: Algoritmos de vector distancia y de vector camino.

→Todos los nodos: Algoritmos de estado del enlace.

Funcionamiento:

→Un router que utiliza un algoritmo Vector distancia maneja la siguiente información de las posibles redes de destino:

Siguiente salto (interfaz o dirección IP)

Distancia (suma de los saltos hasta llegar a la red de destino)

→Las rutas se distribuyen como un vector de la distancia (métrica) y dirección (interfaz o IP del siguiente salto)

→El algoritmo utilizado es una versión distribuida del algoritmo de Bellman-Ford.

→El algoritmo intenta tener conocimiento de toda las redes. Al principio este conocimiento será muy escaso.

→Envía la información que posee de la red sólo a los vecinos con entrega directa.

→Es habitual que esto se haga periódicamente (aunque no siempre) con un periodo de tiempo preestablecido de antemano (p.ej. RIP 30s e IGRP 90s).

→Normalmente se asume un coste de una unidad por salto de router.

→Tras el inicio de un router, se rellena su tabla con las rutas de los vecinos directos.

→Se envían copias de las tablas de enrutamiento a los vecinos inmediatos.

→Cuando un router recibe una tabla de un vecino, examina los destinos y los costes y los compara con los de su propia tabla.

→La tabla se actualiza si aparece un nuevo destino o una distancia mejor para un destino existente

→La actualización supone el incremento de 1 al coste.

→Esto pasa en cada router de la red.

→La edad de la información de la tabla se actualiza con cada actualización.

Actualizaciones de la tabla:

→Periódicas: aunque los routers ya dispongan de la información completa de las redes, siguen enviando la tabla de enrutamiento a los vecinos (usadas en RIP)

→Limitadas: son no periódicas, parciales y destinada sólo a los routers que la necesitan (usadas en EIGRP)

→Activas (triggered update): enviada justo después de que se produzca un cambio de enrutamiento, es decir cuando:

--Cambia el estado de la interfaz

--La ruta pasa a ser inalcanzable

--Se agrega la ruta a la tabla de enrutamiento

--El uso únicamente de actualizaciones activas podrían ser suficientes si llegasen de inmediato a todas las redes, pero no es así.

--Se puede dar el caso de que un router envíe una actualización periódica (no puesta al día) a un vecino al que le ha llegado previamente una actualización activa, provocando una ruta erronea.

--Usada en RIP

Bucles:

→Causas de los Bucles:

- La configuración incorrecta de las rutas estáticas
- La configuración incorrecta de la redistribución de rutas
- La convergencia lenta
- La configuración incorrecta de las rutas de descarte

→Problemas:

- Uso excesivo del ancho de banda
- Mayor exigencia de recursos de la CPU
- Convergencia de la red degradada
- Es posible que se pierdan las actualizaciones de enrutamiento o que no se procesen oportunamente

→Soluciones:

→Prevención de conteo hasta infinito:

Se define una métrica máxima a alcanzar

Ésta depende de cada protocolos (p.ej. para RIP es 16)

Si se llega a tener este métrica en una ruta, se marca esta ruta como inalcanzable

→Prevención con temporizadores de espera hold-down: Cuando una red está caída se establece un periodo en el que sólo se podrá actualizar la ruta si su métrica es mejor

→Prevención mediante la implantación de la regla de horizonte dividido: Consiste en no publicar una red a través de la interfaz por la que llegó la actualización de la red

→Prevención por envenenamiento de ruta: Tras detectar una ruta inalcanzable, se debe anunciar que dicha ruta es inalcanzable (se anuncia la ruta con métrica a infinito)

→Prevención por horizonte dividido con envenenamiento a la inversa: Se publican las rutas inalcanzables a través de la interfaz por la que llegó la actualización de dicha red

→Prevención con campo tiempo de vida (TTL):

Un router reduce el tiempo de vida de cada datagrama que pasa por él

Cuando éste es 0 se descarta y se envía un mensaje ICMP al origen del datagrama

→Desventajas:

→Se transmite demasiada información en el intercambio de tablas (las tablas contienen información de toda la red y por tanto dicha información depende del tamaño de la red).

→Cuando cambia una ruta la información se propaga lentamente de un router a otro, por tanto un router lejano puede tener información de ruteo incorrecta.

RIP V1

Características:

- Protocolo vector-distancia con clase (no transmite la máscara de subred)
- Se toma como métrica el nº de saltos
- Las rutas inalcanzables tienen métrica superior a 15

→ Se definen 4 temporizadores en RIP:

--Actualización: cada 30s se envían mensajes de respuesta

--Invalid: si una ruta no se actualiza durante 180s se le pone métrica 16 quedando invalida

--Flush: tras 60s más (240s) se elimina ruta de tabla

--Hold-down: periodo de 180s que se establece cuando una red está caída para que sólo se pueda actualizar su ruta si llega una actualización con mejor métrica

→ La distancia administrativa es 120

→ Brinda soporte para las reglas de horizonte dividido y horizonte dividido con envenenamiento en reversa

→ Proporciona funcionalidades de balanceo de carga (balancea la carga de hasta 6 rutas de igual coste).

→ Es fácil de configurar

→ Está estandarizado en el RFC 1058, lo que permite que funcione en un entorno de routers de varios fabricantes

Mensajes:

→ Encapsulado en UDP Puerto 520.

→ Tipos:

--Solicitud: Envíado por Broadcast a los vecinos solicitando la tabla de enrutamiento.

--Respuesta: Envía la tabla de enrutamiento al solicitante.

RIP V2

Características:

→ Protocolo de enrutamiento vector-distancia sin clase (envía máscara de subred) que es una mejora respecto a v1

→ Se incluye la próxima dirección de salto en las actualizaciones

→ Las actualizaciones de enrutamiento se envían por medio de multicast a la IP 224.0.0.9

→ Utiliza UDP por puerto 521

→ Posibilidad de utilizar la autenticación como método de seguridad

→ Problemas RIP V1: (RIP V2 NO PRESENTA NINGUN PROBLEMA DE ESTOS)

No hay convergencia si se usan redes no contiguas

No se puede utilizar VLSM (No envía máscaras)

Resume redes en límites de red principales

No admite CIDR (no soporta superredes)

→ RIPV2 resumirá automáticamente las rutas en los límites de red principales y también puede resumir rutas con una máscara de subred más pequeña que la máscara de subred classful

Autenticación:

→ Posibilidad de autenticación:

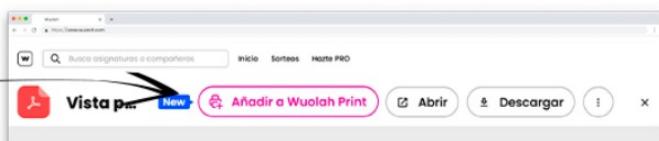
Previene la posibilidad de aceptar actualizaciones de enrutamiento no válidas.

Los contenidos de las actualizaciones de enrutamiento están encriptados.

ahora en Wuolah,
imprimimos apuntes a 0,02€

WUOLAH
print

IMPRIME AQUÍ



RIPng

Características:

- RIP de siguiente generación
- RFC 2080
- Es el protocolo RIP para compartir rutas en redes IPv6
- Similar al RIPv2 en IPv4
- Vector distancia, con un radio de 15 saltos
- Control de bucles similar al RIPv2
- Utiliza IPv6 para el transporte
- Utiliza el grupo multicast FF02::9, como dirección destino para las actualizaciones de RIP.
- Cuando un router RIPng recibe una actualización, incrementa la métrica antes de meterla en su tabla de enrutamiento.
 - Es por ello que la métrica de una ruta con red de destino un salto aparece en la tabla de rutas como 2.
 - En RIPv2 la métrica se incrementa después de almacenarse en la tabla de enrutamiento.

Autenticación:

- Al contrario que RIPv2, NO admite la posibilidad de autenticación.
- Se aprovechan las capacidades de IPv6 para autenticar.

Te lo llevamos
(casi siempre)
donde quieras



El mejor precio
por copia que
hay (en serio)



Lo imprimimos
sin nada de
publi, claro



Y siquieres
recógelo
cerquita



imprime

TEMA 4 .- EIGRP

GENERALIDADES

Características:

- Protocolo vector-distancia sin clase mejorado que fue una evolución de IGRP.
- Utiliza algoritmo DUAL (Diffusing Update Algorithm).
- Actualizaciones de ruta son limitadas (a quien la necesita).
- Las actualizaciones son parciales (solo envían los cambios).
- Las rutas no caducan.
- Solo los cambios provocan actualizaciones de enrutamiento.
- Establecimiento de adyacencias de vecinos.
- Balanceo de carga de mismo costo o con distinto costo.
- EIGRP puede trabajar sobre varios protocolos distintos de la Capa de Red (IPv4 ó 6, IPX y AppleTalk).
- Para cada protocolo utiliza un Módulo Dependiente de Protocolo (PDM) que se encarga de:
 - Mantener las tablas de vecinos y de topología de los routers para cada tipo de protocolos.
 - Construir y traducir paquetes específicos del protocolo para DUAL.
 - Conectar a DUAL con la tabla de routing específica del protocolo.
 - Calcular la métrica y pasar esa información a DUAL.
 - Implementar filtros y listas de acceso.
 - Redistribuir rutas hacia/descubiertas _por otros protocolos de routing
- Para cada protocolo mantiene tres tablas: Tabla de vecinos, de topología, Tabla de encaminamiento con las mejores rutas hacia un destino.
- Se utiliza el protocolo de transporte confiable (RTP) para transmitir y recibir paquetes EIGRP.
- EIGRP es independiente de IP, por ello no puede usar TCP ni UDP.
- Características de RTP:
 - Incluye el envío confiable (con ACK) y no confiable (sin ACK) de mensajes EIGRP.
 - Los paquetes se pueden enviar mediante Unicast o Multicast (por medio de la dirección 224.0.0.10 ó FF02::A).
- Distancia Administrativa: se define como la confiabilidad del origen de una ruta.
- Distancias administrativas por defecto de EIGRP:
 - Rutas sumarizadas = 5
 - Rutas internas = 90
- Autenticación: EIGRP permite autenticar la información de enrutamiento.

Paquetes:

- El paquete EIGRP se encapsula en un datagrama con:
 - Tipo de protocolo 88.
 - Dirección IP de destino puede ser:
 - *Unicast.
 - *Multicast, concretamente se emplea la IP 224.0.0.10.
 - Si se usa Multicast sobre Ethernet, la MAC de destino es 01-00-5E-00-00-0A.
- Cisco diferencia entre paquetes y mensajes:
 - El mensaje es la carga del paquete.
 - Al mensaje se le llama TLV.

→ Puede haber varias instancias de EIGRP (por eso nºAS).

→ El área de datos del paquete contiene al mensaje.

→ Al mensaje se le llama TLV (Tipo/Longitud/Valor).

→ 5 tipos de paquetes:

→ Paquetes de actualización:

-- Se usan para difundir la información de enrutamiento.

-- Sólo se envía cuando hay cambios.

-- Sólo se envía al router que la necesita.

-- Se utiliza entrega fiable.

-- Se usa unicast si sólo se destina a un router y multicast si se destina a varios.

→ Paquetes de ACK:

-- Se usan como acuse de la recepción de los paquetes de actualización, consulta y respuesta.

-- Utilizan Unicast no confiable.

→ Paquetes de consulta

-- Se usa para consultar rutas a vecinos.

-- Utilizan Unicast o Multicast y confiabilidad.

→ Paquetes de respuesta

-- Usan solamente Unicast para responder a consultas con confiabilidad.

→ Paquetes de saludo

-- Se usan para detectar vecinos y formar adyacencias con ellos.

-- Se envían periódicamente (intervalo de saludo).

-- Si no se reciben saludos del vecino durante el triple de tiempo del intervalo de saludo, se declara inalcanzable.

-- Entrega no confiable.

-- Son multicast.

Mensajes:

→ En EIGRP se considera mensaje al área de datos del paquete.

→ A estos mensajes se les llama TLV (Tipo-Longitud-Valor).

→ Existen 3 tipos principales:

-- TLV 1(tipo 0x0001): en él se establecen los multiplicadores que ponderan los parámetros con los que se calcula la métrica compuesta de EIGRP. (pesos K de parámetros de EIGRP)

-- TLV 2(tipo 0x0102): con él se anuncian rutas internas del sistema autónomo.(Para rutas internas del AS)

-- TLV 3(tipo 0x0103): con él se anuncian rutas externas al sistema autónomo.(Para rutas externas al AS)

Funcionamiento Inicial:

→ Paso 1º: Adyacencia con los vecinos (construcción de tabla de vecinos)

→ Paso 2º: Construcción de la tabla de topología

→ Paso 3º: Se alcanza la convergencia EIGRP (construcción de tabla de rutas)

METRICA EIGRP

Parametros:

→ La métrica está compuesta por los siguientes parámetros:

--Ancho de banda (BW): menor valor de ancho de banda entre el router local y el destino. Se mide en Kbit/sec.

--Retraso (DLY): suma de todos los retardos entre origen y destino. Se mide en microsegundos (usec).

→ Opcionalmente también se pueden utilizar los siguientes:

--Fiabilidad (Reliability): mínima fiabilidad entre origen y destino. El calculo se basa en mensajes keepalive. Se expresa como fracción de 255 donde 255/255 supone total fiabilidad. Se calcula como un promedio exponencial durante 5 minutos.

--Carga (Txload y Rxload): mayor caso de carga entre origen y destino. El calculo se basa en la tasa de paquetes y el ancho de banda. Se expresa como una fracción de 255 donde 255/255 supone que la línea está totalmente saturada. Se calcula como un promedio exponencial durante 5 minutos.

→ La MTU no forma parte de la métrica, sólo se usa para descartar rutas de igual costo.

→ Todos los routers del dominio de enrutamiento deben usar los mismos parámetros.

→ A veces, en interfaces serie, el ancho de banda real no coincide con el predeterminado y por ello se debe configurar éste manualmente en la interfaz

→ El retraso (DLY) es un valor estático que depende del tipo de enlace.

Metrica Ancha

→ Para interfaces de mas de 10Gbps se usa:

--Cálculos de 64 bits.

--RIB (Routing Information Base) scaling.

--La velocidad real de la línea (throughput) en vez del ancho de banda.

--Un nuevo parámetro de "Atributos Extendidos".

→ Se emplea cuando las interfaces tienen desde 1 gigabits hasta 4.2 terabits.

ALGORITMO DUAL

Conceptos:

→ DUAL: ALgoritmo de Actualización por Difusión.

→ Proporciona:

--Las mejores rutas a las redes de destino.

--Rutas de respaldo sin bucles que permiten modificar la tabla de rutas sin recalcular tras un cambio de la topología y por tanto una convergencia rápida.

--Uso de poco WB: ya que emplea actualizaciones limitadas.

→ Sucesor: router vecino en el que se inicia la ruta menos costosa hasta una red de destino.

→ Distancia Factible (FD): es la métrica más baja calculada para acceder a una red de destino

→ Sucesor factible (FS): router vecino de acceso por una ruta de respaldo. Se visualizan en la tabla de topología.

quieres trabajar
en Wuolah??

TE BUSCAMOS

sin ánimo
de lucro,
chequea esto:



tú puedes
ayudarnos a
llevar
WUOLAH
al siguiente
nivel
(o alguien que
conozcas)

→ Distancia notificada (RD, Reported Distance) o Distancia publicada (AD, Advertised Distance):

-- es la métrica que un router informa a un vecino acerca de su costo para alcanzar una red.

-- es la distancia factible desde el vecino hasta red destino.

→ Condición de factibilidad (FC): se da cuando la distancia factible (FD) es menor que la distancia notificada (RD):

-- El hecho de que la distancia desde un vecino a un destino (RD) sea menor que la propia distancia (FS), garantiza al router que la ruta anunciada por el vecino no pasa por él.

-- Cuando una ruta cumple la condición se añade a la tabla de topología.

-- Las rutas que no cumplen la condición de factibilidad, es decir que se alcanzan por routers que no son factibles, también se pueden ver en la tabla de topología con el comando all-links.

→ Códigos de la tabla de topología:

P – Passive.

A – Active.

U – Update.

Q – Query.

R – Reply.

r - Reply status.

→ Contiene la lógica para calcular y comparar rutas

→ El caso de que falle la ruta a través del sucesor, se pondrá en marcha la ruta a través del sucesor factible.

→ El proceso se puede observar en detalle con: debug eigrp fsm.

→ En el caso de que no existiese el sucesor factible, el router pasa a estado Activo (A), de manera que se enviaría un Query y se recibiría un Reply con el nuevo sucesor factible.

OPTIMIZACIÓN

Querys:

→ EIGRP se basa en los vecinos para obtener la información de enrutamiento.

→ Si un router pierde una ruta y no existe sucesor factible se pone en modo activo para comenzar la búsqueda una ruta al destino.

→ El router comienza a enviar paquetes Query a los vecinos excepto al sucesor previo (horizonte dividido).

-- Si el vecino tiene una ruta alternativa, éste responde.

-- Si no la tiene, envía el Query a sus propios vecinos, propagándose el Query por la red.

→ Cuando un router contesta a un Query, éste para el envío de Querys en su rama de la red.

→ Cada Query es correspondido con un Reply con independencia de que se encuentre una mejor ruta o no.

→ Se genera un tráfico importante de Querys que a su vez es incrementado por los Replys.

→ Existen dos soluciones principales para optimizar el proceso de propagación de consulta y para limitar la cantidad de carga EIGRP innecesaria en los enlaces:

-- La summarización de rutas.

-- Los routers Stub.

Routers Stub:

→ Son routers que envían información limitada a los vecinos.

→ Además, los routers no stub no envían Querys a los routers Stubs.

→ Con ello se consigue no sobrecargar el procesador del router, un menor uso de ancho de banda y una mejor convergencia.

→ Un router configurado como Stub comparte información de las rutas directamente conectadas y de las sumarizadas.

→ Esta situación se puede cambiar pudiéndose dar las siguientes opciones:

Receive-only: no anuncia nada.

Connected: anuncia rutas directamente conectadas

Static: anuncia rutas estáticas.

Summary: anuncia rutas sumarizadas.

Redistributed: anuncia rutas redistribuidas desde otros protocolos.

→ La 1^a opción no es compatible con las otras, las cuales pueden ir combinadas.

Stuck in Active:

→ El estado “atrapado en activo” (SIA) se produce cuando no se recibe un Reply de un Query en 3 min. (valor por defecto del “active timer”):

→ Este estado puede ocasionar tiempos largos de convergencia e inestabilidad en la red ya que el router “de aguas arriba” (R2) quedará a la espera de la información de la ruta esperada.

→ Esta situación se resuelve con dos nuevos paquetes: Query SIA y Reply SIA.

CONFIGURACION A SABER EN TEORIA:

→ EIGRP necesita identificar a cada router dentro del Sistema Autonómico para la distribución de rutas.

→ Se recomienda usar la IP de una interfaz que preferentemente sea de loopback.

→ Si no existe IP de loopback se identifica con la IP mayor de las interfaces físicas.

→ Existe la posibilidad que se den bucles cuando se dan estas dos condiciones:

---La sumarización automática está activada.

---Se han aprendido subredes con las actualizaciones.

→ Para evitar estos bucles EIGRP hace uso de la interfaz Null0

→ Por defecto, EIGRP puede emplear hasta el 50% del ancho de banda para uso propio.

→ Por defecto se puede hacer balanceo de carga entre 4 routers si todos tienen el mismo costo hasta el destino.

→ EIGRP Nombrado es una nueva forma de configurar los routers Cisco.

Homogeneiza la configuración de EIGRP en doble pila (IPv4 e IPv6).

Hace que dicha configuración se haga de manera similar.

La configuración se organiza de una manera jerárquica.

Difiere mucho de la manera clásica.

Son compatibles, de manera que un router puede ir con una configuración clásica y otro router con una nombrada.

Disponible a partir del Cisco IOS Release 15.0(1)M.

→ VRF (Virtual Routing and Forwarding):

Es una técnica usada para crear varios routers virtuales en uno sólo físico.

Se emplea en:

Los ISPs, para aislar el tráfico de varios clientes.

Las redes empresariales, para separar distintos tipos de tráfico (p.ej. datos y voz).

Con address-family también se pueden configurar aspectos generales como el id. de router, las networks o los routers stub.

TEMA 5.- OSPF

PROTOCOLOS DE ESTADO DE ENLACE

→ Clasificación de los protocolos de enrutamiento en función de la fuente de la cual obtienen información:

→ Local: Por ejemplo, encaminar cada datagrama a la red con la cola de menor longitud y así equilibrar las cargas en las redes. Son raramente utilizados.

→ Nodos adyacentes: Algoritmos de vector distancia y de vector camino.

→ Todos los nodos: Algoritmos de estado del enlace.

→ Clasificación en función del ámbito de trabajo del router: IGP – EGP

Funcionamiento:

→ Se creó como una alternativa al algoritmo de Vector-Distancia intentando paliar sus desventajas.

→ También llamados Primero la Ruta Más Corta (SPF: Shortest Path First)

→ El algoritmo intenta tener conocimiento de la topología de la red.

→ El algoritmo obtiene el estado de sus vecinos (estado del enlace) enviándoles mensajes cortos de los que espera respuesta.

→ Difunde a todos los routers de la red la información que posee de sus vecinos (Inundación).

→ Dicha información se envía cuando hay cambios.

→ El estado de nuestros enlaces se adquiere de interfaces.

→ Los vecinos se conocen intercambiando paquetes de saludos.

→ INUNDACIÓN:

-- Consiste en el envío del LSP (paquete del estado del enlace) por todos los puertos del router.

-- Los LSP se envían cuando:

* Se inicia el router o proceso de enrutamiento

* Cuando hay un cambio en la topología

-- Éste llega a todos los routers vecinos del área de enrutamiento

-- Estos routers obtienen de él la información y lo retransmiten sin modificación por todos sus puertos llegando también a sus vecinos.

-- Así sucesivamente, consiguiendo que la información llegue a todos los routers de la red.

-- Estos paquetes son de tamaño pequeño porque sólo tienen información de los enlaces de un solo router, lo cual supone una ventaja.

→ ALMACENAMIENTO EN LA BD

-- Cuando un router recibe un LSP coloca la información en una BD llamada Base de Datos de Estados de Enlaces.

-- En ella se almacena el estado de los enlaces de cada router de la red.

-- Como todos los routers reciben los mismos LSP, todos tendrán la misma información en la Base de Datos.

→ CREACION DE LA TABLA

-- Cada vez que cambia el estado de un enlace en la base de datos el router aplica el algoritmo de "primero la ruta más corta" (Dijkstra) para obtener la tabla de enrutamiento.

→ VENTAJAS:

-- Construye el mapa topológico

-- El router determina de forma independiente la ruta más corta

-- Convergencia rápida

-- Actualizaciones periódicas: generalmente no.

-- Uso de LSP.

→DESVENTAJAS:

- *Requisitos para el uso de un protocolo de enrutamiento de estado de enlace:
 - Requisitos de memoria mayores que protocolos por vector distancia
 - Requisitos de procesamiento mayores
 - Requisitos de ancho de banda mayores sobre todo al inicio
 - Ello supone que las máquinas que lo implementan son más caras.

OSPF

Areas:

- OSPF permite establecer jerarquía en el ruteo mediante la división del AS en áreas.
- Las áreas hacen que OSPF sea más eficiente y escalable.
- Se utiliza una jerarquía de 2 capas (área troncal y áreas comunes)
- En redes pequeñas sólo se usa un área (área 0, troncal, de tránsito o backbone)
- En redes grandes un sólo área produce problemas, por eso se utiliza multiárea
- Se utiliza una jerarquía de 2 capas.
- Ventajas de OSPF multiárea:
 - Tablas de rutas más pequeñas: se crean menos entradas en las tablas, ya que las direcciones de red pueden resumirse entre áreas. La summarización de ruta no está habilitada de manera predeterminada.
 - Menor sobrecarga de actualizaciones de estado de enlace: minimiza los requisitos de procesamiento y memoria.
 - Menor frecuencia de cálculos de SPF: la probabilidad de cambio de topología del área es menor al haber menos routers dentro de un área.
- 4 tipos dependiendo de la función que realicen:
 - Internos: con todas las interfaces den la misma área.
 - Router de área perimetral (ABR): con interfaces en varias áreas. Mantienen la BD de estado de enlace de dichas áreas.
 - Router límite del sistema autónomo (ASBR): con al menos una interfaz conectada a una red de fuera del AS que incluso puede no ser OSPF.
 - Router de respaldo

Routers:

- Cisco recomienda tener en cuenta las siguientes pautas:
 - Un área no debe tener más de 50 routers.
 - Un router no debe estar en más de tres áreas.
 - Ningún router debe tener más de 60 vecinos.

Redes:

- OSPF define cinco tipos de redes:
 - Punto a punto
 - Accesos múltiples con broadcast
 - Accesos múltiples sin broadcast (NBMA)
 - Punto a multipunto
 - Enlaces virtuales
- Los enlaces virtuales son usados para conectar áreas 0 discontinuas, Y también para conectar un área a la 0

quieres trabajar
en Wuolah??

TE BUSCAMOS

Mensaje OSPF:

- El objetivo del traspaso de mensajes OSPF es el de intercambio de paquetes de estados de enlace.
- En OSPF a estos paquetes se les llama LSA (Anuncios de Estado de enLace).
- Hay varios tipos de mensajes OSPF.
- En algunos tipos se transportan la cabecera LSAs y en otros el LSA entero.
- Campos de cabecera OSPF:
 - Versión.
 - Tipo: 5 tipos
 - Saludo (hello): descubre a los vecinos.
 - Descripción de BD (DBD): sincroniza la BD entre routers.
 - Solicitud estado de enlace (LSR): solicita registros específicos de LS entre routers.
 - Longitud del paquete.
 - Actualización de LS (LSU): envía los registros específicos de LS entre routers.
 - Acuse de recibos de LS (LSAck).
 - Id. de router (32bits): normalmente una IPv4.
 - Identificador de área: n.º del área.
 - Suma de verificación.
 - Tipo de Autentificación: ninguna, con contraseña, MD5
 - Autentificación (64bits)

Mensaje OSPF: HELLO

- Se utiliza para detectar vecinos.
- Se envían periódicamente
- Periodos:
 - Intervalo de saludo: periodo de reenvío del mensaje de saludo
 - *--En redes multiacceso con broadcast y punto a punto: normalmente 10s
 - *--En redes multiacceso sin broadcast: normalmente 30s
 - Intervalo muerto: tiempo sin recibir saludo tras el cual se declara al vecino desactivado (es 4 veces el intervalo de saludo)

Mensaje OSPF: DBD

- Mensaje DataBase Description (Tipo 2): Se utiliza para intercambiar la BD de LSAs
- MTU de interfaz
- Opciones
- Banderas:
 - I (Init): bit de inicio. Puesto a 1 cuando el paquete es el primero de la secuencia.
 - M (More): indica que siguen más paquetes DBD.
 - S (master/Slave): bit maestro/esclavo. Puesto a 1 cuando el "router" es el maestro o a 0 cuando es el esclavo.
- N° secuencia BD: usado para secuenciar la serie de paquetes DBD.
- Cabeceras LSA (se ve más adelante)

Mensajes OSPF: LSR

- Los LSR (Link State Request) tienen tipo 3
- Un router lo utiliza para enviar un mensaje hacia un vecino con objeto de solicitarle información actualizada sobre un conjunto de enlaces

sin ánimo
de lucro,
chequea esto:



tú puedes
ayudarnos a
llevar
WUOLAH
al siguiente
nivel
(o alguien que
conozcas)

Mensaje OSPF: LSU

- Los LSU (Link State Update) tienen tipo 4
 - Un router lo utiliza para difundir información de sus enlaces conectados directamente
- Un LSU contiene LSAs completos.

Mensaje OSPF: LSAck

- Los LSAck (Link State Acknowledgment) tienen tipo 5
 - Un router los utiliza como acuse de recibo de los DBDs y LSUs recibidos.
 - Un LSAck contiene las cabeceras de los LSAs recibidos en los DBSs y LSUs recibidos

Estados:

- Down: No se ha recibido Hello en el enlace.
- Init: se ha detectado un Hello de vecino, pero no hay aún comunicación bidireccional.
- 2-Way: Hay comunicación bidireccional con vecino.
- ExStart: Los enrutadores están tratando de establecer el número de secuencia inicial que se va a utilizar en paquetes de intercambio de BD.
- Exchange: Los enrutadores se intercambian BD mediante paquetes DBD.
- Loading: los routers están finalizando el intercambio de información.
- Completo: la adyacencia está completa.

Funcionamiento:

- La secuencia básica de operaciones realizadas por los router OSPF es:
 - Descubrir vecinos OSPF mediante intercambio de mensajes Hello,
 - Elegir el Router Designado (RD).
 - Formar adyacencias intercambiando la base de datos mediante mensajes DBD.
 - Sincronizar la bases de datos con los mensajes LSR y LSU.
 - Calcular la tabla de encaminamiento mediante el algoritmo SPF (primero el camino más corto).

Establecer Router Designado:

- Para reducir tráfico en redes de accesos múltiples con broadcast (p.ej. Ethernet) se establece:
 - Router Designado (DR): responsable de actualizar a los demás router
 - Router Designado de Respaldo (BDR): que empezará a actualizar a los demás cuando falla el anterior.
 - Estos router se establecen en base al campo Prioridad del Router y en caso de empate, en base al campo Identificador del Router.

Adyacencias:

- Al proceso de formar adyacencias se le conoce como "Intercambio de la BD"
- Despues de que se ha descubierto un vecino, asegurado la comunicación bidireccional, y (en una red multiacceso) elegido un DR, se toma la decisión de si se debería formar una adyacencia con uno de sus vecinos:
 - En redes multiacceso, todos los "routers" se hacen adyacentes al DR y al BDR.
 - En enlaces punto a punto y virtuales, cada "router" forma siempre una adyacencia con el "router" del otro extremo.
- Las adyacencias se establecen usando mensajes DBD (DataBase Description) cuyo tipo es 2.
- Contienen un resumen de la base de datos de estados de enlaces del emisor.

→ Se pueden usar múltiples mensajes para describir la base de datos: con este fin se emplea un procedimiento de sondeo-respuesta:

-- El "router" con mayor ID se convertirá en maestro, el otro en esclavo.

-- Los paquetes DBD enviados por el maestro (sondeos o polls) serán reconocidos por los DBDs del esclavo (respuestas).

-- El paquete contiene números de secuencia para asegurar la correspondencia entre sondeos y respuestas.

Actualizando la BD:

→ Después de terminar el intercambio de la BD cada router debe actualizarla

→ Para ello se intercambian LSAs.

→ El intercambio se hace por medio de una solicitud a la que se le responde con una actualización de estados de enlaces.

→ Los routers designados reenvían las LSA mediante la dirección multicast 224.0.0.5 a todos los otros routers

→ Los routers designados de otras áreas envían LSA mediante la dirección multicast 224.0.0.6 al DR y el BDR de nuestra área

→ La solicitud se hace con paquetes LSR

→ La respuesta a un LSR es un LSU que contiene algunos o todos los LSAs solicitados.

→ Si no se recibe respuesta, se repite la solicitud.

LSAs

→ LSAs (Anuncios de Estado de Enlace) se pueden encontrar en los LSUs.

→ Las cabeceras de los LSA se pueden encontrar en los DBD y LSack.

→ Cada LSA tiene su encabezado y cuerpo

→ Encabezado:

-- LS Age: (16 bits): segundos transcurridos desde el origen del anuncio.

* -- Cuando alcanza su valor máximo, deja de ser usado para determinar las tablas de encaminamiento.

* -- También se emplea para determinar cuál de dos copias idénticas de un anuncio debería usar un "router".

-- Opciones

-- Tipo de enlace: tipo de LSA. Hay hasta 11, siendo los 5 primeros los más importantes (se ven más adelante).

-- ID de LS: Un ID único para el anuncio que depende de su tipo.

* -- Para los tipos 1 y 4 es el ID del router

* -- Para los 3 y 5 es la dirección IP de red

* -- Para el tipo 2 es la dirección IP del router designado

-- Advertising Router: El ID del router que originó el anuncio.

* -- Para el tipo 1, este campo es idéntico al LSID

* -- Para el 2, es el ID del router designado

* -- Para 3 y 4 es el ID de un router del borde del área

* -- Para el 5, es el ID de un router del borde del AS

-- Nº de Secuencia del Enlace: Usado para permitir la detección de anuncios viejos o duplicados.

-- Suma de Verificación: de todo el anuncio menos el campo Link Age.

-- Longitud

→ El Cuerpo puede ser de muchos tipos: Los más utilizados son los 5 primeros: Router LSAs, Network-LSAs, Summary-LSAs, AS-external-LSAs

Tipos de Áreas:

→Área Estándar:

- Área que se conecta a la backbone ó 0.
- Todos los routers del área conocen a los demás routers del área.
- Todos tiene la misma BD topológica.

→Área de Backbone o Área 0:

- Interconecta todas las demás áreas.
- No puede propagar LSA de tipo 7, estos son traducidos previamente a LSA de tipo 5 por el ABR.

→Área Stub:

- No acepta LSAs de tipo 5.
- Se utiliza ruta por defecto para salir del área.
- Útil en routers con pocos recursos para no ser sobrecargados con muchas rutas.

→Área Totally Stub:

- No acepta LSAs de tipo 3, 4 y 5.
- Se utiliza ruta por defecto para salir del área.
- Minimiza tabla de enrutamiento y evita que en ella haya rutas OSPF de otras áreas.
- Solución propietaria de Cisco.

→Área NSSA (Not-So-Stubby Area):

- Área Stub (no permite LSA tipo 5) que puede tener un ASBR.
- El router ASBR pueden recibir rutas externas (de otros protocolos), pero no puede propagarlas hacia el área de backbone ni, por tanto al resto del dominio OSPF como LSA tipo 5.
- Dicho router crea LSA tipo 7 con estas rutas.
- Los LSA tipo 7 se transforman a LSA tipo 5 en el ABR del NSSA, de esta forma se puede propagar al resto del dominio OSPF.

→Área Totally NSSA (Not-So-Totally Stubby Area):

- Área Totally Stub (no permite LSA tipo 3, 4 ó 5) que puede tener un ASBR .
- El router ASBR pueden recibir rutas externas pero no puede lanzarla como LSA tipo 5.
- Dicho router crea LSA tipo 7 con estas rutas.
- Los LSA tipo 7 se transforman a LSA tipo 5 en el ABR de forma que se puedan propagar al resto del dominio OSPF.
- Al no permitir LSA tipo 3 y 4 nunca tendrá rutas OSPF de otras áreas.

quieres trabajar
en Wuolah??

TE BUSCAMOS

TEMA 6.- CORTAFUEGOS

DEFINICIONES:

- Cortafuegos Sistema que hace cumplir una política de control de acceso entre dos redes.
Objetivo: proteger a una red de servicios y protocolos del exterior que puedan suponer una amenaza a la seguridad
- Host Bastión o Gates: Sistema que es el punto de contacto entre las dos redes, la red interna a proteger y la externa.
Objetivo: Filtrar tráfico de E/S. Esconder detalles de configuración de red interna hacia fuera.
- Filtrado de Paquetes o Screening (cribado): Acción de denegar o permitir el flujo de tramas entre dos redes en base a unas reglas.
- Choke: Dispositivo que filtra paquetes.
- Proxy: Software de la capa de aplicación que realiza la función de representar a un cliente cuando accede a un servicio por algunos de los siguientes motivos:
 - permitir o negar el acceso al servicio por seguridad o/y obtener mayor rendimiento.
 - proporcionar anonimato.
 - proporcionar servicio de caché.

FUNCIONES:

- Un cortafuego puede realizar algunas de las siguientes funciones:
 - Máquina Bastión: soportando todas las inclemencias.
 - Choke: filtrando paquetes tras análisis de las cabeceras.
 - Proxy: tomando decisiones denegación/acceso a servicios basadas en datos de aplicación.
 - Monitorización y detección de actividad sospechosa.

DESVENTAJA DE LOS CORTAFUEGOS:

- Centralizan las medidas de seguridad, de manera que si dicha seguridad se ve comprometida toda la red queda vulnerable.
- Dan falsa sensación de seguridad, pensando que la red está segura por completo.
- No protege contra ataques que no pasan por él.
- Actitudes para paliar desventajas: Utilizarlos junto a otros dispositivos de seguridad. No bajar la guardia.

COMPONENTES

Filtrado de paquetes:

- Proporciona un nivel básico de seguridad.
- Consiste en un análisis de las cabeceras de las tramas o de la interfaz de entrada/salida del paquete para determinar si cumplen unas reglas preestablecidas, en función de ello se descartarán o no los paquetes.
- Las reglas se suelen aplicar por orden de aparición.
- A las reglas se les suele llamar ACLs

Proxy de aplicación:

- Complementa al anterior proporcionando un nivel más alto de seguridad.
- Se puede utilizar para limitar los servicios que corren en una red.
- Pueden filtrar protocolos de capa de aplicación (p.ej web no deseadas).
- Ocultan la red protegida.
- Facilitan la autenticación y auditoría del tráfico.
- Simplifican reglas de filtrado.
- Se utiliza un proxy por cada tipo de protocolo (desventaja)

sin ánimo
de lucro,
chequea esto:



tú puedes
ayudarnos a
llevar
WUOLAH
al siguiente
nivel
(o alguien que
conozcas)

Monitorización de la actividad:

→ Actividad fundamental para que el administrador de red este informado de lo que está pasando.

→ El administrador debe leer los registros con frecuencia y debe tomar medidas ante actividades sospechosas.

ARQUITECTURA:

Existen varios tipos de arquitecturas de cortafuegos:

→ Cortafuego de Filtrado de Paquetes

-- Es el cortafuegos más sencillo, está basado en un simple choke.

-- Suele estar implementado en los routers (screening routers).

-- Un router por defecto filtra paquetes (TTL=1, Broadcast, CRC erróneo), se aprovecha esta funcionalidad para establecer políticas de seguridad.

-- Se utilizan las ACLs (Listas de Control de Acceso) para hacer un enrutado selectivo.

-- Arquitectura simple, utilizada cuando no se exigen altos niveles de seguridad y para complementar a otras.

-- Sistema de monitorización simple y distribuido por los routers.

→ Arquitectura Dual-Homed Host

-- Ordenador con dos o más tarjetas de red.

-- Llamado Anfitrion de Dos Bases (Dual-Homed Host) o Multibases (Multi-homed Host).

-- Choke y Bastión coinciden en mismo equipo.

-- Cada tarjeta de red se conecta a una red distinta.

-- En el ordenador deben ejecutarse servidores proxies.

→ Arquitectura Screened Host o Choke-Gate:

-- Unión de las dos anteriores: Router: usado como choke + Ordenador: que contiene proxy, usado como host bastión.

-- 2 posibilidades de arquitectura:

** Router frente a red externa y detrás host bastión (arquitectura mayoritaria).

** Host bastión frente a red externa y detrás router.

→ Arquitectura DMZ (Desmilitarized Zone) o Screened Subnet

-- Consiste en colocar una nueva red entre la red interna y externa (red perimétrica).

-- El Host Bastión se encuentra situado en dicha red: En el caso de que se vea comprometido sólo se tendrá acceso a la red perimétrica y no a la red interna.

-- Es ampliamente utilizada.

→ Arquitectura DMZ (II)

-- Su arquitectura es más compleja.

-- Se utilizan: 2 routers: El interno: que interconecta la red interior con la perimétrica. El externo: que interconecta la red perimétrica con la exterior.

-- El host bastión.

-- Otros elementos visibles desde el exterior, p.ej: servidor web o de correo.

→ Arquitectura DMZ (III)

-- Es más segura: para alcanzar la red interna se deben comprometer los dos routers y el host bastión.

-- Se podría implementar con un solo router con tres interfaces, pero si éste se compromete se tiene acceso a toda la red.

-- Para mayor seguridad se podrían crear varias redes perimétricas en serie, separadas por routers, y cada una con un nivel de seguridad mayor conforme se acercan a la red interna.

CASOS DE USO: ACLs EN ROUTERS CISCO

Introducción:

- Un router Cisco puede proporcionar funciones básicas de filtrado de tráfico mediante el uso de ACLs.
- ACL = lista secuencial de sentencias de permiso o denegación que se aplican a direcciones, protocolos o interfaces.
- Una ACL se puede considerar como un script de configuración del router que controla si el router permite o deniega el paso de cada paquete.

Formas de trabajo:

- ACLs Entrantes: los paquetes se procesan antes del enrutamiento.
- ACLs Salientes: los paquetes se procesan justo antes de llegar a la interfaz de salida, después de haber sido enrutados

Funcionamiento:

- Los paquetes se comprueban en el orden en el que las ACLs fueron introducidas (se debe ser cuidadoso con el orden)
- Si hay coincidencia con alguna de las sentencias de la ACL, el paquete se permite o deniega (según se exprese en la sentencia) y no se comprueban el resto de ACLs.
- Si no hay coincidencia se descarta el paquete.
- Una ACL se puede aplicar a varias interfaces.
- Cada protocolo, dirección o interfaz sólo pueden tener una ACL.

Tipos:

- ACL Estándar: filtran los paquetes basándose en la dirección de origen.
- ACL Extendida: filtran los paquetes basándose en:
 - Direcciones IPs de origen y destino.
 - Puertos de origen y destino.
 - Diversos aspectos de los protocolos (tipo, número,...)

Referencias:

- ACLs Numeradas:
 - Las estándar se enumeran con algún número del intervalo [1,99] ó [1300,1999]
 - Las extendidas usan un número perteneciente a [100,199] ó [2000,2699]
- ACLs con Nombre:
 - Los nombres se escriben normalmente en mayúsculas.
 - Comienzan con una letra y no llevan espacios ni signos de puntuación.

Normas de Colocación:

- Extendidas: se colocan lo más cerca posible del origen.
- Estándar: se colocan lo más cerca del destino posible.

Restricción de Acceso por Telnet:

- Las ACLs permiten definir desde qué IP se tendrá acceso al Telnet.

CASOS DE USO: IPTABLES

Introducción:

- Linux tiene la capacidad de aceptar paquetes de redes IP distintas a la propia para hacer funciones de router.
- Un ejemplo de su uso son los routers con firmware openWRT o DD-WRT.

→ Posteriormente habría que crear las rutas estáticas (con comando route) o poner en marcha un protocolo de enrutamiento.

→ Además es recomendable usar IPTTables, que es una herramienta de linux utilizada para:

- el filtrado de paquetes en linux.

- hacer NAT.

- modificar, clasificar y marcar datagramas.

→ Está integrado en el núcleo de Linux.

→ Es un producto desarrollado por el proyecto Netfilter (<http://www.netfilter.org/>)

Tablas:

→ IPTables trabaja con Tablas. Existen varias tablas:

- filter: usada para filtrar paquetes.

- nat: permite realizar traducción de direcciones, pudiendo traducir tanto origen como destino.

- mangle: diseñada para manipular paquetes.

- raw: Esta tabla permite marcar paquetes que no serán controlados con estado de conexión.

Cadenas:

→ Las Tablas contienen Cadenas (Chains).

- IPTables funciona haciendo pasar los paquetes por las Cadenas.

- Una cadena contiene un conjunto de Reglas que se utilizan para verificar si los paquetes se ajustan a ellas.

- El concepto de cadena es similar al de ACL de Cisco.

Cadenas .- Cadenas de la Tabla Filter

→ Filter se utiliza para filtrar paquetes

→ Filter dispone de tres Cadenas de Filtrado: INPUT, OUTPUT y FORWARD. Estas cadenas no se pueden borrar.

→ Cuando un paquete entra por una tarjeta de red se compara su IP de destino con la de la propia máquina:

- Si coincide pasa a la cadena INPUT

- Si no coincide:

- ** Si está habilitado el enrutamiento pasa FORWARD.

- ** Si no está habilitado el paquete es descartado.

→ Los paquetes originados por las aplicaciones de la propia máquina pasan a la cadena OUTPUT.

Reglas:

→ Las reglas están dentro de las cadenas.

→ Cada regla tiene asociada una acción.

→ Cuando un paquete entra en una cadena se verifica si se ajusta a las reglas de la cadena.

→ Si se ajusta a una regla entonces se ejecuta la acción sobre el paquete.

→ Ejemplo:

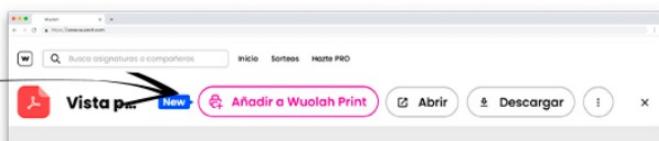
- Si la acción es DROP se descarta paquete.

- Si la acción es ACCEPT sigue su camino por el grafo de cadenas.

→ A estas acciones se les llama OBJETIVOS/SALTOS (Target/Jump).

ahora en Wuolah,
imprimimos apuntes a 0,02€

IMPRIME AQUÍ



Te lo llevamos
(casi siempre)
donde quieras



El mejor precio
por copia que
hay (en serio)



Lo imprimimos
sin nada de
publi, claro



Y si quieras
recógelo
cerquita



imprime

Tema 7

Redistribución de rutas

→ Concepto:

- Capacidad de un router de intercambiar información de las mejores rutas entre los distintos protocolos de enrutamiento que tenga implementado.
- Capacidad de los routers para intercambiar información entre dominios de enrutamiento. (**Dominio de enrutamiento**: cto. de routers que implementan un mismo protocolo de enrutamiento.)

→ Metrica

→ La métrica de los distintos protocolos se basa en distintos parámetros:

- RIP en el número de saltos.
- OSPF en el costo (que es función del WB).
- EIGRP utiliza por defecto una función del WB y del retardo.

Las métricas al estar basada en distintos parámetros hace que no exista manera de compararla entre los distintos protocolos.

Cuando redistribuimos la ruta de un protocolo a otro, no tenemos un punto de referencia para cuantificar la métrica del protocolo origen. Para estos casos se realizará una métrica de partida con un valor mayor a la del dominio de enrutamiento para evitar bucles de enrutamiento y enrutamiento no óptimo.

Cuando tenemos establecida la métrica de partida esta se incrementa de manera normal tras cada salto, a excepción de las rutas provenientes de OSPF E2 puesto que mantiene la métrica desde el borde del AS.

Si no indicamos **MANUALMENTE** la métrica de partida se usa una por defecto son las siguientes para cada protocolo:

- RIP: 0 (inalcanzable)
- EIGRP: 0 (inalcanzable) a excepción de las rutas directamente conectadas o estáticas o redistribuida entre dos AS con EIGRP
- OSPF: en rutas tipo E2 la métrica es 20 a excepto para BGP que será 1
- IS-IS: 0 (pero no tiene por qué ser inalcanzable).

→ Técnicas de Distribución:

Redistribución punto a punto:

- Unidireccional:
 - Redistribución de rutas se hace con un único router de un AS a otro.
 - El AS1 necesitará una ruta estática para conocer al AS2.
- Bidireccional:
 - La redistribución de rutas se hace con un único router en los dos sentidos

Redistribución multipunto:

- Unidireccional:
 - Varios routers frontera redistribuyen la ruta de un AS a otro.

- En el otro sentido se necesitará rutas por defecto o varias estáticas.
- Bidireccional:
 - También llamado redistribución mutua.
 - Varios routers frontera redistribuyen en los dos sentidos.

La redistribución multipunto bidireccional puede ocasionar problemas debido a métricas incompatibles o perdida de parte de la información de la métrica tras la redistribución. Producido los siguientes problemas:

- Enrutamiento no óptimo: ya que sólo parte del costo es considerado en las decisiones de enrutamiento.
- Bucles de enrutamiento, que pueden ocasionar perdidas de rutas.

Estos Bucles se pueden evitar usando la redistribución punto a punto unidireccional pero tiene la desventaja de dejar un único punto de fallo en la red.

En caso de múltiples routers y/o usar la redistribución bidireccional se aconseja:

- Sólo redistribuir rutas internas entre ASs.
- Uso en puntos de redistribución de etiquetas (tag) y filtros basados en estas etiquetas.
- Propagar bien las métricas.
- En lo posible usar rutas por defecto para evitar la redistribución bidireccional

Para verificar el funcionamiento de la redistribución se aconseja:

- Conocer adecuadamente la topología de red.
- Estudiar las tablas de enrutamiento en modo EXEC: **show ip route [ip-address]**
- Estudiar las tablas de topología para apreciar que todas las redes están siendo aprendidas.
- Verificar los caminos usando del comando: **traceroute [ip-address]**
- Además utilizar la depuración (**debug**) en caso de problemas.

LISTAS DE DISTRIBUCIÓN

Introducción

Se usan métodos basados en **mecanismos de filtrado**, nos incrementa las posibilidades de solucionar retos y problemas que surjan.

Estos métodos se usarán para llevar actualizaciones donde sean necesarias y filtrarlas donde no lo sean. Los métodos de filtrado serán los siguientes:

- **Listas de distribución con ACLs.**
- **Listas de distribución con prefix-list.**
- **Route maps:** son filtros complejos que además permiten realizar acciones sobre los paquetes.

→ Las ACLs permite a las redes que interesa anunciar y deniega las que interesa filtrar basándose en 3 factores:

- La interfaz de entrada
- La interfaz de salida
- Y la redistribución desde otro protocolo.

Las ACLs nos permiten no mostrar una visión general de la topología. Usar las en las listas de distribución encontramos los siguientes inconvenientes:

- Una máscara de subred no se puede combinar fácilmente.
- Las listas de acceso se evalúan de manera secuencial para cada prefijo IP de la actualización de enrutamiento.
- Las listas de acceso extendidas pueden ser complicadas de configurar.

→ Las **listas de prefijo** es un sistema específico para el filtrado de rutas mientras que las ACLs es para el filtrado de paquetes y se adapta al filtrado de rutas. Las Prefix-List nos proporciona las siguientes ventajas:

- Interfaz más amigable.
- Procesamiento más rápido: la implementación hace que consuma menos recursos.
- Se organizan por número de secuencia, luego las modificaciones son más sencillas.
- Son más flexibles

Las prefix-list contiene una condición y acción por línea (permit o deny). La IP/máscara de la actualización se compara con la condición de cada línea de la lista:

- Si se cumple la condición se realiza la acción
- Si no existe coincidencia, la acción por defecto es la denegación.

La condición está formada por:

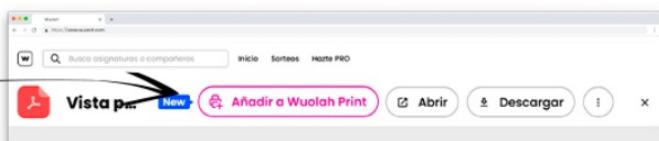
IP/prefixo [**ge valor**][**le valor**]

- Se hace una doble comprobación para garantizar la coincidencia:
 - Se compara la IP de la actualización con la de la condición.
 - Además:
 - En el caso de que existan los valores ge (\geq) y le (\leq), la máscara de la actualización debe ser \geq valor-ge y \leq valor-le.
 - En caso contrario la máscara de la actualización debe coincidir con el prefijo de la condición.

ahora en Wuolah,
imprimimos apuntes a 0,02€

WUOLAH
print

IMPRIME AQUÍ



Tema 8



Te lo llevamos
(casi siempre)
dondequieras



El mejor precio
por copia que
hay(en serio)



Lo imprimimos
sin nada de
publi, claro



Y siquieres
recógelos
cerquita



imprime

INTRODUCCIÓN

→ Los protocolos vector distancia (como RIP) ni de estado de enlace (como OSPF) no son efectivos para el enrutamiento exterior ya que todos los routers del AS comparten una métrica común. Las **prioridades y restricciones de acceso** pueden ser distintas entre los distintos AS.

→ Tenemos como alternativa el encaminamiento de vector camino. Prescinde de la métrica y nos proporciona la siguiente información:

- Qué redes pueden ser alcanzadas por un determinado encaminador.
- Qué AS deben cruzar para llegar al destino.

→ La diferencia entre vector camino y vector distancia es que en el vector camino no incluimos una estimación de distancia o coste. También contiene toda la información de todos los AS a visitar para alcanzar la red de destino. Esto nos permite decidir que AS queremos pasar y cuáles no.

→ Tipos de Protocolo:

- **BGP:** Border Gateway Protocol (Protocolo de pasarela frontera)
- **IDRP:** Inter-Domain Routing Protocol (Protocolo de enrutamiento inter-dominio)

→ BGP: este protocolo se usa en internet entre las distintas organizaciones. Trata de que las tablas de enrutamiento no se actualicen continuamente para no sobrecargar la red. Ya que sus tablas pueden contener miles de rutas.

- Podemos tener rutas SIN CLASES

BGP utiliza 4 tipos de mensajes: Open, Keepalive, Update y Notification.

- Se establece relación de vecindad con el envío de un mensaje **Open** al router par, que provoca la apertura de una conexión TCP por puerto 179.
- Las sesiones se mantienen enviando mensajes **periódicos Keepalive**.
- **Update** se utiliza para enviar la tabla de enrutamiento completa si es la primera vez y para enviar **actualizaciones incrementales** tras cambios de rutas a posteriori.
- Con **Notification** se rompe la relación de vecindad

→ Prevención de bucles: el mecanismo que usa BGP consiste en verificar que el propio nº de AS no está en la ruta.

• Mecanismo de prevención de bucle:

- Cuando una actualización sobre una red deja un AS, ese número de AS se antepone a la lista de ASs por los que ha pasado la actualización.
- Cuando un AS recibe una actualización, se examina la lista de ASs. Si encuentra su propio número en dicha lista, la actualización se descarta.

→ Usos del BGP:

- Cuando conectemos diferentes ASs (Multihomed).
- Cuando necesitemos manipular rutas externas al AS
- Cuando es un AS de transito

No lo utilizaremos cuando:

- Cuando solo tengamos un acceso único al resto de ASs (single-homed)
- Cuando un router no tiene los recursos para manejarlo
- Cuando el personal no tenga buena formación en la selección y manipulación de rutas BGP

→ Tablas BGP:

- BD de Vecinos:
 - Es específica de BGP
 - Mantiene una lista de todos los vecinos BGP configurados.
 - Para verla: show ip bgp summary.
- BD de BGP:
 - Es específica de BGP
 - Mantiene una lista de redes conocidas por BGP, junto con sus caminos y atributos.
 - Para verla: show ip bgp
- Tabla de enrutamiento:
 - Contiene las mejores rutas de la anterior.

FUNCIONAMIENTO

→ Procedimientos funcionales existen 3:

- 1) Adquisición de vecino.
- 2) Detección de vecino alcanzable.
- 3) Detección de red alcanzable.

1) Adquisición de vecinos

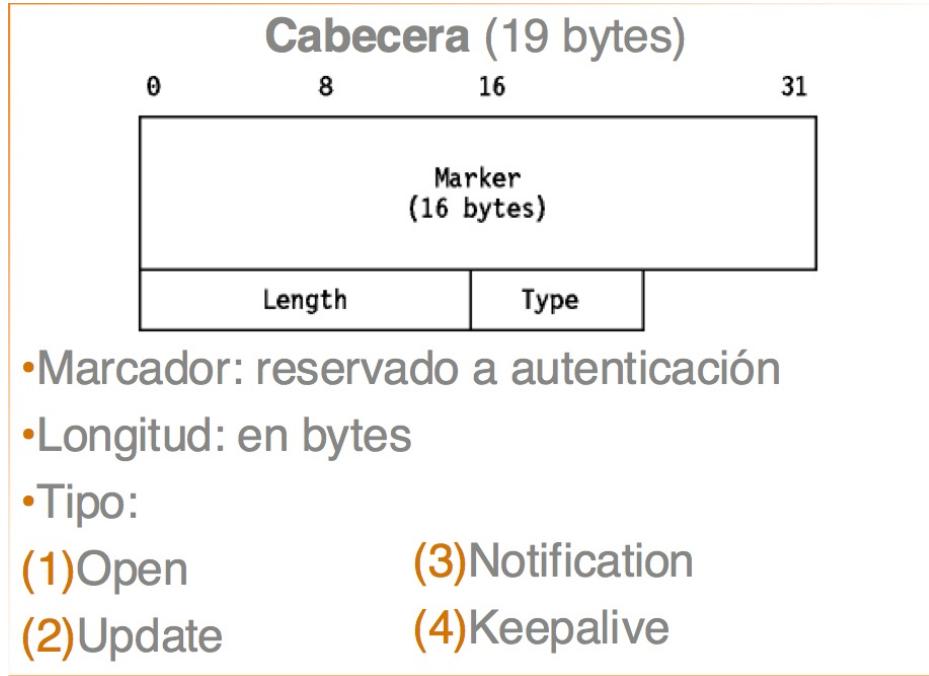
- Los vecinos están unidos a la misma subred.
- Si los routers están en diferentes AS, podrían desear intercambiar información.
- La adquisición de vecino tiene lugar cuando dos routers vecinos se ponen de acuerdo para intercambiar información de encaminamiento regularmente
- Se requiere un procedimiento formal de adquisición, ya que uno de los routers pueden no querer participar,
- **Procedimiento:** un router envía una petición y el otro le responde aceptando o no:
 - La petición se hace con un mensaje de tipo **Open**
 - La respuesta se hace con un tipo de mensaje llamado **Keepalive**
- BGP no se encarga de:
 - Del conocimiento de la existencia de otro encaminador ni de su dirección
 - Ni de como decidir si es necesario intercambiar información con un router concreto
- De ello se encarga el administrador de red bien en el momento de establecer la configuración o bien por una intervención activa.

2) Detección de vecinos alcanzable: Los routers que desean mantener la relación de vecindad se envían periódicamente mensajes **keepalive**.

3) Detección de red alcanzable

- Cada encaminador mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para alcanzarlas (BD BGP).
 - Cuando se realiza un cambio, el encaminador envía un mensaje **update**.
 - Todos los encaminadores BGP pueden acumular y mantener información de encaminamiento por medio de estos mensajes.

MENSAJES BGPv4



- Marcador: reservado a autenticación
 - Longitud: en bytes
 - Tipo:
 - (1) Open
 - (2) Update
 - (3) Notification
 - (4) Keepalive

→Tipos de Mensajes BGPv4

- **Open:** solicitud para establecer una relación de vecinos
 - **Keepalive (la vecindad se mantiene):** se usa en dos casos
 - Como acuse de recibo de un mensaje open
 - Como confirmación periódica de una relación
 - **Notification:** Se envía cuando se detecta una condición de error
 - **Update:**
 - Transmite información sobre una única ruta
 - Enumera las distintas rutas para retirarlas

→ Mensaje Open:

- Version (1B)
 - AS origen (2B): nº que ocupa.
 - Hold Time: tiempo máximo en segundos que puede transcurrir en la recepción de los sucesivos mensajes de Keeplive, notification y/o update
 - Identificador BGP: es un numero de 32 bits que identificar al router y puede ser la IP de cualquiera de sus interfaces
 - Longitud de parámetros opcionales
 - Parámetros opcionales: este campo lleva parámetros definidos como la autentificación

→ Keeplive

- Consta solamente de la cabecera.
- Cada encaminador emite estos mensajes bastante a menudo para prevenir que expire el temporizador de mantenimiento.

→ **Notification:**

- Se utiliza para la notificación de errores
- **Código de error:**
 - 1) Error en la cabecera del mensaje.
 - 2) Error en el mensaje Open.
 - 3) Error en el mensaje Update.
 - 4) Hold time expirado.
 - 5) Error en la máquina de estados finitos.
 - 6) Cese (cierra una conexión en ausencia de cualquier error).
- **Subcódigo de error:** da más detalle del código de error.
- **Datos:** información adicional de error

→ **Mensaje Update**

- Una lista de rutas previamente anunciadas por este encaminador que van a ser eliminadas.
- Información sobre rutas a través de un conjunto de redes:
 - Esta información se puede incorporar a la base de datos de cada encaminador que la recibe.
 - Implica al campo NLRI y el de los atributos del camino
- Longitud de rutas impracticables: longitud del campo siguiente (puede ser 0)
- Rutas apartadas: lista de redes IP que se están retirando del servicio.
 - Cada entrada tiene la forma "<longitud, prefijo>"
 - Longitud: es un sólo byte que indica el nº de unos de la máscara de subred. El valor cero causa coincidencia con todas las direcciones IP.
 - Prefijo: es la IP de subred.
- **Longitud total de atributos del camino:** longitud del campo siguiente.
- **Atributos del camino:** distintos atributos de una ruta. Formado por un conjunto de tripletas <tipo_atributo, longitud, valor>
 - Tipo de atributo:
 - Banderas (1 byte).
 - Código (1 byte).
 - Longitud
 - Valor: que depende del código
- **Información de alcanzabilidad del nivel de red (NLRI):** lista de IPs de las subredes alcanzables desde este router junto con sus máscaras en formato CIDR.

ATRIBUTOS

→ Campos: Formado por tripleta <tipo_atrib, long, valor>

quieres trabajar
en Wuolah??

TE BUSCAMOS

- El tipo de atributo se divide en 2 campos:
 - Banderas (1 byte).
 - Código (1 byte).

→ Banderas

- Bit 1º: define si el atributo es **opcional** (1) o **bien conocido** (0).
- Bit 2º: define si el atributo es **transitivo** (1) o **no transitivo** (0)
- Todos atributo bien conocido es transitivo.
- Bit 3º: define si la info. de un atr. opcional transitivo es **parcial** (1) o **completa** (0).
- Para atributos bien conocido o opcionales no transitivos la información siempre será completa.
- Bit 4º: define la **longitud** del atributo, que puede ser **de un byte** (0) o **de dos** (1).
- Un atributo **bien conocido** debe ser reconocido por todas las implementaciones de BGP.
- Un atributo **opcional** puede no ser reconocido por una implementación de BGP. Éste puede ser:
 - **Opcional transitivo**: se pasará a vecinos BGP sin tocar aunque no se reconozcan.
 - El atributo **opcional transitivo parcial** no se envía sólo con parte de la información.
 - **Opcional no transitivo**: que será eliminado por el router si no lo reconoce.

→ Categorías

- Además el atributo puede ser:
 - **Obligatorio**: debiendo aparecer en todas las actualizaciones BGP.
 - **Discrecional**: pudiendo no aparecer en una actualización BGP.
- De todo lo anterior se deduce que sólo son posibles las siguientes categorías de atributos:
 - Bien conocido obligatorio (well-known mandatory)
 - Bien conocido discrecional (well-known discretionary).
 - Opcional transitivo [parcial].
 - Opcional no transitivo.

→ Códigos

- (1) **ORIGIN**: toma valores [IGP|BGP|Incomplete] dependiendo del origen de la ruta.
- (2) **AS_PATH**: lista de ASs atravesados por una ruta.
- (3) **NEXT_HOP**: Dirección IP del encaminador frontera que se debe utilizar para el siguiente salto.
- (4) **MED** (Multi_Exit_Discriminator): Informa a vecinos del camino preferido dentro del propio AS.
- (5) **LOCAL_PREF**: Informa a otros routers dentro del propio AS de la ruta preferida para salir.
- (6) **ATOMIC_AGGREGATE**,
- (7) **AGREGATOR**: utilizados para summarización.

sin ánimo
de lucro,
chequea esto:



tú puedes
ayudarnos a
llevar
WUOLAH
al siguiente
nivel
(o alguien que
conozcas)

- (8) **COMMUNITY** (Cisco defined): etiqueta rutas para después hacer tratamientos con ellas.
- (9) **ORIGINATOR ID** (Cisco defined)

Operación BGP

→ Intercambio de información

- R1 implementa BGP, y además, como pertenece a AS1, construye una tabla de rutas internas de AS1 utilizando OSPF.
- R1 puede emitir un mensaje update a R5 (en AS2) que incluiría:
 - Camino_AS: identidad del AS1.
 - Siguiente_Salto: dirección IP de R1.
 - NLRI: lista de todas las redes en AS1.

(Con el mensaje se informa a R5 de que todas las redes incluidas en NLRI se alcanzan vía R1 y que sólo hay que atravesar AS1)
- Supongamos que R5 tiene una relación de vecindad con R9 en AS3.
- R5 envía la información (que acaba de recibir de R1) a R9 en un mensaje update.
 - Camino_AS: lista de identificadores {AS2,AS1}.
 - Siguiente_Salto: dirección IP de R5.
 - NLRI: todas las redes en AS1.
- Este mensaje informa a R9 de que:
 - Las redes del NLRI se alcanzan vía R5
 - Para ello hay que atravesar AS2 y AS1
- R9 debe decidir si ésta es su ruta preferida para acceder a las redes del NLRI
- R9 puede tener información alternativa preferida sobre alguna o todas las redes del NLRI basada en criterios como pueden ser rendimiento, métrica ...
- Si R9 se decide por las redes llegadas de R5 entonces:
 - incorpora la información a su tabla de enrutamiento
 - envía la información a los vecinos con el atributo Camino_AS modificado {AS3,AS2,AS1}.
- La información se propaga de esta manera por todos los ASs
- El campo **Camino_AS previene los bucles**: si se recibe un mensaje Update por un router de un AS incluido en Camino_AS, éste se desecha.

→ RELACIONES DE VECINDAD:

Existen 2 tipos de relaciones de vecindad BGP:

- Relaciones de vecindad externas (eBGP)
- Relaciones de vecindad internas (iBGP)
- Si un AS tiene varios routers fronteras, estos también intercambian información haciendo uso de BGP.
- En este caso no se incorpora el identificador del AS común en el campo AS_PATH.
- Si un router selecciona una ruta de destino externa como preferida, se la comunicará también a todos sus vecinos internos.

- Cada router decide si la nueva ruta pasa a ser preferida y en caso afirmativo la incorpora a su tabla y la difunde a los vecinos con mensajes update.
- En un AS, las relaciones de vecindad iBGP (conexiones TCP) se establecen en forma de malla completa.
- Hacerlo parcialmente puede ocasionar problemas pues no se garantiza que todos los routers tengan la misma tabla BGP,
- Esto es debido a que los routers iBGP sólo difunden actualizaciones eBGP y no pasan actualizaciones iBGP entre ellos.
- El uso de Routers Reflectores puede evitar la necesidad de la malla completa.
- Si hay disponibles varios routers frontera en un AS entonces un router de otro AS determina qué router de entrada elegir por medio del atributo MED (Multi_Exit_Discriminator)

→ESTADOS:

- **Idle:** en busca de ruta al vecino.
- **Connect:** en espera de establecer la conexión TCP.
- **Open Sent:** en espera de mensaje Open del vecino.
- **Active:** tras el envío de Open pasan 5 s sin recibir nada.
- **Open Confirm:** en espera de mensaje Keepalive o Notification.
- **Established:** conexión establecida entre pares BGP e intercambios de todo tipo de mensajes con éxito.

La capa Red del modelo TCP se equivale a la capa del modelo OSI:

- Enlace

Cual de los siguientes elementos NO es un elemento de monitorización de redes:

- Choke

¿Que se utiliza para filtrar paquetes?

- ACLs

¿Que LSAs mandan los routers internos?

- Tipo 1

En EIGRP ¿como se denomina el siguiente router para dar el salto?

- Sucesor

¿Que método utiliza la máscara de red para filtrar las rutas?

- Prefix List

¿Que utiliza OSPF para medir la métrica?

- El coste

¿Que hace la técnica de horizonte dividido con envenenamiento inverso?

- A medida que avanzan los paquetes se declaran como inalcanzables las rutas por las que ha venido.

Capacidad de un protocolo en soportar redes que crecen

- Escalabilidad

¿Que hace el mensaje de OSPF DBD?

- Describe la base de datos (En el examen era "Ninguna de las anteriores")

¿Que código BGP se usa para mostrar el camino que ha seguido un paquete?

- AS_PATH

Otra pregunta que no me acuerdo ni de la pregunta exacta ni de las respuestas, pero lo que hay que saber es que RTP no tiene na quever ni con IP ni con TCP ni con UDP.

Un router STUB comparte las rutas:

- Directamente conectadas y sumarizadas.

¿Que actualizaciones manda un router cuando se produce un cambio en la red?

- Activas

¿Que representa una ruta que viene configurada como O E1?

- Ruta OSPF Externa de tipo 1