Módulo 04
La Capa de Red (Pt. 4)

Redes de Computadoras
Depto. Cs. e Ing. de la Comp.
Universidad Nacional del Sur

Copyright

Contenidos

- Modelos de servicios de la capa de red
- Estructura interna de un router
- El protocolo **IP**
- **IPv4** vs. **IPv6**
- Protocolos de ruteo
- Ruteo jerárquico
- Ruteo en internet
- Multicast

Ruteo jerárquico

- El análisis de los algoritmos de ruteo hasta este punto es un tanto idealizado:
  - Todos los routers tienen las mismas capacidades
  - La red presenta una topología aplanada, esto es, todos los nodos están al mismo nivel
- Este modelo no sirve en el mundo real, donde existen cientos de millones de destinos
  - La tabla tendría un tamaño inconcebible
  - El intercambio de tablas saturaría la red

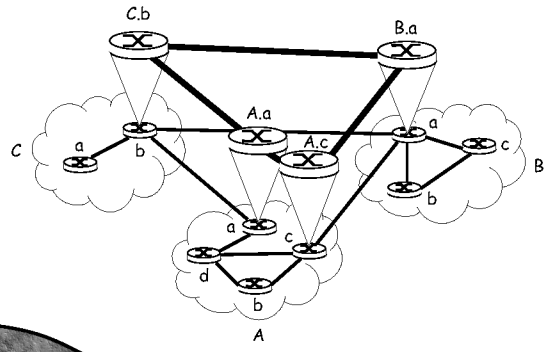
Ruteo jerárquico

- La solución adoptada consiste en implementar un esquema de ruteo jerárquico:
  - Los routers se agrupan por regiones en sistemas autónomos (**AS**)
  - Los routers de un cierto **AS** coordinan correr el mismo protocolo de ruteo (denominado intra-**AS**)
  - Los routers de distintos **AS** pueden haber optado por correr diferentes protocolos de ruteo

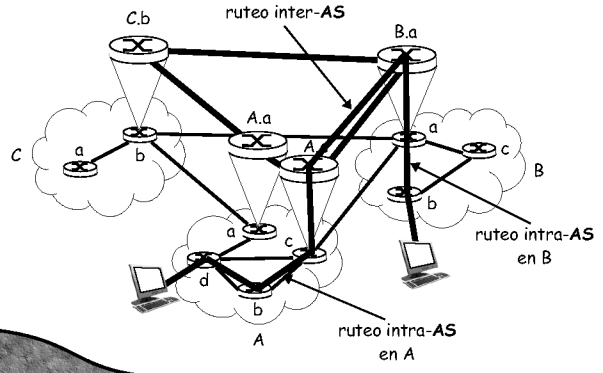
Routers gateway

- Dentro de cada **AS** se destacan uno o más routers especiales denominados gateway
  - Ese router corre el protocolo de ruteo intra-**AS** al igual que el resto
  - Por otra parte, es responsable de rutear hacia los destinos fuera del **AS** (en otras palabras, está conectado a otros **AS**)
  - Por esta razón, también corre el protocolo de ruteo inter-**AS** que se haya elegido para coordinar entre los restantes routers gateway de otros **AS**

Ruteo intra-AS e inter-AS



Ruteo intra-AS e inter-AS



Ruteo en internet

- La organización jerárquica de internet encaja a la perfección con la noción de ruteo jerárquico
- Internet se particiona en un conjunto de sistemas autónomos interconectados
- Esta partición permite hablar de ruteo en dos niveles:
  - Intra-**AS**: el administrador de la red es el responsable de elegir el algoritmo de ruteo
  - Inter-**AS**: se hace uso del protocolo **BGP**, el estándar universal prefijado para el ruteo inter-**AS**

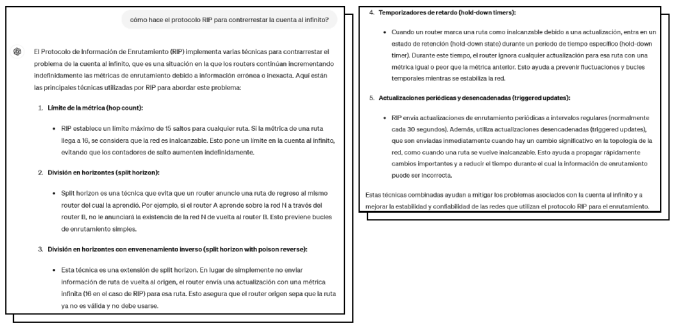
Ruteo intra-AS

- Los protocolos de ruteo intra-**AS** más utilizados son los siguientes:
  - **RIP** (Routing Information Protocol)
  - **OSPF** (Open Shortest Path First)
  - **IGRP** (Interior Gateway Routing Protocol)
- Los dos primeros son estándares abiertos; el tercero es propietario, de la compañía Cisco
- También se los conoce a estos protocolos como **IGP** (Interior Gateway Protocol)

Protocolo RIP

- Se define formalmente en el **RFC 2453**.
- Se basa en el algoritmo vector de distancia
- Utiliza como métrica la distancia en cantidad de saltos (también conocidos como “hops”)
  - El máximo contemplado es 15 saltos
- Los vecinos intercambian sus vectores de distancias cada 30 segundos haciendo uso de mensajes de difusión (Response Message)
- Cada mensaje publicita hasta 25 destinos

¡Parece un algoritmo anytime!



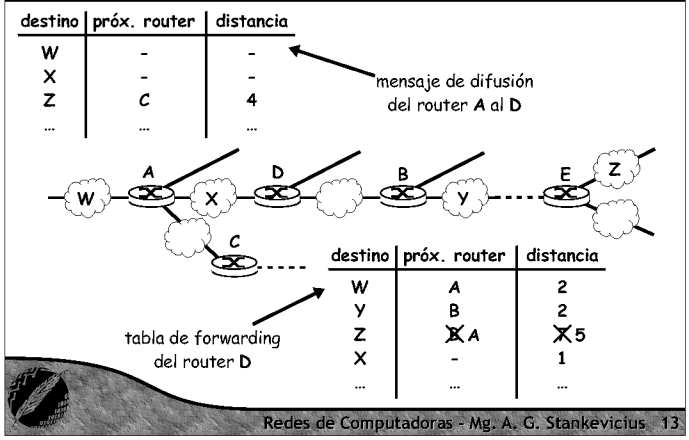
cómo hace el protocolo RIP para contrarrestar la cuenta al infinito?

El Protocolo de Información de Enrutamiento (RIP) implementa varias técnicas para contrarrestar el problema de la cuenta al infinito, que es una situación en la que los routers continúan incrementando indefinidamente las métricas de enrutamiento debido a información errónea o inexacta. Aquí están las principales técnicas utilizadas por RIP para abordar este problema:

1. **Límite de la métrica (hop count):**
   - RIP establece un límite máximo de 15 saltos para cualquier ruta. Si la métrica de una ruta llega a 16, se considera que la red es inalcanzable. Esto pone un límite en la cuenta al infinito, evitando que los contadores de salto aumenten indefinidamente.
2. **División en horizontes (split horizon):**
   - Split horizon es una técnica que evita que un router anuncie una ruta de regreso al mismo router del cual la aprendió. Por ejemplo, si el router A aprende sobre la red N a través del router B, no le anunciará la existencia de la red N de vuelta al router B. Esto previene bucles de enrutamiento simples.
3. **División en horizontes con envenenamiento inverso (split horizon with poison reverse):**
   - Esta técnica es una extensión de split horizon. En lugar de simplemente no enviar información de ruta de vuelta al origen, el router envía una actualización con una métrica infinita (16 en el caso de RIP) para esa ruta. Esto asegura que el router origen sepa que la ruta ya no es válida y no debe usarse.
4. **Temporizadores de retardo (hold-down timers):**
   - Cuando un router marca una ruta como inalcanzable debido a una actualización, entra en un estado de retención (hold-down state) durante un período de tiempo específico (hold-down time). Durante este tiempo, el router ignora cualquier actualización para esa ruta con una métrica igual o peor que la métrica anterior. Esto ayuda a prevenir fluctuaciones y bucles temporales mientras se estabiliza la red.
5. **Actualizaciones periódicas y desencadenadas (triggered updates):**
   - RIP envía actualizaciones de enrutamiento periódicas a intervalos regulares (normalmente cada 30 segundos). Además, utiliza actualizaciones desencadenadas (triggered updates), que son enviadas inmediatamente cuando hay un cambio significativo en la topología de la red, como cuando una ruta se vuelve inalcanzable. Esto ayuda a propagar rápidamente cambios importantes y a reducir el tiempo durante el cual la información de enrutamiento puede ser incorrecta.

Estas técnicas combinadas ayudan a mitigar los problemas asociados con la cuenta al infinito y a mejorar la estabilidad y confiabilidad de las redes que utilizan el protocolo RIP para el enrutamiento.

RIP en acción

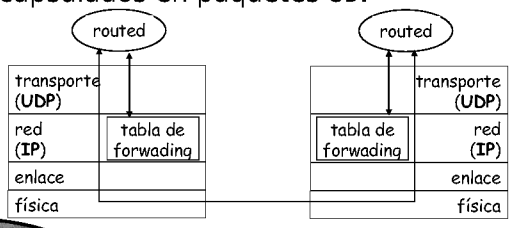


Fallos y recuperación

- Pasados 180 segundos sin recibir un mensaje de difusión de un dado vecino, se asume que el enlace y/o el vecino están muertos
  - Se invalidan todas las rutas que pasan por ese vecino
  - Se comunica la novedad a los restantes vecinos
  - Los vecinos a su vez envían nuevas actualizaciones (en caso de que sus tablas cambien)
  - La noticia de la falla del enlace se propaga rápidamente al resto de la red
  - Se usa la técnica vista para evitar la cuenta al infinito

Mensajes de difusión

- Las tablas de ruteo **RIP** son mantenidas y por un proceso alojado en la capa de aplicaciones
- Los mensajes de difusión se distribuyen encapsulados en paquetes **UDP**



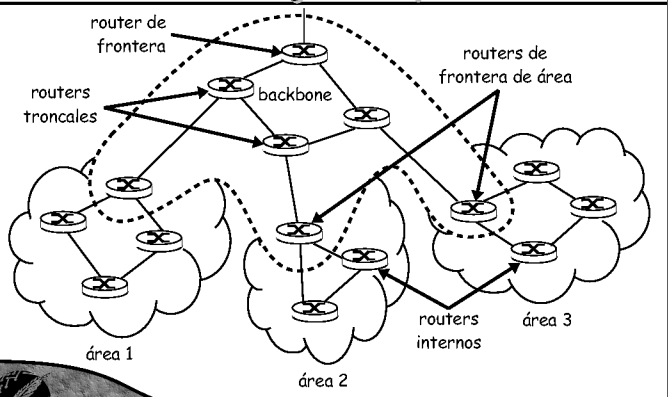
Protocolo OSPF

- Se trata un estándar abierto al igual que **RIP**
  - Se define formalmente en el **RFC 2328**
- Hace uso del algoritmo estado de los enlaces
  - El administrador determina el costo de cada enlace
  - Las rutas se resuelven con el algoritmo de Dijkstra
  - Cada router comunica por inundación a sus pares el costo de los enlaces que lo unen a sus vecinos inmediatos usando un mensaje **OSPF**
  - Los mensajes **OSPF** se encapsulan directamente dentro de un datagrama **IP**

Protocolo OSPF

- **OSPF** disfruta de algunas características avanzadas no presentes en **RIP**:
  - Cuenta con un mejor esquema de seguridad, pues los mensajes **OSPF** están autenticados
  - Se pueden configurar múltiples enlaces entre un mismo par de nodos (algo no permitido bajo **RIP**)
  - Soporta unicast y multicast de forma nativa
  - Posibilita registrar múltiples métricas en paralelo
  - En grandes organizaciones se puede hacer uso de un esquema **OSPF** jerárquico

OSPF jerárquico



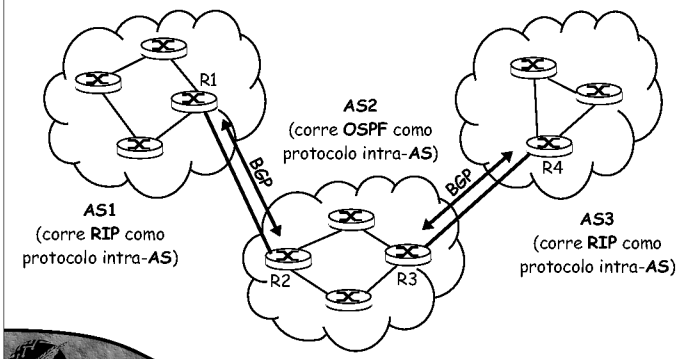
OSPF jerárquico

- En grandes organizaciones, **OSPF** permite adoptar una jerarquía de dos niveles:
  - Un conjunto de áreas locales
  - Un troncal (backbone)
- Los mensajes publicitando el costo de los enlaces sólo se distribuyen en el área local
  - Cada nodo tiene información detallada de la topología del área local
  - También cuenta con información de cuál es el camino más corto hacia las distintas redes en otras áreas

OSPF jerárquico

- En base a la ubicación y el rol de cada uno de los routers **OSPF**, se distinguen principalmente cuatro categorías:
  - Router interno: sólo enruta tráfico dentro de su propia área
  - Router de frontera de área: recopila las distancias a las redes en su propia área y las publicita con los otros routers de frontera de área
  - Router troncal: corre el algoritmo de ruteo **OSPF**, pero con un alcance limitado al backbone
  - Router de frontera: se conecta con otros **AS**

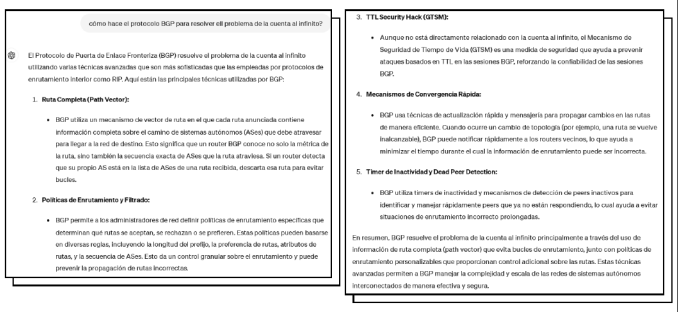
Protocolo BGP



Protocolo BGP

- El protocolo **BGP** (Border Gateway Protocol) es el estándar de facto adoptado como algoritmo de ruteo inter-**AS**
  - Se define formalmente en el **RFC 4271**
- Se basa en el algoritmo vector de caminos
  - Análogo al algoritmo vector de distancias
  - Cada router gateway informa a sus vecinos el camino completo a cada destino
- **BGP** sólo se preocupa de rutear a redes (**AS**), no a computadoras individuales

Rendido a los pies de la IA...



cómo hace el protocolo BGP para resolver ell problema de la cuenta al infinito?

El Protocolo de Puerta de Enlace Fronteriza (BGP) resuelve el problema de la cuenta al infinito utilizando varias técnicas avanzadas que son más sofisticadas que las empleadas por protocolos de enrutamiento interior como RIP. Aquí están las principales técnicas utilizadas por BGP:

1. **Ruta Completa (Path Vector):**
   - BGP utiliza un mecanismo de vector de ruta en el que cada ruta anunciada contiene información completa sobre el camino de sistemas autónomos (ASes) que debe atravesar para llegar a la red de destino. Esto significa que un router BGP conoce no solo la métrica de la ruta, sino también la secuencia exacta de ASes que la ruta atraviesa. Si un router detecta que su propio AS está en la lista de ASes de una ruta recibida, descarta esa ruta para evitar bucles.
2. **Políticas de Enrutamiento y Filtrado:**
   - BGP permite a los administradores de red definir políticas de enrutamiento específicas que determinan qué rutas se aceptan, se rechazan o se prefieren. Estas políticas pueden basarse en diversas reglas, incluyendo la longitud del prefijo, la preferencia de rutas, atributos de rutas, y la secuencia de ASes. Esto da un control granular sobre el enrutamiento y puede prevenir la propagación de rutas incorrectas.
3. **TTL Security Hack (GTSM):**
   - Aunque no está directamente relacionado con la cuenta al infinito, el Mecanismo de Seguridad de Tiempo de Vida (GTSM) es una medida de seguridad que ayuda a prevenir ataques basados en TTL en las sesiones BGP, reforzando la confiabilidad de las sesiones BGP.
4. **Mecanismos de Convergencia Rápida:**
   - BGP usa técnicas de actualización rápida y mensajería para propagar cambios en las rutas de manera eficiente. Cuando ocurre un cambio de topología (por ejemplo, una ruta se vuelve inalcanzable), BGP puede notificar rápidamente a los routers vecinos, lo que ayuda a minimizar el tiempo durante el cual la información de enrutamiento puede ser incorrecta.
5. **Timer de Inactividad y Dead Peer Detection:**
   - BGP utiliza timers de inactividad y mecanismos de detección de peers inactivos para identificar y manejar rápidamente peers que ya no están respondiendo, lo cual ayuda a evitar situaciones de enrutamiento incorrecto prolongadas.

En resumen, BGP resuelve el problema de la cuenta al infinito principalmente a través del uso de información de ruta completa (path vector) que evita bucles de enrutamiento, junto con políticas de enrutamiento personalizables que proporcionan control adicional sobre las rutas. Estas técnicas avanzadas permiten a BGP manejar la complejidad y escala de las redes de sistemas autónomos interconectados de manera efectiva y segura.

Rol del protocolo BGP

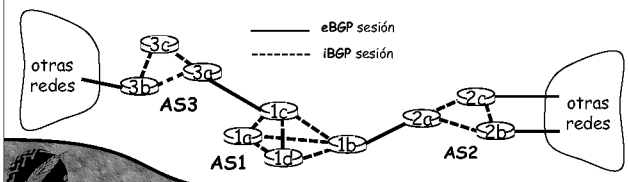
- El protocolo **BGP** desempeña un papel central en todo **AS**:
  - A través de las sesiones **eBGP** permite obtener información de la accesibilidad mediante los **AS** circundantes
  - Luego, esa información es propagada a todos los routers del **AS** mediante las sesiones **iBGP**
  - Esta información permite determinar las rutas óptimas a cada subred
  - En cierta forma, **BGP** permite que las distintas subredes digan fuerte y claro “aquí estoy”

Sesiones BGP

- Denominaremos sesión **BGP** al intercambio de información entre pares a través del protocolo
  - Los routers intercambian información acerca de la accesibilidad provista a distintos destinos
  - Esta información es intercambiada a través de conexiones **TCP** semi-permanentes
  - Cuando un dado router publicita una determinada ruta en esencia está comprometiéndose a encauzar tráfico hacia ese destino
  - Es conveniente hacer uso del agregado de rutas

Sesiones BGP

- Usando una sesión **eBGP** entre **3a** y **1c**, **AS3** envía los prefijos que puede alcanzar a **AS1**
  - **1c** luego usa sesiones **iBGP** para distribuir estos prefijos al resto del **AS**
  - **1b** puede seguir propagando esta información a **AS2** usando la sesión **eBGP** entre **1b** y **2a**



Atributos de rutas

- En la jerga **BGP**, una ruta se compone del prefijo de red más un conjunto de atributos:
  - **AS-PATH**: este atributo recopila la secuencia de **AS** que el prefijo publicitado ha atravesado
  - **NEXT-HOP**: este atributo registra el **IP** del gateway dispuesto a recibir el tráfico originado fuera del **AS** que tenga como destino ese prefijo de red
- En cierto sentido, el atributo **NEXT-HOP** vincula la información manejada a nivel intra-**AS** con la intercambiada a nivel inter-**AS**

Selección de rutas

- Un router al recibir una nueva ruta puede optar por aceptarla o no en función de su política
- Para elegir entre múltiples rutas a un mismo destino cuenta con diversos criterios:
  - La preferencia local (es decir, su política)
  - El camino **AS-PATH** de menor longitud
  - El router **NEXT-HOP** más próximo (hot potato routing)
  - Otros criterios estipulados por el administrador local

Mensajes BGP

- El protocolo **BGP** implementa su funcionalidad a través del siguiente conjunto de mensajes:
  - **OPEN**: establece una conexión **TCP** autenticada con un vecino inmediato
  - **UPDATE**: publicita un nuevo camino o bien retira una ruta previamente publicada
  - **KEEPALIVE**: sirve para mantener una conexión activa aun al no disponer de nuevos mensajes de **UPDATE**
  - **NOTIFICATION**: se usa para reportar que en el mensaje anterior se detectó un error; también sirve para cerrar una conexión

¿Preguntas?