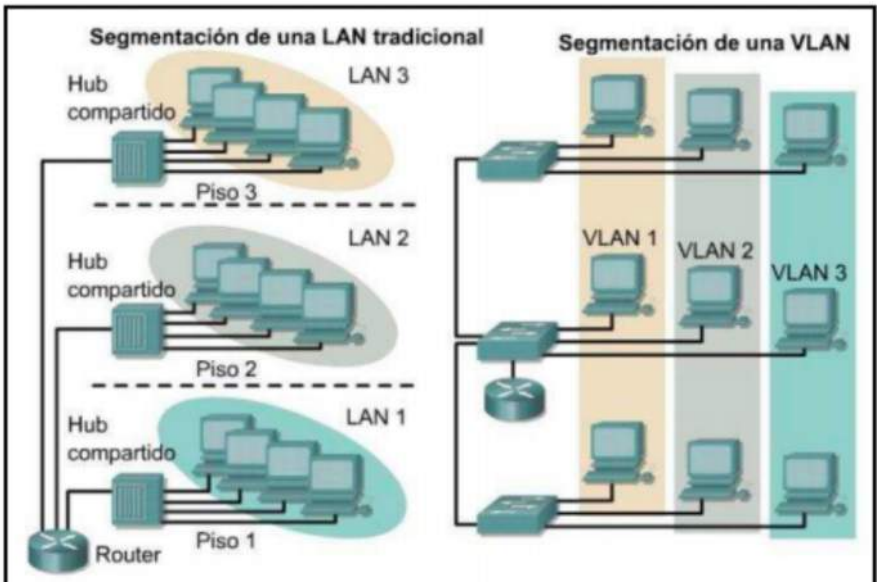
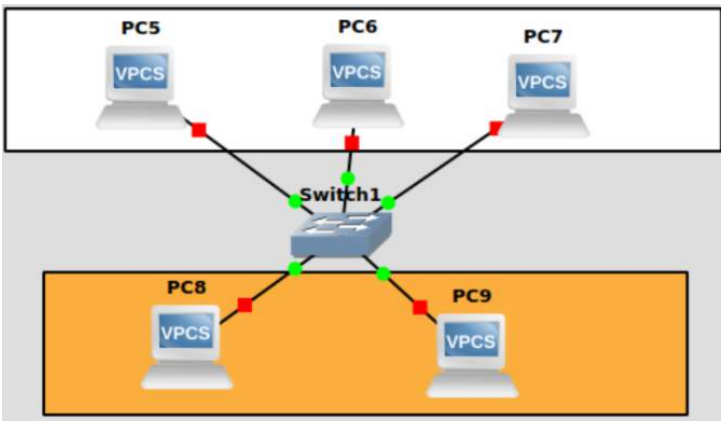
Configuración de una VLAN

- Recordamos funcionamiento del Switch
  - Es posible que un switch se sature y ocasione la pérdida de tramas
  - Control de congestión a nivel de enlace de datos
- VLAN
  - Segmentación lógica de la red, que separa los dominios de broadcast
  - Ventajas
    - Transporta distintos segmentos desde un solo puerto físico.
    - Mayor seguridad y facilidad de administración
    - Mejor aprovechamiento de los recursos de red
    - Mayor capacidad para redes con múltiples servicios
  - Existen varias técnicas para definir VLANs, pero en todos se dene la pertenencia de un puerto switch a una o muchas VLANs.
  - A la recepción de una trama sobre un puerto, la trama se remite solo a los puertos que pertenece a una misma VLAN
  - En el caso de una dirección de destino broadcast, la trama es remitida solo a los puertos que pertenecen a la misma VLAN
  - Una máquina puede pertenecer a una o más VLAN.
- LAN vs VLAN



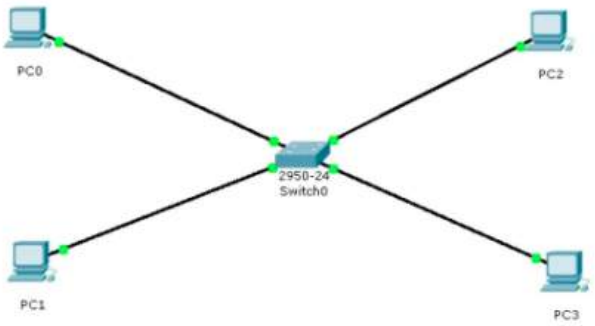
- VLAN por puerto de Switch
  - Asociamos un VLAN a cada puerto del switch
  - El más simple y seguro, aunque estático



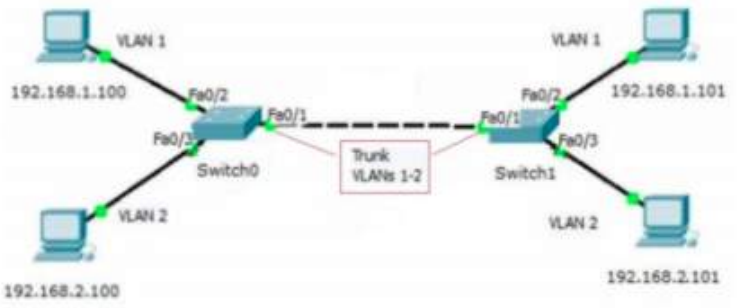
- VLAN por dirección MAC
    - En el Switch hay que llenar una tabla (dirección MAC, VLAN)
    - Más exible, permite nuevos usuarios, permite a un usuario cambiar el enlace ordenador switch, y continuar perteneciendo a la misma VLAN
    - No es tan seguro, ya que un usuario puede cambiar la dirección MAC de una máquina.
    - Difícil para el administrador ya que debe saber las direcciones MAC

- VLAN por dirección IP
    - En el Switch hay que llenar una tabla (dirección IP de red, VLAN)
    - Es menos seguro, ya que el usuario puede cambiar de dirección IP
    - Tiene menos desempeño ya que debe analizar las cabeceras de la IP
    - Más simple para el administrador
    - Llamado generalmente VLAN por subred
- VLAN por Filtros
    - Se basa en información de protocolos de red (IPX, IP, Apple Talk).
    - La pertenencia a la VLAN se basa en la utilización de filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN
    - Los filtros han de aplicarse por cada trama que entre por uno de sus puertos del switch
    - Ventajas
        - Segmentación por protocolo
        - Asignación dinámica
    - Desventajas
        - Problemas de rendimiento y control de broadcast: requieren complejas búsquedas en tablas de pertenencia y si el nodo es multiprotocolo recibira muchas peticiones broadcast
        - No soporta protocolos de nivel 2 ni protocolos dinámicos
- Herramientas de administración de VLAN
  Entre los más rankeados son:
    - SolarWinds Network Conguration Manager
    - ManageEngine Network Conguration Manager

    - WhatsUp Gold: basado en SNMP
    - Paessler PRTG Network Monitor: basado en sensores
- Configuración de puertos de switch: Modo acceso
    - Este tipo de configuración en el puerto permite pasar solo una Vlan, los paquetes no van etiquetados, y por lo general se usa para conectar dispositivos finales.

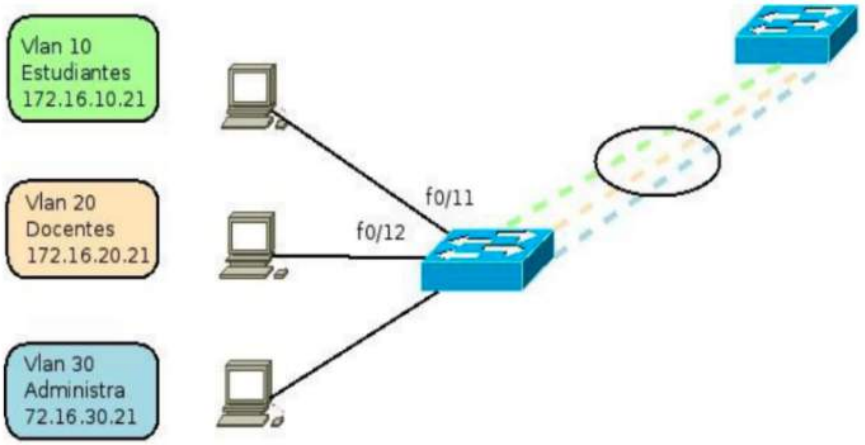


    - Comando para configurar en modo acceso
        - # Configure terminal
        - # interface gigabitethernet 1/0/10
        - # switchport access vlan 2
        - # no shutdown
- Configuración de puertos de switch: Modo trunk
    - Permite manejar el tráfico de distintas Vlan en un mismo puerto, o sea que cada paquete irá etiquetado y cuando se envíe a una vlan se podrá resolver correctamente. Este tipo de configuración se usa para interconectar distintos tipos de equipos de red, como pueden ser 2 switches.



    - Comando para configurar en modo trunk
        - # Configure terminal
        - # interface gigabitethernet 1/0/10
        - # switchport mode trunk
        - # no shutdown
- Funciones de las VLAN en Redes Convergentes

    - Red convergente
        - Red donde coexisten servicios de distinta naturaleza como es la voz, videos y comunicación de datos.
        - Se define como un arquitectura que soporta todos los medios de información en todas las tecnologías de red
    - Funciones
        - Optimización del Ancho de Banda: crean dominios de broadcast más pequeños.
        - Seguridad: permiten desarrollar un nivel de seguridad más alto, ya que no permiten que la información salga del mismo grupo de trabajo.
        - Balance de carga: combinado con ruteo, determinan la mejor ruta hacia un destino.
        - Aíslan las fallas: reducen el impacto de problemas en la red.
- Trunk en redes convergentes
    - Enlace troncal
        - Enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Permite extender una VLAN a través de una red.
    - El estándar 802.1Q es el más utilizado para el establecimiento de enlaces troncales.
    - Permite el tráfico de múltiples VLAN en un mismo medio



Subnetting

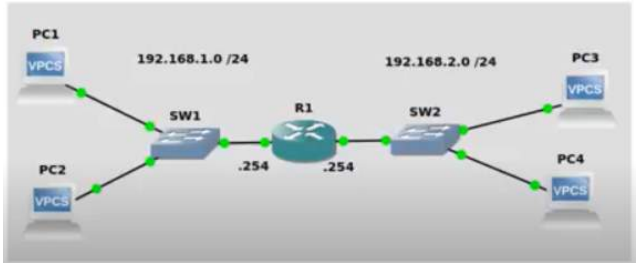
- Modelo ISO /OSI
    - ¿Cuál es la capa que hace el direccionamiento y enrutamiento y cómo se llama su PDU? Capa de red, paquete
    - ¿Cuál es la capa que hace un puente para hacer reenvío de paquete de datos y como se llama su PDU? Capa de enlace de datos, trama
    - ¿Cuál es la capa que establece, administra y termina las conexiones y como se llama su PDU? Capa de sesión
    - ¿Cual es la capa que permite comunicación host-to-host y como se llama su PDU? Capa de transporte, segmento
- Dispositivos de red
    - El modem opera en capa 1 y capa 2? SI
    - El switch opera en capa 2 y puede operar en capar 3? SI
    - El router opera en capa 4? NO, opera en capa 3
    - El hub o concentrador opera en capa 2? No, opera en la capa 1
    - El puente opera en capa 2? SI
    - El repetidor opera en capa 1? SI
- Preguntas de repaso
    - Cable UTP categoría 3 soporta hasta 10 Mbps? es usado todavía? SI, aún es usado en los cables de telefonía
    - Cable UTP categoría 4 soporta 18 Mbps? No, 16 Mbps
    - Cable UTP categoría 5 es usado en LANs Ethernet? hasta cuando soporta? Si, hasta 100 Mbps, hasta 100 metros
    - Cable UTP categoría 5e cual es el máximo de velocidad? 1Gbps
    - Cable UTP categoría 6 soporta hasta cuando Gbps? y cual es la distancia que soporta? 10Gbps, 100 metros
    - Cable UTP categoría 6a en que diere de la categoría 6? Resistencia a interferencias
    - Cable de fibra óptica monomodo (single mode) es más barato que el multimodo? NO
    - ¿El cable de fibra óptica multimodo soporta hasta 550 o 600 metros? ¿Cuál es el rango de su rango de velocidad en Gbps? 550m - 10km, 10Gbps
    - Mencione los 3 tipos de comunicación en la capa de red: unicast, multicast
    - ¿Qué protocolo nos permite acceder remotamente sobre conexiones encriptadas? SSH
    - La caché ARP mapea de direcciones IP a puertos de switch? NO
    - Internet está gobernado por direcciones privadas? NO
    - LACNIC es una organización que se encarga de? Asignar y administrar los recursos ipv4 y v6, a nivel de latinoamérica y el caribe
    - ¿Cuáles son los estándares de la IEEE para redes cableadas Ethernet y redes inalámbricas? 802.3, 802.11

Busquen el RFC 1889 en la base de datos de la RFC https://www.rfc-editor.org/.

- ¿Cuál es la entidad de Normalización que ha emitido este documento? IETF
- ¿Cuál es el estado del RFC 1889? Obsoleto, porque salió la RFC 3550
- ¿Cuál es el objetivo del protocolo RTP definido en esta RFC? Proteger un protocolo de transporte en tiempo real (audio, video)
- ¿Cuál es el protocolo citado para trabajar con RTP? RTCP

- ¿Cuál es la propiedad, que no satisface la red de internet descrita en el documento, que justifica el uso de RTP? No te da los mecanismos que garantizan el orden ni tiempo adecuado de llegada
- La clase A va de 0-127, es que el 127 se puede tomar para una red? Para red local
- ¿Cuál es el prefijo de la clase B ? /16
- El prefijo permite identificar?
  - (a) **red y la cantidad de hosts de la red**
  - (b) número de subredes
  - (c) número de bits de una red
- Podemos asignar la dirección broadcast a un host? No, es para difundir a todas las máquinas
- Si hace ping a 192.168.1.255, cual es la dirección MAC que retorna?, retorna F para todos
- Dada la dirección y prejo 183.26.103.215 /30. Ingrese el último octeto en binario y decimal (VER SOLUCIONARIO PC1)
  - De Red
  - De broadcast
  - El primer host usable
  - EL ultimo host usable
- La red 10.0.0.0 /8, cuántos hosts máximo puede tener? USAR FÓRMULA
- ¿Puede haber comunicación entre PC1 y PC3?

Si se enruta si es posible.

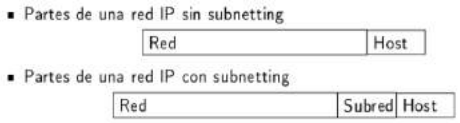


- Reverse ARP (RARP)
    - Obtener una dirección IP a partir de la dirección MAC
    - Descripción contenida en RFC (Request For Comments) 903
    - El problema de hoy en dia: asignación dinámica de dirección IP
    - RARP no es suficiente para el uso moderno:
        - BOOTP (RFC 951) mejoras a RARP
        - DHCP (RFC 1541) extiende y reemplaza BOOTP
    - El formato de RARP es idéntico al de ARP
- Problemas con RARP
    - Las peticiones RARP no son encaminadas por el router
    - Genera tráfico en la red, muchos servidores RARP necesitan ser configurados en la misma Ethernet, pero esto implica que todos los servidores respondan a una petición RARP
    - Solo permite obtener la dirección IP, pero los otros parámetros de configuración del modelo TCP/IP ? Se tuvo que cambiar por el BOTP, luego DHCP
- ICMP
    - Permite reportar diversas incidencias o situaciones excepcionales que se producen en el envío de datagramas IP.
    - Todos los mensajes ICMP se envían en datagramas IP con valor 1 en el campo protocolo
    - Los mensajes ICMP incluyen como datos la cabecera del paquete que ha provocado el mensaje.
- Principales tipos de mensajes ICMP

Mensaje	Significado
Destino inaccessible	Red, host, protocolo, o puerto destino (nivel transporte) desconocido
Echo request y echo reply	Sirve para comprobar la accesibilidad de una direccion IP
Tiempo excedido (ttl)	Se ha descartado un datagrama por agotamiento de ttl
Cambio de ruta	El router informa de una ruta mas directa que la que se esta utilizando
Calmar al emisor	Ejerce control de flujo sobre el emisor cuando se produce congestion

- Subnetting
    - Subdivisión de una red en muchas subredes
    - Interés del subnetting
        - Segmentación en muchos dominios de broadcast. Por ejemplo, tenemos una dirección clase B 131.175.0.1 que va hasta 131.175.255.254. Eso significaría que tendríamos 65534 hosts en la misma red sica. El desempeño de la red y su mantenimiento no son buenos.
- Idea de tener más niveles de jerarquía
    - subdividir una red en muchas subredes
    - cada subred= red física (Ethernet, FDDI, ATM)
    - Probablemente se use el tercer byte para identificar la subred

- Estructura de una dirección IP



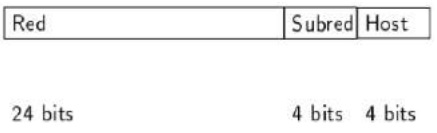
- Máscaras de subred por defecto

    - Clase A
        - 8 bits para red, 24 bits para hosts
        - Mascara por defecto 255.0.0.0
    - Clase B
        - 16 bits para red, 16 bits para hosts
        - Mascara por defecto 255.255.0.0
    - Clase C
        - 24 bits para red, 8 bits para hosts
        - Mascara por defecto 255.255.255.0
- Metodo de calculo general
    1. Determinar la cantidad de bits que se tomaran prestados
    2. Calcule la nueva máscara de subred
    3. Identifique los diferentes rangos de dirección IP
    4. Identique los rangos de dirección IP no utilizadas
    5. Identifique las direcciones de red y de broadcast
    6. Determine los rangos de dirección utilizables por los hosts

  Calcule el número de hosts
    - Calcule el número de bits necesarios para codificar el número de hosts deseados

    - Ejemplo
        - Buscamos obtener subredes compuestas de 12 hosts
        - 12 en binario es 0000 1100, bastará entonces 4 bits (16 posibilidades) para codificar los hosts deseados

  Calcule el número de bits necesarios para codificar el número de subredes deseadas
    - Ejemplo
        - Buscamos obtener 9 subredes
        - 9 en binario es 0000 1001, bastará entonces 4 bits (16 posibilidades) para codificar las subredes deseadas
- Regla 2^s y 2^h − 2
    - Deseamos subdividir la clase C siguiente: 192.168.10.0 en 9 subredes de 12 hosts cada uno

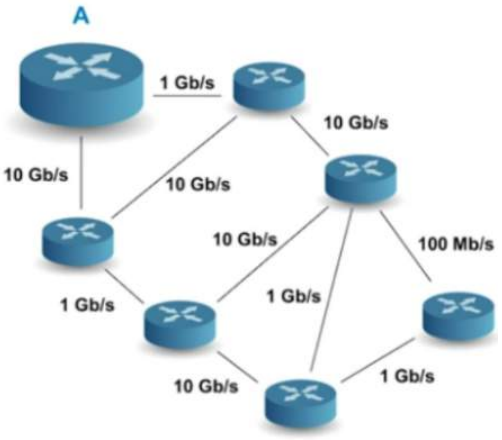


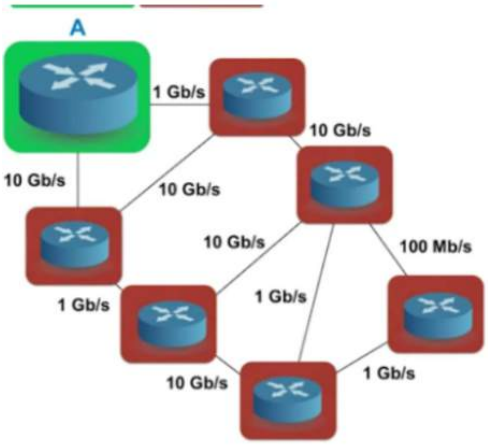
    - Aplicamos la fórmula para subredes 2^s donde s es el número de bits para subredes y 2^h − 2 donde h es el número de bits para la cantidad de hosts
    - La nueva mascara de subred correspondiente es 255.255.255.240
- Ejercicios
    - Tenemos la dirección de red clase C 192.168.1.0 /24 para realizar mediante subnetting obtener 4 subredes con un mínimo de 50 host por subred.
    - Dada la red 192.168.21.0, se necesita generar 28 subredes. ¿Qué máscara de subred se deberá utilizar?
    - Dada la dirección IP 195.106.14.0 /24, cual es el número total de redes y el número total de nodos por red que se obtiene?
    - Utilizando una dirección de clase C, necesita 5 subredes con un máximo de 17 nodos en cada una de esas subredes. ¿Qué máscara de subred deberás utilizar?
    - Dada la red 192.141.27.0 /28, cual de estas direcciones de hosts son válidas?
        - 192.141.27.208
        - 192.141.27.175
        - 192.141.27.119
        - 192.141.27.148
    - Cual es el rango de nodos válidos del cual es la dirección IP 172.16.10.22 /28
    - Indique la dirección de difusión (broadcast) para una red de clase B que utiliza la máscara de subred por defecto?
    - Indique una direccion de difusion perteneciente a la red 192.57.78.0/27
- Mascara de longitud variable (VLSM)
    - Permite aplicar subnetting de forma anidada.
    - Permite interconectar un grupo de subredes con distintas máscaras
    - Antes de VLSM: FLSM (Fixed length Subnet Mask)
        - Uso de máscaras de igual longitud en todas las subredes
        - Poco escalable
        - Uso de direcciones IP no optimizado
        - Poca flexibilidad para el correcto diseño IP
    - Ejemplo:
        - Tenemos una mascara original /22 y nos desplazamos 7 bits, ¿cuántas subredes podemos hacer?. De ahí tomamos una subred, y lo dividimos en dos subredes, dar el rango de host válidos
- Supernetting o Classless Inter-Domain Routing (CIDR)
    - Identificador de subred de cualquier longitud
    - Otra forma de marcar la separación es mediante la máscara de subred
    - Utiliza VLSM para optimizar el espacio de direcciones
    - Descripción en RFC 1517
    - Solución fundamental en el problema de las tablas de enrutamiento
- Direccionamiento IP Classful y classless
    - En enero 2007. existia mas de 433 millones de hosts en el internet
    - Las iniciativas para optimizar el espacio de direcciones IPv4 fueron:
        - VLSM y la notación CIDR
        - NAT (traducción de direcciones de red)
        - Direccionamiento privado
    - una dirección IP tiene dos Partes

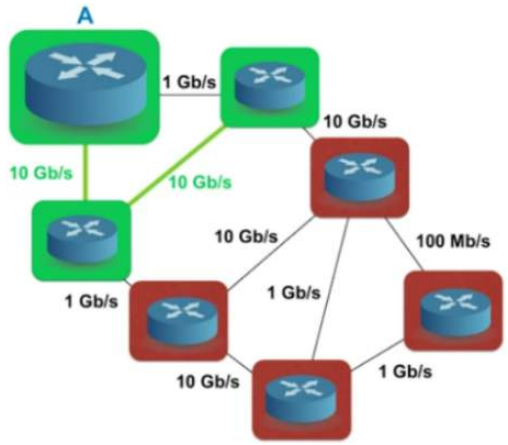
        - la parte de red
        - la parte de host
    - El objetivo de una máscara de subred es determinar la parte de red de una dirección IP
- Modelo CIDR
    - Elimina completamente los conceptos de clase A,B yC
    - Basado en prefijos de red
        - El protocolo de enrutamiento debe tener la capacidad de identificar el prefijo de red (BGPv4)
        - Se requiere el prefijo de red para hacer determinar parte host y parte red
    - En esencia CIDR=VLSM aplicado a todo el internet

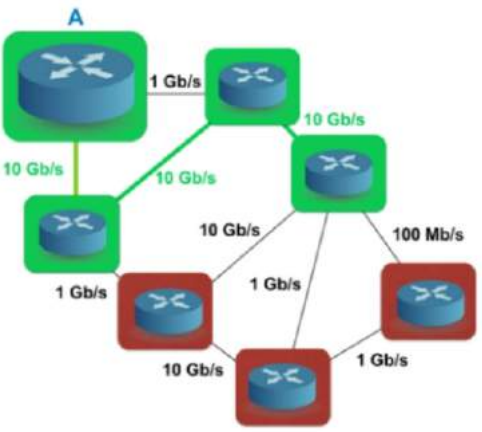
Open Shortest Path First (OSPF)

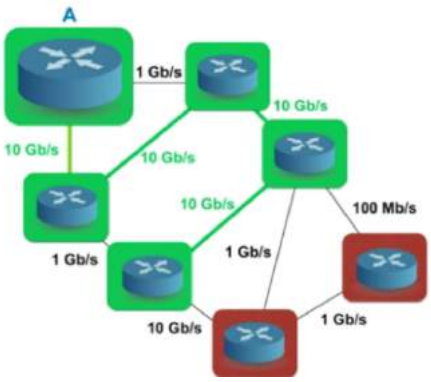
- OSPF
  - Conocido como algoritmo de Dijkstra
  - Tres versiones
    - OSPFv1: no usada en el mercado
    - OSPFv2: usado para IPv4
    - OSPFv3: usado para IPv6
  - Los routers almacenan información de la red en LSA (Advertencias estado enlace) organizado en LSDB (base de datos de estado enlace)
  - Los routers inundan LSAs hasta que todos los routers en el área OSPF desarrollen el mismo mapa de red.
- Algoritmo de Dijkstra

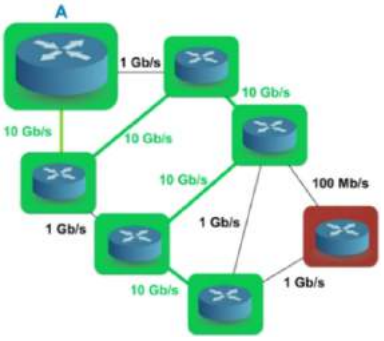


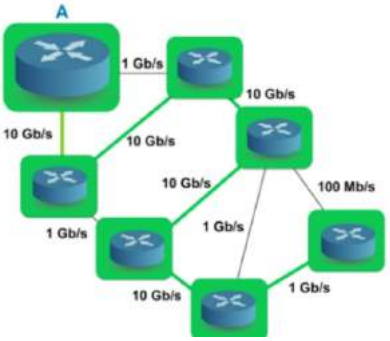












- Costo adicional de algoritmos de enrutamiento

Algoritmo	Informacion transmitida	Destinatario
Enrutamiento aleatorio		
Inundacion		
Vector distancia Estado enlace	Toda la tabla de enrutamiento Hola vecino	Vecinos inmediatos Vecinos inmediatos. Todos los routers
Estatico centralisado	Vecindad. Toda la tabla de enrutamiento	Centro de control. Todos los routers
Pre-calculado	Vecindad	Centro de control

- Calidad de la rutas

Algoritmo	Calidad de la ruta
Enrutamiento aleatorio	Potencialmente muy malo
Inundacion	Todas
Vector distancia Estado enlace	Optima Optima
Estatico centralisado	Optima
Pre-calculado	Pasa por un intermediario

- Robustez de protocolo de enrutamiento

Algoritmo	Robustez
Enrutamiento aleatorio	No sensible a falla
Inundacion	No sensible a falla
Vector distancia Estado enlace	No sensible a falla No sensible a falla
Estatico centralisado	Punto debil: el centro de control
Pre-calculado	Punto critico: el centro de control

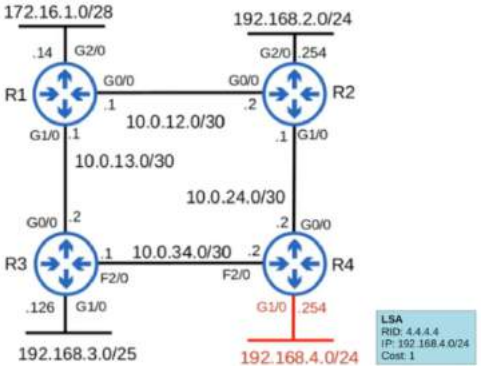
- Convergencia de protocolo de enrutamiento

Algoritmo	Tiempo de convergencia
Enrutamiento aleatorio	Ninguno
Inundacion	Ninguno
Vector distancia Estado enlace	Funcion de diametro de la red Constante: tiempo de inundacion
Estatico centralisado	Constante: tiempo de inundacion
Pre-calculado	Rapido: prevenir el centro de control

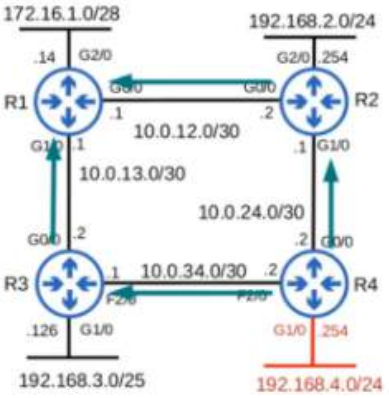
- Resumen de desempeño de las rutas

- Algoritmo de estado enlace
    - Cada router tiene una base de datos que representa un mapa de toda la topología
        - Enlaces
        - Su estado (incluyendo el costo)
    - Todos los routers obtienen la misma información
    - Todos los routers calculan la mejor ruta a cada destino
    - Cualquier cambio de estado de un enlace se difunde a través de toda la red, llamado Difusión global de información local
- Ventajas de OSPF
    - Evita routers intermediarios que incrementan la cantidad de saltos
    - Menos información y mayor ancho de banda útil que con RIP
    - Usa algoritmo de Dijkstra enlace-estado (LSA Link State Algorithm) para el cálculo de ruta más corta
    - Usa cost como medida de métrica
    - Construye una base de datos enlace-estado idéntica en todos los enrutadores de la zona
    - Puede operar con MD5 para autenticar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado
- Requisitos de diseño OSPF
    - Abierto: no es propiedad de una compañía
    - Permita reconocer diferentes métricas (entre ellas distancia física y retardo)
    - Dinámico: rápida adaptación a los cambios en la topología
    - Capacidad de encaminamiento dependiendo del tipo de servicio
    - Capaz de equilibrar las cargas entre diferentes líneas
    - Reconocer sistemas jerárquicos
    - Implemente mecanismos mínimos de seguridad
- Características de OSPF
    - Uno de los IGP más importantes
    - Recomendado por IETF (Internet Engineering Task Force) para redesIP
    - Basado en algoritmo de estado de enlaces SPF
    - Soporta prejos longitud variable: prefijos+máscaras
    - Enrutamiento jerárquico
    - Enrutamiento multimétrico
    - Control sobre inyección rutas externas:
        - descubrimiento dinámico de routers vecinos
        - Adaptación a redes locales

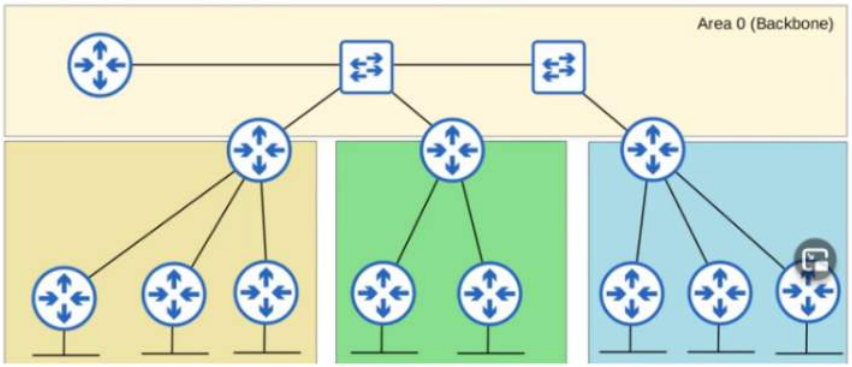
        - Soporte autenticación de mensajes
        - Capaz de etiquetar rutas y propagar etiquetas por otras rutas
        - Capaz de descomponer en redes más pequeñas
    - Posee área especial backbone que forma la parte central de la red (donde hay otras áreas conectadas a ella)
    - Direcciones multidifusión usadas son 224.0.0.5 y 224.0.0.6
    - Al contrario que RIP y BGP (no usa ni TCP ni UDP)
- Inundación LSA (Advertencias estado enlace)



    - LSA es inundado por toda la red hasta que todos los routers lo hayan recibido
    - Al final, todos los routers comparten la misma LSDB
    - Cada router usa el algoritmo SPF para calcular la mejor ruta a 192.168.4.0 /24
    - Cada LSA es inundado cada 30 min por defecto



- Pasos del Proceso de compartir LSA y determinar la mejor ruta
    - Hacer vecinos con otros routers conectados al mismo segmento
    - Intercambiar LSA con routers vecinos
    - Calcular las mejores rutas para cada destino e insertarlos en la tabla de enrutamiento
- Áreas OSPF



    - OSPF usa áreas para dividir la red
    - En redes pequeñas una única área es suficiente
    - Caso contrario en redes grandes, más de una área
    - Si usamos una sola área los efectos serían que
        - el algoritmo tomará más tiempo para calcular las rutas
        - el algoritmo requeriría más recursos en el router
        - grandes LSDB toma más memoria en los routers
        - cualquier cambio en la red causaría que cada router inunde con LSA y corra el algoritmo SPF nuevamente
    - Una área es un conjunto de routers y conexiones que comparten la misma LSDB
    - El área backbone(área 0) es un área a la cual todas las otras áreas deben conectarse
    - Routers con todas sus interfaces en el misma área son llamados de routers internos
    - Routers con interfaces en múltiples áreas son llamadas router de borde de área (ABR)
    - ABR mantienen un LSDB separado para cada área que conectan
    - Es recomendable conectar un ABR a máximo dos áreas
    - Routers conectados al área backbone son llamados de routers backbone
    - Un router intra-área es un router destino en la misma área OSPF
    - Un router inter-area es un router destino en una area diferentes
    - Deben ser contiguas
    - Todas las áreas deben tener al menos un ABR conectado al area backbone
    - Interfaces OSPF en la misma subred deben estar en la misma área
- Configuración básica de OSPF
    - R1 (config) # router ospf 1
    - R1 (config-router) # network X.Y.Z.W A.B.C.D area NRO

También tiene el comando passive-interface que hace lo mismo en RIP.
El comando default-information originate funciona de la misma manera que RIP

- OSPF
    - Definir el Router ID prioridad OSPF es el mismo procedimiento que se hacía en RIP
    - Un router de borde de sistema autónomo (ASBR) es un router que conecta la red OSPF con una red externa
- Ejercicios

¿Cual de las siguientes sentencias son falsas?

- En redes OSPF multiárea, todas las áreas no-backbone tiene un ABR conectada al área 0
- **Un área OSPF debe tener el área 0**
- Dos routers OSPF con diferentes procesos IDs pueden convertirse en vecinos OSPF
- El área OSPF debe ser especificada en el comando network
- Un ASBR conecta la red interna OSPF a redes fuera del dominio OSPF
- **El proceso ID OSPF debe coincidir con el número de área**

Cual de los siguientes comandos haría un router R1 un OSPF ASBR?

- R1 (config-router)# network 10.0.0.0 0.0.0.255 area 0
- **Alternativa 2**
    - R1 (config) # ip route 0.0.0.0 0.0.0.0 203.0.113.2
    - R1 (config) # router ospf 1
    - R1 (config-router)# default-information originate

    - R1 (config-router)# network 0.0.0.0 255.255.255.255 area 0
    - R1 (config-router)# default-route originate

Cual de los siguientes comandos es usado para configurar manualmente el router ID OSPF?

    - **R1 (config-router)# router-id 1.1.1.1**
    - R1 (config-router)# ospf router-id 1.1.1.1
    - R1 (config)# interface loopback0
    - R1 (cong-if) # ip address 1.1.1.1 255.255.255.255
    - R1 (config-router)# ospf router id 1.1.1.1

- Costo OSPF
    - La métrica del OSPF es llamado costo
    - Es calculado automáticamente basado en el ancho de banda (velocidad) de la interfaz
    - Es calculado dividiendo el ancho de banda referencial entre el ancho de banda de la interfaz
    - El ancho de banda referencial por defecto es 100 mbps
    - Todos los valores menor que 1 son convertidos a uno
    - Por consiguiente, Fast Ethernet, Gigabit Ethernet, 10Gig Ethernet, etc son iguales en que tiene igual costo
    - Tu puedes cambiar el ancho de banda referencial con el comando:
        - R1(config-router)# auto-cost reference-bandwidth megabits-per-second
    - Se debe configurar el ancho de banda referencial con valor mayor a los mayores enlaces en tu red para permitir futuras mejoras
    - El costo OSPF a un destino es el costo total de las interfaces de salida
    - El costo de la interfaz loopback es de 1
    - El valor de ancho de banda es usado para calcular el costo OSPF, sin embargo eso no cambia la velocidad con que opera la interfaz
    - Para cambiar la velocidad de la interfaz se usa el comando speed
    - Es recomendable primero cambiar el ancho de banda referencial para luego evaluar si cambia el ancho de banda de la interfaz
    - Otra forma de cambiar el ancho de banda de la interfaz es
        - R1(config-if)# bandwith kilobits-per-second
- Vecinos OSPF
    - Asegurar que los routers sean vecinos OSPF es la tarea principal en configurar OSPF
    - Una vez que los routers son vecinos OSPF, automáticamente hacen el trabajo de compartir información de la red, calcular rutas, etc
    - Cuando OSPF es activado en una interfaz, el router empieza enviando mensajes Hello OSPF fuera de la interfaz de forma periódica
    - determinado por un Hello reloj. Esto es usado para presentarse a otros
    - OSPF vecinos.
    - El hello reloj está configurado por defecto en una conexión ethernet a 10 segundos
    - Los mensajes Hello son multicast a 224.0.0.5
    - Los mensajes OSPF son encapsulados en la cabecera IP con el valor 89 en el campo protocolo
- Vecino OSPF: estado de baja

    - OSPF es activado en la interface G0/0
    - Envia un mensaje Hello OSPF a 224.0.0.5
    - No conoce algún vecino OSPF todavía, entonces el actual vecino está en estado de baja, y el identificador vecino con que envía el mensaje es 0.0.0.0
- Vecino OSPF: estado inicial
    - Cuando R2 recibe el paquete Hello, agrega una entrada para R1 en su tabla de vecinos OSPF
    - En la tabla de vecinos de R2, la relación con R1 está en estado inicial
    - Estado inicial= Paquete Hello recibido, pero el router ID de R2 no está en el paquete Hello
- Vecino OSPF: estado dos caminos
    - R2 envía un paquete Hello con los routers IDs de ambos routers
    - R1 insertará en su tabla de vecinos OSPF a R2 en estado de dos caminos
    - R1 enviará otro mensaje Hello esta vez conteniendo el router ID de R2
    - Ahora ambos routers están en estado de dos caminos
    - Estado dos caminos significa que el router ha recibido el paquete Hello con su router ID en el paquete
    - Si ambos routers alcanzan estado dos caminos, significa que todas las condiciones han sido satisfechas para que se conviertan en vecinos
    - OSPF. Ya estaría listo para compartir LSA y construir un común LSDB
    - En algunas redes, un router designado (DR) y un router designado para backup (BDR) son elegidos en este punto
    - Ahora ambos routers están en estado de dos caminos
- Vecino OSPF: estado Ex Comienzo
    - Dos routers ahora se preparan para intercambiar información sobre su LSDB
    - Antes de intercambiar, se debe escoger quien comienza el intercambio
    - Esto se hace en el estado Ex Comienzo
    - El router con el mayor router ID se convierte en maestro e inicializa el intercambio, el router con menor RID se convierte en esclavo
    - Para decidir maestro esclavo, ellos intercambian paquetes DBD (descripción de base datos)
- Vecino OSPF: estado Intercambio
    - Routers intercambian DBDs que contienen listas de LSA contenidos en su LSDB
    - Estos DBDs no incluyen información detallada de LSA, solo información básica
    - Los routers comparan la información en DBD con su LSDB para determinar que LSA deben recibir de sus vecinos
- Vecino OSPF: estado Cargando
    - Routers envían mensajes Peticion Estado Enlace (LSR) para solicitar que sus vecinos le envíen LSA que no tienen
    - LSA son enviados en mensajes Actualizacion Estado enlace (LSU)
    - Los routers envían mensajes LSAck para hacer conocer que han recibido los LSAs
- Vecino OSPF: estado Lleno
    - Los routers tienen la adyacencia de OSPF llena y identicos LSDB
    - Los routers continúan enviando y escuchando mensajes Hello(10 segundos por defecto) para mantener la adyacencia de vecinos
    - Cada mensaje Hello que es recibido, el reloj Dead es reseteado (40 segundos por defecto)

    - Si el reloj Dead llega a contar menor que cero y no mensaje Hello es recibido, el vecino es removido
    - Los routers continuarán compartiendo LSAs para asegurar que cada router tenga un mapa completo de la topología de red
- Comando para saber los vecinos ospf
    - show ip ospf neighbor
- Configuración OSPF
    - Se puede activar directamente OSPF en una interfaz
        - R1 (config-if)#ip ospf identificador-proceso area NroArea
    - Para configurar todas las interfaces como OSPF pasivas
    - R1 (config-router)#passive-interface default
- Ejercicios

Cual de las sentencias es correcta sobre el costo OSPF por defecto

- Todas las interfaces tienen el mismo costo
- **Ethernet y Fastethernet tienen el mismo costo**
- Fastethernet, Gigabit Ethernet, y 10 Gig Ethernet tienen el mismo costo
- Ethernet, Fastethernet, Gigabit Ethernet, y 10 Gig Ethernet tienen el mismo costo

En cuál de los estados del vecino OSPF, los roles maestro-esclavo es decidido

- **Excomienzo**
- 2 caminos
- Intercambio
- Cargando

Qué comando puede ser usado para hacer una interfaz fastEthernet con costo OSPF de 100

- R1 (config-router) # auto-cost reference bandwith 100
- R1 (config-router) # auto-cost reference bandwith 1000
- **R1 (config-router) # auto-cost reference bandwith 10000**
- R1 (config-router) # auto-cost reference bandwith 100000

Cuales son los valores por defecto de los relojes OSPF hello y dead en una conexión ethernet

- Hello 2, Dead 20
- **Hello 10, Dead 40**
- Hello 30, Dead 120
- Hello 60, Dead 180

Introducción a redes

- Normalización
    - En el inicio responsabilidad de DARPA
    - Organismos reguladores
        - ITU (International Telecommunication Union)
        - ISO (International Organization for Standardization)
        - IEEE (Institute of Electrical and Electronic Engineers)
        - IETF (Internet Engineering Task Force)
- RFC (Request for Comments) - Pedido de Comentarios
    - Documentación oficial de internet
    - Documentos públicos que todos pueden acceder
    - Jon Postel
        - contribuyó para la especificación de muchos protocolos fundamentales de internet.
        - Papel fundamental en la gestión de infraestructura
        - Algunos de los RFCs:
            - User Datagram Protocol (UDP)
            - Simple Mail Transfer Protocol (SMTP)
            - Internet Control Message Protocol (ICMP)
- Administración de Red de ordenadores
    - Se reere a las actividades , métodos, procedimientos como la vigilancia de una red y herramientas de implementación por parte del administrador de la red relacionadas con la operación, administración, mantenimiento y suministro de una red.
    - Actividades concernientes
        - Supervisión
        - Administración
        - Operación
- Tipos de la administración de redes
    - Administracion de Usuarios
        - Accesibilidad y conexión a las aplicaciones
        - Acceso a los servidores
        - Confidencialidad y seguridad
        - Calidad del servicio (QoS)
    - Administración de Servicios
        - Conexión y la distribución de aplicaciones sobre toda la red
        - Gestión y distribución de los datos
        - Gestión de aplicaciones
    - Administración de Transporte
        - Operaciones de la red
        - Lista de incidentes en la red para la puesta en marcha de protocolos de deteccion y correccion
        - Desempeño de la red
        - Costos
        - Configuración de la red para mejorar el desempeño y QoS
        - Determinar nuevos requerimientos y las partes del sistema
- Roles de un administrador de red

    - Instalar y mantener una infraestructura de red
    - Instalar y mantener los servicios necesarios al funcionamiento de la red
    - Asegurar los datos internos de la red
    - Asegurar que los usuarios acceden a información que les corresponde
    - Administrar logins (nombres de usuarios, derechos de acceso, permisos particulares. . .)
    - Administrar los sistemas de cheros compartidos y mantenerlos
- Nivel de decisiones de la Administración de Red de Ordenadores
    - Decisiones operacionales: decisión a corto tiempo, en tiempo real de la administración de red
    - Decisiones tácticas: decisión a mediano tiempo, envuelve la evolución de la red y la aplicación de políticas a largo tiempo
    - Decisiones estratégicas: son decisiones a largo plazo, involucra estrategias para futuros requerimientos de los usuarios.
- Símbolo de los dispositivos de Red

- Modelo TCP/IP

Capas del Modelo TCP/IP	Algunos protocolos
Capa de Aplicacion o Proceso	SNMP, SSH, DNS, NFS, HTTPS, SMTP
Capa de transporte o Host-to-Host	TCP, UDP
Capa de Internet o Red	ICMP, ARP, RARP,IP
Capa de Acceso a la Red o Capa de interfaz de red	Etherne, Fast Ethernet, Token Ring, FDDI

- Protocolo de Interconexión (IP)
    - Encaminamiento de datagramas
    - Pocas funcionalidades
    - No hay garantías si falla un nodo
- Comprendiendo las interfaces de Red de linux
    - Loopback (lo):
        - Esta interface tiene la direccion IP 127.0.0.1
        - Representa al nodo mismo
        - Esta dirección IP no es accesible desde la red.
    - Ethernet Versión 2 estándar (en)
    - Ethernet (eth):
    - Red en anillo (tr): Usadas en LAN.

    - SLIP: usada para conexiones en serie. Obsoleto en PCs,pero usado para microcontroladores.
    - FDDI: mediante cables de fibra óptica.
    - PPP (Protocolo punto a punto): cuando se conecta a otro sistema o red a través de un módem.
- ARP
    - Si la comunicación es a través de la tecnología de red Ethernet, los datagramas IP van encapsulados en tramas con dirección origen, la dirección MAC del equipo origen y destino. Por ello se necesita un mecanismo de resolución de dirección que permita obtener la dirección MAC de un equipo.
    - Protocolo de resolución de direcciones IP
        - Descripción contenida en el RFC 826
        - Método común en redes IP basadas en tecnología Ethernet.
        - Diseñado para soportar todo tipo de protocolos y direcciones de red
        - Solo se puede utilizar en redes que admiten envíos broadcast
        - Permite obtener la dirección de subred a partir de la dirección IP asociada
        - Basado en el modelo solicitud/respuesta (2 tipos de mensajes)
        - Los mensajes ARP se encapsulan directamente en PDU de la subred
            - No se encapsula el datagrama IP
- Proceso ARP

    - Suponer que A quiere comunicarse mediante IP con C
    - Problema: El equipo A conoce la IP de C pero no su dirección MAC
    - Solución:
        - A envía en modo broadcast un mensaje ARP a todos los ordenadores
        - C responde con mensaje en modo unicast a A con la información de MAC
- Mensaje ARP

Tipo de Hardware(1=Ethernet)		Tipo de Protocolo (800=IP)
Long. Dir. Hard(6)	Long Dir. Red (4)	Operacion (1 Request - 2 Replay)
Dir. MAC Emisor (oct 0-3)		
Dir. MAC Emisor (oct 4-5)		Dir. IP Emisor (oct 0-1)
Dir. IP Emisor (oct 2-5)		Dir. MAC Destino (oct 0-1)
Dir. MAC Destino (oct 2-5)		
Dir. IP Destino		

Protocolos de la capa de transporte

- BGP utiliza un protocolo de la capa de transporte
- TCP y UDP son protocolos de la capa de transporte
- BGP pertenece a la categoría EGP
- Usa segmentos. Un segmento tiene 16 bits

- Funciones de la capa de transporte
    - Proveer la transferencia de datos de forma transparente entre los hosts finales
    - Proveer servicios a las aplicaciones (recuperación de errores, control de flujo, etc)
    - Proveer direccionamiento a la capa 4 (número de puertos)
        - Rangos: conocidos (0-1023, TCP pertenece aquí) , registrados (1024-49151), efímero (49152-65535)
- Multiplexación por puerto
    - El puerto identifica a la aplicación corriendo en determinada máquina
    - El par (IP, puerto) se denomina socket e identifica unívocamente a un proceso de aplicación en una máquina que puede enviar y recibir datos
    - La aplicación escuchando en un puerto recibirá todos los paquetes dirigidos a esa (IP, puerto, nivel de transporte).
    - Lista completa de puertos en el fichero /etc/services en Linux.
    - Envío de un datagrama a un puerto sin aplicación escuchando devuelve:
        - En el caso de UDP: ICMP de error de puerto inalcanzable.
        - En el caso de TCP: mensaje de RESET.
    - Puerto bidireccional: transmisión/recepción.
    - Buffers de entrada/salida de tamaño configurable por el sistema operativo.
- Puertos y sockets
    - Los número de puertos son identificadores de buffers en las máquinas de origen y destino.
    - Estos buffers son la interfaz entre la capa de aplicación y la capa de red de forma que cada aplicación o proceso de la capa de aplicación tiene asignado un buffer a través del cual intercambia información con la capa de transporte.
    - Después la capa de transporte envía esta información en bloques de tamaño adecuado a la capa de red.
    - De esta manera, una misma máquina puede tener varios procesos independientes que emitan o reciban paquetes a nivel de transporte
    - Los sockets permiten la transmisión bidireccional de datos que puede ser en modo full-dúplex si el SO lo permite.
    - Con el uso de sockets, se diferencian dos procesos:
        - Cliente: siempre solicita establecer una conexión (crear socket)
        - Servidor: ofrecen un tipo de servicio al cliente
- Protocolos de transporte en el Protocolo de Control de Transporte (TCP) y en el Protocolo de Datagramas de Usuario (UDP)
- TCP

- TCP esta orientada a la conexión y servicio fiable
  - Antes de enviar datos al host destino, los dos hosts establecen una conexión.
- Provee una comunicación confiable
  - El host destino debe reconocer que ha recibido cada segmento TCP
  - Si el segmento no es reconocido, lo envía de nuevo
- TCP provee secuenciación
  - Números secuenciales en la cabecera TCP permiten a los hosts destinos poner el segmento en el correcto orden si llegan fuera de orden
- Provee flujo de control
  - El host destino puede advertir al origen para aumentar o disminuir la cantidad de datos que envía

- Formato del segmento TCP

Bits	0-3	4-7	8-15	16-31
0	Puerto Origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	Longitud Cabecera TCP	Reservado	Flags	Ventana
128	Suma de Verificación (Checksum)			Puntero Urgente
160	Opciones + Relleno (Opcional)			
224	DATOS			

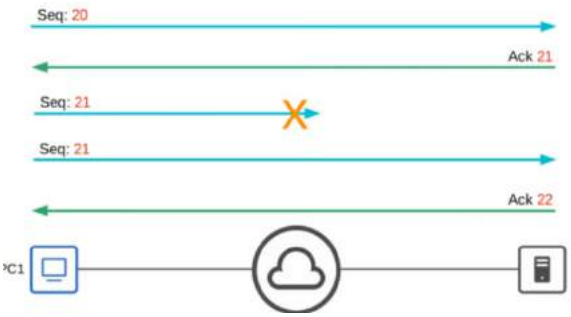
  Flags del campo de control (6 bits)
  - URG y puntero urgente. (URG=1) El segmento transporta datos urgentes a partir del número de byte especificado en el campo puntero urgente.
  - ACK: (ACK=1) El segmento tiene un número de confirmación válido. Todos los segmentos de una conexión TCP, excepto el primero, llevan ACK=1.
  - PUSH: Los datos deben ser enviados inmediatamente a la aplicación (PUSH=1), o pueden almacenarse en el buffer (PUSH=0).
  - RST: Utilizado para abortar una conexión
  - SYN: Utilizado en el establecimiento de la conexión y sincronizar los números de secuencia iniciales
  - FIN:Utilizado en la nalización de la conexión
- Transferencia

  Tamaño del segmento fijado independientemente.
  - PUSH (Emisor). Crea un segmento inmediatamente y lo envía (sin esperar MSS).
  - PUSH (Receptor) Pasa los datos a la aplicación inmediatamente.
  - TCP actúa orientado a fragmento y no a byte

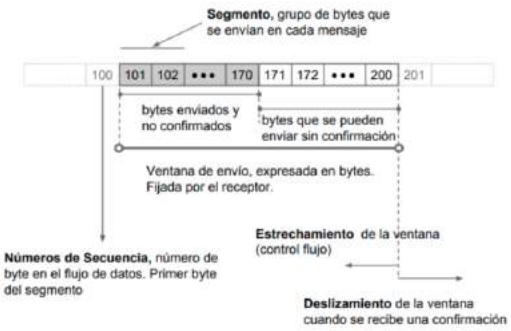
  URG, desde el primer byte hasta el marcado por el puntero de urgente.
  - TCP notifica a la aplicación de los datos urgentes (SIGURG).
  - El tratamiento de urgencia
  - corresponde a la aplicación no a TCP

- TCP y fragmentación
    - Fragmentación de la información en varios datagramas provoca congestión en los routers, ya que deben encaminar más paquetes.
    - TCP negocia para establecer el tamaño máximo de datos que se va utilizar para los paquetes TCP de esa conexion y asi evitar la fragmentación.
    - Este valor se conoce como MSS y depende del valor de MTU
    - MSS=MTU-20 bytes cabecera TCP-20 bytes de cabecera IP
    - Una vez establecida la conexión, se emplea el menor valor de MSS intercambiados
    - Además con la RFC 1191 se evita que datagramas IP que contienen paquetes TCP sean fragmentados en la red.
- TCP: secuenciamiento / acuse de recibo
    - Los hosts establecen un número aleatorio para la secuencia
    - Forward acknowledgement es usado para indicar el número de secuencia del siguiente segmento que el host espera recibir

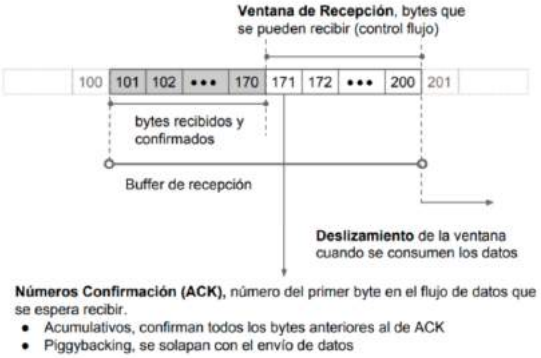
- TCP retransmisión



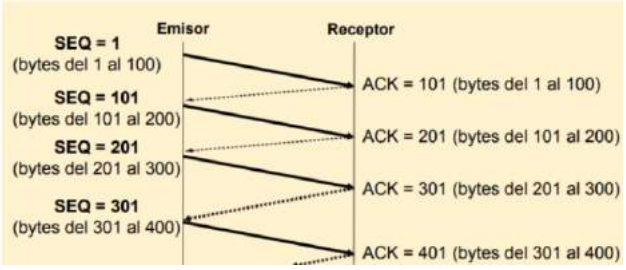
- Control de Flujo: Tamaño de ventana
  El tamaño de la ventana va a permitir que más datos sean enviados
- Ventana de envío



- Ventana de recepción



- Ejemplo de ventana funcionando
  Transmisión sin errores. Tamaño de la ventana 100 bytes, Tamaño del segmento 50 bytes.



- Control de Errores: Confirmaciones

El control de errores se realiza usando el mecanismo de ventana deslizante que permite gestionar:

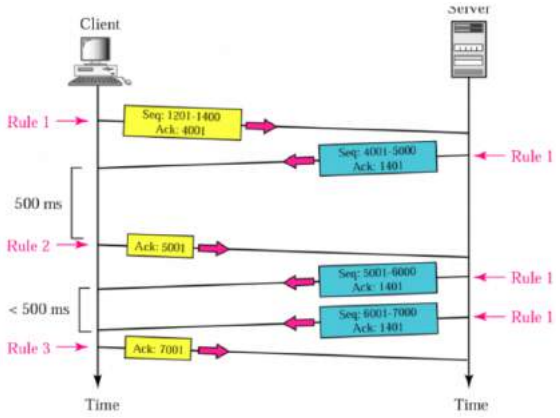
  - La recepción de paquetes duplicados
  - La retransmisión de paquetes erróneos o perdidos
  - La recepción de paquetes fuera de línea

Confirmaciones

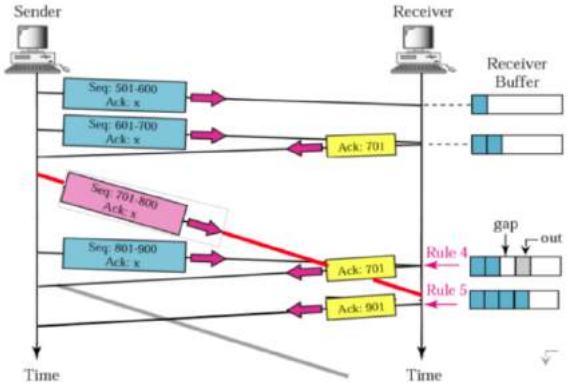
  - Acumulativas, siguiente byte que espera recibir y solapadas con los envíos (piggyback)
  - Las confirmaciones de paquetes en-orden se retrasan para solaparla con un envío máximo de 500ms.
  - Sólo se retrasan un máximo de dos confirmaciones en orden.
  - Los paquetes fuera de orden se confirman con el siguiente byte que se espera recibir.
  - Los paquetes duplicados se confirman para prevenir pérdidas de ACK's.
  - (opcional) SACK, confirmaciones selectivas de paquetes fuera de orden
    - No reemplazan los ACK, informativos para el emisor
    - Implementados como opción TCP

- Control de Errores: Retransmisión
  - La capacidad para retransmitir un segmento TCP cuando no se recibe o se recibe erróneamente es el núcleo del control de errores.
  - TCP dispone de dos mecanismos de retransmisión:
    - Temporizador de Retransmisión (RTO, Retransmission Time-Out)

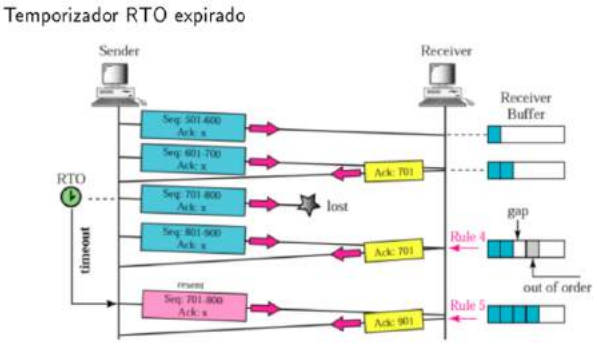
        - Cada conexión tiene asociado un único temporizador
        - Cuando el RTO expira se envía el primer segmento sin confirmar de la ventana
        - Existen diversos algoritmos para jar RTO que es dinámico y debe ser mayor que el RTT (round-trip time)
    - Retransmisión por recepción de 3 ACKs duplicados
        - Retransmisión rápida, no requiere que expire el RTO
- Transmisión sin errores



- Recepción fuera de orden



- Pérdida de un segmento



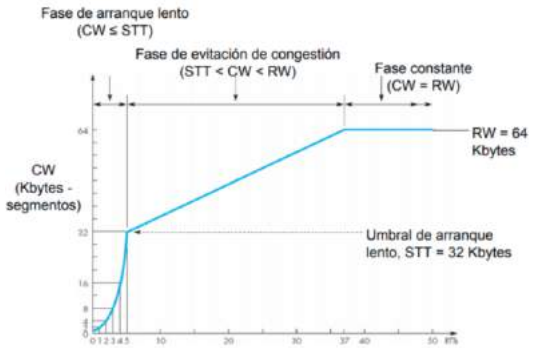
- Temporizador de retransmisión

La elección del tiempo de vencimiento del temporizador de retransmisión (timeout) está basada en los retardos observados en la red

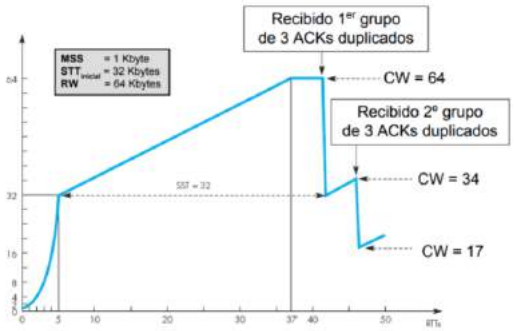
    - Los retardos en la red pueden variar dinámicamente, por tanto los timeouts debe adaptarse a esta situación
    - Las principales técnicas utilizadas para jar los temporizadores de retransmisión son las siguientes:
        - Método de la media ponderada (algoritmo de Jacobson)
        - Método de la varianza (algoritmo de Jacobson/Karels)
        - Algoritmo de Karn
- Control de flujo
    - Controla la tasa de envío de datos para evitar la sobrecarga del receptor
    - El control de flujo se realiza mediante la ventana de recepción, anunciada en cada ACK.
- Control de Flujo: Síndrome de la ventana trivial
    - El síndrome de la ventana trivial (silly window) se produce cuando:
        - La aplicación emisora genera datos a un ritmo muy lento (ej. byte a byte)
        - La aplicación receptora consume datos a un ritmo muy lento
    - Ventana trivial en el emisor (ej. Aplicaciones interactivas)
        - Cada carácter necesita 4 mensajes TCP/IP (40bytes de cabeceras)
        - Un carácter (1 bytes) usa más de 160 bytes
    - Algoritmo de Nagle
        - El emisor envía el primer mensaje (aunque sea un sólo byte)
        - Los siguientes mensajes se retrasan hasta que:
            - se recibe un ACK del receptor
            - se acumulan MSS bytes de la aplicación
            - expira un temporizador
    - Ventana trivial en el receptor
        - La aplicación consume los datos a un ritmo lento
        - Se anuncian ventanas de tamaño reducido, produciendo el efecto anterior
    - Algoritmo de Clark
        - Anunciar un tamaño de ventana 0 hasta que:
            - Se puede recibir un segmento completo (MSS)
            - Se ha liberado la mitad del buffer de recepción
    - Retrasar los ACKs
        - Para el desplazamiento de la ventana del emisor
        - Reduce el tráfico (número de ACKs) pero puede provocar retransmisiones innecesarias
        - TCP establece que no deben retrasarse más de 500ms
- Control de congestión
    - Cuando se pierde paquetes en Internet, la mayoría de las veces se debe a un problema de congestión en algún punto de la red:
        - El router no puede procesar y reexpedir paquetes al ritmo al que los recibe
        - Cuando el router se satura, empieza a descartar paquetes (incluidas las confirmaciones)
    - El control de la congestión y el ujo son dos mecanismos diferentes
    - El emisor utiliza el ritmo de llegada de confirmaciones para regular el ritmo de envío de segmentos de datos

- Esto se implementa mediante la ventana de congestión (CW)
  - La ventana de congestión es complementaria a la ventana de recepción (RW) usada para el control de ujo
  - En una situación de no congestión (sin pérdida o retraso de segmentos) la ventana de congestión alcanza el mismo tamaño que la ventana de recepción (CW=RW)
  - Cuando se produce una situación de congestión el tamaño de CW se va reduciendo progresivamente
  - Cuando la situación de congestión desaparece, el tamaño de CW se va aumentando progresivamente
  - El número máximo de bytes que puede enviar el emisor (AW, Allowed Window) es el mínimo de ambos tamaños de ventana: AW = min { RW, CW}
- La red está sin congestión cuando no se pierden o retrasan segmentos
- La transmisión comienza con un tamaño de ventana de congestión CW = 1
  - El emisor envía un único segmento de tamaño máximo igual a MSS
- A continuación, la CW va aumentando, pasando por tres fases distintas:
  - Fase de arranque lento (slow start)
    - La CW se incrementa en uno por cada segmento enviado y confirmado
    - Esto provoca un crecimiento exponencial (CW = 1, 2, 4, 8, 16, 32, . . .)
    - Esta fase termina cuando el tamaño de CW alcanza un cierto umbral, denominado umbral de arranque lento (STT, Slow Start Threshold)
    - Inicialmente, el valor del STT suele ser de 64 Kbytes
  - Fase de evitación de congestión (congestion avoidance)
    - A partir del STT, la CW se incrementa en 1 cada vez que se envía y se confirma una ventana completa (es decir, CW segmentos)
    - Esto provoca un crecimiento lineal
    - Esta fase termina cuando la CW alcanza el tamaño de la ventana de recepción (RW)
  - Fase constante
    - En esta fase, la CW se mantiene a un valor constante (CW = RW)

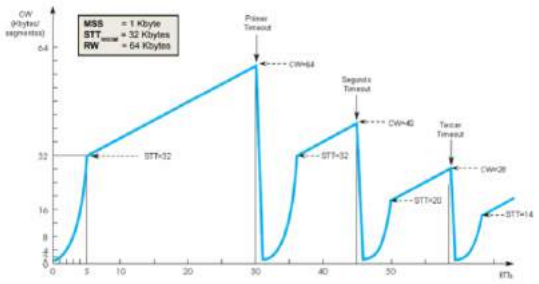
- Expiración de los temporizadores de retransmisión



- Control de congestión
    - La situación de congestión en la red se detecta indirectamente
    - Recepción de 3 ACKs duplicados
        - Nivel de congestión leve, sigue habiendo tráfico en la red (llegan las confirmaciones)
        - Se activa el método de recuperación rápida (fast recovery):
            - Dividir el valor de CW a la mitad
            - Ejecutar el método de evitación de colisiones a partir de ese valor de CW



    - Expiración del temporizador de retransmisión (timeout)
        - Nivel de congestión elevado, se interpreta que el tráfico en la red está interrumpido (no llegan confirmaciones)
        - En este caso se realizan las siguientes acciones:
            - Inicializar el tamaño de la ventana de congestión a CW = 1
            - Reducir el umbral de arranque lento (STT), fijandolo a la mitad del valor que tenía la CW antes de producirse el timeout
            - Ejecutar el método de arranque lento a partir de CW = 1



- Protocolo de datagramas de usuario (UDP)
    - No es orientado a la conexión, el host envía datos sin establecer comunicación con el host destino
    - Los segmentos son enviados como mejor esfuerzo. Si se pierde uno no hay como retransmitir
    - No provee secuenciamiento, si un segmento llega fuera de orden entonces no hay como ponerlo donde corresponde
    - No hay control de ujo
    - RFC 768
    - Ofrece un servicio de datagramas (no orientado a conexión). Cada datagrama enviado es independiente.

    - No buffered, UDP acepta datos y los transmite inmediatamente (siempre que los niveles inferiores se lo permitan)
    - Habitualmente menos del 5-10 % del tráfico total de redes de área local o troncales es UDP. El resto del tráfico es mayoritariamente TCP.
- Características UDP
    - Deficiencias cubiertas por otros niveles de transporte:
        - UDP no es fiable
            - Los paquetes se pueden perder.
            - Los paquetes se pueden entregar fuera de orden.
        - UDP no incorpora mecanismos de control de ujo y congestión
            - La aplicación ha de implementarlos.
            - Si todas las aplicaciones de una red fueran UDP y empezasen a mandar a elevadas tasas, se producirían desbordamientos en las colas de los routers sin ningún tipo de control.
        - UDP ofrece:
            - Multiplexación de aplicaciones gracias al uso de puertos.
            - Checksum del mensaje.
- Cuándo usar UDP
    - La falta de fiabilidad y segmentación supone más tareas para la aplicación.
    - Sin embargo, UDP es:
        - Rápido, no hay fase de establecimiento de conexión.
        - Ligero, supone poca sobrecarga de protocolo (8 bytes).
    - Será por tanto útil para:
        - Aplicaciones de control y gestión.
        - Aplicaciones de difusión.
        - Aplicaciones de tiempo real.
    - Aplicaciones de control y gestión
        - Requieren normalmente poco intercambio de información, del tipo petición-respuesta.
        - Los paquetes son pequeños. Dependiendo de la aplicación pueden generarse en gran número.
        - UDP evita el coste de apertura y cierre de conexiones TCP.
    - Aplicaciones de difusión
        - Necesiten usar direcciones destino Multicast o Broadcast.
        - Con TCP no es posible.
    - Aplicaciones de tiempo real
        - Necesitan un control absoluto de los paquetes generados en la red, por ejemplo, del espaciado entre paquetes.
        - El retardo extremo a extremo y el jitter son importantes.
            - El buffer en recepción permite ocultar parte del retardo y jitter.
        - Pequeñas pérdidas de paquetes son tolerables.
            - Algunas de estas pérdidas pueden ser ocultadas por los codecs.
        - Ejemplos:
            - Aplicaciones de voz sobre IP (VoIP).
            - Transmisión de audio/video en tiempo real (la aplicación es la encargada del control de la comunicación casi en su totalidad). Streaming.

- Comparando TCP y UDP
    - TCP provee más características que UDP, pero el costo es aumento en el gasto de recursos
    - Para aplicaciones que requieren comunicaciones confiables , TCP es confiable
    - Para aplicaciones como voz y video, UDP se prefiere
    - Hay algunas aplicaciones que usan UDP, pero proveen confiabilidad dentro de la aplicación misma
- Algunos número de puertos

FTP datos 20, FTP control 21, SSH 22, Telnet 23, SMTP 25, HTTP 80, POP3 110, HTTPS 443, DHCP Server 67, DHCP client 68, TFTP 69, SNMP agent 161, SNMP manager 162, Syslog 514, *DNS 53* **TCP**/UDP/*ambos*

Resumen:

- Usamos multiplexación cuando usamos el mismo puerto, necesitamos un dato más para diferenciar.
- PDU -> C. Transporte (segmento) , C. red (paquetes), C. Enlace (tramas), C. Física (bits)
- MMS: Tamaño máximo de segmento, MTU: Unidad máxima de transferencia
- Es un puerto conocido por IANA: **1010**
- De acuerdo a IANA, el rango de puertos que un *host debe seleccionar* para el número de puerto origen de la capa de transporte es el **efimero**
- Características de TCP y no de UDP: Recuperación de errores

Border Gateway Protocol - BGP

- Por qué Inter vs Intra
    - Porque no usar OSPF en todo lugar ya que tiene jerarquías de Áreas OSPF
    - El escalamiento no es la unica limitacion
    - BGP es una política de control y un protocolo que oculta información, lo que es intra se puede confiar en comparación con inter que no es confiable
- Por qué estudiar BGP
    - Protocolo crítico: hace que exista internet
    - Problemas relacionados
        - Eficiencia
        - Partición de internet
- Border Gateway Protocol (BGP)
    - Es un EGP
    - Es de tipo Camino Vector
    - Tres versiones
        - BGPv2: usado para IPv4
        - BGPv3: usado para IPv6
    - Usa puerto TCP 179
    - Usa dos tipos de distancias administrativas:
        - AD Externo 20
        - AD Interno 200
    - Protocolo de Vector de Caminos
    - Actualizaciones Incrementales
    - Muchas opciones para forzar medidas administrativas (de rutas)
    - Soporta Enrutamiento Inter-Dominio Sin Clases
    - Muy utilizado en la espina dorsal de Internet
    - Sistemas Autónomos
- Protocolo de Vector de Caminos

Define una ruta como la correlación entre un destino y los atributos del camino a dicho destino

- Definiciones
    - Tránsito carga de tráfico sobre la red
    - Interconexión intercambio de información de enrutamiento y tráfico
    - Por Defecto a dónde enviar tráfico cuando no hay una ruta específica en la tabla de enrutamiento
- Zona Libre de Rutas Por Defecto
    - La zona libre de rutas por defecto es una colección de enrutadores que tienen información de enrutamiento específica para cada ruta del resto de Internet, y por tanto no necesitan una ruta por defecto
- Ejemplo de interconexión y tránsito

A y B pueden interconectarse, pero necesitan acuerdos de tránsito con D para que los paquetes desde/hacia C puedan transitar

- Características

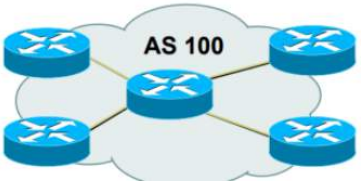
Definido en las siguientes RFC:

  - RFC 4271: describe en general BGP
  - RFC 4893: describe sobre los sistemas autónomos
  - RFC 2858: describe sobre las familias de direccionamiento usados en BGP

Trabaja con extensiones por protocolo (Address-family)

  - Las extensiones son usadas para transportar múltiples protocolos como
  - IPv4,IPv6, Multicast, MPLS VPNv4 o L2VPN
  - Utiliza atributos por cada prefijo y basado en esto se determina el mejor camino
  - Necesita un sistema autónomo (público o privado)
  - Utiliza un identificador de router
  - Necesita de un protocolo interno IGP para sesiones internas: transporte de loopback de vecindades BGP y prefijos internos
  -

- Terminología
  - External BGP (eBGP): Adyacencias BGP que cruzan las fronteras de sistema autónomo
  - Internal BGP (iBGP): Adyacencias formadas de un mismo AS
  - Sincronización: Una ruta debe ser conocida por un IGP antes de ser publicada a pares BGP
  - Tabla de vecinos: Lista de todos los vecinos/peers de BGP
  - Tabla BGP: Contiene todas las redes aprendidas por cada vecino y los atributos BGP para cada prefijo
  - BGP RIB: Base de datos que almacena información de todos los peers antes de modificar o agregar atributos y filtros
  - IP RIB: Base de datos del router que almacena todas las rutas
- Sistemas Autónomos (AS)



  - Colección de redes bajo la misma política de enrutamiento
  - Con un mismo protocolo de enrutamiento
  - Usualmente bajo un mismo propietario y control administrativo
  - Identificado por un único número, conocido como Número de Sistema Autónomo (ASN)

Clasificación

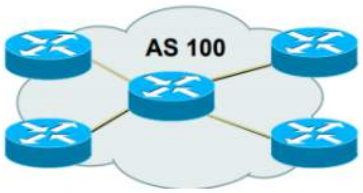
  - Stub AS: se conecta solo a un AS (ISP), generalmente es la conexión hacia internet

    - Multihomed AS: se conecta a dos o más AS como redundancia hacia internet ISP
    - Transit AS: conexión a través del mismo AS hacia otras redes
- Tipos de presentación de AS
    - AS de 2 byte (1-65535)
        - Rango publico: 1- 64511
        - Rango privado: 64512-65535
    - AS de 4 byte
        - Reservado para compatibilidad : 23456
        - Nuevos atributos: AS4 Path, AS4 aggregator
    - Asplain: (default) la escritura decimal de los AS
    - Asdot: escritura en notación punto X.Y. Para ellos se divide el número de sistema autónomo entre 65536, y X corresponde al cociente, y Y al residuo
- ¿ Quién asigna a los sistemas autónomos ?

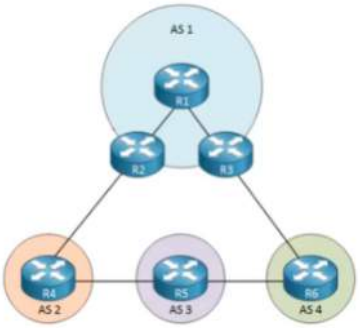
La IANA asigna los AS a través de los registros regionales de internet (RIR)

- Zona de demarcación

Es la Red compartida entre uno o más AS

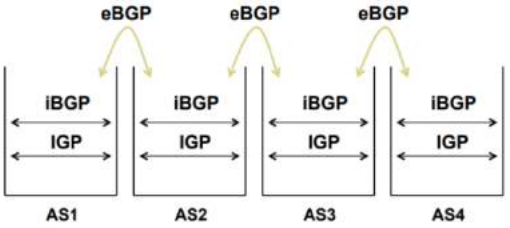


- Operación en BGP
    1. Acumula múltiples caminos de BGP anunciadas por routers internos y externos
    2. Escoge el mejor camino para cada prefijo de red anunciada, y la instala en la tabla de reenvío
    3. El mejor camino su vez se envía a los routers BGP vecinos
    4. Las políticas se aplican modificando la selección de la mejor camino (Paso 2)
- Sesiones de eBGP
    - Un router no puede recibir prefijos que tenga su propio AS de un vecino eBGP.



    - eBGP se usa para intercambiar prefijos con otros ASes

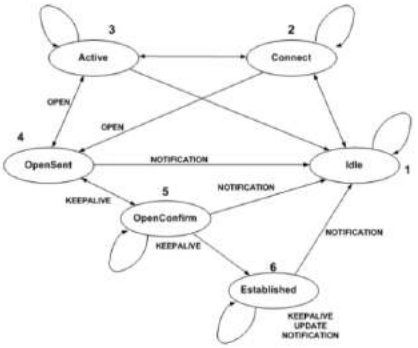
    - eBGP se usa para implementar políticas (reglas) de enrutamiento
    - Un router no puede anunciar prefijos recibidos de un vecino iBGP hacia otro vecino iBGP
    - Las sesiones iBGP requiere de un fullmesh para evitar loops
- Modelo BGP/IGP usado en redes de proveedores (ISP)



- Tipos de mensajes BGP
    - Open: intercambio básica de cada peer
    - Update: información de nuevos prefijos o prefijos que deben eliminarse
    - Notification: notificación de errores
    - KeepAlive: mantener las conexiones entre peer vivas
- Tipos de estado de un vecino

Tipo	Descripcion
Idle	Esta buscando el vecino, inicio de conexion TCP
Connect	La sesion TCP fue completada
Open sent	Comparacion de mensajes open
Open confirm	El vecino confirma el inicio
Established	La vecindad se completo

- Máquina de estado finito



- Distancia administrativa de protocolos

Protocolo	Distancia
Directamente Conectada	0
Estática	1
eBGP	20
EIGRP (Interno)	90
IGRP	100
OSPF	110
ISIS	115
RIP	120
EGP	140
EIGRP (Externo)	170
iBGP	200
BGP Local	200
Desconocido	255

- Resultados deseados

Implementación de políticas de enrutamiento que sean:

- Escalable
- Estable
- Simple

Necesitas escalar tu IGP

- Eres un cliente con dos conexiones a ISPs
- Necesitas transitar todas las rutas en Internet
- Necesitas implementar una política de enrutamiento, o expandir las
- políticas de QoS

- Clasificación de atributos: 4 categorías

Tipo	Descripcion
Well-known mandatory (WKM)	▪ Atributo que todos los routers deben soportar y comprender. ▪ Siempre debe ser enviado a los vecinos
Well-known Discretionary (WKD)	▪ Atributo que todos los routers deben soportar y comprender ▪ El envio de este hacias los vecinos es opcional
Optional transitive (OT)	▪ Este puede ser comprendido o no por el router local ▪ Siempre debe ser enviado a los vecinos
Optional Nontransitive (ONT)	▪ Atributo opcional ▪ No es reenviado si no se reconoce localmente

- Atributos en cada categoría

WKM	WKD	OT	ONT
▪ AS-Path ▪ Next-hop ▪ Origin	▪ Local preference ▪ Atomic aggregate	▪ Aggregator ▪ Community	▪ Originator ID ▪ Cluster ID ▪ Multiple Exit Discriminator

- Descripción de los atributos

Atributo	Descripcion
AS-Path	Lista los sistemas autonomos que deben ser atravesados para llegar al prefijo
Next-hop	Direccion IP del router que esta publica el prefijo
Origin	Determina si el prefijo fue publicado con el comando Network por EGP o fue redistribuido
Local preference	Valor numerico de significado local, se prefiere el valor mayor (100 por defecto para eBGP)
Atomic aggregate	Determina si un prefijo fue sumarizado
Aggregator	Identifica el router que genero el prefijo sumarizado
Community	Etique que determina una restriccion de reenvio para el prefijo
Originator ID	Indica el ID del router iBGP que publica el prefijo en escenario de router-reflector como prevencion de loop

Atributo	Descripcion
ClusterID	Indica el ID de router RR que publica el prefijo en escenarios de multiples RR como prevencion de loop
MED	Agrega la metrica IGP a los prefijos y poder ser publicada y manipulada para los prefijos externos

- Atributos de Cisco

Atributo	Descripcion
Weight	Atributo propietario de Cisco. Valor numerico de significado local, se prefiere el mayor valor (default 32,768 para el peer eBGP)

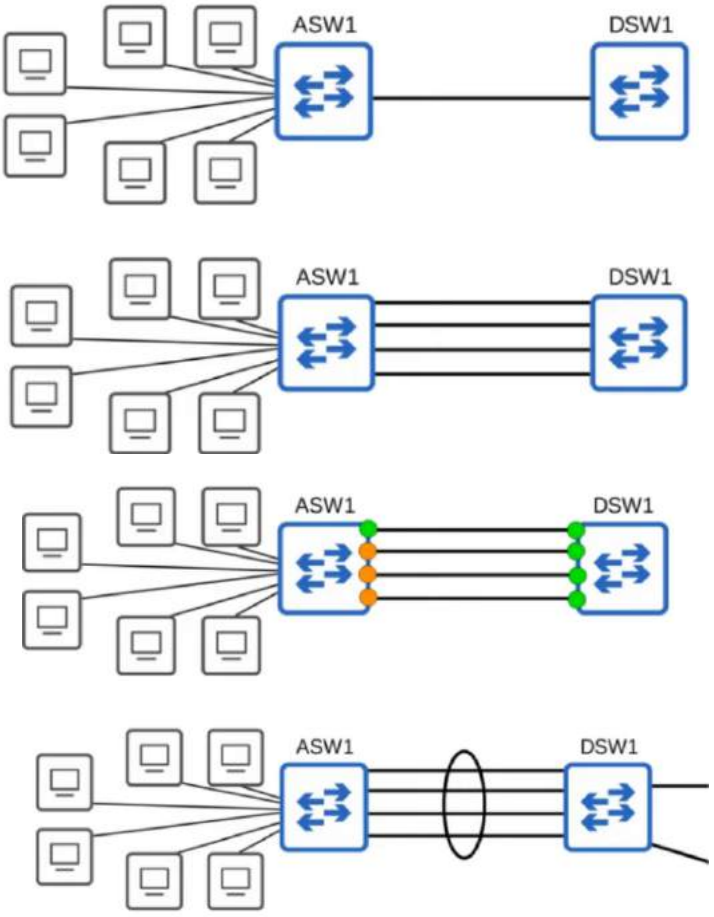
- Selección de la mejor ruta
    - Ignora todas las rutas con un siguiente salto inaccesible
    - Prefiere las rutas con el mayor weight
    - Prefiere las rutas con el mayor local- preference
    - Prefiere las rutas con Local originated(directamente conectadas)
    - Prefiere las rutas con el menor AS-Path
    - Prefiere las rutas con el menor Origin
    - Prefiere las rutas con el menor MED
    - Prefiere las rutas de vecinos eBGP sobre iBGP
    - Prefiere las rutas con la métrica IGP más baja hacia el BGP Next -hop
    - Prefiere las rutas eBGP más vieja
    - Prefiere la ruta que tenga el vecino BGP con el menor router-id
    - Prefiere la ruta que tenga el vecino con la dirección IP más baja
- Configurar BGP en Cisco IOS
    - Esta instrucción activa BGP en IOS: router bgp 100
    - Para ASNs mayores a 65535, el número de AS puede ser especificado en formato simple o dot: router bgp 131076 o router bgp 2.4
    - IOS muestra el ASN en formato simple por defecto.

Protocolo de Enrutamiento dinámico

- Congestión de red

Una excesiva cantidad de paquetes almacenados en los buffers de varios nodos en espera de ser transmitidos. En donde la congestión es indeseable porque aumenta los tiempos de viaje de los paquetes y retrasa la comunicación entre usuarios.

- Etherchannel



- Etherchannel

Tecnología de Cisco construida en base a los estándares 802.3 full-duplex Fast Ethernet

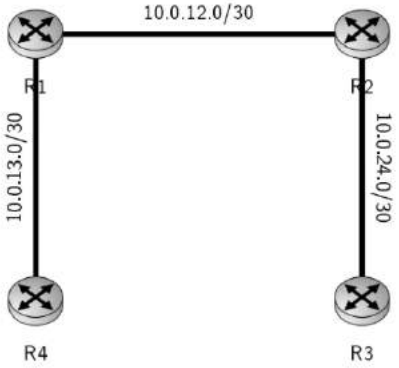
  - Permite la agrupación de varios enlaces físicos Ethernet en una interfaz lógica,
  - Esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.
  - STP lo va a tratar como una única interfaz
  - Funciona a nivel de capa 2 y capa 3

- Balanceo de carga
  - Permite al dispositivo dividir el tráfico entrante y saliente en varias interfaces para reducir la congestión de la red.
  - Mejora la utilización de varias rutas de red y proporciona un ancho de banda de red más eficaz.

Etherchannel tiene algoritmos para balanceo de carga que pueden ser por:

  - origen-destino IP

    - origen MAC
    - destino MAC
    - origen-destino MAC
    - origen IP
    - destino IP
- Enrutamiento

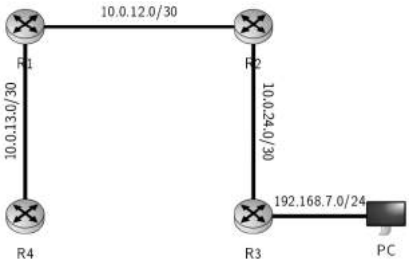


- Protocolo de Enrutamiento Dinámico
    - Es un lenguaje que un ruteador habla con otros ruteadores a fin de compartir informaciones sobre:
        - Alcanzabilidad
        - Estados de la red
    - Son usados desde finales de los años 80.
    - Las versiones más recientes soportan comunicación con base IPv6
- Componentes principales de los protocolos de enrutamiento dinámico
    - Estructura de datos: Usan tablas o bases de datos para sus operaciones. Estas son mantenidas en la RAM
    - Mensajes de enrutamiento de protocolos: se usa diferentes tipos de mensajes para descubrir routers vecinos, intercambiar informaciones de enrutamiento
    - Algoritmo: para determinar el mejor camino
- Características de un algoritmo de enrutamiento dinámico
    - Procedimiento para pasar y recibir información de alcanzabilidad de redes a otros ruteadores.
    - Procedimiento para determinar las rutas óptimas
    - Procedimiento para reaccionar, compensar y propagar cambios de topología en una red.
- Factores que consideran un algoritmo de enrutamiento
    - Métrica: Número de saltos, Ancho de banda, Costo, Retardo
    - Balance de carga
    - Alcanzabilidad
    - Convergencia : todos los tablas contienen la misma información de la red
- Principales categorías de protocolos de enrutamiento dinámico
    - IGP (Interior Gateway Protocol): usado para compartir enrutamientos dentro de un sistema autónomo, por ejemplo la red de una compañía
    - EGP (Exterior Gateway Protocol): usado para compartir enrutamientos entre diferentes sistemas autónomos
- Clasificación de los protocolos de enrutamiento dinámico

- Clases de Algoritmos de Enrutamiento Dinámico
    - Vector distancia
        - Basados en los trabajos de E. Bellman, Ford y Fulkerson.
        - Comparte lo que sabe pero solo con los vecinos
        - RIP v1/v2, IGRP, EIGRP
    - Estado enlace
        - Basado en los trabajos de Dijkstra
        - Cada nodo tiene un mapa topológico de toda la red, incluye todos los nodos y el costo de los enlaces
        - OSPF v2/v3, ISIS
    - Vector camino
        - Mantiene información del camino que se actualiza dinámicamente
        - BGP
- Protocolos de Enrutamiento Vector distancia
    - Inventados antes de los estados enlace
    - RIPv1
    - Protocolo de cisco IGRP
    - Operan enviando a sus vecinos conectados las redes que ellos conocen y las métricas para alcanzarlas
    - Este método de compartir información es conocido como enrutamiento por rumor
    - Esto es porque el router no conoce las redes que estan mas alla de sus vecinos, solo conoce lo que sus vecinos saben
    - Se llaman vector distancia porque los routers solo aprenden la distancia (métrica) y vector (dirección del siguiente salto) de cada router

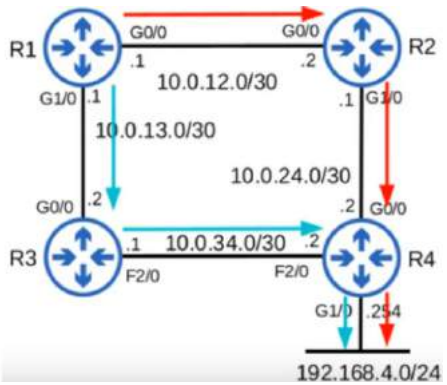
  Características de los protocolos vector distancia
    - Actualizaciones periódicas
    - Vecinos
    - Actualizaciones de broadcast
    - Toda la tabla de enrutamiento se incluye en la actualización de enrutamiento

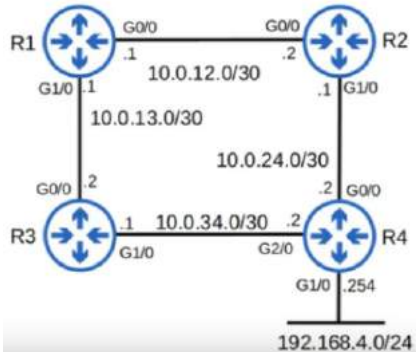
  Ejemplo:



- Protocolos de enrutamiento estado enlace
    - En este protocolo, cada router crea un mapa de conectividad de la red
    - Para esto, cada router comunica información sobre sus interfaces a sus
    - vecinos. Esta información compartida con sus vecinos se comparten con otros routers, hasta que todos desarrollen el mapa
    - Cada router independientemente uso este mapa para calcular las mejores rutas para cada destino
    - Los protocolos estado enlace usan más recursos de CPU en el router porque la cantidad de información que comparten es grande

    - Sin embargo, son rápidos para adaptarse a cambios en la red que los vectores distancia
- Métricas de los protocolos de enrutamiento dinámico
    - Si un router usando un protocolo de enrutamiento dinámico aprende dos diferentes rutas para el mismo destino, ¿cómo debería elegir para tener la mejor ruta?
    - El router usa el valor de la métrica de las rutas para determinar la mejor ruta. Una menor valor en la métrica es la de preferencia





Si el router conoce dos rutas que tienen la misma métrica al mismo destino usando mismo protocolo de enrutamiento dinámico, ambas rutas se agregan a la tabla de enrutamiento. El traco va a ser balanceado en ambas rutas.

- ECMP
    - Equal Cost Multi Path: es un protocolo de enrutamiento y sólo está disponible en los routers Linux
    - ECMP es un algoritmo para enrutamiento de datos a través de una red donde existen dos o más rutas de igual mérito para enviar datos sobre su próximo salto a través de una red.
    - RIPv2, ISIS, y OSPF usan ECMP
- Métricas de los protocolos de enrutamiento dinámico

IGP	Metrica	Explicacion
RIP	Cuento de saltos	Cada router en la ruta cuenta como un salto. La metrica total es el numero total de saltos al destino
EIGRP	Basado en ancho de banda y retraso (delay)	Formula compleja que tiene muchos parametros. Uno de ellos es el ancho de banda y el delay de los enlaces
OSFP	Costo	El costo de cada enlace es calculado con el ancho de banda
ISIS	Costo	El costo de cada enlace es de 10 por defecto

- Distancia administrativa por defecto

Conectado directamente	0
Estatica	1
eBGP	20
EIGRP	90
IGRP	100
OSPF	110

ISIS	115
RIP	120
external EIGRP	170
IGRP	100
internal BGP	200
Ruta no usada	255

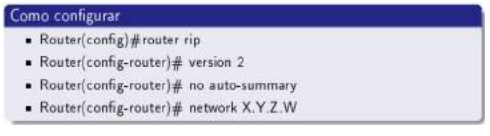
- Routing Information Protocol (RIP)
    - Tiene tres versiones
        - RIPv1 y RIPv2 para IPv4
        - RIPng para IPv6
    - Máximo número de saltos es 15
    - Usa dos tipos de mensajes
        - Request: pregunta si el vecino usa RIP para enviarle su tabla de enrutamiento
        - Response: Envía la tabla de enrutamiento local a sus vecinos

Ventajas de RIP
- Es fácil de configurar (comparado con otros protocolos)
- Es abierto (admite versiones derivadas aunque no necesariamente compatibles)
- Está soportado por la mayoría de los fabricantes

Desventajas de RIP
- Para determinar mejor métrica sólo tiene en cuenta el número de saltos (congestión, etc)
- No diseñado para resolver cualquier problema de enrutamiento
- Coste máximo permitido 16 (red inalcanzable) inadecuado para redes grandes
- No soporta máscaras de subred de tamaño variable
- Carece de servicio para garantizar que las actualizaciones proceden de routers autorizados (inseguro)
- Sólo usa métricas jas para comparar rutas alternativas (no apropiado para situaciones en la que las rutas han de elegirse basándose en parámetros de tiempo real, retardo, habilidad de la carga, etc)

RIPv1
- Solo avisa las direcciones classful
- No soporta VLSM CIDR
- No incluye información de la máscara de subred
- Mensajes broadcast al 255.255.255.255

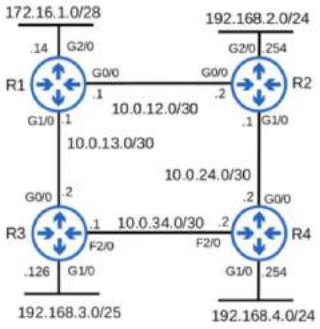
RIPv2
- Soporta VLSM CIDR
- Incluye información de la máscara de subred mensajes son multicast a 224.0.0.9
- RIP convierte automáticamente a redes Classful y por eso no es necesario poner la máscara de red



El comando network

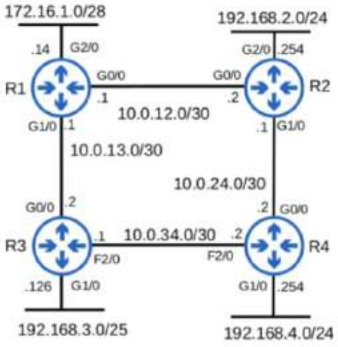
- Indica al router que busque interfaces con una dirección IP que está en el rango especificado
- Indica al router que active RIP en las interfaces que están en el rango forma adyacencias con los vecinos que usan RIP
- OSPF y EIGRP tienen el mismo comando y operan en una manera similar

Ejemplo

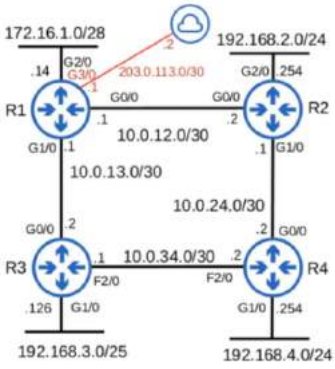


Explique que hace

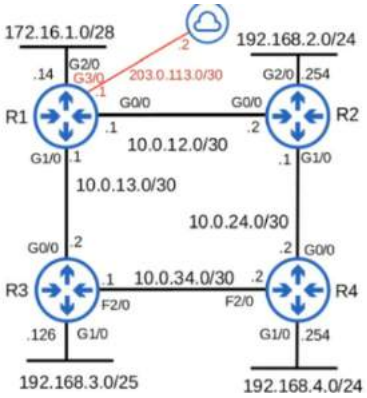
- network 10.0.0.0
- network 172.16.0.0



Aunque no hay vecinos RIP conectados a G2/0, R1 va a continuar enviando avisos RIP fuera de G2/0. Esto es trafico innecesario, entonces G2/0 deberia ser configurado como **passive interface G2/0**



Como haria para notificar la existencia de un router por 203.0.113.2



Con el comando **default-information originate**

- Enhanced Gateway Routing Protocol (EIGRP)
    - Al incio propietario de Cisco, pero ahora es libre
    - Es un protocolo híbrido de vector distancia
    - Más rápida adaptación que RIP a cambios de la red
    - No tiene el límite de 15 saltos
    - Envia mensajes multicast a la direccion 224.0.0.10
    - Es la única IGP que puede hacer un balanceo de carga con desigual costo (unequal cost)
    - Usa el algoritmo DUAL
- Algoritmo DUAL

Mecanismo de recálculo de rutas para el protocolo EIGRP. Para DUAL, los ciclos (incluyendo los temporales) en las rutas son perjudiciales para el desempeño de una intranet. DUAL utiliza diffusing computations (propuesto por E.W. Dijkstra y C.S Scholten) con el fin de poder llevar a cabo un enrutamiento distribuido de distancias más cortas evitando los ciclos a toda costa.

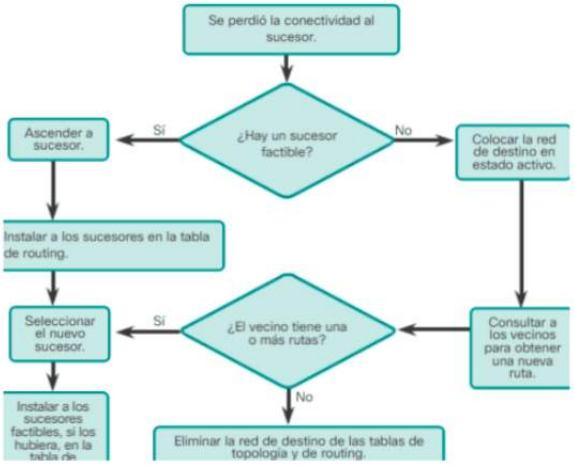
Proporciona:

- Rutas sin bucles
- Rutas de respaldo sin bucles que se pueden utilizar inmediatamente
- Convergencia rápida
- Mínimo uso de ancho de banda con actualizaciones limitadas

Condiciones que sean cumplidas para usar DUAL

- Un nodo debe detectar en un tiempo nito la existencia de un nuevo vecino o la pérdida de conectividad con un vecino.
- Todos los mensajes transmitidos sobre un enlace son recibidos de forma correcta y en la secuencia apropiada en un tiempo finito.
- Todos los mensajes, cambios en el costo de un enlace, fallas de enlaces o notificaciones de nuevos vecinos deben ser procesados uno a la vez
- en un tiempo nito y en el orden que hayan sido detectados.

Máquina de estados finito DUAL



- Comandos para configurar EIGRP

```
Router(config)#router eigrp 1
Router(config-router)# no auto-summary
Router(config-router)# passive-interface g2/0
Router(config-router)# network X.Y.Z.W
Router(config-router)# network X.Y.Z.W A.B.C.D
```

Al costado de EIGRP se debe especificar el número de sistema autónomo
para que compartan información. A.B.C.D es una máscara wildcard

- Máscara wildcard
    - Es una máscara de subred invertida
    - Todos los unos se convierten en cero, y viceversa.
    - De 255.0.0.0 su wildcard es 0.255.255.255
    - De 255.255.255.240 su wildcard 0.0.0.15
    - 255.252.0.0 su wildcard es ?
- EIGRP usa mascara wildcard
    - Si es 0 los debe ser idéntico
    - Si es 1 no es necesario que sea idéntico
    - R1 G2/0 Direccion IP 172.16.1.14
    - EIGRP en su network command pone la direcion 172.16.1.0
    - Es que EGIRP se activa en G2/0
- Router ID en EIGRP
  Se utiliza para identificar de forma única a cada router en el dominio de enrutamiento EIGRP.
  El valor puede ser por:
    - Configuración manual
    - La dirección IP de mayor valor en su interfaz loopback
    - La dirección IP de mayor valor en su interfaz que no es loopback

Resumen y ejercicios:

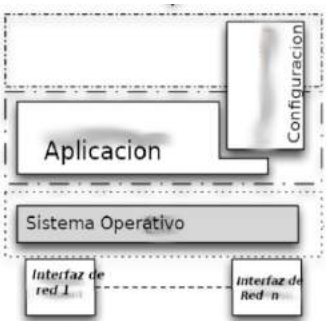
- R1 y R2 ambas usan RIP para compartir rutas. R1 tiene un ruta por defecto a internet que tu quieres advertir a R2. ¿Qué comando usarías?
    - **R1(config-router) # default-information originate**
    - R1(config-router) # network 203.0.113.0
    - R2(config) # ip route 0.0.0.0 0.0.0.0 10.0.12.1
    - R2(config-router) # default-information originate
- R1 G1/0 interface tiene una dirección IP de 172.20.20.17 y su interfaz G2/0 tiene una dirección IP 172.26.20.12. Cual de los siguientes comandos activaría EIGRP en ambas interfaces
    - **R1(config-router) # network 128.0.0.0 127.255.255.255**
    - R1(config-router) # network 172.16.0.0 0.0.255.255
    - R1(config-router) # network 172.20.0.0 0.0.127.255
    - R1(config-router) # network 172.20.0.0 0.3.255.255

Enrutamiento Estático

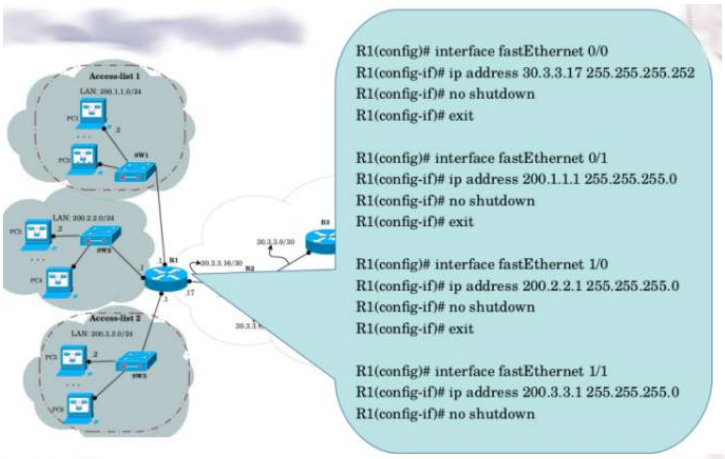
- Switches multicapa
    - Dispositivo que permite la combinación de la conmutación tradicional de capa 2 con la operación de enrutamiento de capa 3 en un solo dispositivo, mediante acciones de hardware de alta velocidad
    - Los switches multilayer son más rápidos y baratos que los routers.
- Routers
    - Dispositivo de capa 3 que toma decisiones basadas en direcciones de red. Estos utilizan tablas de enrutamiento para almacenar estas direcciones de capa 3.
    - Su función es elegir el mejor camino para enviar los datos a su destino y enrutar los paquetes al puerto de salida adecuado. Dan acceso a redes (WAN), la cuales están destinadas a comunicar o enlazar LANs
    - Principales marcas: Cisco, Juniper, Huawei

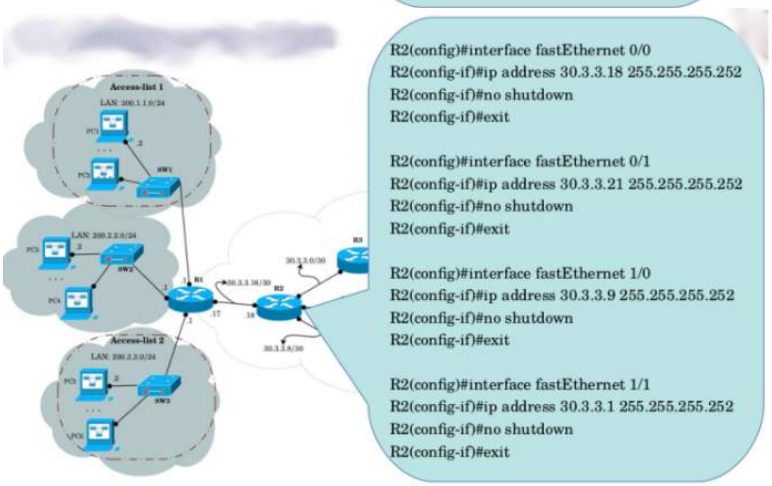
Configuración interna de un router

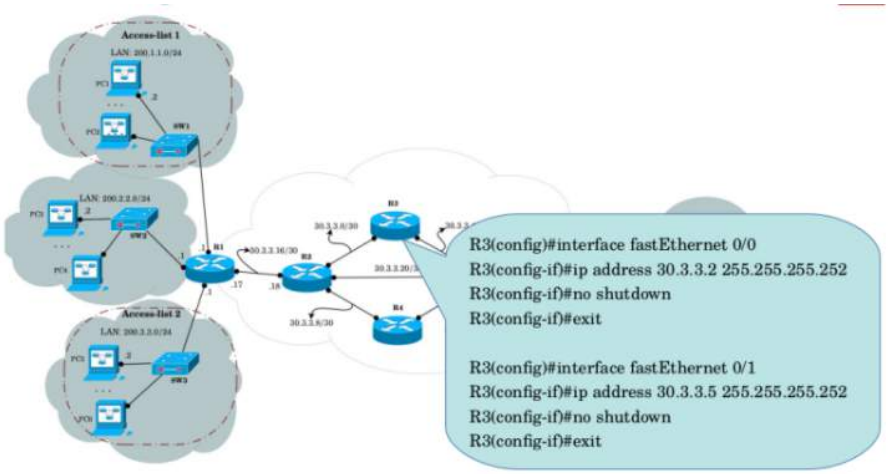
- Se distingue de los otros dispositivos de conexión como los puentes, hubs y switches por el hecho de que tiene un procesador, un sistema operativo y memoria.



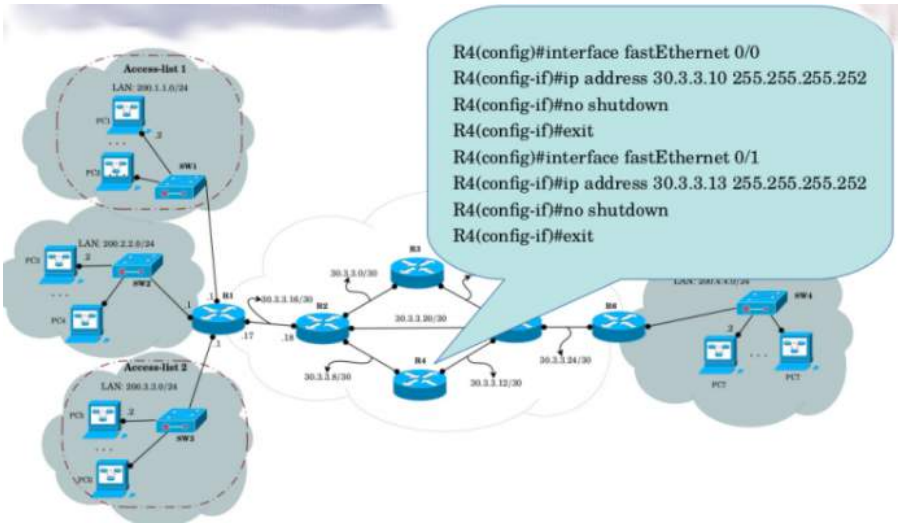
Configuración de routers





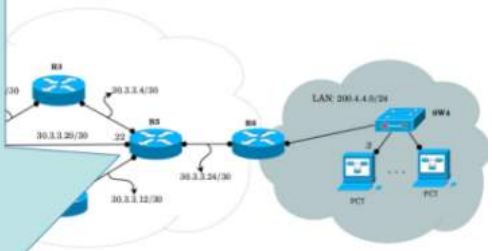



```
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip address 30.3.3.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit

R3(config)#interface fastEthernet 0/1
R3(config-if)#ip address 30.3.3.5 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
```

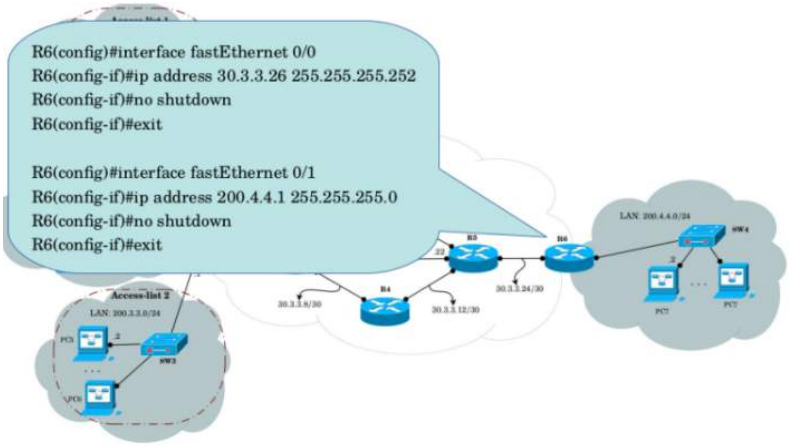



```
R4(config)#interface fastEthernet 0/0
R4(config-if)#ip address 30.3.3.10 255.255.255.252
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface fastEthernet 0/1
R4(config-if)#ip address 30.3.3.13 255.255.255.252
R4(config-if)#no shutdown
R4(config-if)#exit
```

```
R5(config)#interface fastEthernet 0/0
R5(config-if)#ip address 30.3.3.14 255.255.255.252
R5(config-if)#no shutdown
R5(config-if)#exit

R5(config)#interface fastEthernet 0/1
R5(config-if)#ip address 30.3.3.6 255.255.255.252
R5(config-if)#no shutdown
R5(config-if)#exit

R5(config)#interface fastEthernet 1/0
R5(config-if)#ip address 30.3.3.25 255.255.255.252
R5(config-if)#no shutdown
R5(config-if)#exit

R5(config)#interface fastEthernet 1/1
R5(config-if)#ip address 30.3.3.22 255.255.255.252
R5(config-if)#no shutdown
```




```
R6(config)#interface fastEthernet 0/0
R6(config-if)#ip address 30.3.3.26 255.255.255.252
R6(config-if)#no shutdown
R6(config-if)#exit

R6(config)#interface fastEthernet 0/1
R6(config-if)#ip address 200.4.4.1 255.255.255.0
R6(config-if)#no shutdown
R6(config-if)#exit
```



- Enrutamiento IP
    - Proceso de escoger los caminos por los cuales los paquetes son transmitidos al host destino.
    - Proceso basado sobre una tabla de enrutamiento que contiene la información relativa a los diferentes destinos posibles y a la manera de alcanzarlos.

A recordar:

- El emisor no conoce la ruta completa pero la dirección del siguiente nodo IP que lo acercara al destino
- Mantener la simplicidad de las tablas de enrutamiento
- Poder realizar cambios debido a fallas eventuales

- Nociones básicas
    - Camino en la red
        - Conjunto de enlaces y nodos intermediarios a recorrer para llegar de un origen a un destino en la red.
    - Tabla de enrutamiento
      Tabla que asocia para cada destino conocido, el salto próximo a utilizar. El destino puede ser especificado bien por su IP o prefijo de red al que pertenece.
      Almacena:
        - Rutas conectadas directamente
        - Rutas remotas

      show ip route
- Enrutamiento IP: algoritmo
    - Extraer del datagrama la dirección IP destino
    - Calcula la dirección de red del destino
    - Si esta dirección corresponde a la dirección de red de la LAN, entonces
        - La dirección destino es accesible
        - La capa de red intenta la traduccion de la direccion logica de la IP destino en una dirección sica a través de la tabla mantenida en la caché
        - Si la red es de tipo Ethernet, el protocolo ARP es utilizado en caso no tuviera las entradas en la tabla de la dirección MAC
    - Caso contrario (no es un host accesible):
        - Si la red de destino está dentro de la tabla entonces
        - Encaminar el datagrama según las indicaciones de la tabla (hacia un otro nodo de la LAN con la resolución de dirección IP- dirección física, o con otro router conectado a una red externa)
        - Caso contrario (que no está en la tabla)
        - Escoger la ruta por defecto indicada en la tabla
        - Enrutar el datagrama según las indicaciones de entrada por defecto de la tabla
- Tabla de Enrutamiento IP en Linux
  La consulta o modificación de la tabla de enrutamiento puede ser hecha con el comando *route* o *ip route*

Ejemplo	
Agregar una ruta por defecto	route add default gw @IPGateway ip route add default via @IPGateway
Agregar una ruta hacia un host	route add -host @IPHost gw @IPGateway dev *iface* ip route add @IPHost via @IPGateway dev *iface*
Agregar una ruta hacia una red	route add -net @IPRed netmask @Mascara dev *iface* gw @IPGateway ip route add @IPRed/@Mascara via @IPGateway dev *iface*

- Linux y enrutamiento
    - Kernel de linux soporta enrutamiento
    - Se requiere activar la funcionalidad de puente en el Kernel
    - Dos modos de activación:
        - Modificar el parámetro que controla la funcionalidad
          echo 1 > /proc/sys/net/ipv4/ip_forward
        - Configurar automáticamente a cada inicio
          net.ipv4.ip_forward=1
          en el chero /etc/systcl.conf
- Diferencias entre routers y gateways

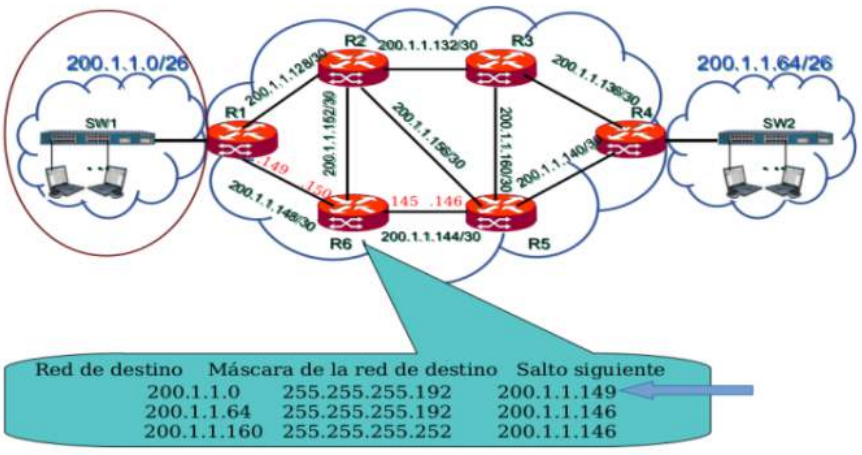
Gateway (pasarela)

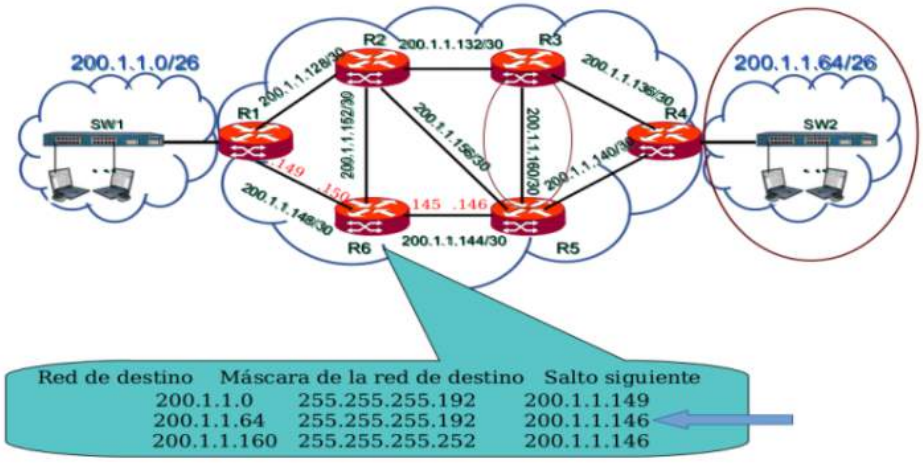
- Puede ser definido como un nodo que actua como el portero de la red
- Es responsable de permitir el trafico en la red
- Usado para comunicarse con redes que tienen diferentes tipos de protocolos y responsable por la conversion de un tipo a otro.
- No soporta enrutamiento dinamico

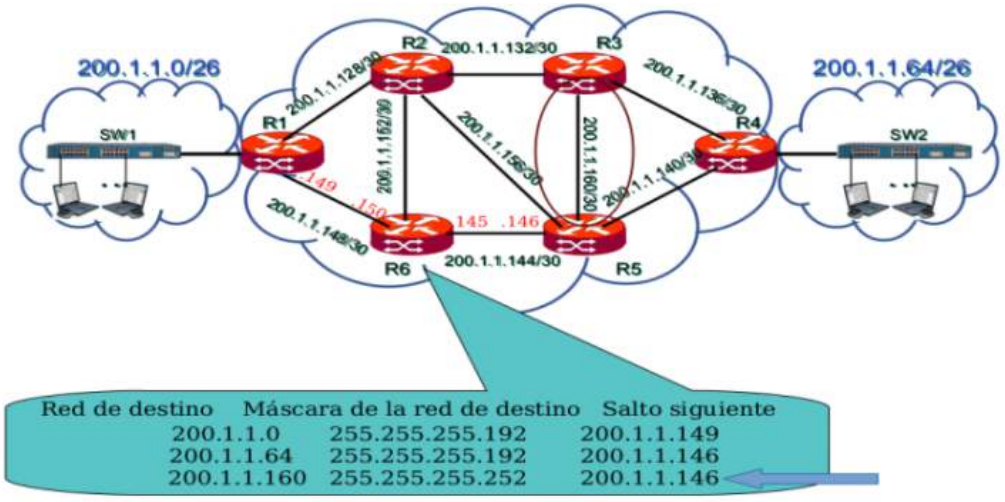
Router

- Dispositivo que conecta dos redes diferentes
- Recibe, analiza, y retransmite paquetes a otras redes
- Soporta enrutamiento dinamico

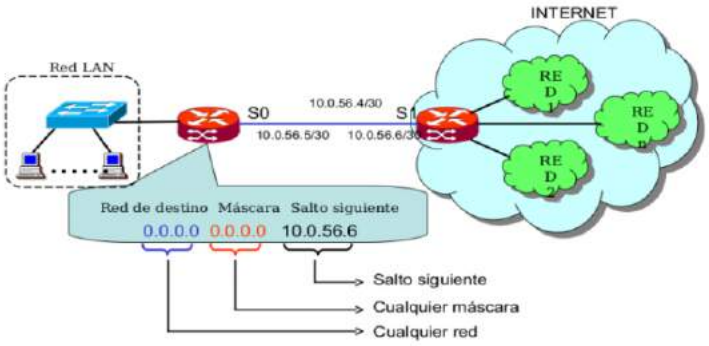
- Clases de Enrutamiento
    - Enrutamiento Estático
        - Ventajas : Simple, menor sobrecarga con respecto al enrutamiento dinámico
        - Desventajas: no escalable y no dinámico
    - Enrutamiento Dinámico
        - Ventajas: Robustez frente a fallos
        - Desventajas:
            - Crean tráfico extra en la red
            - Posible ocurrencia de iteración de paquetes cuando la información de enrutamiento está siendo intercambiada entre los ruteadores
- Enrutamiento Estático
    - Las informaciones son actualizadas manualmente a cada modificación de la topología
    - Lo define el administrador
    - La red no se adapta a fallas



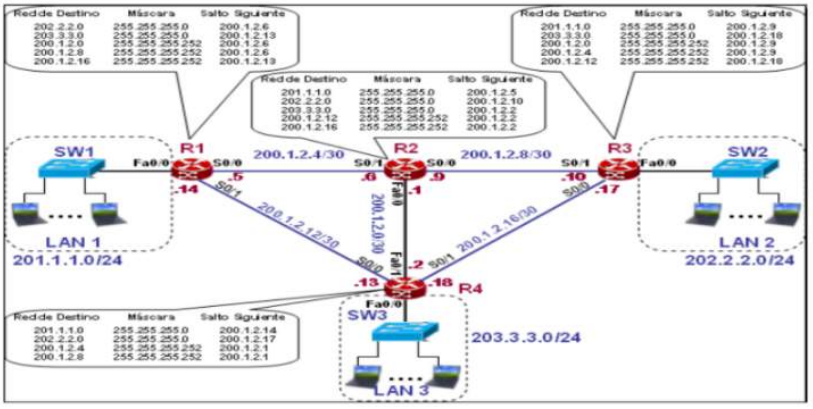




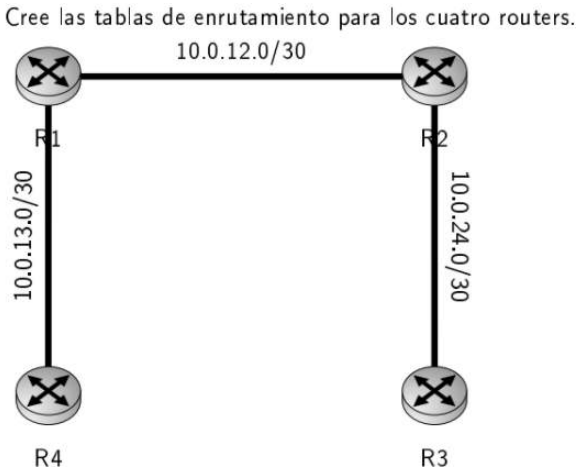
- Enrutamiento estático por defecto



- Ejemplo de tabla de enrutamiento



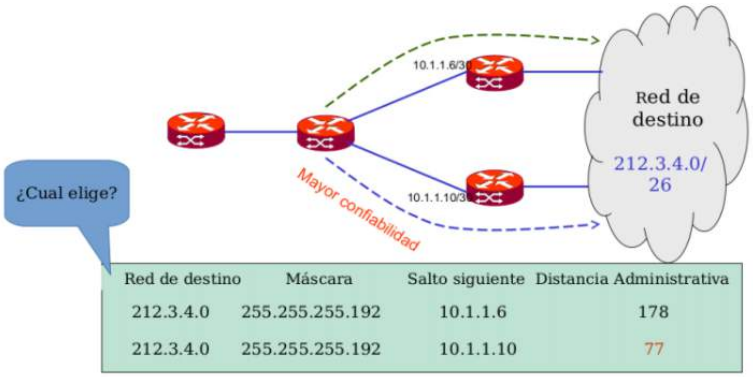
- Ejercicio

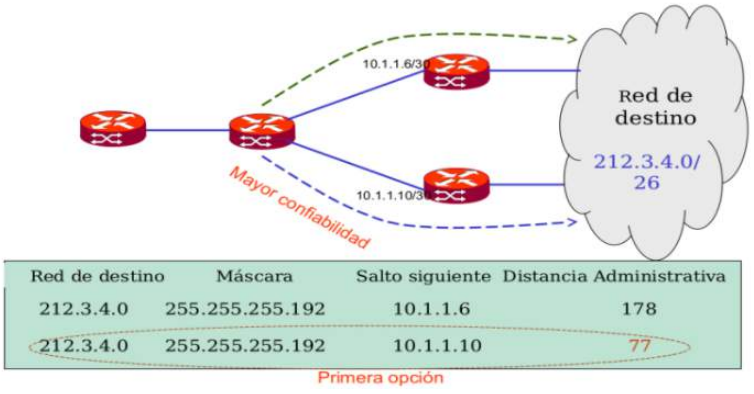


- Distancia administrativa
    - Cada Protocolo tiene una métrica y algoritmo que es diferente de otro protocolo
    - En una red con diferentes protocolos de enrutamiento, el intercambio de información de la ruta y la capacidad para seleccionar el mejor
    - El camino entre los diferentes protocolos es crítico.

¿Cuál es el primer criterio del router para determinar qué protocolo usar cuando dos protocolos proveen la misma información del destino?

- Medida de confianza sobre la información de ruteo. Solo tiene significado local
- Menor distancia administrativa, más confiable es el protocolo
- La distancia puede ser modificada

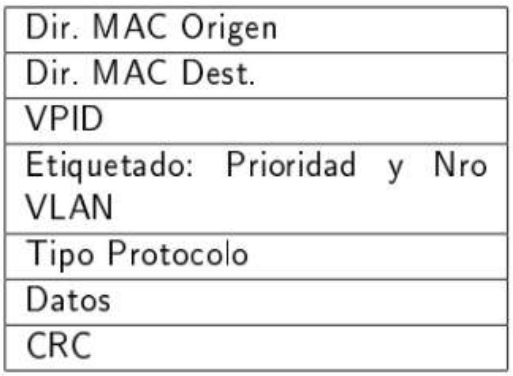




- Listas de control de acceso (ACL)
    - Grupo de sentencias que define como se procesan los paquetes
        - Entran a las interfaces de entrada
        - Se re envían a través del router
        - Salen de las interfaces de salida del router
    - Permite habilitar o denegar el tráfico que paso por los routers
- Tipos de ACL
    - Estándar:
        - Filtra paquete basados en la dirección de origen
        - Son designadas por numeración entre 1-99 y 1300 a 1999.
        - Se configuran lo más cerca del destino
    - Extendida:
        - Se configuran lo más cerca del origen
        - Son designada por numeración entre 100-199 y de 2000-2699
        - Al nal de la sentencia ACL extendida, se puede especificar opcionalmente el número del protocolo TCP o UDP

Spanning Tree Protocol (STP)

- 802.1Q
  - VPID : identifica una trama 802.1Q
  - VID: número de identificación de la VLAN, admite hasta 4096 ID de VLAN
  - Gestión de prioridades: 3 bits posibles

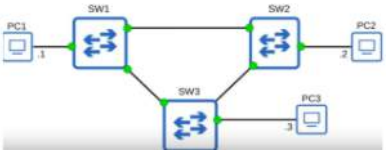


- Definiciones
  - Dominio de colisión
    - Grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado será una colisión entre las dos señales.
    - Mejor es tener muchos dominios de colisión pequeños que pocos y grandes
  - Dominio de difusión (broadcast)
    - Grupo de dispositivos de la red que envían y reciben mensajes de difusión entre ellos.
- VLAN Dinámica (DVLAN)
  - Se puede configurar los puertos automáticamente con la ayuda del etiquetado.
    - La asociación de puertos a las VLANs puede ser con la ayuda del protocolo GVRP
    - Podemos mezclar las asociaciones estáticas (host-switch) y dinámicas (switch-switch)
  - El mayor beneficio de las DVLAN es el mejor trabajo de administración de la red cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

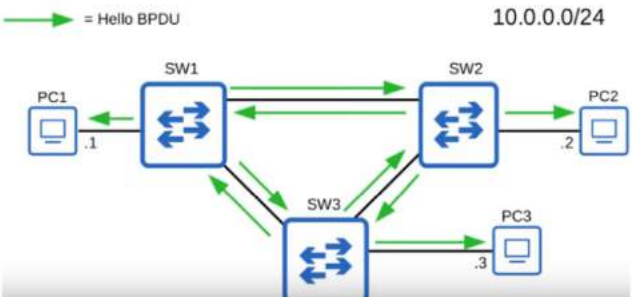
  Ejemplo de DVLAN
  - Asociamos VLAN 1 a los dos hosts y usamos GVRP en los dos hosts y dos switches para comunicarse
  - GVRP va a propagar con la ayuda de una trama particular la pertenencia a esa VLAN en los switches.
  - La información será propagada entre los switches
  - Los puertos de los switches seran automaticamente asociados a la VLAN 1

- STP
  - Switches de todas las compañías implementan STP por defecto

- STP cambia una red física con forma de malla, en la que existen bucles, por una red lógica en un árbol en la que no existe ningún bucle.
- El protocolo clásico es la IEEE 802.1D
- STP previene bucles en la capa 2 a través de puertos redundantes en estado de bloqueo, es decir, deshabilita la interfaz.
- Estas interfaces actúan como backups que pueden pasar a estado de reenvío si una interfaz activa cae.
- Interfaces en estado de bloqueo solo envía o recibe mensajes STP (llamados BPDUs)
- El estado bloqueo deshabilita la conexión en el puerto del switch

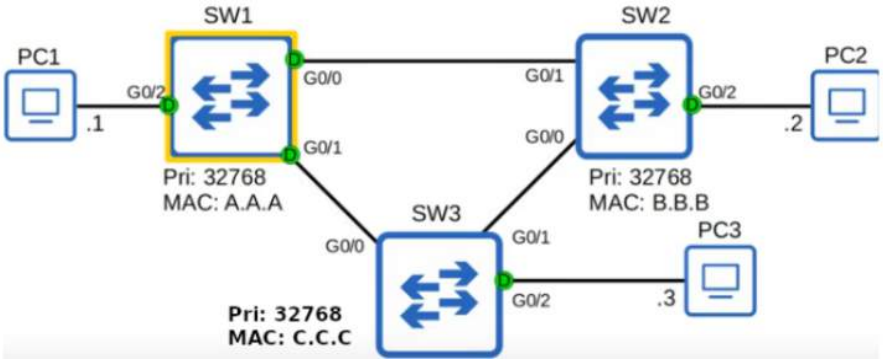


- Por la selección de qué puertos están en estado de reenvío o de bloqueo, STP crea un único camino desde el origen al destino.
- Esto previene la existencia de bucles
- Hay un conjunto de procesos que STP usa para determinar qué puertos deben estar en reenvío o en bloqueo.
- El switch envía/recibe un Hello BPDU a todas las interfaces
- El tiempo límite es dos segundos
- Si el switch recibe un BPDU en una interfaz, conoce que esa interfaz está conectada a un switch, porque los otros dispositivos PC, router no usan STP.



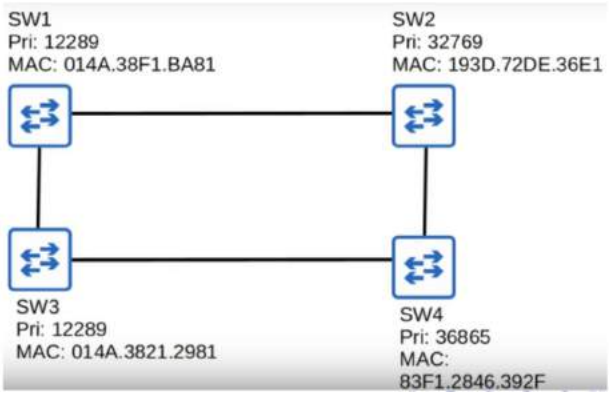
- BPDU: Bridge Protocol Data Units
  - Enviadas periódicamente por los puentes
  - STP usa como MAC destino 01:80:C2:00:00:00 (Bridge Group
  - Address) y PVST de Cisco usa 01:00:0C:CC:CC:CD.
  - No son reenviadas
  - Switches usan un campo en el STP BPDU, el ID puente, para elegir el puente que será la raíz del árbol en la red.
  - El puente raíz es el ID puente con el menor valor.
  - Todos los puertos en el puente raíz son puestos en el estado de reenvío y los otros switches en la topología tiene que tener un camino para alcanzar el puente raíz.

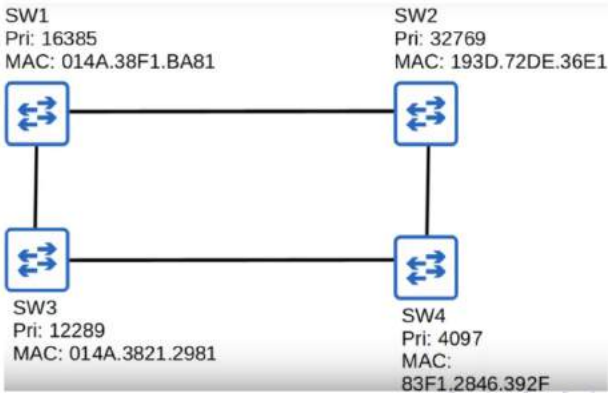
- El puente prioridad por defecto es el 32728 en todos los switches.
- Si todos los switches tienen el mismo puente prioridad, entonces el MAC con el menor valor se convierte en puente raíz
- El puente prioridad en Cisco switches se dividen en dos, la prioridad y VLAN ID, ya que los switches de cisco usan PVST (Per VLAN Spanning tree)



Solo la raiz puente puede enviar BPDUs y todas las interfaces son puertos designados. Los puertos designados están en estado de reenvío.

Ejercicio:



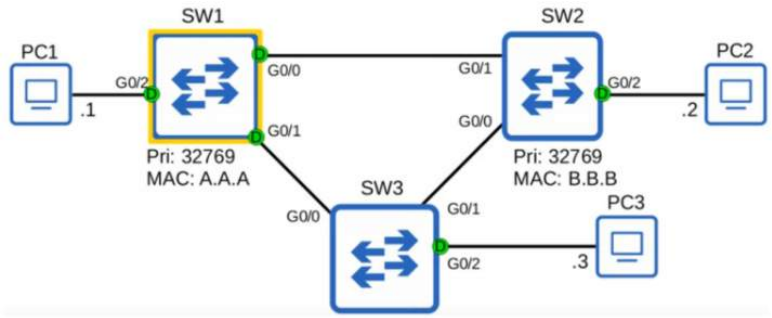


- STP
  - Cada switch que no es raíz puente, selecciona un puerto como puerto raíz, el cual es el que tiene el menor costo total. Los puertos raíz están en estado de reenvío. El costo de un puerto es obtenido de acuerdo al tipo de conexión usada.

Velocidad	Costo STP
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

    - El costo total se obtiene de un puerto se obtiene del costo de su interfaz más el costo que recibe en el BPDU. En caso que los puertos tengan el mismo costo, se selecciona el puerto raíz por el menor vecino puente ID.
    - Si todos tendría la misma prioridad, entonces se selecciona por el menor valor del STP puerto ID
    - Recordar que el STP puerto ID = puerto prioridad + el número de puerto
- Determinando el puerto raíz

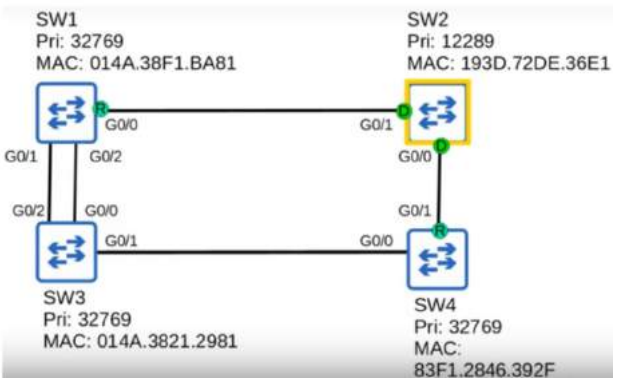
El costo de la raíz puente es 0, y de los otros switches agregan costo de acuerdo a las interfaces de salida.



Cada enlace entre nodos intermedios de red es un dominio de colisión, y cada dominio de colisión tiene un único STP puerto designado.

Ejercicios

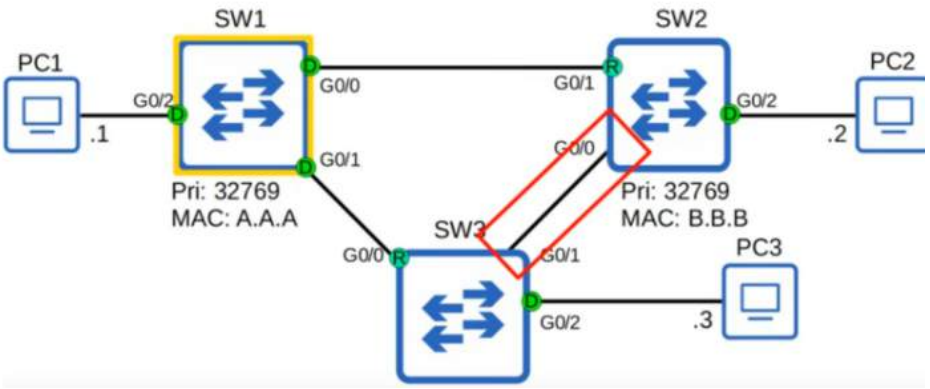
Indique cual es el puerto raiz del switch 3



Identifique el puente raiz, y el rol de cada interfaz en cada switch (raiz, designado, no designado)

- Puerto no designado

Siempre en cada dominio de colisión se necesita un puerto designado. El switch con el menor costo raíz tiene un puerto designado. Si el costo raíz es el mismo, el switch con el menor puente ID va a ser el puerto designado.
Los otros puertos en el dominio de colisión son no designados en estado de bloqueo.



- Estado de los puertos en STP
    - Estado de bloqueo: permanece estable
    - Estado de reenvío: permanecen estable
    - Estado de escucha: es transitorio
    - Estado de aprendizaje: es transitorio
    - Estado deshabilitado: está apagado la interfaz

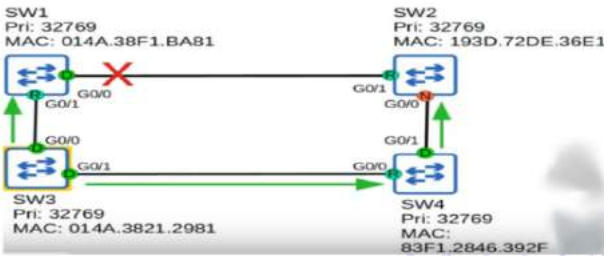
Puertos raíz y designados quedan estables en estado de reenvío.
Puertos no-designados quedan estables en el estado de bloqueo.
Los estados transitorios son cuando la interfaz se activa o cuando un puerto bloqueo pasa a reenviar debido al cambio de la topología.

- Estado de bloqueo
    - Puertos no designados están en estado de bloqueo
    - Interfaces en estado de bloqueo son deshabilitadas para prevenir bucles
    - Interfaces en estado de bloqueo no envían ni reciben tráfico de red
    - Interfaces en estado de bloqueo reciben STP BPDUs
    - Interfaces en estado de bloqueo no reenvían STP BPDUs
    - Interfaces en estado de bloqueo no aprende la dirección MAC
- Estado de escucha
    - Solo los puertos raíz y designados entran en el estado de escucha y toma 15 segundos por defecto, el cual es determinado por el reloj de retraso de reenvío
    - Una interface en estado de escucha solo envía y recibe BPDUs, no envía o recibe tráfico regular, no aprende la dirección MAC
- Estado de aprendizaje
    - Solo raíz o designado entra al estado de aprendizaje. Demora 15 segundos.
    - Aprende la dirección MAC
    - Solo envía o recibe BPDU
- Estado de Reenvío
    - Un puerto en este estado opera normal
    - Envía recibe BPDUs

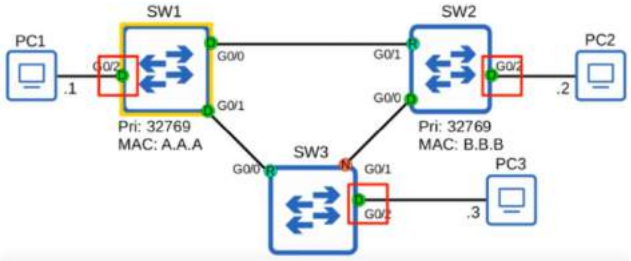
    - Envía recibe tráfico normal
    - Aprende la dirección MAC
- STP Relojes (temporizadores)

Reloj STP	Funcionalidad	Tiempo por default
Hello	Cada cuanto tiempo el puente raiz envia hello BPDUs	2
Retraso de reenvio	Cuanto tiempo estan en escucha y aprendizaje	15
Vida maxima	Cuanto tiempo una interfaz debe esperar despues de haber dejado de recibir Hello BPDUs para cambiar la topologia STP	20

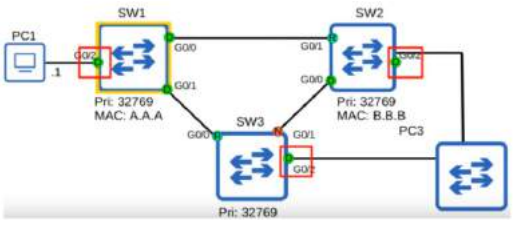
    - El reloj en la raíz puente determina los relojes STP de toda la red.
- Vida Máxima STP
    - Puede tomar unos 50 segundos pasar de estado de bloqueo a estado de reenvío.
    - Estos relojes y estados transitorios son usados para asegurar que los bucles no son accidentalmente creados por una interfaz y haciendo que el paso a estado de reenvío tome su tiempo.



- Características adicionales de STP: Portfast
    - Permite al puerto mover inmediatamente al estado de reenvío, sin pasar por escucha y aprendizaje. El comando es $: spanning-tree portfast.
    - Solo para puertos conectados a nodos terminales.
    - Si se activara en un puerto que conecta switch, podría ocasionar bucles en capa 2



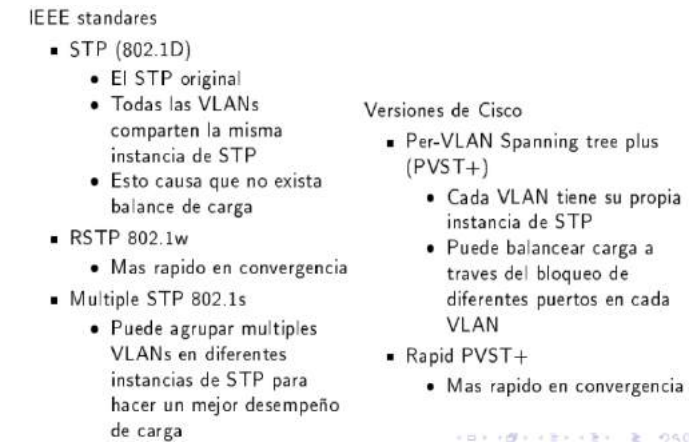
- Características adicionales de STP: BPDU Guard
    - Si una interfaz tiene activa el BPDU guard, entonces si recibiera un BPDU de en otro switch, la interfaz se apaga.



- Características adicionales de STP: Root y Loop Guard
    - Root guard: si recibe un BPDU superior en esa interfaz, el switch no aceptará el nuevo switch como raíz puente. La interfaz se deshabilitará.
    - Loop guard: si la interfaz ya no recibe BPDU, no re enviará ningún mensaje y se deshabilita la interfaz.
- Ejercicios

  Conectas una PC al switch, sin embargo, después de medio minuto no puedes conectarte a la red. Cual de las siguientes opciones resolvería el problema y te permitirá conectarte a la red rápidamente?
    A. Habilitar portfast en el puerto de switch que te conectas
    B. Reducir el tiempo de reloj que envía hello BPDUs
    C. Reducir el tiempo del reloj de retraso de reenvío
    D. Reducir el reloj de máxima vida

  Quieres asegurar que un bucle de capa 2 no ocurra si un usuario conecta un switch al puerto donde antes estaba conectado una PC. ¿Qué característica adicional de STP debería ser activada?
    A. Portfast
    B. Loop guard
    C. Root guard
    D. BPDU guard
- Spanning tree versions



- Rapid STP
    - Los estados de puerto en STP mezclan por un lado si el puerto reenvía o no tramas y por otro el papel que juega el puerto en el árbol.
    - RSTP mejora este problema y divide los puertos en puertos estados y puertos rol
        - Los estados denen si se reenvían las tramas y si se aprenden direcciones MAC
        - Los roles definen el papel que juega el puerto en el árbol
    - STP obsoleto y retirado del estándar
    - RSTP es IEEE 802.1w
    - RSTP es el STP que aparece en 802.1D-2004
    - Tiempos de convergencia de 2-3 segs (aunque según la topología

    - puede llegar a 30s y cuentas a infinito)
    - Tres estados posibles para un puerto:
        - Desechado: ni envia ni acepta paquetes de usuario
        - Aprendizado: no envia ni acepta paquetes de usuario pero aprende MACs
        - Reenvio: funcionamiento normal
- Roles de Puertos
    - Raíz,y designado, se comportan igual
    - Alternado y Backup
        - Corresponden a lo que antes eran puerto de bloqueo
        - Backup es todo puerto que no es ni raíz ni designado y el puente es designado para esa LAN (si no, es alternado)
        - Un puerto alterno da un camino alternativo hacia la raíz frente al puerto que se tiene como raíz
        - Puerto Backup da un camino alternativo pero siguiendo el mismo camino que el puerto raíz
        - Puerto Backup solo existe donde haya 2 o más enlaces de un puente a una LAN
        - Puerto alternado está bloqueado porque se han recibido BPDUs mejores (menor coste) de otro switch en el mismo segmento
        - Puerto Backup está bloqueado porque se han recibido BPDUs mejores del mismo switch en el mismo segmento