Protocolo IPv4

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Protocolo IPv4

El protocolo IP define a la capa de red del modelo TCP/IP. Es tal su importancia en el conjunto de protocolos TCP/IP que su nombre es uno de los dos que lo definen.

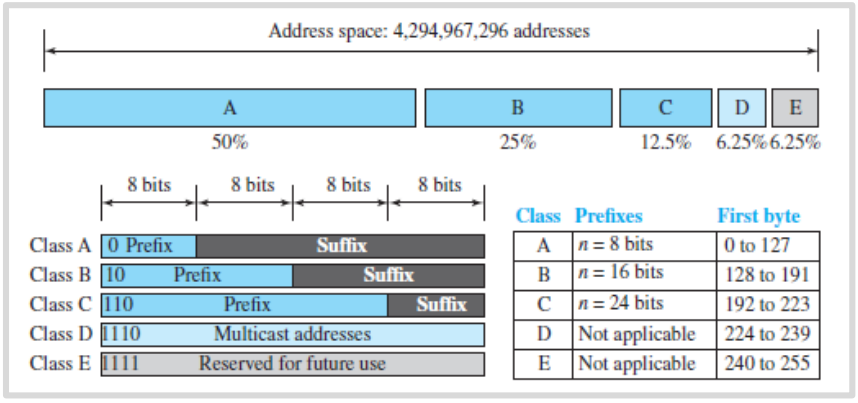
La implementación de IPv4 no tuvo en cuenta el explosivo crecimiento de la red Internet, por lo que diversas modificaciones y técnicas fueron surgiendo para posibilitar que la red continúe su expansión. Finalmente, como analizaremos luego en este módulo, se diseñó una nueva versión del protoolo IP, denominada IPv6.

Direccionamiento

Para que dos computadoras se comuniquen entre si se requiere el uso de direcciones lógicas (de capa 3), además de las direcciones físicas Ethernet. La implementación 4 del protocolo asigna 32 bits a cada dirección utilizada en un dispositivo. Originalmente estas direcciones estaban divididas en clases: A, B, C, D, E.

Cada clase tiene un número fijo de bits asignados al prefijo de red (8 bits para la clase A por ejemplo) y al sufijo de host (24 bits para hosts). Estos bits hacen que la cantidad de redes disponibles sea fija, al igual que la cantidad de dispositivos posibles para cada red. Como se observan en la figura 1, esto trajo serios inconvenientes ya que no existen organizaciones que requieran 2^{24} direcciones IP para una sola red, como es el caso de las clase A. La consecuencia es el gran desperdicio de direcciones IP. Imaginemos que una empresa tiene una dirección de red clase A asignada y solo utiliza 100.000 direcciones. Más de 16 millones de direcciones IP quedarán si uso.

Figura 1: Direcciones IPv4 con clase



Fuente: Forouzan, 2012, p. 531

En el otro extremo del mismo problema, una empresa que tiene asignada una IP clase C, tiene muy pocas direcciones IP disponibles para sus dispositivos (254).

En un principio estos problemas no eran muy graves, pero cuando Internet comenzó su crecimiento exponencial, los diseñadores se dieron cuenta que desperdiciar direcciones IP limitaría ese crecimiento y decidieron tomar cartas en el asunto.

Subredes

Si utilizamos bits originalmente utilizados como sufijos de host para subdividir la red asignada, se construye lo que se denomina una subred.
Para poder diferenciar ahora una subred de lo que antes era una IP de dispositivo, se utiliza la denominada máscara de subred.

Una máscara de subred se compone de 32 bits, los cuales se corresponden con los 32 bits de la dirección IP. Si el bit de la máscara de subred está en 1, significa que el bit de la dirección IP corresponde al prefioj de subred; en cambio si está en 0, significa que ese bit corresponde al sufijo de host.

Ejemplifiquemos con la dirección IP clase A 13.0.0.0.
La máscara de subred 255.0.0.0 indica que el primer octeto o byte (13) corresponde a la dirección de subred. En este caso, aún no se han realizado subredes. Como cualquier clase A, existen 2^{24} direcciones asignables a dispositivos.

Si en lugar de disponer de una sola red con 2^{24} direcciones se decide subdividirla en dos subredes, se deberá utilizar uno de esos 24 bits de host para las nuevas dos subredes.

La nueva máscara de subred será 255.128.0.0. El 128 es el equivalente del binario 10000000 en el segundo octeto.

Cómo se utiliza un solo bit, se pueden realizar dos subredes y las mismas serán:

- 13.0.0.0 /25
- 13.0.0.128 /25

La notación /25 significa que 25 bits de la máscara de subred son 1, lo que es equivalente a escribir 255.128.0.0

Utilizando máscaras de subred es posible distinguir lo que antes era una dirección IP asignable a host (13.0.0.128) de la nueva dirección de subred. Sin la utilización de máscaras de subred, esto no sería posible.

VLSM

En el ejemplo anterior, una red clase A fue subdivida en dos redes exáctamente iguales. Ambas subredes utilizan la misma máscara de subred (/25).
Hagamos una analogía: la dirección de red clase A era una pizza entera, la cual fue divida en dos porciones exáctamente iguales.
¿Qué sucede si la pizza debe ser repartida entre 1 adulto y 2 niños? Necesitamos volver a dividir una de las dos porciones nuevamente, para que las tres personas puedan comer.

Para poder volver a dividir necesitamos tomar nuevamente un bit de host y asignarlo a subredes.
Si ahora se utilizan dos bits en lugar de uno, la nueva máscara de subred para esta división es /26 (255.192.0.0), pero para la porción más grande de la pizza sigue siendo /25 (255.128.0.0).

Estamos en presencia de máscaras de longitud variable (Variable Lengh Subnet Mask). En general, la cantidad de dispositivos por red y el tamaño de estas últimas es variable y no fijo. Utilizar un esquema VLSM permite que una organización se adapte a sus necesidades y pueda armar subredes de acuerdo a sus necesidades. De lo contrario, si usara máscaras de longitud fija, todas sus subredes serían iguales y podrían tanto desperdiciarse una gran cantidad de IPs como disponer de subredes cuya disponibilidad de direcciones IP no sea suficiente para asignar a todos los dispositivos.

Profundiza tus conocimientos sobre subredes y VLSM en http://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

Direccionamiento sin clase (CIDR)

Los dispositivos encarados de interconectar redes se denominan Routers. Estos equipos tienen la misión fundamental de recibir paquetes, leer la dirección IP de destino, y en base a información interna que analizaremos cuando estudiemos Ruteo, reenviar ese paquete hacia otro Router hasta que pueda llegar a destino

Cuando se utiliza direccionamiento con clase, para un Router es sencillo descifrar a que red pertenece la dirección IP, ya que solo debe consultar los primeros bits de la dirección IP. Si el primer bit es un 0, corresponde a una clase A, si comienza con 10, clase B y si comienza con 110, clase 0.

El Router sabe de antemano que cada clase tiene una cierta cantidad de bits para el prefijo de red, y el resto es el sufijo de host. En base a esta información, consulta una tabla en donde se guarda información sobre redes de destino y la correspondiente interfaz por donde debe salir el paquete.

Pero, ¿qué sucede cuando las clases desaparecen? ¿por qué desaparecen las clases?

Las clases desaparecen porque la técnica de subredes fijas no fue suficiente para evitar el maluso de los rangos de direcciones IP. Al utilizarse máscaras de subred de longitud variable, se requiere que los Routers decidan sobre el destino de un paquete ya no en base a los bits iniciales, sino a estas máscaras.

La máscara de subred indica la cantidad de bits que corresponden a la subred, por lo que extrayendo esta información el Router podrá buscar en su tabla y decidir a que interfaz debe redireccionar el paquete.

Ejemplo: dirección IP 170.3.2.15 / 27

El /27 indica que los primeros 27 bits de la máscara son 1 (255.255.255.224). Para extraer cuál es la dirección de red, se utilizan esos 27 bits y se determina que IP de la red es: 170.3.2.0.
Cómo los 3 primeros bytes de la máscara están en 1, los 3 primeros bytes de la dirección IP corresponden al prefijo de red; pero además hay 3 bits del último octeto. Si se convierte el 15 decimal a binario (00001111) se puede determinar que los tres primeros bits son cero lo que determina que es la primera de todas las posibles subredes. Además, para que una dirección IP sea de red, todos los bits de host deben ser 0, con lo cual la IP de red es 170.3.2.0.

De la misma forma pueden determinarse las direcciones IP para los hosts, que irán desde el 00000000 al 000111110, siendo la dirección de broadcast la 170.3.2.31, la cual se genera al activar todos los bits del sufijo de host. (00011111)

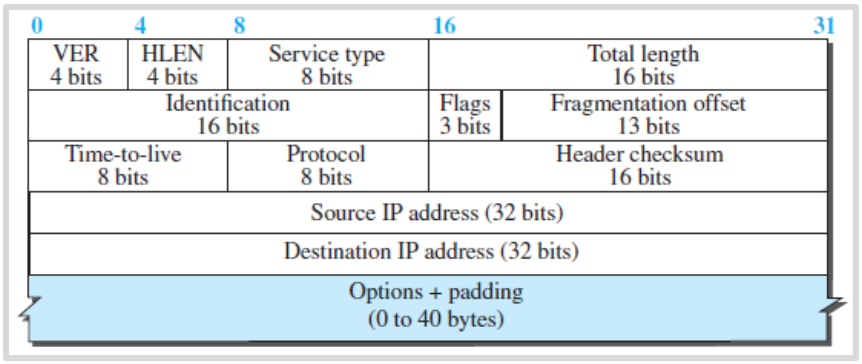
Formato del datagrama

En la capa inferior, Ethernet formaba tramas con sus correspondientes campos, los cuales almacenaban las direcciones físicas, el tipo, un CRC y el área de Datos.

De manera similar, el protocolo IP define lo que se denomina Paquete, el cual posee un encabezado donde se almacenan las direcciones IP y diversos campos que cumplen funciones específicas.

En la figura 2 se observa el encabezado del datagrama IPv4. Para conocer que función cumple cada campo, consulta el capítulo 5 del libro Redes de Computadoras de Tanenbaum.

Figura 2: Encabezado Datagrama IPv4



Fuente: Forouzan, 2012, p. 563

El encabezado IPv4 es de longitud variable. Las primeras 5 palabras de 32 bits son obligatorias, pero luego vienen campos de Opciones y relleno, las cuales son opcionales y pueden hacer que el tamaño crezca. El tamaño máximo del paquete IP lo define el campo Total Lenght o longitud total. 216 = 65535 bytes.

Es conveniente recordar que la longitud máxima del área de datos de la trama Ethernet es de 1500 Bytes. Pero ¿por qué es esto importante? Debido a que el paquete IP se encapsula en ese campo de la trama.

Cuando el paquete IP es mayor a 1500 bytes, debe fragmentarse, lo que equivale a dividirlo en paquetes de un tamaño máximo de 1500 bytes. De lo contrario, no puede viajar en tramas Ethernet.

Profundiza tus conocimientos sobre la fragmentación en el capítulo 5 del libro Redes de Computadoras de Tanenbaum.

Referencias

Stallings, W (2004). Introducción a las comunicaciones de datos y redes en *Comunicaciones y Redes de Computadoras.* Madrid: Editorial Pearson Education

Forouzan, B (2012). Introduction en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill

Tanenbaum, W (2012). La capa de red en *Redes de Computadoras.* Mexico: Editorial Pearson Education

Protocolo IPv6

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Protocolo IPv6

El protocolo IPv4 funciona correctamente pero cuando Internet comenzó a crecer exponensialmente surgió un gran problema: la cantidad de direcciones IP disponibles en algún momento iba a ser insuficiente y limitaría que el crecimiento continúe.
Cada dispositivo que quiera estar conectado a la red Internet necesita una dirección IP pública. Si bien hay técnicas que permiten que hoy en día millones de dispositivos puedan acceder a Internet utilizando una dirección IP privada (NAT), esto limita su presencia y condiciona a los proveedores de servicios de Internet (ISP) a aumentar su cantidad de clientes.

Los diseñadores decidieron diréctamente diseñar un nuevo protocolo que solucione el problema de la falta de direcciones y a su vez mejore el rendimiento.

Agotamiento IPv4

Las direcciones IP son gestionadas por el IANA (Internet Assigned Numbers Authority) quién a su vez delega su trabajo en 5 RIRs o Regional Internet Registries los cuales comprenden 5 regiones: Africa (AfriNIC), Asia/Pacífico (APNIC), Europa/Oriente Medio/Asia Central (RIPE NCC), Latinoamérica (LACNIC) y América del Norte (ARIN).

La IANA asigna bloques de direcciones /8 a los diferentes RIR. Estos bloques de direcciones están 100% asignados.
Cada RIR dispone de direcciones /8 que subdivide y asigna en bloques a los ISP. En el año 2017, solo AfriNIC tiene más de un pool /8 disponible.

En nuestra región, el LACNIC también agotó el último bloque /10 disponible, por lo que actualmente solo es posible asignar bloques entre /22 y /24.

Todo esto no quiere decir que se vaya a producir una catástrofe en Internet, sin embargo el crecimiento está seriamente comprometido. Si un ISP necesita un bloque de direcciones IPv4 para sus nuevos clientes, le es muy dificil obtenerlo.

Es por ello que algunos proveedores se han tomado muy en serio la problemática y han migrado sus redes al nuevo protocolo IPv6. Puedes leer un caso en el siguiente enlace: http://portalipv6.lacnic.net/el-exitoso-despliegue-de-ipv6-de-telecentro-argentina/

Direccionamiento IPv6

Las direcciones IPv4 tienen 32 bits, lo que da una cantidad de 2^{32} direcciones disponbles (a las que se les deberá descontar las direcciones de red, broadcast y reservadas).

Las direcciones IPv6 aumentan la disponibilidad al utilizar 128 bits. Se expresan en hexadecimal debido a su gran longitud en decimal.

En la figura 1 se observan los prefijos utilizados para IPv6. Hay bloques reservados, para Unicast global, Unicast local, Link Local y Multicast.

Figura 1: Prefijos para IPv6

Block prefix	*CIDR*	*Block assignment*	*Fraction*
0000 0000	0000::/8	Special addresses	1/256
001	2000::/3	Global unicast	1/8
1111 110	FC00::/7	Unique local unicast	1/128
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

Fuente: Forouzan, 2012, p. 668

Global Unicastcomunicación entre dos dispositivos de Internet. Ocupan 1/8 del total de direcciones disponibles y están divididas en tres: prefijo de ruteo global, identificador de subred e identificador de interfaz. Se recomiendan 48, 16 y 64 bits respectivamente para cada división.
Los 45 bits restantes del prefijo de ruteo global identifican por ejemplo a un ISP. Cada ISP podrá disponer de 16 bits para subredes (65.535) con 2^{64} direcciones asignables a dispositivos por cada una de esas subredes.

Mapeo de direcciones

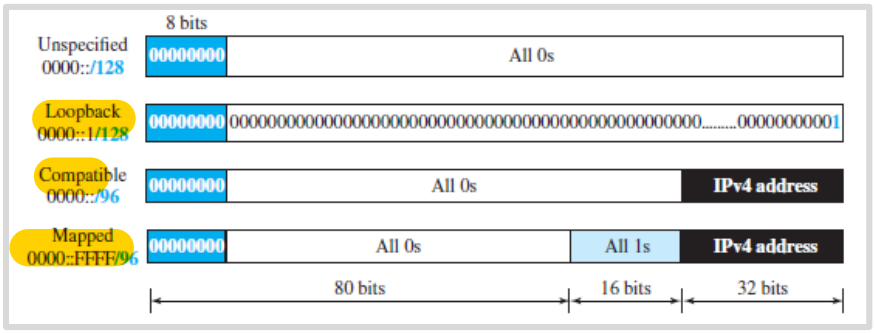
En los 64 bits correspondientes al identificador de interfaz es posible mapear directamente la dirección física de la capa de enlace. En el caso de Ethernet, se utilizan 48 bits por lo que es necesario agregar 16 bits (FFFE) y además cambiar el bit que identifica si una dirección es local o global a 1, es decir, hacerla global.

Ejemplo: un dispositivo tiene la dirección MAC A**5**:12:F0:22:10:21
Su dirección mapeada será: A**7**12:F0FF:FE22:1021
El 7 (01**1**1) es el resultado de invertir el bit local por global en el 5 (01**0**1) original. El FF:FE fue agregado para completar los 64 bits.

Direcciones especiales

Si una dirección IPv6 comienza con 000 0000 significa que es una dirección especial, lo cual tiene varios significados como se observa en la figura 2.

Figura 1: Direcciones IPv6 especiales



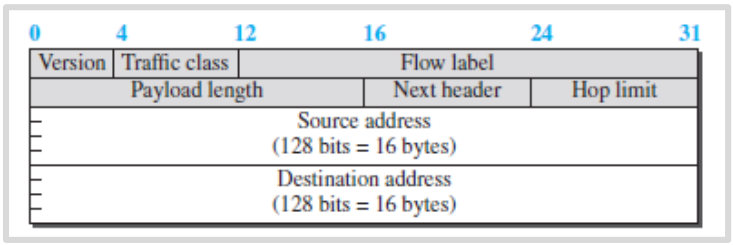
Fuente: Forouzan, 2012, p. 671

Además de reservar una dirección "sin especificar" que se usa cuando un host no conoce su IP y busca una, o cuando se hace referencia al propio dispositivo (loopback), IPv6 contempla la transición de IPv4 a IPv6 permitiendo que los hosts usen su dirección IPv4 embebida en la IPv6. Una dirección compatible se usa cuando una computadora usa IPv6 y le quiere enviar información a otra que también usa IPv6.
En cambio una dirección mapeada se usa cuando una computadora ya migrada a IPv6 se quiere comunicar con otra que utiliza IPv4.

Datagrama IPv6

El formato del datagrama IPv6 difiere sustancialmente del IPv4. Está formado por un encabezado base de 40 bytes el cual puede ser extendido con mas encabezados. El área de datos tiene un máximo de 65535 bytes.
En el encabezado base, 32 de los 40 bytes son ocupados por las direcciones IPv6, con lo cual apenas 8 bytes se usan para definir campos que permitan el funcionamiento. Uno de esos campos se denomina "Next header" y hace referencia otros encabezados cuando estos se utilicen.

Figura 2: Encabezado base IPv6



Fuente: Forouzan, 2012, p. 674

Este diseño tiene una gran ventaja. Recordemos el encabezado IPv4, el cual posee 20 bytes con campos obligatorios. Algunos de estos campos puede que no se utilicen, por ejemplo si no es necesaria la fragmentación. Enviar datagramas con campos sin uso significa desperdicar capacidad del canal y ocupar espacios que podrían ser usados por bits de datos de usuario.
El datagrama IPv6 resuelve este problema usando extensión de encabezados solo cuando se los requiere.

Para conocer la función de cada campo, lee el capítulo 5 del libro “Redes de Computadoras de Tanenbaum.

Mejoras con respecto a IPv4

La primera diferencia con respecto a IPv4 son los tipos de direcciones. Mientras que en IPv4 existen direcciones Unicast, Multicast y Broadcast, en IPv6 se eliminan las direcciones Broadcast, se mantienen las Unicast y Multicast y se agregan las direcciones Anycast. Este tipo de direcciones se asigna a un grupo de dispositivos (si, varios dispositivos tienen la misma dirección IP) y el datagrama será entregado al dispositivo más cercano en relación al transmisor. Esto tiene la particularidad de poder disponer de un grupo de servidores para determinado fin dispersos en diferentes regiones, y ahorrar tráfico de datagramas.

Otra diferencia es en la fragmentación. A diferencia de IPv4, la misma courre en el dispositivo que origina el datagrama y no en un router intermedio. Esto ahorra recursos en los routers por lo que son liberados para tareas mas específicas.

Puedes profundizar tus conocimientos sobre el funcionamiento de IPv6 leyendo el RFC 2460 (https://www.ietf.org/rfc/rfc2460.txt)

Compatibilidad IPv6 / IPv4

¿Puede un dispositivo que utiliza IPv6 comunicarse con otro que utiliza IPv4? La respuesta es si y no.

Los protocolos no son compatibles entre si, ya que el formato del datagrama y el tipo de direccionamiento es diferente. Recordemos que para que exista comunicación entre similares niveles o capas del modelo OSI, ambos extremos deben utilizar el mismo protocolo.

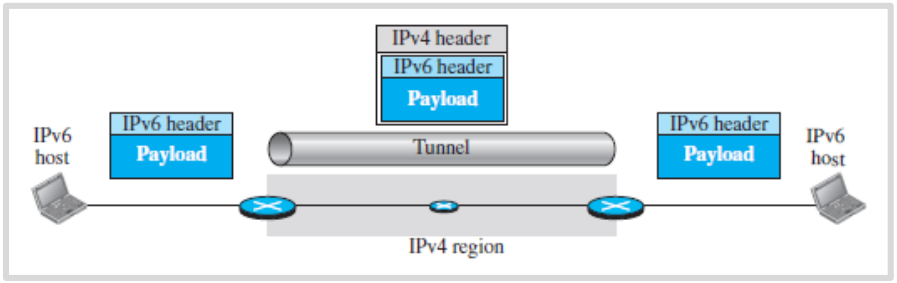
Tampoco es posible realizar un “apagado” de IPv4 para dar lugar a IPv6, ya que sería una tarea monstruosa y con grandes disrupciones en la red.

Para resolver este inconveniente es posible construir “túneles” los cuales permiten que dos dispositivos que utilizan IPv6 puedan comunicarse entre sí a través de redes que utilizan IPv4.

Los datagramas IPv6 originados por un dispositivo, se encapsulan en el área de datos de un datagrama IPv4 en el dispositivo donde inicia el tunel, es decir la frontera entre redes que soportan IPv6 e IPv4.
El datagrama IPv4 viajará por las redes IPv4 normalmente hasta llegar al otro extremo del túnel. Aquí el dispositivo deberá desencapsular el datagrama IPv6 y enviarlo a destino.

La estrategia de tunelización se muestra en la figura 3 y es eficiente cuando la mayoría de las redes funcionan bajo IPv4.

Figura 3: Tunelización



Fuente: Forouzan, 2012, p. 684

Cuando todas las redes intermedias funcionan con IPv6 pero el host de destino todavía no, la estrategia de traducción de encabezados resulta más conveniente; en este caso el datagrama IPv6 llega a destino y su encabezado es convertido a IPv4 para que sea interpretado por el destinatario.

Referencias

Forouzan, B (2012). Introduction en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill

Tanenbaum, W (2012). La capa de red en *Redes de Computadoras.* Mexico: Editorial Pearson Education

IANA (2017). IANA IPv4 Address Space Registry. Recuperado de https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

LACNIC (2017). Fases de agotamiento de IPv4. Recuperado de http://www.lacnic.net/web/lacnic/agotamiento-ipv4

IANA (2017). Number Resources. Recuperado de https://www.iana.org/numbers

VLANs

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

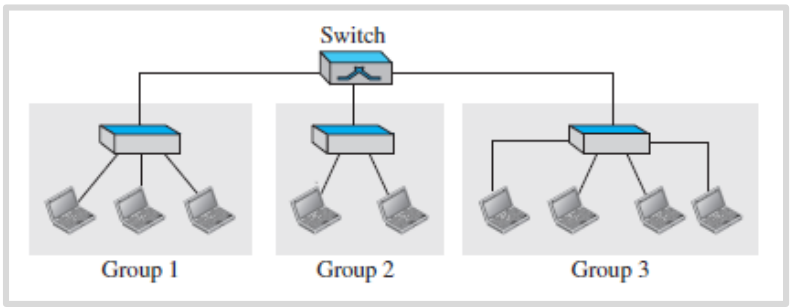
VLANs

En una red de área local (LAN) con topología estrella, todos los dispositivos se conectan a un nodo central. Antiguamente se utilizaban Hubs, los cuales no tenían ningún tipo de inteligencia y solo repetían la señal que ingresaba por uno de sus puertos en los demás. La tecnología de conmutación presente en los Switches permitió mejorar las prestaciones de las redes LAN. Los dispositivos se conectan a este nodo central y cuando se trabaja con modalidad full-duplex las colisiones ya no están más presentes.

Una LAN es una forma de segmentar dispositivos que tienen los mismos objetivos. Por ejemplo, una oficina de una empresa. Pero, ¿qué sucede si la empresa quiere separar lógicamente sus areas? ¿o si la empresa dispone de muchas oficinas separadas donde trabajan empleados de las mismas areas?

Se requiere algún mecanismo que permita que dos empleados pertenecientes a una misma área ubicados en oficinas diferentes (con switches diferentes) puedan pertenecer a una misma LAN. Este mecanismo existe y consiste en crear LAN virtuales, o virtual LANs / VLANS.

Figura 1: Tres redes LAN interconectadas

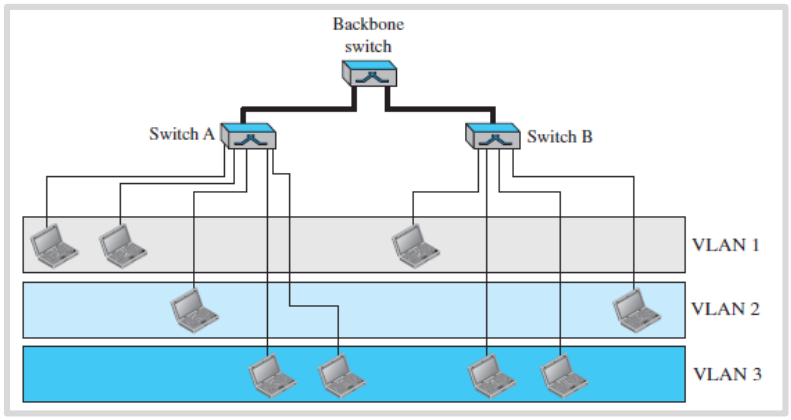


Fuente: Forouzan, 2012, p. 502

En la figura 1 se observa un esquema tradicional en donde existen tres grupos separados, por ejemplo, las áreas de Recursos Humanos (grupo 1) de Ingeniería (Grupo 2) y de Finanzas (Grupo 3) de una empresa. Los empleados de cada área están ubicados en la misma oficina. Pero este esquema no puede funcionar cuando los empleados de cada área están dispersos en diferentes oficinas.

El problema se soluciona creando redes LAN virtuales para cada área de la empresa y configurando a el o los switches de tal forma que sin importar donde se encuentre un empleado de determinada área, pertenecerá a la misma red que sus compañeros.

Figura 2: Tres VLANs



Fuente: Forouzan, 2012, p. 503

En la figura 2 se observa un esquema basado en VLANs, en donde el Switch A está ubicado en un edificio, y el Switch B en otro. Además, existe un switch denominado de backbone que los interconecta.
En este ejemplo, 3 VLANs han sido creadas y nombradas VLAN 1, VLAN 2 y VLAN3. Los dispositivos que pertenezcan a una determinada VLAN podrán comunicarse entre sí a pesar de estar en LAN diferentes. Los dispositivos de diferentes VLANs no pueden comunicarse entre sí a pesar de compartir el mismo switch físico, a menos que se configure un Router.

¿Cómo se configuran las VLANs en los switches? El primer paso consiste en crear las VLANs en cada switch.
La cantidad de VLANs que pueden crearse no es infinito, y dependen de la cantidad de bits de un campo de la trama 802.1q que será analizada más adelante. Como el campo permite 12 bits, 4096 VLANs es el máximo posible. De este número, hay que no pueden usarse por estar reservadas, la VLAN0 y la VLAN4095. Generalmente la VLAN1 está creada por defecto, no puede eliminarse y todas las interfaces se encuentran allí.

Una vez que se crean las VLANs con su correspondiente número, es posible asignarles un nombre y descripción. Finalmente es necesario agregar cada interfaz a la VLAN correspondiente. Para mayor flexibilidad, también es posible hacer miembro de una VLAN a una dirección MAC o IP independientemente de la interfaz del switch a la que se haya conectado.

Seguramente pueda surgir esta pregunta: ¿A qué VLAN deben pertenecer las interfaces que conectan a los switches A y B con el Backbone switch?

La respuesta está dividida en dos partes:

- En primer lugar, estas interfaces se denominan trunk o troncales y así deben configurarse, a diferencia de las interfaces donde se conectan las

computadoras que se denominan Access o de acceso. Una interfaz troncal permite que tramas de una o más VLANs sean conmutadas.

- En segundo lugar, debe configurarse cuáles son las VLANs aceptadas. Siguiendo el ejemplo de la figura 2, se deber permitir el paso de las VLAN 1, 2 y 3.

Protocolo 802.1q

En una red LAN ethernet, las comunicaciones entre dispositivos son posibles gracias a la informacion contenida en la trama (direcciones MAC de destino y de origen principalmente).

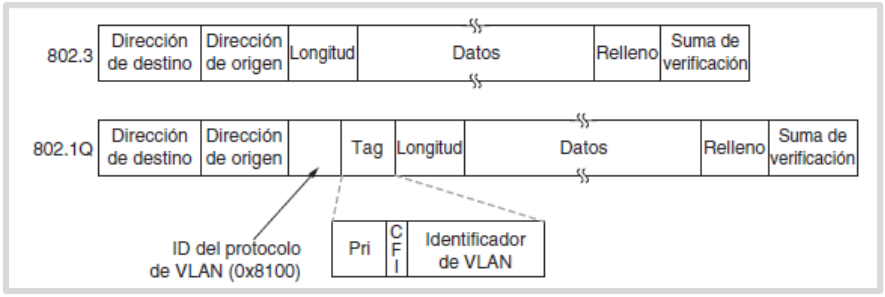
Los switches verifican la trama en busca de la dirección MAC de destino, chequean una tabla donde se almacenan las distintas direcciones MAC que están conectadas y su correspondiente número de interfaz o puerto.

Cuando se utilizan VLANs, el switch también tiene que saber desde que VLAN proviene la trama, para poder reenviarla solo a la o las interfaces que pertenezcan a la misma VLAN. Para que esto sea posible se requiere un campo nuevo en la trama Ethernet / 802.3 que contenga el número de VLAN.

Para permitir la compatibilidad con placas de red fabricadas antes de que existan las VLANs, las cuales solo pueden crear una trama Ethernet con los campos ya conocidos, se adoptó la siguiente solución: si la computadora no soporta el nuevo formato de trama, el switch a donde esta computadora se conecta (que por supuesto si debe soportar VLANs) los agrega. El último switch, es decir donde está conectada la PC de destino, remueve esos campos.
En caso de que las computadoras soporte el nuevo formato de trama, el origen directamente agrega los campos.

En la figura 3 se observa la trama original 802.3 y el nuevo formato de trama 802.1q, en donde se agregan dos campos de 2 bytes cada uno llevando el tamaño máximo de trama a 1522 bytes.

Figura 3: nuevo formato de trama 802.1q



Fuente: Tanenbaum, 2012, p. 299

- Campo Tag Protocol Identifier (TPID). Siempre tiene el valor 0x8100 identificando a la trama como 802.1q.
- Campo Tag Protocol information (TPI). Se encuentra subdividido en tres:
  - Priority Code Point (PCP). Prioriza distintos tipos de tráfico. 3 Bits.
  - Drop Eligible Indicator (DEI). Si hay congestión, se indica que la trama puede o no ser descartada. 1 Bit.
  - VLAN ID (VID): número que identifica a la VLAN. 12 bits.

Ejemplo de configuracion de VLANs en Switch Cisco

Si bien cada fabricante de equipos maneja sus propios comandos, los cuales pueden variar inclusive entre diferentes modelos de equipos, este ejemplo ilustra como crear una VLAN, agregar 6 interfaces a la misma y finalmente configurar como troncal una interfaz permitiendo el paso de esa VLAN.

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# name Ingenieria
```

Para agregar interfaces a la VLAN5 pueden utilizarse los siguientes comandos. Range hace referencia a un rango de interfaces, en este caso de la 1 la 6, las cuales serán agregadas a la VLAN5 en un solo paso, luego de configurarse en modo Acceso.

```
Switch(config)#interface range FastEthernet 0/1-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 5
```

Para configurar una interfaz como troncal, se utiliza el siguiente comando:

```
Switch(config)#interface FastEthernet 0/24
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed VLAN 5
```

Ejemplo de configuracion de VLANs en Switch Mikrotik

Para crear 2 VLANs y configurarlas en la interfaz troncal ether24

```
/interface vlan add name=vlan-10 vlan-id=10 interface=ether5 disabled=no
/interface vlan add name=vlan-20 vlan-id=20 interface=ether5 disabled=no
```

Para que sea posible reenviar paquetes desde puertos de acceso al puerto troncal se deben crear bridges.

```
/interface bridge add name=br-vlan10 disabled=no
```

/interface bridge add name=br-vlan20 disabled=no

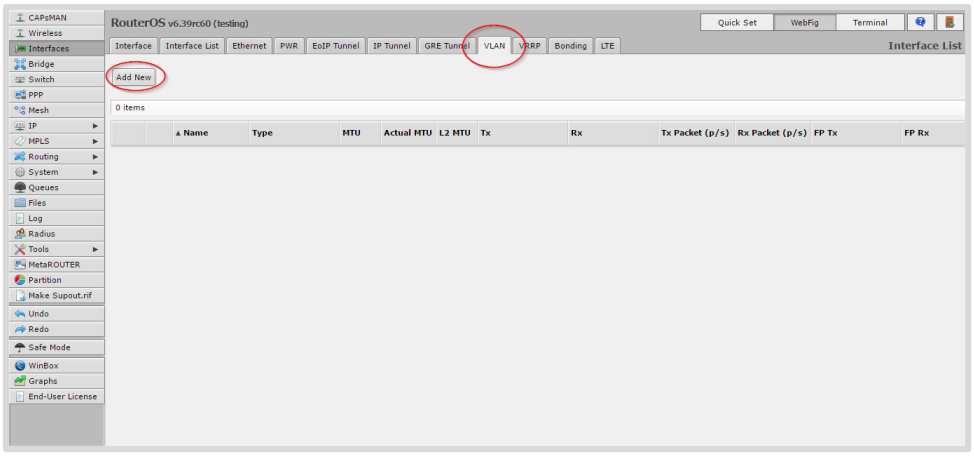
Finalemente se agregan interfaces a estos bridges. En este ejemplo, las interfaces ether1 y ether2 son interfaces de acceso donde se van a conectar dos computadoras.

/interface bridge port add interface="vlan-10" bridge="br-vlan10" disabled=no
/interface bridge port add interface="ether1" bridge="br-vlan10" disabled=no
/interface bridge port add interface="vlan-20" bridge="br-vlan20" disabled=no
/interface bridge port add interface="ether2" bridge="br-vlan20" disabled=no

Configuración en GUI

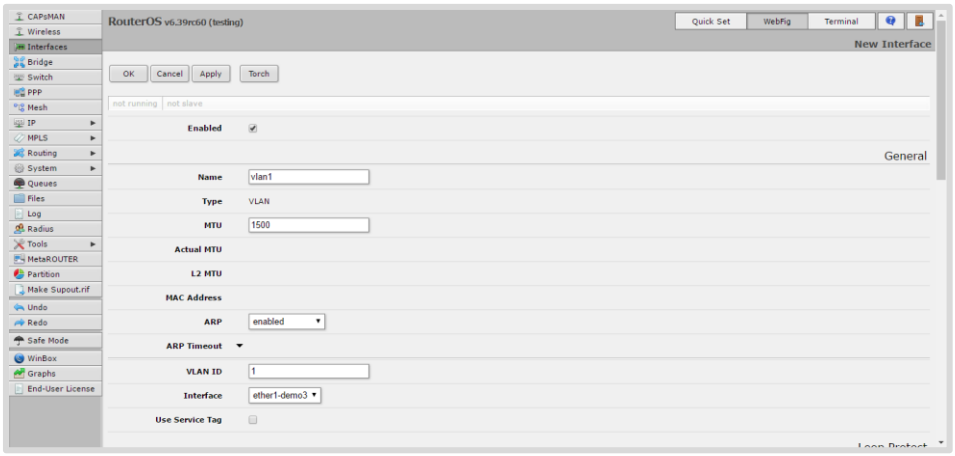
Los fabricantes incluyen una interfaz gráfica de usuario (GUI) donde es posible realizar diferentes configuraciones. En la siguientes figuras se ejemplifica como crear una VLAN en la GUI de Mikrotik.

Figura 4: creación de VLANs en Mikrotik. Paso 1



Fuente: Captura de pantalla RouterOS

Figura 5: creación de VLANs en Mikrotik. Paso 2



Fuente: Captura de pantalla RouterOS

Referencias

Forouzan, B (2012). Introduction en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill

Tanenbaum, W (2012). La capa de red en *Redes de Computadoras.* Mexico: Editorial Pearson Education

Cisco (2016). Cisco Nexus 5000 Series NX-OS Software Configuration Guide. Recuperado de http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/VLANs.html#58514

Mikrotik (2011). Vlans on Mikrotik environment. Recuperado de https://wiki.mikrotik.com/wiki/Vlans_on_Mikrotik_environment

Enrutamiento

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Enrutamiento

La capa 3 o de red cumple diversas funciones, entre ellas lograr que los paquetes viajen a través de diferentes redes para poder llegar a destino. Los dispositivos encargados de cumplir esta tarea se denominan Routers o enrutadores. ¿Cómo cumplen su trabajo?

Las tramas Ethernet llegan a un Router, el cual debe analizar el datagrama IP que se encuentra encapsulada en busca del campo IP de Destino dentro del encabezado IP. Esa información indica hasta donde debe llegar el datagrama. Para poder saber donde enviarlo, el Router consulta en su memoria la denominada Tabla de Ruteo. Esta tabla contiene campos que hacen posible la toma de decisión:

Tabla 1: Ejemplo tabla de ruteo Cisco

Código	Red de destino	Métrica	Siguiente salto	Interfaz
C	10.0.0.0 / 8	-	Diréctamente conectada	FastEthernet 0/0
C	20.0.0.0 / 8	-	Diréctamente conectada	FastEthernet 0/1
R	30.0.0.0 / 8	120/1	20.0.0.2	FastEthernet 0/1

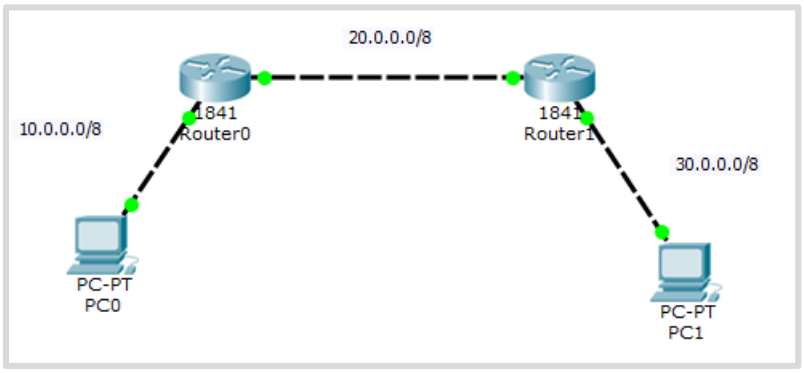
Fuente: elaboración propia

La tabla 1 muestra un ejemplo de tabla de ruteo del Router0 de la imagen 1. Las tablas de ruteo pueden construirse manualmente o mediante protocolos de ruteo dinámico. Esa información se indica con un código en la primera columna de la tabla.
La segunda columna contiene direcciones de redes de destino que el Router conoce. El Router compara la dirección IP del campo IP de Destino del datagrama IP con todas las redes de destino del Router, y determina cuál es la que coincide.
La métrica determina indica cuál es el mejor camino que debe seguir un datagrama en caso de que haya varias opciones.
El siguiente salto indica hacia donde debe ir el datagrama. Finalmente la la columna interfaz indica por cuál de todas las interfaces del Router debe enviarse el datagrama para que continúe viajando.

Si en el ejemplo de la figura 1, la PC0 quiere enviar información a PC1, el datagrama IP contentrá la dirección IP de PC1 en el campo IP de destino.

Cuando ese datagrama ingrese a Router0, este consultará la tabla de ruteo ejemplificada en Tabla 1 y concluirá que la ruta que debe seguir el datagrama es a trasvés del Router1.
Router1 tendrá una tabla similar, en donde una de sus entrada será la red 30.0.0.0/8, la cual está diréctamente conectada, por lo que la trama Ethernet podrá contener la dirección MAC de PC1 en su campo MAC de destino.

Figura 1: 2 Routers interconectando redes



Fuente: Elaboración propia, captura de Cisco Packet Tracer

En este ejemplo simple solo hay 3 redes, y cada Router tiene 3 entradas en su respectiva tabla. Si bien la tabla de ruteo del ejemplo fue configurada con un protocolo de ruteo dinámico, hubiera sido muy sencillo configurarla manualmente, ya que solo debe agregarse una ruta en cada Router (las conectadas diréctamente se cargan solas). Pero cuándo la cantidad de redes comienza a incrementarse se vuelve muy complicado realizar configuraciones a mano; además, los protocolos de ruteo permiten calcular las mejores rutas o disponen de mecanismos para recuperarse cuando hay determinados problemas, como por ejemplo redes inaccesibles.

Ruta por defecto

Un caso particular podría darse cuando ingresa un datagrama a un Router, y este no tiene una ruta cargada hacia la red de destino. En este caso, debería descartar el datagrama.
Como no es posible que cada router contenga rutas a todas las redes del mundo, se utiliza la denominada ruta por defecto. Todos las redes que no tengan una entrada específica en la tabla de ruteo, estarán implícitamente contenidas en esta rúta por defecto y los datagramas serán reenviados a la interfaz declarada en esa ruta.

Todos los hosts conectados a una red tienen configuradas tablas de ruteo. Cuando se genera un datagrama con una IP de destino, el sistema operativo debe decidir que hacer con el, por ejemplo, si ese dispositivo tiene más de

una interfaz de red. Es por ello que al igual que un Router, los dispositivos finales utilizan una tabla de ruteo para tomar esa decisión. Es mandatorio configurar la denominada puerta de enlace predeterminada o default gateway cuando se asigna una dirección IP a una interfaz de red de una computadora. De lo contrario, cuando los datagramas tengan como destino una red diferente a la red local, no podrán salir de dicha red al no conocer una ruta hacia otras redes.

Protocolos de ruteo dinámico

Antes de describir los protocolos de ruteo dinámico mas utilizados, es importante aclarar que es un Sistema Autónomo. Un Sistema Autónomo (Autonomous System en inglés o simplemente AS) es un conjunto de redes bajo el control de una entidad. Un ejemplo de AS puede ser un proveedor de servicios de internet (ISP).

Cada AS posee un número de identificación, el cuál es asignado por el RIR donde está ubicado, quién a su vez obtuvo un pool de números del IANA. La cantidad de AS es 2^{16}.

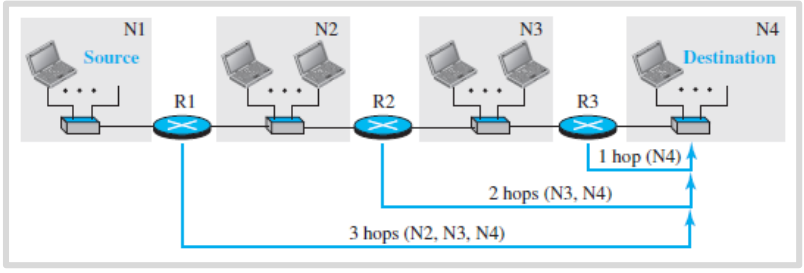
Los protocolos de ruteo dinámico están divididos en dos grupos:

1) Protocolos de ruteo interior: son aquellos protocolos que se utilizan para difundir rutas dentro de un sistema autónomo.
2) Protocolos de ruteo exterior: son aquellos que se utilizan para difundir rutas entre sistemas autónomos.

Protocolo de ruteo interior RIP

RIP (Routing information Protocol) utiliza el concepto de vector-distancia para determinar el costo que tiene un Router en alcanzar una red de destino. Este costo es medido en saltos, es decir, la cantidad de routers que se deben atravesar hasta llegar a destino. Mientras mas álto seal el número de saltos, más alejada está la red. El número máximo de saltos en RIP es de 15, es decir que una red ubicada a más de 15 saltos es inaccesible.

Figura 2: 2 Saltos en RIP



Fuente: Forouzan, 2012, p. 613

En la figura 3 se indican la cantidad de saltos que atraviesa un datagrama para viajar entre N1 y N4 (3 saltos).

El protocolo funciona intercambiando mensajes entre routers sobre las redes que conoce cada uno. De esta forma, los Routers van aprendiendo las rutas que otros conocen hasta lograr la convergencia, es decir, que todas las tablas son uniformes.

Para profundizar sobre RIP, revisa el paper del aula abierta.

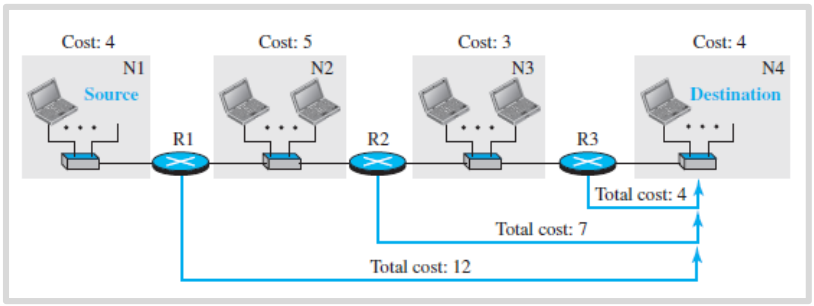
Protocolo de ruteo interior OSPF

A diferencia de RIP, el cual utiliza el algoritmo vector-distancia, OSPF (Open Shortest Path First) utiliza el algoritmo de Dijkstra para calcular la distancia mas corta a otros Routers de la red partiendo desde cada uno de los Routers que la componen. Chequea en el aula abierta como funciona este algoritmo.

A diferencia de RIP que considera solamente los saltos como costo, en OSPF es posible definir otras métricas como por ejemplo confiabilidad, throughput, tiempo de ida y vuelta, etc. Entonces es posible que llegar a una red tenga "menos costo" cuando se atraviesan cinco redes de menor tiempo de ida y vuelta en lugar de solo una red con tiempos mayores.

En la figura se observa un esquema de red similar al de la figura 1, pero en este caso se indican los costos de alcanzar cada red (4, 5, 3 y 4). El costo de viajar entre R1 y el destino es de 12 ya que se suman los costos.

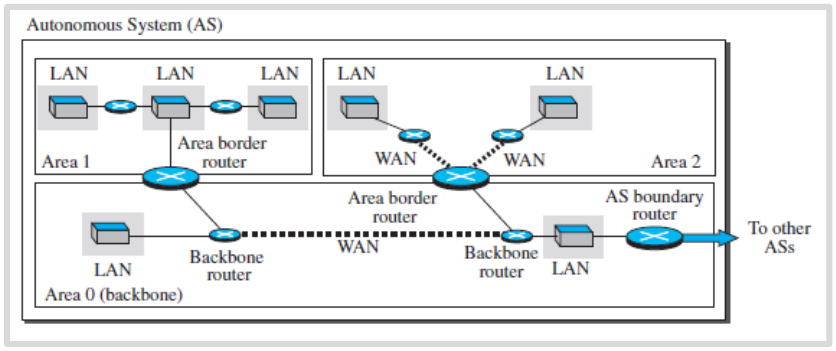
Figura 3: costos en OSPF



Fuente: Forouzan, 2012, p. 618

Debido al intenso tráfico que genera OSPF cuando se crea la base de datos de estados de enlace (LSDB), un sistema autónomo que utiliza OSPF se divide en áreas y cada una de estas áreas es un dominio de inundación, reduciendo el tráfico total del AS significativamente. Una de las áreas se denomina de backbone, y es la encargada de transmitir información sobre el estado de enlace a las demás.

Figura 4: áreas en OSPF



Fuente: Forouzan, 2012, p. 619

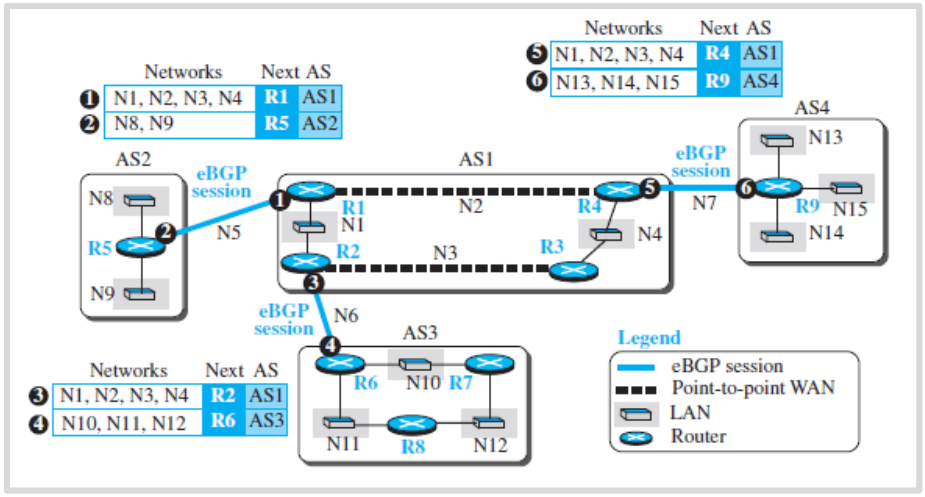
En la figura 3 se observa el área 0 (backbone) encargada de difundir información a las áreas 1 y 2 a través de los ABR o Área Border Router.

Profundiza tus conocimientos sobre OSPF con el instructivo de Cisco disponible en el aula abierta.

Protocolo de ruteo exterior BGP

Cada Sistema autónomo puede usar el protocolo de ruteo interior que decida y todos los Routers en su interior conocen las redes que están dentro de dicho AS. Para conocer redes de otros AS se implementa el protocolo BGP en los denominados Routers de frontera, es decir aquellos que se comunican con otro u otros AS. Dos Routers que corren BGP y se comunican entre sí se denominan Pares o Peers.

Figura 5: Internet con 4 Sistemas Autónomos



Fuente: Forouzan, 2012, p. 624

En la figura 4, R5 es peer de R1; R2 de R6 y R4 de R9. Entre Routers peers se intercambian información sobre las rutas que se conocen en cada Sistema Autónomo. En el ejemplo de la figura, R5 le envía a R1 las redes que conoce (N8 y N9), por lo que R1 ahora sabe que para alcanzarlas debe utilizar a R5.

Cada Router peer debe luego inyectar esas rutas en su propio sistema autónom.

Para conocer más sobre la configuración de BGP, puedes consultar el siguiente documento de Cisco: http://www.cisco.com/cisco/web/support/LA/7/76/76167_bgp-toc.html

Referencias

Forouzan, B (2012). Introduction en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill

Tanenbaum, W (2012). La capa de red en *Redes de Computadoras.* Mexico: Editorial Pearson Education

LACNIC (2017). Manual de políticas. Recuperado de http://www.lacnic.net/web/lacnic/manual-3

CISCO (2013). Estudios de casos de BGP. Recuperado de http://www.cisco.com/cisco/web/support/LA/7/76/76167_bgp-toc.html

IETF (2006). RFC4271. A Border Gateway Protocol 4 (BGP-4) Recuperado de https://tools.ietf.org/html/rfc4271

IETF (2006). RFC2178. OSPF Version 2. Recuperado de https://tools.ietf.org/html/rfc2178

IETF (2006). RFC2453. RIP Version 2. Recuperado de https://tools.ietf.org/html/rfc2453