DISPOSITIVOS Y PROTOCOLOS DE REDES LAN Y WAN

CONMUTADORES Y ENCAMINADORES

DISPOSITIVOS Y PROTOCOLOS DE REDES LAN Y WAN

CONMUTADORES Y ENCAMINADORES

Santiago Cristóbal Pérez e Higinio Alberto Facchini

UTN Regional Mendoza
Mendoza, 2017

Diseño de Tapa: Renzo Guido Facchini
Diseño de Interior: Renzo Guido Facchini
Corrección de Estilo: Renzo Guido Facchini

La amistad es

un alma que habita en dos cuerpos;

un corazón que habita en dos almas.

Aristóteles

Santiago Cristóbal PEREZ

Es Ingeniero en Electrónica de la UTN (1985), Magister en Redes de Datos de la UNLP (2006) y Doctor en Ingeniería (2016), mención Teleinformática y Telecomunicaciones. Docente de grado y posgrado de la UTN, Regional Mendoza, en la temática de Redes de Datos. Docente investigador UTN categoría A, y III en el Ministerio de Educación. Es Director del Grupo GRID ATyS (Grupo de Investigación y Desarrollo en Análisis de Tráfico y Seguridad).

Higinio Alberto FACCHINI

Es Ingeniero en Electrónica de la UTN (1985) y Magister en Redes de Datos de la UNLP (2016). Docente de grado y posgrado de la UTN, Regional Mendoza, en la temática de Redes de Datos. Docente investigador UTN categoría C, y V en el Ministerio de Educación. Es Subdirector del Grupo GRID ATyS (Grupo de Investigación y Desarrollo en Análisis de Tráfico y Seguridad).

PRÓLOGO

La obra tiene como objetivo complementar con contenidos más prácticos, los más bien teóricos de los libros de grado universitarios sobre la temática de Redes de Datos, abarcando capítulos concretos sobre los dispositivos y protocolos más utilizados en las Redes LAN (como son los conmutadores y los protocolos asociados a las VLANs y STP), y en las Redes WAN (como son los encaminadores y los protocolos de encaminamiento, como son RIP, OSPF y BGP), incluyendo imágenes, y aspectos de configuración y ejercitación. También se incluyen los tópicos fundamentales de las normas asociadas a las Redes MAN Cableadas (como MetroEthernet) e Inalámbricas (como WiMax). Estos contenidos están organizados en los siguientes Capítulos: Capítulo 1: Redes LAN y WAN; Capítulo 2: Conjunto de Protocolos TCP/IP, Capítulo 3: Conmutadores, VLANs y STP; Capítulo 4: Encaminadores y Protocolos de Encaminamiento; Capítulo 5: Protocolos de Encaminamiento RIP, OSPF y BGP; y Capítulo 6: Tecnologías MAN MetroEthernet y Wi-Max.

El libro ha sido pensando especialmente para los alumnos de grado de las carreras de Ingeniería en Sistemas e Ingeniería en Electrónica, y Tecnicaturas Universitarias en TICs de la UTN, y de las carreras TICs en general de cualquier institución universitaria o terciaria. Sus contenidos complementan la bibliografía de las Cátedras afines a las Redes de Datos.

Agradecemos la colaboración de los miembros de la Academia CISCO-ORACLE de la UTN Mendoza, quienes generosamente han aportado su tiempo y conocimientos para la revisión y elaboración de las tablas, gráficas y figuras. Además, el apoyo de las autoridades, presididas por el Ing. José Balacco, Decano de la Facultad Regional Mendoza, el Ing. Hugo Morales, Director del Departamento de Electrónica, y del CeReCoN (Centro de Investigación y Desarrollo en Computación y Neuroingeniería).

Santiago Pérez – Higinio Facchini
Mendoza, Argentina, enero de 2017

CAPÍTULO 1

Redes LAN y WAN

1.1 Introducción a las Redes de Datos

1.2 Clasificación de las Redes de Datos

1.3 Tendencias de las Redes de Datos

1.4 Símbolos de los dispositivos de red

Capítulo 1

Redes LAN y WAN

1.1 Introducción a las Redes de Datos

En la evolución histórica de los diversos sistemas de comunicaciones que vinculan un dispositivo origen con un dispositivo destino para transferir voz, video o archivos de datos, se observa que la solución habitual es el uso de redes. Es decir, ambos extremos se conectan entre sí a través de una red de comunicaciones.

Tal es el caso de los sistemas de telefonía fija, donde los dispositivos extremos son teléfonos y la comunicación se hace usando la Red de Telefonía Pública Conmutada. Cada usuario dispone de un solo cable hacia la red, aunque está en condiciones de comunicarse con cualquier teléfono fijo del mundo. No existe desde cada origen un cable hacia cada potencial destino de una comunicación de voz, sino que hay una red de comunicaciones telefónicas de uno o más proveedores que los vincula. Esta solución se usa mucho más frecuentemente que el recurso de conectar directamente los dispositivos mediante un enlace punto a punto.

Lo mismo sucede con las redes destinadas a las comunicaciones entre otro tipo de dispositivos, como las computadoras. Cada equipo dispone de único cable que lo une a la red, más allá que pueda comunicarse con otro ubicado en el mismo edificio, en otra ciudad o en cualquier

lugar del mundo. Nuevamente, la solución al problema de las comunicaciones entre dos computadoras es usar redes de comunicaciones, conocidas genéricamente como Redes de Datos.

1.2 Clasificación de las Redes de Datos

Desde sus orígenes, las Redes de Datos se clasifican en dos grandes categorías: las Redes de Área Amplia *(WAN – Wide Area Network)* y las Redes de Área Local *(LAN – Local Area Network)*. Posteriormente se agregaron otras, como las Redes de Área Personal *(PAN – Personal Area Network)* y las Redes de Área Metropolitana *(MAN – Metropolitan Area Network)*.

Las diferencias entre estas Redes son cada vez menores en algunos aspectos, tanto en términos tecnológicos como en cuanto a sus posibles aplicaciones. No obstante, la perspectiva del alcance geográfico sigue siendo una clasificación útil y didáctica que se conserva para organizar los estudios.

Las redes LAN tienen una cobertura geográfica pequeña, como un edifico o un *campus*, y hay dos configuraciones habituales: las LAN conmutadas, cableadas o alámbricas, y las LAN inalámbricas, *wireless* LAN o WLAN (Figura 1.1). Los medios de transmisión más comunes para la interconexión en redes LAN cableadas son el par trenzado (apantallado o no) y la fibra óptica. Entre los dispositivos activos habituales están el conmutador Ethernet *(Ethernet switch)* para las LAN Cableadas Ethernet y el Punto de

Acceso Wi-Fi *(AP Access Point)* para las LAN Inalámbricas Wi-Fi.

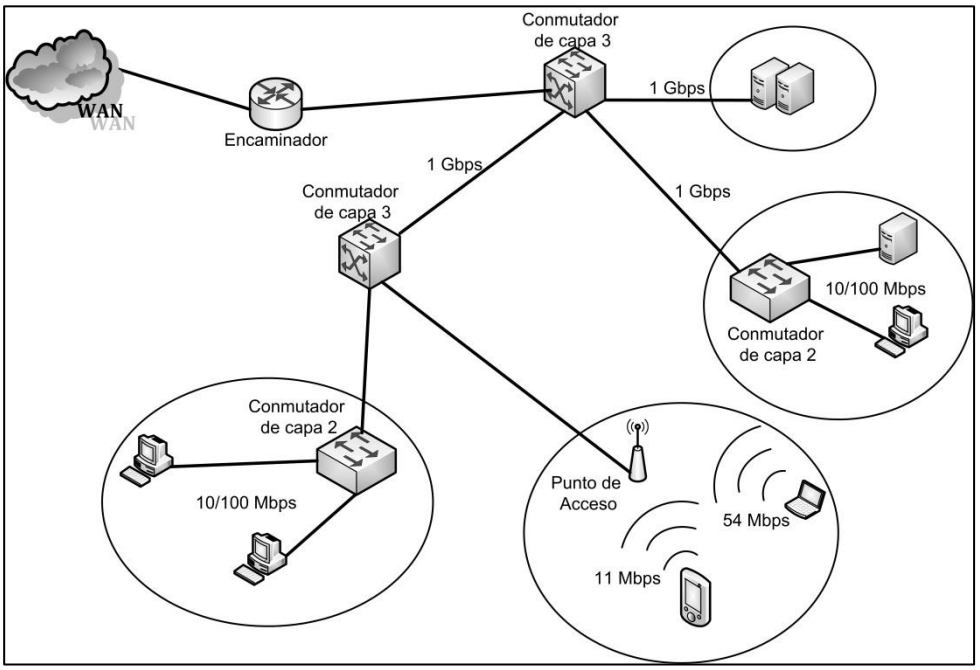


Fig. 1.1. Ejemplo de red LAN.

Generalmente, el propietario de una red LAN es una organización, empresa o persona que la utiliza para interconectar sus propios equipos. Los enlaces internos de la Red LAN Cableada e Inalámbrica pueden alcanzar velocidades estándares desde 54 Mbps hasta los 10 Gbps.

Las redes WAN cubren un área geográfica más extensa y pueden ser vistas como la integración de diversas redes LAN dispersas (Figura 1.2). Emplean tecnologías de conmutación de circuitos y de paquetes, y diversos esquemas de multiplexado. Los medios de transmisión más comunes

para interconectar las redes LAN cableadas son los medios cableados, aunque también se usan vínculos inalámbricos. Uno de los dispositivos activos habituales de las redes WAN es el encaminador *(router).*

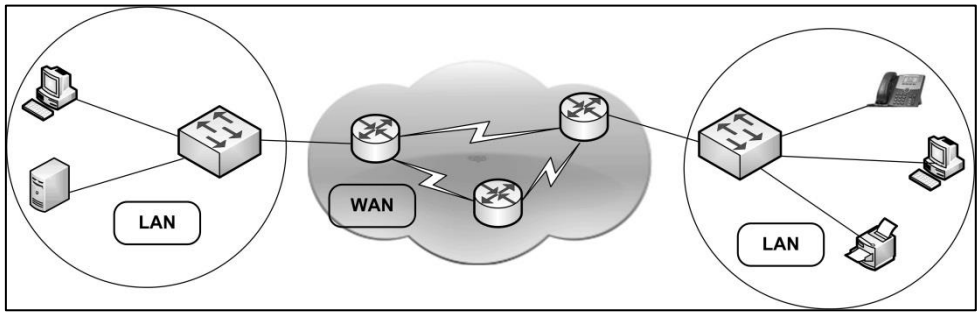


Fig. 1.2. Ejemplo de red WAN.

Las redes WAN pueden ser privadas, aunque lo más frecuente es usar redes públicas de proveedores para interconectar las redes LAN que las componen. En general, tienen menor tasa de velocidad que las LAN.

1.3 Tendencias de las Redes de Datos

La demanda de las redes WAN está en aumento para apoyar el enorme crecimiento de la velocidad y cantidad de redes LAN. La gran proliferación de las LAN de alta velocidad en ámbitos empresariales ha requerido alternativas más sólidas para interconectar las redes de este tipo, que usualmente están geográficamente dispersas.

Basándose en la Recomendación X.25 del UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT), se construyeron –y se siguen construyendo– varias generaciones de servicios de conmutación de alta velocidad para redes

WAN, que actualmente están disponibles para el ámbito empresarial. Cada una tiene sus fortalezas y debilidades relativas; los servicios WAN más demandados por las empresas son: Retransmisión de Tramas (*Frame Relay*), ATM (Modo de Transferencia Asíncrono - *Asynchronous Transfer Mode*), MPLS (Conmutación por Rótulo Multiprotocolo - *Multi Protocol Label Switching*), y WAE (Ethernet de Área Amplia – *Wide Area Ethernet*).

También se utiliza a Internet como infraestructura WAN primaria o secundaria para conectar computadoras en lugares dispersos. Cada vez es más raro que un negocio no tenga presencia en Internet a través de su sitio web, o sus propios desarrollos de *intranets*, *extranets* y redes privadas virtuales (VPN).

Además, los sistemas inalámbricos suelen mencionarse asimismo como una de las alternativas para brindar servicios WAN. Sin embargo, los diseñadores de redes empresariales no pueden pasar por alto las desventajas de las comunicaciones inalámbricas con respecto a los medios guiados (cable, fibra óptica). Éstas se caracterizan por su extrema dependencia de las condiciones de entorno, su baja eficiencia en escenarios con múltiples dispositivos móviles y el débil soporte a niveles adecuados de la calidad del servicio (*Quality of Service* – QoS).

1.4 Símbolos de los dispositivos de red

La simbología de redes es la forma gráfica que se emplea para representar los elementos que componen una

red de computadoras: son los símbolos que se presentan en los proyectos, esquemas o planeamientos de redes futuras.

A los dispositivos se los clasifica en dispositivos finales o intermedios de la red. Por ejemplo, entre los finales se usan símbolos diferenciados para distinguir una computadora de escritorio –PC (*host*)– de una portátil (*notebook, laptop, netbook,* o *minibook* en general). También encontraremos servidores que son computadoras que comparten sus recursos o brindan algún tipo de servicios a las demás computadoras clientes de una red.

Como ejemplo de dispositivos intermedios se encuentra el *switch* o conmutador que normalmente interconecta dispositivos finales de red. El *switch* es el dispositivo intermedio más utilizado en redes LAN; también está el *router*, encaminador, o ruteador que se usa para interconectar redes LAN.

Finalmente, entre las representaciones simbólicas se utiliza la nube para graficar resumidamente a un grupo de dispositivos de red cuando sus detalles no son importantes en el análisis; el enlace LAN para representar la conexión por cable en una red LAN y el enlace WAN para realizar conexiones entre redes LAN.

La Figura 1.3 muestra los símbolos que utilizaremos en este libro.

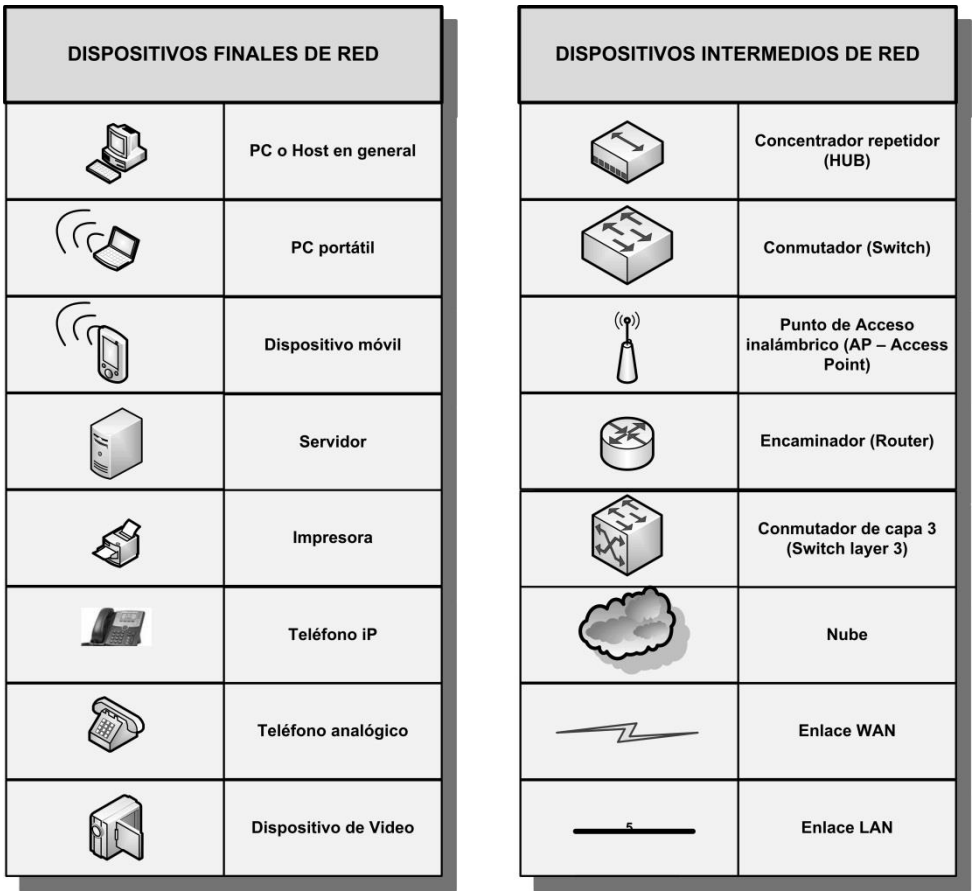


Fig. 1.3. Símbolos de los dispositivos de red.

CAPÍTULO 2

Conjunto de Protocolos TCP/IP

2.1 Introducción

- **2.1.1 Tecnología de Interconexión**
- **2.1.2 Arquitectura de Protocolos**
- **2.1.3 Arquitectura de Protocolos e Internet**
- **2.1.4 Evolución de TCP/IP y de Internet**

2.2 Modelo OSI

2.3 Familia de Protocolos de Internet o TCP/IP

- **2.3.1 Introducción**
- **2.3.2 Capas de TCP/IP**
- **2.3.3 Algunas consideraciones importantes sobre TCP/IP**
- **2.3.4 Conjunto de Protocolos TCP/IP**

2.4 Bibliografía y Referencias

- **2.4.1 Libros impresos**
- **2.4.2 Enlaces y Referencias**

Capítulo 2

Conjunto de Protocolos TCP/IP

2.1 Introducción

2.1.1 Tecnología de Interconexión

En los 1970 surgió la tecnología de interconexión para vincular diversas redes independientes, que usaban distintas tecnologías, con el objeto de que operaran como una unidad coordinada. La interconexión (*internetworking*) se basa en un conjunto de convenciones de comunicaciones que las redes individuales usan para operar entre ellas. Esta tecnología oculta los detalles del hardware de la red y permite que las computadoras se comuniquen independientemente de sus conexiones físicas. Dado las características de esta tecnología, cualquier arquitectura de hardware que soporte redes de conmutación de paquetes podrá hacer funcionar una amplia variedad de aplicaciones y utilizar sistemas operativos arbitrarios.

Entre los 1970s y 1980s, algunas agencias del gobierno de EUUU establecieron la importancia y potencial de la tecnología de interconexión, y las bases de líneas de investigación dirigidas a hacer posible una Internet global. Específicamente, la Agencia de Proyectos de Investigación Avanzada de Defensa de EEUU (DARPA) precisó un conjunto de estándares de red y convenciones para interconectar

redes, retransmitir tráfico, y además, detalles de cómo se comunican las computadoras.

2.1.2 Arquitectura de Protocolos

¿Por qué es necesaria una arquitectura de protocolos?

En el intercambio de datos entre computadoras, terminales y/u otros dispositivos fijos o móviles de procesamiento, los procedimientos involucrados pueden ser bastantes complejos. Por ejemplo, consideremos la transferencia de un archivo entre dos computadoras. En este caso, debe haber un camino entre ambas, directo o a través de una o más redes de comunicaciones. Es evidente que debe haber un alto grado de cooperación entre las computadoras involucradas. Y en lugar de implementar toda la lógica para llevar a cabo la comunicación en un único módulo, el problema se divide en subtareas. En una arquitectura de protocolos, los distintos módulos se disponen formando una pila vertical.

Cada capa de la pila realiza el subconjunto de tareas relacionadas entre sí que son necesarias para comunicarse con el otro sistema. Por lo general, las funciones más básicas se dejan a la capa inmediatamente inferior, olvidándose en la capa actual de los detalles de estas funciones. Además, cada capa proporciona un conjunto de servicios a la capa inmediatamente superior. Idealmente, las capas deberían estar definidas de forma tal que los cambios en una capa no necesitaran cambios en las demás.

Evidentemente, para que haya comunicación se necesitan dos entidades, por lo que debe existir la misma pila de capas o funciones en los sistemas. La comunicación se consigue haciendo que las capas correspondientes, o pares, intercambien bloques de datos que verifican una serie de reglas o convenciones denominadas protocolos.

Las arquitecturas de protocolos normalizadas más realistas y complejas son el Modelo OSI y el Conjunto de Protocolos TCP/IP. Estas arquitecturas han sido determinantes y básicas en el desarrollo de los estándares de comunicación. Las arquitecturas de protocolos normalizadas tienen las siguientes ventajas:

- Los fabricantes están motivados para implementar las normalizaciones con la esperanza de que, debido al uso generalizado de las normas, sus productos tendrán un mercado mayor, y
- Los clientes pueden exigir que cualquier fabricante implemente los estándares, y por lo tanto, obtener costos menores y seguridad en la inversión.

Tanto el Modelo OSI como TCP/IP se basaron en principios o propiedades fundamentales:

- Encapsulado: Ocultar la arquitectura de red subyacente a los usuarios y permitir la comunicación sin demandar conocimiento de dicha estructura.
- Independencia topológica: No obligar al uso de una topología de interconexión de red.

- Independencia de ubicación: Enviar datos a través de las redes intermedias no demandando que estén directamente conectadas a las computadoras origen o destino.
- Identificación universal: Todas las computadoras en la interconexión comparten un conjunto universal de identificadores de máquina (nombres o direcciones).
- Independencia de redes y computadoras: El conjunto de operaciones para establecer una comunicación o transferir datos debe permanecer independiente de las tecnologías de la red subyacente y de la computadora destino.

Además, estas arquitecturas debieron diseñarse para afrontar los problemas típicos que aparecen cuando se comunican las computadoras sobre una red de datos:

- Fallas de hardware: Una computadora o un encaminador (*router*) pueden fallar por problemas en el hardware o debido al sistema operativo. Además, un enlace de comunicaciones puede fallar o salirse de servicio. En cualquier caso, un programa (software) de la pila de protocolos debe detectar tales fallas y recuperarse si es posible.
- Congestión de red: Las redes tienen capacidad finita, aunque puede pretenderse someterlas a un exceso de tráfico. Un software de la pila de protocolos debe organizar una forma de detectar la congestión y suprimir cualquier tráfico ulterior para evitar que la situación empeore.
- Retardo o pérdida de paquetes: Algunas veces, los paquetes experimentan retardos extremadamente largos o simplemente se pierden. Un software de la pila de

protocolos necesita aprender acerca de las fallas o adaptarse a los grandes retardos.

- Corrupción de los datos: La interferencia eléctrica o magnética, o las fallas del hardware pueden causar errores de transmisión que corrompan los contenidos de los datos transmitidos. La interferencia puede ser severa en ambientes inalámbricos. Un software de la pila de protocolos debe detectar y recuperarse de tales errores.
- Duplicación de datos o arribos fuera de orden: Las redes que ofrecen múltiples rutas pueden transmitir los paquetes fuera de secuencia o pueden liberar duplicados de paquetes. Un software de la pila de protocolos necesita registrar los paquetes y remover los duplicados.

Estos problemas implican varios protocolos trabajando cooperativamente. En los múltiples protocolos hay que definir las representaciones necesarias para los datos que se pasan entre los módulos del software de comunicación. Este pasaje de las representaciones de los datos entre protocolos usa una secuencia lineal, donde la salida de un protocolo es la entrada de otro adyacente.

Conceptualmente, el envío de un mensaje de una aplicación sobre una computadora a una aplicación sobre otra, implica transferir el mensaje hacia abajo en las capas sucesivas del software de los protocolos en la máquina transmisora, retransmitir el mensaje a través de la red y transferir el mensaje hacia arriba a través en las capas sucesivas del software de los protocolos en la máquina receptora.

Se denomina PDU a la información intercambiada entre entidades pares, es decir, dos entidades pertenecientes a la misma capa, pero en dos sistemas diferentes, utilizando una conexión.

Para establecer la transmisión de datos, la capa de aplicación recibe el mensaje del usuario y le añade una cabecera constituyendo así la PDU de la capa de aplicación. La PDU se transfiere a la capa de aplicación del nodo destino, que elimina la cabecera y entrega el mensaje al usuario. Un criterio similar se utiliza para las restantes capas.

2.1.3 Arquitectura de Protocolos TCP/IP e Internet

DARPA comenzó a trabajar en la tecnología de interconexión a mediados de los 1970s, y ha sido reconocida como la fundadora de las líneas de investigación en redes de conmutación de paquetes y pionera en varias ideas con su bien conocida ARPANET (*Advanced Research Projects Agency Network*). ARPANET usó enlaces punto a punto cableados de un proveedor de red, pero también realizó estudios sobre redes de radio y canales de comunicación satelital. DARPA planificó reuniones informales de investigadores para compartir ideas y discutir sus resultados experimentales sobre las tecnologías de interconexión. Informalmente, al grupo se lo conoció como el Grupo de Investigación de Internet (*Internet Research Group*). En 1979, varios investigadores estaban involucrados en el diseño de los protocolos y arquitectura del Internet emergente.

El Internet global comenzó alrededor de 1980 cuando DARPA inició el proceso de conversión de las computadoras de sus redes de investigación a los nuevos protocolos TCP/IP. La ARPANET rápidamente se convirtió en el backbone del nuevo Internet y fue utilizada por los primeros experimentos de TCP/IP. La transición se completó en el año 1983.

Para estimular el uso en ambientes universitarios, ARPA hizo una implementación de bajo costo usando una versión del sistema operativo UNIX, conocida como la Distribución de Software Berkeley (BSD) de la Universidad de California. De esta forma, rápidamente se integraron los protocolos TCP/IP y UNIX. Además, UNIX Berkeley creó una nueva abstracción de sistema operativo, conocida como *socket*, que permitió que las aplicaciones accedieran a los protocolos de Internet. Esto facilitó el uso de TCP/IP por parte de los programadores.

Luego, la *National Science Foundation* (NSF) jugó un rol activo para expandir la interconexión TCP/IP a tantos científicos como fuese posible. En 1985, NSF comenzó un programa para establecer redes de acceso centralizadas alrededor de 6 centros con supercomputadoras. En paralelo, varias corporaciones de computadoras, de petróleo, automotrices, de firmas electrónicas, de compañías farmacéuticas se conectaron a Internet. Las compañías medias y pequeñas comenzaron a conectarse en los 1990s.

En 1984, Internet usando TCP/IP tenía más de 1.000 usuarios, y para 1993 excedía los 14.000.000. En 2001, el

tamaño superó los 500.000.000, y en 2014, Internet alcanzó prácticamente los 3.000.000.000 de usuarios.

2.1.4 Evolución de TCP/IP y de Internet

Internet ha crecido rápidamente y nuevos protocolos están siendo propuestos constantemente. La exigencia y demanda más significativa no es sólo el crecimiento de las conexiones de red, sino también las nuevas tecnologías de red, el tráfico adicional y los nuevos patrones de tráfico que aparecen.

Como se observa, ni Internet ni TCP/IP son estáticos. Las innovaciones continúan cuando se desarrolla una nueva aplicación y se usan nuevas tecnologías para mejorar los mecanismos e infraestructura subyacente.

Por ejemplo, uno de los esfuerzos más significativos, en Internet y TCP/IP, involucra una revisión del Protocolo de Internet IP. La versión corriente del Protocolo de Internet (IPv4) ha permanecido casi sin cambios desde su establecimiento a fines de los 1970s. Sin dudas, IP ha demostrado claramente que fue una propuesta flexible y potente. En ese periodo de tiempo se han producido importantes cambios tecnológicos: apareció la tecnología inalámbrica, o el ancho de banda de los enlaces se multiplicó por un factor de 1.000.000, por ejemplo. La IETP (*Internet Engineering Task Force*) asignó a la revisión de la versión de IP el número 6 (IPv6). IPV6, inherentemente tiene varios de los conceptos, principios y mecanismos encontrados en IPv4. Aunque IPv6 cambia la mayoría de los detalles del protocolo.

2.2 El Modelo OSI

El primer modelo de capas se basó en los trabajos tempranos realizados por la Organización Internacional de Estandarización (ISO – *International Organization for Standarization*), conocido como Modelo de Referencia de *Open System Interconnection* ISO. Frecuentemente referido como el modelo OSI. Desafortunadamente, el modelo OSI es un trabajo anterior a Internet, no describe bien los protocolos de Internet y contiene capas no usadas por los protocolos TCP/IP. Por otro parte, en lugar de una capa dedicada a 'internet", el modelo OSI se diseñó para una simple red y tiene una capa de "red". El modelo contiene 7 capas conceptuales organizadas como en la Figura 2.1.

Aunque fue diseñado para suministrar un modelo conceptual y no una guía de implementación, el esquema de capas OSI fue usado como la base de implementaciones tempranas de protocolos de red. Entre los protocolos comúnmente asociados con el modelo OSI, la suite de protocolos conocidos como X.25 fue probablemente el más reconocido y ampliamente usado. X.25 fue adoptado para las redes de datos públicas y se volvió especialmente popular en Europa.

Los formatos de información, el proceso de encapsulamiento en la computadora que transmite datos de la aplicación X, y el desencapsulado de la computadora que recibe datos de la aplicación Y, para cada una de las capas, se muestran en la Figura 2.2.

Fig. 2.1 Capas del Modelo de Referencia OSI.

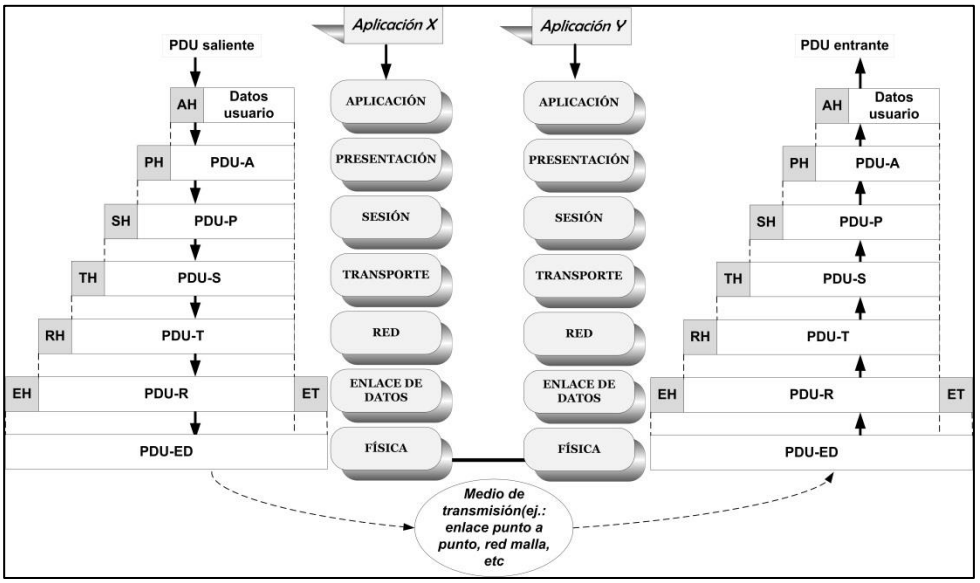


Fig. 2.2 Proceso de encapsulado en el Modelo OSI.

2.3 Familia de Protocolos de Internet o TCP/IP

2.3.1 Introducción

El segundo mayor modelo de capas no apareció desde una cuerpo o institución de estándares formal. El modelo surgió desde los investigadores que diseñaron el Internet y la suite de protocolos TCP/IP. Cuando los protocolos TCP/IP se volvieron populares, los proponentes del más viejo modelo OSI intentaron ajustar su modelo para acomodar TCP/IP. Sin embargo, el problema no pudo resolverse dado que el modelo OSI original no proveía una capa de internet, y las capas de sesión y presentación no son pertinentes a los protocolos TCP/IP.

Una de las mayores diferencias conceptuales entre los modelos de capa OSI y TCP/IP aparecen debido a la forma en que fueron definidos. El modelo OSI fue prescriptivo, es decir, la organización ISO convocó a un comité que escribió las especificaciones sobre cómo deberían construirse los protocolos. Luego, comenzaron a implementarlos. La cuestión importante es que el modelo anticipa a la implementación. Por el contrario, el modelo de Internet es descriptivo, dado que los investigadores consumieron años entendiendo cómo estructurar los protocolos, construyendo implementaciones prototipo y documentando los resultados. Luego que los investigadores comprendieron el diseño se construyó el modelo.

Los protocolos TCP/IP están organizados en 5 capas conceptuales; 4 capas definen el procesamiento de paquete y una 5ª capa define el hardware de red convencional. La Figura 2.3 muestra la relación entre las capas del Modelo OSI y el Conjunto TCP/IP.

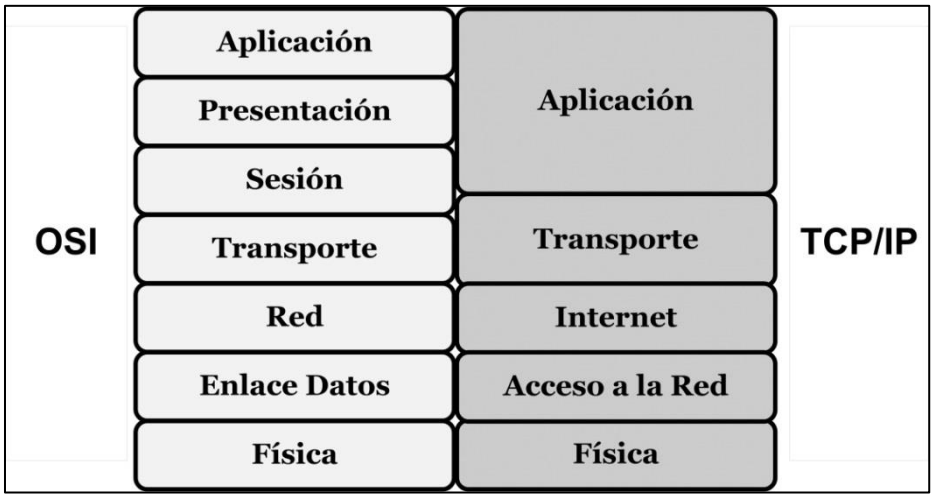


Fig. 2.3 Vista de las capas del Modelo OSI y el Conjunto TCP/IP.

En la Figura 2.4 se observa el procesamiento de encapsulado y los nombres de los mensajes según la capa para TCP/IP.

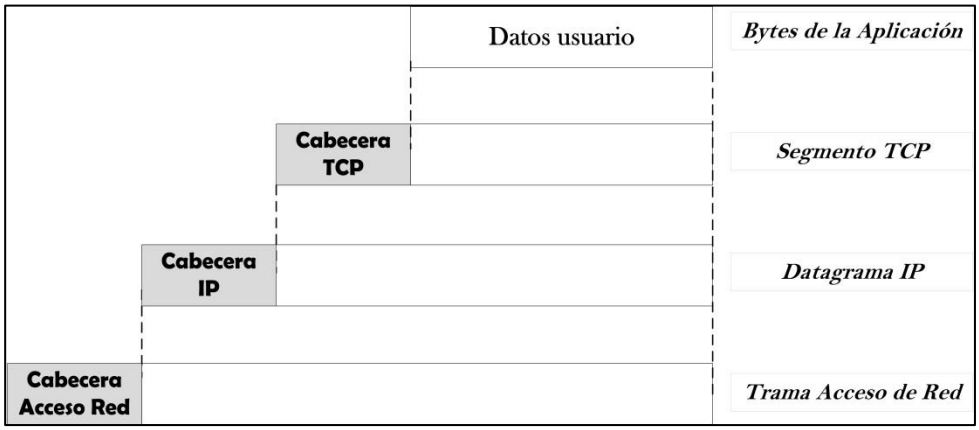


Fig. 2.4 Encapsulado y nombres de los mensajes TCP/IP.

2.3.2 Capas de TCP/IP

El propósito general de cada capa es el siguiente:

- Capa de aplicación: En la capa superior, los usuarios invocan los programas de aplicación que acceden a los servicios disponibles a través de una interconexión TCP/IP. Una aplicación interactúa con uno de los protocolos de la capa de transporte para enviar o recibir los datos. Cada programa de aplicación pasa los datos en la forma requerida por la capa de transporte para el envío.
- Capa de transporte: La función primaria de la capa de transporte es suministrar comunicación desde un programa de aplicación a otro. Tales comunicaciones son llamadas extremo a extremo a causa de que involucran las aplicaciones sobre dos puntos extremos más que los encaminadores intermedios. Una capa de transporte puede regular el flujo de información. Puede también proveer transporte confiable, asegurando que los datos arriben sin error y en secuencia. Para hacer esto, el software del protocolo de transporte del lado de la recepción envía reconocimientos y del lado de transmisión retransmite los paquetes perdidos. El software de transporte divide la secuencia de datos a transmitir en pequeñas piezas (algunas veces llamados segmentos) y pasa cada paquete de acuerdo a una dirección destino a la capa siguiente para transmisión. Como se describe luego, una computadora de propósito general puede tener múltiples aplicaciones accediendo a las redes en un momento determinado. La capa de transporte debe aceptar los datos desde algunas aplicaciones y enviarlos a la capa siguiente más baja. Para hacer esto, a cada segmento le suma

información adicional, incluyendo los valores que identifican qué programa de aplicación envía los datos y qué aplicación en el extremo de recepción recibe los datos. Los protocolos de transporte también usan una verificación para protegerse contra los errores que causan los cambios de bits. La máquina receptora usa el control de verificación para asegurarse que el segmento arribó intacto y usa la información del destino para identificar el programa de aplicación al cual debería liberarse.

- Capa de internet: La capa de internet manipula la comunicación desde una computadora a otra. Acepta las solicitudes para enviar un paquete desde la capa de transporte con una identificación de la computadora a la cual debería enviarse el paquete. El software del protocolo encapsula el paquete de transporte en un paquete IP, llena la cabecera y envía el paquete IP directamente al destino (si el destino está sobre la red local), o lo envía a un encaminador para que sea retransmitido a través de las redes (si el destino es remoto). El software de la capa de internet también manipula los paquetes IP entrantes, verificando su validez y usando el algoritmo de retransmisión para decidir si el paquete debería procesarse localmente o retransmitirlo. Para los paquetes destinados a la máquina local, el software de la capa de internet elige el protocolo de transporte que gestionará el paquete.
- Capa de interfaz de red: La capa más baja del software TCP/IP comprende una capa de interface de red, responsable de aceptar los paquetes IP y retransmitirlos a una red específica. Una interfaz de red puede consistir en un driver de dispositivo (por ejemplo, cuando la red es LAN

a la cual la computadora se vincula) o un subsistema complejo que implementa un protocolo de enlace de datos.

2.3.3 Algunas consideraciones importantes sobre TCP/IP

En la práctica, el software del protocolo de interconexión TCP/IP es mucho más complejo que el modelo simple de la Figura 2.3. Cada capa toma decisiones acerca de la corrección del mensaje y elige una acción apropiada en base al tipo de mensaje o la dirección destino. Por ejemplo, la capa de internet en la máquina receptora debe decidir si el mensaje ha alcanzado el destino correcto. La capa de transporte debe decidir qué programa de aplicación debería recibir el mensaje.

Se observa que los protocolos TCP/IP colocan mucho de la inteligencia en los *hosts*. En Internet, los encaminadores retransmiten los paquetes, pero no participan en los servicios de capa superior como los *hosts*.

Por otro lado, el modelo de capas incluye dos límites conceptuales que pueden no ser obvios: un límite de dirección de protocolo que separa el direccionamiento de alto nivel y bajo nivel, y un límite de sistema operativo que separa el software de protocolo de los programas de aplicación.

Los límites se caracterizan por:

- Límite de direcciones de protocolo de alto nivel: Existen diferentes direcciones que usan los varios tipos de hardware de red. Es importante distinguir dónde se usan las dos formas de direccionamiento. El modelo de capas lo

deja claro. Hay un límite conceptual entre la Capa 2 y la Capa 3. Las direcciones hardware o físicas (MAC) se usan en las Capas 1 y 2, pero no más arriba. Las direcciones de internet se usan en las Capas 3 a 5, pero no por el hardware subyacente. Resumiendo: Los programas de aplicación y todo el software de protocolo desde la capa de internet hacia arriba usan sólo direcciones de Internet; las direcciones usadas por el hardware de red están aisladas en las capas inferiores.

- Límite de sistema operativo: Existe otro límite importante: la división entre el software de protocolo que es implementado en un sistema operativo y el software de aplicación que no lo es. Aunque los investigadores han experimentado que una parte de TCP/IP esté en una aplicación, la mayoría de las implementaciones colocan el software de protocolo en el sistema operativo, donde puede ser compartido por todas las aplicaciones. El límite es importante debido a que el pasaje de datos entre los módulos dentro del sistema operativo es mucho menos oneroso que pasar datos entre el sistema operativo y una aplicación. Se necesita una API (*application program interface*) especial que permita que una aplicación interactúe con el software de protocolo.

Finalmente, se ha indicado que el apilado de capas es una idea fundamental que suministra la base para el diseño de protocolos. Esto permite al diseñador dividir un problema complicado en subproblemas y resolver cada uno independientemente. Desafortunadamente, el software que resulta de una división en capas estricta puede ser

extremadamente ineficiente. Como un ejemplo, consideremos el trabajo de la capa de transporte. La misma debe aceptar una secuencia de bytes desde un programa de aplicación, dividir la secuencia en segmentos, y enviar cada segmento a través de la red subyacente. Para optimizar las transferencias, la capa de transporte debería elegir el tamaño de segmento más grande que permitirá a un segmento viajar en una trama de la red. En particular, si la máquina destino está unida directamente a la misma red que la de origen, sólo una red física estará involucrada en la transferencia y el emisor puede optimizar el tamaño de segmento para esa red. Si el software de protocolo preserva estrictamente el apilado de capas, la capa de transporte no puede saber cómo el módulo de internet retransmitirá el tráfico o cuáles redes ataca directamente. Y por lo tanto, la capa de transporte no entenderá los formatos de los paquetes usados por las capas inferiores, ni será capaz de determinar cuántos bytes se sumarán a la cabecera del mensaje a enviar. Así, el apilado de capas estricto impide a la capa de transporte optimizar las transferencias.

2.3.4 Conjunto de Protocolos TCP/IP

Los diferentes protocolos dentro de TCP/IP se mantienen de forma regular por un conjunto de Grupos de Trabajo (*Task Force*) que son parte de la organización de Internet (Figura 2.5).

Cada capa interactúa con sus capas adyacentes inmediatas. Sin embargo, la arquitectura TCP/IP no requiere el uso de cada capa individual. La Figura 2.5 sugiere que es

posible desarrollar aplicaciones que invoquen directamente los servicios de cualquiera de las otras capas (respetando lógicamente la jerarquía). La mayoría de las aplicaciones que requieren una comunicación confiable extremo a extremo usarán TCP (*Transmission Control Protocol*). Otras que no tengan esa demanda podrán usar UDP (*User Datagram Protocol*). Y algunas podrán usar directamente IP.

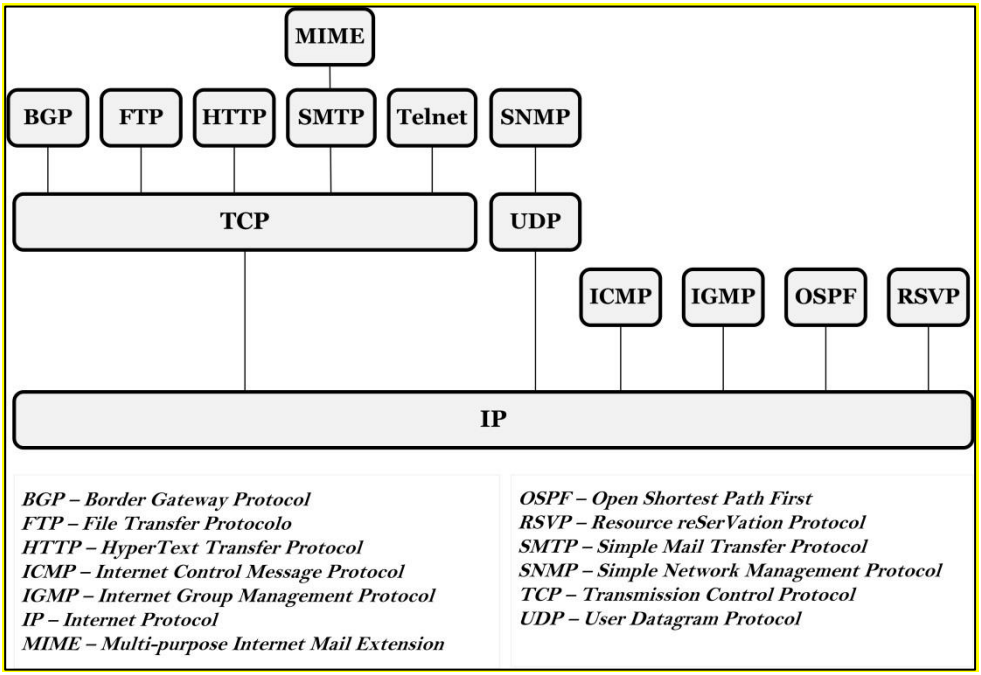


Fig. 2.5 Vista resumida del conjunto de protocolos TCP/IP por Capas

2.4 Bibliografía y referencias

2.4.1 Libros impresos

- Douglas E. Comer, “The Internet Book”, Pearson Prince Hall, 4° Ed., 2007.
- William Stallings, “Data and Computer Communications”, Pearson Education, 10° Ed., 2014.
- Douglas E. Comer, “Internetworking with TCP/IP, Volume One, Pearson Education, 6° Ed., 2014.
- William Stallings y Thomas Case, “Business Data Communications”, Pearson Education, 7° Ed., 2013.
- Uyless Black, “Tecnologías Emergentes para Redes de Computadoras”, Ed. Prentice-Hall, 1999.
- D. Comer, “Redes Globales de Información con Internet y TCP/IP”, Ed. Prentice-Hall, 3° Ed., 2000.
- CCNA de CISCO Press
- Request for Comments referidos a la temática.
- Artículos de revistas (IEEE, ACM, etc.) referidos a la temática.

2.4.2 Enlaces y Referencias

- Estándares generales de la IEEE
- http://standards.ieee.org/about/get/index.html
- Estándares de protocolos de Internet
- http://www.ietf.org/rfc.html

CAPÍTULO 3

Conmutadores, VLANs y STP

3.1 Conmutador
- 3.1.1 Dispositivos en Redes LAN
- 3.1.2 Rendimiento de la Red
- 3.1.3 Almacenamiento y Técnicas de Conmutación
- 3.1.4 Dominios de Colisión y Difusión
- 3.1.5 Configuración

3.2 ARP

3.3 VLAN
- 3.3.1 Visión general
- 3.3.2 Clasificación
- 3.3.3 Etiquetas y Troncales
- 3.3.4 Configuración

3.4 STP
- 3.4.1 Visión general
- 3.4.2 Algoritmo
- 3.4.3 Estado de Puertos
- 3.4.4 Evolución

3.5 Ejercitación

3.6 Bibliografía y Referencias
- 3.6.1 Libros impresos
- 3.6.2 Enlaces y Referencias

Capítulo 3

Conmutadores, VLANs y STP

3.1 Conmutador

3.1.1 Dispositivos en Redes LAN

El objetivo es presentar los contenidos sobre Redes Ethernet, resaltando uno de los dispositivos activos principales como es el conmutador.

En la Figura 3.1 se observa la evolución de los principales dispositivos activos usados en las Redes Ethernet. Inicialmente se usaron repetidores para su construcción. Cuando el desempeño de estas redes comenzó a bajar, a causa que demasiados dispositivos compartían el mismo segmento, se sumaron puentes (en inglés, *bridges*) para crear múltiples y más pequeños dominios de colisión. Posteriormente, las redes crecieron en tamaño y complejidad, y el puente evolucionó al moderno conmutador, extendiendo el concepto para reducir los dominios de colisión al mínimo, permitiendo la microsegmentación de la red.

Las redes de hoy en día, típicamente se construyen usando conmutadores y encaminadores y, en algunos casos, con la función de conmutación (*switching*) y encaminamiento (*routing*) en el mismo dispositivo.

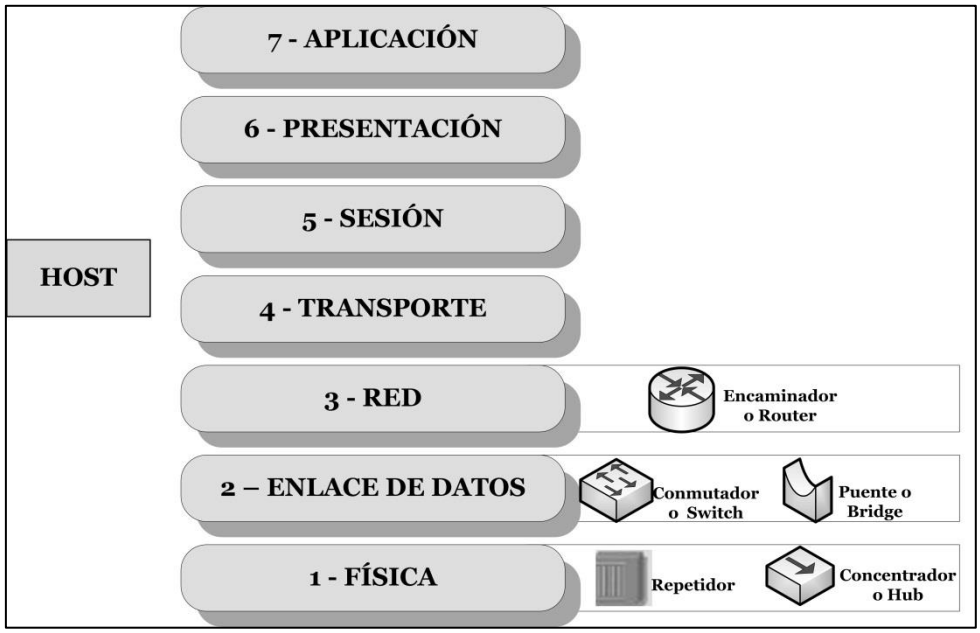


Fig. 3.1. Dispositivos de red en relación al modelo OSI.

Los conmutadores crean un circuito virtual entre dos dispositivos conectados, estableciendo una ruta de comunicación dedicado entre ellos. Al crear microsegmentación, permiten máxima utilización del ancho de banda disponible. Sin embargo, las tramas de difusión (*broadcast*), necesitadas por cualquier protocolo de red y/o aplicación, llegan a todos los dispositivos conectados sobre la red. Decimos entonces que hay un solo dominio de difusión que se extiende sobre toda la red.

Un encaminador es un dispositivo de Capa 3 usado para encaminar (enrutar o rutear) tráfico entre dos o más redes (Imagen 3.1). Los encaminadores toman decisiones basadas en grupos de direcciones o clases de red IP, en

oposición a las direcciones MAC individuales de Capa 2 con que trabajan los conmutadores.

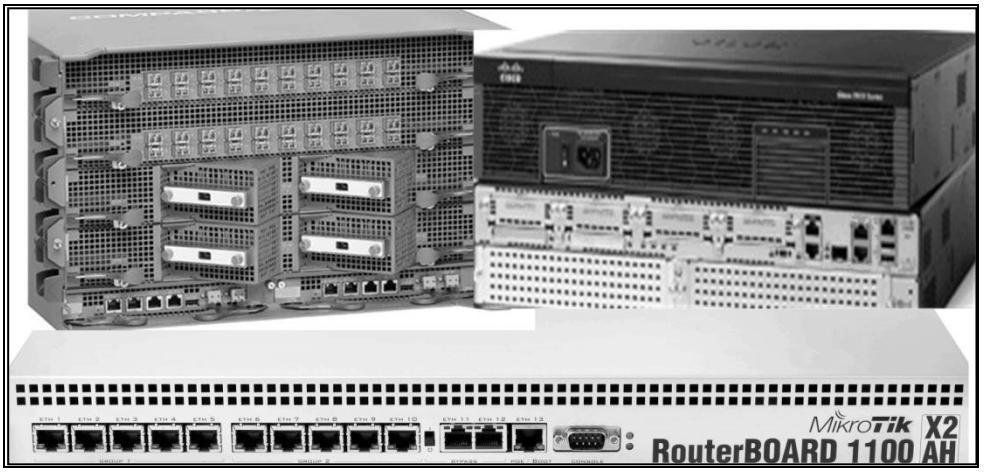


Imagen 3.1. Fotografía de encaminadores.

Las tablas de encaminamiento (*routing*) registran las direcciones de Capa 3 de las redes que están directamente conectadas a sus interfaces, y las rutas de red aprendidos desde los encaminadores vecinos. A diferencia de los conmutadores, los encaminadores no están obligados a retransmitir tramas de difusión.

En el diseño de campus multicapa escalable se distinguen los siguientes niveles: capa de núcleo, capa de distribución y capa de acceso.

Los conmutadores de capa de acceso operan en la Capa 2 del modelo OSI, y proveen servicios tales como membresía VLAN, o Virtual LAN (Imagen 3.2). El propósito principal de un conmutador de capa de acceso es permitir a

los usuarios finales entrar a la red. Deberían proveer esta funcionalidad con bajo costo y alta densidad de puertos.

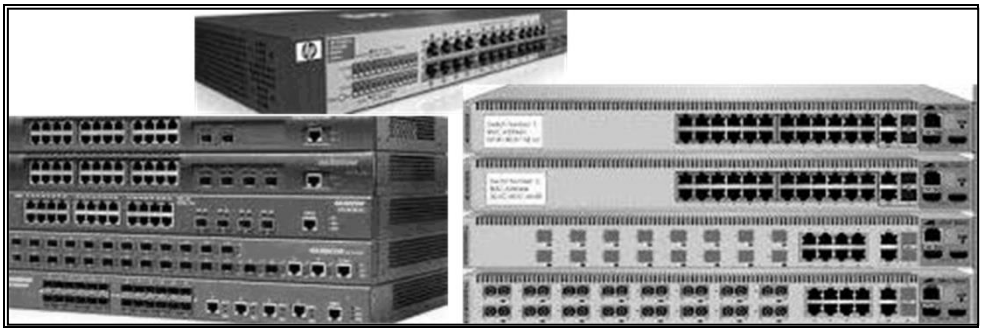


Imagen 3.2. Fotografía de conmutadores.

El propósito de la capa de distribución en el diseño multicapa (*multilayer*) del campus es proveer una definición de contorno en el cual pueda tener lugar la manipulación de paquetes. Por ejemplo, como segmentar los dominios de difusión, aplicar políticas y listas de control de acceso para filtrar paquetes y/o prevenir problemas que afecten la capa de núcleo. Los conmutadores de distribución operan en Capa 2 y Capa 3 en el modelo OSI. La capa de distribución incluye algunas funciones, tales como: la concentración de las conexiones de cableado, la definición de dominios de difusión/multidifusión (*multicast*), el encaminamiento de Virtual LANs (*VLANs*) o inter-VLAN, las transiciones entre medios de comunicación que sean necesarias, la seguridad, entre otros aspectos.

Los conmutadores de capa de distribución son puntos de concentración para múltiples conmutadores de capa de acceso. Deben ser capaces de acomodar la cantidad total de

tráfico desde los dispositivos de capa de acceso. Además, deben combinar el tráfico VLAN y aplicar las decisiones de políticas acerca del flujo de tráfico. Por estas razones los conmutadores de capa de distribución operan tanto en Capa 2 y Capa 3.

La capa de núcleo es el componente central de conmutación de alta velocidad. Si la conmutación del núcleo no tiene un módulo de encaminador asociado, se usa un encaminador externo para la función de Capa 3. Esta capa en el diseño de la red no debería realizar ninguna manipulación de paquetes, ya que volvería lenta la conmutación de paquetes. Provee una infraestructura de núcleo con pasos alternativos redundantes, y dando estabilidad a la red, ante la posibilidad de una falla de dispositivos.

3.1.2 Rendimiento de la Red

La Figura 3.2 presenta las causas típicas de congestión en la red, entre las que se destacan el tipo y cantidad de aplicaciones, el número y perfil de los usuarios y las características propias de la red, dadas por el cableado estructurado y demás dispositivos pasivos, y la clase y configuración de los dispositivos activos.

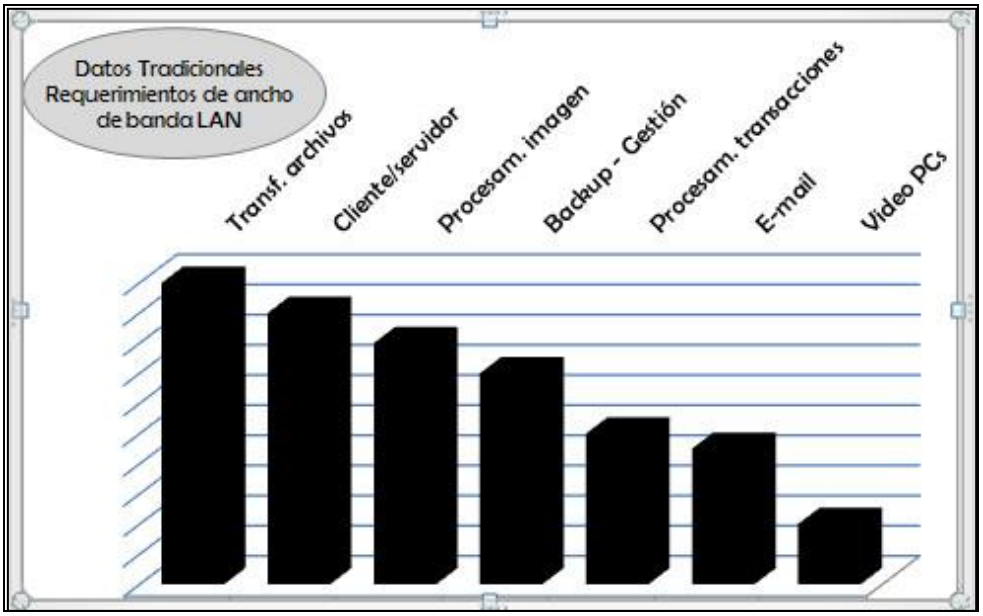


Fig. 3.2. Requerimientos de ancho de banda LAN
según las aplicaciones.

Un aspecto importante en las redes es el incremento constante en la transmisión de varias formas de tráfico de datos con alta demanda de ancho de banda, como la manipulación de archivos gráficos grandes, imágenes, video on-line, aplicaciones multimedia, etc.

Se llama latencia o retardo de la red al tiempo que a una trama le toma viajar desde la estación origen a la destino. La latencia tiene al menos tres componentes:

- El tiempo que le toma a la NIC (Placa de Interface de Red – *Network Interface Card*) origen colocar los pulsos de tensión sobre el cable y el tiempo que le toma a la NIC destino interpretar estos pulsos.
- El retardo de propagación real que es el tiempo que le toma a la señal viajar a lo largo del cable.

- La latencia sumada de acuerdo a los dispositivos de red (dependiendo si son de Capa 1, 2, o 3), y en el paso entre las dos computadoras que se comunican.

La latencia del conmutador Ethernet es el periodo de tiempo desde el momento en que el comienzo de la trama entra hasta cuando la cola de la trama sale del conmutador. Esta latencia está directamente relacionada a las características propias del conmutador, a los procesos de conmutación configurados y el volumen de tráfico.

El tiempo de transmisión es igual a la cantidad de bits enviados por el número de tiempo de bit, para una tecnología dada. Otra forma de pensar el tiempo de transmisión es como el tiempo que toma transmitir la trama. Las tramas pequeñas insumen menos tiempo, y las grandes una cantidad mayor. Por simplicidad, consideremos el tiempo de transmisión en Ethernet 10Base-T. Cada bit de Ethernet 10 Mbps ocupa una ventana de transmisión de 100 ns. Por lo tanto, transmitir 1 byte insume al menos 800 ns. Una trama de 64 bytes, la más pequeña de las tramas 10BASE-T, que permite el funcionamiento adecuado de CSMA/CD, tomará 51.200 ns o 51,2 microsegundos. La transmisión de una trama entera de 1000 bytes desde la estación origen requiere 800 microsegundos.

El tiempo de transmisión de una trama en 10 Mbps en full dúplex es igual al tiempo en half dúplex. Sin embargo, Ethernet full-dúplex permite transmitir un paquete y recibir otro diferente en el mismo momento. El Ethernet original de 10 Mbps half dúplex, puede solo usar 50%-60% del ancho de

banda disponible de 10 Mbps a causa de las colisiones y de la latencia. Y el Ethernet full-dúplex ofrece 100% de ancho de banda en ambas direcciones. Es decir, una productividad potencial de 20 Mbps, que resulta de 10 Mbps en la transmisión y 10 Mbps en la recepción. Y entonces, la productividad en half-dúplex en el transcurso del tiempo es sustancialmente menor a full dúplex.

3.1.3 Almacenamiento y Técnicas de Conmutación en Conmutadores

Un conmutador Ethernet puede usar una técnica de almacenamiento (*buffering*) para resguardar y transmitir tramas. El almacenamiento también se puede usar cuando el puerto destino está ocupado. Este buffer de memoria puede usar dos métodos para transmitir tramas:

- El almacenamiento de memoria basada en puerto: las tramas se colocan en colas que se destinan a puertos específicos; y
- El almacenamiento de memoria compartida: las tramas se resguardan en una cola de memoria común, que se comparte con todos los puertos.

Por otro lado, un conmutador Ethernet (Figura 3.3) puede usar diferentes técnicas de conmutación:

- Almacena y envía (*Store-and-forward*) – La trama entera se recibe antes de que ocurra la transmisión. Se leen las direcciones destino y origen, y se aplican los filtros antes de transmitir la trama. Además, se hace el chequeo CRC.

- Método de corte (*Cut-through*) – La trama se transmite a través del conmutador antes de haberla recibido totalmente. Sólo es necesario leer la cabecera de capa 2 para conocer la dirección MAC destino. Este modo disminuye la latencia de la transmisión, pero también reduce la detección de errores.

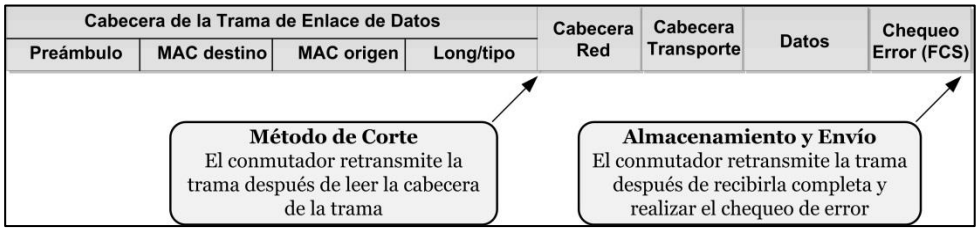


Fig. 3.3. Diferentes técnicas de conmutación de un conmutador.

Según la marca y modelo del conmutador, estos modos pueden ser configurables.

3.1.4 Dominios de Colisión y de Difusión con Conmutadores

Introducimos los aspectos a tener en cuenta en la reducción de los dominios de colisión y dominios de difusión. En general, se usa el término segmentación a cualquier técnica, que usando conmutadores y/o encaminadores, tenga como objetivo reducir sus efectos nocivos.

La Figura 3.4 muestra una red con 4 subredes que usan concentradores (*hubs*), y 1 encaminador que las vincula. Los encaminadores proveen segmentación de red, sumando una latencia de 20% a 30% sobre la red

conmutada. La latencia aumenta porque el encaminador opera en la capa de red (Capa 3) y usa las direcciones IP para determinar la mejor ruta al nodo destino.

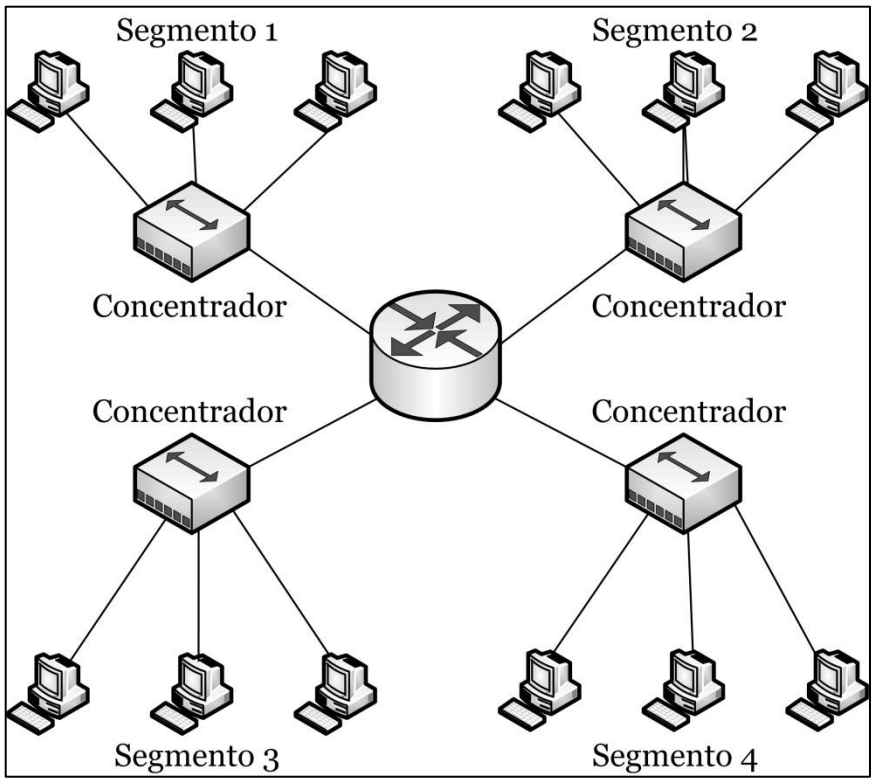


Fig. 3.4. Red con 4 subredes usando concentradores.

En general, se puede establecer que:

- Los puentes y conmutadores proveen segmentación de dominios de colisión dentro de una simple red o subred,
- Los encaminadores proveen segmentación de dominios de difusión, y brindan conectividad entre redes y subredes, y

- Los encaminadores no retransmiten tramas de difusión mientras que los conmutadores y puentes deben retransmitir las tramas de difusión.

El uso de conmutador en lugar de un concentrador, desde la perspectiva de la segmentación de colisiones, tiene como objetivo aislar el tráfico entre segmentos. En los concentradores existe un único segmento compartido. El principio de la microsegmentación de los conmutadores es que hay tantos segmentos como puertos tenga. Además, otra ventaja es que se obtiene más ancho de banda por usuario al crear dominios de colisión más pequeños.

Los conmutadores inundan o difunden tramas que pueden ser (Figura 3.5):

- Tramas de unidifusión (*unicast*) desconocidos,
- Tramas de difusión (*broadcast*) de Capa 2, o
- Tramas de multidifusión (*multicast*), a menos que esté ejecutando un protocolo tipo IGMP.

Las tramas multidifusión usan direcciones especiales de Capa 2 y Capa 3 que son enviadas a dispositivos que están unidos a ese grupo

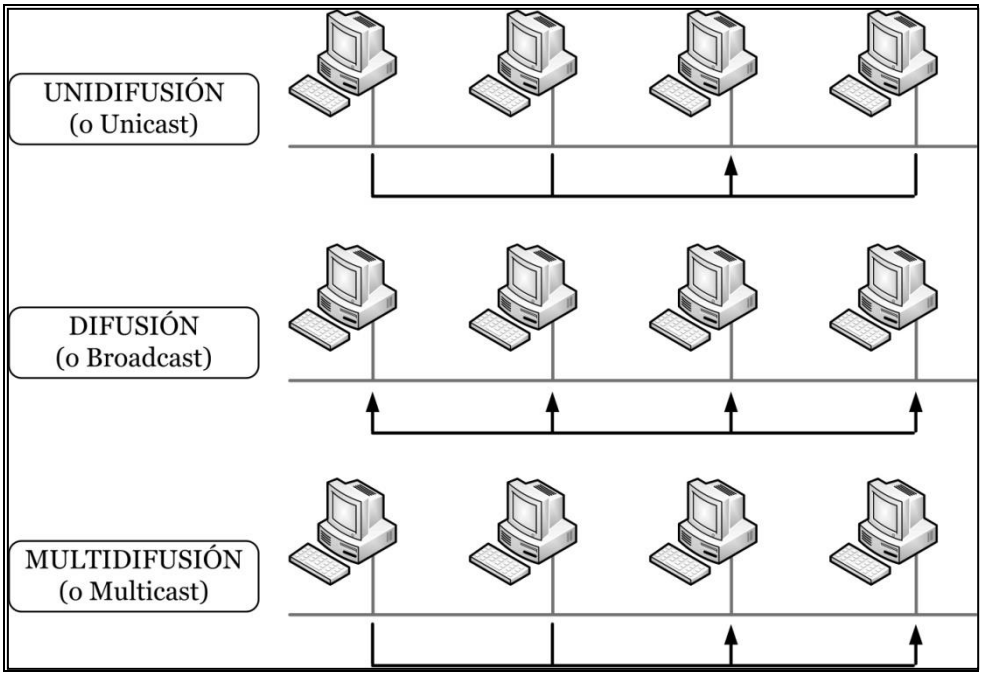


Fig. 3.5. Ejemplo de tráfico de tramas de unidifusión, difusión y multidifusión.

Un conmutador de Capa 3 es básicamente un conmutador de Capa 2 (Figura 3.6) que incluye capacidad de encaminamiento, entre redes y subredes (o VLANs), la posibilidad de filtrado de paquetes, etc. La segmentación con VLAN es fundamental para reducir los dominios de difusión con conmutadores.

La conmutación de Capa 3 (Figura 3.7) es una función de capa de red que examina la información de la cabecera (*header*) de Capa 3 de un paquete, y que retransmite según la dirección IP destino.

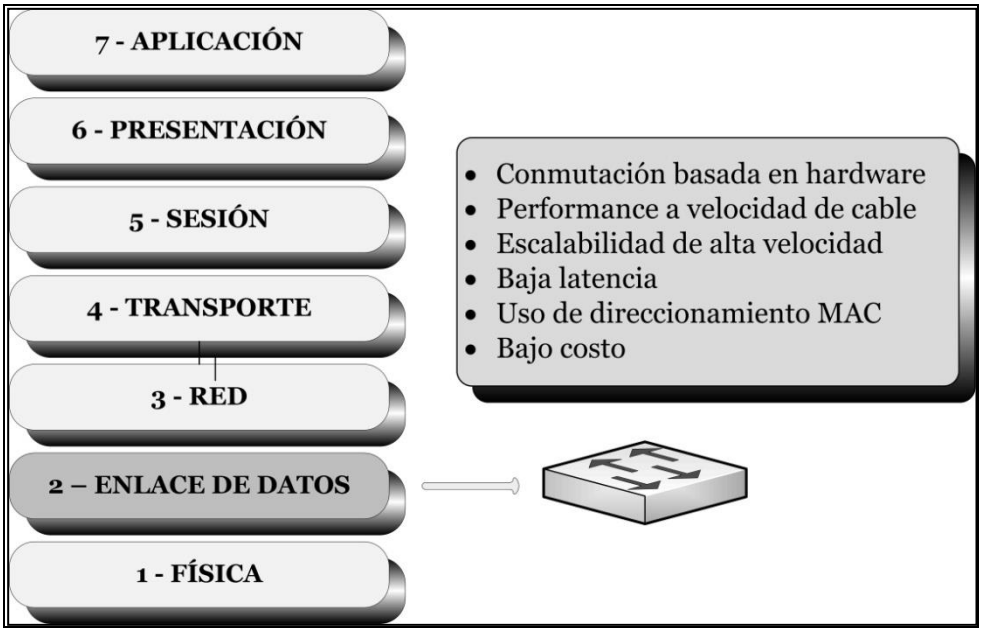


Fig. 3.6. Conmutador de Capa 2 en relación al modelo OSI.

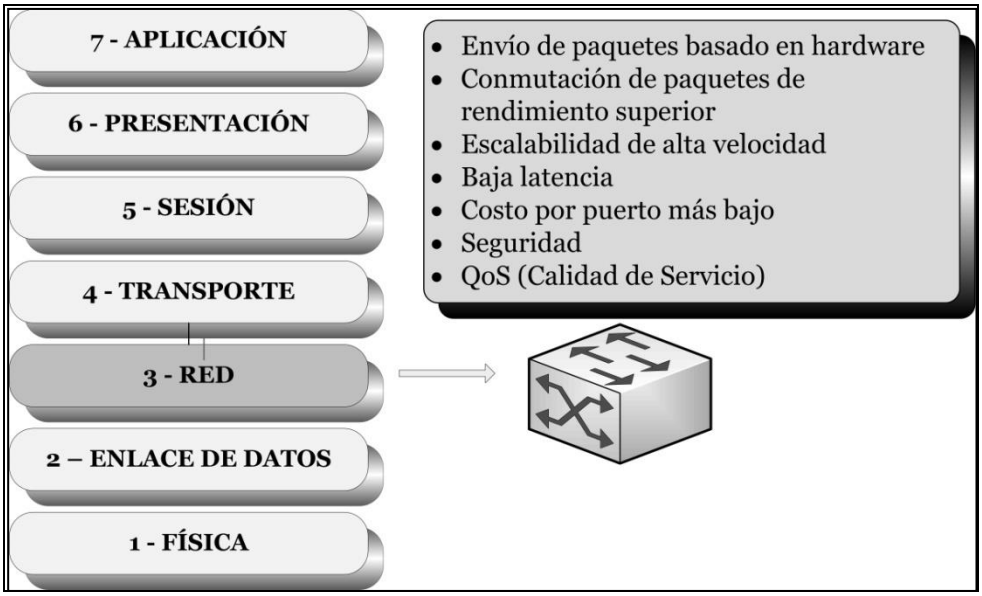


Fig. 3.7. Conmutador de Capa 3 en relación al modelo OSI.

3.1.5 Configuración de Conmutadores

Se presentan los aspectos de configuración sobre un conmutador real, tomando como ejemplo una marca, aunque las consideraciones generales son válidas a cualquier otra. Los conmutadores son computadoras especializadas y dedicadas con:

- CPU o Unidad Central de Proceso,
- Memoria del tipo RAM (Memoria de Acceso Aleatorio), y un
- Sistema Operativo.

Un conmutador se puede administrar localmente o *in-situ*, conectándose al puerto de consola para ver y hacer cambios en la configuración (Figura 3.8). O remotamente, a través de la red.

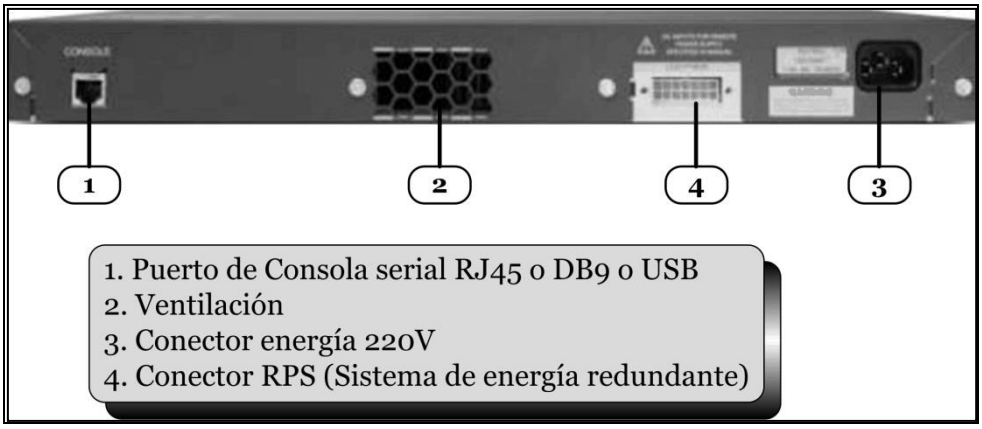


Fig. 3.8. Administración local del conmutador
a través de un puerto de consola.

El panel frontal de un conmutador tiene algunas luces o LEDs (*Light-Emitting Diode* - diodo emisor de luz) para ayudar a monitorear su actividad (Figura 3.9). Puede tener LEDs del tipo:

- Led del sistema: que indica si el sistema está encendido y funciona correctamente,
- Led de alimentación de energía eléctrica remota RPS (*Remote Power Supply*): que indica si está o no en uso la alimentación remota,
- Led de modo del puerto: que indica el estado actual del botón Modo. Los modos son usados para determinar cómo se interpretan los leds de Estado de Puerto, y
- Leds de estado de puerto: que tienen diferentes significados, dependiendo del led de Modo.

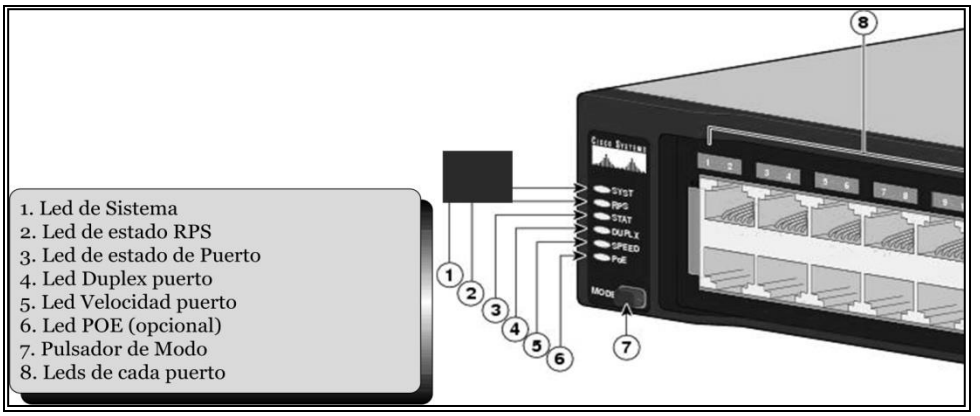


Fig. 3.9. Panel frontal de un conmutador.

Cuando se conecta el cable de alimentación al conmutador, se inicia una serie de verificaciones llamada autoprueba de encendido (*POST - power-on self test*). El led

del sistema indicará si el POST fue exitoso o si se ha producido una falla, considerado un error fatal.

Puede accederse a la configuración del conmutador conectando, a través de un cable de consola, una PC que se usa como terminal, al puerto de consola del conmutador. La interfaz de línea de comandos (*CLI – command line interface*) para los conmutadores es muy similar para todos los dispositivos de red.

En la Tabla 3.1, se muestra la instrucción *show* (según el fabricante, la instrucción puede ser *print*), con sus alternativas, aplicadas desde la interfaz de línea de comandos. Se supone que se tiene acceso y autoridad para aplicar estos comandos.

Instrucción	Descripción
show version	Da información sobre la versión del software y el hardware. Usado para ver exactamente qué modulos y software están en uso
show running-config	Muestra el archivo de configuración corriente del equipo
show interface	Muestra el estado administrativo y operacional de un puerto, de los paquetes entrantes y salientes, y de los errores
show controllers	Da información sobre el hardware del puerto, y estadísticas de la cantidad de tramas descartadas, de tramas diferidas, de errores, de colisiones, etc
show post	Indica si el equipo pasó el POST (Power On Self Test)

Tabla 3.1. Diversas alternativas de la instrucción show.

Para permitir el acceso remoto al conmutador (usando Telnet, SSH y otras aplicaciones TCP/IP) deben configurarse la dirección IP y una puerta de enlace (*default Gateway*). Por defecto, en los conmutadores CISCO la VLAN 1 es la VLAN de

administración. En una red basada en conmutadores, todos los dispositivos de interconexión deberían estar en la VLAN de administración. Esto permite que una simple estación de trabajo tenga acceso, configure y administre todos los dispositivos.

En la Figura 3.10, se muestran algunos aspectos de interés sobre la tabla de direcciones MAC del conmutador. Por ejemplo, la instrucción show se usa en este caso para informar las características y estado de la tabla MAC.

```
Switch#show mac-address-table
Dynamic Address Count:                    2
Secure Address Count:                     0
Static Address (User-defined) Count:      0
System Self Address Count:                13
Total MAC address:                        15
Maximum MAC address:                      8192
Non-static Address Table:
Destination Address Port  Address Type VLAN       Destination
------------------------------------------------------------------------
0010.7a60.ad7e            Dynamic          1 FastEthernet0/2
00e0.2917.1884            Dynamic          1 FastEthernet0/5
```

Fig. 3.10. Instrucción que da la Tabla de direcciones MAC del conmutador.

Algunos conmutadores pueden traer una aplicación web para la configuración. Estas aplicaciones aunque son más fáciles de usar también son más limitadas para la administración. Un navegador web puede acceder a este servicio usando la dirección IP y el puerto 80. El servicio

HTTP puede activarse o desactivarse, y puede elegirse la dirección del puerto (Figura 3.11).

```
Switch#show configure terminal
Enter configuration commands, one per linte. End with CNTL/
Switch(config)#ip http ?
  access-class          Restrict access by access-class
  authentication        Set http authentication method
  path                  Set base path for HTML
  port                  HTTP port
  server                Enable HTTP server
Switch(config)#ip http server
Switch(config)#ip http port ?
  <0-65535>  HTTP port
Switch(config)#ip http port 80
Switch(config)#
```

Fig. 3.11. Activación del Servidor HTTP del conmutador.

3.2 ARP - Protocolo de Resolución de Direcciones

El Protocolo ARP (Protocolo de Resolución de Colisiones - *Protocol Resolution Address*) es parte de la pila TCP/IP y responsable de encontrar la dirección hardware, física o MAC Ethernet que corresponde a una determinada dirección IP. Cada PC y también el conmutador mantiene una caché ARP con las direcciones traducidas para reducir el retardo y la carga.

Nos interesa su aplicación dentro de las redes LAN, y su relación con las direcciones físicas o MAC de Capa 2.

Los dispositivos usan direcciones IP para alcanzar otros dispositivos dentro de su propia red/subred o a través de diferentes redes/subredes. Una vez que se envía el paquete IP, estas direcciones no cambian desde el origen al destino. Las direcciones de enlace de datos, tales como las direcciones MAC Ethernet se usan para entregar el paquete IP dentro de la misma red, o a un salto a la siguiente red. Si el emisor y el receptor están sobre diferentes redes (o subredes), la dirección de enlace de datos en la trama se modificará para reflejar las nuevas direcciones de origen y destino.

Necesitamos la direcciones IP origen y destino porque identifican los dispositivos de red que se comunican, y la dirección MAC para enviar el paquete IP interno en una trama Ethernet a la red local, o a la red de siguiente salto a lo largo de la ruta (Figura 3.12). El siguiente salto puede ser el destino final.

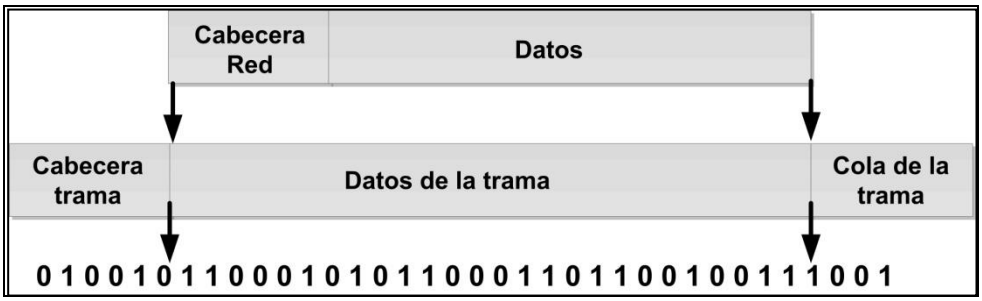


Fig. 3.12. Formato de la trama Ethernet.

Las direcciones IP de los host pertenecientes a una misma LAN, tienen en común la misma máscara de subred. La operación AND sobre la dirección IP del host y la máscara

de subred le dice al host a qué red pertenece. La dirección de red resultante debe ser común a todos los host.

¿Qué función cumple la dirección MAC destino? Permite transmitir desde un host Ethernet los datos de capa superior a un dispositivo de la misma LAN que también tenga una placa o NIC Ethernet.

¿Qué dispositivos están sobre la misma LAN? Hosts, impresoras, encaminadores, conmutadores etc. que están sobre la misma red IP y tengan configuradas una dirección IP sobre ella.

En la Figura 3.13 se presentan dos subredes separadas por un encaminador.

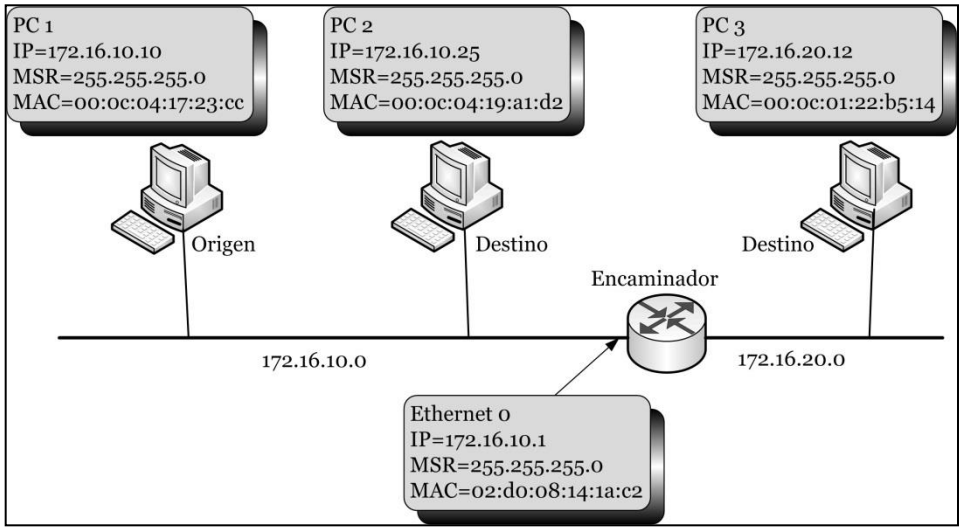


Fig. 3.13. Las subredes 172.16.10 y 172.16.20 separadas por un encaminador.

Las subredes son la 172.16.10.0 y la 172.16.20.0. ¿Cuál sería la dirección MAC destino para los paquetes IP enviados desde un host a otro de la misma LAN? La dirección MAC destino sería del dispositivo al que vamos a enviar el paquete IP, y estaría asociada con la dirección IP destino.

¿Cuál sería la dirección MAC destino para los paquetes IP enviados por un host a otro que está fuera de la LAN, sobre una red diferente? La dirección MAC destino será la dirección MAC asociada con la dirección IP de la puerta de enlace, que es la dirección IP de la NIC del encaminador de lado de la LAN origen. El host debe conocer la dirección IP de la puerta de enlace predeterminada, para comunicarse con los dispositivos fuera de su propia red, usando al encaminador como recurso encaminamiento.

¿Cómo hace para conocer el host emisor si la dirección IP fuente y la dirección IP destino están sobre la misma red? Hace una operación AND sobre su dirección IP y su máscara de subred. La dirección de red resultante debe ser la misma que al hacer la operación AND, pero con la dirección IP destino. De lo contrario están sobre diferentes redes.

Una vez que se ha determinado que el host destino está en la misma red, ¿dónde o cómo el host emisor encuentra la dirección MAC destino?

El protocolo ARP mantiene la relación o mapa entre la dirección IP y la dirección MAC. Cuando el host necesita conocer una dirección MAC mira su tabla ARP o caché ARP.

Cada dispositivo que participa en Ethernet e IP tendrá tal tabla, incluyendo los host y los encaminadores.

Pero, ¿qué sucede si la dirección IP destino no está en la tabla ARP? ¿Cómo hace para obtener la dirección MAC destino? El host debe efectuar una Solicitud ARP (*ARP Request*) del protocolo ARP.

La solicitud ARP efectúa la siguiente consulta a través de una trama de difusión: "¿Quién tiene la dirección IP 172.16.10.25? Por favor, envíeme su dirección MAC". Esa dirección MAC se suma a la tabla ARP para la próxima vez. Y el host usa esa dirección MAC para completar y enviar la trama al host de la IP destino.

En el otro caso, que se ha determinado que el host destino está en otra red, ¿dónde o cómo el host emisor encuentra la dirección MAC destino? La solicitud ARP efectúa la misma consulta anterior a través de una trama de difusión, pero sobre la IP de la puerta de enlace: "¿Quién tiene la dirección IP 172.16.10.1? Por favor, envíeme su dirección MAC". Esa dirección MAC se agrega a la tabla ARP para la próxima vez. Y el host usa esa dirección MAC para completar y enviar la trama a la puerta de enlace.

3.3 VLANs - LANs Virtuales

3.3.1 Visión General

El objetivo es presentar el concepto de VLAN, y entender su aplicación dentro de las Redes Ethernet, resaltando algunos aspectos de interés.

Las VLANs creadas en los conmutadores, proveen segmentación basada sobre dominios de difusión. Las VLANs pueden lograr dicha segmentación lógica en redes conmutadas en base a la ubicación física, en la departamentalización de una organización, o en la función del personal. A cada VLAN se le puede asociar una subred, proveyendo servicios tradicionalmente resueltos con encaminadores físicos o conmutadores multicapa en las configuraciones LANs, permitiendo escalabilidad, seguridad, y administración de redes

Un dominio de difusión en una red, o porción de ella, recibirá un paquete de difusión desde cualquier nodo perteneciente a la misma. En una red típica, todo lo que está en el mismo lado del encaminador, forma parte del mismo dominio de difusión. En un conmutador donde se han creado muchas VLANs, hay múltiples dominios de difusión. Aun así, se sigue necesitando un encaminador, o un conmutador multicapa, para realizar un encaminamiento de paquetes de una VLAN a otra. El conmutador común de Capa 2 no puede hacer esto por sí mismo.

De tal forma que una gran red, puede segmentarse o dividirse en subredes con dominios de difusión más chicos. Desde esta perspectiva, el término VLAN podría considerarse como sinónimo de subred, dado que normalmente a cada VLAN se le hace corresponder una subred dentro de nuestra red.

Las VLANs pueden segmentar lógicamente redes conmutadas basadas en:

- Ubicación física (por ejemplo, según los edificios),
- Departamentos de la Organización (por ejemplo: Comercial) (Figura 3.14), o
- Por función del personal (por ejemplo, Gerencias), u otros criterios.

Para construir las VLANs tradicionalmente se usaron encaminadores físicos. Actualmente se puede resolver con conmutadores que soporten VLANs y conmutadores multicapa. Las VLANs proveen directamente segmentación de difusión, e indirectamente y no menos importante, aspectos como la escalabilidad, seguridad, ancho de banda, departamentalización, y administración de redes. Por ejemplo:

- Seguridad: Separando sistemas que tienen datos privados con respecto al resto de la red, reduciendo las opciones para que la gente no pueda acceder a información privilegiada que no está autorizada a ver,
- Ancho de banda: El uso de VLANs puede organizar y evitar la creación desmedida de una red de computadoras que no tienen por qué convivir, y por lo

tanto, aprovechar de una mejor manera el ancho de banda existente en la red,

- Departamentos o trabajos específicos: Las compañías muchas veces requieren entornos para que algunos departamentos con mucha carga de trabajo, o grupos dedicados a ciertas tareas, deban estar confinados sin accesos externos, o al menos con un control cuidadoso.

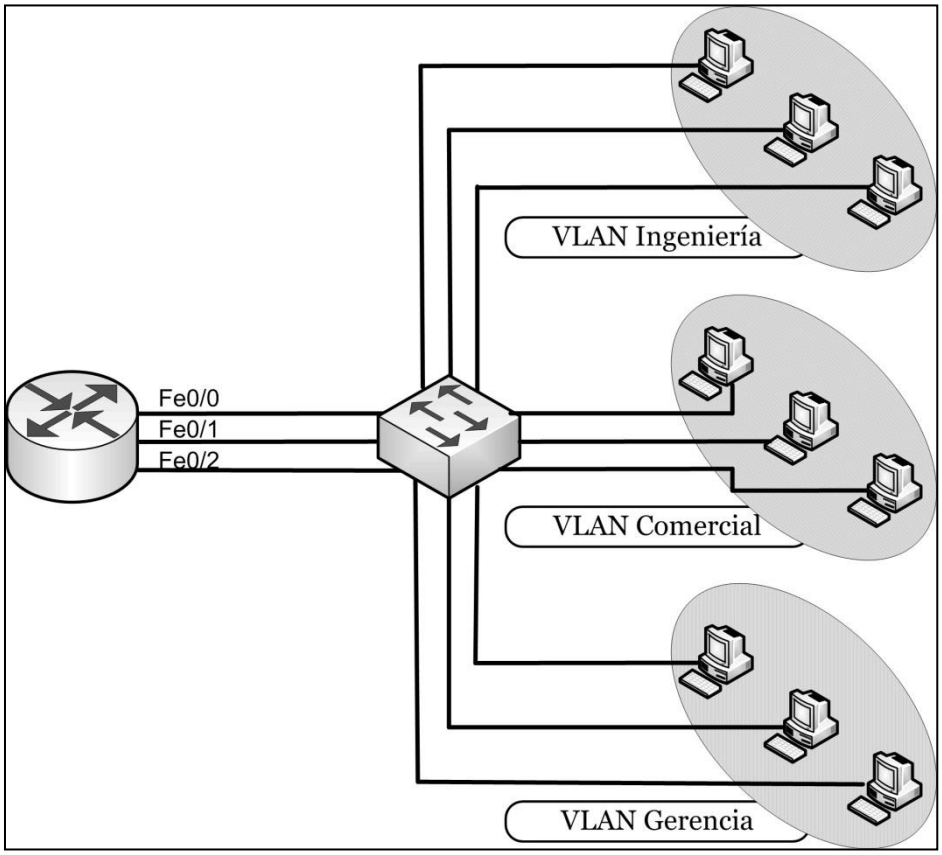


Fig. 3.14 Ejemplos de VLANs dentro de una organización.

Los puertos asignados a la misma VLAN comparten el mismo dominio de difusión.

Las VLANs se puedan configurar:

- Estáticamente: cuando los administradores de la red configuran puerto por puerto, y cada puerto está asociado a una única VLAN; es un proceso manual, y
- Dinámicamente: cuando los puertos se autoconfiguran a su VLAN, generalmente mediante algún software de asignación, previamente configurado con diversos criterios; es un proceso automático (Figura 3.15).

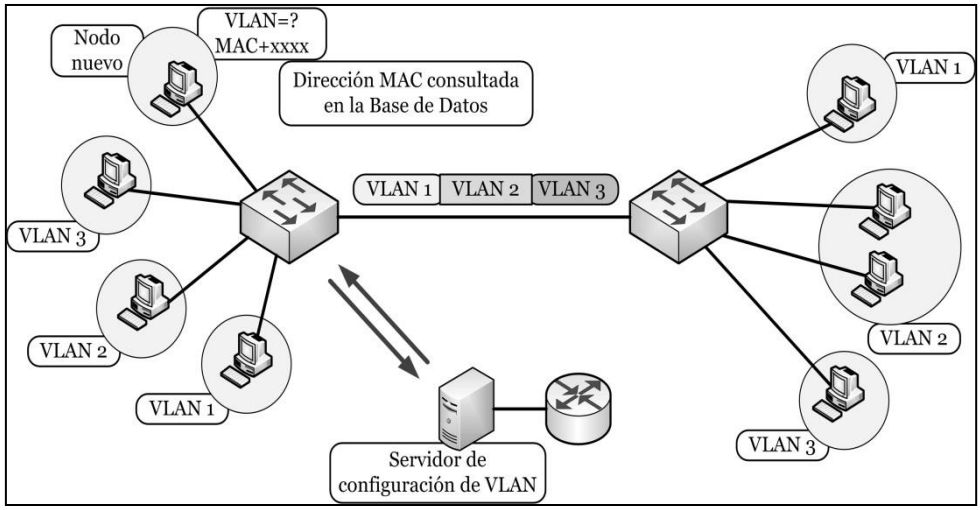


Fig. 3.15. Configuración dinámica de VLANs.

Los miembros de VLANs estáticas se conocen como "basados en puerto". Este es el método más común de asignar puertos a las VLANs. Cuando un dispositivo entra a la red, automáticamente asume la membresía de VLAN del puerto al cual está unido. En la mayoría de los conmutadores que soportan VLANs, existe una VLAN nativa que viene de fábrica conteniendo todos los puertos.

La membresía dinámica de las VLANs se crea a través de un software de administración de red (no como en las VLANs estáticas). Las VLANs dinámicas permiten la membresía, por ejemplo, basada sobre la dirección MAC de los dispositivos conectados al puerto del conmutador. Cuando un dispositivo entra a la red, consulta una base de datos dentro del conmutador por su membresía VLAN.

La red configurada sobre patrones de flujo de tráfico conocidos puede tener un 80% del tráfico contenido dentro de una VLAN. El restante 20% cruzaría el encaminador o conmutador multicapa a los servidores de la empresa, a Internet o a la WAN. A esto se lo conoce como la regla 80/20. Sin embargo, algunos patrones de tráfico en la actualidad dentro de las VLANs han vuelto a esta regla obsoleta, o al menos no aplicable en todos los contextos. La regla 20/80 se aplica a varias redes de hoy en día con 20% del tráfico dentro de la VLAN, y 80% fuera de la VLAN. No obstante el concepto es interesante porque introduce la necesidad de tener una idea sobre las características del tráfico dentro de cada VLAN a los efectos de la escalabilidad, dimensionamiento y seguridad.

3.3.2 Clasificación de VLANs

Se presenta una clasificación de las VLANs, dependiendo como se efectúa el agrupamiento de los dispositivos, por funcionalidad o por disposición física, en:

- VLANs Extremo a Extremo (*End-to-End o Campus-wide*) (Figura 3.16)
- VLANs Geográficas o Locales (Figura 3.17)

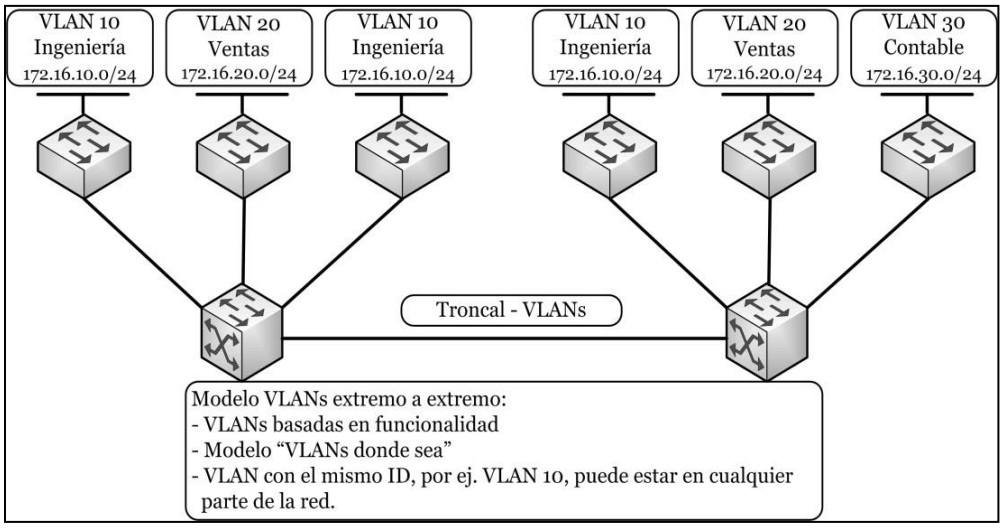


Fig. 3.16. VLANs Extremo a Extremo.

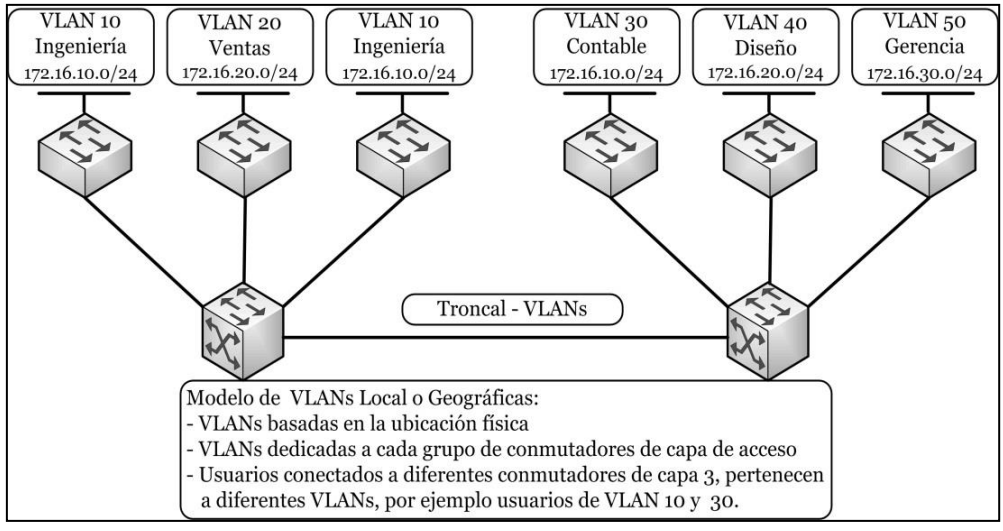


Fig. 3.17. VLANs Geográficas.

La preferencia de las VLANs Geográficas o Locales sobre las VLANs Extremo a Extremo se debe a una serie de aspectos:

- Cuando las redes corporativas tienden a centralizar sus recursos, las VLANs Extremo a Extremo se vuelven más difíciles de mantener,
- Los usuarios a veces son obligados a usar diferentes recursos, varios de los cuales no están en su VLAN,

A causa de este desplazamiento en el lugar y uso de los recursos, ahora las VLANs se crean más frecuentemente alrededor de límites geográficos más que límites comunitarios o funcionales.

3.3.3 Etiquetas y Troncales

Se presentan los conceptos de etiquetamiento y troncales en VLANs. El etiquetamiento (*tagging*) en VLAN se usa cuando un enlace necesita transportar tráfico de más de una VLAN, a los efectos de rotular y diferenciar una trama de otra. Y existe un enlace troncal (*trunk*) entre los conmutadores cuando el enlace trafica datos provenientes de diferentes VLANs. Cuando los paquetes se reciben por el conmutador desde cualquier dispositivo final, se suma un único identificador de paquete dentro de cada cabecera. Esta cabecera de información designa la membresía VLAN de cada paquete.

Las VLANs se pueden extender por varios conmutadores en una red, y se puede tener más de una

VLAN en cada conmutador (Figura 3.18). Para que se puedan comunicar múltiples VLANs en varios conmutadores hay que utilizar el proceso llamado troncal (*trunking*), que es una tecnología que permite que la información de muchas VLANs se pueda llevar por un único enlace entre conmutadores. Para ello, se utiliza el protocolo VTP (*Vlan Trunking Protocol*), que permite comunicar la configuración de VLANs entre conmutadores (este es un protocolo propietario de CISCO Systems).

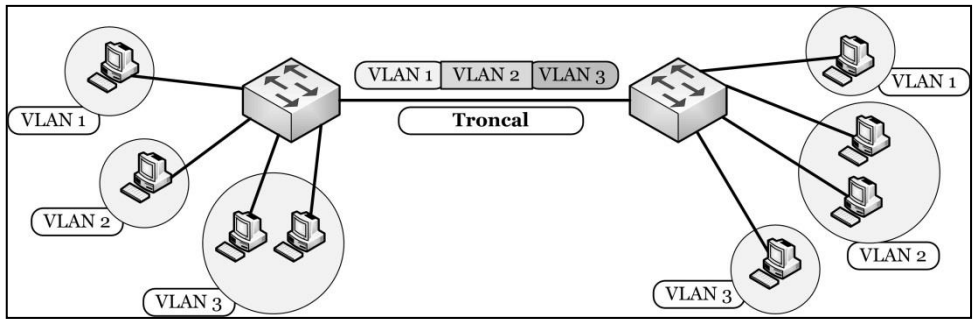


Fig. 3.18. Ejemplo de troncal de VLANs.

El paquete es entonces transmitido a los conmutadores o encaminadores apropiados basado sobre el identificador (*ID*) de la VLAN y la dirección MAC. Para alcanzar el nodo destino, el conmutador adyacente elimina el ID de la VLAN del paquete y lo transmite al dispositivo final. El etiquetamiento de paquetes provee un mecanismo para controlar el flujo de tramas de difusión mientras no interfiere con la red y las aplicaciones.

Hay dos métodos para etiquetar las tramas: (Figura 3.19)

- El ISL (*Inter-Switch L*ink), propietario de CISCO, y
- El IEEE 802.1Q.

Se recomienda usar 802.1Q, que es un estándar, especialmente cuando se combinan dispositivos de diferentes fabricantes.

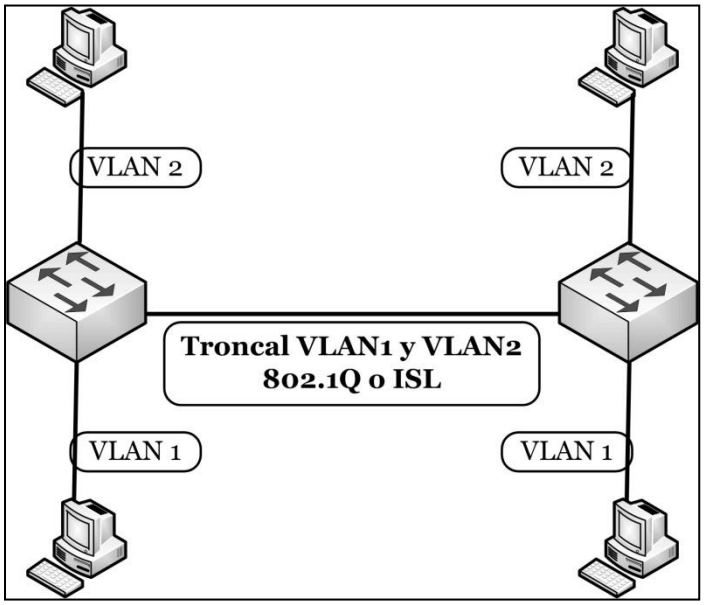


Fig. 3.19. Etiquetado de paquetes de VLANs.

El formato de la trama 802.1Q, surge del agregado de 4 bytes a la trama original de Ethernet, de acuerdo a la figura 3.20. En los mismos se diferencian 2 campos generales:

- TPID (*Tag Protocol ID* - Identificador de Etiqueta de Protocolo): 2 bytes que originalmente tienen un valor fijo de 0x8100, que indica que es una trama con etiqueta de VLAN (en las últimas modificaciones

de la norma existen otros valores, como por ejemplo etiquetas de Servicio)

- TCI (*Tag Control Information* - Información de Control de Etiqueta): 2 bytes que tienen 3 subcampos:
    - PCP (*Priority Code Point*): 3 bits de parámetros de prioridad.
    - DEI (*Drop Eligibility Indicator*): 1 bit indicador para descarte.
    - VID (*VLAN ID*): 12 bits de Identificador de VLAN, que etiqueta hasta 4094 VLANs (los números 0 y 495 están reservados)

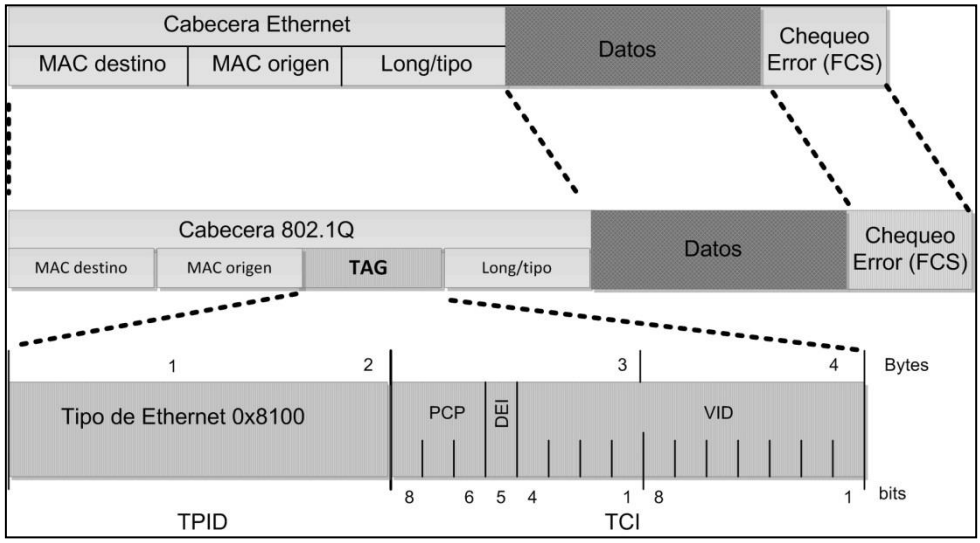


Fig. 3.20. Formato de trama 802.1Q.

3.3.4 Configuración de VLANs

Introduciremos algunos ejemplos de configuración básica de VLANs sobre conmutadores.

Supondremos la utilización de un conmutador CISCO 29xx, aunque las consideraciones generales son aplicables a conmutadores de las diversas marcas, que soporten VLANs. El número máximo de VLANs depende del conmutador. Los conmutadores 29xx permiten normalmente 4.094 VLANs; y la VLAN 1 es la VLAN por defecto de fábrica. La dirección IP del conmutador CISCO Catalyst 29xx está sobre el dominio de difusión de la VLAN 1 por defecto.

En la Figura 3.21 se muestran las instrucciones de configuración del conmutador para crear VLANs y asignarles puertos a las mismas. Se trata de un ejemplo específico para crear la VLAN 10 y asignarle el puerto fastethernet 9.

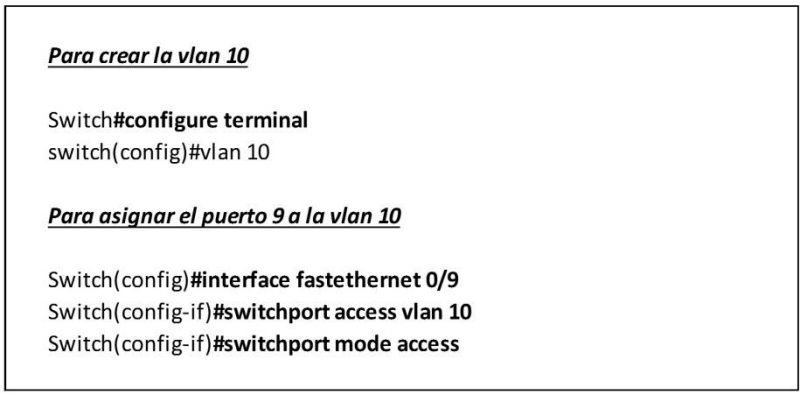
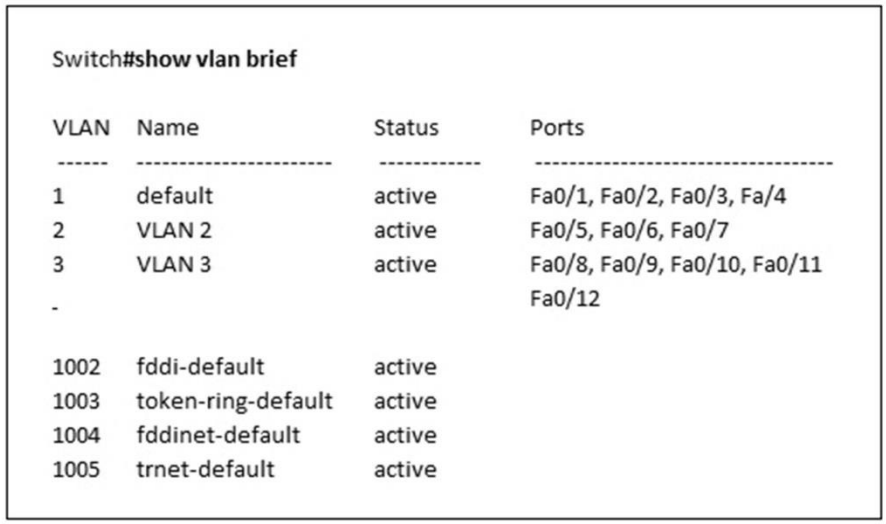


Fig. 3.21. Creación de VLANs y asignación de puertos en el conmutador.

Por defecto, todos los puertos están configurados como *switchport mode dynamic desirable*, lo que significa que si el puerto está conectado a otro conmutador con un puerto configurado con el mismo modo por defecto (*desirable o auto*), este enlace se convertirá en troncal automáticamente.

En las Figuras 3.22 y 3.23 se muestra la instrucción *show*, con dos variantes, para verificar la configuración de VLANs en el conmutador.



Switch#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa/4
2	VLAN 2	active	Fa0/5, Fa0/6, Fa0/7
3	VLAN 3	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11
-			Fa0/12
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Fig. 3.22. Verificación de VLAN con la instrucción *show vlan brief*.

```
Switch#show vlan

VLAN  Name                 Status      Ports
----  -------------------- ----------- -------------------------------
1     default              active      Fa0/1, Fa0/2, Fa0/3, Fa/4
2     VLAN 2               active      Fa0/5, Fa0/6, Fa0/7
3     VLAN 3               active      Fa0/8, Fa0/9, Fa0/10, Fa0/11
-                                      Fa0/12
1002  fddi-default         active
1003  token-ring-default   active
1004  fddinet-default      active
1005  trnet-default        active

VLAN  Type  SAID    MTU   Parent RingNo BridgeNo Stp  BridgNode Trans1 Trans2
----  ----- ------- ----- ------ ------ -------- ---- --------- ------ ------
1     enet  100001  1500  -      -      -        -    -         1002   1003
2     enet  100002  1500  -      -      -        -    -         0      0
```

Fig. 3.23. Verificación de VLAN con la instrucción *show vlan*.

La Figura 3.24 presenta los comandos para administrar el conmutador, como la configuración de la dirección IP y de la puerta de enlace, y la Figura 3.25 para su acceso remoto con Telnet.

```
Switch#interface vlan 1
Switch(config-if)#ip address 10.1.0.5 255.255.0.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 10.1.0.1
```

Fig. 3.24. Configuración IP y de la puerta de enlace del conmutador.

```
Switch(config)#enable secret class
Switch(config)#line vty 0 4
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config)#interface vlan 1
Switch(config-if)#ip address 10.1.0.5 255.255.0.0
Switch(config-if)#no shutdown
Swtich(config)#ip default-gateway 10.1.0.1
```

Fig. 3.25. Configuración de acceso remoto del conmutador con Telnet.

3.4 STP – Protocolo de Árbol de Expansión

3.4.1 Visión General

La técnica de árbol de expansión es un mecanismo en el que los puentes y los conmutadores Ethernet desarrollan automáticamente una tabla de encaminamiento y la actualización de la misma, en respuesta a cambios en la topología de la red. El STP (*Spanning Tree Protocol* - Protocolo de Árbol de Expansión) usa esta técnica para resolver de manera automática la selección de los mejores enlaces ante las redundancias previstas por diseño y/o una falla de dispositivo o humana.

Dicho de otra forma, el protocolo STP es un protocolo de prevención de lazos (*loops*). Este protocolo permite que los dispositivos de Capa 2 se comuniquen entre sí para

descubrir los lazos físicos en la red, y luego, crear una topología lógica libre de lazos (Figura 3.26).

Los lazos pueden existir en la red, como parte de una estrategia de diseño que use redundancia, para mejorar la confiabilidad del sistema. STP no se necesitaría en redes sin lazos. Sin embargo, éstos pueden ocurrir accidentalmente a manos del personal de redes o aún de los usuarios.

Las tramas de difusión y los lazos de Capa 2 por diseño de red o accidentales pueden ser una combinación dañina. Las tramas Ethernet no tienen el campo TTL (*Time To Live*) como en los paquetes IP, y por lo tanto, pueden estar en la red, y específicamente en un lazo indefinidamente. Después que una trama Ethernet comienza un lazo, probablemente continuará hasta que alguien apague uno de los conmutadores o rompa un enlace.

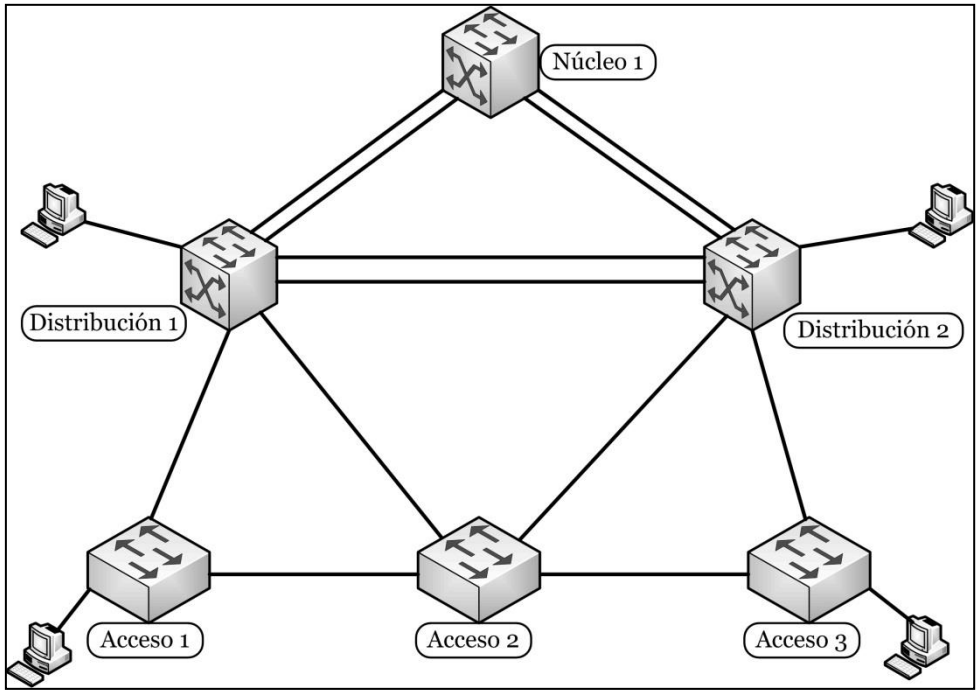


Fig. 3.26. Configuración típica para usar STP.

El propósito de STP es evitar y eliminar los lazos en la red al negociar una ruta libre de ellos, a través de un puente o conmutador especial llamado puente raíz (*root bridge*) (Figura 3.27).

El STP ejecuta un algoritmo llamado Algoritmo de Árbol de Expansión (*STA - Spanning Tree Algorithm*). El STA elige el puente raíz como punto de referencia, y luego, determina los enlaces disponibles hacia el mismo. Si existen más que dos enlaces, el STA selecciona el mejor y bloquea el resto.

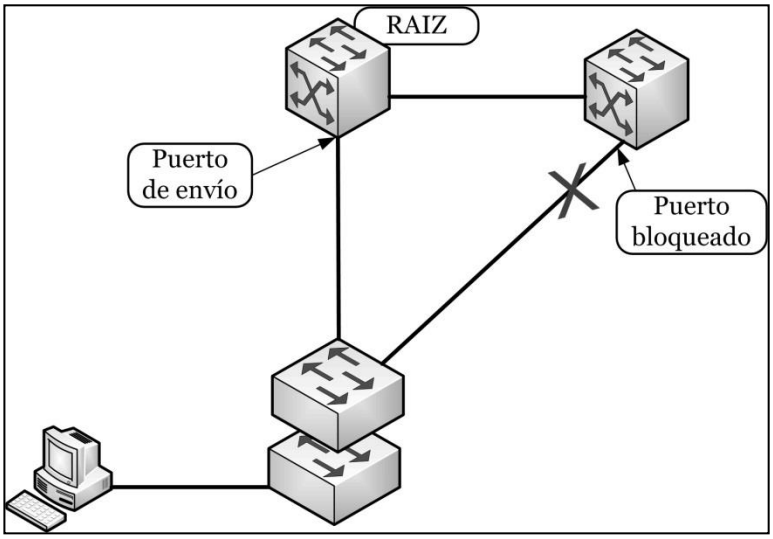


Fig. 3.27. Bloqueo de enlaces usando STP.

Los cálculos de STP hacen uso extensivo de dos conceptos claves para crear una topología libre de lazos:

- El BID (ID de Bridge - *Bridge ID*) y
- El costo del Enlace o Ruta.

El BID identifica cada puente o conmutador, y el STP determina con él, el raíz o centro de la red (Figura 3.28).

Cada conmutador debe tener un único BID. En el estándar original 802.1D, el BID es el campo Prioridad y la MAC del conmutador, y todas las VLANs están representadas por un árbol de expansión común o CST (*Común Spanning Tree*). Debido a que una versión de STP llamada PVST requiere una instancia separada de árbol de expansión por VLAN, el campo de BID tiene información de ID de VLAN (Figura 3.29).

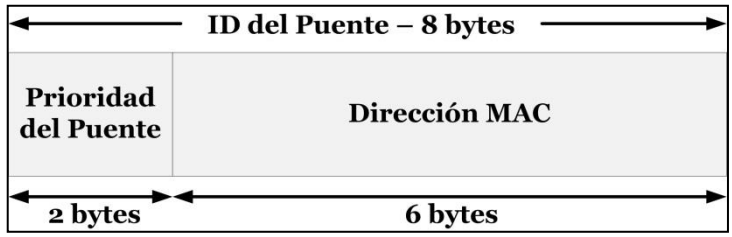


Fig. 3.28. Formato del ID de Bridge (BID).

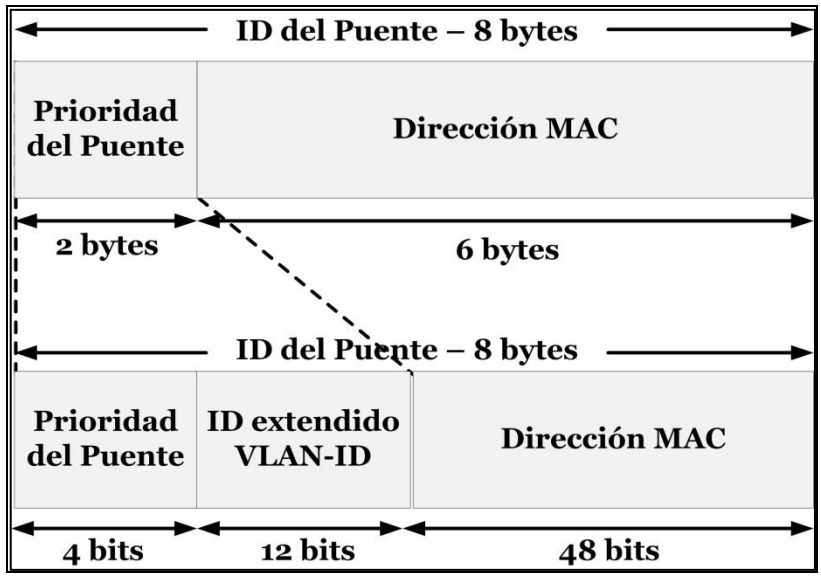


Fig. 3.29. Formato extendido del ID de Bridge (BID).

Como se indicó, el BID se usa para elegir el bridge raíz. El conmutador raíz es el que tiene menor BID. Si la prioridad es la misma, el conmutador con menor dirección MAC es el conmutador raíz.

Además, cada conmutador usa el concepto de costo para evaluar el camino a otros conmutadores. Originalmente

802.1D definió los costos como 10^9/(ancho de banda) del enlace en Mbps. Por ejemplo:

- El costo del enlace de 10 Mbps = 100 (de costo)
- El costo del enlace de 100 Mbps = 10
- El costo del enlace de 1 Gbps = 1

Este esquema no tenía previsto los enlaces Ethernet de 10 Gbps. La IEEE modificó los costos en una escala no lineal de la siguiente manera:

- Para 4 Mbps 250 (de costo),
- 10 Mbps 100,
- 16 Mbps 62,
- 45 Mbps 39,
- 100 Mbps 19,
- 155 Mbps 14,
- 622 Mbps 6,
- 1 Gbps 4,
- 10 Gbps 2.

Se observa que a mayor velocidad menor costo.

3.4.2 Algoritmo STP

La comunicación STP entre conmutadores adyacentes se realiza con información de Capa 2, intercambiando mensajes BPDUs (*Bridge Protocol Data Units* - Unidad de Datos de Protocolo de Bridge). Cada puerto del conmutador envía BDPUs que contienen la información requerida para la configuración de STP. El campo Tipo de Mensaje (*Message Type*) (Tabla 3.2) para el mensaje de BPDU es 0x00, y usa la dirección MAC multicast 01-80-C2-00-00-00.

Bytes	Campo
2	ID de protocolo
1	Version
1	Tipo de mensaje
1	Flags
8	ID de Raíz
4	Costo de paso
8	ID de Bridge
2	ID de Puerto
2	Tiempo del mensaje
2	Tiempo máximo
2	Tiempo de Hello
2	Retardo de transmisión

Tabla 3.2. Formato de mensajes de STP.

El algoritmo STP realiza 3 acciones para converger en una topología sin lazos:

- Acción 1 Elige un Conmutador Raíz,
- Acción 2 Elige los Puertos al Raíz (*Root Ports*), y
- Acción 3 Elige los Puertos Designados (*Designated Ports*).

Cuando la red se inicia por primera vez, todos los conmutadores envían BPDUs e inmediatamente aplican la secuencia o proceso de decisión de STP de 5 pasos. Los conmutadores deben elegir un único Conmutador Raíz con el menor BID, y que tendrá entonces la "prioridad más alta".

La secuencia de decisión de 5 pasos, es la siguiente:

- Paso 1 – BID menor (*Lowest BID*),
- Paso 2 – Ruta de costo menor al Conmutador Raíz (*Lowest Path Cost to Root Bridge*),
- Paso 3 – BID de transmisor menor (*Lowest Sender BID*),
- Paso 4 – Prioridad de puerto menor (*Lowest Port Priority*),
- Paso 5 – ID de puerto menor (*Lowest Port ID*)

Los conmutadores usan BPDUs de configuración durante este proceso.

A través del protocolo STP deben resolverse las siguientes preguntas:

- ¿Quién es el Conmutador Raíz?,
- ¿Cuán lejos se está del Conmutador Raíz?,
- ¿Cuál es el BID del conmutador que envía esa BPDU?, y
- ¿De qué puerto del conmutador emisor viene esa BPDU?.

Esta información debe obtenerse de los datos que tienen los campos de las BDPUs.

La primera acción es elegir el Conmutador Raíz. Al comienzo, todos los conmutadores se autodeclaran como Conmutador Raíz, ubicando su propio BID en el campo *Root BID* de la BPDU. Aunque, una vez que todos los conmutadores saben cuál es el que tiene el BID más bajo, lo aceptan como el Conmutador Raíz.

La segunda acción es elegir los Puertos al Raíz. Un Puerto al Raíz de un conmutador es el puerto más cercano al Conmutador Raíz. Los conmutadores usan el costo para determinar su cercanía. Cada conmutador no raíz selecciona un Puerto al Raíz. El costo de la ruta hacia la raíz es la suma del costo de todos los enlaces al Conmutador Raíz. El Conmutador Raíz envía BPDUs con un costo de ruta 0. Los otros conmutadores reciben estas BPDUs y suman el costo de ruta de la interface FastEthernet al costo de ruta raíz contenido en la BPDU.

Los conmutadores ahora envían BPDUs con su costo de ruta raíz a las otras interfaces. Los costos STP se incrementan cuando se reciben las BPDUs en un puerto, no cuando se envían fuera del mismo.

Cada conmutador no raíz debe seleccionar un Puerto al Raíz, que deberíamos entender el puerto a la raíz con el menor costo. Es decir, un Puerto al Raíz es el puerto más cercano al Conmutador Raíz, y está determinado por el costo directo, o a través de una secuencia de enlaces. ¿Qué sucede cuando los costos son iguales para dos puertos? Se continúa con la secuencia de 5 pasos. En el paso 3 se indica que el conmutador que tenga un BID de transmisor menor será elegido entre los dos.

La tercera acción es elegir los Puertos Designados. Durante esta acción quedará evidente el objetivo de prevención de lazos por parte de STP. Un Puerto Designado funciona como un puerto común que envía y recibe tráfico entre ese segmento y el Conmutador Raíz. Cada segmento en

una red conmutada tiene un Puerto Designado, elegido en base a un costo de la ruta raíz al Conmutador Raíz. El conmutador que contiene el Puerto Designado es el Conmutador Designado para ese segmento. Para ubicar a los Puertos Designados debemos observar cada segmento.. Desde un dispositivo en este segmento, "¿a través de qué conmutador debería ir para alcanzar el Conmutador Raíz?". Se decide usando el menor costo del costo de ruta a la raíz publicado desde cada conmutador.

Todos los otros puertos que no son Puerto Raíz ni Puertos Designados, se convierten en Puertos no Designados. Los Puertos no Designados se ponen en estado de bloqueo, que permite la prevención de lazos de STP.

Si el costo del paso y los BIDs son iguales, situación que se presenta con enlaces paralelos, el conmutador sigue la secuencia de decisión de 5 pasos: usa la prioridad de puerto. La más baja prioridad de puerto gana. La misma puede estar configurada por defecto a un cierto valor, y es modificable. Si todos los puertos tienen la misma prioridad, sigue la secuencia de decisión de 5 pasos: usa el número de puerto más bajo (ID de puerto).

3.4.3 Estados de los Puertos en STP

Los estados de los puertos en STP, son: retransmisión (*forwarding*), aprendizaje (*learning*), escucha (*listening*), bloqueo (*blocking*) y deshabilitado (*disabled*) (Tabla 3.3).

Todos los puertos arrancan en modo bloqueo para evitar que se cree un posible lazo. Los puertos escuchan (o reciben) BPDUs y no se transmiten datos de usuarios. El puerto permanece en este estado si STP determina que hay un mejor paso a un Conmutador Raíz. Puede tomar hasta 20 segundos la transición a otro estado.

Estado	Propósito
Retransmisión	Envío/Recepción de datos de usuario
Aprendizaje	Construcción de tabla de "bridging"
Escucha	Construcción de topología "activa"
Bloqueo	Recepción de solo BPDUs
Deshabilitado	Administrativamente bloqueado

Tabla 3.3. Estado de los puertos STP.

El puerto pasa de un estado de bloqueo a otro de escucha. Intenta aprender si hay otras rutas al Conmutador Raíz escuchando las tramas. No se transmiten datos de usuarios. Permanece en este estado durante 15 segundos. Los puertos que pierden la elección de Puerto Designado se vuelven Puertos no Designados, y retornan al estado de Bloqueo.

El estado de aprendizaje es muy similar al anterior, excepto que el puerto puede agregar información que ha aprendido a su tabla de direcciones. Es decir, coloca direcciones MAC en la tabla de direcciones MAC. Aún no permite enviar o recibir datos de usuarios. Tiene un período de 15 segundos.

Y en el de retransmisión, el puerto puede enviar y recibir datos de usuario. Un puerto llega y se mantiene en el estado de retransmisión si:

- No hay enlaces redundantes, o si
- Se determinó que es el mejor paso al Conmutador Raíz.

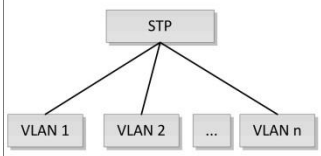
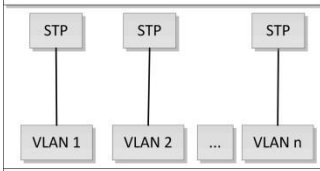
En resumen:

- Se elige un Puerto Raíz por cada conmutador y un Puerto Designado por cada segmento,
- Estos puertos proveen la mejor ruta desde el conmutador hasta el Conmutador Raíz (la ruta con el costo más bajo),
- Estos puertos se ponen en modo de retransmisión,
- Los puertos que no están en modo de retransmisión se colocan en modo bloqueo,
- Estos puertos continuarán enviando y recibiendo información de BPDUs, pero no datos de usuario.

3.4.4 Evolución de las Versiones de STP

Presentamos un caso especial: el estado *PortFast* de CISCO. PortFast provoca que un puerto salte los modos de Escucha y Aprendizaje, y pase inmediatamente al estado de Retransmisión. Cuando se habilita PortFast en los puertos de acceso de Capa 2, conectados a un simple puesto de trabajo o a un servidor, se permite a estos dispositivos acceder a la red inmediatamente, sin esperar la convergencia de ST. El propósito de PortFast es minimizar el tiempo de acceso a la red.

Además, el propio protocolo STP ha evolucionado desde su versión original (Figura 3.30). Una mejora es la que se denomina RSTP (*Rapid Spanning Tree Protocol* - Spanning Tree Rápido. RSTP está basado en el estándar IEEE 802.1w y STP en 802.1d. RSTP requiere conexión punto a punto y full-duplex entre conmutadores adyacentes para alcanzar rápida convergencia. RSTP tiene designaciones de puertos distintas como: Alternativo (*Alternate*) y Resguardo (*Backup*). Los puertos que no participan en el Árbol de Expansión se conocen como Puertos de Borde (*Edge Ports*), y funcionan de manera similar a los puertos PortFast. Los Puertos de Borde no transmiten BPDUs, pero se vuelven inmediatamente un Puerto que no es de Borde si escuchan una BPDU en ese puerto.

<table>
<tr><th>Proceso SPT</th><th>Estándar IEEE</th><th>Implementación CISCO</th></tr>
<tr><td rowspan="2"> 
</td><td>STP:
- 802.1D</td><td>STP:
- 802.1D
Mejoras CISCO (1° Evolución):
- PortFast
- UplinkFast
- BackboneFast</td></tr>
<tr><td>RSTP (Rapid STP):
- 802.1w
- Edge Fast
- Uplink fast RSTP
- Backbone Fast Engine</td><td>RSTP (Rapid STP):
- 802.1w
- Edge Fast
- Uplink fast RSTP
- Backbone Fast Engine</td></tr>
<tr><td> 
</td><td></td><td>PVSTP (STP por VLAN)

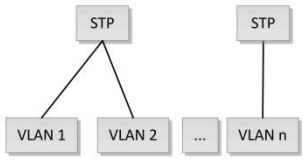
PVRST (RSTP por VLAN)</td></tr>
<tr><td> 
</td><td>MSTP (Multiple STP):
- 802.1s
- Usa RSTP</td><td>MSTP (Multiple STP):
- 802.1s
- Usa PVSTP</td></tr>
</table>

Fig. 3.30. Evolución del protocolo STP.

RSTP evita la necesidad de temporizadores de retardo como en 802.1D. RSTP reemplaza a 802.1D mientras sigue siendo compatible. El formato de la trama BPDU es el mismo, excepto que el campo de Versión se indica con 2.

Múltiple Árbol de Expansión (*Multiple Spanning Tree* - MST) extiende la norma IEEE 802.1w RST a múltiples árboles. El principal propósito de MST es reducir el número total de instancias de árboles de expansión que se pueden plantear en una topología física de red, y así reducir los ciclos de CPU de un conmutador. MST usa un número mínimo de instancias STP.

Y Árbol de Expansión por VLAN Plus (o PVST+) mantiene una instancia separada de árbol de expansión por cada VLAN. Cada instancia de PVST en una VLAN tiene un único Conmutador Raíz. PVST+ puede proveer un balanceo de carga basado en VLAN. PVST+ permite la creación de diferentes topologías lógicas usando VLANs en una red conmutada para asegurar que se puedan usar todos los enlaces. Por lo tanto, no hay puertos en estado de bloqueo.

3.5 Ejercitación

Ejercicio n° 1:
Explique las diferencias de funcionamiento entre Repetidor, Concentrador, Puente y Conmutador.

Ejercicio n° 2:
Indique si las siguientes afirmaciones son verdaderas o falsas:
a) Un concentrador debe esperar a que el canal esté desocupado antes de enviar datos por una interfaz Ethernet half-duplex.
b) Si un host A manda un paquete IP al host B a través del conmutador X, estando los 3 en la misma LAN, entonces la MAC de destino de la trama Ethernet es la dirección MAC de X.
c) Un conmutador Ethernet no utiliza la dirección IP para decidir por cuál puerto debe retransmitir.
d) Si un conmutador que trabaja en modo Almacena y Envía recibe una trama con errores, la descarta y no la reenvía.
e) Cuando un conmutador tiene una trama lista para enviar a través de una interfaz Ethernet half-duplex, debe sensar el medio y esperar a que se desocupe.

Resolución Ejercicio n° 2:

a. Falso
b. Falso
c. Verdadero
d. Verdadero
e. Verdadero

Ejercicio n° 3:
Busque en las especificaciones técnicas de por lo menos 3 (tres) conmutadores comerciales administrables, e indique en una tabla las características propias de cada uno.
Ejemplo:

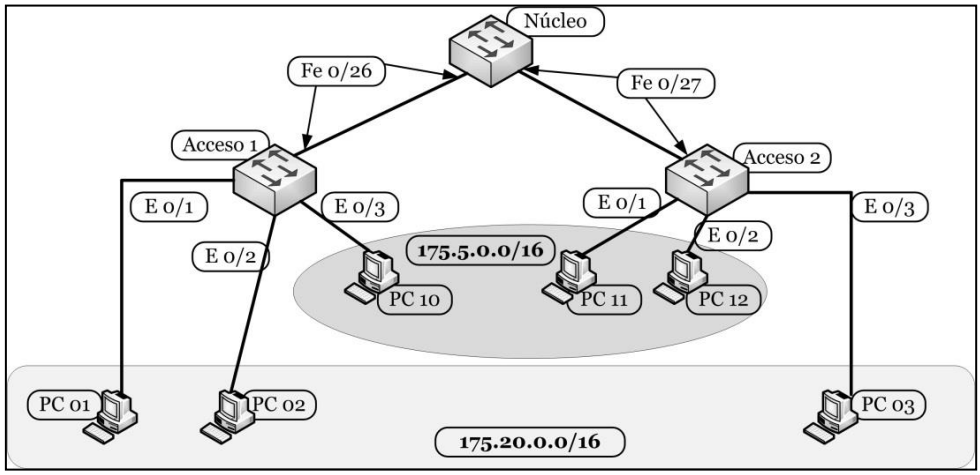
Cantidad de puertos,
Velocidad de puertos,
Alimentación POE,
Forwarding modes,
Switching capacity,
Capacidad tabla MAC,
Spanning tree,
802.3ad link aggregation,
VLAN,
Seguridad,
Autenticación, etc.

Ejercicio n° 4:
Comparar el formato (los campos) de una trama Ethernet con una trama que cumpla con el estándar 802.1q, explicando los campos adicionales.

Ejercicio n° 5:
De la figura, indique si las siguientes afirmaciones son verdaderas o falsas:

a) Los enlaces llamados “troncales” son los que están en las interfaces FE0/26 y FE0/27 del conmutador “Core”.
b) Es posible la comunicación entre la PC01 y la PC12
c) Es posible la comunicación entre la PC02 y la PC03
d) El campo de VLAN ID está presente en las tramas que salen de la interface E0/3 del conmutador Acceso02.
e) El campo de VLAN ID está presente en las tramas que salen de la interface FE0/26 del conmutador Acceso01.

f) Todas las PCs tienen acceso a la administración de los conmutadores.
g) Ninguna PC tiene acceso a la administración de los conmutadores.



Resolución Ejercicio n° 5:

a. Verdadero
b. Falso
c. Verdadero
d. Falso
e. Verdadero
f. Falso
g. Falso

Ejercicio n° 6:

En el esquema del ejercicio anterior, explicar qué sucede si PC03 envía una trama de difusión y a quiénes les llega esa trama.

Resolución Ejercicio n° 6:
En un esquema de VLANs, las tramas de difusión) emitidas por un host, le llega solamente a todas los hosts que se encuentran en la misma VLAN. En el ejemplo a la PC01 y PC02.

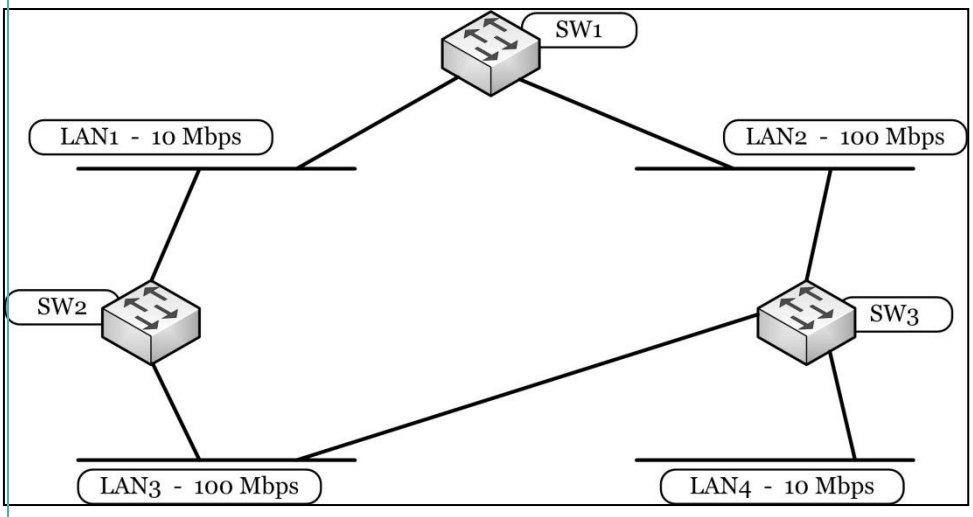
Ejercicio n° 7:
Con el uso de puentes, explique el problema que se presenta en las topologías con lazos.

Ejercicio n° 8:
Explique las características del protocolo “spanning tree” utilizado para solucionar los problemas del ejercicio 1.

Ejercicio n° 9:
Indique si las siguientes afirmaciones son verdaderas o falsas:
a) El protocolo de Spanning Tree permite a los conmutadores aprender la ubicación de las direcciones MAC en la red y así evitar el envío de las tramas Ethernet a través de todos los puertos.
b) El protocolo de Spanning Tree puede generar caminos subóptimos entre hosts y subutilizar recursos de la red.

Resolución Ejercicio n° 9:
a. Falso
b. Verdadero

Ejercicio n° 10:
En la red de la figura, los conmutadores aplican el algoritmo STP para obtener una topología libre de lazos. La MAC de SW1 es: 1111:1111:1111, del SW2 es 2222:2222:2222 y del SW3 es 3333:3333:3333 y la prioridad de cada uno es la por defecto (32768).
Indique si las siguientes afirmaciones son verdaderas o falsas:
a) El puerto del SW2 con interfaz en la LAN3 queda en modo Forwarding después de converger el algoritmo STP.
b) Mientras SW1 se encuentra en estado Listening puede aprender direcciones MAC de las tramas que recibe.
c) El puerto de SW1 con interfaz en la LAN1 quedará en modo Blocking, porque tiene menor capacidad que el puerto con interfaz en la LAN2.
d) Si se agregara una segunda conexión de SW1 a la LAN2, la misma quedará en modo Blocking.



Resolución Ejercicio n° 10

a. Verdadero
b. Falso
c. Falso
d. Verdadero

Ejercicio n° 11:

De la topología del ejercicio 4, dibujar el árbol STP final.

3.6 Bibliografía y referencias

3.6.1 Libros impresos

- William Stallings, “Data and Computer Communications”, Pearson Education, 10° Ed., 2014.
- William Stallings y Thomas Case, “Business Data Communications”, Pearson Education, 7° Ed., 2013.
- William Stallings, “Data and Computer Communications”, Pearson Education, 8° Ed., 2009.
- CCNA de CISCO Press.
- William Stallings, “Wireless Communications & Networks”, Prentice Hall, 2° Ed., 2005.
- Michael Daoud Yacoub “Wireless Technology: Protocols, Standards, and Techniques”, CRC Press, 2002.
- William Stallings, “Local and Metropolitan Area Networks”, Prentice Hall, 6° Ed., 2000.
- Uyless Black, “Tecnologías Emergentes para Redes de Computadoras”, Ed. Prentice-Hall, 1999.
- D. Comer, “Redes Globales de Información con Internet y TCP/IP”, Ed. Prentice-Hall, 3° Ed., , 2000.

- Request for Comments referidos a la temática.
- Artículos de revistas (IEEE, ACM, etc.) referidos a la temática.

3.6.2 Enlaces y Referencias

- Estándares generales de la IEEE http://standards.ieee.org/about/get/index.html
- Información Ethernet general, especificaciones técnicas, lista de lecturas Ethernet http://www.ethermanage.com/ethernet/ethernet.html
- Consorcio que promociona la tecnología y productos Ethernet. El sitio incluye numerosos documentos http://www.ethernetalliance.org/
- Últimos documentos que incluyen los documentos de la Task Force para Ethernet de 40-Gbps y 100-Gbps http://www.ieee802.org/3/
- University of New Hampshire (equipamiento de testing de ATM, FDDI, Fast Ethernet, FDSE, Ethernet, OSPF, Network Management (SNMP), Token Ring, VG-AnyLAN) http://www.iol.unh.edu/
- Documento sobre el Protocolo STP http://etutorials.org/Networking/Lan+switching+first-step/Chapter+7.+Spanning+Tree+Protocol+STP/
- Documento sobre VLANs http://etutorials.org/Networking/Lan+switching+first-step/Chapter+8.+Virtual+LANs+VLANs/
- Documento sobre diseño de redes LAN switchadas http://etutorials.org/Networking/Lan+switching+first-step/Chapter+10.+LAN+Switched+Network+Design/

- Documento sobre administración de redes LAN switchadas
  http://etutorials.org/Networking/Lan+switching+first-step/Chapter+11.+Switch+Network+Management/
- Documento de la empresa CISCO sobre aplicaciones VLANs
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm
- Documento sobre Redes Privadas Virtuales (VLANs)
  http://www.textoscientificos.com/redes/redes-virtuales
- Calidad de Servicio (QoS) en LANs
  http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-1/lan_qos.html
- Estándar 802.1q
  http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf
- Soluciones de networking
  http://www.cisco.com/en/US/prod/switches/ps5718/ps708/networking_solutions_products_genericcontent0900aecd805f0955.pdf

CAPÍTULO 4

Encaminadores y Protocolos de Encaminamiento

4.1 Encaminadores

- **4.1.1 Introducción**
- **4.1.2 Características Generales de los Encaminadores**
- **4.1.3 CPU, Memorias y Sistema Operativo de los Encaminadores**
- **4.1.4 Puertos o Interfaces**
- **4.1.5 Encaminador como dispositivo de Capa 3**
- **4.1.6 Instrucciones de configuración básicas**

4.2 Protocolos de Encaminamiento y Encaminados

- **4.2.1 Introducción**
- **4.2.2 Encaminamiento Adaptativo o Dinámico**
- **4.2.3 Sistemas Autónomos y Protocolos IRP – ERP**
- **4.2.4 Tipos de Encaminamiento**
- **4.2.5 Algoritmos de Encaminamiento**

4.3 Ejercitación

4.4 Bibliografía y referencias

- **4.4.1 Libros impresos**
- **4.4.2 Enlaces y Referencias**

Capítulo 4

Encaminadores y Protocolos de Encaminamiento

4.1 Encaminadores

4.1.1 Introducción

Un encaminador, también conocido como enrutador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel de Capa 3 en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador; y que por lo tanto, tienen números o prefijos de red distintos. El funcionamiento básico de un encaminador consiste en almacenar un paquete y reenviarlo a otro encaminador o al *host* final. Cada encaminador se encarga de decidir el siguiente salto en función de una tabla de reenvío, de ruteo o de encaminamiento.

4.1.2 Características Generales de los Encaminadores

Los primeros encaminadores fueron minicomputadores que controlaban el flujo de datos entre redes de computadoras. Actualmente ofrecen una amplia

gama de servicios a “ese flujo” de datos. Básicamente son computadoras con su CPU, RAM, ROM y sistema operativo.

El primer dispositivo que tenía fundamentalmente la misma funcionalidad que lo que al día de hoy entendemos por encaminador, era el IMP. Los IMPs del año 1969 eran los dispositivos que formaban la ARPANET, la primera red de conmutación de paquetes, antecesora de Internet. La idea de un encaminador (llamado por aquel entonces *gateway* o compuerta) vino inicialmente de un grupo internacional de investigadores en redes de computadoras, creado en 1972. A finales de 1976, tres encaminadores basados en PDP-11s entraron en servicio en el prototipo experimental de Internet. Posteriormente, en 1981 se desarrolló el primer encaminador multiprotocolo (*multiprotocol router),* en Stanford, que soportaba más de un protocolo y también estaba basado en PDP-11s. Desde mediados de los años 70 y en los años 80, los miniordenadores de propósito general servían como encaminadores.

Luego, a principio de los años ‘80, se desarrollaron los primeros módems encaminadores en Internet. Y siguiendo las innovaciones, nació CISCO en 1984, que adoptó, mejoró y comercializó el encaminador multiprotocolo. Actualmente, los encaminadores de alta velocidad están muy especializados, ya que se emplea un hardware específico para acelerar las funciones más importantes, como son el encaminamiento de paquetes y algunas funciones especiales, como la encriptación IPsec.

Los encaminadores envían paquetes a la red de conmutación de paquetes, desde la fuente original hasta el destino final, seleccionando la mejor ruta basado en la dirección IP destino. Y conecta múltiples redes a través de sus interfaces o puertos asociados a diferentes redes IP. El encaminador R1, en la Figura 4.1, se conecta con sus interfaces, hacia la izquierda con una red LAN y hacia la derecha a través de una red WAN con el encaminador R2. Los encaminadores disponen de interfaces para su conexión con las redes LAN, con las redes WAN, e interfaces para su administración.

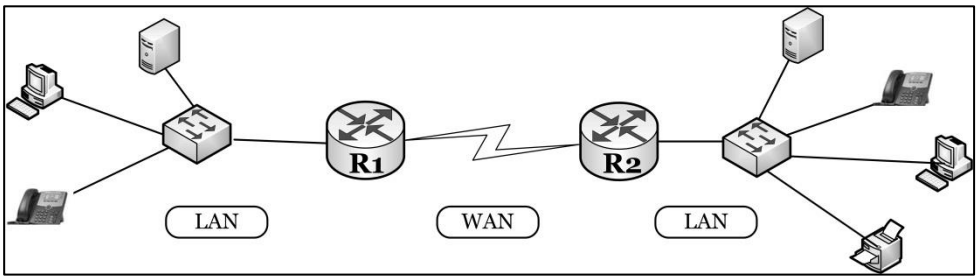


Fig. 4.1. Ejemplo de interconexión de redes LAN usando encaminadores.

La función primaria de un encaminador es recibir los paquetes en un puerto de entrada, determinar la mejor ruta al destino para cada paquete de acuerdo a una métrica, y enviar los paquetes hacia su destino por el puerto de salida seleccionado. Como se observa en la Figura 4.2, el paquete IP entra por la interfaz Ethernet del encaminador. El mismo examina la dirección IP destino del paquete, y determina la red destino a la que pertenece. Por la interfaz de salida en la ruta, el paquete se envía al próximo encaminador al destino final. El encaminador busca la mejor opción de la dirección IP destino del paquete y la dirección de red en la tabla de

encaminamiento. Ésta sirve para determinar el mejor paso, es decir, la mejor opción entre dirección IP destino y dirección de red en la tabla (Figura 4.2).

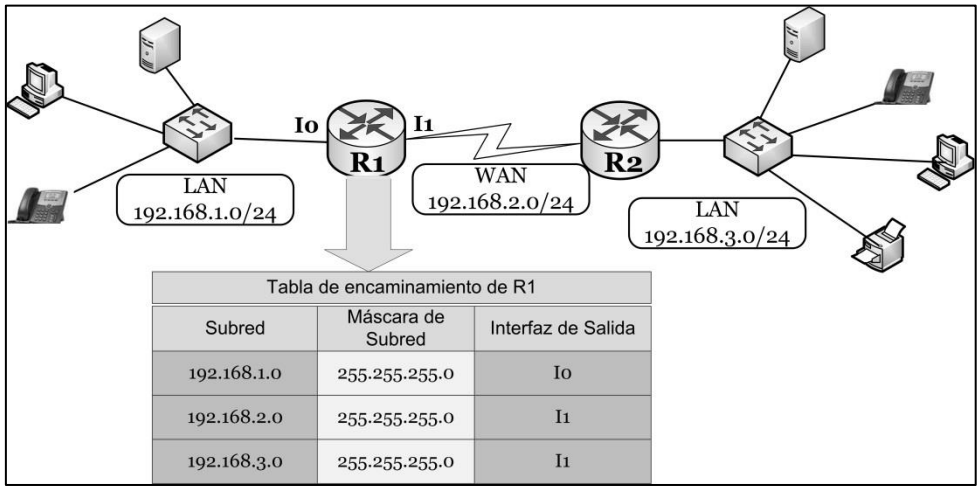


Tabla de encaminamiento de R1

Subred	Máscara de Subred	Interfaz de Salida
192.168.1.0	255.255.255.0	I0
192.168.2.0	255.255.255.0	I1
192.168.3.0	255.255.255.0	I1

Fig. 4.2. Ejemplo de encaminamiento de un paquete usando encaminadores.

4.1.3 CPU, Memorias y Sistema Operativo de los Encaminadores

Como se indicó previamente, los primeros encaminadores se construyeron sobre miniordenadores de propósito general. Los encaminadores actuales siguen siendo básicamente una computadora, salvo que ahora no disponen a la vista de los periféricos habituales, como un monitor o teclado, dado que no son necesarios. Para la administración se recurre a otra computadora desde la que se harán las supervisiones y configuraciones necesarias.

Un encaminador básicamente consta de una CPU, memorias y puertos (o interfaces) de comunicaciones. En la CPU se ejecutan las instrucciones y procesos de su sistema operativo. Pueden existir distintos tipos de memorias: una memoria RAM sobre la que se almacena el sistema operativo activo, el archivo de configuración en ejecución, la tabla de encaminamiento, la caché ARP, los buffers de entrada/salida de los puertos, etc. En la memoria ROM se almacena el *software* de diagnóstico usado cuando el encaminador se enciende, el programa bootstrap de arranque y una versión limitada del sistema operativo. La memoria *Flash* se utiliza para almacenamiento permanente de archivos, como el sistema operativo, copias de archivos de configuración, etc. Puede existir una memoria NVRAM donde se almacena el archivo de configuración de inicio (es decir, ante un arranque o reinicio del encaminador, esta copia se carga en la memoria RAM). El encaminador dispone de múltiples interfaces físicas que se usan para conectarse a la red correcta. Por ejemplo, puertos Ethernet y/o fast Ethernet, puertos seriales y puertos de consola para administración.

Se observan en la Figura 4.3, a título ejemplificativo, las instrucciones que en el modo comando pueden aplicarse a un encaminador particular para determinar las características de los recursos que posee.

El sistema operativo o IOS (*Internetwork Operating System*) del encaminador es el responsable de administrar sus recursos de hardware y software, el mapeo de memoria, la administración de los procesos, la seguridad, la

administración de los archivos de configuración y de sistemas, etc. El encaminador puede almacenar diferentes imágenes IOS, aunque una sola estará en servicio. Una imagen IOS es un archivo que contiene el IOS completo para ese encaminador. Cada imagen corresponderá a un modelo particular de encaminador, aunque podrá variar en sus características. Por ejemplo, una versión de IOS puede dar soporte a IPv6 o a un protocolo de encaminamiento particular como BGP.

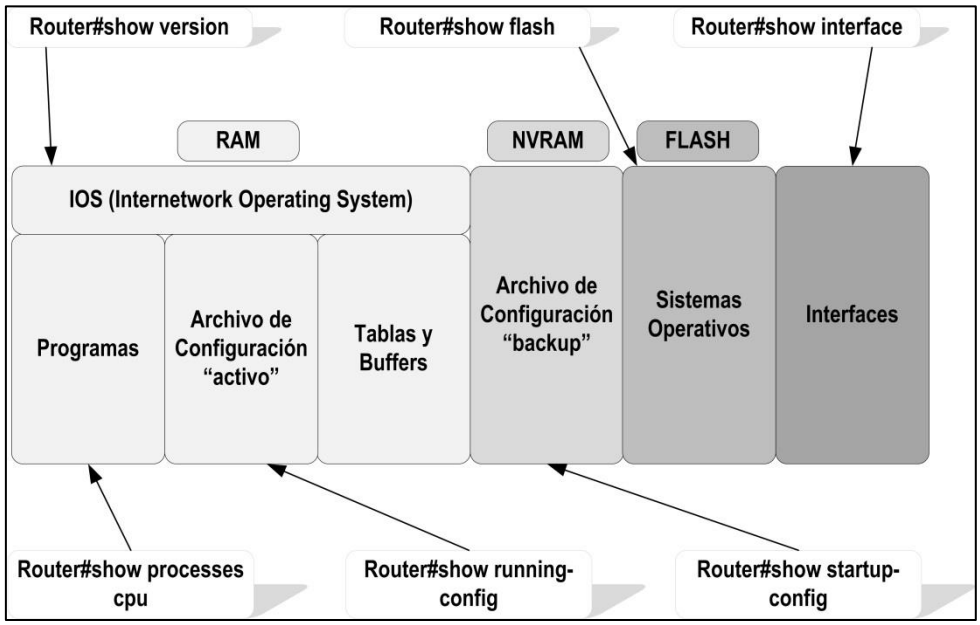


Fig. 4.3. Instrucciones en el modo comando sobre un encaminador.

El proceso de arranque (*boot process*) del encaminador es similar a cualquier computadora (inclusive que a un conmutador). En este proceso grabado en ROM se produce

una sucesión de operaciones desde el momento que se lo enciende hasta el momento que está en condiciones de realizar las operaciones para las cuales está configurado. La primera operación que se realiza es el denominado POST (*Power-On Self-Test*) que se refiere a las rutinas que se ejecutan inmediatamente después del encendido. El POST incluye rutinas para configurar valores iniciales para señales internas y externas, para ejecutar verificaciones, entre otros aspectos. Al terminar el POST exitosamente, se invoca el código del *boststrap* de ROM que carga el sistema operativo. Es necesario ubicar y cargar el sistema operativo que podrá estar almacenado en memoria flash o en un servidor TFTP. Finalmente, se ubica y carga el archivo de configuración almacenado habitualmente en la memoria NVRAM o en un servidor TFTP.

Como ejemplo podemos mencionar la instrucción *show version* del IOS de un producto en particular que permite observar varias de las características mencionadas precedentemente, como: versión de IOS, versión del boostrap, modelo del encaminador y tipo de CPU, número y tipo de interfaces, y cantidad de memoria NVRAM y Flash (Figura 4.4).

```
Router#show version
Cisco Internetwork Operating System Software
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
System returned to ROM by power-on
System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of NVRAM.
62720K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

Fig. 4.4. Verificación de las características principales del encaminador.

4.1.4 Puertos o Interfaces

Algunos fabricantes usan indistintamente los términos puerto o interfaz. Sin embargo, otros se refieren a puerto para indicar uno de los puertos de administración usados para acceso administrativo al encaminador, y usan el término interfaz para los puertos que son capaces de enviar y recibir tráfico de usuario (Figura 4.5).

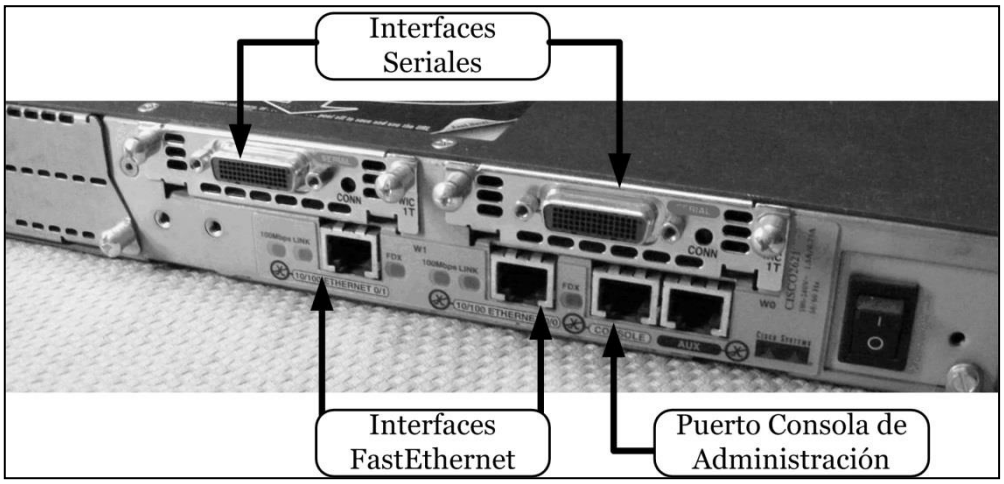


Fig. 4.5 Puertos e interfaces en un encaminador.

El puerto de consola se utiliza para la administración desde un dispositivo externo tipo terminal, o por una PC que ejecuta un *software* emulador de terminal (por ejemplo, *putty*). Se usa para la configuración inicial, y no se lo utiliza para los accesos a la red, mientras que el puerto auxiliar (AUX) se emplea también para la administración, pero a través de un módem. Hoy en día no todos los encaminadores tienen disponible este puerto.

Las interfaces se utilizan para recibir y enviar paquetes. Dada la función del encaminador para interconectar distintos tipos de redes, podrá disponer de interfaces con sus conectores para los medios correspondientes. Por ejemplo, interfaces Fast Ethernet para LANs, o serie para WAN, incluyendo T1, E1, DSL, ISDN, etc.

4.1.5 Encaminador como Dispositivo de Capa 3

Un encaminador es un dispositivo de Capa 3 debido a que su decisión primaria de envío se basa en la información del paquete IP de dicha Capa; específicamente en la dirección IP destino. El proceso se conoce como encaminamiento o enrutamiento (en inglés, *routing*) de los paquetes.

Las direcciones de Capa 2, física o MAC se usan en la trama para la comunicación interfaz a interfaz en la misma red. Y deben cambiarse cada vez que los paquetes se encapsulan y desencapsulan de red a red (Figuras 4.6 y 4.7). Mientras que las direcciones de Capa 3 de la fuente original o IP origen, y del destino final o IP destino, transportadas dentro del paquete IP de la trama, no cambian excepto cuando se usa NAT.

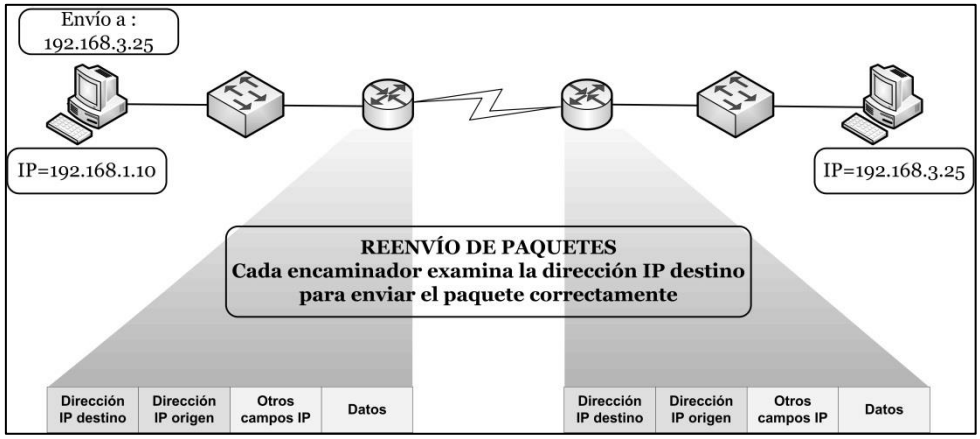


Fig. 4.6. Proceso de reenvío de paquetes a través de la red.

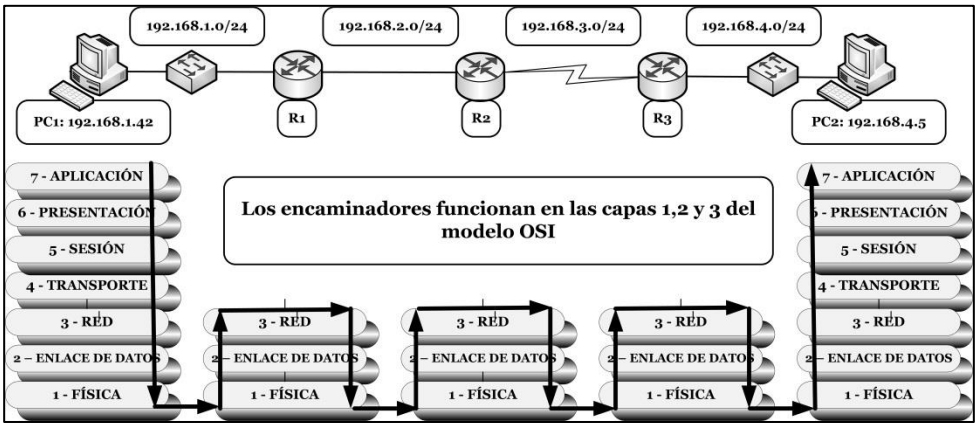


Fig. 4.7. Procesos de encapsulamiento y desencapsulamiento.

La mejor ruta para encaminar un paquete a una red destino debería ser la óptima o "más corta". Esto depende del protocolo de encaminamiento. Los protocolos de encaminamiento dinámicos usan sus propias reglas y métricas. Una métrica es el valor cuantitativo usado para medir la distancia a una ruta determinada. La mejor ruta a una red es el camino con la métrica más baja.

4.1.6 Instrucciones de Configuración Básicas

Desde la Figura 4.8 a la Figura 4.12 se muestran algunas instrucciones de configuración básicas del IOS de un encaminador (de un producto comercial en particular), aplicados sobre una interfaz Ethernet y una interface serial, y las instrucciones para verificar las interfaces y el archivo de configuración.

```
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#description LAN R1
Router(config-if)#no shutdown
```

Fig. 4.8. Configuración básica de una interfaz fastethernet del encaminador.

```
Router(config)#interface serial 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#description Link a R2
Router(config-if)#clock rate 512000
Router(config-if)#no shutdown
```

Fig. 4.9. Configuración básica de una interfaz serial del encaminador.

```
Router#show interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 00d0.bc4c.c901 (bia 00d0.bc4c.c901)
  Description LAN R1
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 1023 bits/sec, 8 packets/sec
(salida omitida)
```

Fig. 4.10. Instrucción de verificación de las interfaces fastethernet.

```
Router#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description Link a R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)

(salida omitida)
```

Fig. 4.11. Instrucción de verificación de las interfaces Seriales.

Estas configuraciones y verificaciones se han realizado a través de la interfaz de líneas de comando o CLI, aunque de acuerdo al producto también podrían realizarse, parcial o totalmente, usando las herramientas gráficas que se disponga, o vía un acceso WEB.

```
Router#show running-config
Current configuration : 632 bytes
version 12.4

no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname Router

interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto

interface Serial0/0/0
 ip address 192.168.2.1 255.255.255.0
 clock rate 500000

ip classless

line con 0

line aux 0

line vty 0 4
login
```

Fig. 4.12. Instrucción de verificación de archivo de configuración del encaminador.

En la Figura 4.13 se observa la instrucción *show ip route* que nos muestra la tabla de encaminamiento del encaminador R1 asociado al ejemplo de red. La tabla de encaminamiento es un arreglo de datos en RAM que se usa

para almacenar la información de ruta de las redes directamente conectadas y de las redes remotas.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

Fig. 4.13. Instrucción de verificación de la tabla de encaminamiento del encaminador.

Una red directamente conectada es aquella que está físicamente unida a una de las interfaces del encaminador. Cuando una interfaz del encaminador se configura con una dirección IP y máscara de subred, la interfaz se vuelve un host más de esa red. Las redes activas directamente conectadas se agregan automáticamente a la tabla de encaminamiento.

Una red remota no está directamente conectada al encaminador; solo puede alcanzarse enviando el paquete a otro encaminador. Éste a su vez, si es necesario, lo deriva hacia otro encaminador, y así sucesivamente hasta llegar al

último. Las redes remotas se agregan a la tabla de encaminamiento usando protocolos de encaminamiento dinámicos como RIP u OSPF, o rutas estáticas.

4.2 Protocolos de Encaminamiento y Encaminados

4.2.1 Introducción

Los protocolos de encaminamiento son esenciales para el funcionamiento de Internet. Los encaminadores envían paquetes o datagramas IP a través de una secuencia de dispositivos similares, que une el origen con el destino. Para ello, el encaminador debe tener una idea de la topología de la red. Los protocolos de ruteo proveen esta información para la toma de decisiones.

La función de los encaminadores es recibir y enviar datagramas. Toman decisiones de ruteo en base al conocimiento de la topología y las condiciones de la red. Las decisiones se basan en criterios del menor costo.

IP es un protocolo encaminado (*routed*, enrutado o ruteado). Es un protocolo de Capa 3 que contiene la información de la dirección de la red destino. Esta información la usan los encaminadores para determinar a qué interface y próximo encaminador enviar este paquete.

Un encaminador debe conocer cómo llegar a redes no-directamente conectadas. Existen dos formas: estática o dinámica. En la forma estática se usa una ruta programada que un administrador de red configura en el encaminador; y

en la forma dinámica se usa una ruta que un protocolo de encaminamiento ajusta automáticamente de acuerdo a cambios en la topología o en el tráfico.

Una ruta estática es una ruta única permanente configurada para cada par origen-destino. Los problemas aparecen cuando cambia la topología. En dicho caso habrá que reconfigurar manualmente la ruta estática. El criterio para elegir la ruta no se basa en datos dinámicos. La elección normalmente está basada en volúmenes de tráfico estimados y/o capacidades de los enlaces.

Las rutas estáticas se usan en conjunto con los protocolos dinámicos de encaminamiento. Se prefiere una ruta estática cuando el uso de los protocolos de encaminamiento dinámicos plantea desventajas (por ejemplo, restricciones de seguridad), o cuando no se necesitan porque existe una sola ruta.

En la Figura 4.14 se observan 5 redes, desde la Red 1 hasta la Red 5, conectadas a través de 8 encaminadores identificados como Encaminador A hasta Encaminador F. Se observa que existe un costo de enlace en la salida de cada encaminador para cada red. Por ejemplo, el Encaminador A tiene un costo de 7 hacia la Red 1 y un costo de 1 hacia la Red 4.

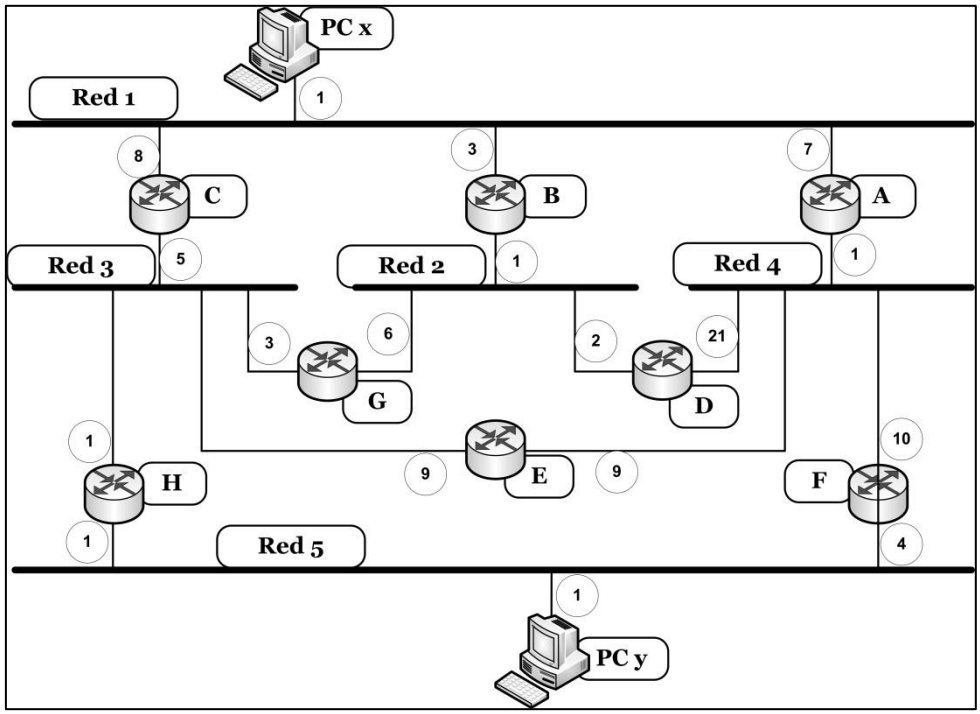


Fig. 4.14. Ejemplo de interconexión de 5 Redes usando 8 Encaminadores.

Para la gestión del tráfico, cada encaminador tiene una tabla de encaminamiento. Se requiere una tabla de encaminamiento por cada encaminador que tendrá entradas para cada red. La dirección de la red se obtiene de la porción de la red de la IP destino. Cuando se alcanza el encaminador junto a la red destino, luego de que se ha atravesado la secuencia de encaminadores, aquél puede enviar el datagrama al host destino. Cada entrada en la tabla de ruteo muestra sólo el próximo nodo en la ruta, no la ruta completa.

Las tablas de encaminamiento pueden también estar presentes en los hosts. Si el host está unido a una única red, y esa red tiene un único encaminador conectado, no se necesita la tabla de encaminamiento porque todo el tráfico debe pasar por ese encaminador, que es la puerta de enlace de la red. Sin embargo, cuando existen múltiples encaminadores conectados a esa red, el host necesita de la tabla de encaminamiento para saber qué encaminador usar para llegar a una red destino determinada.

En las Figuras 4.15, 4.16 y 4.17 se presentan las tablas de encaminamiento para la red de la Figura n° 4.14. Se observa que cada tabla pertenece a un encaminador o un host, e indica la red destino que se puede alcanzar y a través de qué encaminador. La tabla siempre indicará la ruta de menor costo.

Por ejemplo, en la Tabla del Encaminador A se indica que para llegar a la Red 3 los paquetes deben enviarse al Encaminador D a través de la salida de costo 1. Y aunque luego se debe seguir la ruta atravesando el Encaminador G, para llegar a la Red 3, este camino es más económico que seguir la secuencia o ruta por el Encaminador C usando la salida de costo 7. En las tablas de encaminamiento en las que aparecen guiones, sin mencionar ningún encaminador, se presentan los casos de conexiones directas a las Redes, cuando el costo de la salida correspondiente es la mejor opción.

TABLA ENCAMINADOR A

RED	ENCAMINADOR
1	D
2	D
3	D
4	---
5	F

TABLA ENCAMINADOR B

RED	ENCAMINADOR
1	---
2	---
3	G
4	D
5	G

TABLA ENCAMINADOR C

RED	ENCAMINADOR
1	---
2	B
3	---
4	A
5	H

Fig. 4.15. Tablas de encaminamiento
de los Encaminadores A, B y C.

TABLA ENCAMINADOR D

RED	ENCAMINADOR
1	B
2	---
3	G
4	---
5	F

TABLA ENCAMINADOR E

RED	ENCAMINADOR
1	D
2	D
3	---
4	---
5	H

TABLA ENCAMINADOR F

RED	ENCAMINADOR
1	H
2	H
3	H
4	---
5	---

Fig. 4.16. Tablas de encaminamiento
de los Encaminadores D, E y F.

TABLA ENCAMINADOR G

RED	ENCAMINADOR
1	B
2	---
3	---
4	D
5	H

TABLA ENCAMINADOR H

RED	ENCAMINADOR
1	C
2	G
3	---
4	G
5	---

TABLA PC X

RED	ENCAMINADOR
1	---
2	B
3	B
4	A
5	A

Fig. 4.17. Tablas de encaminamiento
de los Encaminadores G y H, y de la PC X.

4.2.2 Encaminamiento Adaptativo o Dinámico

Cuando las condiciones de la red cambian, las rutas pueden o deben cambiar. Esto puede producirse por la inclusión de redes nuevas, fallas en los dispositivos y/o los enlaces, problemas de lazos de encaminamiento, o problemas de congestión en la red.

Las decisiones de encaminamiento son más complejas y aumentan el procesamiento del encaminador. Dichas decisiones se basan en información obtenida en un lugar, pero usada en otra parte. Es decir, se trata de información que generan los encaminadores para que la usen otros encaminadores. Mientras más información se intercambia entre los encaminadores mejoran las decisiones de encaminamiento, porque seguramente aumenta la calidad de la información. Sin embargo, esto incrementa la sobrecarga de tráfico. En los dos extremos operativos puede suceder que

el sistema reaccione demasiado rápido ante un cambio en la red, provocando congestión y oscilaciones. En el otro caso puede reaccionar muy lentamente y ser irrelevante. Existen dos casos especiales: Agitación (*Fluttering*) y Formación de lazos (*Looping*).

Se llama agitación a las oscilaciones rápidas en el encaminamiento, debido a que el encaminador intenta hacer balanceo o reparto de cargas entre una cierta cantidad de rutas disponibles. El problema es que los paquetes sucesivos de una transferencia pueden llegar al mismo destino tomando rutas muy diferentes.

Si la agitación sólo aparece en un sentido, las características de las rutas pueden diferir en las dos direcciones, incluyendo diferencias en la temporización y características de error. Esto puede confundir a las aplicaciones de gestión y de localización de averías que tratan de medir las características de las rutas. Con dos rutas distintas entre origen y destino, se dificultan las estimaciones de tiempo y de capacidades disponibles. Por ejemplo, los segmentos TCP llegarían fuera de orden, se producirían retransmisiones espurias y aparecerían reconocimientos duplicados.

Los lazos se producen cuando los paquetes enviados por un encaminador retornan a ese mismo encaminador. Los algoritmos de encaminamiento se diseñan para prevenir los lazos. Pueden ocurrir cuando los cambios en la conectividad de la red no se propagan lo suficientemente rápido a todos los otros encaminadores.

El encaminamiento dinámico ofrece varias ventajas, mientras deben prevenirse sus eventuales desventajas. Se destaca que mejora la prestación vista por el usuario. Además, puede ayudar a controlar la congestión. Los beneficios dependen de las características del diseño del algoritmo de encaminamiento. Estos algoritmos son muy complejos y están en continua evolución.

Se puede plantear una comparación entre el encaminamiento estático y el dinámico. En el estático la configuración de las tablas es manual. Aunque hay un mayor control, no es escalable para una gran cantidad de encaminadores debido a los tiempos de configuración que se requerirían. Además, la actividad manual necesaria para ajustar los encaminadores, ante los cambios que se producen en la red, hace lenta la adaptación. Con el encaminamiento dinámico se obtienen rutas óptimas y rapidez de adaptación a los cambios en la red. Además, son escalables. Lógicamente que se incrementa la demanda de recursos de CPU, de ancho de banda y de memoria de los encaminadores. Y la configuración y ajuste del encaminamiento dinámico, especialmente en grandes redes, son tareas complejas.

Las estrategias para el encaminamiento dinámico pueden clasificarse según el origen de la información que utilicen en: Local, de Nodos Adyacentes y de Todos los nodos. La estrategia local encamina cada paquete a la red por la interfaz de cola más corta. Su objetivo es el balance de cargas en las redes, aunque puede suceder que el datagrama no sea dirigido en la dirección correcta. Se sugiere la

inclusión de una dirección preferida. Esta estrategia es muy poco usada. La estrategia que obtiene la información de los nodos adyacentes es propia de los algoritmos denominados vector distancia, y la que obtiene información de todos los nodos es utilizada por los algoritmos de estado de enlace. Estos algoritmos necesitan que el protocolo de encaminamiento intercambie información entre los nodos.

Las características más importantes a considerar en los protocolos de encaminamiento dinámico son: el tiempo de convergencia, la escalabilidad, su formato en la forma de manejar el direccionamiento IPv4 de acuerdo o no a las clases (classless o classful), el uso de recursos, y la implementación y mantenimiento. El tiempo de convergencia a un estado estable, luego de un cambio en la red, es una característica muy importante de los protocolos dinámicos. Mientras más rápido mejor. La escalabilidad hace referencia al tamaño de la red que se puede gestionar. El protocolo puede ser *classless* o *classful* en cuanto a la capacidad de soporte de VLSM y CIDR. El uso de recursos quiere destacar el nivel de la demanda de memoria RAM, CPU y ancho de banda de enlace que requiere el algoritmo, mientras que el tipo de implementación y mantenimiento plantea el conocimiento que se requiere para un administrador de la red.

4.2.3 Sistemas Autónomos y Protocolos IRP - ERP

Se plantearán tres conceptos que están relacionados: los Sistemas Autónomos, los Protocolos de Encaminamiento

(Interior Routing Protocol - IRP) y los Protocolos de Encaminamiento (Exterior Routing Protocol - ERP). Se llama Sistema Autónomo (SA) al grupo de encaminadores que intercambian información vía un protocolo de encaminamiento común. También se puede definir como el conjunto de encaminadores y redes administradas por una única organización. En la Figura 4.18 se presentan dos sistemas autónomos llamados Sistema Autónomo 1 y Sistema Autónomo 2. Como se observa, estos Sistemas Autónomos a su vez están vinculados entre sí.

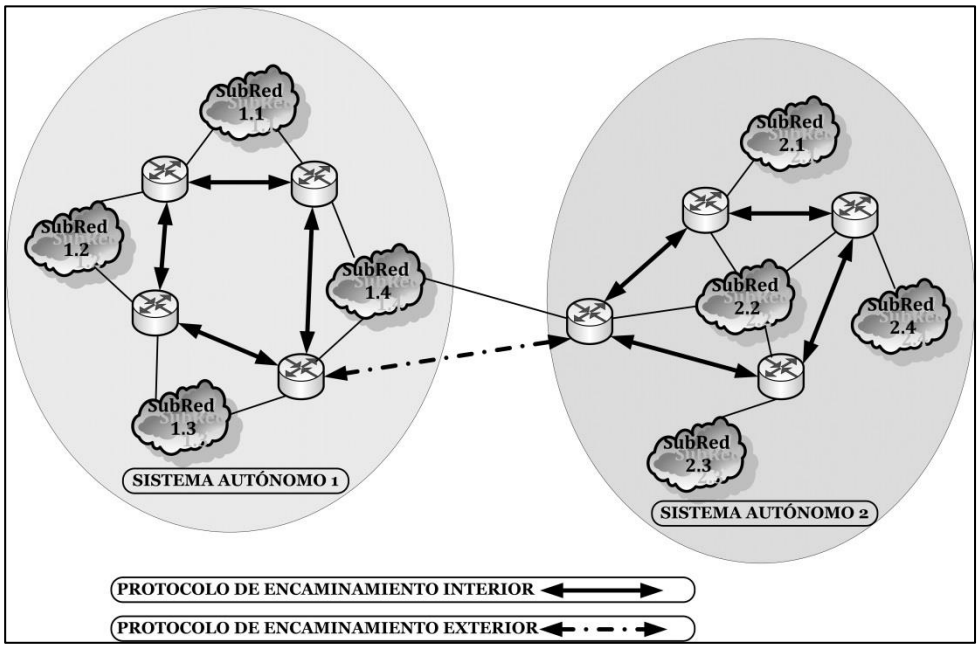


Fig. 4.18. Ejemplo de interconexión
de los Sistemas Autónomos 1 y 2.

Los protocolos de encaminamiento interior (IRP) reciben este nombre porque transmiten información de encaminamiento entre los encaminadores de un Sistema Autónomo. Dado que los Sistemas Autónomos tienen dimensiones físicas limitadas y están gestionados por una autoridad administrativa, los IRP se diseñan o configuran "a medida". Pueden usarse diferentes algoritmos de encaminamiento en diferentes SA conectados. Los Sistemas Autónomos necesitan mínima información de otro SA conectado. Esa conexión se obtiene al menos a través de un encaminador en cada SA. Tales encaminadores usan protocolos de encaminamiento exterior (ERP)

Los protocolos de encaminamiento exterior (ERP) pasan menos información que los IRP. Solo es necesario que el encaminador en el primer Sistema Autónomo determine la ruta al Sistema Autónomo destino. Los encaminadores en el Sistema Autónomo destino cooperan para enviar el paquete. El ERP no conoce los detalles de la ruta seguida dentro del Sistema Autónomo destino.

La Figura 4.19 presenta algunos ejemplos de protocolos de encaminamiento interior IRP vector distancia y de estado de enlace, como son: RIP, IGRP, OSPF, IS-IS y EIGRP. También se presenta BGP como ejemplo de protocolo de encaminamiento exterior ERP.

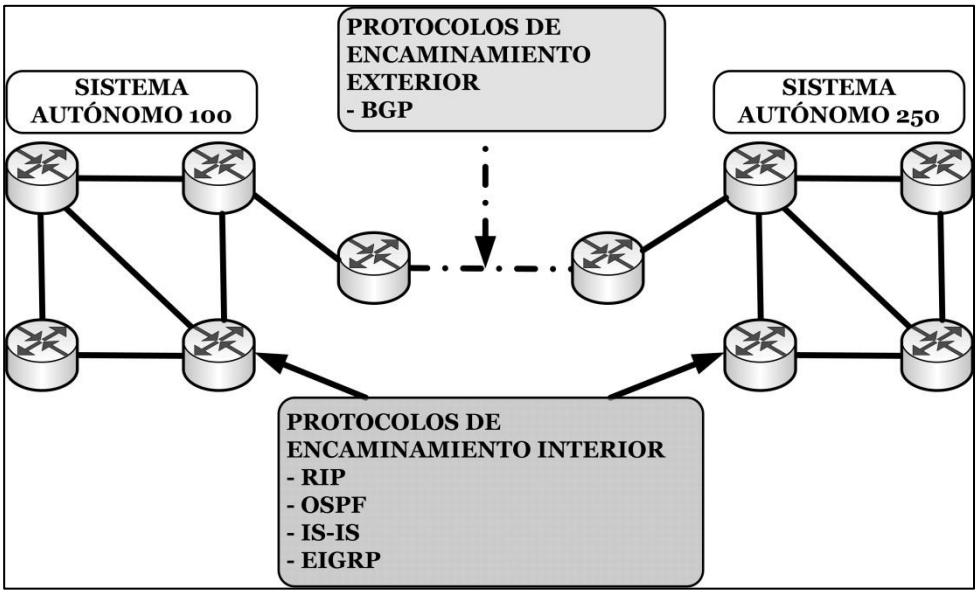


Fig. 4.19. Ejemplos de Protocolos IRP y ERP.

4.2.4 Tipos de Encaminamientos: vector distancia, de estado de enlace y vector-paso

En el encaminamiento vector distancia, cada nodo (encaminador o host) intercambia información con los nodos vecinos. Se llaman vecinos cuando los encaminadores están conectados directamente a la misma red. La técnica de encaminamiento vector distancia fue la primer generación de algoritmos de encaminamiento usados por ARPANET. Cada nodo mantiene un vector de los costos de enlace para cada red conectada directamente, y la distancia y los vectores del siguiente salto para cada destino. RIP es un ejemplo de protocolo vector distancia. Para el funcionamiento del encaminamiento vector distancia se requiere la transmisión de mucha información por cada encaminador, dado que es necesario enviar el vector distancia a todos los vecinos. Este

encaminamiento contiene un costo de paso estimado a todas las redes en la configuración, y los cambios insumen mucho tiempo en propagarse.

El encaminamiento de estado de enlace se diseñó para evitar las desventajas del encaminamiento vector-distancia. Cuando el encaminador se inicializa, fija el costo de enlace para cada interfaz, y notifica el conjunto de costos de enlace a todos los encaminadores en la topología. Es decir, no sólo envía la información a los encaminadores vecinos sino a todos. A partir de ese momento, cada encaminador monitorea sus costos de enlace, y si hay un cambio significativo, notifica de nuevo sus costos de enlace. Con esta información cada encaminador puede construir la topología de la configuración entera, y calcular el camino más corto a cada red destino. Se concluye que cada encaminador construye su propia tabla de encaminamiento, conteniendo el primer salto a cada destino. No se trata de un encaminamiento distribuido. Y podría usarse cualquier algoritmo para determinar los caminos más cortos, aunque en la práctica se utiliza el algoritmo de Dijkstra. OSPF es un ejemplo de protocolo de encaminamiento de estado de enlace. Comenzó a usarse en la segunda generación de ARPANET.

Los protocolos de encaminamiento exterior, también denominados de vector paso, prescinden de las métricas de encaminamiento. Su función es proveer información sobre qué redes pueden alcanzarse por un encaminador dado y qué sistema autónomo cruza para llegar a esa red. No se incluye distancia o estimación de costos. Cada bloque de información lista todos los sistemas autónomos visitados en esta ruta.

Está especializado para realizar políticas de encaminamiento, como por ejemplo: evitar el camino que transita por un sistema autónomo particular, velocidad de enlace, capacidad, tendencia a volverse congestionado, calidad de funcionamiento, seguridad, minimizar el número de sistemas autónomos de tránsito, entre otros aspectos.

La Figura 4.20 presenta un interesante detalle cronológico de la mayoría de los protocolos de encaminamiento interior y exterior existentes. Además, la progresión de las diversas versiones de los mismos agrupados según se trate de protocolos de encaminamiento vector distancia, de estado de enlace o de vector paso, y si son *classless*, *classful* o utilizados para IPv6.

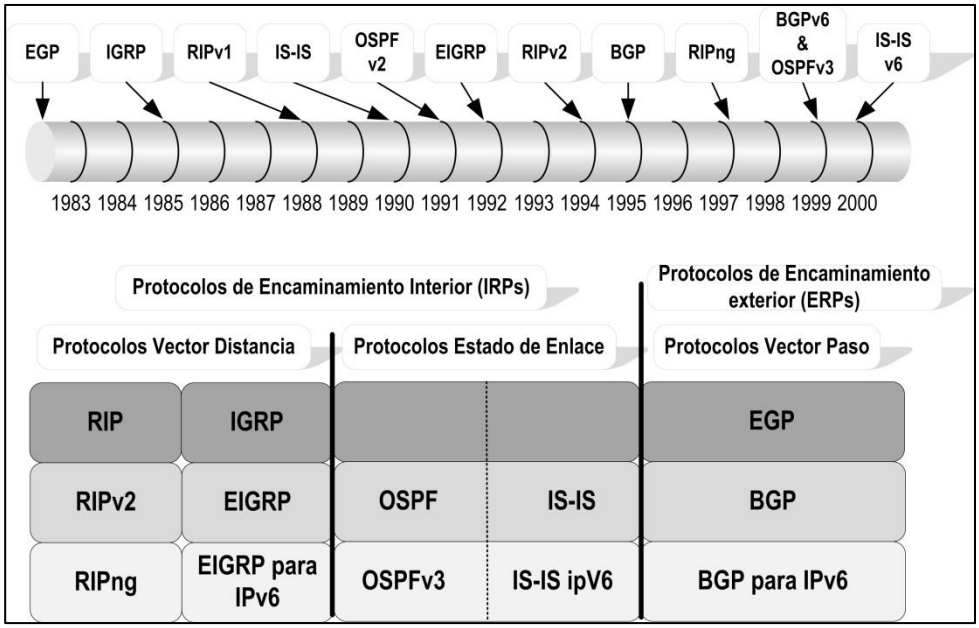


Fig. 4.20. Evolución de los Protocolos de Encaminamiento.

4.2.5 Algoritmos de Encaminamiento

Casi todas las redes de conmutación de paquetes y todas las de Internet basan sus decisiones de encaminamiento en algún criterio de mínimo costo. Un criterio es minimizar el número de saltos, en cuyo caso cada enlace tendrá asociado un valor de 1. Con otros criterios más frecuentes, el valor asociado al enlace es inversamente proporcional a su capacidad, proporcional a su carga actual o una combinación de ellos. Este costo puede ser diferente para cada uno de los dos sentidos. Se define el costo de una ruta entre dos nodos como la suma de los costos de los enlaces atravesados. Y para cada par de nodos se busca el camino de mínimo costo.

La mayor parte de los algoritmos de encaminamiento de mínimo costo son variantes de uno de los dos algoritmos más conocidos: el Algoritmo de *Dijkstra* y el Algoritmo de *Bellman-Ford*.

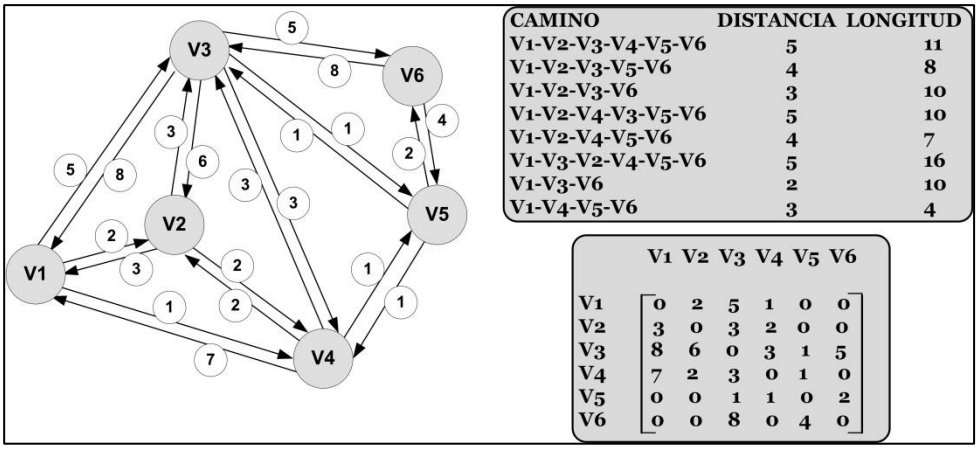
El algoritmo de Dijkstra se puede enunciar como sigue: Encontrar los pasos más cortos desde un nodo origen dado a todos los otros nodos, por desarrollo de caminos en orden creciente de longitud de camino.

Procede en etapas:

- en la etapa k se determinan los caminos más cortos a los k nodos más cercanos al origen especificado;
- estos nodos se almacenan en el conjunto T;

- en la etapa (k + 1), se añade a la lista T aquel nodo que presente el camino más corto desde el nodo origen y que no se encuentre ya incluido en dicha lista.
- A medida que se incorporan nuevos nodos a T, se define su camino desde el origen.

En las Figuras 4.21 y 4.22 se presenta un ejemplo con un grafo que describe los nodos de la red y los costos de los enlaces en ambos sentidos que hay entre los nodos, la matriz V que tiene cargado el costo de los enlaces entre nodos, y la secuencia de costo mínimo para la ruta 1-6. Para llegar del nodo V1 al V6 se deben atravesar 3 enlaces, y el costo o longitud es de 4.



CAMINO	DISTANCIA	LONGITUD
V1-V2-V3-V4-V5-V6	5	11
V1-V2-V3-V5-V6	4	8
V1-V2-V3-V6	3	10
V1-V2-V4-V3-V5-V6	5	10
V1-V2-V4-V5-V6	4	7
V1-V3-V2-V4-V5-V6	5	16
V1-V3-V6	2	10
V1-V4-V5-V6	3	4

	V1	V2	V3	V4	V5	V6
V1	0	2	5	1	0	0
V2	3	0	3	2	0	0
V3	8	6	0	3	1	5
V4	7	2	3	0	1	0
V5	0	0	1	1	0	2
V6	0	0	8	0	4	0

Fig. 4.21. Grafo que describe los nodos de la red y los costos de enlaces.

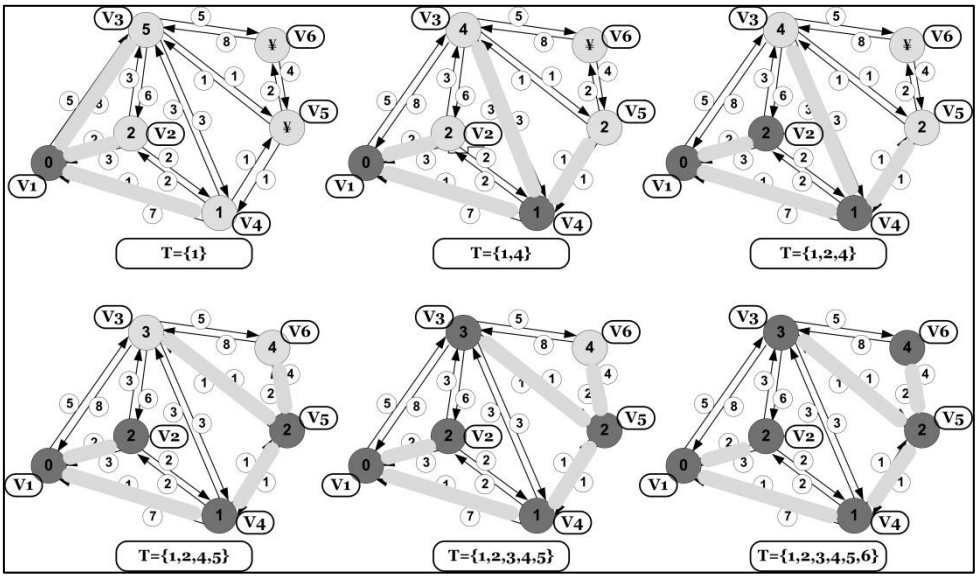


Fig. 4.22. Aplicación del algoritmo de Dijkstra
para llegar del nodo V1 al V6.

El algoritmo de Bellman-Ford se puede enunciar así: encontrar los caminos más cortos desde un nodo origen dado con la condición de que éstos contengan a lo sumo un enlace; a continuación encontrar los caminos más cortos con la condición de que contengan dos enlaces como máximo, y así sucesivamente.

La Figura 4.23 muestra el resultado de aplicar el algoritmo de Bellman-Ford sobre el mismo ejemplo anterior. Se destaca que dichos resultados coinciden con los obtenidos por el algoritmo de Dijkstra.

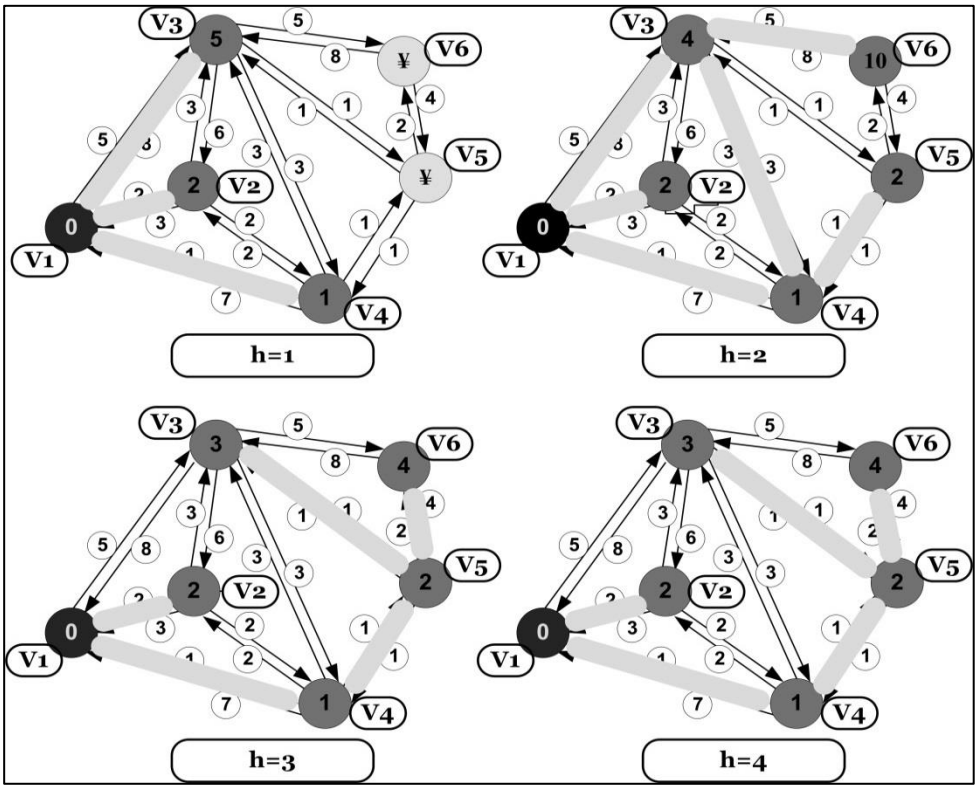


Fig. 4.23. Ejemplo de aplicación del algoritmo Bellman-Ford.

Es interesante comparar estos dos algoritmos en función de la información necesaria para su ejecución. En el caso de Bellman-Ford, para el cálculo del nodo *n* es necesario el costo del enlace a todos los nodos vecinos, más el costo del camino total de cada uno de estos nodos vecinos, desde un nodo de origen particular *s*. Entonces, cada nodo puede mantener un conjunto de costos y caminos asociados para todos los otros nodos de la red e intercambiar periódicamente esta información con sus vecinos directos. Cada nodo puede usar Bellman-Ford basándose sólo en la información dada por sus vecinos y conociendo sus costos de enlace asociados,

para actualizar sus caminos y costos. En el caso de Dijkstra, cada nodo debe conocer todos los enlaces y los costos asociados a ellos, es decir, debe conocer la topología completa de la red. Esa información debe intercambiarse con todos los otros nodos de la red.

En la evaluación de ventajas relativas de ambos algoritmos se debe considerar el tiempo de procesamiento y la cantidad de información del resto de nodos de la red. Ambos algoritmos convergen a la misma solución bajo condiciones estables de la topología y los costos de los enlaces. Si los costos de enlace cambian con el tiempo, el algoritmo intentará ponerse al corriente de estos cambios. Cuando el costo del enlace depende del tráfico, que a su vez depende de las decisiones de encaminamiento, se produce una condición de realimentación que puede resultar en inestabilidades.

4.3 Ejercitación

Ejercicio n° 1:
Defina que es un protocolo encaminado y explique sus principales características. De ejemplos.

Ejercicio n° 2:
Defina que es un protocolo de encaminamiento y explique sus principales características. De ejemplos.

Ejercicio n° 3:
Para las siguientes direcciones IPv4 de hosts y máscaras de subred encuentre la subred a la que pertenece cada host, la

dirección de difusión de cada subred y el rango de direcciones de hosts para cada subred:

a) 10.14.87.60/19
b) 172.25.0.235/27
c) 172.25.16.37/25

Resolución Ejercicio n° 3:

a. 10.14.87.60/19
   Dirección de subred: 10.14.64.0
   Rango de direcciones IP disponibles: 10.14.64.1 a 10.14.95.254
   Dirección de broadcast: 10.14.95.255
b. 172.25.0.235/27
   Dirección de subred: 172.25.0.224
   Rango de direcciones IP disponibles: 172.25.0.225 a 172.25.0.254
   Dirección de broadcast: 172.25.0.255
c. 172.25.16.37/25
   Dirección de subred: 172.25.16.0
   Rango de direcciones IP disponibles: 172.25.16.1 a 172.25.16.126
   Dirección de broadcast: 172.25.16.127

Ejercicio n° 4:
Se desea configurar una interfaz con la dirección IPv4 192.168.13.175 con una máscara de 255.255.255.240, ¿hay algún problema?

Resolución Ejercicio n° 4:

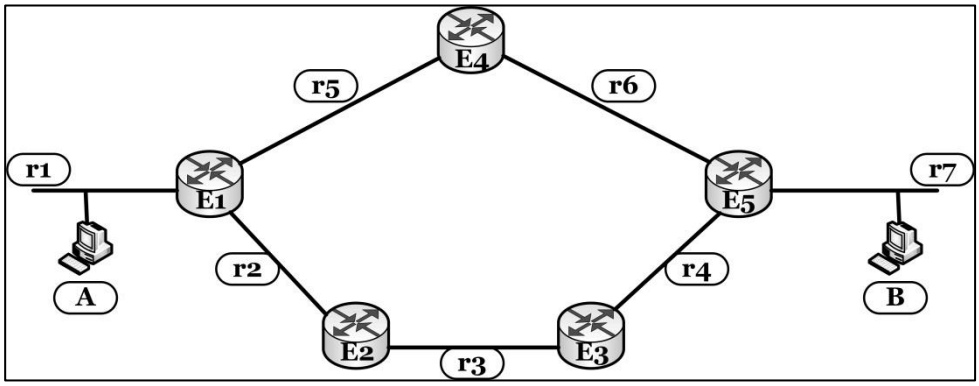
Sí, ya que es una dirección de difusión.

Ejercicio n° 5:
Indicar a qué tipo de direcciones IPv6 pertenecen las siguientes direcciones:
2001:db8:fe80:ffff::a:b:c
2a01:48:1:1:2c0:26ff:fe26:4ba
fe80::9ce4:ecde:cf33:a2a2
2002:1bc3:1b::1:2
::1
fd00:a:b:17c2::1
ff0e::1:2:3:4
ff05::a:b:c

Ejercicio n° 6:
De la red de la Figura considere un paquete de 1200 bytes (incluyendo el encabezado IP de 20 bytes), que se envía de la estación A a la B
Los valores de MTU de cada red son:
MTU n1: 600 B
MTU n2: 600 B
MTU n3: 400 B
MTU n4: 1500 B
MTU n5: 600 B
MTU n6: 1500 B
MTU n7: 1500 B

R1 realiza balance de carga, enviando alternativamente paquetes por R2 y R4 (es decir un paquete va por R2 y el siguiente por R4, el siguiente por R2, y el siguiente por R4, etc).

a. Se pide describir el proceso de fragmentación, y todos los fragmentos asociados, considerando que cada fragmento posee el mayor tamaño posible, y que el primer paquete que pasa por R1 sigue la ruta por R2.
b. ¿Qué efecto puede tener esta característica sobre protocolos de Capa de transporte como TCP?



Resolución Ejercicio n° 6:

a. Cuando el emisor transmite, el mensaje se fragmenta ya que el MTU_n1=600B, por lo tanto tendremos:
l = 1200b – 20b = 1180b; donde l=longitud del mensaje

La cantidad máxima de datos por paquetes será:
lmáx = MTU – 20b = 600b – 20b = 580b

Por lo tanto por el enlace n1 se transmitirán:
= 1480b/580b = 3 paquetes (p1, p2 y p3).

Como R1 está usando balanceo, p1 y p3 irán por el enlace n2 mientras que P2 lo hará por n5

El paquete p2 al ser enviado por la ruta R1-R4-R5 no necesitara ser fragmentado en ningún momento ya que el menor mtu es igual al tamaño del paquete.
En cambio los paquetes p1 y p3 al seguir la ruta R1-R2-R3-R5 serán nuevamente fragmentados para ser transmitidos por n3 (MTU=400B). Al igual que antes:
580b/380b = 2 paquetes
Por último los paquetes serán recibidos y re ensamblados en el destino B

b. En TCP no habría problemas, ya que al tener identificado cada paquete, lo reordena en el destino.

   En UDP puede haber problemas, ya que los paquetes pueden llegar en distinto orden respecto al inicio.

4.4 Bibliografía y referencias

4.4.1 Libros impresos

- William Stallings, "Data and Computer Communications", Pearson Education, 10° Ed., 2014.
- William Stallings y Thomas Case, "Business Data Communications", Pearson Education, 7° Ed., 2013.
- William Stallings, "Data and Computer Communications", Pearson Education, 8° Ed., 2009.
- CCNA de CISCO Press.
- William Stallings, "Wireless Communications & Networks", Prentice Hall, 2° Ed., 2005.

- Michael Daoud Yacoub “Wireless Technology: Protocols, Standards, and Techniques”, CRC Press, 2002.
- William Stallings, “Local and Metropolitan Area Networks”, Prentice Hall, 6° Ed., 2000.
- Uyless Black, “Tecnologías Emergentes para Redes de Computadoras”, Ed. Prentice-Hall, 1999.
- D. Comer, “Redes Globales de Información con Internet y TCP/IP”, Ed. Prentice-Hall, 3° Ed., , 2000.
- Request for Comments referidos a la temática.
- Artículos de revistas (IEEE, ACM, etc.) referidos a la temática.

4.4.2 Enlaces y Referencias

- Artículos técnicos de Cisco sobre encaminamiento
  https://supportforums.cisco.com/community/netpro/network-infrastructure/routing
  https://supportforums.cisco.com/community/netpro/small-business/routers
- Normas de RIP
  http://tools.ietf.org/html/rfc2453
  http://www.ietf.org/rfc/rfc1058
- Normas de OSPF
  http://www.ietf.org/rfc/rfc2328.txt
  http://www.ietf.org/rfc/rfc5340.txt
- Normas de BGP
  http://tools.ietf.org/html/rfc4274
  http://www6.ietf.org/rfc/rfc4271
- Sistemas autónomos de Argentina
  http://bgp.he.net/country/AR

- Definición y actualización de sistemas autónomos http://www.nro.net/technical-coordination/asn

CAPÍTULO 5

Protocolos de Encaminamiento RIP, OSPF y BGP

5.1 Protocolo RIP

5.1.1 Conceptos fundamentales en RIP

5.1.2 Evolución

5.2 Protocolo OSPF

5.2.1 Conceptos fundamentales en OSPF

5.2.2 Paquetes

5.2.3 Tipos de encaminadores en OSPF

5.2.4 Concepto de Área OSPF

5.3 Protocolo BGP

5.3.1 Introducción

5.3.2 Conceptos fundamentales en BGP

5.3.3 Operación

5.3.4 Mensajes

5.3.5 Estados

5.3.6 Atributos

5.4 Ejercitación

5.5 Bibliografía y Referencias

5.5.1 Libros impresos

5.5.2 Enlaces y Referencias

Capítulo 5

Protocolos de Encaminamiento RIP, OSPF y BGP

5.1 Protocolo RIP

5.1.1 Conceptos fundamentales en RIP

RIP es un protocolo de encaminamiento interior del tipo vector distancia. En los protocolos vector distancia, cada nodo intercambia información con los encaminadores vecinos, que son los que están directamente conectados por la misma red. En general, éstos mantienen tres vectores conocidos como: de costo de enlace, de distancia y de próximo salto. Cada 30 segundos, se intercambia el vector distancia con los encaminadores vecinos. Con estos datos se actualizan la distancia y el vector del próximo salto.

RIP es una versión distribuida del algoritmo de Bellman-Ford. Cada intercambio simultáneo de vectores entre encaminadores es equivalente a una iteración del paso 2 de dicho algoritmo. En el arranque, se obtienen los vectores de los vecinos, lo que permite definir un encaminamiento inicial. A través de un temporizador, se producen las actualizaciones cada 30 segundos. Estos cambios se propagan a través de la red, y el encaminamiento converge en un tiempo finito a un estado estable, que es proporcional al número de encaminadores.

El algoritmo original supone que todas las actualizaciones de los vecinos llegan en un corto lapso de tiempo, y con toda esta información, el encaminador que corre RIP actualiza su tabla. Esto no es del todo práctico, y en su lugar se usa actualización incremental. Cuando llega dicha actualización, se modifica la tabla. Las tablas se actualizan después de recibir cualquier vector distancia individual, y entonces agrega cualquier nueva red destino, reemplaza rutas existentes con pequeños retardos, y si la actualización viene del encaminador R, actualiza todas las rutas usando R como próximo salto. Los paquetes RIP son transportados sobre el protocolo de transporte UDP.

Si no hay actualizaciones recibidas desde un encaminador dentro de los 180 segundos, se marca la ruta como inválida. El encaminador espera actualizaciones cada 30 segundos; si transcurren 180 segundos sin novedad supone que el dispositivo falló o que la conexión de red se volvió inestable. Y por lo tanto, hubo un cambio en la topología. El marcado de la ruta como inválida se efectúa asignando a la misma el valor distancia infinito. En realidad se coloca el valor codificado 16 que simboliza lo mismo, ya que es la máxima distancia permitida.

Uno de los problemas en RIP es la denominada cuenta al infinito, asociada a su convergencia lenta. El ejemplo de la Figura 5.1 ilustra la situación.

Tenemos un sistema autónomo con 5 redes, desde Red 1 a Red 5, vinculadas con 4 encaminadores, desde el encaminador A al encaminador D. Se asume que todos los costos de enlace valen 1. El encaminador B tiene una distancia 2 a la Red 5, con el siguiente salto en el encaminador D. Los encaminadores A y C tienen distancia 3 a la Red 5 y próximo salto a través de B. Si el encaminador D falla, B determina que no puede llegar a la Red 5 por esa vía, y entonces cambia la distancia a 4 para la Red 5 basado en el reporte de los encaminadores A o C. En la próxima actualización, el encaminador B le informa a los encaminadores A y C sobre esta modificación. Luego, en éstos, la distancia a la Red 5 toma el valor 5. El valor 5 se obtiene del valor de distancia 4 que les dice el encaminador B más 1 para que ellos puedan acceder al encaminador B. En esa situación, el encaminador B recibe el conteo de distancia 5 a la Red 5, y asume que dicha red está a 6 de él, dado que para llegar debe hacerlo a través de A o C.

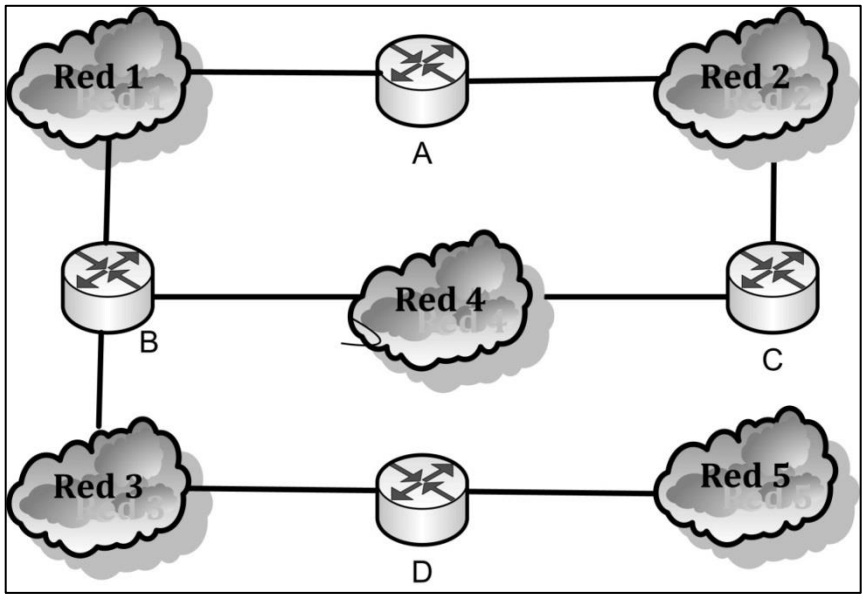


Fig. 5.1. Ejemplo que ilustra el problema de RIP sobre la cuenta al infinito.

El proceso se repite hasta alcanzar el valor infinito o 16; esto puede insumir 8 a 16 minutos.

El problema de la cuenta al infinito aparece por un malentendido entre los encaminadores A y B, y entre los encaminadores B y C. Cada uno piensa que puede alcanzar la Red 5 vía el otro. Como posible solución se utiliza la regla del Horizonte Dividido que dice que no se debe enviar información sobre una ruta en el sentido de donde proviene. De esta forma, el encaminador que envía la información es el que está más cerca del destino, y ahora se elimina una ruta errónea dentro de los 180 segundos.

Una solución aún más rápida es aplicar el concepto de Ruta Envenenada o Envenenamiento Inverso. Con este recurso se envían actualizaciones, con una cuenta de saltos de 16, a los vecinos para rutas aprendidas desde esos vecinos. Si dos encaminadores tienen rutas apuntándose mutuamente entre sí, el aviso de rutas inversas con métrica 16 rompe el lazo inmediatamente.

Evidentemente los tiempos juegan un rol importante en el funcionamiento del protocolo. Por ese motivo, se asocia un temporizador con cada entrada de la tabla de encaminamiento. Si no se actualiza la entrada al cabo del tiempo asignado al temporizador, se la marca con infinito.

Normalmente se configura el temporizador con un tiempo equivalente a 6 veces el intervalo de transmisión. Un cambio en la tabla provoca la publicación del mismo. La publicación de las tablas se realiza normalmente cada 30 segundos. Si se recibe un incremento en alguna ruta, su métrica se pasa inicialmente a infinito. Pero se adopta si luego se confirma el incremento.

5.1.2 Evolución de RIP

El origen de RIP se remonta a los primeros encaminamientos realizados por distancia vectorial en la red ARPANET en los años 60. Luego, hay otros antecedentes importantes con un desarrollo para BSD Unix. En 1988, a través de la RFC 058 se estandariza la versión 1 de RIP, y luego evoluciona con mejoras sucesivas, en los años 1993 y

1998, a la versión 2, a través de los estándares fijados en las RFC 1388 y 2453.

En la Figura 5.2 se presenta el formato estandarizado de un paquete RIP. Los campos más importantes son el tipo de comando, la versión, la dirección de red y la métrica para dicha dirección.

RIP versión 1 presenta una serie de limitaciones: los destinos con una métrica mayor que 15 son inalcanzables. De cualquier forma, si se permitiera una métrica mayor, la convergencia se volvería muy lenta.

Una métrica tan simple origina tablas de encaminamiento sub-optimizadas. Los paquetes podrían enviarse sobre los enlaces más lentos.

Otro problema es que se aceptan actualizaciones RIP de cualquier dispositivo. Si éste está mal configurado, puede originar el mal funcionamiento de toda la red.

Fig. 5.2. Formato estandarizado de un paquete RIP.

Además, otras limitaciones de RIP versión 1 son las siguientes: no envía información de máscara de subred en sus actualizaciones, envía actualizaciones a los otros encaminadores como paquetes de difusión a 255.255.255.255, y no soporta autenticación ni VLSM y CIDR.

Las limitaciones fueron resueltas por RIP versión 2 que mejora los siguientes aspectos: envía información de máscara de subred en sus actualizaciones, por lo que soporta VLSM y CIDR; envía actualizaciones como multidifusión a la

dirección 224.0.0.9, lo que reduce procesamiento a los hosts que no corren RIP; soporta autenticación en texto plano y encriptado, y usa etiquetas de rutas externas, lo que permite identificar rutas aprendidas por RIP o de otro protocolo.

5.2 Protocolo OSPF

5.2.1 Conceptos fundamentales en OSPF

La otra alternativa que analizaremos como protocolo IRP es OSPF. Ya hemos visto que RIP es limitado para funcionar en grandes redes, mientras que se prefiere OSPF como IRP para interredes basadas en TCP/IP. Usa enrutamiento de estado de enlace, soporta *Classless* (VLSM y CIDR), introduce el concepto de áreas para obtener escalabilidad, y tiene como métrica un valor arbitrario llamado costo según la RFC 2328.

El IETF OSPF Working Group comenzó a desarrollarlo en 1987, y en 1989 se publicó su primera versión en la RFC 1131. Posteriormente, en 1991, se introdujo la segunda versión en la RFC 1247. IETF eligió OSPF como IRP recomendado. Y en 1998 se actualizó la segunda versión con la RFC 2328.

Cuando se inicializa, el encaminador determina el costo de enlace en cada interfaz, y anuncia estos costos a los otros encaminadores en la topología. Luego, el encaminador monitorea sus costos de enlace, y si hay cambios, los nuevos costos se re-anuncian. Con la información que recibe cada

encaminador, construye su topología y calcula el camino más corto a cada red destino.

OSPF no necesita una versión distribuida del algoritmo de encaminamiento, ya que el encaminador tiene la topología completa de la red. Para su funcionamiento se puede utilizar cualquier algoritmo, aunque en la práctica se usa Dijkstra, también llamado SPF (Primero el Paso más Corto).

Una forma sencilla de iniciar el algoritmo es por inundación. En este caso se envían paquetes del encaminador origen a cada vecino. Los paquetes entrantes se reenvían a todos los enlaces salientes excepto al enlace origen. Los paquetes duplicados ya transmitidos se descartan, previniendo la retransmisión permanente, como se observa en la Figura 5.3.

Con esta técnica se examinan todas las rutas posibles entre origen y destino, de modo que un paquete siempre llega a destino. La técnica de inundación es altamente robusta. De esta forma, al menos un paquete sigue la ruta de menor retardo, la información inundada llega muy pronto a todos los encaminadores, y se recorren todos los nodos que están directa o indirectamente conectados a un nodo origen. Todos los encaminadores obtienen la información necesaria para construir su tabla de encaminamiento. La principal desventaja es la carga elevada de tráfico.

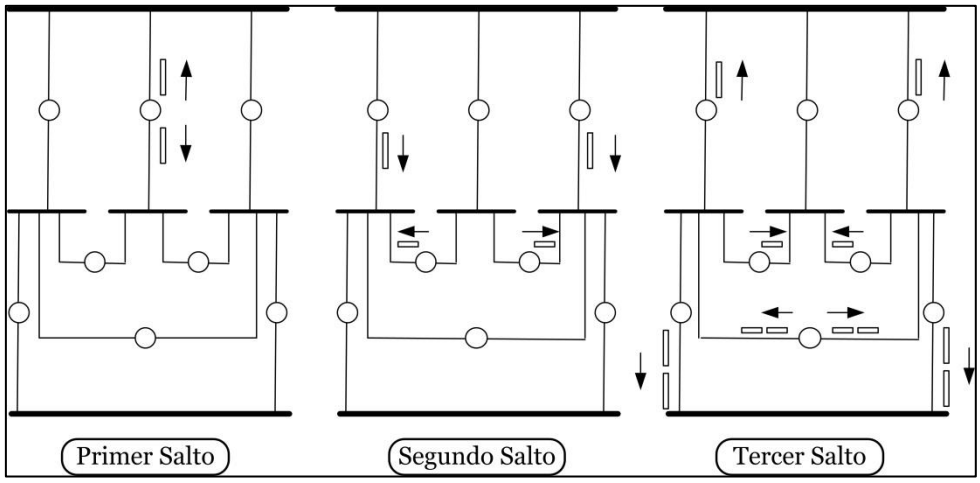


Fig. 5.3. Algoritmo de inundación.

Con OSPF, cada encaminador mantiene descripciones del estado de sus enlaces locales, y transmite actualizaciones de su información de estado a todos los encaminadores que conoce. Los encaminadores que reciben las actualizaciones de otros encaminadores deben confirmarlas. De esta forma, se genera un tráfico moderado dentro de la red. Cada encaminador mantiene su base de datos que refleja la topología de la red, que puede representarse como un grafo dirigido. La Figura 5.4 muestra un ejemplo de un grafo que representa la topología de la red a partir de la base de datos del encaminador. En este gráfico los vértices serían los encaminadores R o las redes N, sean de tránsito o *Stub*. Las aristas conectan dos encaminadores o un encaminador con una red.

El costo de salto en cada dirección se llama métrica de encaminamiento. OSPF provee un esquema de métricas flexibles basadas en el tipo de servicio (TOS) (que se

encuentra en la cabecera de IPv4). El servicio normal tiene TOS 0, y es el valor predeterminado si no se aclara lo contrario. Para minimizar el costo monetario se usa TOS 2, para maximizar la fiabilidad TOS 4, para maximizar el rendimiento real TOS 8, y para minimizar retardos TOS 15. Cada encaminador puede generar 5 árboles *spanning-trees* y 5 tablas de encaminamiento correspondientes.

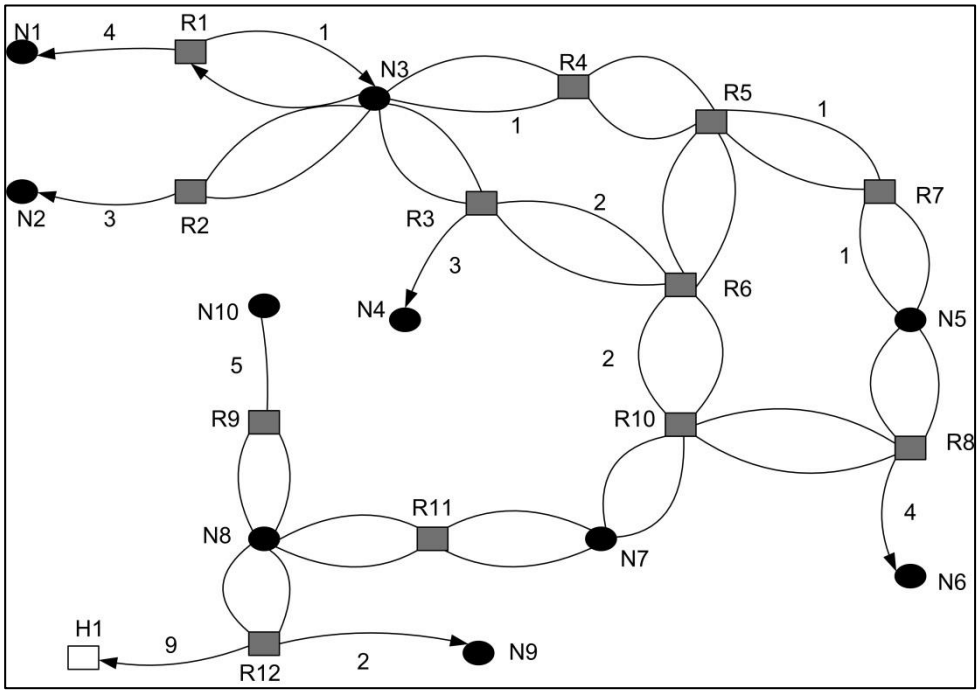


Fig. 5.4. Ejemplo de un grafo dirigido
que muestra la topología de la red.

5.2.2 Paquetes OSPF

En el ruteo OSPF se usan paquetes denominados LSU (actualizaciones de estado de enlace), y 11 tipos diferentes de LSAs (avisos de estado de enlace). Los paquetes LSU y LSA se usan indistintamente. OSFP usa el algoritmo de Dijkstra como se indica en la Figura 5.5.

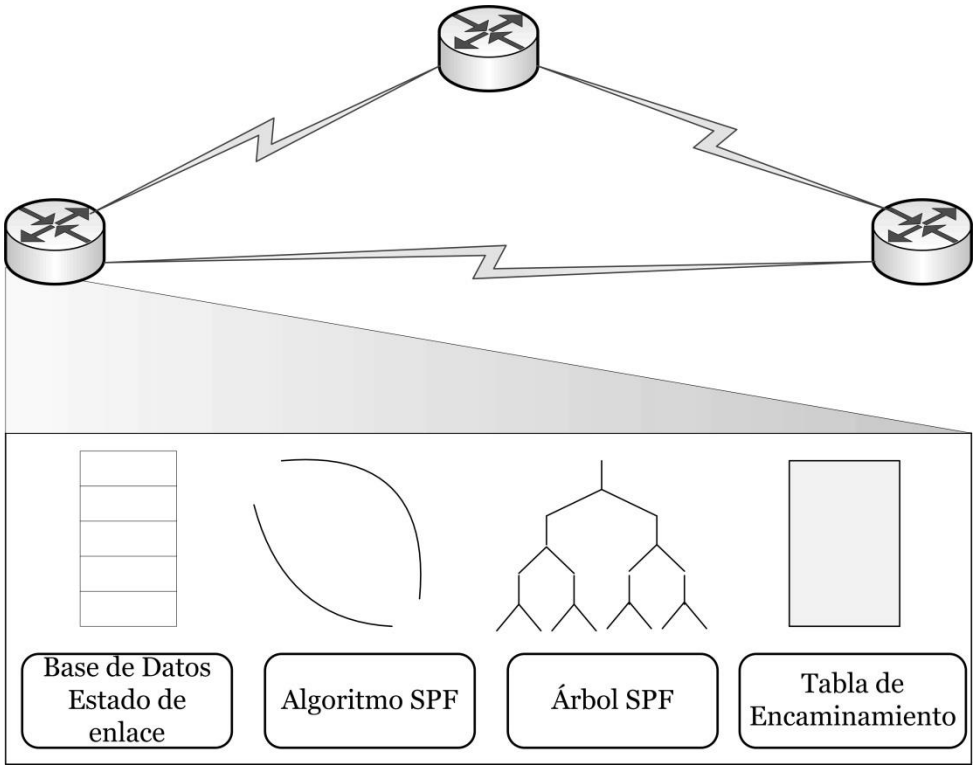


Fig. 5.5. Uso del Algoritmo de Dijkstra de OSFP.

El paquete OSPF tiene una cabecera de 24 bytes. Los campos, presentados en la Figura 5.6, se utilizan para indicar el número de versión, uno de los tipos posibles de paquetes, la longitud del paquete en bytes incluyendo la cabecera, una identificación de encaminador origen, una

identificación del área a la cual pertenece el encaminador origen, una campo de verificación de error, y el tipo y datos para la autenticación.

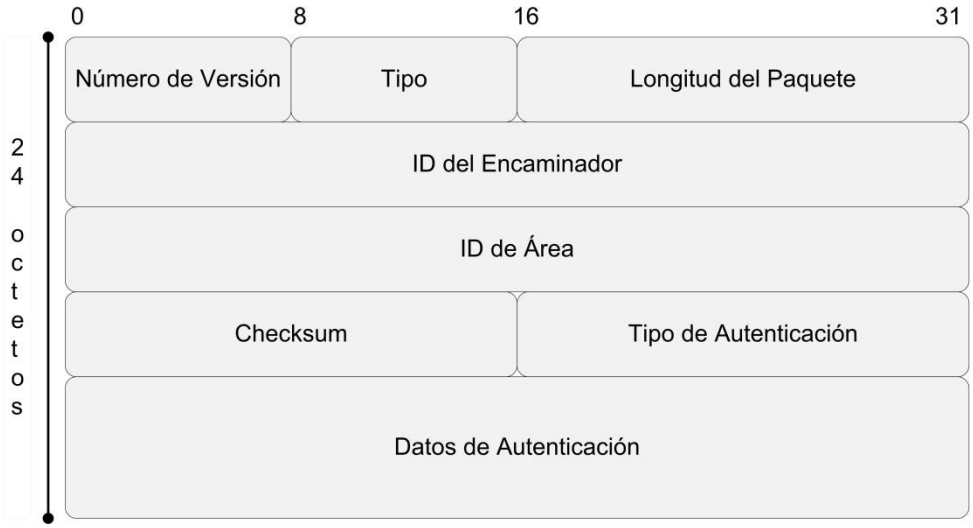


Fig. 5.6. Formato estandarizado de un paquete OSPF.

Los paquetes en OSPF pueden clasificarse en:

- *Hello*: usado en la búsqueda de los vecinos,
- *Database description* (DBD): define la información del conjunto de estado de enlace, y que está presente en la base de datos de cada encaminador,
- *Link state request* (LSR): para la petición total o parcial del estado de enlace a un vecino,
- *Link state update* (LSU): para las actualizaciones de estado de enlace a los vecinos,
- *Link state acknowledgement* (LSA): para confirmar la llegada de una actualización fiable.

En la Figura 5.7 se presenta el encapsulamiento de un paquete OSPF dentro de un paquete IP, que a su vez se encuentra encapsulado dentro de una trama. En la cabecera IP se observa el valor 89 de OSPF en el campo de protocolo, la dirección destino que es típicamente una dirección multidifusión 224.0.0.5 o 224.0.0.6. En la cabecera de Capa 2 también se usan direcciones multidifusión 01-00-5E-00-00-05 o 01-00-5E-00-00-06.

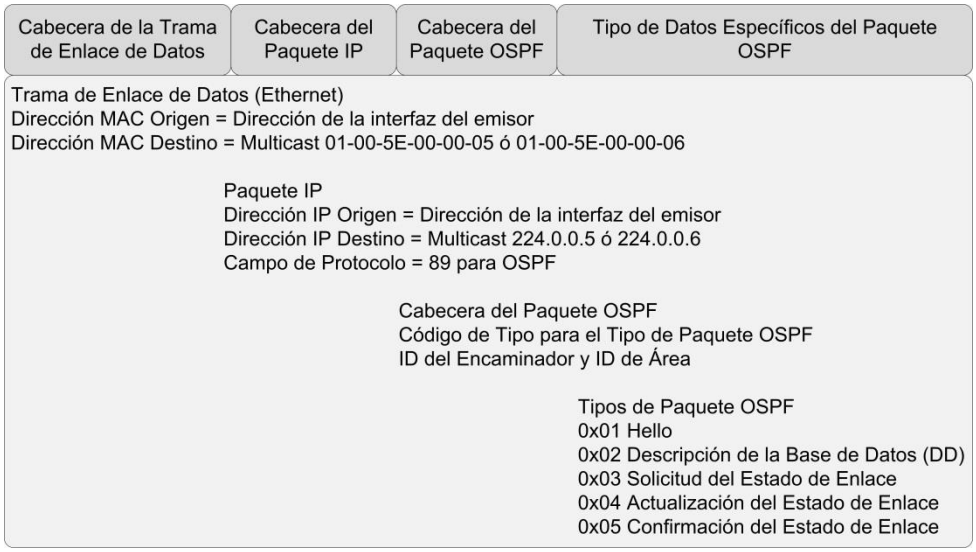


Fig. 5.7. Encapsulamiento de un paquete OSPF.

Y en la Figura 5.8 se observa el interior de un paquete OSPF del tipo *Hello*. Su utiliza para descubrir vecinos OSPF, estableciendo adyacencias con intercambio de parámetros, como por ejemplo: Intervalo *Hello*, Intervalo Muerto, Tipo de red, etc. Además, se lo utiliza para elegir encaminadores especiales llamados Encaminador Designado (DR) y Encaminador Designado Backup (BDR) en redes multiacceso del tipo Ethernet y Frame Relay.

Antes que un encaminador OSPF inunde sus estados de enlace, debe descubrir o establecer sus vecinos. Luego de que han sido descubiertos los encaminadores vecinos, debe formar adyacencia con tres parámetros: el Intervalo *Hello* de 10 a 30 segundos, el Intervalo Muerto para espera de un *Hello* antes de dar de baja al vecino, el tipo de red punto a punto o multiacceso, etc. Ambas interfaces de los vecinos deben ser parte de la misma red, incluyendo la misma máscara de subred.

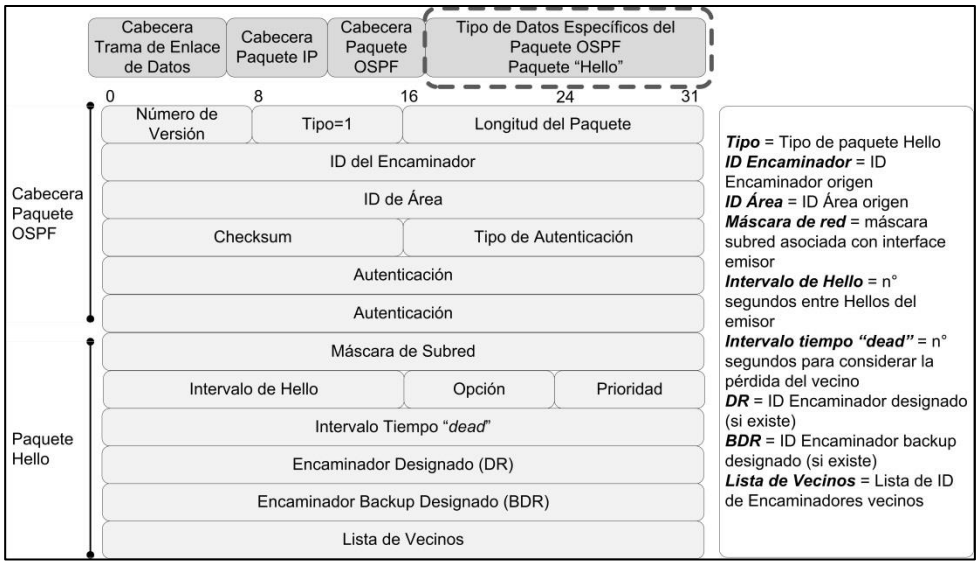


Fig. 5.8. Interior de un paquete OSPF del tipo *Hello*.

5.2.3 Tipos de Encaminadores en OSPF

A esta altura es necesario definir o clasificar los tipos de redes en cuanto a su acceso. Definimos una red multiacceso como aquella red con más de dos dispositivos en el mismo medio compartido, como por ejemplo las redes Ethernet, Token Ring y Frame Relay. Y una red punto a punto como una red con sólo dos dispositivos.

OSPF define 5 tipos de redes: Punto a Punto, Multiacceso de Difusión, Multiacceso sin Difusión, Punto a Multipunto y Enlaces Virtuales. Las redes multiaccesso pueden originar dos dificultades para OSPF debido a la inundación de LSAs. Por un lado, la creación de adyacencias múltiples, con una adyacencia por cada par de encaminadores, y una inundación numerosa de LSAs. La creación de una adyacencia entre cada par de encaminadores en una red originaría un número innecesario de adyacencias. Esto daría como resultado un número excesivo de LSAs circulando entre encaminadores sobre la misma red. El número de adyacencias crecería exponencialmente.

Los encaminadores de estado de enlace inundan sus paquetes de estado de enlace cuando OSPF se inicializa o cuando hay un cambio en la topología. En una red multiacceso, como en la Figura 5.9, esta inundación puede convertirse en excesiva. La solución para administrar el número de adyacencias y la inundación de LSAs sobre una red multiacceso es el uso de un Encaminador Designado (DR). En las redes multiaceso, OSPF elige un encaminador designado para la colección y distribución de LSAs enviados y

recibidos. También se elige un encaminador designado backup (BDR) para el caso en que el DR falle. A los demás encaminadores se les llama Otros DR. Éstos sólo forman adyacencia con DR y BDR, y envían sus LSAs al DR y BDR usando las direcciones multifidifusión 224.0.0.6.

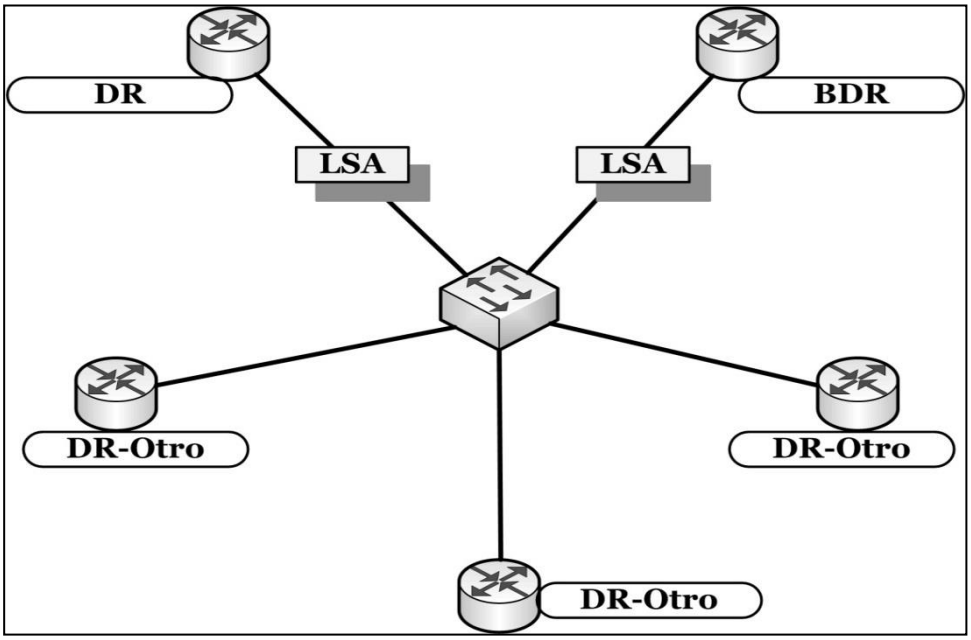


Fig. 5.9. Inundación de paquetes OSFP en una red multiacceso.

5.2.4 Concepto de Área OSPF

Cuando los sistemas autónomos son grandes por sí mismos y nada sencillos de administrar, OSPF permite dividirlos en áreas numeradas, donde un área es una red o un conjunto de redes inmediatas, como se observa en la Figura 5.10.

Un área es una generalización de una subred. Fuera de un área, su topología y detalle no son visibles. OSPF distingue el Área Troncal, también denominada Área 0 (Cero), que forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red.

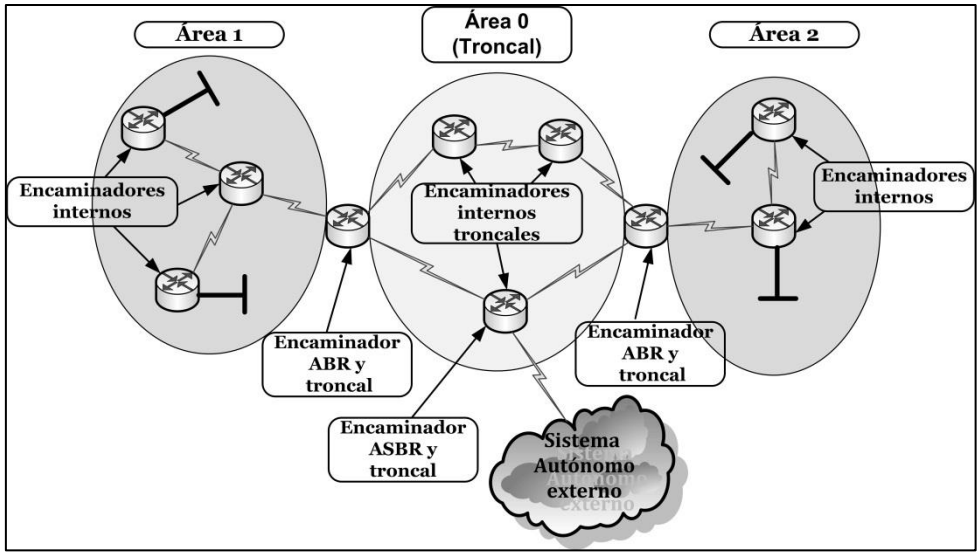


Fig. 5.10. División de un sistema autónomo en áreas.

Con el concepto de área se logra que cada una de ellas corra una copia separada del algoritmo de estado de enlace. De esta forma, cada área administra su base de datos topológica y su grafo; y la información de estado de enlace se difunde sólo a los encaminadores de esa área. Además, se reduce el tráfico de datos, dado que si el origen y destino de un paquete IP están en la misma área, sólo se necesita

encaminamiento intra-área, y la información de encaminamiento depende solo del estado de enlace de esa área

El encaminamiento inter-área establece un camino formado por tres pasos: 1) uno dentro del área origen del tipo intra-área; 2) otro a través del troncal que tiene propiedades de un área y usa el algoritmo de encaminamiento de estado de enlace para ruteo inter-área; 3) y finalmente, dentro del área destino que también es del tipo intra-área. En un nivel superior, OSPF ve el conjunto de redes como una estrella, donde la raíz es el troncal y cada área está unida a éste.

Un encaminador OSPF interno es capaz de encaminar cualquier paquete destinado a cualquier punto del área en el que se encuentra (encaminamiento intra-área). Para el encaminamiento entre distintas áreas del AS (encaminamiento inter-área) y desde el AS hacia el exterior (encaminamiento exterior), OSPF utiliza encaminadores especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse: los encaminadores ABR (*Area Border Router* – Encaminadores de Borde de Área), que mantienen la información topológica de su área y conectan ésta con el resto de las áreas, permitiendo encaminar paquetes a cualquier punto de la red. Y los encaminadores ASBRs (*Autonomous System Border Router* – Encaminadores de Borde de Sistema Autónomo), que permiten encaminar paquetes fuera del sistema autónomo en que se alojan, es decir, a otras redes conectadas al Sistema Autónomo o al

resto de Internet. La Figura 5.11 presenta un ejemplo de aplicación.

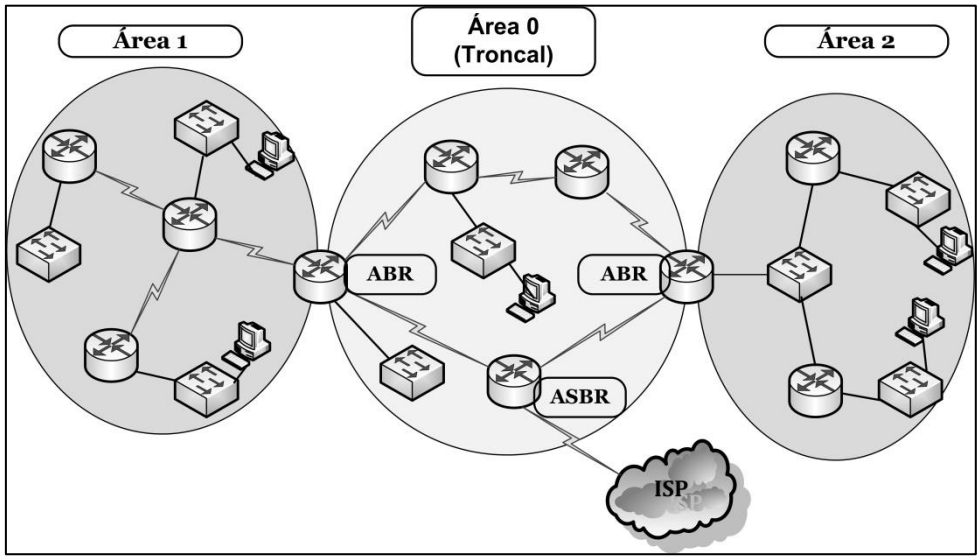


Fig. 5.11. Aplicación con los diferentes tipos de encaminadores OSPF.

5.3 Protocolo BGP

5.3.1 Introducción

Internet es un conjunto descentralizado de redes de comunicación interconectadas que emplea la familia de protocolos TCP/IP para garantizar que las redes físicas que la componen funcionen como una red lógica única, accesible desde cualquier parte del mundo. Para conseguir esto, Internet emplea los llamados ISPs (*Internet Service Providers*).

Estos ISPs se estructuran atendiendo a una jerarquía basada en tres grandes niveles: ISPs de nivel 1 (Troncal), ISPs de nivel 2 (Regionales y Nacionales) e ISPs locales. La Figura 5.12 presenta un esquema que aproxima la estructura de los ISPs.

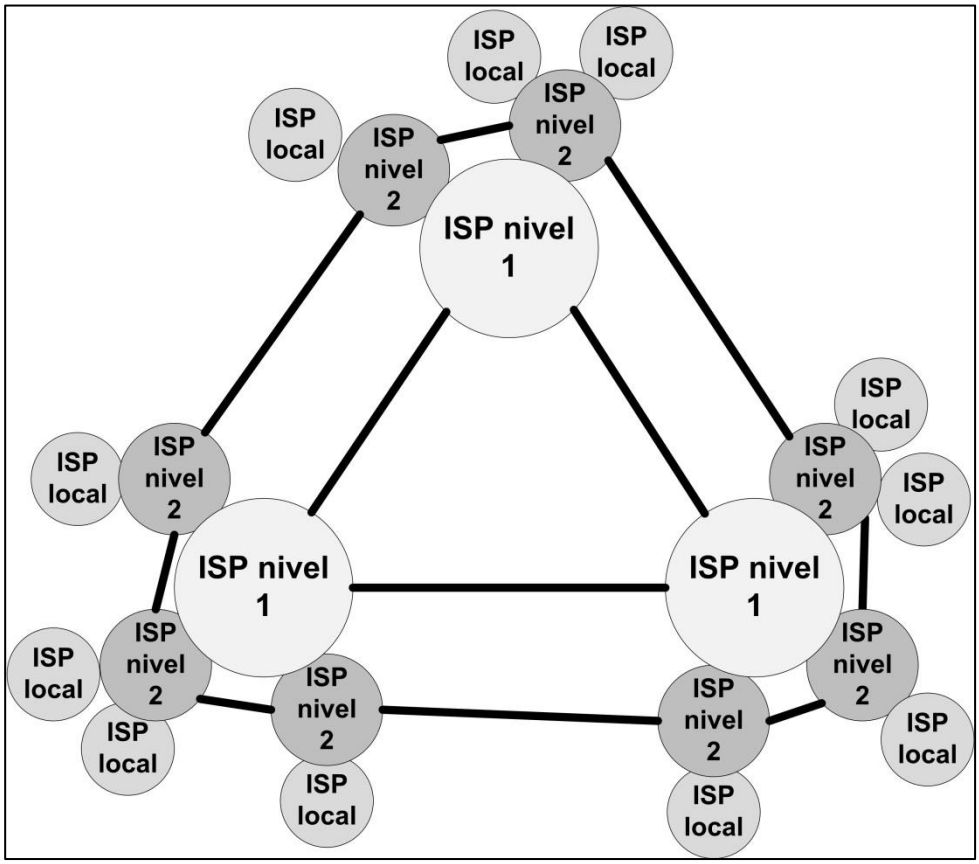


Fig. 5.12. Esquema aproximado de la organización de los ISPs.

Los ISPs de nivel 1 se encuentran en el extremo más alto de la jerarquía y a nivel mundial son relativamente pocos. Su funcionamiento es el mismo que el de cualquier

red; tiene enlaces y encaminadores, pero éstos deben soportar una cantidad de datos de transmisión muy elevada al mismo tiempo. Los ISPs de nivel 1 están conectados entre sí y su cobertura es internacional. Son la columna vertebral de Internet.

Los ISPs de nivel 2 funcionan por debajo del troncal y están necesariamente conectados a éste. Abarcan territorios regionales y nacionales, y están también interconectados entre sí, para evitar una sobrecarga de los ISPs de nivel 1. Finalmente, los ISPs de nivel local son nuestro primer acceso a Internet, por ejemplo, desde nuestra casa. Se encuentran en el punto más bajo de la jerarquía y son los más abundantes. Generalmente, no están conectados entre sí.

Un Sistema Autónomo (AS), como ya vimos en las secciones precedentes, se define como un grupo de redes IP que poseen una política de rutas propia e independiente, que hace su particular gestión del tráfico, el cual fluye entre él y los restantes Sistemas Autónomos que forman Internet. Originalmente se asignaba un número de Sistema Autónomo de 16 bits que identificaba de manera única a sus redes dentro de Internet. En la Figura 5.13 se observa un ejemplo.

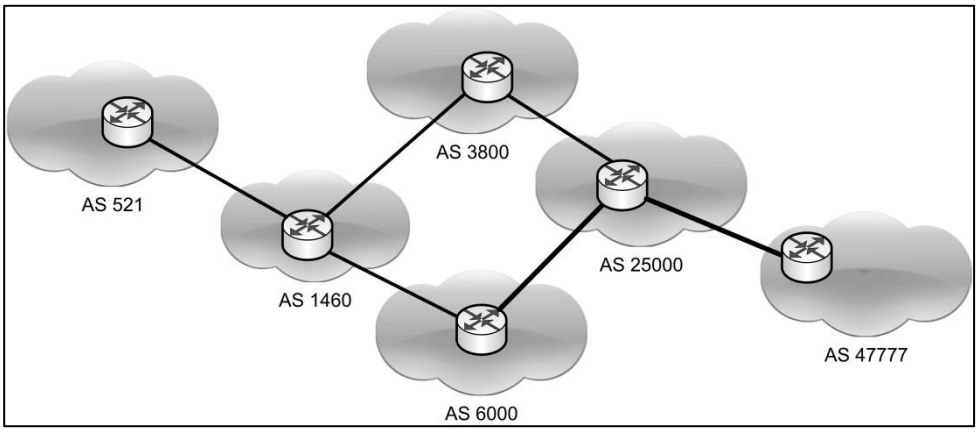


Fig. 5.13. Ejemplo de la conexión de distintos Sistemas Autónomos.

Puede plantearse que la propagación de las rutas de Internet se realiza usando una jerarquía de protocolos de encaminamiento de 2 niveles: un protocolo de encaminamiento interior (IRP) que selecciona cada sistema autónomo, y un protocolo de encaminamiento exterior (ERP) que se usa entre sistemas autónomos de Internet. La información de las rutas se propaga en varios niveles: los *hosts* conocen el encaminador local, los encaminadores locales conocen los encaminadores regionales, los encaminadores regionales conocen los encaminadores de núcleo y los encaminadores de núcleo conocen "todo".

Entonces, podemos presentar una nueva definición de sistema autónomo planteada desde el encaminamiento. Un sistema autónomo es un dominio de enrutamiento autónomo al que se le ha asignado un Número de Sistema Autónomo (ASN).

Un sistema autónomo está definido con precisión en la RFC 1771, indicando que es: un conjunto de encaminadores bajo una única administración técnica, que usa un IRP y métricas para encaminar los paquetes dentro del sistema autónomo, y un ERP para encaminar los paquetes a otros sistemas autónomos.

El número de AS original tenía un campo de 16 bits. Más recientemente se han implementado los ASNs de 32 bits que proveen 2^{32} o 4.294.967296 números de ASs. Estos números incluyen todos los ASNs de 16 bits, desde el 0 al 65535. Esto ayuda en la interoperabilidad de los ASs que usan ASNs de 32 bits con los que usan ASNs de 16 bits.

Y como sucede con las direcciones IP públicas, se obtiene un ASN público de su ISP o directamente del RIR (*Regional Internet Register* – Registro Regional de Internet) correspondiente. Y como con las direcciones IP privadas, los ASNs privados no se publican en Internet.

Los RIRs son organizaciones que supervisan la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo. Los recursos incluyen direcciones IP (tanto IPv4 como IPv6) y números de sistemas autónomos para su uso en encaminamiento BGP.

Hay actualmente 5 RIRs en funcionamiento: el *American Registry for Internet Numbers* (ARIN) para América Anglosajona; el *RIPE Network Coordination Centre* (RIPE NCC) para Europa, el Oriente Medio y Asia Central; el *Asia-Pacific Network Information Centre* (APNIC) para Asia y la

Región Pacífica; el *Latin American and Caribbean Internet Address Registry* (LACNIC) para América Latina y el Caribe; y el *African Network Information Centre* (AfriNIC) para África, tal como se presenta en la Figura 5.14.

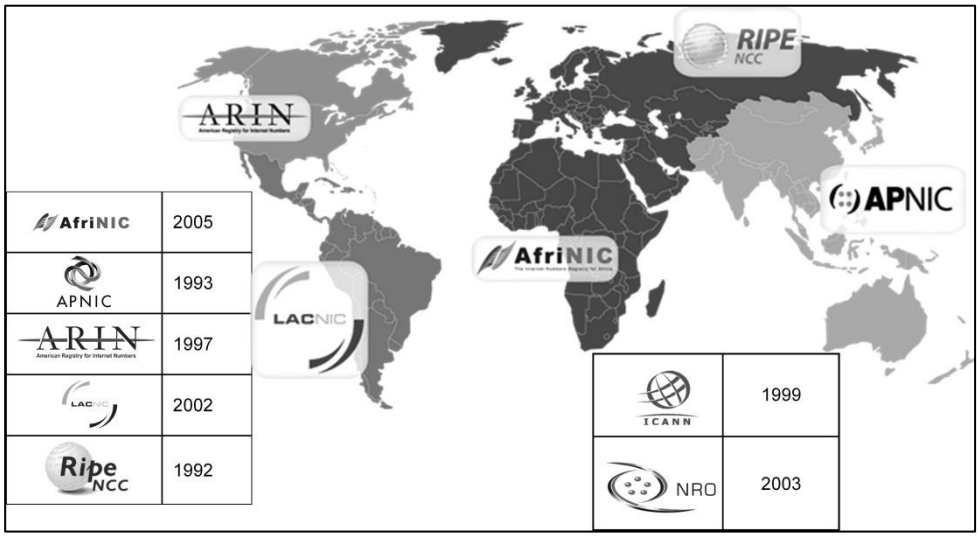


Fig. 5.14. Distribución de los Registros Regionales de Internet RIR.

La función de los RIRs es el manejo neutral y efectivo de las direcciones y números de Internet para asegurar la distribución justa e igualitaria, así como para prevenir el acaparamiento. A su vez los RIRs siguen sus políticas regionales para una posterior subdelegación de recursos a los ISPs y otras organizaciones. Colectivamente, los RIRs participan en la NRO (*Number Resource Organization* – Organización de Números de Recursos) formada como una entidad para representar sus intereses colectivos, llevar a cabo actividades conjuntas y coordinar las actividades de los RIRs globalmente. En las Figuras 5.15 y 5.16 se muestran

las asignaciones de los números de AS de 16 bits por parte de los RIRs a sus clientes a junio de 2015, y en el rango de años 1999 a 2015.

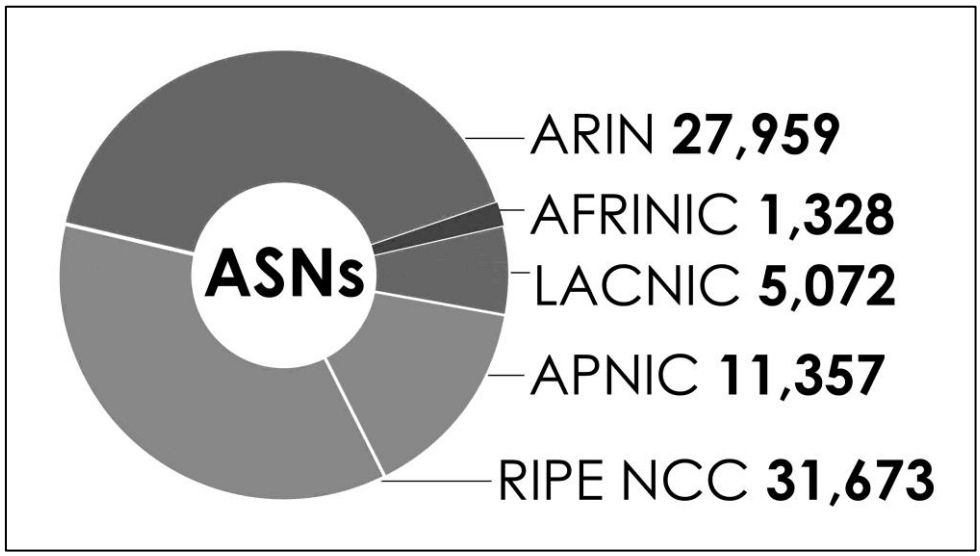


Fig. 5.15. Distribución de asignación de números de AS de 16 bits (junio de 2015).

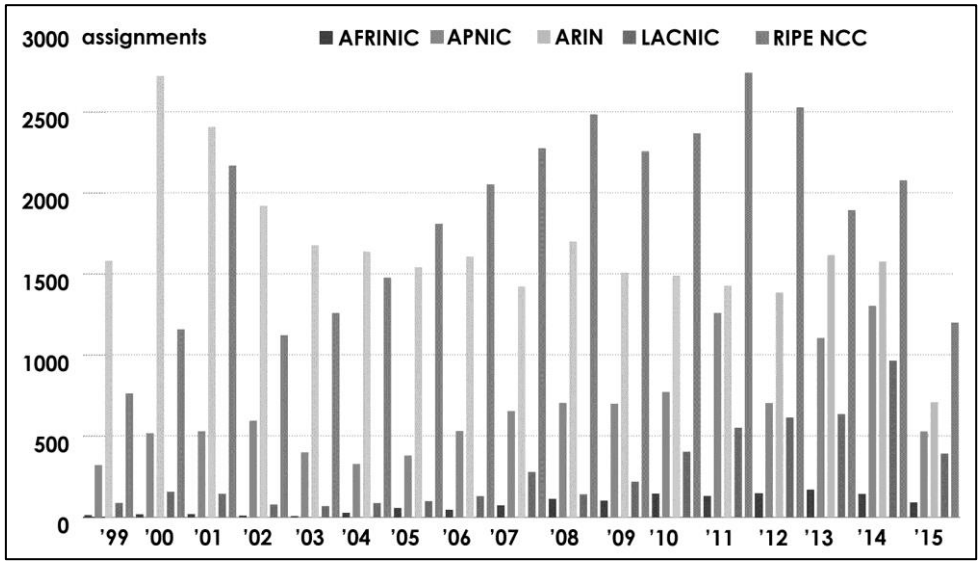


Fig. 5.16. Distribución de asignación de números de AS de 16 bits 1999-2015.

En las Figuras 5.17 y 5.18 se muestran las asignaciones de los números de AS de 32 bits por parte de los RIRs a sus clientes a junio de 2015, y en el rango de años 1999 a 2015.

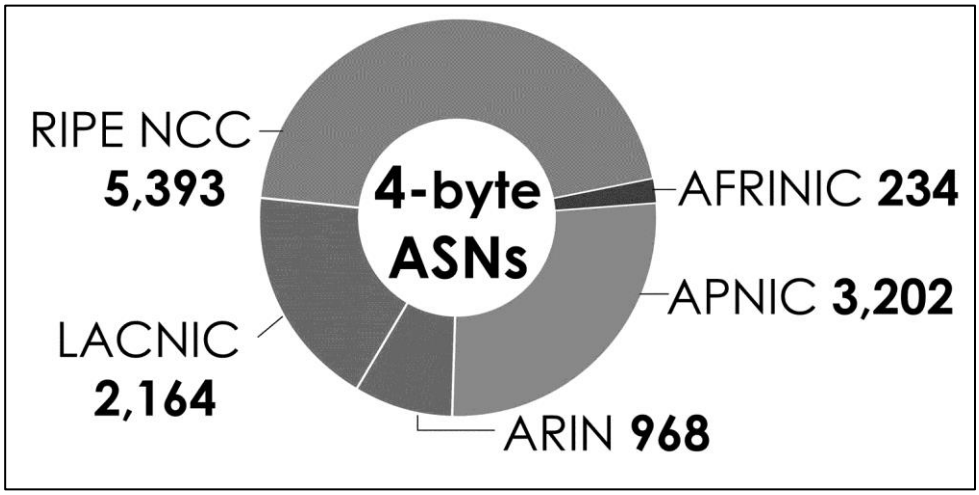


Fig. 5.17. Distribución de asignación de números de AS de 32 bits (junio de 2015).

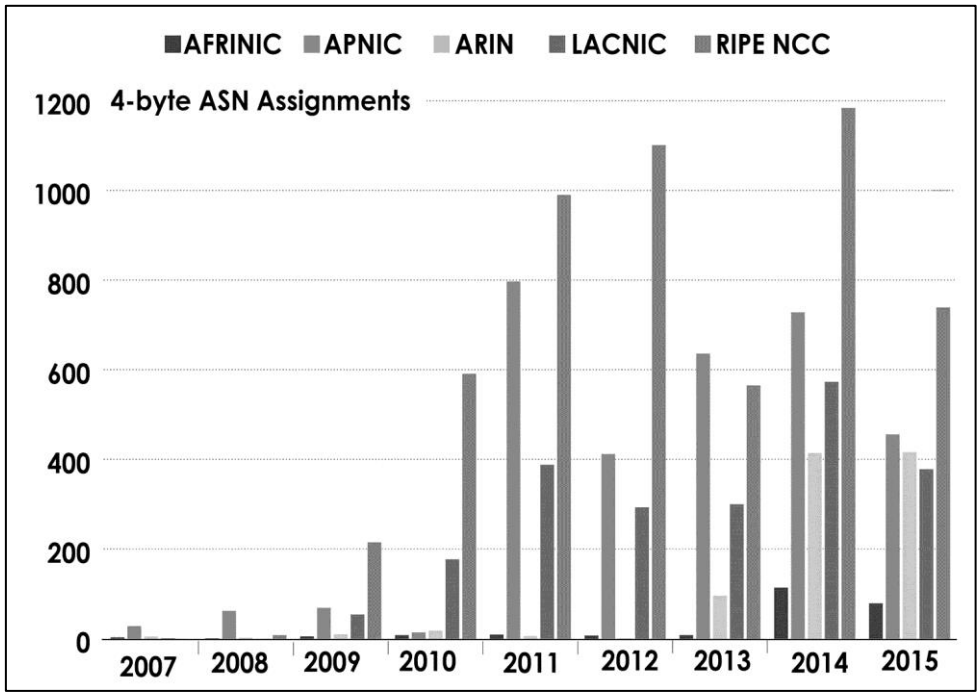


Fig. 5.18. Distribución de asignación de números de AS de 32 bits (1999-2015).

Los sistemas autónomos se pueden clasificar por el número de conexiones a ISPs en:

- *Single-homed AS*: cuando existe una sola salida al ISP. En este caso no se requiere un ERP, aunque puede ser deseable. El sistema autónomo tendrá una ruta predeterminada al ISP, mientras que éste configurará rutas estáticas a las redes internas de aquél.
- *Multi-homed AS*: cuando tiene múltiples salidas a ISP(s). A su vez, se pueden clasificar en *Non-transit ASs* cuando no permiten tráfico de la conexión de un ISP a la conexión de otro ISP, que es usado habitualmente para un AS corporativo. Y en *Transit ASs* cuando permite que el tráfico sea encaminado desde un AS

externo, a través del AS local, a otro AS. Los ISPs son *ASs multi-homed transit*. El encaminamiento del tráfico de tránsito lo hacen encaminadores configurados como encaminadores IBGP (BGP interno), también llamados encaminadores de tránsito.

5.3.2 Conceptos fundamentales en BGP

EGP fue el protocolo de ruteo estándar original de Internet a comienzo de los ’80. Se lo diseñó para Internet con una estructura árbol y con un simple troncal. Su objetivo era la posibilidad de acceso, no la búsqueda de rutas óptimas. Los mensajes de protocolo básicos eran:

- Adquisición vecino (*neighbor acquisition*): cuando un encaminador intercambia información de posibilidad de acceso con su par,
- Accesibilidad vecino (*neighbor reachability*): un encaminador verifica periódicamente si el otro encaminador es todavía su vecino mediante el intercambio de mensajes *Hello/Ack*,
- Actualización de encaminamiento (*routing update*): los pares intercambian periódicamente sus tablas de encaminamiento usando un método básico de vector distancia

EGP presentó rápidamente algunos problemas operativos. EGP es un protocolo vector distancia básico, donde las actualizaciones envían listas de destinos y distancias, pero las distancias no son confiables. Como se indicó previamente, EGP fue diseñado para topologías tipo

árbol, no mallas. Las falsas rutas inyectadas a la red por error ocasionan graves problemas. Además, en ese contexto los lazos son difíciles de evitar. EGP no fue diseñado para transportar paquetes IP fragmentados – todos los datos están en la MTU. Las soluciones a estos problemas fueron parciales y no alcanzaron los resultados esperados, hasta la aparición de BGP.

El protocolo BGP (*Border Gateway Protocol* – Protocolo de Puerta de Enlace de Borde) es un protocolo de encaminamiento basado en política, del tipo vector-paso. Es el EGP de facto para Internet. Reconocido como un protocolo relativamente simple, pero también de configuración compleja, que requiere conocimiento especializado. Los errores de configuración repercuten en todo Internet. Se trata de un protocolo altamente escalable, de encaminamiento entre dominios, usado por las redes corporativas que se conectan a sus ISPs, y también por los ISPs para conectarse con otros ISPs. Se puede usar también dentro de un AS como IRP.

Debido a su importancia, el protocolo BGP requirió sucesivos ajustes después que se publicara el estándar original. Sus desarrolladores tuvieron no sólo que corregir problemas, sino además, efectuar ajustes debido a otros cambios introducidos en el conjunto de protocolos TCP/IP, como la invención del direccionamiento *classless*.

Como una secuencia, BGP ha evolucionado a través de algunas versiones. Con la RFC 1105, en 1989, se introdujo la definición inicial del protocolo BGP, conocida como BGP-1.

En 1990, a través de la RFC 1163 se estandarizó BGP-2, efectuando algunos ajustes sobre el significado y uso de algunos de los tipos de mensajes, y la introducción del concepto de paso. Luego, en 1991, se presentó BGP-3 a través de la RFC 1267, cuya versión optimizó y simplificó el intercambio de información de encaminamiento. En 1994, con la RFC 1654 se introdujo la versión conocida como BGP-4. La misma fue ratificada y mejorada con la RFC 1771 del año 1995. Se trata del estándar corriente, que introdujo como ajuste principal el soporte para CIDR. Luego, se efectuaron otros ajustes como los dados en la RFC 1772.

La Figura 5.19 muestra un ejemplo del uso de BGP. Como sabemos los IRPs operan dentro de un sistema autónomo, mientras que BGP se usa entre sistemas autónomos. De esta forma se garantiza una información de encaminamiento libre de bucles. No se muestran detalles de las topologías dentro de cada sistema autónomo.

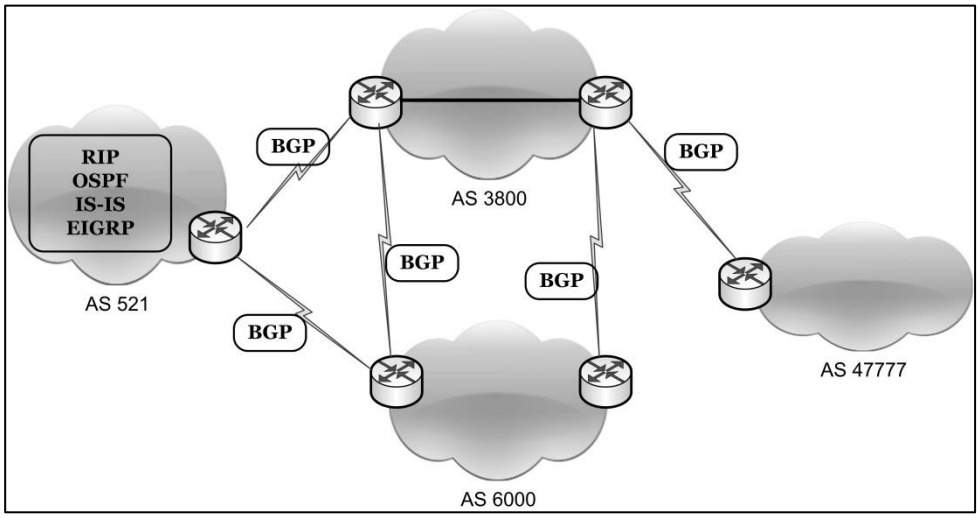


Fig. 5.19. Ejemplo de uso de BGP.

5.3.3 Operación BGP

Mientras que los IRPs anuncian las redes y describen las métricas para alcanzar esas redes, BGP anuncia pasos y las redes que son alcanzables al final del paso. Para ello, BGP usa una lista de números de sistemas autónomos, a través de los cuales debe pasar un paquete para llegar a su destino, y describe el paso usando atributos, que son similares a las métricas. Además, BGP permite que los administradores definan políticas o reglas sobre cómo deben transmitirse los datos a través de los ASs.

Para garantizar una elección de camino libre de lazos, BGP construye un grafo de sistemas autónomos basado en la información intercambiada entre vecinos BGP. BGP ve toda la red como un grafo o árbol de sistemas autónomos.

La conexión entre dos sistemas autónomos cualesquiera forma un camino. En este contexto, se define como camino o paso (*path)* de sistema autónomo a la colección de información de caminos expresada como una secuencia de números de AS. Esta secuencia forma una ruta a cada destino específico.

La lista de números de sistemas autónomos asociados con una ruta BGP es uno de los atributos asociados con esa ruta. Se elige el camino inter-sistema autónomo más corto, que está simplemente determinado por la menor cantidad de números de sistemas autónomos. En la Figura 5.20, el sistema autónomo 7 usará el camino más corto (4,2,1) para comunicarse con el sistema autónomo 1.

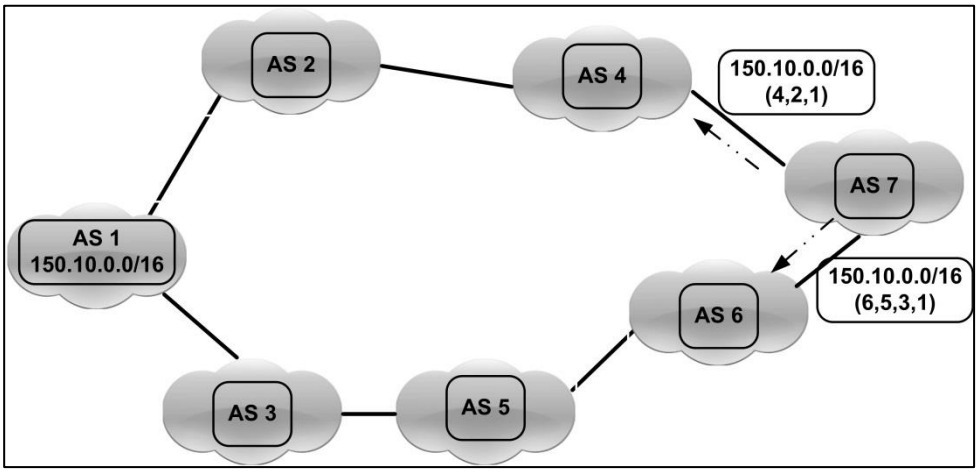


Fig. 5.20. Comunicación entre el sistema autónomo 7 y el 1.

Los lazos de encaminamiento son fácilmente detectados cuando un encaminador recibe una actualización que contiene su propio número de sistema autónomo local en el atributo AS_PATH. Cuando ocurre esto, el encaminador no debe aceptar la actualización, evitando así el lazo posible.

En su funcionamiento básico BGP usa una conexión TCP para establecer las relaciones de vecinos con otros encaminadores BGP y transmitir todo el tráfico BGP. Dado que se requiere TCP, la única pila de protocolo permitida en Internet es TCP/IP. El tráfico de otras pilas (por ejemplo IPX/SPX) deberían traducirse en tráfico TCP/IP en el encaminador de borde antes de propagarse en Internet. Para establecer la conexión BGP usa el puerto TCP 179. La Figura 5.21 muestra cómo se vería una trama que contiene un paquete BGP.

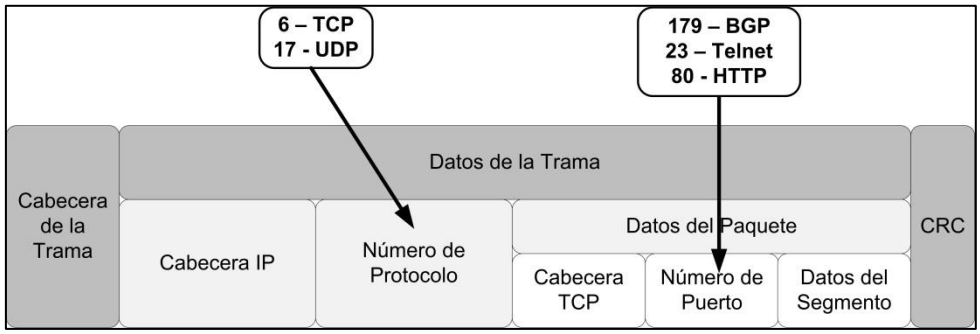


Fig. 5.21. Trama conteniendo un paquete BGP.

Cuando dos encaminadores establecen una conexión BGP habilitada por TCP, se llaman vecinos o pares (*neighbors o peers*). Cada encaminador que corre BGP es un participante o locutor BGP (BGP *speaker*). Los encaminadores vecinos intercambian múltiples mensajes para abrir y confirmar los parámetros de conexión, como por ejemplo la versión de BGP. Si no hay correspondencia entre los vecinos, se notifican los errores y la conexión falla.

Cuando los vecinos BGP confirman la conexión, intercambian todas las rutas BGP candidatas. Después de ese intercambio inicial, las actualizaciones parciales (o incrementales) se envían cuando se producen cambios en la red. Las actualizaciones parciales son más eficientes que las tablas completas. Este es un tema muy importante en los encaminadores EBGP (BGP externo), los cuales pueden contener tablas de encaminamiento muy grandes (más de 300.000 rutas en internet).

Los clientes, en general, no necesitan BGP. El encaminamiento estático es lo que más frecuentemente se

usa para comunicar un cliente con su proveedor de Internet. Sin embargo, hay una diversidad de situaciones que se pueden plantear en casos muchos más generales.

En la Figura 5.22 se presentan cuatro ejemplos distintos:

- Caso A: se presenta un sistema autónomo *single-homed*, donde normalmente no necesita BGP dado que se usa una ruta predeterminada.
- Caso B: aún si un sistema autónomo tiene pasos redundantes a su ISP, no necesariamente se requiere BGP. Aunque se puede usar para implementar políticas de encaminamiento externo.
- Caso C: aún si un sistema autónomo tiene pasos redundantes a su ISP, pero diferentes POPs (puntos de acceso), no se requiere necesariamente BGP, aunque se lo puede usar para implementar políticas de ruteo externo.
- Caso D: Un sistema autónomo con múltiples ISPs requiere BGP. La precaución es que el sistema autónomo no sea de tránsito.

Los sistemas autónomos *single-homed* tienen un enlace con un ISP, con sólo un punto de salida a redes externas. En estos casos, a las redes se las llama redes *stubs*. Normalmente usan una ruta predeterminada para manejar todo el tráfico destinado a las redes no locales. Por lo tanto, BGP no es necesario.

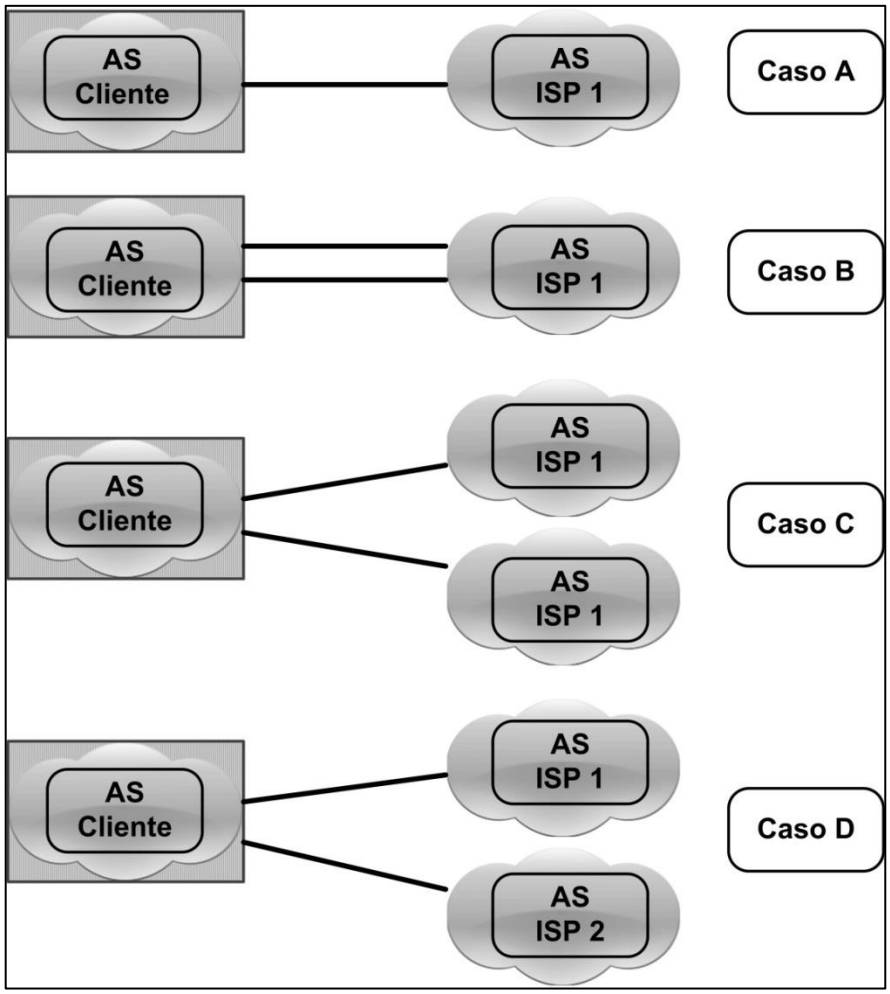


Fig. 5.22. Cuatro ejemplos de posibles configuraciones con BGP.

En el caso de sistemas *single-home* que usan BGP, las políticas de encaminamiento del cliente son una extensión de las políticas del proveedor. No se asignan oficialmente números de sistema autónomo, como es el caso de las IP privadas. Los números de sistemas autónomos del conjunto

privado están en el rango de 64.512 a 65.535. El proveedor no publicará estos números hacia el núcleo de Internet.

Otra situación se plantea con la configuración de un sistema autónomo *dual-homed*, donde existen dos o más enlaces por ISP, y un ISP. Se plantean las mismas opciones que *single-homed*. Normalmente se prefiere una conexión sobre otra que actúa de resguardo (*backup*). Usa ambos caminos; cada uno actúa como un respaldo del otro.

Un caso más interesante se presenta cuando se tiene la configuración de sistema autónomo *single multi-homed*, con un enlace por ISP y dos o más ISPs. Este sería el caso típicamente recomendado para correr BGP. Se presentan algunas opciones:

- ISP1 e ISP2: con rutas *full* Internet,
- ISP1: con rutas *full* Internet e ISP2: con actualizaciones parciales (seleccionadas),
- ISP1: con ruta predeterminada e ISP2: actualizaciones parciales (seleccionadas)

Debe tenerse en cuenta que aunque sean deseables rutas *full* Internet *single multi-homed*, las mismas pueden generar grandes tablas de ruteo. Unas 100.000 rutas requieren alrededor de 70 MB de RAM para la tabla BGP. Las tablas de encaminamiento *full* internet tienen fácilmente más de 300.000 rutas.

También se puede plantear el caso *dual multi-homed*, donde existen dos o más enlaces por ISP, y dos o más ISPs. Se trata de similares opciones que el caso *single multi-homed.*

Los sistemas autónomos pueden ser normalmente *mutihomed no transit*. Como se ha indicado previamente, un sistema *multihomed* tiene más de un punto de salida a redes externas. En esta situación, el sistema autónomo puede ser de tránsito o no-tránsito.

Se llama tráfico de transito al que tiene un origen y destino fuera del AS. Un sistema autónomo es de tránsito cuando permite tráfico de tránsito, y es de no tránsito cuando no lo permite. El sistema advierte solamente sus propias rutas a ambos proveedores, pero no anuncia rutas que él aprendió desde un proveedor a otro. En el ejemplo de la Figura 5.23, el ISP1 no usará el sistema autónomo 24 para alcanzar destinos que crucen por ISP2, y viceversa.

Las advertencias de rutas entrantes influyen sobre su tráfico saliente, y las advertencias salientes influyen su tráfico entrante. Si el proveedor anuncia rutas en su sistema autónomo via BGP, los encaminadores internos del sistema autónomo tienen información más segura sobre destinos externos. Con el mismo criterio anterior, si los encaminadores internos del sistema autónomo anuncian al proveedor vía BGP, tiene influencia sobre qué rutas se informan en cada punto de salida.

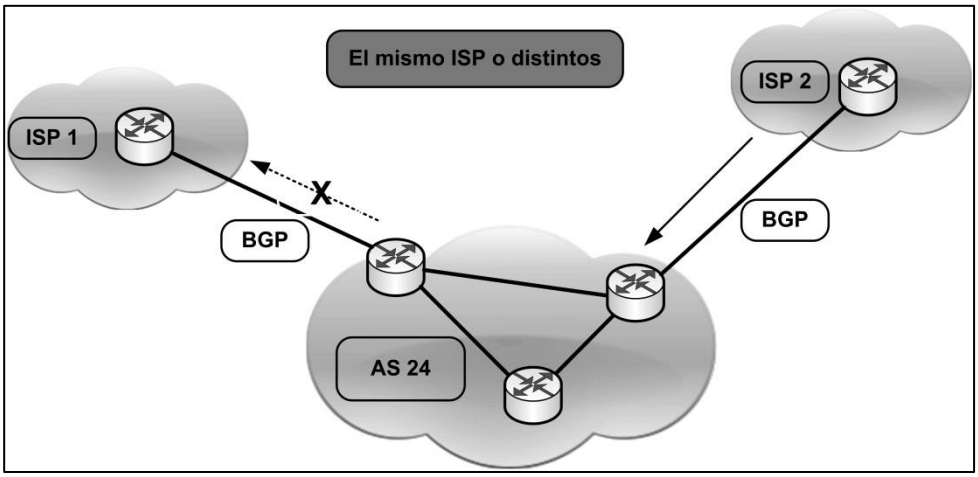


Fig. 5.23. Ejemplo de sistema autónomo de no tránsito.

5.3.4 Mensajes BGP

Un participante BGP es cualquier encaminador que corre BGP. Dicho encaminador BGP puede establecer o no una relación con otro encaminador, dependiendo si también es o no un participante. Se usa el término vecino BGP, peer BGP o neighbor BGP para referirse específicamente a los speakers BGP que han establecido una relación de vecinos, es decir, han realizado una conexión TCP para intercambiar información de ruteo BGP.

Se usa el término BGP externo o EBGP cuando BGP está corriendo entre vecinos que pertenecen a distintos sistemas autónomos. Los vecinos EBGP, por defecto, necesitan estar directamente conectados.

Y se usa el término BGP interno o IBGP cuando BGP está corriendo entre vecinos dentro del mismo sistema autónomo. No es necesario que los vecinos IBGP estén

directamente conectados. Sí deben poder establecer una conexión TCP, ya sea por una red directamente conectada, rutas estáticas o un IRP.

En la Figura 5.24 se presentan algunas instrucciones de configuración necesarias, de un equipo en particular, para establecer la relación vecino entre participantes BGP. Se observa que aparecen como ejemplos los casos de configuración de la relación vecino EBGP entre el encaminador A y el encaminador C, y la relación vecino de IBGP entre el encaminador A y el encaminador B.

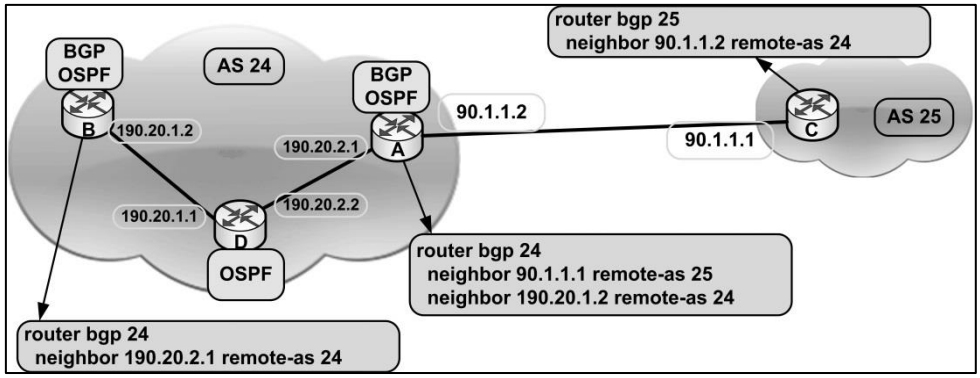


Fig. 5.24. Instrucciones OSPF para establecer la relación vecino.

Todos los tipos de mensajes BGP contienen la misma cabecera de paquete, como se observa en la Figura 5.25:

- Un campo de 16 bytes de Marcado (*Marker*): para detectar la pérdida de sincronización o autenticación de mensajes BGP entrantes,
- Un campo de 2 bytes de Longitud de Paquete (*Length*): que especifica la longitud del mensaje BGP en bytes (la

longitud no puede ser menor a los 19 bytes de la cabecera sin datos ni mayor a 4096), y

- Un campo de 1 byte de Tipo (*Type*): que indica el tipo de mensaje.

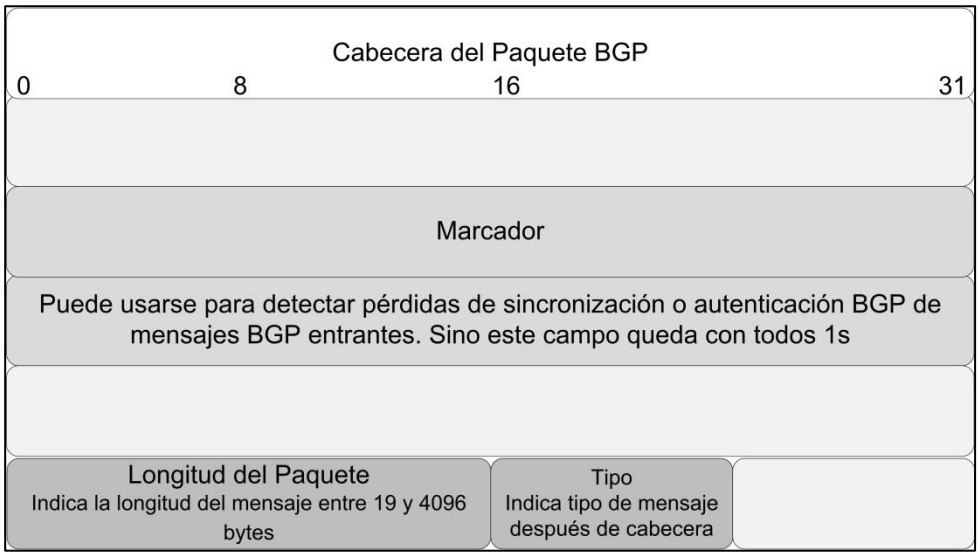


Fig. 5.25. Cabecera de Paquete BGP.

Los datos que siguen a la cabecera del paquete pueden ser de 0 hasta 4.077 bytes, para dar una longitud máxima posible de 4.096.

BGP define los siguientes tipos de mensajes:

- *Open*: el primer mensaje enviado después de establecer la conexión TCP,
- *Update*: inicialmente se envía toda la tabla de encaminamiento; luego la actualización es incremental con información solo de un paso (podrían ser múltiples

redes). Incluye atributos de paso y redes sólo cuando hay modificaciones,

- *Keepalive*: se usa para la confirmación que se aceptó el mensaje *Open* y establece la conexión BGP. Se envía continuamente para confirmar la conexión,
- *Notification*: Cuando se detecta un error, se envía y cierra la conexión.

El mensaje *Open* lo transmite cada participante BGP para negociar parámetros, como:

- El número de versión: que es la más alta que ambos encaminadores soportan. Hoy en día es BGP4.
- El número de AS del encaminador local: el encaminador vecino verifica esta información, para habilitar o no la sesión BGP.
- El tiempo de mantenimiento: que es el máximo número de segundos que puede pasar sin un *keepalive*. Cuando recibe un mensaje *Open*, el encaminador calcula el valor del *hold* temporizador usando el más pequeño, ya sea el suyo o el que le llegó.
- El ID del encaminador BGP: es un campo de 32 bits del BGP ID del transmisor. Es una dirección IP que se asigna al encaminador, y se determina al inicio como en OSPF. Se trata de la IP activa más alta, excepto que exista una interfaz virtual (*loopback)*. En este caso será la IP más alta de las *loopbacks* existentes. También se puede configurar estáticamente.
- Parámetros opcionales.

El mensaje *Update* tiene una longitud mínima de 23 bytes, de los cuales 19 son para la cabecera del paquete, 2 para la longitud de rutas no factibles y 2 bytes para longitud de atributos de paso. La longitud de rutas no factibles especifica el tamaño, en bytes, de rutas que se vuelven inaccesibles o que han cambiado su información de atributo. Estas rutas se expresan en formato prefijo/longitud, conocido como notación CIDR. Por ejemplo, en 10.1.1.0/24 el prefijo es 10.1.1.0 y la longitud es 24. Y la longitud de atributos de paso especifica el tamaño, en bytes, de atributos de paso.

En el mensaje *Update* también se puede enviar la información de accesibilidad a nivel de capa de red (NLRI - *Network Layer Reachability Information)*; contiene una lista de prefijos de direcciones IP alcanzables a través de las publicaciones de un encaminador, expresadas en formato prefijo/longitud.

El mensaje *Keepalive* se intercambia entre pares BGP, una vez que la conexión se ha negociado y está establecida, para mantener la sesión BGP activa. Está conformada sólo por la cabecera de paquete de 19 bytes. Este mensaje no tiene datos, y se envía por defecto cada 60 segundos. En el IOS de Cisco, el *Hold* Temporizador es 3 veces el intervalo *Keepalive*. Si el *Hold* Temporizador se coloca a cero no se envian mensajes *Keepalive*. El mensaje *Update* también se usa para restablecer el *Hold* Temporizador.

El mensaje *Notification* se envía cuando se detecta un error y se cierra inmediatamente la conexión BGP. El campo

del Código de Error especifica el tipo de *Notification* y el campo Subcódigo de error brinda información más específica de la naturaleza del error reportado. Los campos se observan en la Figura 5.26. El mensaje de *Notification* grabará la razón del cierre de la conexión al final del *log* del par remoto.

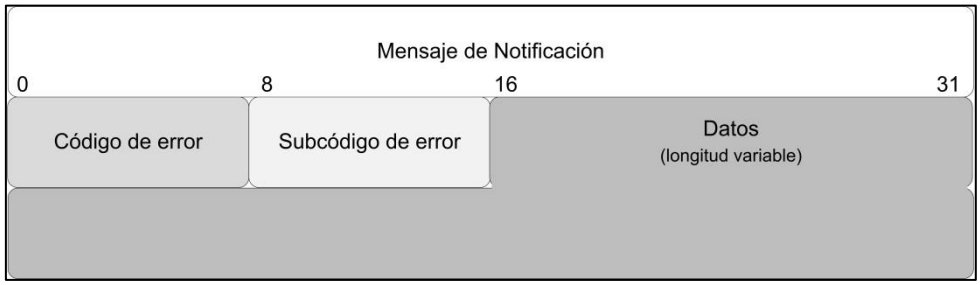


Fig. 5.26. Campos de Código de Error del mensaje *Notification*.

Los códigos de error utilizados en los mensajes de *Notification* son:

Código de Error	Nombre Simbólico
1	*Message Header Error*
2	*Open Message Error*
3	*Update Message Error*
4	*Hold Timer Expired*
5	*Finite State Machine Error*
6	*Cease*

5.3.5 Estados BGP

Cuando se establece una sesión BGP se produce la evolución de una máquina de estados finitos como se representa en la Figura 5.27. Estos estados son:

- Inactivo: Se trata del estado inicial, en espera de un evento de arranque o después de un error.

- Conectado: cuando el encaminador encontró una ruta al vecino y completó el acuerdo de tres vías TCP.
- Activo: cuando, estando establecida la sesión, TCP busca sus pares.
- Envío de mensaje *Open*: cuando se produce el envío del mensaje *Open*, con los parámetros para la sesión BGP.
- Confirma *Open*: Cuando el encaminador recibió correctamente los parámetros para establecer la sesión. Si no hay respuesta del envío de mensaje *Open* vuelve al estado Activo.
- Establecido: Cuando la sesión se estableció con éxito y empieza el proceso de encaminamiento.

En el estado Inactivo, el encaminador no tiene sesión BGP y no puede alcanzar la dirección IP del vecino. Esto se puede deber a que está a la espera de una configuración estática o que el IRP aprenda cómo llegar a dicha IP. Otra posibilidad es que el vecino no esté anunciando su dirección IP. Se mantiene en este estado hasta un evento de arranque para inicializar una sesión TCP y establecer un temporizador de Reintentar Conexión.

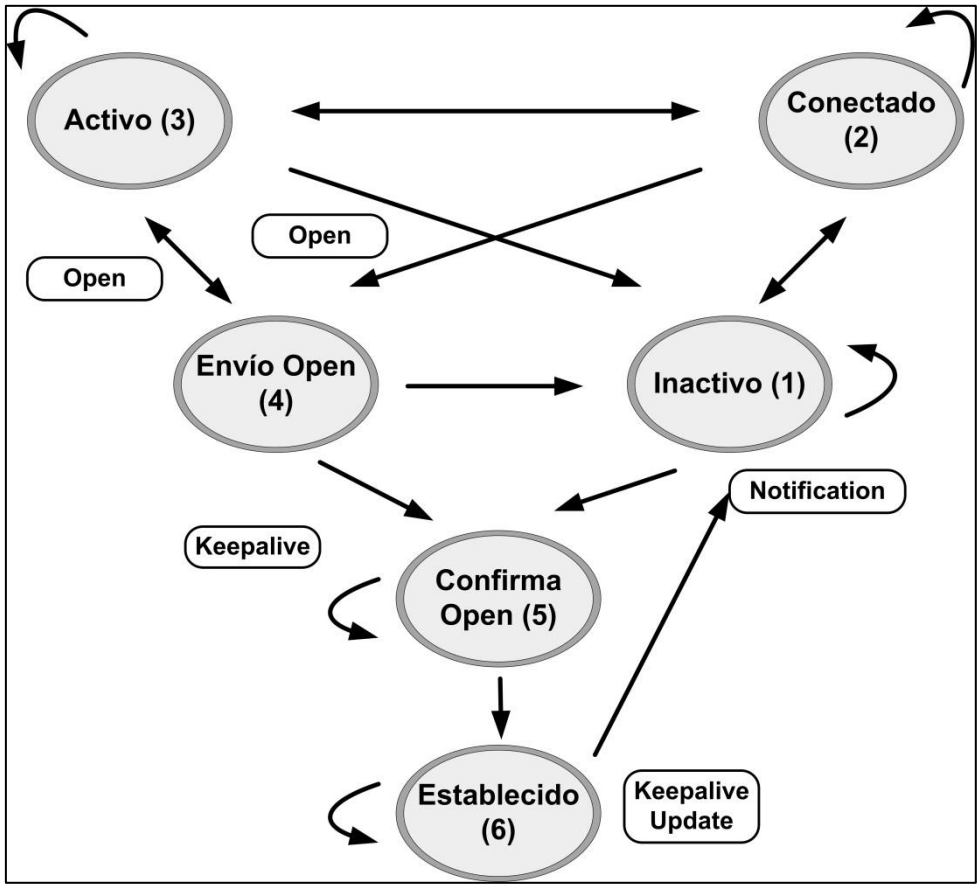


Fig. 5.27. Máquina de estados finito de una sesión BGP.

En el estado Conectado, el encaminador encontró un camino al vecino e inicia una sesión TCP, y espera que se complete. Si el inicio de la sesión fue satisfactorio, porque se recibió un ACK del vecino, el sistema envía un mensaje de *Open* y pasa al estado Envío de mensaje *Open*. Si la conexión TCP falla por un vencimiento de temporizador, el sistema reinicia el temporizador Reintentar Conexión, pasa al estado Activo y queda en escucha para que un par BGP inicie una

conexión TCP. Si el temporizador *Reintentar Conexión* expira, el sistema lo reinicia, comienza una conexión TCP a otro par, y escucha los intentos de establecimiento por parte del mismo. El encaminador permanece en el estado *Conectado*. Ante cualquier otro evento volverá al estado Inactivo.

En el estado Activo, el encaminador trata de iniciar una sesión TCP y espera que se complete. Si fue satisfactoria, porque recibió un ACK del vecino, el sistema envía un mensaje de *Open* y pasa al estado Envío de mensaje *Open*. Si el temporizador *Reintentar Conexión* expira, vuelve al estado Conectado. Ante cualquier otro evento volverá al estado de Inactivo.

- Existen algunos problemas que se presentan en el estado Activo. El encaminador puede entrar en un lazo entre los estados Activo e Inactivo. En el estado Activo, el encaminador encontró una dirección del vecino y envió un paquete *Open*, pero el vecino tal vez no conozca cómo retornar a este encaminador por una serie de causas:
- El vecino no tiene una ruta a la dirección IP origen del paquete BGP *Open* generado por este encaminador,
- La dirección IP que apunta a este encaminador no es la correcta,
- El vecino no tiene una instrucción vecino (*neighbor)* para este encaminador, o
- Hay un error de configuración de número de AS

En el estado Envío de Mensaje *Open*, el encaminador espera por un mensaje *Open* del par. Cuando se recibe un mensaje *Open*, se verifican posibles problemas. Por ejemplo, de versión errónea, distinto número de AS, etc. Si se detectan errores, se envía un mensaje de *Notification* y el estado pasa nuevamente a Inactivo. Si es correcto, se negocian los temporizadores *Hold* y *Keepalive*, y se envían mensajes usados para mantener la conexión (*Keepalives)*. También con el número de AS recibido se sabe si va a trabajar como IRP o ERP, y se pasa al estado Confirma *Open*. Ante cualquier otro evento volverá al estado Inactivo.

En el estado Confirma *Open* se espera por un mensaje de *Keepalive* o de *Notification*. Si se recibe un *Keepalive*, el estado cambia a Establecido, pero si el temporizador *Hold* expira, el sistema envía un mensaje de *Notification* y vuelve al estado de Inactivo, o si el sistema recibe una *Notification*, vuelve al estado de Inactivo. Ante cualquier otro evento volverá al estado Inactivo.

En el estado Establecido, el encaminador puede intercambiar mensajes de *Update*, *Keepalive* o de *Notification* con sus pares. Cada vez que el sistema recibe un *Update* o *Keepalive*, reinicia su temporizador *Hold* a menos que el mismo sea cero. Si el temporizador *Keepalive* expira, envía un *Keepalive* y reinicia el temporizador. Si el sistema recibe un mensaje de *Notification*, el estado vuelve a Inactivo. El sistema envía un mensaje de *Notification* y retorna a Inactivo cuando el temporizador *Hold* expira, o cuando se detecta un error en un mensaje recibido de *Update*. Ante cualquier otro evento volverá al estado Inactivo.

En la Figura 5.28 se presenta como un ejemplo de aplicación el uso de la instrucción *show ip bgp neighbors* de un equipo en particular. Como se aprecia, la salida de la instrucción muestra la información referida a un par, y todas las rutas recibidas de ese par.

```
R1#show ip bgp neighbor
BGP neighbor is 172.31.1.3, remote AS 64998, external link
    BGP version 4, remote router ID 172.31.2.3
    BGP state = Established, up for 00:19:10
    Last read 00:00:10, last write 00:00:10, hold time es 100, keepalive interval is 60 second
    Neighbor capabilities
      Route refresh: advertised and received (old & new)
      Address family IPv4 Unicast: advertised and received
    Message statistics:
      InQ depth is 0
      OutQ depth is 0
                         Sent    Rcvd
      Opens:             7       7
      Notifications:     0       0
      Updates:           13      38
<salida omitida>
```

Fig. 5.28. Instrucción de verificación de vecinos BGP del encaminador.

5.3.6 Atributos BGP

Los encaminadores BGP envían mensajes *Update* sobre redes destino a otros encaminadores BGP. Los mensajes *Update* contienen una o más rutas y un conjunto de métricas BGP llamadas atributos de paso. Un atributo puede ser:

- Bien Conocido u Opcional,
- Obligatorio o Discrecional, o
- Transitivo o No Transitivo

Un atributo también puede ser parcial. No todas las combinaciones de estas características son válidas.

Los atributos de paso son Bien Conocidos cuando son reconocidos por todas las implementaciones de BGP y pueden clasificarse a su vez en:

- Obligatorio Bien Conocido: cuando los atributos se deben incluir en todas las implementaciones de BGP; si no están en el mensaje *Update*, se envía un mensaje de error de *Notification*, y
- Discrecional Bien Conocido: cuando los atributos pueden o no estar presentes en un mensaje *Update*.

Los atributos son Opcionales cuando son reconocidos por algunas implementaciones. En este caso, puede ser que algunos encaminadores BGP no los reconozcan. Los reconocidos se envían a los otros encaminadores basados en su significado. De esta forma se clasifican en:

- Transitivo Opcional: cuando si no se reconocen, se marcan como parciales y se propagan a los vecinos, y
- No Transitivo Opcional: cuando si no se reconocen simplemente se descartan.

Los mensajes *Update* contienen una lista de atributos de paso para la ruta advertida en el campo NLRI. El campo longitud especifica la cantidad en bytes del campo atributos de paso. El contenido de los campos son banderas (*flags*). Los primeros 3 bits de mayor orden especifican si el atributo es *Bien Conocido Obligatorio, Bien Conocido Discrecional, Transitivo Opcional* o *No Transitivo Opcional*. El cuarto bit de

mayor orden especifica la longitud del campo código (si hay más datos). Los bits remanentes no están especificados y se configuran a cero.

Por ejemplo, en el Cisco IOS, el Código de atributo contiene 1 de 10 tipos, siete soportados por todas las implementaciones BGP y tres específicos de Cisco, como se indica en la Tabla 5.1 y se detalla a continuación:

- El atributo Origen (*ORIGIN*): es uno Bien Conocido Obligatorio que especifica cómo el encaminador receptor aprendió la ruta listada en el campo NLRI.
- El Paso a SA (*AS_PATH*): es un atributo Bien Conocido Obligatorio que se compone de una secuencia de segmentos de pasos por AS.
- El Siguiente Salto (*NEXT_HOP*): es un atributo Bien Conocido Obligatorio que define la dirección IP del encaminador de borde que debería usarse como próximo salto.
- El Discriminador Multi-salida (*MULTI_EXIT_DISC*): es un atributo No Transitivo Opcional que especifica la ruta externa preferida que debería tomarse en el AS local.

Código de Tipo de Atributo	Categoría de Atributo	Nombre del Atributo
1	Obligatorio bien conocido	ORIGIN
2	Obligatorio bien conocido	AS_PATH
3	Obligatorio bien conocido	NEXT_HOP
4	No transitivo opcional	MULTI_EXIT_DISC
5	Discrecional bien conocido	LOCAL_PREF
6	Discrecional bien conocido	ATOMIC_AGGREGATE
7	Transitivo opcional	AGGREGATOR
8	Transitivo Opcional (definido por Cisco)	COMMUNITY
9	Transitivo Opcional (definido por Cisco)	ORIGINATOR_ID
10	Transitivo Opcional (definido por Cisco)	CLUSTER_LIST

Tabla 5.1. Códigos de atributos soportados por CISCO.

- La Preferencia Local (*LOCAL_PREF*): es un atributo Bien Conocido Discrecional usado por un encaminador BGP para informar a sus pares IBGP el grado de preferencia para la ruta advertida.
- La Agrupación Atómica (*ATOMIC_AGGREGATE*): es un atributo Bien Conocido Discrecional usado por un encaminador BGP para alertar a los pares BGP que se han agrupado múltiples destinos en una única actualización.
- La Agregación (*AGGREGATOR*): es un atributo Transitivo Opcional. Por ejemplo, cuando se configura agregación de dirección, también se puede incluir en el

encaminador su ID y el número de AS local junto con la ruta a la superred.

Un ejemplo de atributo propietario es el llamado Peso (*WEIGHT*) que usa CISCO. Es local al encaminador y no se propaga. Por lo tanto, no es un código de tipo de atributo. Su función es similar a Preferencia Local, dado que el encaminador elegirá el camino con el valor más alto de Peso, que es un número de 16 bits de 0 a 65.535.

5.4 Ejercitación

Ejercicio n° 1:
Para el esquema de la Figura complete las tablas, con las métricas en cada uno de los nodos para alcanzar a todos los otros (la métrica de cada enlace se muestra en la figura).

a. Al inicio, cuando cada encaminador (o nodo) conoce solo las distancias a su vecino inmediato.
b. Cuando la red ha convergido (cada nodo conoce todas las distancias a los demás).

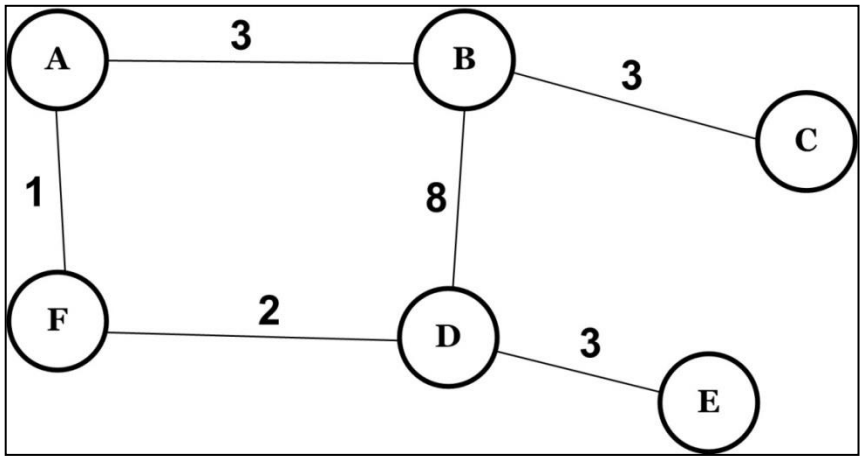


Tabla a:

Nodo origen	Métrica a nodo destino					
	A	B	C	D	E	F
A	0	3	-	-	-	1
B						
C						
D						
E						
F						

Tabla b:

Nodo origen	Métrica a nodo destino					
	A	B	C	D	E	F
A	0	3	6	3	6	1
B						
C						
D						
E						
F						

Ejercicio n° 2:
Para el esquema de la Figura del ejercicio 1, indique las tablas de encaminamiento para el encaminador C y E, considerando que se utiliza el protocolo RIP v1 (métrica = n° de saltos).

Resolución Ejercicio n° 2 Tabla del encaminador C:

Encaminador C		
Red Destino	Métrica	Próximo Salto
A	2	B
B	1	B
C	0	-
D	2	B
E	3	B
F	3	B

Ejercicio n° 3:
Para el esquema de la Figura del Ejercicio n° 1, indique las tablas de encaminamiento para el encaminador C y E, considerando que se utiliza el protocolo OSPF (métrica = indicada en el gráfico).

Resolución Ejercicio n° 3 Tabla del encaminador C:

Encaminador C		
Red Destino	Métrica	Próximo Salto
A	6	B
B	3	B
C	0	-
D	9	B
E	12	B
F	7	B

Ejercicio n° 4:
Realice una comparación entre el protocolo RIP y OSPF, de acuerdo a los resultados obtenidos en los ejercicios 2 y 3.

Ejercicio n° 5:
Suponga un encaminador con una tabla de encaminamiento como la siguiente.

Subred	Máscara de Subred	Próximo Salto
128.96.170.0	255.255.254.0	Interfaz 0
128.96.168.0	255.255.254.0	Interfaz 1
128.96.166.0	255.255.254.0	R2
128.96.164.0	255.255.252.0	R3
{por defecto}		R4

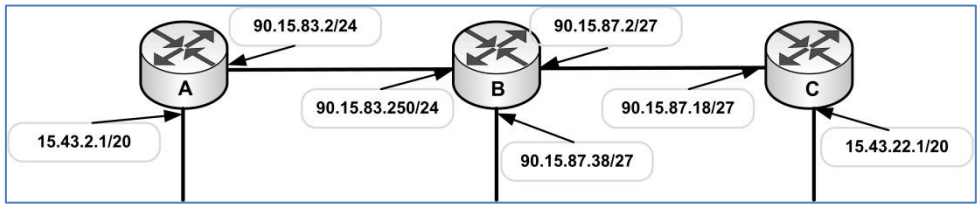
El encaminador puede enviar paquetes directamente por las interfaces 0 y 1, o a los encaminadores R2, R3 o R4. Indique qué hace el encaminador con un paquete direccionado a los siguientes destinos:

a. 128.96.171.92
b. 128.96.167.12
c. 128.96.163.151
d. 128.96.169.192
e. 128.96.165.121
f. 128.96.166.254

Resolución Ejercicio n° 5:

a. Interfaz 0
b. R2
c. R4
d. Interfaz 1
e. R3
f. R2

Ejercicio n° 6:
En el escenario de la Figura se utiliza RIPv1. Indique los resultados que se obtendrán en lo que respecta al encaminamiento: las tablas y problemas posibles.



Resolución Ejercicio n° 6:

El problema que presenta esta topología con su respectivo direccionamiento es que la red no converge. Así la configuración de RIPv1 sea correcta, pero no puede determinar todas las redes en esta topología contigua. Esto es debido a que un encaminador sólo publicará las direcciones de red principales en las interfaces que no pertenecen a la ruta advertida.
Como sabemos RIPv1 no envía información de máscaras de subred en sus actualizaciones, por lo que no soporta VLSM o CIDR.
En esta topología se utilizan dos redes con clase:
15.0.0.0 /8
90.0.0.0 /8
La red 15.0.0.0 /8, se divide en dos subredes:
15.43.2.0 /20
15.43.22.0 /20
La red 90.0.0.0 /8, se divide en tres subredes:
90.15.83.0 /24

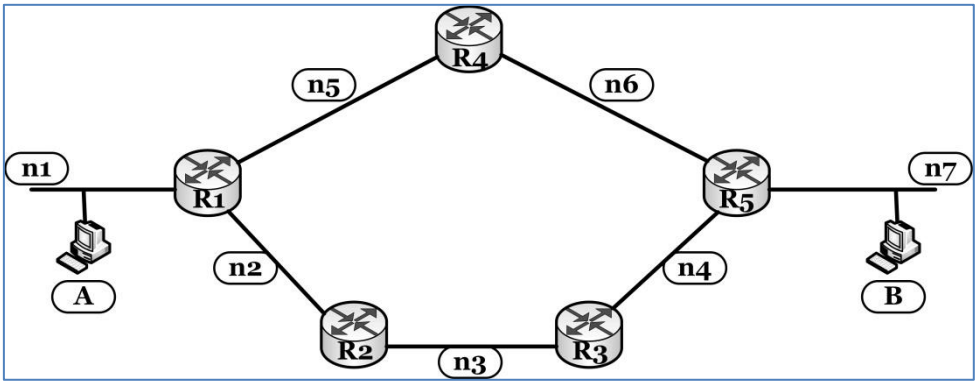
90.15.87.0 /27
90.15.87.32/27
Las redes se resumen automáticamente a través de los bordes de redes principales, ya que el encaminador receptor no puede determinar la máscara de la ruta.
RA no tiene rutas hacia la red 15.43.22.0/20 del Encaminador C. Además, RB equilibrará las cargas de tráfico destinadas a cualquier subred 15.0.0.0/8

Ejercicio n° 7:
Ídem ejercicio anterior para RIPv2

Resolución Ejercicio n° 7:

El problema anterior acá no existe ya que RIPv2 si publica en sus actualizaciones y la máscara de subred, y cada encaminador aprende correctamente todas las subredes.

Ejercicio n° 8:
Del siguiente gráfico considere un paquete de 1200 bytes (incluyendo el encabezado IP de 20 bytes), que se envía de la estación A a la B
Los valores de MTU de cada red son:
MTU n1: 600 B
MTU n2: 600 B
MTU n3: 400 B
MTU n4: 1500 B
MTU n5: 600 B
MTU n6: 1500 B
MTU n7: 1500 B



R1 realiza balance de carga, enviando alternativamente paquetes por R2 y R4.

c. Se pide describir el proceso de fragmentación, y todos los fragmentos asociados, considerando que cada fragmento posee el mayor tamaño posible, y que el primer paquete que pasa por R1 sigue la ruta por R2.
d. ¿Qué efecto puede tener esta característica sobre protocolos de capa de transporte como TCP?

Ejercicio n° 9:
BGP provee una lista de Sistemas Autónomos en el camino al destino. Sin embargo esta información no se considera una métrica de distancia (algoritmo vector-distancia). ¿Por qué?

5.5 Bibliografía y Referencias

5.5.1 Libros impresos

- William Stallings, "Data and Computer Communications", Pearson Education, 10° Ed., 2014.
- William Stallings y Thomas Case, "Business Data Communications", Pearson Education, 7° Ed., 2013.

- William Stallings, “Data and Computer Communications”, Pearson Education, 8° Ed., 2009.
- CCNA de CISCO Press.
- William Stallings, “Wireless Communications & Networks”, Prentice Hall, 2° Ed., 2005.
- Michael Daoud Yacoub “Wireless Technology: Protocols, Standards, and Techniques”, CRC Press, 2002.
- William Stallings, “Local and Metropolitan Area Networks”, Prentice Hall, 6° Ed., 2000.
- Uyless Black, “Tecnologías Emergentes para Redes de Computadoras”, Ed. Prentice-Hall, 1999.
- D. Comer, “Redes Globales de Información con Internet y TCP/IP”, Ed. Prentice-Hall, 3° Ed., , 2000.
- Request for Comments referidos a la temática.
- Artículos de revistas (IEEE, ACM, etc.) referidos a la temática.

5.5.2 Enlaces y Referencias

- Artículos técnicos de Cisco sobre enrutamiento
  https://supportforums.cisco.com/community/netpro/network-infrastructure/routing
  https://supportforums.cisco.com/community/netpro/small-business/routers
- Normas de RIP
  http://tools.ietf.org/html/rfc2453
  http://www.ietf.org/rfc/rfc1058
- Normas de OSPF
  http://www.ietf.org/rfc/rfc2328.txt
  http://www.ietf.org/rfc/rfc5340.txt

- Normas de BGP
  http://tools.ietf.org/html/rfc4274
  http://www6.ietf.org/rfc/rfc4271
- Sistemas autónomos de Argentina
  http://bgp.he.net/country/AR
- Definición y actualización de sistemas autónomos
  http://www.nro.net/technical-coordination/asn

CAPÍTULO 6

Tecnologías MAN Metro Ethernet y Wi-Max

6.1 Metro Ethernet
- 6.1.1 Introducción
- 6.1.2 Modelo de Referencia
- 6.1.3 Conexiones Virtuales Ethernet
- 6.1.4 Tecnologías de Transporte de Ethernet

6.2 Wi-Max
- 6.2.1 Introducción
- 6.2.2 Estándares
- 6.2.3 Servicios y Tecnologías
- 6.2.4 Implementaciones
- 6.2.5 Relaciones de OFDM y estándares Wi-Max

6.3 Ejercitación

6.4 Bibliografía y Referencias
- 6.4.1 Libros impresos
- 6.4.2 Enlaces y Referencias

Capítulo 6

Tecnologías MAN MetroEthernet y Wi-Max

6.1 Metro Ethernet

6.1.1 Introducción

Hay nuevas necesidades de ancho de banda, en los siguientes aspectos, para:

Reducir costos con:

- La consolidación de servidores,
- Redes de área de almacenamiento,
- La convergencia de redes de datos, voz y video, y
- La contratación de nuevos modelos de Tecnologías de Información.

Aumentar la productividad con:

- Aplicaciones de oficina multimedia,
- Aplicaciones distribuidas,
- Aplicaciones basadas en Web, e
- Integración de Aplicaciones.

Responder a incertidumbres con:

- Centros de datos distribuidos,
- La continuidad de negocios,
- La Recuperación de desastres,

- El almacenamiento remoto, y
- Redes seguras.

Mejorar el valor para el Cliente con:

- Administración de la relación con los clientes,
- *Data warehousing*, y
- Portales de clientes.

El uso de las tecnologías WAN Ethernet para crear redes de área metropolitana MANs se denomina habitualmente Metro Ethernet. Metro Ethernet se usa para suministrar servicios de acceso a Internet a los clientes LANs y residenciales, u otros servicios WAN. Las agencias de gobierno, institutos educacionales, y corporaciones pueden usar los servicios Metro Ethernet para crear intranets que interconectan oficinas o campus remotos.

Se llama red Metro Ethernet a cualquier red destinada a suministrar servicios Metro Ethernet, y en general, se aplica a redes de operadores (ISPs). Los servicios Metro Ethernet se refieren a la conectividad MAN/WAN de Capa 2 a través de Ethernet. Este tipo de redes puede implementarse con varias opciones de transporte físico.

Ethernet se ha convertido en una tecnología exclusiva para las redes LAN, MAN y WAN. Se trata de una arquitectura eficiente para redes de paquetes, en enlaces punto a punto, punto a multipunto, y multipunto a multipunto. Ofrece una interfaz con costo ventajoso, con flexibilidad de ancho de banda, y velocidades de 10 a 10000

Mbps, y más. Ethernet se usó originalmente para entornos LAN, pero hoy se ofrece con independencia geográfica, en diversas implementaciones físicas: Ethernet óptico, sobre IP o MPLS.

Metro Ethernet no afecta en absoluto el diseño y desarrollo de las redes empresariales; puede mantenerse la misma estructura y jerarquía. Metro Ethernet permite satisfacer los requerimientos de ancho de banda de las aplicaciones y es fácilmente escalable. Los tipos de servicios dictarán las consideraciones de diseño.

Se observa en la Tabla 6.1 un cuadro comparativo con las diferencias principales entre Ethernet, Frame Relay y ATM, en base a las siguientes características: escalabilidad, soporte de QoS, flexibilidad de servicio, costo por puerto y por Mbps, entre otros aspectos. Ethernet se presenta como una tecnología sólida, al compararla con las de conmutación de paquetes tradicionales.

	Ethernet	Frame Relay	ATM
Escalabilidad	10M a 10G	56K a 45M	1.5M a 622M
QoS	Soportado	Limitado	Si
Flexibilidad del Servicio	Alta	Baja	Baja
Eficiencia del Protocolo	Alta	Media	Baja
Optimizado para IP	Si	No	No
Aprovisionamiento	Rápido	Lento	Lento
CPE: Costo por Puerto	$	$$	$$$
Costo/Mb	$	$$	$$$

Tabla 6.1. Cuadro comparativo
entre Ethernet, Frame Relay y ATM.

Las tecnologías de Frame Relay y ATM son las VPNs de Capa 2 tradicionales. Cada CE (*Customer Equipment* – Equipamiento del Cliente) dispone de *n* circuitos, cada uno de ellos conectado a otro CE, en topología de malla parcial. En la red del proveedor, los nodos conmutan los paquetes del cliente basándose en información de Capa 2 (DLCI en Frame Relay y VC en ATM). Metro Ethernet es otra VPN de Capa 2, en la que la red del proveedor transporta tramas Ethernet (las direcciones MAC se usan para determinar el encaminamiento). Se puede asimilar una VLAN a un DLCI o un VC.

Se observa una gran diversidad de servicios y tecnologías Metro Ethernet. Cada uno de ellos con sus particularidades. Entre los servicios, encontramos a *E-Line* (Línea-E - Servicio de Línea Privada Virtual Ethernet); *E-LAN (*LAN E - Servicio Multipunto); *L2VPN* (VPN de Capa 2 - Servicio de conexión de Capa 2 extremo a extremo); *EVC* (*Connection Virtual Ethernet* - Servicio de conexión virtual Ethernet con interfaces usuario a red UNI); *TLS* (*Service LAN Transparent* - Servicio LAN Transparente); *VPLS* (*Service LAN Virtual Private* -Servicio LAN Privado Virtual, entre otros.

Entre las tecnologías, podemos encontrar nombres como EoW (Ethernet over High Speed Wireless – Ethernet sobre Redes Inalámbricas de Alta Velocidad), EoS (Ethernet over SONET/SDH – Ethernet sobre SONET/SDH)), Optical Ethernet (Ethernet Óptico - Ethernet nativo sobre fibra óptica), EoMLPS (Ethernet over MPLS – Ethernet sobre MPLS), entre otras.

El Foro de Metro Ethernet tiene como misión acelerar la adopción de las tecnologías y servicios Ethernet a nivel de operador. Para ello, tiene como objetivo principal construir consenso y unir a proveedores de servicios, fabricantes de equipos y clientes finales en las definiciones de servicios, especificaciones técnicas e interoperabilidad; facilitar el desarrollo de los estándares existentes o nuevos para permitir el uso de los servicios de Metro Ethernet y hacer que Ethernet sea la clase de transporte; y difundir los beneficios de los servicios de Ethernet y redes de transporte basadas en Metro Ethernet.

Las principales competencias del Foro Metro Ethernet son:

1. Definir servicios Ethernet para las redes de transporte metropolitanas. Dichos servicios deberán ser suministrados sobre redes Metro Ethernet nativo y podrán estar soportadas por otras tecnologías de transporte. Y además, definir las tecnologías de transporte de Ethernet para áreas metro a nivel de transportista, especificando arquitecturas, protocolos y gestión.
2. Con menor prioridad, especificar el trabajo que deben hacer otras organizaciones sobre tecnologías de transporte (actividad de enlace y coordinación), e interfaces no-Ethernet, si no están definidas por otras organizaciones.

6.1.2 Modelo de Referencia

En la Figura 6.1 se inicia la descripción del modelo de referencia. Se describen a continuación los componentes del modelo.

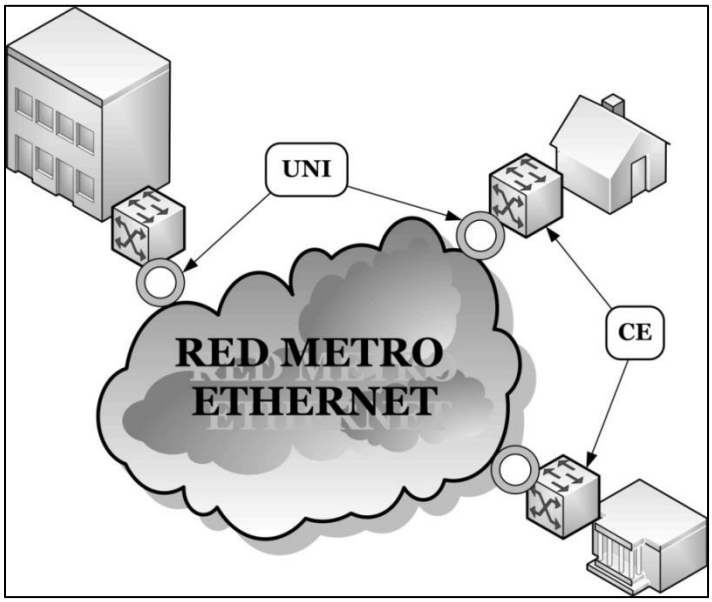


Fig. 6.1. Modelo de referencia Metro Ethernet.

El CE se conecta a través de una UNI (*User Network Interface*). El CE puede ser un encaminador o un conmutador IEEE 802.1Q.

La UNI responde al estándar IEEE 802.3, en cuanto a las capas físicas y MAC Ethernet, con velocidades de 10Mbps a 10Gbps. Se da soporte a varias clases de servicios (QoS). La red Metro Ethernet puede usar distintas tecnologías de transporte y de provisión de servicio, como por ejemplo: SONET/SDH, WDM, PON, RPR, MAC-in-MAC, QiQ (VLAN stack), o MPLS.

Y finalmente, entre estas definiciones, está prevista para un futuro la interface NNI (*network to network interface*).

Sobre el anterior modelo, se añade un cuarto componente: una EVC (*Ethernet Virtual Connection*). Una EVC es una asociación entre dos o más UNIs. El proveedor del servicio la crea para un cliente. Una trama en una EVC puede ser enviada a una o más UNIs de la EVC. Nunca será enviada de vuelta a la UNI de entrada, ni a una UNI que no pertenezca a la EVC.

Las EVCs pueden ser:

- Punto a punto (*E-Line*), y
- Multipunto a multipunto (*E-LAN*)

Cada tipo de servicio Ethernet tiene un conjunto de atributos de servicio y sus correspondientes parámetros que definen las capacidades del mismo.

Entre los atributos de un servicio Ethernet en particular se encuentra la:

- Multiplexación de servicios: que asocia una UNI con varias EVC. Pueden ser: varios clientes en una sola puerta o varias conexiones de servicios distintos para un solo cliente.
- Transparencia de VLAN: significa que el proveedor del servicio no cambia el identificador de la VLAN (la red Metro Ethernet aparece como un gran switch). En el servicio de acceso a Internet tiene poco importancia.
- Agrupamiento de VLAN (*Bundling*): Más de una VLAN de cliente está asociada a la EVC en una UNI.

Hay atributos asociados a la interface UNI, y atributos asociados a la EVC. Por ejemplo, entre los atributos de la UNI: identificador de tipo de medio, de velocidad, de dúplex, etc; atributo de soporte de etiqueta de VLAN, atributo de multiplexación de servicio, atributo de agrupamiento de VLAN, atributo de filtros de seguridad, etc. Y entre los atributos de EVC encontramos: parámetros de tráfico (CIR, PIR, entrada, salida, etc), parámetros de prestaciones (retardo, variación de retardo, etc), parámetros de clase de servicio, VLAN-ID, etc), atributo de servicio de despacho de tramas (tramas de unidifusión, tramas de multidifusión), etc.

6.1.3 Conexiones Virtuales Ethernet *E-Line* y *E-LAN*

El servicio Ethernet *E-Line*, presentado en la Figura 6.2, puede operar con ancho de banda dedicado o compartido:

- EPL (*Ethernet Private Line*): Es un servicio EVC punto a punto con un ancho de banda dedicado. El cliente siempre dispone del CIR, normalmente en canales SDH o en redes MPLS. Es como una línea en TDM (*Time Division Multiplexing* - Multiplexación por División de Tiempo), pero con una interfaz Ethernet.
- EVPL (*Ethernet Virtual Private Line*): En este caso hay un CIR y un EIR, y una métrica para el soporte de acuerdos con el proveedor. Es similar a Frame Relay. Se suele implementar con canales TDM compartidos o con redes de conmutación de paquetes usando conmutadores y/o encaminadores.

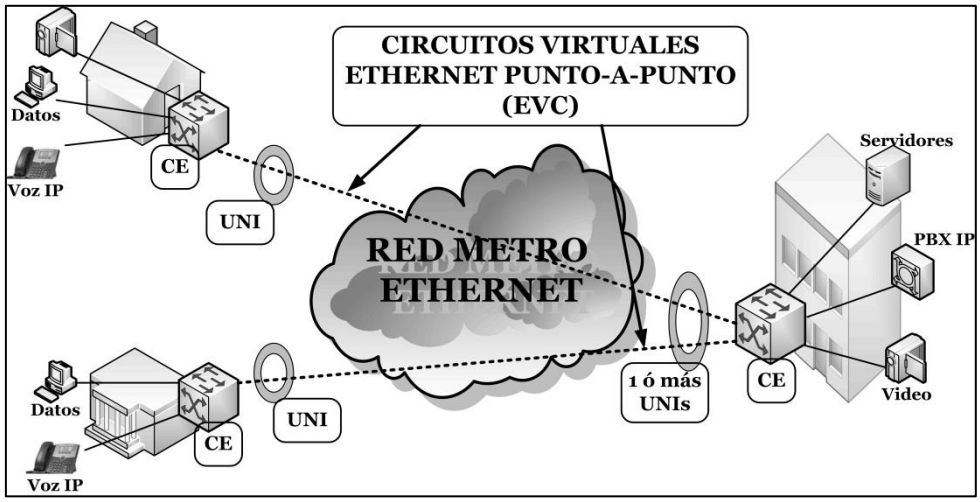


Fig. 6.2. Servicio Ethernet *E-Line*.

El servicio Ethernet *E-LAN*, presentado en la Figura 6.3, puede operar también con ancho de banda dedicado o compartido:

- EPLan (*Ethernet Private LAN*): Suministra una conectividad multipunto entre dos o más UNIs, con un ancho de banda dedicado.
- EVPLan (*Ethernet Virtual Private LAN*): También suele conocerse con los nombres de VPLS (*Virtual Private Lan Service*), TLS (*Transparent LAN Service*), VPSN (*Virtual Private Switched Network*). La separación de clientes se obtiene vía encapsulación usando etiquetas de VLANs del proveedor.

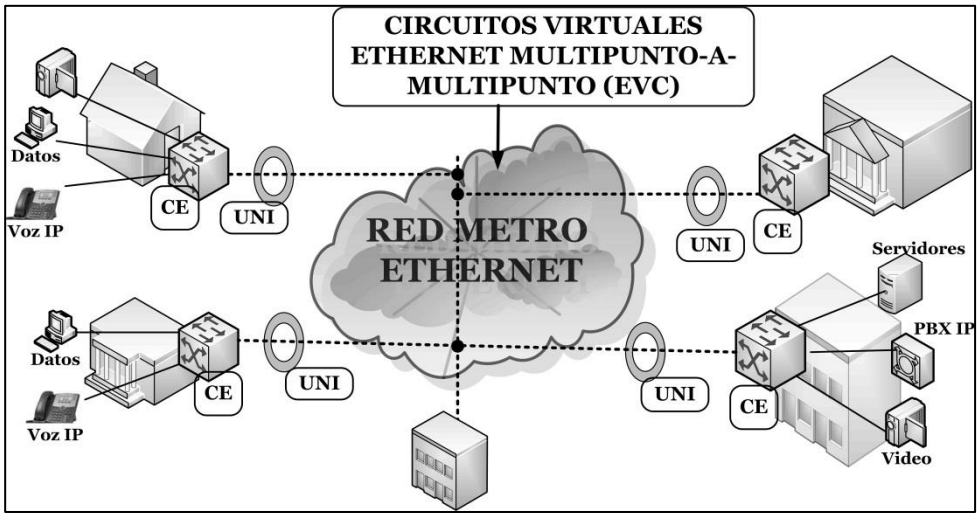


Fig. 6.3. Servicio Ethernet *E-LAN*.

6.1.4 Tecnologías de Transporte de Ethernet

Los servicios Metro Ethernet no necesitan que toda la red de Capa 1 y 2 sea exclusivamente Ethernet. También puede ser: Ethernet Óptico con MPLS o *Ethernet sobre SONET*, por mencionar algunas de las diversas soluciones, como se muestra en la Figura 6.4.

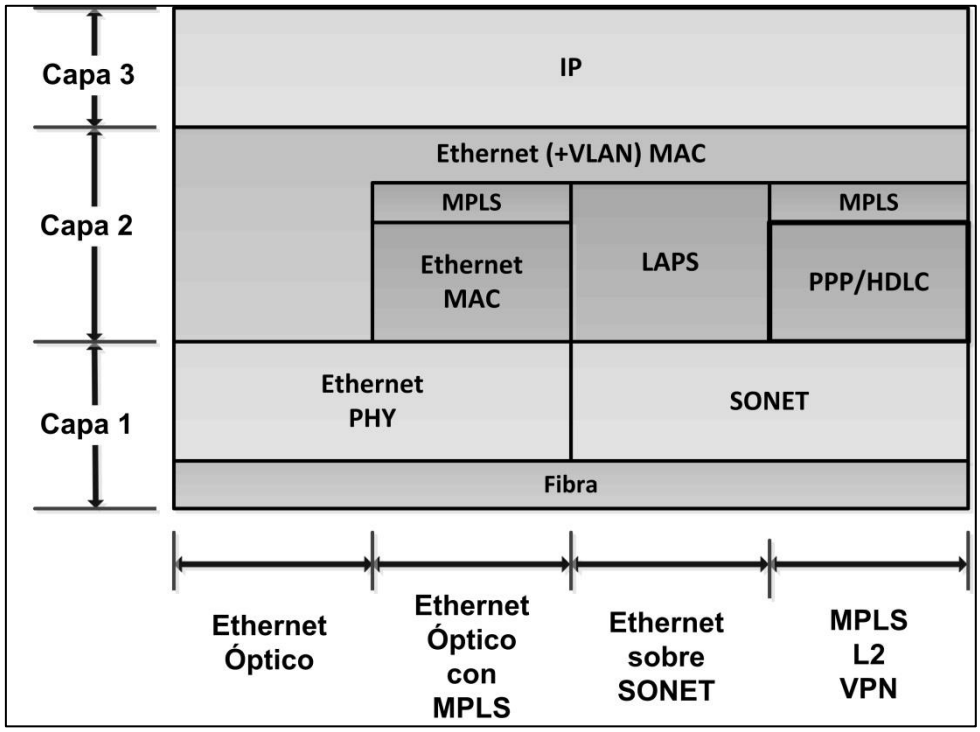


Fig. 6.4. Soluciones de Capa 1 y 2
para el transporte de Ethernet.

Por ejemplo, EoS (*Ethernet over SONET*) es un conjunto de estándares de la industria que han sido desarrollados para el transporte óptimo de Ethernet sobre topologías de conmutación de circuitos (SDH/SONET). Hay técnicas de encapsulación disponibles: las técnicas de concatenación virtual (VCAT), y el esquema de ajuste de la capacidad del enlace (LCAS), que definen el método de transporte. Y por otro lado, las técnicas de procedimiento de entramado (*framing*) genérico (GFP) y el procedimiento de acceso de enlace para SDH (LAPS), que son protocolos de adaptación de la Capa 1 de transporte.

La concatenación de tributarios puede ser contigua (basada en punteros) o virtual. La VCAT no necesita que los tributarios sean contiguos. Pueden viajar por distintos caminos entre los extremos. Al contrario de la concatenación contigua, que requiere que la funcionalidad la tengan todos los nodos intermedios en la red, además de los extremos, VCAT sólo la exige en estos últimos.

El esquema de ajuste de la capacidad del enlace LCAS está definido en el ITU-T G.7042. LCAS es un mecanismo de señalización para que los extremos se sincronicen cuando añaden o eliminan algún miembro del grupo de concatenación virtual VCG (V*irtual Concatenation Group*). Permite cambiar el ancho de banda bajo demanda.

El procedimiento de entramado genérico GFP está definido en el G.7041 del ITU-T. Es un mecanismo genérico de encapsulado que resulta de asignaciones directas de varios tipos de tráfico en contenedores de SONET/SDH virtual. Hay dos tipos de asignaciones: *Frame-GFP* y el *Transparent-GFP*. Mientras que el Ethernet LAPS es un protocolo del tipo HDLC (*High-Level Data Link Control*) para usar en la carga datos de SDH. Tiene secuencias prohibidas que deben ser sustituidas. El ITU-T X.85 define IP sobre LAPS y el ITU-T X.86 define Ethernet sobre LAPS.

Como en otros casos, las empresas no usarán los servicios Ethernet a menos que haya acuerdos con el proveedor, con compromisos de prestaciones y disponibilidad del servicio en sitios críticos. De cumplirse estas condiciones, las empresas construirán redes privadas. Los atributos de

servicios críticos en los acuerdos son: el perfil de ancho de banda y la performance del servicio.

El Foro Metro Ethernet ha definido tres perfiles de ancho de banda en su ETM (*Ethernet Traffic Management*), como se indica en la Figura 6.5: el perfil de ancho de banda de ingreso por UNI de ingreso, por EVC y por identificación ID de CoS (*Class of Service* - Clase de Servicio). Se utilizan 4 parámetros: CIR, CBS, EIR y EBS. El CIR y el CBS determinan la cantidad de tramas liberadas por objetivos a nivel de servicio, y el EIR y el EBS determinan la cantidad de tramas liberadas en exceso permitidas.

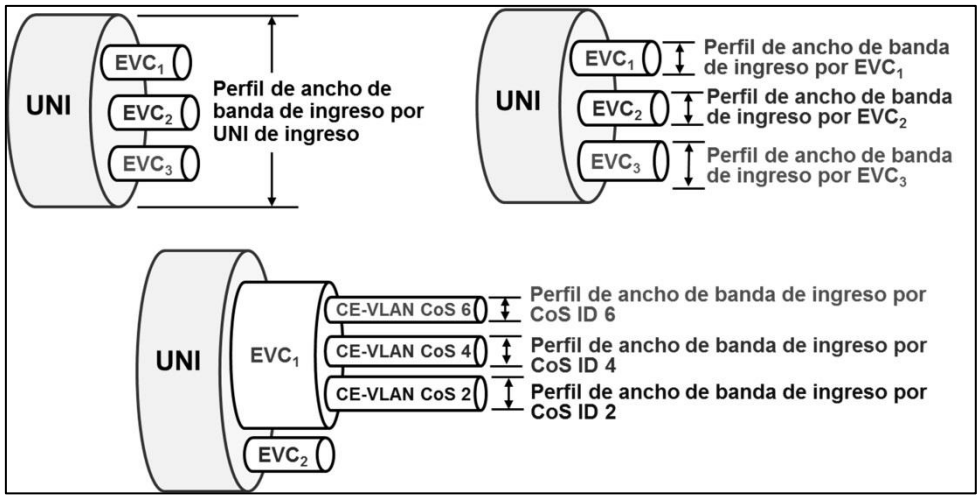


Fig. 6.5. Perfiles de ancho de banda en el ETM.

Respecto a los parámetros asociados a las prestaciones del servicio, se enumeran: la disponibilidad, el retardo, la variación del retardo y la pérdida de tramas. El nivel de prestaciones del servicio para transmisión está determinado

por la identificación de CoS, la prioridad 802.1p de usuario por EVC, y por puerto UNI.

6.2 Wi-Max

6.2.1 Introducción

Los sistemas de microondas terrestres se usan principalmente en servicios de telecomunicaciones de larga distancia, como alternativa al cable coaxial, y especialmente a la fibra óptica, que se ha vuelto muy competitiva. Se usa frecuentemente para transmitir televisión, voz y datos. También se usa en los enlaces punto a punto a cortas o largas distancias. En vista de su aplicación en redes de datos MAN y WAN, se presentará la tecnología de microondas terrestres Wi-MAX.

Wi-Max (*Worldwide Interoperability for Microwave Access*) es una tecnología de microondas terrestres normalizada que habilita enlaces y el acceso de banda ancha inalámbrica. Está especificada por el Instituto de Ingenieros en Electricidad y Electrónica IEEE, como el estándar IEEE 802.16.

El Foro Wi-Max es un organismo de la industria, sin fines de lucro, dedicado a promover la adopción de esta tecnología y asegurar que diferentes productos de fabricantes puedan interoperar entre sí. Esto lo realiza a través de planes de desarrollo y test de interoperabilidad, y programas de certificación. Wi-MAX *Forum Certified*™ significa que un

proveedor de servicio puede comprar equipamiento de más de una compañía y estar seguro que van a trabajar entre sí.

Wi-MAX se diseñó para proveer conectividad fija, nómade y portátil de banda ancha inalámbrica sin la necesidad de LOS (*Line Of Sight* - línea de visión directa) con una estación base. En un desarrollo, con un radio de celda típico de 3 a 10 km, los sistemas certificados por el Foro Wi-MAX pueden brindar una capacidad de hasta 40 Mbps por canal, para aplicaciones de acceso fijo y portátil. Para desarrollos de redes móviles pueden suministrar típicamente hasta 15 Mbps de capacidad dentro de un radio de celda de 3 kms.

De acuerdo al Foro Wi-Max se soportan 5 clases de aplicaciones:

- Juegos interactivos multi-jugador,
- Conferencias de VoIP y Video,
- *Streaming*,
- *Browsing* Web y mensajería instantánea, y
- Descargas de contenidos.

6.2.2 Estándares Wi-Max

Wi-Fi es un conjunto de tecnologías basadas en los estándares IEEE 802.11 a, b, g y n, que se resumen en la Tabla 6.2. Se la considera una de las primeras redes inalámbricas de banda ancha ampliamente desarrolladas. La arquitectura Wi-Fi consiste de una estación base que interconecta estaciones en forma inalámbrica para acceder a

los recursos de la red. Mientras que los usuarios estén dentro del radio de cobertura (aprox. 100-200 m) que brinda un AP (Access Point – Punto de Acceso), podrán mantener la conectividad.

Estándar	Velocidad	Rango	Frecuencia
802.11b	Hasta 11 Mbps	~ 100 m	2.4 Ghz
802.11a	Hasta 54 Mbps	~ 30 m	5 Ghz
802.11g	Hasta 54 Mbps	~ 100 m	2.4 Ghz
802.11n	Hasta 300 Mbps	> 100 m	2.4 y 5 Ghz

Tabla 6.2. Resumen de las tecnologías basadas en el estándar 802.11.

Wi-Fi presenta algunas desventajas en las comunicaciones inalámbricas de microondas. Tiene un nivel limitado de movilidad, es susceptible a las interferencias, y lo que es muy importante, fue diseñada técnicamente para funcionar en rangos cortos y básicamente el interior de instalaciones.

Es posible establecer una relación entre las tecnologías Wi-Fi y Wi-Max. Wi-Max elimina las restricciones de Wi-Fi, dado que está diseñada para trabajar en el exterior sobre grandes distancias. Se trata de una tecnología más compleja y puede manejar características importantes como QoS, confiabilidad de transporte de portadora, NLOS (*Non Line Of*

Sight), etc. Y desde este punto de vista, Wi-Max no intenta reemplazar a Wi-Fi, sino que es un complemento, y en algunos casos simplemente no compiten entre sí dado que resuelven diferentes problemáticas de conectividad inalámbrica.

En la Tabla 6.3 se presentan brevemente algunas de las características básicas de diferentes estándares que se han presentado en el tiempo, para satisfacer una gama de soluciones.

	802.16	802.16a	802.16-2004	502.16e-2005
Fecha de Liberación	Diciembre 2001	Enero 2003	Junio 2004	Diciembre 2005
Espectro	10-66 GHz	< 11 GHz	< 11 GHz	< 6 GHz
Operación	LOS	No-LOS	No-LOS	No-LOS y Movilidad
Bit Rate	32-134 Mbps	Hasta 75 Mbps	Hasta 75 Mbps	Hasta 15 Mbps
Radio de Celda	1-5 Km	4-8 Km	4-8 Km	1-5 Km

Tabla 6.3. Resumen de las tecnologías basadas en el estándar 802.16.

6.2.3 Servicios y Tecnologías Wi-Max

Wi-Max puede proveer 2 formas de servicios inalámbricos:

- Sin línea de vista (NLOS): como una clase de servicio Wi-Fi, donde una estación con una pequeña antena se

conecta a un nodo. Usa un rango de frecuencias relativamente bajo (de 2 a 11 GHz).

- Con línea de vista (LOS): donde puntos de antenas fijos se unen al nodo. La conexión LOS es más fuerte y más estable, de modo que es capaz de enviar alta tasa de datos con pocos errores. Usa frecuencias más altas, de hasta 66 GHz. Y la tecnología, en general, se puede suministrar hasta un radio de 48 Kms.

- El Foro Wi-Max anticipa el avance de sus tecnologías en 3 alternativas distintas, para:
- La comunicación con ubicación fija, servicios de línea privados, concentradores hot spot, etc.
- Brindar acceso inalámbrico de banda ancha (*DSL Wireless*).
- Los usuarios móviles y nómadas.

Además, está enfocado en usar bandas espectrales para implementación global, que comprende las siguientes:

- No licenciada de 5 GHz: Incluye las bandas entre 5.25 y 5.85 GHz. En la banda superior (5.725 – 5.850 GHz) muchos países permiten alta potencia de salida (hasta 4 Watts), lo que la hace muy atractiva.
- Licenciada de 3.5 GHz: Incluye las bandas entre 3.4 y 3.6 GHz en la mayoría de los países.
- Licenciada de 2.5 GHz: las bandas entre 2.5 y 2.6 GHz están permitidas en US, México, Brasil y algunos otros países.

Las opciones de las bandas espectrales licenciadas y no licenciadas tienen sus ventajas y desventajas. En las bandas licenciadas se obtiene una mejor respuesta a los requerimientos de QoS, una mejor recepción en aplicaciones NLOS en bajas frecuencias, aunque habrá complicaciones por el tema de la gestión de la licencia, mientras que en la banda no licenciada se obtienen desarrollos más rápidos a un costo inferior, y con toda una serie de opciones mundiales para la implementación.

Se pueden comparar rápidamente los aspectos técnicos fundamentales de las soluciones de banda licenciada y no licenciada. Ambas soluciones se basan en el estándar IEEE 802.16-2004, que usa OFDM en la Capa 1. OFDM provee beneficios como mejor SNR (Signal to Noise Ratio - Relación Señal a Ruido) de estaciones de clientes y una mejor respuesta a interferencias multipaso o multitrayectoria. Para crear canales bi-direccionales full-duplex, las soluciones licenciadas usan FDD (*Frequency Division Duplex* – Duplexación por División de Frecuencias) mientras que las no licenciadas usan TDD (*Time Division Duplex* – Duplexación por División de Tiempo). Tanto FDD y TDD se refieren a la duplexación o transmisión inalámbrica de dos vías (canal ascendente y canal descendente).

TDD requiere sólo un canal para transmitir las subtramas del canal ascendente y descendente en dos ranuras (*slots*) de tiempos distintos. TDD tiene por lo tanto una mayor eficiencia espectral que FDD. TDD puede manipular flexiblemente el tráfico de banda ancha simétrico y asimétrico. Su campo de aplicación especial es cuando se

transmiten datos asimétricos, en entornos con patrones de tráfico variable, donde la eficiencia de RF es más importante que el costo.

FDD requiere dos canales distintos para transmitir la subtrama del canal ascendente y la subtrama del canal descendente en el mismo tiempo de ranura. Por ello, FDD es apropiada para servicios de voz bidireccionales dado que ocupa ambos canales de manera simétrica. No se puede desarrollar cuando el espectro no está balanceado. En este caso, el espectro es normalmente licenciado, por lo que involucra mayores costos. Se usa en entornos con patrones de tráfico predecible, donde los costos del equipamiento son más importantes que la eficiencia de RF. FDD se usa comúnmente en las redes celulares 2G y 3G.

6.2.4 Implementaciones Wi-Max

Las implementaciones Wi-Max no están exentas de desafíos. Las interferencias de RF interrumpen la transmisión, y como consecuencia, el rendimiento disminuye. Las formas más comunes de interferencias son las interferencias multi-paso y la atenuación.

La superposición de interferencias diversas genera ruido aleatorio. Además, otro desafío es la ubicación de la infraestructura. La estructura física que alberga o apoya la estación base debe estar libre de RF. Las estructuras metálicas pueden distorsionar las señales, u obstáculos en movimiento pueden la intensidad de la señal. Los obstáculos

tales como árboles y edificios a menudo bloquean los caminos de la señal.

Es necesario resolver los aspectos que afectan la calidad del servicio de la implementación Wi-Max. El diseño adecuado de las redes y la ubicación de la infraestructura son fundamentales para solucionar los problemas. Por ejemplo,

- Estudiar el sitio del abonado, reunir estadísticas, coordinar el uso de RF con los proveedores de vecinos.
- La definición de las características más adecuadas de las antenas (tipo, ángulos de inclinación, matriz de ganancia, diversidad, etc.)
- El buen diseño e implementación del nodo del proveedor, y de las estaciones base o celdas con acceso, las estructuras de RF prácticas y la protección contra eventos meteorológicos.

6.2.5 Relación de OFDM y los Estándares Wi-Max

Los perfiles definidos por el Foro Wi-Max especifican una interfaz de aire en OFDM de 256 portadoras, y aún más. OFDM permite transmitir simultáneamente las señales digitales en múltiples ondas portadoras de RF. Esto favorece una gran adaptación a los contextos NLOS. Además, OFDM es resistente a efectos multi-paso, espectralmente eficiente para transmitir datos digitales inalámbricos, y tiene buena eficiencia a mayor ancho de banda.

Sin embargo, también hay algunos problemas, como un pico muy alto de potencia promedio llamada PAPR (*Peak to Average Power Ratio* – Relación entre la Potencia Pico y Promedio).

En la Tabla 6.4 se pueden apreciar las diferencias entre cada uno de los distintos estándares de Wi-Max, es decir, el protocolo original 802.16, Wi-Max fijo 802.16 2004, y Wi-Max móvil 802.16e 2005.

	802.16	802.16-2004	802.16e-2005
Estado	Completado en Diciembre de 2001	Completado en Junio de 2004	Completado en Diciembre de 2005
Banda de frecuencia	10GHz-66GHz	2GHz-11GHz	2GHz-11GHz para red 2GHz-66Hz para aplicaciones móviles
Aplicación	LOS Fijo	NLOS Fijo	NLOS fijo y móvil
Arquitectura MAC	Malla punto-multipunto	Malla punto - multipunto	Malla punto-multipunto
Esquema de transmisión	Únicamente portadora sencilla	Portadora sencilla. 256 OFDM o 2.048 OFDM	Portadora sencilla. 256 OFDM u OFDM variable con 128, 512, 1.024 o 2.048 subportadoras
Modulación	QPSK, 16 QAM, 64QAM	QPSK, 16 QAM, 64QAM	QPSK, 16 QAM, 64 QAM
Tasa de transmisión de datos absoluto	32Mbps-134.4Mbps	1Mbps-75Mbps	1Mbps-75Mbps
Multiplexado	TDM/TDMA	TDM/TDMA/OFDMA	TDM/TDMA/OFDMA
Duplexado	TDD y FDD	TDD y FDD	TDD y FDD
Ancho de banda de los canales	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHZ, 15MHz, 8,75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHZ, 15MHz, 8,75MHz
Designación de interfaz aérea	Wireless MAN-SC	WirelessMAN-Sca, WirelessMAN-OFDM, WirelessMAN-OFDMA, Wireless HUMAN	WirelessMAN-Sca, WirelessMAN-OFDM, WirelessMAN-OFDMA, Wireless Human
Implementación	Ninguna	256-OFDM como WiMAX fijo	OFDMA variable como WiMAX Móvil

Tabla 6.4. Diferencias entre los estándares 802.16.

El estándar 802.16 esencialmente estandariza dos aspectos de la interfaz aérea - la Capa 1 y la Capa 2 de control de acceso al medio (MAC).

Como se planteó previamente, la versión 802.16e usa OFDMA para transportar datos, soportando anchos de banda en el canal de entre 1.25 MHz y 20 MHz, consiguiendo hasta 2048 sub-portadoras. Soporta codificación adaptativa, de modo que en condiciones de buena recepción de la señal, se puede llegar a usar un mecanismo de codificación de alta eficiencia como 64 QAM, mientras que cuando la señal es más débil se usa un mecanismo de codificación más robusto como BPSK. En condiciones intermedias también se puede usar 16 QAM y QPSK.

Otra característica de Capa 1 es que incluye soporte para antenas MIMO (*Multiple-in Multiple-out*).

Aunque el estándar permite operaciones en cualquier banda desde los 2 hasta los 66 GHz, las operaciones móviles funcionan mejor en las bandas más bajas, que son también las más demandadas, y por tanto, las más caras.

La MAC 802.16 describe unas capas de convergencia similares a las tecnologías basadas en cable, como Ethernet, ATM e IP y cómo se clasifican los datos. También cómo se establecen las conexiones seguras, usando un intercambio confiable de clave durante la autenticación y encriptación usando el método AES (*Advanced Encryption Standard* – Estándar de Cifrado Avanzado) durante la transferencia de datos.

Además, las características de la Capa 2 incluyen mecanismos de ahorro de energía como el modo dormir (*sleep mode*) y el modo inactivo (*idle mode*), y mecanismos de traspaso.

Una característica del 802.16 es que se trata de una tecnología orientada a conexión. La estación de abonado no puede transmitir datos hasta que la estación base le asigne un canal. Esto permite al 802.16e ofrecer un soporte robusto para QoS (Quality of Service - Calidad de Servicio).

El estándar IEEE 802.16e fue ratificado en diciembre de 2005. Se trata de una extensión de IEEE 802.16-2004, que cubre las Capas 1 y 2, incluyendo el funcionamiento combinado fijo y móvil en bandas licenciadas. Por ejemplo, permite que un usuario móvil siga conectado mientras se desplaza a una velocidad de 120 a 150 km/h. La Capa 1 de Wi-Max móvil está basada sobre la tecnología OFDM escalable, lo que resulta en menor complejidad de equipamiento y administración de movilidad más simple, debido a un núcleo de red todo IP.

La movilidad Wi-Max debe superar algunas dificultades. Por ejemplo, la disponibilidad y diversidad de dispositivos comerciales, la demora en la introducción efectiva al mercado, y los altos costos iniciales que limitan su crecimiento.

Además, en algunos mercados la disponibilidad de espectro es limitada. Por este motivo, la demanda actual para

Wi-Max es principalmente para servicios MAN fijos, en especial en las regiones no atendidas o mercados en desarrollo.

Por otro lado, la demanda para datos inalámbricos está en crecimiento, pero aún es limitado. Los operadores móviles ven la necesidad de una topología inalámbrica sólo para datos cuando la demanda sea mayor.

La demanda puede manejar otras alternativas adicionales del espectro para servicios de datos móviles inalámbricos. Además, debe tenerse en cuenta que Wi-Max no suplanta ni suplantará otras tecnologías inalámbricas. Es decir, no reemplazará Wi-Fi en las redes LAN, y al menos por ahora, las tecnologías celulares seguirán siendo útiles para voz y datos en las redes WAN.

Se espera que Wi-Max se transforme en el estándar dominante para MAN Inalámbricas. Para ello, es necesario que los productos Wi-Max que salgan al mercado para los usuarios finales sean fáciles de instalar. Además, deben considerarse los aspectos de implementación sobre orientación y configuración. Mientras, Wi-Fi prevalecería en LAN Inalámbricas y la tecnología celular en dispositivos móviles livianos.

6.3 Ejercitación

Ejercicio n° 1:

Explicar qué es y para qué se utiliza Metro Ethernet.

Ejercicio n° 2:
Explicar qué diferencias hay entre EPL y EVPL, y cuándo usaría cada una.

Ejercicio n° 3:
Indicar algunos servicios de Metro Ethernet.

Ejercicio n° 4:
Comparar los distintos estándares de WI-MAX.

Ejercicio n° 5:
Qué ventajas y desventajas pueden existir entre FDD y TDD en WI-MAX?

6.4 Bibliografía y referencias

6.4.1 Libros impresos

- William Stallings, “Data and Computer Communications”, Pearson Education, 10° Ed., 2014.
- William Stallings y Thomas Case, “Business Data Communications”, Pearson Education, 7° Ed., 2013.
- William Stallings, “Data and Computer Communications”, Pearson Education, 8° Ed., 2009.
- CCNA de CISCO Press.
- William Stallings, “Wireless Communications & Networks”, Prentice Hall, 2° Ed., 2005.

- Michael Daoud Yacoub “Wireless Technology: Protocols, Standards, and Techniques”, CRC Press, 2002.
- William Stallings, “Local and Metropolitan Area Networks”, Prentice Hall, 6° Ed., 2000.
- Uyless Black, “Tecnologías Emergentes para Redes de Computadoras”, Ed. Prentice-Hall, 1999.
- D. Comer, “Redes Globales de Información con Internet y TCP/IP”, Ed. Prentice-Hall, 3° Ed., , 2000.
- Request for Comments referidos a la temática.
- Artículos de revistas (IEEE, ACM, etc.) referidos a la temática.

6.4.2 Enlaces y Referencias

- Respuestas de expertos de Cisco en el funcionamiento de Metro Ethernet
  https://supportforums.cisco.com/community/netpro/service-providers/metro
- Forum de Metro Ethernet
  http://metroethernetforum.org/
- Informes del Sector de Radiocomunicaciones de la UIT
  http://www.itu.int/es/ITU-R/Pages/default.aspx
- Tecnologías satelitales
  http://www.etsi.org/technologies-clusters/technologies/satellite
- Forum de Wi-Max http://www.wimaxforum.org/

Índice de Contenidos:

Capítulo 1 Redes LAN y WAN
1.1 Introducción a las Redes de Datos 8
1.2 Clasificación de las Redes de Datos.....9
1.3 Tendencias de las Redes de Datos.....11
1.4 Símbolos de los dispositivos de red 12

Capítulo 2 Conjunto de Protocolos TCP/IP
2.1 Introducción.....16
2.1.1 Tecnología de Interconexión.....16
2.1.2 Arquitectura de Protocolos.....17
2.1.3 Arquitectura de Protocolos TCP/IP e Internet.....21
2.1.4 Evolución de Internet.....23
2.2 El Modelo OSI.....24
2.3 Familia de Protocolos de Internet o TCP/IP 26
2.3.1 Introducción.....26
2.3.2 Capas de TCP/IP 29
2.3.3 Algunas consideraciones importantes sobre TCP/IP..31
2.3.4 Conjunto de Protocolos TCP/IP.....33
2.4 Bibliografía y Referencias.....35
2.4.1 Libros impresos 35
2.4.2 Enlaces y referencias 35

Capítulo 3 Conmutadores, VLANs y STP
3.1 Conmutador 38
3.1.1 Dispositivos en Redes LAN 38
3.1.2 Rendimiento de la Red 42
3.1.3 Almacenamiento y Técnicas de Conmutación en Conmutadores.....45
3.1.4 Dominios de Colisión y Difusión con Conmutadores..46
3.1.5 Configuración de Conmutadores 51
3.2 ARP - Protocolo de Resolución de Direcciones 55
3.3 VLANs - LANs Virtuales 60
3.3.1 Visión General 60
3.3.2 Clasificación de VLANs 65
3.3.3 Etiquetas y troncales 66

3.3.4 Configuración de VLANs 70
3.4 STP - Protocolo de Árbol de Expansión 73
3.4.1 Visión General 73
3.4.2 Algoritmo STP 78
3.4.3 Estados de los Puertos en STP 82
3.4.4 Evolución de las Versiones de STP 84
3.5 Ejercitación 86
3.6 Bibliografía y Referencias 92
3.6.1 Libros impresos 92
3.6.2 Enlaces y referencias 93

Capítulo 4 Encaminadores y Protocolos de Encaminamiento
4.1 Encaminadores 96
4.1.1 Introducción 96
4.1.2 Características Generales de los Encaminadores 96
4.1.3 CPUs, Memorias y Sistema Operativo de los Encaminadores 99
4.1.4 Puertos o Interfaces 103
4.1.5 Encaminador como Dispositivo de Capa 3 105
4.1.6 Instrucciones de Configuración Básicas 106
4.2 Protocolos de Encaminamiento y Encaminados 111
4.2.1 Introducción 111
4.2.2 Encaminamiento Adaptativo o Dinámico 116
4.2.3 Sistemas Autónomos y Protocolos IRP-ERP 119
4.2.4 Tipos de Encaminamientos: vector distancia, estado de enlace y vector-paso 122
4.2.5 Algoritmos de Encaminamiento 125
4.3 Ejercitación 129
4.4 Bibliografía y Referencias 133
4.4.1 Libros impresos 133
4.4.2 Enlaces y referencias 134

Capítulo 5 Protocolos de Encaminamiento RIP, OSPF y BGP
5.1 Protocolo RIP 138
5.1.1 Conceptos fundamentales en RIP 138
5.1.2 Evolución de RIP 142
5.2 Protocolo OSPF 145
5.2.1 Conceptos fundamentales en OSPF 145

5.2.2 Paquetes OSPF 149
5.2.3 Tipos de Encaminadores en OSPF 153
5.2.4 Concepto de Área OSPF 154
5.3 Protocolo BGP 157
5.3.1 Introducción 157
5.3.2 Conceptos fundamentales de BGP 166
5.3.3 Operación BGP 169
5.3.4 Mensajes BGP 176
5.3.5 Estados BGP 181
5.3.6 Atributos BGP 186
5.4 Ejercitación 190
5.5 Bibliografía y Referencias 197
5.5.1 Libros impresos 197
5.5.2 Enlaces y referencias 198

Capítulo 6 Tecnologías MAN Metro Ethernet y Wi-Max
6.1 Metro Ethernet 202
6.1.1 Introducción 202
6.1.2 Modelo de Referencia 207
6.1.3 Conexiones Virtuales Ethernet E-Line y E-LAN 210
6.1.4 Tecnologías de Transporte de Ethernet 212
6.2 Wi-MAx 216
6.2.1 Introducción 216
6.2.2 Estándares Wi-Max 217
6.2.3 Servicios y Tecnologías Wi-Max 219
6.2 4 Implementaciones Wi-Max 222
6.2.5 Relación de OFDM y los Estándares Wi-Max 223
6.3 Ejercitación 227
6.4 Bibliografía y Referencias 228
6.5.1 Libros impresos 228
6.5.2 Enlaces y referencias 229

Índice 231
Lista de Figuras 235
Lista de Tablas 241

Lista de Figuras:

Capítulo 1 Redes LAN y WAN
Figura 1.1 Ejemplo de red LAN 10
Figura 1.2 Ejemplo de red WAN 11
Figura 1.3 Símbolos de los dispositivos de red 14

Capítulo 2 Conjunto de Protocolos TCP/IP
Figura 2.1 Capas del Modelo de Referencia OSI.....25
Figura 2.2 Proceso de encapsulamiento en el Modelo OSI ..26
Figura 2.3 Vista de las capas del Modelo OSI
y el Conjunto TCP/IP.....28
Figura 2.4 Encapsulamiento y nombres de los mensajes
TCP/IP 28
Figura 2.5 Vista resumida del conjunto de protocolos
TCP/IP por Capas.....34

Capítulo 3 Conmutadores, VLANs y STP
Figura 3.1 Dispositivos de red en relación al modelo OSI ...39
Imagen 3.1 Fotografía de encaminadores 40
Imagen 3.2 Fotografía de conmutadores.....41
Figura 3.2 Requerimientos de ancho de banda LAN
según las aplicaciones 43
Figura 3.3 Diferentes técnicas de conmutación
de un conmutador 46
Figura 3.4 Red con 4 subredes usando hubs 47
Figura 3.5 Ejemplo de tráfico de tramas de unidifusión,
de difusión y de multidifusión.....49
Figura 3.6 Conmutador de Capa 2 en relación
al modelo OSI 50
Figura 3.7 Conmutador de Capa 3 en relación
al modelo OSI 50
Figura 3.8 Administración local del conmutador
a través de puerto consola 51
Figura 3.9 Panel frontal de un conmutador.....52
Figura 3.10 Instrucción que da la Tabla
de direcciones MAC del conmutador 54
Figura 3.11 Activación del Servidor HTTP del conmutador .55

Figura 3.12 Formato de la trama Ethernet 56
Figura 3.13 Las subredes 172.16.10 y 172.16.20
separadas por un encaminador 57
Figura 3.14 Ejemplos de VLANs dentro de una
organización 62
Figura 3.15 Configuración dinámica de VLANs 63
Figura 3.16 VLANs Extremo a Extremo 65
Figura 3.17 VLANs Geográficas 65
Figura 3.18 Ejemplo de troncal de VLANs 67
Figura 3.19 Etiquetamiento de paquetes de VLANs 68
Figura 3.20 Formato de trama 802.1Q 69
Figura 3.21 Creación de VLANs y asignación de puertos
en el conmutador 70
Figura 3.22 Verificación de VLAN con la instrucción
show vlan brief 71
Figura 3.23 Verificación de VLAN con la instrucción
show vlan 72
Figura 3.24 Configuración IP y de la puerta de enlace
del conmutador 72
Figura 3.25 Configuración de acceso remoto
del conmutador con Telnet 73
Figura 3.26 Configuración típica para usar STP 75
Figura 3.27 Bloqueo de enlaces usando STP 76
Figura 3.28 Formato del ID de Bridge (BID) 77
Figura 3.29 Formato extendido del ID de Bridge (BID) 77
Figura 3.30 Evolución del protocolo STP 85

Capítulo 4 Encaminadores y Protocolos de Encaminamiento
Figura 4.1 Ejemplo de interconexión de redes LAN
usando encaminadores 98
Figura 4.2 Ejemplo de encaminamiento de un paquete
usando encaminadores 99
Figura 4.3 Instrucciones en el modo comando
sobre un encaminador 101
Figura 4.4 Verificación de las características principales
del encaminador 103
Figura 4.5 Puertos o interfaces en un encaminador 104

Figura 4.6 Proceso de reenvío de paquetes a través de la red 105
Figura 4.7 Procesos de encapsulamiento y desencapsulamiento 106
Figura 4.8 Configuración básica de intefaz fastethernet del encaminador 107
Figura 4.9 Configuración básica de interfaz serial del encaminador 107
Figura 4.10 Instrucción de verificación de las interfaces fastethernet 107
Figura 4.11 Instrucción de verificación de las interfaces s seriales 108
Figura 4.12 Instrucción de verificación del archivo de configuración del encaminador 109
Figura 4.13 Instrucción de verificación de tabla de encaminamiento del encaminador..... 110
Figura 4.14 Ejemplo de interconexión de 5 Redes usando 8 Encaminadores 113
Figura 4.15 Tablas de encaminamiento de los Encaminadores A, B y C 115
Figura 4.16 Tablas de encaminamiento de los Encaminadores D, E y F 115
Figura 4.17 Tablas de encaminamiento de los Encaminadores G y H y de la PC X 116
Figura 4.18 Ejemplo interconexión de los Sistemas Autónomos 1 y 2 120
Figura 4.19 Ejemplos de Protocolos IRP y ERP..... 122
Figura 4.20 Evolución de los Protocolos de Encaminamiento 124
Figura 4.21 Grafo que describe nodos de la red y los costos de enlaces..... 126
Figura 4.22 Aplicación algoritmo Dijkstra para llegar del nodo 1 al 6 127
Figura 4.23 Ejemplo de aplicación del algoritmo Bellman Ford 128

Capítulo 5 Protocolos de Encaminamiento RIP, OSPF y BGP
Figura 5.1 Ejemplo que ilustra problema RIP sobre cuenta al infinito 141
Figura 5.2 Formato estandarizado de un paquete RIP 144
Figura 5.3 Algoritmo de inundación 147
Figura 5.4 Ejemplo de un grafo dirigido que muestra la topología de la red 148
Figura 5.5 Uso del Algoritmo de Dijkstra de OSFP 149
Figura 5.6 Formato estandarizado de un paquete OSPF ... 150
Figura 5.7 Encapsulamiento de un paquete OSPF 151
Figura 5.8 Interior de un paquete OSPF del tipo Hello..... 152
Figura 5.9 Inundación de paquetes OSFP en una red multiacceso 154
Figura 5.10 División de un sistema autónomo en áreas ... 155
Figura 5.11 Aplicación con los diferentes tipos de encaminadores OSPF..... 157
Figura 5.12 Esquema aproximado de la organización de los ISPs..... 158
Figura 5.13 Ejemplo de la conexión de distintos Sistemas Autónomos 160
Figura 5.14 Distribución de los Registros Regionales de Internet RIR 162
Figura 5.15 Distribución de asignación de números de AS de 16 bits (junio de 2015) 163
Figura 5.16 Distribución de asignación de números de AS de 16 bits (1999-2015)..... 163
Figura 5.17 Distribución de asignación de números de AS de 32 bits (junio de 2015) 164
Figura 5.18 Distribución de asignación de números de AS de 32 bits (1999-2015)..... 165
Figura 5.19 Ejemplo de uso de BGP..... 168
Figura 5.20 Comunicación entre el sistema autónomo 7 y el 1 170
Figura 5.21 Trama conteniendo un paquete BGP..... 171
Figura 5.22 Cuatro ejemplos de posibles configuraciones con BGP 173
Figura 5.23 Ejemplo de sistema autónomo de no tránsito 176

Figura 5.24 Instrucciones OSPF para establecer la relación vecino 177
Figura 5.25 Cabecera de Paquete BGP 178
Figura 5.26 Campos de Código de Error mensaje Notification 181
Figura 5.27 Máquina de estados finito de una sesión BGP 183
Figura 5.28 Instrucción de verificación de vecinos BGP del encaminador 186

Capítulo 6 Tecnologías MAN Metro Ethernet y Wi-Max
Figura 6.1 Modelo de referencia Metro Ethernet 208
Figura 6.2 Servicio Ethernet E-Line 211
Figura 6.3 Servicio Ethernet E-LAN 212
Figura 6.4 Soluciones de Capa 1 y 2 para el transporte de Ethernet 213
Figura 6.5 Perfiles de ancho de banda en el ETM 215

Lista de Tablas:

Capítulo 3 Conmutadores, VLANs y STP
Tabla 3.1 Diversas alternativas de la instrucción show 53
Tabla 3.2 Formato de mensajes de STP.....79
Tabla 3.3 Estado de los puertos STP.....83

Capítulo 5 Protocolos de Encaminamiento RIP, OSPF y BGP
Tabla 5.1 Códigos de atributos soportados por CISCO 189

Capítulo 6 Tecnologías MAN MetroEthernet y Wi-Max
Tabla 6.1 Cuadro comparativo entre Ethernet,
Frame Relay y ATM..... 205
Tabla 6.2 Resumen de las tecnologías basadas en el
estándar 802.11 218
Tabla 6.3 Resumen de las tecnologías basadas en el
estándar 802.16 219
Tabla 6.4 Diferencias entre los estándares 802.16 224