

REDES ADMINISTRATIVAS

Apuntes de la cátedra

01/08/2021

UAI

Prof. Ing. Jorge Colombo



Contenido

CAPITULO 1	13
Introducción a las redes WAN	13
¿Por qué una WAN?	14
Son necesarias las WAN?	14
Internet.....	15
Intranet	15
Topologías WAN.....	16
Punto a punto.....	16
De estrella.....	16
Malla completa.....	17
Topología de seguridad preventiva doble	17
WAN en el modelo OSI	18
Terminología común de WAN	19
Dispositivos WAN	20
Requisitos de diseño WAN.	22
Comutación de circuitos	22
Comutación de paquetes	23
Opciones de conexión de enlace WAN	24
Infraestructura de la red del proveedor de servicios.....	25
Líneas arrendadas	26
Frame Relay.....	27
ATM	27
WAN Ethernet	29
MPLS.....	30
VSAT	30
DSL.....	31
Cable	31
Tecnología inalámbrica	33
Celular 3G/4G	33
Tecnología VPN.....	34
Elección de una conexión de enlace WAN	36
¿Cuál es el propósito de la WAN?	36
¿Cuál es el alcance geográfico?	36

¿Cuáles son los requisitos de tráfico?	36
Ventajas y desventajas de una WAN.....	37
Protocolos de encapsulación WAN	37
Encapsulación HDLC.....	38
Tipos de tramas HDLC	38
Conceptos de PPP	40
¿Qué es PPP?	40
Arquitectura de capas PPP	42
Protocolo de control de enlace (LCP)	43
Protocolo de control de red (NCP).....	43
Funcionamiento de LCP	44
Establecimiento del enlace	45
Mantenimiento del enlace	45
Terminación del enlace.....	46
Paquete LCP	47
Proceso NCP.....	47
Ejemplo de IPCP	48
Opciones de configuración del PPP	49
Habilitación de PPP en una interfaz	50
Comandos de compresión de PPP.....	50
Comando de control de calidad del enlace PPP	51
Comandos de PPP multilink	52
Verificación de la configuración de PPP	53
Protocolos de autenticación PPP.....	54
Autenticación PAP	54
Autenticación CHAP.....	55
Configuración de PPP con PAP	57
Configuración de PPP con CHAP	57
CAPITULO 2	59
Redes ópticas de transporte.....	59
Estructuras de multicanalización	59
Introducción a SONET/SDH.	59
Definiciones importantes.....	59
Qué es SONET/SDH.	60

Velocidades SONET/SDH	61
Arquitectura de la Red	63
Anillo de fibra con diferentes conexiones.....	63
Conexión entre anillos.....	63
Estándares SDH/SONET.....	64
Aplicaciones de SONET/SDH.	64
Componentes de una red síncrona.....	66
Gestión de los elementos de la red.....	66
Estructura de la trama STM-1	67
Medidas en las redes SDH:.....	68
Medida del tiempo de respuesta APS.	68
Características principales de SDH.....	68
Desventajas de SDH.....	69
Sincronización de las señales digitales.....	69
Sincronización Jerárquica.....	70
SONET Sincronizado.	70
Elementos de la Red SONET.....	70
La señal básica de SONET.....	71
Estructura de trama de la señal STS-1.....	71
Esquema de la capacidad útil.....	72
Sincronización.	72
Configuración de la red SONET.	72
Beneficios de la Red SONET	73
Ventajas de SONET.....	73
Futuro de las redes de transporte.....	74
SDH de nueva generación	74
Perspectivas de la Tecnología SDH.....	74
DWDM(Dense Wavelength Division Multiplexing)	76
Que es y motivos de invención.	76
Historia	76
Componentes y funcionamiento.....	77
Funciones del sistema	77
Funcionamiento de un Transponder Basado en el Sistema DWDM.....	78
Topologías y esquemas de protección para DWDM.....	80

Protección Óptica	80
FUTURO DE DWDM	80
Ventajas DWDM	80
Desventajas DWDM	81
CWDM (Coarse wavelength Division Multiplexing),	82
Topologías	83
Ventajas.....	84
Mapa mental	85
Redes Ópticas de Nueva Generación	86
Componentes y Redes Ópticas.....	86
Redes Ópticas Pasivas. (PON- Passive Optical Networks)	86
Características comunes de los sistemas PON.....	87
Breve descripción para las topologías PON.....	88
Variantes de Redes Ópticas: APON, BPON y GPON.	89
Nuevo modelo para Red de Transporte	90
FDDI Fiber Distributed Data Interface (Interfaz de Datos Distribuida por Fibra).....	91
Características	91
Historia	92
Norma.....	92
Estructura	92
Topología Funcional	93
Arquitectura de red	94
Aplicaciones.....	94
Problemas de FDDI.....	95
FDDI en la actualidad.....	95
CAPITULO 3	97
Introducción a Frame Relay	97
Introducción:	97
Circuitos Virtuales Frame Relay	98
Circuitos Virtuales Comutados.....	98
Circuitos Virtuales Permanentes.....	98
Identificador de Conexión del Enlace de Datos	99
Mecanismos de control de saturación	99
BIT DE	100

Verificación de errores en Frame Relay	100
Interface LMI	100
Tecnología:	100
Estructura OSI de la red Frame Relay.....	101
Encapsulación Frame Relay.....	101
Topologías de Frame Relay	103
Topología en estrella (hub-and-spoke)	103
Topología de malla completa	104
Topología de malla parcial	104
Asignación de direcciones de Frame Relay	105
ARP inverso	105
Asignación dinámica.....	105
Asignación estática de Frame Relay	106
Configuración de la asignación estática	106
Interfaz de administración local (LMI)	107
Verificación del funcionamiento de Frame Relay: operaciones de LMI	109
Verificación del funcionamiento de Frame Relay: estado de PVC	109
Verificación del funcionamiento de Frame Relay: ARP inverso	110
La contratación:.....	111
Velocidad de acceso y velocidad de información comprometida	111
Sobresuscripción	112
Ráfaga.....	112
Comandos de configuración básica de Frame Relay.....	113
Configuración de un mapa estático Frame Relay	115
Verificación de un mapa estático de Frame Relay	115
Configuración de las subinterfaces punto a punto	115
Configuración de las subinterfaces punto a punto	116
Mapa mental	118
CAPITULO 4	119
Introducción a VPN	119
Aspectos básicos de las VPN	119
Beneficios de las VPN	120
Los beneficios de una VPN incluyen lo siguiente:	120
Tipos de VPNs.....	121

VPN de sitio a sitio.....	121
VPN de acceso remoto	122
Qué es GRE	123
Características de GRE.....	124
Las características de GRE son las siguientes:.....	124
Configuración de túneles GRE.....	125
Comandos de configuración de túneles GRE	125
Descripción de los comandos.....	126
Verificación del túnel GRE.....	127
IPsec	128
Seguridad de protocolo de Internet.....	128
Estructura IPsec.....	129
Confidencialidad.....	129
Cifrado simétrico	130
Cifrado asimétrico	131
Integridad de datos	132
Hay dos algoritmos HMAC comunes:.....	134
Autenticación	134
Tipos de VPN de acceso remoto	137
VPN de acceso remoto con IPsec	138
Mapa Conceptual	140
CAPITULO 5	143
Protocolo BGP	143
Tipos de conexiones a ISPs.....	144
Singlehommed ISP Connectivity.....	144
Dual-Homed ISP Connectivity	144
Multihomed ISP Connectivity.....	145
Sistema Autónomo de transito	145
Multihomed mejor ruta	146
IBGP y EBGP.....	147
Problemas de Update.....	147
Tipos de Sistemas Autónomos	147
Sistema autónomo de transito.....	147
Sistema Autónomo de no transito	148

¿Cuándo usar BGP?	149
Configuración de vecinos	149
Regla de sincronización de BGP	150
Funcionamiento del proceso BGP	151
Esquema funcional del proceso BGP:.....	151
Estados de un Neighbor BGP.....	152
Tablas de BGP.....	152
Tipos de mensajes de BGP	153
Mensaje Update, intercambio de tabla de enrutamiento.	154
Estados de un Neighbor BGP.....	154
Verificación rápida de estado de vecinos.....	154
Atributos BGP	154
Atributo AS-PATH	156
Atributo Next-hop	156
Atributo Origin	156
Atributo Local Preference	156
Atributo MED	157
Atributo WEIGHT.....	157
Selección de la mejor ruta:.....	157
Configurando BGP	158
Anunciando redes	158
Ejemplo Adyacencia con loopbacks.	159
Actualizar políticas aplicadas a rutas.	160
Hard reset:.....	160
Soft reset:.....	160
Route refresh:	160
EBGP Multihop	161
Dirección del próximo salto	161
Peer groups	163
Autenticación	163
Filtro de rutas con lista de distribución.....	164
Comandos de verificación de BGP	165
Identificando atributos.....	165
Comprobando mejor ruta	165

CAPITULO 6	166
Introducción a MPLS.....	166
CELL SWITCHING ROUTER (CSR).....	167
IP SWITCHING.....	167
TAG SWITCHING.....	167
Estructuras	168
MPLS e IP	168
ARQUITECTURA MPLS	169
Componentes.....	169
Componentes de Envío y Control:.....	171
Etiquetas y Asociación de Etiquetas.....	172
Formato genérico de la etiqueta MPLS.....	173
Ventajas del reenvío basada en etiquetas	174
Tablas de enrutamiento y envío.....	174
Creación y clasificación de etiquetas.	175
Clasificación de etiquetas:.....	175
Distribución de etiquetas.....	176
Unión de etiquetas.....	177
Pila de etiquetas.....	177
Mecanismos de señalización.....	177
Imposición de etiquetas en el contorno de la red MPLS	178
Clases equivalentes de envío (FEC).-	178
Enrutamiento MPLS	179
Descripción del proceso LDP entre dos LSR	181
Trayectorias comutadas de etiquetas (LSP):.....	181
Descripción Funcional de las operaciones MPLS.	182
Funcionamiento del envío de paquetes en MPLS.....	182
Componente de control en MPLS.	183
Ejemplo: Envío de un paquete IP.	184
Funcionamiento de MPLS en modo Trama	185
Commutación de etiquetas en MPLS en modo trama	185
Convergencia en una red MPLS.....	186
Interacción de MPLS con el Protocolo de Gateway Fronterizo.....	186
Aplicaciones.....	186

Ingeniería de tráfico	186
Diferenciación de niveles de servicio mediante clases (CoS).....	186
Servicios de Redes Privadas Virtuales (VPN).....	187
CAPITULO 7	188
Introducción a los servicios MetroEthernet.....	188
Introducción	188
Topología de la red	189
¿Qué es un servicio ethernet?.....	189
Conexión de Ethernet Virtual (EVC).....	190
Definición Servicio Ethernet	190
Tipos de servicio Ethernet	191
Tipo de Servicio Línea de Ethernet _ Punto a punto.....	191
Tipo de Servicio LAN de Ethernet _ Multipunto a Multipunto.....	192
Configuración Punto a Punto en E-LAN	193
Interface física de Ethernet	194
Características del ancho de banda	194
Parámetros	194
Servicio Color De La Trama	195
CIR y CBS.....	195
EIR y EBS	195
SOPORTE VLAN TAG.....	196
Servicio de multiplexación	196
CAPITULO 8	198
Introducción a las redes de acceso residencial.....	198
El bucle de abonado y las tecnologías dsl	198
Características del bucle.....	198
Atenuación	199
Efecto pelicular (Skin effect)	199
Ruido	200
Capacidad máxima del canal: Teorema de Shannon – Hartley.....	201
Tecnologías xDSL	201
Línea de abonado digital de alta velocidad (HDSL).....	202
Línea de abonado digital simétrica (SDSL)	202
Línea de abonado digital de alta velocidad simétrica (G.SHDSL).....	203

Línea de abonado digital asimétrica (ADSL).....	203
Alcance	205
Arquitecturas de Red	205
DSLAM	207
Elementos de la red.....	207
Modulación en ADSL	208
Redes CATV	215
RED HFC (Hibrid fiber-coaxial).....	215
Introducción	215
¿Qué es una red HFC?	216
Canal de retorno:	217
El cable MODEM:.....	218
Topologías y elementos de las redes HFC.....	219
Cabecera.....	219
CMTS	220
Fibra Óptica	221
Nodos de Fibra	221
Red de distribución Coaxial.....	221
Equipos Terminales	221
Telefonía.....	222
DOCSIS.....	223
FTTX ¿Qué es?	224
Funcionamiento:	224
Retorno.....	224
Las arquitecturas FTTX más importantes son:	225
FTTH (home).....	225
FTTC (Fiber To The Curb):.....	225
FTTB (building).....	226
FTTN (node o neighborhood).	226
Las diferentes arquitecturas.....	227
Una visión general de la red de acceso FTTH con GPON	227
Arquitectura de la red de acceso FTTH con GPON.....	228
La arquitectura FTTB	229
FTTH vs FTTB	230

Mapa Conceptual	231
CAPITULO 9	234
Introducción a las redes Wirless Wan	234
Introducción	234
Motivos de desarrollo	234
GSM	234
Arquitectura del GSM.....	235
3G	236
4G (LTE)	236
Movilidad y Portabilidad	240
IP Móvil.....	240
Introducción	240
¿Qué es IP móvil?	240
Conceptos básicos.....	240
Descripción general.....	241
Integración de los protocolos del IETF en 3G.....	241
Terminología de IP móvil.....	242
Ventajas de IP móvil	242
Funcionamiento de IP móvil.....	243
Proceso de IP móvil (simplificado)	243
Comunicación de hosts de la HN con el MN	244
Que es WIMAX?	246
Componentes de una red WIMAX	247
Topología de red	247
Arquitectura Punto-Multipunto (PMP).	248
Redes Enmalladas (Mesh).	250
Dispositivos usados para establecer una conexión por WiMAX.....	251
CPE.....	251
Tarjeta WiMAX	251
Equipos para Terminales del Abonado:	252
CARACTERISTICAS TECNICAS: OFDM.....	252
OFDMA	253
Funcionamiento	253
Estación Base	254

Como conectar la Torre base y el CPE.....	254
CERTIFICACIONES Y ESTANDARES	255
WiMAX Forum	255
Estándar 802.16 (WiMAX).....	255
Seguridad.....	255
Mapa Conceptual	257
CAPITULO 10.....	258
REDES DE NUEVA GENERACION (NGN).....	258
Concepto IMS	258
¿Porque IMS?	259
¿Qué es IMS?.....	260
Arquitectura del IMS	260
Identificador de recursos universal.....	262
Funcionalidad, precio y calidad	262
Principios tecnológicos.....	263
CAPITULO 11.....	265
Redes Definidas Mediante Software (SDN).....	265
Redes Definidas por Software (SDN).....	265
Cómo funciona SDN?.....	265
Arquitectura SDN	266
Plano de datos.....	267
Plano de control	270
Plano de gestión.....	271
Tipos de Switch OpenFlow	272
El Canal OpenFlow.....	272
Encripción TLS	272
El Controlador SDN OpenDayLight.....	273
Módulos de OpenDayLight.....	274
Mapa Conceptual	276
ANEXOS DE CONFIGURACION	277
10 comandos a configurar en un dispositivo nuevo	277

CAPITULO 1

Introducción a las redes WAN

Es posible clasificar a una red de distintas maneras de acuerdo a su alcance, la relación funcional de sus componentes y su método de conexión. La noción de red WAN se enmarca en la clasificación de una red según su alcance.

WAN es la sigla de Wide Area Network, una expresión en lengua inglesa que puede traducirse como Red de Área Amplia. Esto quiere decir que la red WAN es un tipo de red que cubre distancias de entre unos 100 y unos 1.000 kilómetros, lo que le permite brindar conectividad a varias ciudades o incluso a un país entero.

Las redes WAN pueden ser desarrolladas por una empresa o una organización para un uso privado, o incluso por un proveedor de Internet (ISP, Internet Service Provider) para brindar conectividad a todos sus clientes.

Por lo general, la red WAN funciona punto a punto, por lo que puede definirse como una red de paquete conmutado. Estas redes, por otra parte, pueden utilizar sistemas de comunicación de radio o satelitales.

Entre los componentes de la red WAN aparecen los equipos que se dedican a ejecutar los programas de usuario y que reciben el nombre de hosts; los Routers que concretan la división entre las líneas de transmisión y los elementos de conmutación; y las subredes formadas a partir de la interconexión de varios hosts.

Su velocidad de transmisión se encuentra entre 1 Mbps y 1 Gbps, aunque este último límite puede cambiar drásticamente con los avances tecnológicos. La red WAN se utiliza para establecer comunicaciones privadas y los principales medios de transmisión en los que se basa son la fibra óptica y el cable de teléfono. Ofrece una gran versatilidad para hacer modificaciones en el software y en el hardware de los equipos que vincula y además permite establecer conexiones con otras redes.

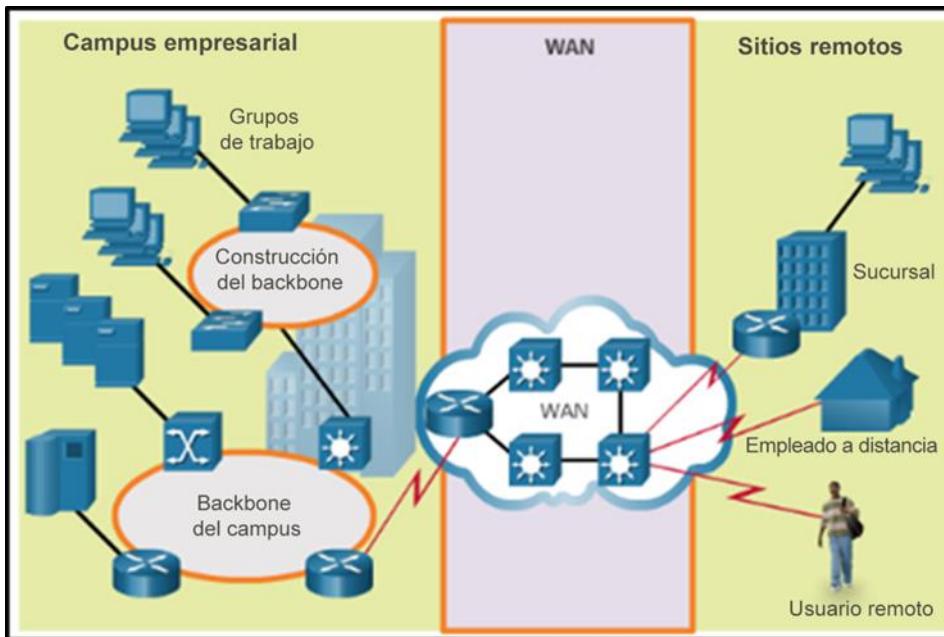
Entre las características que poseen las Redes WAN enumeraremos 6 características, estas son:

1. Suministra velocidad parcial y continua.
2. Operan dentro de un área geográfica extensa.
3. Conecta dispositivos separados por grandes distancias, incluso a nivel mundial.
4. Permite el acceso a través de interfaces seriales que operan a velocidades más bajas.
5. Tiene máquinas dedicadas a la ejecución de programas de usuario.
6. Posee elementos de conmutación de datos como por ejemplo, Routers.

¿Por qué una WAN?

Las WAN funcionan más allá del ámbito geográfico de una LAN.

Las WAN se usan para interconectar la LAN de la empresa a las LAN remotas en las sucursales y las ubicaciones de los empleados a distancia.



Una WAN es de propiedad de un proveedor de servicios. Para conectarse a sitios remotos, una organización debe pagar una tarifa para usar los servicios de red del proveedor. Los proveedores de servicios WAN incluyen empresas prestadoras de servicios, como una red telefónica, una empresa de cable o un servicio satelital. Los proveedores de servicios proporcionan enlaces para interconectar los sitios remotos, con el fin de transportar datos, voz y video.

En cambio, las LAN normalmente son de propiedad de una organización y se utilizan para conectar computadoras, periféricos y otros dispositivos locales en un único edificio u otra área geográfica pequeña.

Son necesarias las WAN?

Sin las WAN, las LAN serían una serie de redes aisladas. Las LAN proporcionan velocidad y rentabilidad para la transmisión de datos en áreas geográficas relativamente pequeñas. Sin embargo, a medida que las organizaciones se expanden, las empresas requieren capacidad de comunicación entre sitios geográficamente separados. Los siguientes son algunos ejemplos:

- Las oficinas regionales o las sucursales de una organización necesitan poder comunicarse y compartir datos con el sitio central.
- Las organizaciones necesitan compartir información con las organizaciones de los clientes. Por ejemplo, los fabricantes de software comunican regularmente información de producto y promocional a los distribuidores que venden los productos a los usuarios finales.
- Los empleados que viajan por negocios de la empresa con frecuencia necesitan acceder a información ubicada en las redes empresariales.
- Los usuarios de computadoras domésticas también necesitan enviar y recibir datos a través de distancias cada vez más grandes. Estos son algunos ejemplos:

- En la actualidad, los consumidores se comunican normalmente con los bancos, las tiendas y una variedad de proveedores de bienes y servicios a través de Internet.
- Para investigar para sus clases, los estudiantes acceden a índices de bibliotecas y publicaciones ubicados en otras partes del país y del mundo.

No se pueden conectar computadoras a través de un país, o del mundo, con cables físicos. Por lo tanto, las distintas tecnologías evolucionaron para admitir este requisito de comunicación. Internet se usa cada vez más como una alternativa económica a las WAN empresariales.

Existen nuevas tecnologías disponibles para las empresas, que tienen el fin de proporcionar seguridad y privacidad a las comunicaciones y transacciones a través de Internet. Las WAN, ya sea que se usen solas o en conjunto con Internet, permiten que las organizaciones y las personas cubran sus necesidades de comunicación en un área extensa.

Internetwork

Son mallas de redes interconectadas que cubren las necesidades de comunicación humanas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, La internetwork más conocida, es Internet.

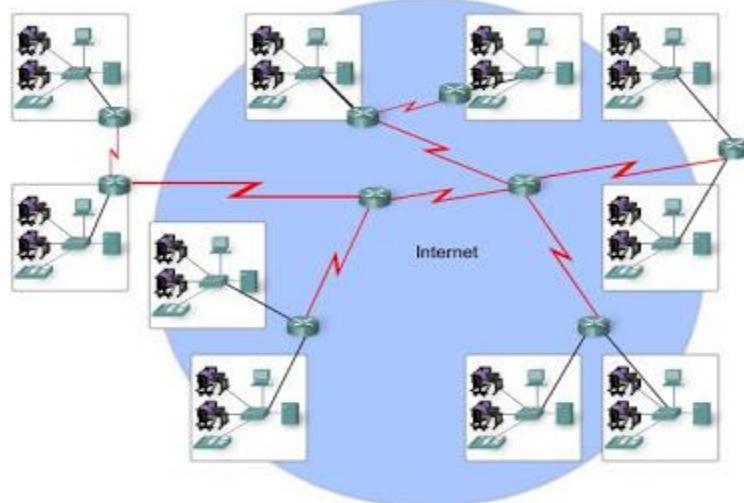
Internet se creó por la interconexión de redes de los Proveedores de servicios de Internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo. Garantizar la comunicación a través de esta infraestructura diversa.

Intranet

Es utilizado generalmente para una conexión privada de algunas LAN y WAN que pertenecen a una organización y que está diseñada para que puedan acceder solamente los miembros y empleados de la organización.

Nota: Es posible que los siguientes términos sean sinónimos: internetwork, red de datos y red. Una conexión de dos o más redes de datos forma una internetwork: una red de redes. También es habitual referirse a una internetwork como una red de datos o simplemente como una red, cuando se consideran las comunicaciones a alto nivel. El uso de los términos depende del contexto y del momento, a veces los términos pueden ser intercambiados.

Las LAN y WAN pueden estar conectadas a internetworks.



Topologías WAN

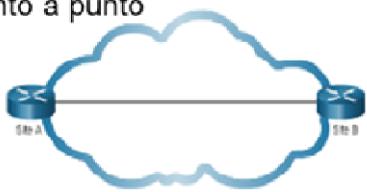
La interconexión de varios sitios a través de WAN puede incluir una variedad de tecnologías del proveedor de servicios y de topologías de WAN. Las topologías de WAN más comunes son:

- Punto a punto
- De estrella
- Malla completa
- De seguridad preventiva doble

Punto a punto

Una topología punto a punto, utiliza un circuito punto a punto entre dos terminales. Generalmente se trata de conexiones de líneas alquiladas dedicadas como las líneas T1/E1. Una conexión punto a punto implica un servicio de transporte de capa 2 a través de la red del proveedor de servicios. Los paquetes enviados desde un sitio se entregan a otro sitio y viceversa. Una conexión punto a punto es transparente para la red del cliente, como si hubiera un enlace físico directo entre dos terminales.

Punto a punto

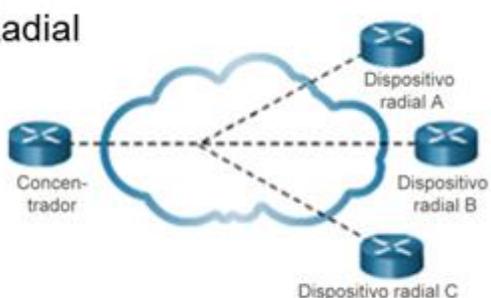


De estrella

Si se requiere una conexión de red privada entre varios sitios, entonces una topología punto a punto con múltiples circuitos punto a punto es una opción. Cada circuito punto a punto requiere su propia interfaz de hardware dedicada que requiere múltiples routers con tarjetas de interfaz WAN. Suele ser una opción costosa. Una opción menos costosa es una topología de punto a multipunto, también conocida como topología de estrella (hub and spoke).

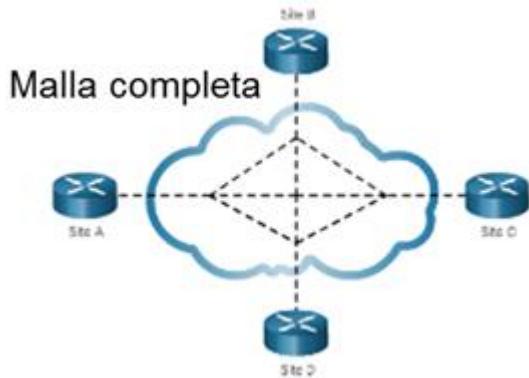
Con una topología de estrella (hub-and-spoke) una sola interfaz a hub puede ser compartida por todos los circuitos de radio. Por ejemplo, los sitios radiales se pueden interconectar a través del sitio de hubs mediante circuitos virtuales y subinterfaces enrutadas del hub. Una topología de estrella (hub and spoke) también es un ejemplo de una topología de localización simple. La topología de estrella (hub and spoke) de ejemplo, que consta de cuatro routers con un router como concentrador conectado a los otros tres routers radiales a través de una nube WAN.

Radial



Malla completa

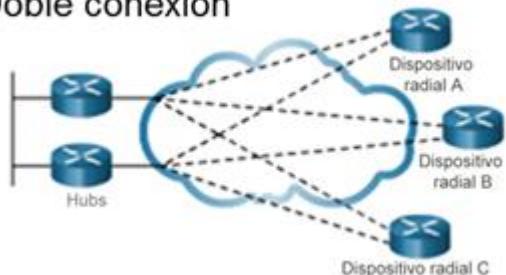
Una de las desventajas de las topologías de estrella es que la comunicación debe pasar a través del hub. Con una topología de malla completa con circuitos virtuales, cualquier sitio puede comunicarse directamente con cualquier otro sitio. La desventaja aquí es la gran cantidad de circuitos virtuales que se deben configurar y mantener. Una topología de malla completa de ejemplo, que consta de cuatro routers conectados entre sí a través de una nube WAN.



Topología de seguridad preventiva doble

Una topología de seguridad preventiva doble proporciona redundancia. Como vemos en el ejemplo, dos routers concentradores de seguridad preventiva doble están conectados en redundancia a tres routers radiales a través de una nube WAN. La desventaja de las topologías de seguridad preventiva doble es que son más costosas de implementar que las topologías de localización simple. Esto es porque requieren hardware de red, como routers y switches adicionales. Las topologías de seguridad preventiva doble son más difíciles de implementar porque requieren configuraciones adicionales y complejas. Sin embargo, la ventaja de las topologías de seguridad preventiva doble es que ofrecen redundancia de red, equilibrio de carga, computación o proceso distribuido mejorados, y la capacidad de implementar las conexiones del proveedor de servicio de respaldo.

Doble conexión



WAN en el modelo OSI

Las operaciones WAN se centran principalmente en la capa física (capa 1 del modelo OSI) y en la capa de enlace de datos (capa 2 del modelo OSI). En general, los estándares de acceso WAN describen métodos de distribución de la capa física y requisitos de la capa de enlace de datos. Los requisitos de la capa de enlace de datos incluyen asignación de direcciones físicas, control de flujo y encapsulamiento.

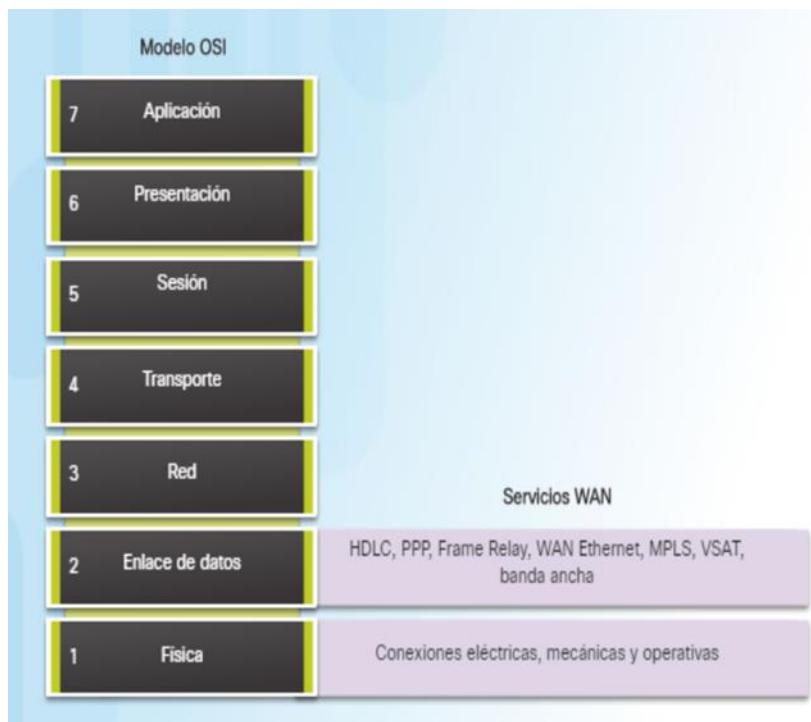
Varias autoridades reconocidas definen y administran los estándares de acceso WAN:

- Asociación de la Industria de Telecomunicaciones y Alianza de Industrias Electrónicas (TIA/EIA)
- Organización Internacional para la Estandarización (ISO)
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

Los protocolos de capa 1 describen la manera de proporcionar conexiones eléctricas, mecánicas, operativas y funcionales a los servicios de un proveedor de servicios de comunicación.

Los protocolos de capa 2 definen la forma en que se encapsulan los datos para la transmisión a una ubicación remota, así como los mecanismos para transferir las tramas resultantes. Se usa una variedad de tecnologías diferentes, como el protocolo punto a punto (PPP), Frame Relay y ATM. Algunos de estos protocolos usan el mismo entramado básico o un subconjunto del mecanismo de control de enlace de datos de alto nivel (HDLC).

La mayoría de los enlaces WAN son punto a punto. Por este motivo, no se suele utilizar el campo de dirección de la trama de capa 2.

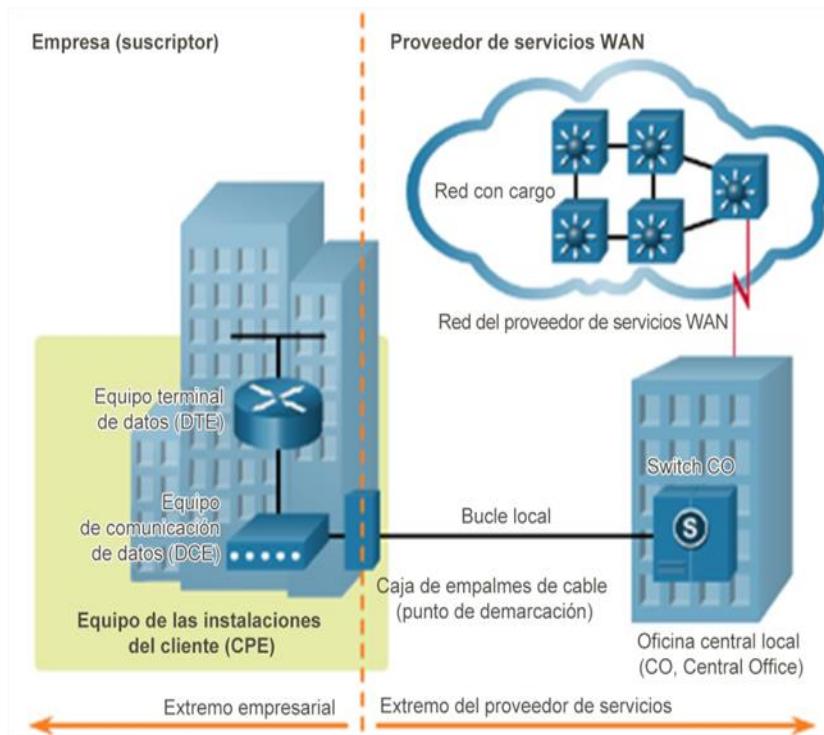


Terminología común de WAN

Una diferencia principal entre una WAN y una LAN es que, para usar los servicios de red de una prestadora de servicios WAN, una empresa u organización se debe suscribir a un proveedor de servicios WAN externo. WAN utiliza los enlaces de datos proporcionados por los servicios de la empresa para acceder a Internet y conectar diferentes ubicaciones de una organización entre sí. Estos enlaces de datos también se conectan con las ubicaciones de otras organizaciones, los servicios externos y los usuarios remotos.

La capa física de una WAN describe las conexiones físicas entre la red de la empresa y la red del proveedor de servicios. La figura muestra la terminología que se usa normalmente para describir las conexiones WAN:

- **Equipo de las instalaciones del cliente (CPE):** el CPE consiste de cables internos y dispositivos ubicados en el perímetro empresarial que se conectan a un enlace de una prestadora de servicios. El suscriptor es dueño del CPE o lo alquila al proveedor de servicios. En este contexto, un suscriptor es una empresa que obtiene los servicios WAN de un proveedor de servicios.
- **Equipo de comunicación de datos (DCE):** también llamado “equipo de terminación de circuito de datos”, el DCE consta de dispositivos que colocan los datos en el bucle local. Principalmente, el DCE proporciona una interfaz para conectar a los suscriptores a un enlace de comunicación en la nube WAN.
- **Equipo terminal de datos (DTE):** dispositivos del cliente que transmiten los datos desde un equipo host o la red de un cliente para la transmisión a través de la WAN. El DTE se conecta al bucle local a través del DCE.
- **Punto de demarcación:** es un punto establecido en un edificio o un complejo para separar el equipo del cliente del equipo del proveedor de servicios. En términos físicos, el punto de demarcación es la caja de conexiones del cableado, ubicada en las instalaciones del cliente, que conecta los cables del CPE al bucle local. Por lo general, se coloca de modo que sea de fácil acceso para un técnico. El punto de demarcación es el lugar donde la responsabilidad de la conexión pasa del usuario al proveedor de servicios. Cuando surgen problemas, es necesario determinar si el usuario o el proveedor de servicios es responsable de la resolución o la reparación.
- **Bucle local:** cable de cobre o fibra propiamente dicho que conecta el CPE a la CO del proveedor de servicios. A veces, el bucle local también se denomina “última milla”.
- **Oficina central (CO):** la CO es la instalación o el edificio del proveedor de servicios local que conecta el CPE a la red del proveedor.
- **Red interurbana:** consta de líneas de comunicación, switches, routers y otros equipos digitales, de largo alcance y de fibra óptica dentro de la red del proveedor de servicios WAN.



Dispositivos WAN

Existen muchos tipos de dispositivos que son específicos de los entornos WAN:

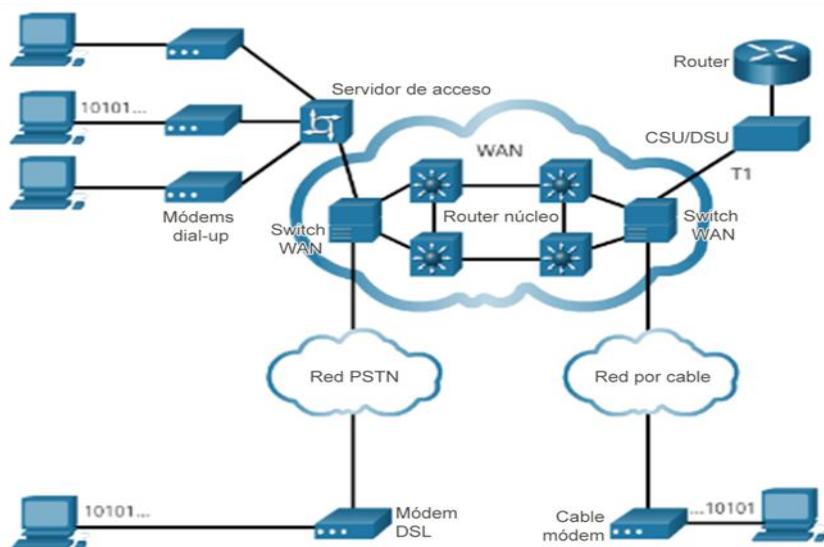
- **Módem de Internet por acceso telefónico:** los módems de banda de voz se consideran una tecnología WAN heredada. Un módem de banda de voz convierte (es decir, modula) las señales digitales producidas por una computadora en frecuencias de voz. Estas frecuencias luego se transmiten a través de líneas analógicas de la red de telefonía pública. En el otro lado de la conexión, otro módem convierte nuevamente los sonidos en una señal digital (es decir, los demodula) como entrada para una computadora o una conexión de red.
- **Servidor de acceso:** este servidor controla y coordina el módem de Internet por acceso telefónico, y las comunicaciones de los usuarios de entrada y salida telefónica. Considerado una tecnología antigua; un servidor de acceso puede tener una combinación de interfaces analógicas y digitales y admitir cientos de usuarios simultáneos.
- **Módem de banda ancha:** un tipo de módem digital que se utiliza con servicio de Internet por DSL o por cable de alta velocidad. Ambos funcionan de manera similar al módem de banda de voz, pero usan mayores velocidades de transmisión y frecuencias de banda ancha.
- **CSU/DSU:** las líneas arrendadas digitales requieren una CSU y una DSU. Una CSU/DSU puede ser un dispositivo separado, como un módem, o puede ser una interfaz en un router. La CSU proporciona terminación de la señal digital y asegura la integridad de la conexión mediante la corrección de errores y el monitoreo de la línea. La DSU convierte las tramas de línea en tramas que la LAN puede interpretar y viceversa.
- **Switch WAN:** un dispositivo de internetworking de varios puertos utilizado en las redes de los proveedores de servicios. Por lo general, estos dispositivos comutan el tráfico, como la retransmisión de tramas (Frame Relay) o ATM, y operan en la capa 2.
- **Router:** proporciona internetworking y puertos de interfaz de acceso WAN que se usan para conectarse a la red del proveedor de servicios. Estas interfaces pueden ser conexiones seriales, Ethernet u otras interfaces WAN. Con algunos tipos de interfaces WAN, se

requiere un dispositivo externo, como una DSU/CSU o un módem (analógico, por cable o DSL) para conectar el router al proveedor de servicios local.

- **Router principal/switch multicapa:** router o switch multicapa que reside en el centro o en el backbone de la WAN, en lugar de en la periferia. Para desempeñar esta función, un router o switch multicapa debe poder admitir varias interfaces de telecomunicaciones con la mayor velocidad usada en el núcleo de la WAN. También debe poder reenviar paquetes IP a máxima velocidad en todas esas interfaces. El router o switch multicapa también debe admitir los protocolos de routing que se utilizan en el núcleo.

Nota: la lista anterior no es exhaustiva y pueden ser necesarios otros dispositivos, según la tecnología de acceso WAN elegida.

Las tecnologías WAN se comutan por circuitos o por paquetes. El tipo de dispositivo usado depende de la tecnología WAN implementada.



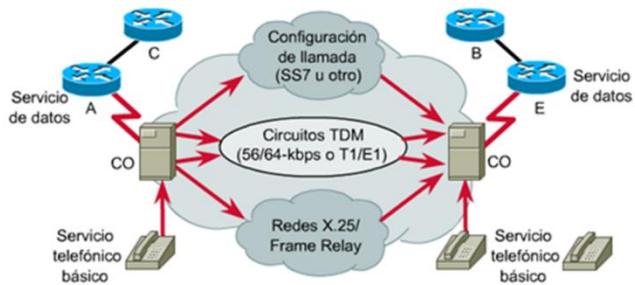
Requisitos de diseño WAN.

La comunicación WAN se produce entre áreas geográficamente separadas. Cuando una estación final local desea comunicarse con una estación final remota (es decir, una estación final ubicada en un sitio diferente), la información se debe enviar a través de uno o más enlaces WAN. Los routers dentro de las WAN son puntos de conexión en una red. Estos routers determinan la ruta más adecuada a través de la red para las corrientes de datos requeridas.

La comunicación WAN a veces se denomina servicio porque el proveedor de la red a menudo les cobra a los usuarios por los servicios WAN que proporciona.

Las tecnologías de conmutación por circuito y por paquete son dos tipos de servicios WAN, cada uno de los cuales presenta ventajas y desventajas. Por ejemplo, las redes conmutadas por circuito ofrecen a los usuarios anchos de banda dedicada al que otros usuarios no pueden acceder. Por otro lado, la conmutación por paquete es un método en el que los dispositivos de red comparten un solo enlace punto a punto para transportar paquetes desde un origen hasta un destino a través de una red portadora. Las redes conmutadas por paquete tradicionalmente han ofrecido mayor flexibilidad y uso más eficiente del ancho de banda de red que las redes conmutadas por circuito.

Proveedores de servicios WAN



Comutación de circuitos

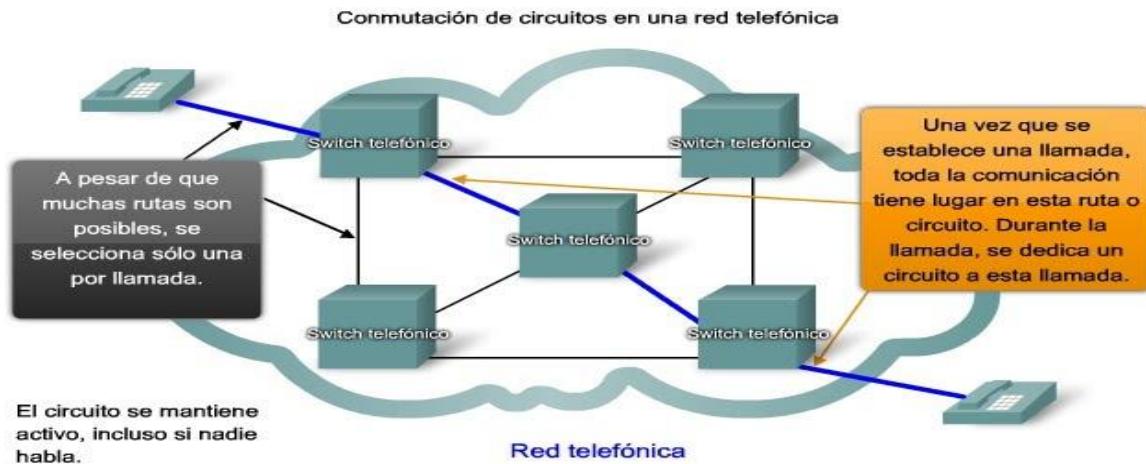
Las red de conmutación de circuitos son aquellas que establecen un circuito (o canal) dedicado entre los nodos y las terminales antes de que los usuarios se puedan comunicar. Específicamente, la conmutación de circuitos establece una conexión virtual dedicada para voz o datos entre un emisor y un receptor en forma dinámica. Antes de que la comunicación pueda comenzar, es necesario establecer la conexión a través de la red del proveedor de servicios.

Como ejemplo, cuando un suscriptor realiza una llamada telefónica, el número marcado se usa para establecer los switches en los intercambios a lo largo de la ruta de la llamada, de modo que haya un circuito continuo desde el origen hasta el destinatario de la llamada. Debido a la operación de conmutación utilizada para establecer el circuito, el sistema telefónico se denomina "red de conmutación de circuitos". Si los teléfonos se reemplazan por módems, el circuito de conmutación puede transportar datos informáticos.

Si el circuito transporta datos informáticos, es posible que el uso de esta capacidad fija no sea eficaz. Por ejemplo, si el circuito se utiliza para acceder a Internet, se produce una ráfaga de actividad en el circuito cuando se transfiere una página web. A esto lo podría seguir un período sin actividad, en el que el usuario

lee la página, y luego otra ráfaga de actividad cuando se transfiere la página siguiente. Esta variación en el uso, entre un uso nulo y un uso máximo, es típica del tráfico de la red de computadoras. Debido a que el suscriptor tiene uso exclusivo de la asignación de la capacidad fija, los circuitos de conmutación generalmente son una manera costosa de mover datos.

Los dos tipos más comunes de tecnologías WAN de conmutación de circuitos son la red pública de telefonía de conmutación (PSTN) y la red digital de servicios integrados (ISDN).



Existen muchísimos circuitos, pero son una cantidad finita. Durante los períodos de demanda pico, es posible que se denieguen algunas llamadas.

Comutación de paquetes

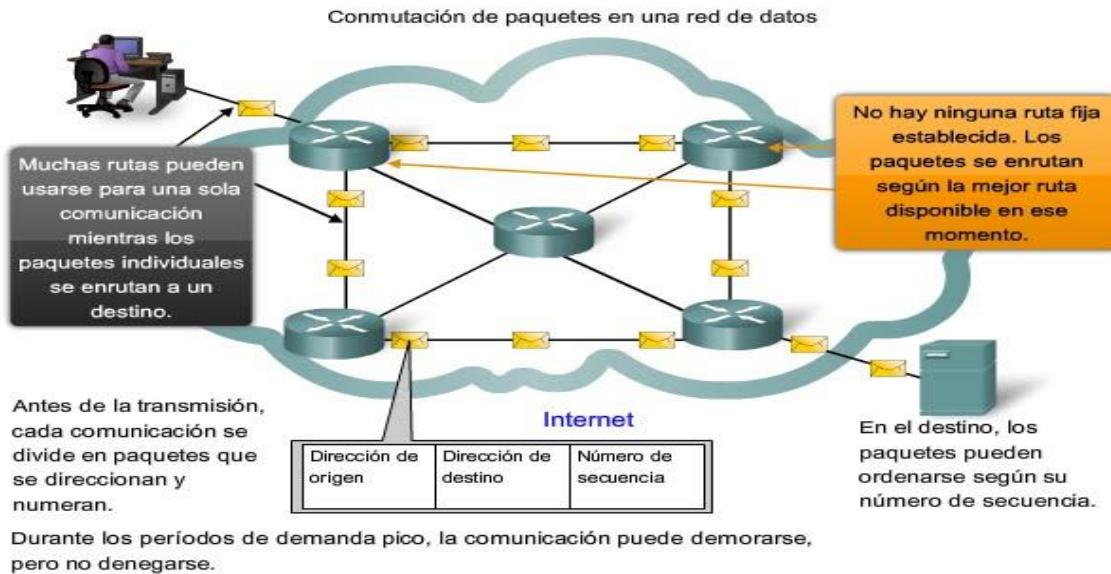
A diferencia de la conmutación de circuitos, la conmutación de paquetes divide los datos en tráfico en paquetes que se enrutan a través de una red compartida. Las redes con conmutación de paquetes no requieren que se establezca un circuito y permiten que muchos pares de nodos se comuniquen a través del mismo canal.

En una red de conmutación de paquetes (PSN), los switches determinan los enlaces a través de los que se deben enviar los paquetes según la información de direccionamiento en cada paquete. Los siguientes son dos enfoques de esta determinación de enlaces:

- **Sistemas sin conexión:** se debe transportar toda la información de direccionamiento en cada paquete. Cada switch debe evaluar la dirección para determinar adónde enviar el paquete. Un ejemplo de sistema sin conexión es Internet.
- **Sistemas orientados a la conexión:** la red predetermina la ruta para un paquete, y cada paquete solo tiene que transportar un identificador. El switch determina la ruta siguiente al buscar el identificador en las tablas almacenadas en la memoria. El conjunto de entradas en las tablas identifica una ruta o un circuito particular a través del sistema. Si el circuito se establece en forma temporal mientras un paquete viaja a través de él y luego se divide nuevamente, se lo denomina "circuito virtual" (VC). Un ejemplo de un sistema orientado a la conexión es Frame Relay. En el caso de Frame Relay, los identificadores utilizados se denominan "identificadores de conexión de enlace de datos" (DLCI).

Debido a que varios usuarios comparten los enlaces internos entre los switches, el costo del switching de paquetes es inferior al del switching de circuitos. Sin embargo, los retrasos (latencia) y la variabilidad de

retraso (vibración) son mayores en las redes de conmutación de paquetes que en las redes de conmutación de circuitos. Esto se debe a que se comparten los enlaces, y los paquetes se deben recibir por completo en un switch antes de pasar al siguiente. A pesar de la latencia y la vibración inherentes en las redes compartidas, la tecnología moderna permite el transporte satisfactorio de las comunicaciones de voz y video en estas redes.

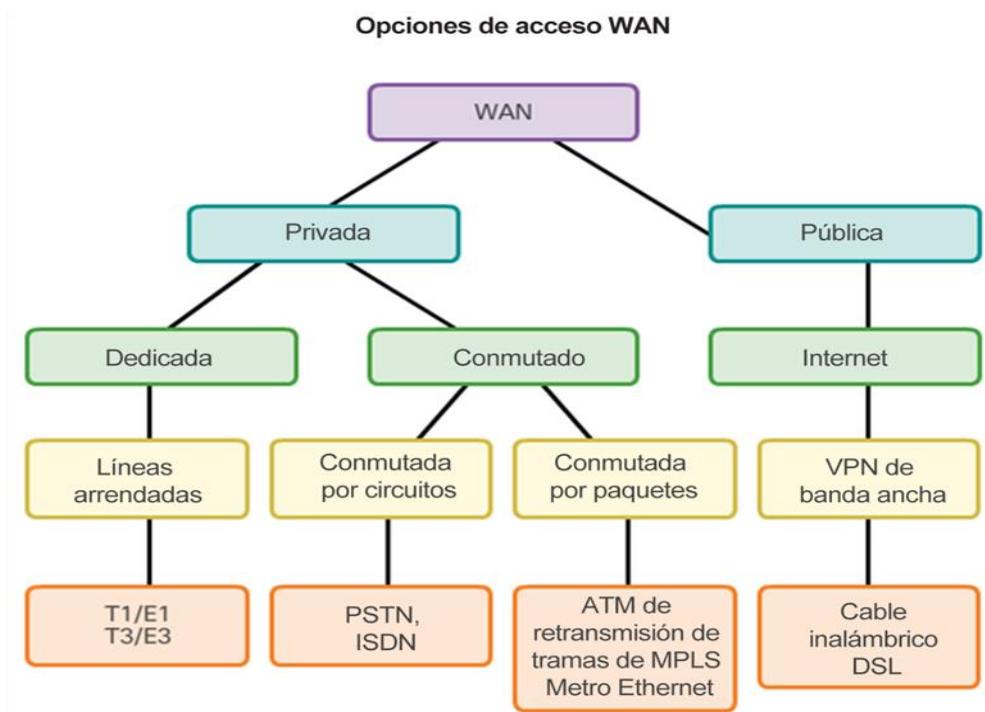


Opciones de conexión de enlace WAN

Existen diversas opciones de conexión de acceso WAN que los ISP pueden utilizar para conectar el bucle local al perímetro empresarial. Estas opciones de acceso WAN varían en términos de tecnología, velocidad y costo. Cada una tiene ventajas y desventajas diferentes. Familiarizarse con estas tecnologías es una parte importante del diseño de red.

Como se muestra en la siguiente figura, existen dos maneras en que una empresa puede tener acceso WAN:

- **Infraestructura WAN privada:** los proveedores de servicios pueden ofrecer líneas arrendadas punto a punto dedicadas, enlaces de conmutación de circuitos, como PSTN o ISDN, y enlaces de conmutación de paquetes, como WAN Ethernet, ATM o Frame Relay.
- **Infraestructura WAN pública:** los proveedores de servicios pueden ofrecer acceso a Internet de banda ancha mediante una línea de suscriptor digital (DSL), cable y acceso satelital. Las opciones de conexión de banda ancha normalmente se usan para conectar oficinas pequeñas y trabajadores a distancia a un sitio corporativo a través de Internet. Los datos que se transmiten entre sitios corporativos a través de la infraestructura WAN pública se deben proteger mediante VPN.



Infraestructura de la red del proveedor de servicios

Cuando un proveedor de servicios WAN recibe datos de un cliente en un sitio, debe reenviar los datos al sitio remoto para la entrega final al destinatario. En algunos casos, el sitio remoto se puede conectar al mismo proveedor de servicios que el sitio de origen. En otros casos, el sitio remoto se puede conectar a un ISP diferente, y el ISP de origen debe transmitir los datos al ISP conectado.

Las comunicaciones de largo alcance normalmente son esas conexiones entre ISP o entre sucursales en empresas muy grandes.

Las redes de los proveedores de servicios son complejas. Constan principalmente de medios de fibra óptica de ancho de banda de alta velocidad, que usan el estándar de red óptica síncrona (SONET) o de jerarquía digital síncrona (SDH). Estos estándares definen cómo transferir diverso tráfico de datos, voz y video a través de fibra óptica mediante láseres o diodos emisores de luz (LED) por grandes distancias.

SONET es un estándar de ANSI con base en los Estados Unidos, mientras que SDH es un estándar de ETSI y de ITU con base en Europa. Ambos son básicamente iguales y, por lo tanto, con frecuencia se los presenta como SONET/SDH.

Un avance más reciente en los medios de fibra óptica para las comunicaciones de largo alcance se denomina “multiplexación por división de longitud de onda densa” (DWDM). DWDM multiplica la cantidad de ancho de banda que puede admitir un único hilo de fibra.

Existen varias formas en que DWDM permite la comunicación de largo alcance:

- Habilita comunicaciones bidireccionales a través de un hilo de fibra.
- Puede multiplexar más de 80 canales de datos (es decir, longitudes de onda) diferentes en una única fibra.
- Cada canal puede transportar una señal multiplexada de 10 Gb/s.
- Asigna señales ópticas entrantes a longitudes de onda de luz específicas (es decir, frecuencias).

- Puede amplificar esas longitudes de onda para mejorar la intensidad de la señal.
- Admite los estándares SONET y SDH.

Los circuitos DWDM se usan en todos los sistemas de cables submarinos de comunicaciones modernos y en otros circuitos de largo alcance.

Líneas arrendadas

Cuando se requieren conexiones dedicadas permanentes, se utiliza un enlace punto a punto para proporcionar una ruta de comunicaciones WAN preestablecida desde las instalaciones del cliente hasta la red del proveedor. Por lo general, un proveedor de servicios arrienda las líneas punto a punto, que se llaman "líneas arrendadas".

Las líneas arrendadas existen desde comienzos de los años cincuenta y, por este motivo, se las conoce con nombres diferentes como circuito arrendado, enlace serial, línea serial, enlace punto a punto y línea T1/E1 o T3/E3. El término "línea arrendada" hace referencia al hecho de que la organización paga una tarifa mensual de arrendamiento a un proveedor de servicios para usar la línea. Hay líneas arrendadas disponibles de distintas capacidades y, por lo general, su precio depende del ancho de banda necesario y de la distancia entre los dos puntos conectados.

En América del Norte, los proveedores de servicios usan el sistema de portadora T para definir la capacidad de transmisión digital de un enlace serial de medios de cobre, mientras que en Europa se usa el sistema de portadora E, como se muestra en la ilustración. Por ejemplo, un enlace T1 admite 1,544 Mb/s, un E1 admite 2,048 Mb/s, un T3 admite 43,7 Mb/s y una conexión E3 admite 34,368 Mb/s. Para definir la capacidad de transmisión digital de una red de fibra óptica, se utilizan las velocidades de transmisión de la portadora óptica (OC).

Existen ventajas en el uso de líneas arrendadas:

- **Simplicidad:** los enlaces de comunicación punto a punto requieren conocimientos mínimos de instalación y mantenimiento.
- **Calidad:** los enlaces de comunicación punto a punto generalmente ofrecen una alta calidad de servicio si tienen un ancho de banda adecuado. La capacidad dedicada elimina la latencia o fluctuación entre los terminales.
- **Disponibilidad:** la disponibilidad constante es esencial para algunas aplicaciones, como el comercio electrónico. Los enlaces de comunicación punto a punto proporcionan la capacidad dedicada permanente que se necesita para VoIP o para video sobre IP.

También existen desventajas en el uso de líneas arrendadas:

- **Costo:** en general, los enlaces punto a punto son el tipo de acceso WAN más costoso. Cuando se usan para conectar varios sitios a través de distancias cada vez mayores, el costo de las soluciones de línea arrendada puede ser significativo. Además, cada terminal requiere una interfaz en el router, lo que aumenta los costos de los equipos.
- **Flexibilidad limitada:** el tráfico WAN suele ser variable, y las líneas arrendadas tienen una capacidad fija, de modo que el ancho de banda de la línea rara vez coincide con la necesidad de manera precisa. Por lo general, cualquier cambio en la línea arrendada requiere que el personal del ISP visite el sitio para ajustar la capacidad.

Generalmente, el protocolo de capa 2 es HDLC o PPP

Frame Relay

La retransmisión de tramas (Frame Relay) es una tecnología WAN multiacceso sin difusión (NBMA) simple de capa 2 que se utiliza para interconectar las redes LAN de una empresa. Para conectarse a varios sitios mediante PVC, se puede usar una única interfaz de router. Los PVC se usan para transportar tráfico de voz y datos entre origen y destino y admiten velocidades de datos de hasta 4 Mb/s, si bien algunos proveedores ofrecen velocidades aún mayores.

Los routers perimetrales solo requieren una única interfaz, incluso cuando se usan varios circuitos virtuales (VC). La línea arrendada al perímetro de la red de retransmisión de tramas permite conexiones rentables entre las redes LAN que se encuentran dispersas.

Frame Relay crea PVC que se identifican únicamente por un identificador de conexión de enlace de datos (DLCI). Los PVC y los DLCI aseguran la comunicación bidireccional de un dispositivo DTE a otro.

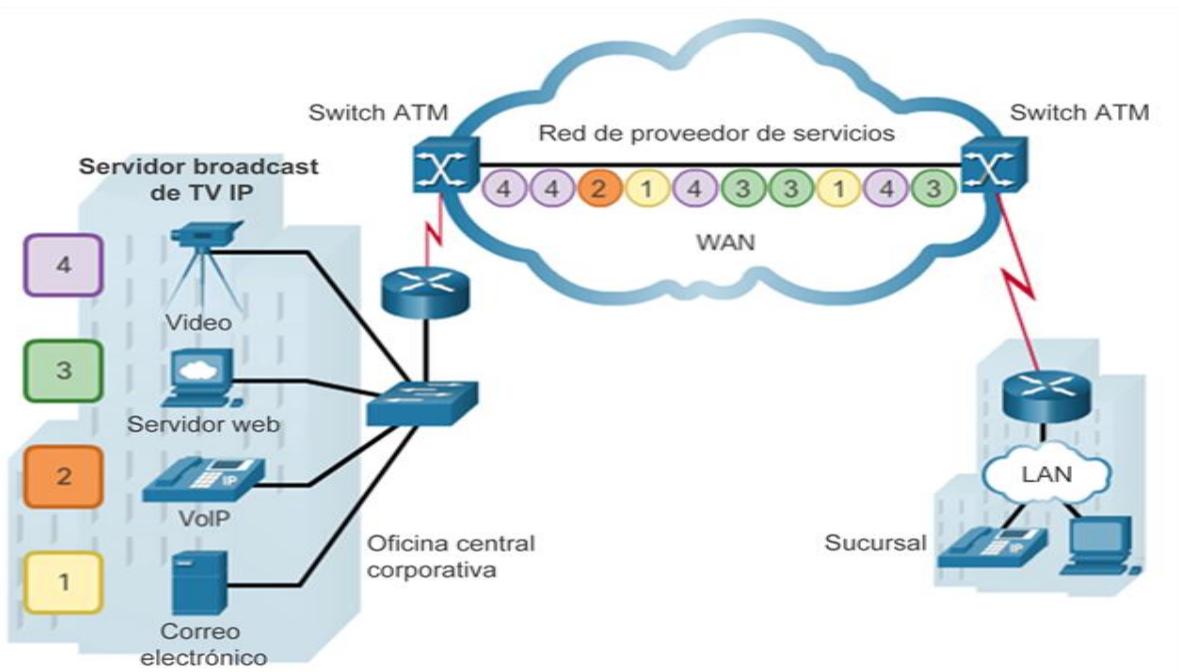
ATM

La tecnología del modo de transferencia asíncrona (ATM) puede transferir voz, video y datos a través de redes privadas y públicas. Se construye sobre una arquitectura basada en celdas, en vez de una arquitectura basada en tramas. Las celdas ATM tienen siempre una longitud fija de 53 bytes. La celda ATM contiene un encabezado ATM de 5 bytes, seguido de 48 bytes de contenido ATM. Las celdas pequeñas y de longitud fija son adecuadas para transportar tráfico de voz y video, debido a que este tipo de tráfico no admite retrasos. El tráfico de voz y video no tiene que esperar a que se transmitan paquetes de datos más grandes.

La celda ATM de 53 bytes es menos eficaz que las tramas y los paquetes más grandes de Frame Relay. Además, la celda ATM tiene por lo menos 5 bytes de sobrecarga por cada contenido de 48 bytes. Cuando la celda transporta los paquetes de capa de red segmentados, la sobrecarga es mayor debido a que el switch ATM debe poder rearmar los paquetes en el destino. Una línea ATM típica necesita casi un 20% más de ancho de banda que Frame Relay para transportar el mismo volumen de datos de capa de red.

ATM se diseñó para ser extremadamente escalable y para admitir las velocidades de enlace de T1/E1 a OC-12 (622 Mb/s) y más.

ATM ofrece PVC y SVC, si bien los PVC son más comunes con las WAN. Al igual que sucede con otras tecnologías de uso compartido, ATM permite varios VC en una única conexión de línea arrendada al perímetro de la red.



WAN Ethernet

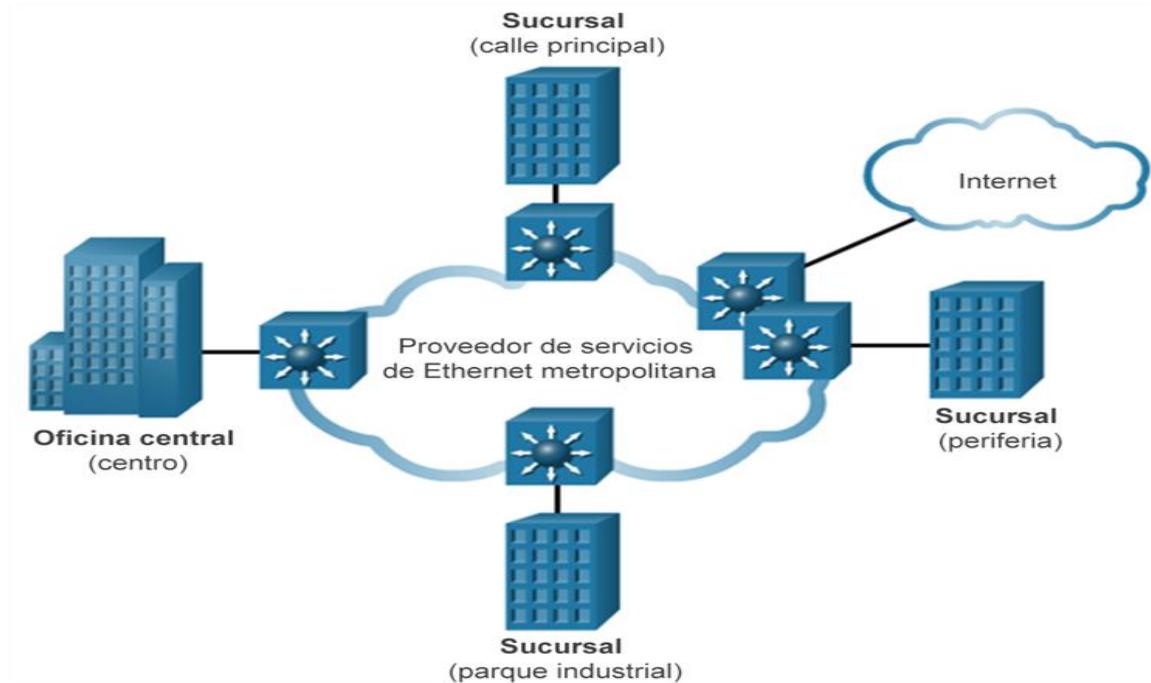
Originalmente, Ethernet se desarrolló para que fuera una tecnología de acceso a LAN. En un principio, Ethernet no era conveniente como tecnología de acceso WAN porque, en ese momento, la longitud de cable máxima era un kilómetro. No obstante, los estándares de Ethernet más recientes que utilizan cables de fibra óptica hicieron de Ethernet una opción de acceso WAN razonable. Por ejemplo, el estándar IEEE 1000BASE-LX admite longitudes de cable de fibra óptica de 5 km, mientras que el estándar IEEE 1000BASE-ZX admite longitudes de cable de hasta 70 km.

Los proveedores de servicios ahora ofrecen servicio WAN Ethernet con cableado de fibra óptica. El servicio WAN Ethernet se puede conocer con distintos nombres, incluidos Ethernet metropolitana (MetroE), Ethernet por MPLS (EoMPLS) y el servicio de LAN privada virtual (VPLS).

Existen varios beneficios de una WAN Ethernet:

- **Reducción de gastos y administración:** WAN Ethernet proporciona una red de commutación de capa 2 con un ancho de banda elevado que es capaz de administrar datos, voz y video en la misma infraestructura. Esta característica aumenta el ancho de banda y elimina las conversiones costosas a otras tecnologías WAN. La tecnología permite que las empresas conecten varios sitios en un área metropolitana, entre sí y a Internet, de forma económica.
- **Fácil integración con las redes existentes:** WAN Ethernet se conecta fácilmente a las LAN Ethernet existentes, lo que reduce los costos y el tiempo de instalación.
- **Productividad mejorada de la empresa:** WAN Ethernet permite que las empresas aprovechen las aplicaciones IP para mejorar la productividad, como las comunicaciones IP alojadas, VoIP y transmisión y difusión de video, que son difíciles de implementar en las redes TDM o Frame Relay.

Nota: las WAN Ethernet ganaron popularidad y ahora se usan comúnmente para reemplazar los tradicionales enlaces de Frame Relay y WAN ATM.



MPLS

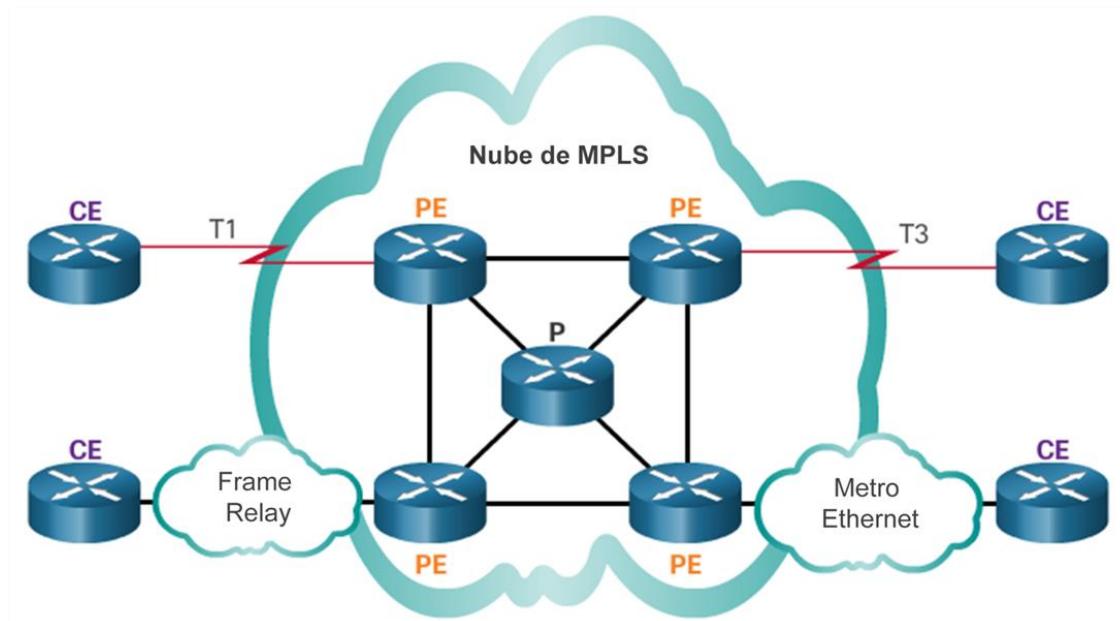
El switching por etiquetas multiprotocolo (Multiprotocol Label Switching, MPLS) es una tecnología WAN de alto rendimiento multiprotocolo que dirige los datos desde un router al siguiente. MPLS se basa en etiquetas de ruta cortas en lugar de direcciones de red IP.

MPLS tiene varias características que la definen. Es multiprotocolo, lo que significa que tiene la capacidad de transportar cualquier contenido, incluido tráfico IPv4, IPv6, Ethernet, ATM, DSL y Frame Relay. Usa etiquetas que le señalan al router qué hacer con un paquete. Las etiquetas identifican las rutas entre routers distantes —en lugar de entre terminales—, y mientras MPLS enruta paquetes IPv4 e IPv6 efectivamente, todo lo demás se commuta.

MPLS es una tecnología de proveedor de servicios. Las líneas arrendadas entregan bits entre sitios, y Frame Relay y WAN Ethernet entregan tramas entre los sitios. Sin embargo, MPLS puede entregar cualquier tipo de paquete entre sitios. MPLS puede encapsular paquetes de diversos protocolos de red. Admite una amplia variedad de tecnologías WAN, que incluyen los enlaces de portadoras T y E, Carrier Ethernet, ATM, Frame Relay y DSL.

En el ejemplo de topología de la ilustración, se muestra cómo se utiliza MPLS. Observe que los diferentes sitios se pueden conectar a la nube MPLS mediante diferentes tecnologías de acceso. En la ilustración, CE hace referencia al perímetro del cliente, PE es el router perimetral del proveedor que agrega y quita etiquetas, y P es un router interno del proveedor que commuta paquetes con etiquetas MPLS.

Nota: MPLS es principalmente una tecnología WAN de proveedor de servicios.



VSAT

En todas las tecnologías WAN privadas analizadas hasta ahora se usan medios de cobre o de fibra óptica. ¿Qué sucedería si una organización necesitara conectividad en una ubicación remota donde no hubiera proveedores de servicios que ofrecieran un servicio WAN?

Una terminal de apertura muy pequeña (VSAT) es una solución que crea una WAN privada mediante comunicaciones satelitales. Una VSAT es una pequeña antena parabólica similar a las que se usan para Internet y televisión en el hogar. Las VSAT crean una WAN privada a la vez que proporcionan conectividad a ubicaciones remotas.

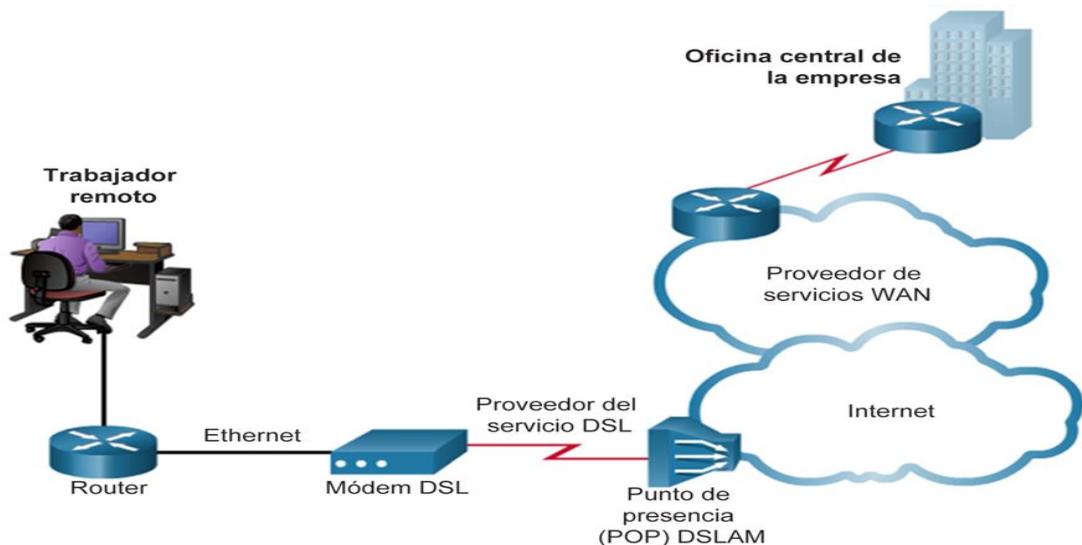
Especificamente, un router se conecta a un plato satelital que apunta al satélite de un proveedor de servicios. Este satélite se encuentra en órbita geosincrónica en el espacio. Las señales deben recorrer alrededor de 35.786 km (22.236 mi) hasta el satélite y regresar.

DSL

La tecnología DSL es una tecnología de conexión permanente que usa las líneas telefónicas de par trenzado existentes para transportar datos con un ancho de banda elevado y proporciona servicios IP a los suscriptores. Un módem DSL convierte una señal de Ethernet del dispositivo de usuario en una señal DSL, que se transmite a la oficina central.

Varias líneas de suscriptor DSL se multiplexan en un único enlace de alta capacidad mediante un multiplexor de acceso DSL (DSLAM) en la ubicación del proveedor. Los DSLAM incorporan la tecnología TDM para la agregación de varias líneas de suscriptor en un único medio, generalmente una conexión T3 (DS3). Para lograr velocidades de datos rápidas, las tecnologías DSL actuales utilizan técnicas sofisticadas de codificación y modulación.

Existe una amplia variedad de tipos, estándares y estándares emergentes de DSL. En la actualidad, DSL es una opción popular para la provisión de soporte a los trabajadores en el hogar por parte de los departamentos de TI corporativos. Generalmente, un suscriptor no puede elegir conectarse a una red empresarial directamente, sino que primero se debe conectar a un ISP y, luego, se realiza una conexión IP a la empresa a través de Internet. Se generan riesgos de seguridad en este proceso, pero se pueden remediar con medidas de seguridad.

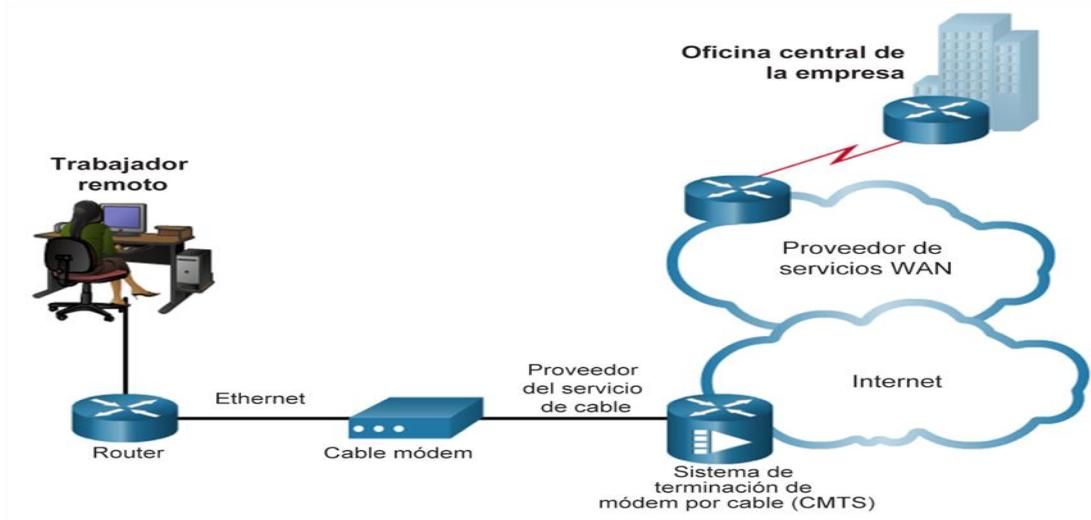


Cable

En áreas urbanas, para distribuir las señales de televisión se usa ampliamente el cable coaxial. Muchos proveedores de televisión por cable ofrecen acceso a la red. Esto permite un ancho de banda superior al del bucle local de telefonía convencional.

Los cable-módems proporcionan una conexión permanente y tienen una instalación simple. Un suscriptor conecta una computadora o un router LAN al cable módem, que traduce las señales digitales por frecuencias de banda ancha que se usan para la transmisión en una red de televisión por cable. La oficina local de televisión por cable, que se denomina "cabecera de cable", contiene el sistema de computación y las bases de datos que se necesitan para proporcionar acceso a Internet. El componente más importante ubicado en la cabecera es el sistema de terminación de cable módem (CMTS), que envía y recibe señales digitales de cable módem en una red de cable y es necesario para proporcionar servicios de Internet a los suscriptores.

Los suscriptores de cable módem deben usar el ISP asociado con el proveedor de servicios. Todos los suscriptores locales comparten el mismo ancho de banda de cable. A medida que se unen más usuarios al servicio, es posible que el ancho de banda disponible caiga por debajo de la velocidad esperada.



Tecnología inalámbrica

Para enviar y recibir datos, la tecnología inalámbrica usa el espectro de radio sin licencia. Cualquier persona que tenga un router inalámbrico y tecnología inalámbrica en el dispositivo que utilice puede acceder al espectro sin licencia.

Hasta hace poco tiempo, una limitación del acceso inalámbrico era la necesidad de estar dentro del alcance de transmisión local (normalmente, inferior a los 100 ft [30 m]) de un router inalámbrico o de un módem inalámbrico con una conexión por cable a Internet. Los siguientes avances en la tecnología inalámbrica de banda ancha están cambiando esta situación:

- **Wi-Fi municipal:** muchas ciudades comenzaron a instalar redes inalámbricas municipales. Algunas de estas redes proporcionan acceso a Internet de alta velocidad de manera gratuita o por un precio sustancialmente inferior al de otros servicios de banda ancha. Otras son solo para uso de la administración de la ciudad y permiten que la policía, los bomberos y otros empleados municipales realicen ciertos aspectos de su trabajo de manera remota. Para conectarse a Wi-Fi municipal, por lo general un suscriptor necesita un módem inalámbrico, que proporciona una antena de radio y direccional más potentes que los adaptadores inalámbricos convencionales. La mayoría de los proveedores de servicios proporcionan los equipos necesarios de manera gratuita o por una tarifa, de manera similar a lo que sucede con los módems DSL o los cable módems.
- **WiMAX:** la interoperabilidad mundial para el acceso por microondas (WiMAX) es una tecnología nueva que acaba de comenzar a usarse. Se describe en el estándar IEEE 802.16. WiMAX proporciona un servicio de banda ancha de alta velocidad con acceso inalámbrico y proporciona una amplia cobertura como una red de telefonía celular, en vez de pequeñas zonas de cobertura inalámbrica Wi-Fi. WiMAX funciona de manera similar a Wi-Fi, pero con velocidades más altas, a través de distancias mayores y para una mayor cantidad de usuarios. Usa una red de torres WiMAX que son similares a las torres de telefonía celular. Para acceder a una red WiMAX, los suscriptores se deben suscribir a un ISP con una torre WiMAX a menos de 30 mi (48 km) de su ubicación. Para tener acceso a la estación base, también necesitan algún tipo de receptor WiMAX y un código de cifrado especial.
- **Internet satelital:** generalmente utilizado por usuarios en áreas rurales, donde no hay cable ni DSL. Una VSAT proporciona comunicaciones de datos bidireccionales (subida y descarga). La velocidad de subida es aproximadamente un décimo de la velocidad de descarga de 500 kb/s. Cable y DSL tienen velocidades de descarga mayores, pero los sistemas satelitales son unas diez veces más rápidos que un módem analógico. Para acceder a los servicios de Internet satelital, los suscriptores necesitan una antena parabólica, dos módems (uplink y downlink) y cables coaxiales entre la antena y el módem.

Celular 3G/4G

Cada vez más, el servicio celular es otra tecnología WAN inalámbrica que se usa para conectar usuarios y ubicaciones remotas donde no hay otra tecnología de acceso WAN disponible. Muchos usuarios con smartphones y tablet PC pueden usar los datos móviles para enviar correos electrónicos, navegar la Web, descargar aplicaciones y mirar videos.

Los teléfonos, las tablet PC, las computadoras portátiles e incluso algunos routers se pueden comunicar a través de Internet mediante la tecnología de datos móviles. Estos dispositivos usan ondas de radio para comunicarse por medio de una torre de telefonía móvil. El dispositivo tiene una pequeña antena de radio,

y el proveedor tiene una antena mucho más grande que se ubica en la parte superior de una torre en algún lugar a una distancia determinada del teléfono.

Estos son dos términos de redes celulares comunes de la industria:

- **3G/4G inalámbrico:** abreviatura para el acceso celular de tercera y cuarta generación. Estas tecnologías admiten acceso inalámbrico a Internet.
- **Evolución a largo plazo (LTE):** hace referencia a una tecnología más reciente y más rápida, que se considera parte de la tecnología de cuarta generación (4G).

Tecnología VPN

Cuando un trabajador remoto o un trabajador en una oficina remota utilizan un servicio de banda ancha para acceder a la WAN corporativa a través de Internet, se generan riesgos de seguridad. Para abordar las cuestiones de seguridad, los servicios de banda ancha proporcionan capacidades para usar conexiones VPN a un dispositivo de red que acepte conexiones VPN, que por lo general se encuentra en el sitio corporativo.

Una VPN es una conexión cifrada entre redes privadas a través de una red pública, como Internet. En vez de usar una conexión dedicada de capa 2, como una línea arrendada, una VPN usa conexiones virtuales llamadas “túneles VPN”, que se enrutan a través de Internet desde la red privada de la empresa hasta el host del sitio o del empleado remoto.

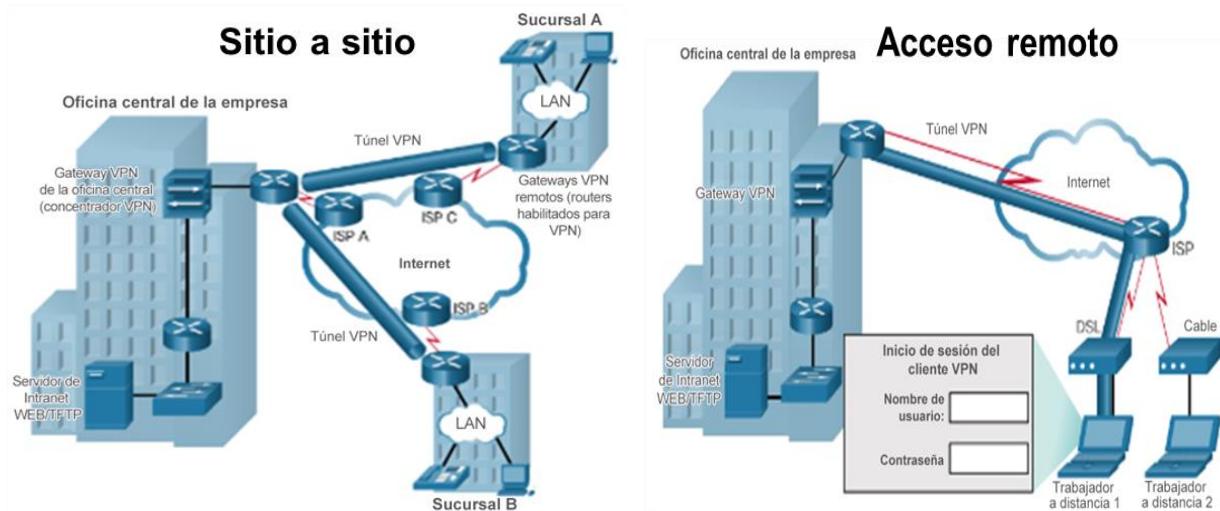
Existen varios beneficios en el uso de VPN:

- **Ahorro de costos:** las VPN permiten que las organizaciones usen la Internet global para conectar oficinas remotas, y para conectar usuarios remotos con el sitio corporativo principal. Esto elimina los enlaces WAN dedicados y costosos, y los bancos de módem.
- **Seguridad:** las VPN proporcionan el nivel máximo de seguridad mediante dos protocolos avanzados de cifrado y autenticación que protegen los datos del acceso no autorizado.
- **Escalabilidad:** debido a que las VPN usan la infraestructura de Internet en los ISP y los dispositivos, es fácil agregar nuevos usuarios. Las empresas pueden incrementar ampliamente la capacidad, sin agregar una infraestructura significativa.
- **Compatibilidad con la tecnología de banda ancha:** los proveedores de servicio de banda ancha, como DSL y cable, admiten la tecnología VPN. Las VPN permiten que los trabajadores móviles y los empleados a distancia aprovechen el servicio de Internet de alta velocidad de su hogar para acceder a las redes corporativas. Las conexiones de banda ancha de alta velocidad para uso empresarial también pueden proporcionar una solución rentable para la conexión de oficinas remotas.

Existen dos tipos de acceso a VPN:

- **VPN de sitio a sitio:** las VPN de sitio a sitio conectan redes enteras entre sí; por ejemplo, pueden conectar la red de una sucursal a la red de la oficina central de la empresa. Cada sitio cuenta con un gateway VPN, como un router, un firewall, un concentrador VPN o un dispositivo de seguridad. En la ilustración, una sucursal remota utiliza una VPN de sitio a sitio para conectarse a la oficina central de la empresa.

- **VPN de acceso remoto:** las VPN de acceso remoto permiten que los hosts individuales, como los empleados a distancia, los usuarios móviles y los consumidores de extranets, accedan a la red de una empresa de manera segura a través de Internet. Por lo general, cada host (trabajador a distancia 1 y trabajador a distancia 2) tiene cargado un software de cliente VPN o usa un cliente basado en Web..



Elección de una conexión de enlace WAN

Al elegir la conexión WAN apropiada, se deben tener en cuenta varios factores importantes. Para que un administrador de red decida cuál es la tecnología WAN que mejor cumple con los requisitos de una empresa específica, debe responder las siguientes preguntas:

¿Cuál es el propósito de la WAN?

Se deben considerar algunos problemas:

- ¿La empresa conectará sucursales locales en la misma área urbana, conectará sucursales remotas o realizará una conexión a una única sucursal?
- ¿Se usará la WAN para conectar a los empleados internos, los socios comerciales externos, los clientes o los tres grupos?
- ¿La empresa se conectará a los clientes, a los socios comerciales, a los empleados o a alguna combinación de los tres?
- ¿La WAN proporcionará a los usuarios autorizados un acceso limitado o total a la intranet de la empresa?

¿Cuál es el alcance geográfico?

Se deben considerar algunos problemas:

- ¿Es la WAN local, regional o global?
- ¿La WAN es de una sucursal a una sucursal, de una sucursal a varias sucursales o de varias sucursales a varias sucursales (distribuida)?

¿Cuáles son los requisitos de tráfico?

Se deben considerar algunos problemas:

- ¿Cuál es el tipo de tráfico que se debe admitir (solo datos, VoIP, video, archivos grandes, archivos de transmisión)? Esto determina los requisitos de calidad y rendimiento.
- ¿Cuál es el volumen por tipo de tráfico (voz, video o datos) que se debe admitir para cada destino? Esto determina la capacidad de ancho de banda que se necesita para la conexión WAN al ISP.
- ¿Cuál es la calidad de servicio que se requiere? Esto puede limitar las opciones. Si el tráfico es muy sensible a la latencia y a la vibración, elimine todas las opciones de conexión WAN que no pueden proporcionar la calidad requerida.
- ¿Cuáles son los requisitos de seguridad (integridad de datos, confidencialidad y seguridad)? Estos son factores importantes si el tráfico es de una naturaleza muy confidencial o si proporciona servicios esenciales, como respuesta de emergencia.

Además de reunir información sobre el ámbito de la WAN, el administrador también debe determinar lo siguiente:

- **¿La WAN debe usar infraestructura pública o privada?** Una infraestructura privada ofrece la mejor seguridad y la mejor confidencialidad, mientras que la infraestructura de Internet pública ofrece la mayor flexibilidad y el menor gasto continuo. La elección depende del propósito de la WAN, los tipos de tráfico que transporta y el presupuesto operativo disponible. Por ejemplo, si el propósito es proporcionarle servicios seguros de alta velocidad a una sucursal cercana, una conexión privada dedicada o de comutación puede ser la mejor opción. Si el propósito es conectar varias oficinas

remotas, una WAN pública que utilice Internet puede ser la mejor opción. Para operaciones distribuidas, la solución puede ser una combinación de las opciones.

- **Para una WAN privada, ¿la conexión debe ser dedicada o de conmutación?** Las transacciones de gran volumen en tiempo real tienen requisitos especiales que podrían inclinar la elección por una línea dedicada, como el flujo de tráfico entre el centro de datos y la oficina central de la empresa. Si la empresa se conecta a una única sucursal local, se podría usar una línea arrendada dedicada. Sin embargo, esa opción se volvería muy costosa para una WAN que conecte varias oficinas. En ese caso, podría ser mejor una conexión de conmutación.
- **Para una WAN pública, ¿qué tipo de acceso VPN se necesita?** Si el propósito de la WAN es conectar una oficina remota, una VPN de sitio a sitio puede ser la mejor opción. Para conectar a los trabajadores a distancia o a los clientes, las VPN de acceso remoto son una mejor opción. Si la WAN brinda servicio a una combinación de oficinas remotas, trabajadores a distancia y clientes autorizados, como en el caso de una empresa global con operaciones distribuidas, es posible que sea necesaria una combinación de opciones de VPN.
- **¿Qué opciones de conexión están disponibles a nivel local?** En ciertas áreas, no todas las opciones de conexión WAN están disponibles. En este caso, se simplifica el proceso de selección, si bien la WAN resultante puede proporcionar un rendimiento inferior al óptimo. Por ejemplo, en un área rural o remota, es posible que la única opción sea VSAT o acceso celular.
- **¿Cuál es el costo de las opciones de conexión disponibles?** Según la opción elegida, la WAN puede implicar un gasto continuo significativo. Se debe analizar el costo de una opción particular según cuán bien cumpla esta con los otros requisitos. Por ejemplo, una línea arrendada dedicada es la opción más costosa, pero el gasto puede estar justificado si es fundamental proteger la transmisión de grandes volúmenes de datos en tiempo real. Para aplicaciones menos exigentes, puede ser más conveniente una opción de conmutación o de conexión a Internet menos costosa.

Ventajas y desventajas de una WAN

Ventajas	Desventajas
<ul style="list-style-type: none">• Las WAN pueden utilizar un software especializado para incluir mini y macrocomputadoras como elementos de red.• La WAN no está limitada a espacio geográfico para establecer comunicación entre PC's o mini o macrocomputadoras.• Puede llegar a utilizar enlaces de satélites, fibra óptica, aparatos de rayos infrarrojos y de enlaces	<ul style="list-style-type: none">• Los equipos deben poseer gran capacidad de memoria, si se quiere que el acceso sea rápido.• No destaca por la seguridad que ofrece a sus usuarios.• Los virus y la eliminación de programas son dos de los males más comunes que sufre la red WAN

Protocolos de encapsulación WAN

En cada conexión WAN, se encapsulan los datos en las tramas antes de cruzar el enlace WAN. Para asegurar que se utilice el protocolo correcto, se debe configurar el tipo de encapsulación de capa 2 correspondiente. La opción de protocolo depende de la tecnología WAN y el equipo de comunicación. En la ilustración, se muestran los protocolos WAN más comunes y dónde se utilizan. Las siguientes son descripciones breves de cada tipo de protocolo WAN:

- **HDLC:** es el tipo de encapsulación predeterminado en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuitos cuando el enlace utiliza dos dispositivos de Cisco. Ahora, HDLC es la base para PPP síncrono que usan muchos servidores para conectarse a una WAN, generalmente Internet.

- **PPP:** proporciona conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos. PPP funciona con varios protocolos de capa de red, como IPv4 e IPv6. PPP utiliza el protocolo de encapsulación HDLC, pero también tiene mecanismos de seguridad incorporados como PAP y CHAP.
- **Protocolo de Internet de línea serial (SLIP):** es un protocolo estándar para conexiones seriales punto a punto mediante TCP/IP. PPP reemplazó ampliamente al protocolo SLIP.
- **Procedimiento de acceso al enlace balanceado (LAPB) X.25:** es un estándar del UIT-T que define cómo se mantienen las conexiones entre un DTE y un DCE para el acceso remoto a terminales y las comunicaciones por computadora en las redes de datos públicas. X.25 especifica a LAPB, un protocolo de capa de enlace de datos. X.25 es un antecesor de Frame Relay

Encapsulación HDLC

HDLC es un protocolo sincrónico de capa de enlace de datos orientado a bits desarrollado por la Organización Internacional para la Estandarización (ISO). El estándar actual para HDLC es ISO 13239. HDLC se desarrolló a partir del estándar de control de enlace de datos síncronos (SDLC) propuesto en la década de los setenta. HDLC proporciona servicio orientado a la conexión y sin conexión.

HDLC utiliza la transmisión serial síncrona, que proporciona una comunicación sin errores entre dos puntos. HDLC define una estructura de trama de capa 2 que permite el control del flujo y de errores mediante el uso de acuses de recibo. Cada trama presenta el mismo formato ya sea una trama de datos o una trama de control.

Cuando las tramas se transmiten por enlaces síncronos o asíncronos, esos enlaces no tienen ningún mecanismo para marcar ni el principio ni el fin de las tramas. Por este motivo, HDLC utiliza un delimitador de trama, o indicador, para marcar el principio y el fin de cada trama.



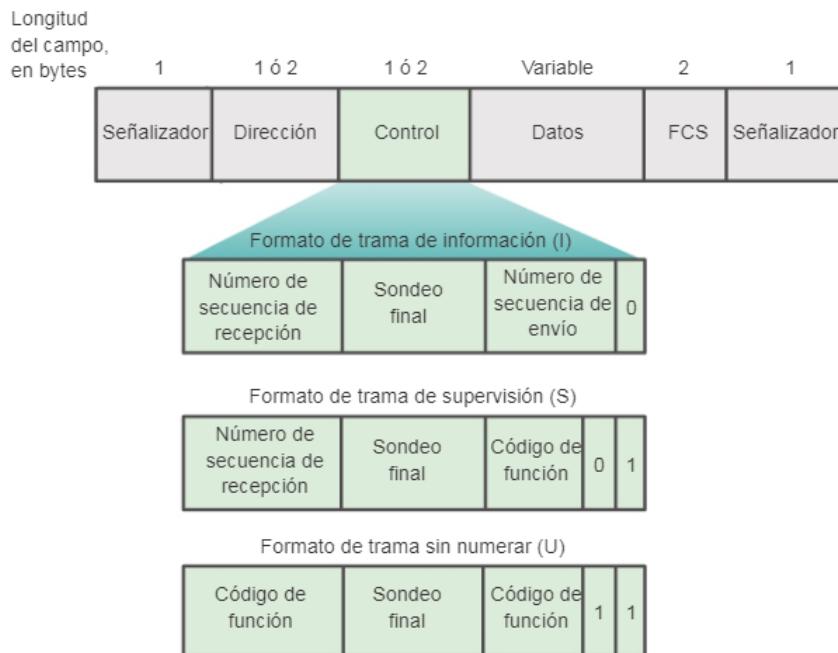
Tipos de tramas HDLC

HDLC define tres tipos de tramas, cada uno con un formato diferente de campo de control.

- **Señalizador:** El campo Indicador inicia y termina la verificación de errores. La trama siempre comienza y termina con un campo Indicador de 8 bits. El patrón de bits es 01111110. Debido a que existe una probabilidad de que este patrón ocurra en los datos propiamente dichos, el sistema HDLC emisor siempre inserta un bit 0 después de cada cinco 1 consecutivos en el campo de datos, de modo que en la práctica, la secuencia de indicadores solo se puede producir en los extremos de la trama. El sistema receptor elimina los bits introducidos. Cuando las tramas se transmiten en forma consecutiva, el indicador de fin de la primera trama se utiliza como indicador de inicio de la trama siguiente.
- **Dirección:** El campo Dirección contiene la dirección HDLC de la estación secundaria. Esta dirección puede contener una dirección específica, una dirección de grupo o una dirección de difusión. Una dirección principal es un origen o un destino de comunicación, lo que elimina la necesidad de incluir la dirección de la estación principal.

- **Control:** El campo Control utiliza tres formatos diferentes, según el tipo de trama HDLC que se use:
 - **Trama de información (I):** las tramas I transportan información de capa superior y determinada información de control. Esta trama envía y recibe números de secuencia, y el bit de sondeo final (P/F) realiza el control del flujo y de errores. El número de secuencia de envío se refiere al número de la trama que se debe enviar a continuación. El número de secuencia de recepción proporciona el número de la trama que se recibe a continuación. Tanto el emisor como el receptor mantienen números de secuencia de envío y recepción. Las estaciones principales usan el bit P/F para informarles a las secundarias si requieren una respuesta inmediata. Las estaciones secundarias usan el bit P/F para informarles a las principales si la trama actual es la última en su respuesta actual.
 - **Trama de supervisión (S):** las tramas S proporcionan información de control. Las tramas S pueden solicitar y suspender la transmisión, informar sobre el estado y confirmar la recepción de las tramas I. Las tramas S no tienen un campo de información.
 - **Trama sin numerar (U):** las tramas U admiten funciones de control y no son secuenciales. Según la función de la trama U, el campo de control es de 1 byte o 2 bytes. Algunas tramas U tienen un campo de información.
- **Protocolo:** Solo se usa en HDLC de Cisco. Este campo especifica el tipo de protocolo encapsulado dentro de la trama (p. ej., 0x0800 para IP).
- **Datos:** El campo de datos contiene una unidad de información de ruta (PIU) o información de identificación de intercambio (XID).
- **Secuencia de verificación de trama (FCS, Frame Check Sequence):** La FCS precede al delimitador del indicador de fin y generalmente es un resto del cálculo de la comprobación de redundancia cíclica (CRC). El cálculo de CRC se vuelve a realizar en el receptor. Si el resultado difiere del valor en la trama original, se supone que existe un error.

Tipos de tramas HDLC



Conceptos de PPP

¿Qué es PPP?

El protocolo punto a punto (PPP) es un protocolo TCP/IP que se emplea para conectar un sistema informático a otro. Las máquinas emplean PPP o el protocolo punto a punto, para comunicarse por la red telefónica o por Internet.

Existe una conexión PPP cuando dos sistemas están conectados físicamente por medio de una línea telefónica. Podrá emplear PPP para conectar un sistema con otro. Por ejemplo, una conexión PPP establecida entre una sucursal y una oficina central permite a cada una de las oficinas transferir datos a la otra a través de la red.

PPP es un estándar de Internet. Es el protocolo de conexión que más se utiliza entre los proveedores de servicios de Internet (ISP). Podrá utilizar PPP para conectarse con el ISP; luego, el ISP le dará conectividad con Internet.

El protocolo punto a punto (PPP) permite que haya interoperatividad entre el software de acceso remoto de distintos fabricantes. También permite que múltiples protocolos de comunicaciones de red utilicen una misma línea de comunicaciones física.

PPP es un protocolo WAN de enlace de datos. Se diseñó como un protocolo abierto para trabajar con varios protocolos de capa de red, como IP, IPX y Apple Talk.

Se puede considerar a PPP la versión no propietaria de HDLC, aunque el protocolo subyacente es considerablemente diferente. PPP funciona tanto con encapsulación síncrona como asíncrona porque el protocolo usa un identificador para denotar el inicio o el final de una trama.

Dicho indicador se utiliza en las encapsulaciones asíncronas para señalar el inicio o el final de una trama y se usa como una encapsulación síncrona orientada a bit. Dentro de la trama PPP el Bit de entramado es el encargado de señalar el comienzo y el fin de la trama PPP (identificado como 01111110).

El campo de direccionamiento de la trama PPP es un Broadcast debido a que PPP no identifica estaciones individuales.

El protocolo PPP esta descrito en los RFC 1661 a 1663. Es el estándar usado en Internet para conexiones de un nodo aislado (por ejemplo una computadora en el hogar) hacia un servidor en Internet (por ejemplo, un servidor de terminales de una LAN en Internet). PPP provee los siguientes servicios:

- Un método de framing que delimita sin ambigüedad los límites de los marcos.
- El formato de las tramas contempla una cadena de chequeo que permite la detección de errores.
- Un protocolo LCP (Link Control Protocol) para levantar, probar, negociar y eliminar los enlaces apropiadamente.
- Un mecanismo (Network Control Protocol) para negociar opciones con la capa de red que permite soportar varios protocolos de capa de red.

El formato de trama de PPP se escogió de modo que fuera muy parecido al formato de marco de HDLC. La diferencia principal entre PPP y HDLC es que el primero está orientado a caracteres.

PPP, al igual que SLIP, usa el relleno de caracteres en las líneas por discado con módem, por lo que todos las tramas tienen un número entero de bytes.

La encapsulación PPP provee multiplexamiento de diferentes protocolos de la capa de red sobre el mismo enlace. Ha sido diseñada cuidadosamente para mantener compatibilidad con el hardware mayormente usado.

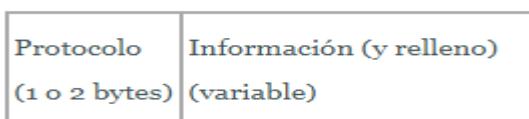
Sólo son necesarios 8 bytes adicionales para formar la encapsulación cuando se usa dentro del enramado por defecto. En ambientes con escaso ancho de banda, la encapsulación y el enramado pueden requerir menos bytes.

El formato de la trama completa es:

1 Delimitad. 01111110	1 Dirección 11111111	1 Control 00000011	1 ó 2 Protocolo	Variable Datos	2 ó 4 CRC	1 Delimitad. 01111110
-----------------------------	----------------------------	--------------------------	--------------------	-------------------	--------------	-----------------------------

- Todas las tramas comienzan con el byte indicador "01111110".
- Luego viene el campo dirección, al que siempre se asigna el valor "11111111".
- La dirección va seguida del campo de control, cuyo valor predeterminado es "00000011".
- Este valor indica un marco sin número ya que PPP no proporciona por omisión transmisión confiable (usando números de secuencia y acuses) pero en ambientes ruidosos se puede usar un modo numerado para transmisión confiable.
- El anteúltimo campo es el de suma de comprobación, que normalmente es de 2 bytes, pero puede negociarse una suma de 4 bytes.
- La trama finaliza con otro byte indicador "01111110".

Debido a que los campos indicados anteriormente son utilizados para encapsular la información fundamental del protocolo, desde ahora nos centraremos en el siguiente esquema:



Campo protocolo

- Este campo es de 1 o 2 bytes y su valor identifica el contenido del datagrama en el campo de información del paquete (cuando hablamos de "paquete" nos estamos refiriendo al marco de la capa de enlace, que es en la que opera el PPP; no debe confundirse con los de la capa de red, manejados por IP).
- El bit menos significativo del byte menos significativo debe ser 1 y el bit menos significativo del byte más significativo debe ser 0. Los marcos recibidos que no cumplan con estas reglas deben ser tratados como irreconocibles.
- Los valores en el campo de protocolo dentro del rango de 0hex a 3hex identifican el protocolo de capa de red de los paquetes específicos, y valores en el rango de 8hex a Bhex identifican paquetes pertenecientes al protocolo de control de red asociado (NCPs). Los valores en el campo de protocolo dentro del rango de 4hex a 7hex son usados para protocolos con bajo volumen de tráfico, los cuales no tienen asociados NCP. Valores en el rango de Chex a Fhex identifican paquetes de los protocolos de control de la capa de enlace (como LCP).

Campo información

- Puede tener 0 o más bytes. Contiene el datagrama para el protocolo especificado en el campo protocolo. La máxima longitud para este campo, incluyendo el relleno pero no incluyendo el

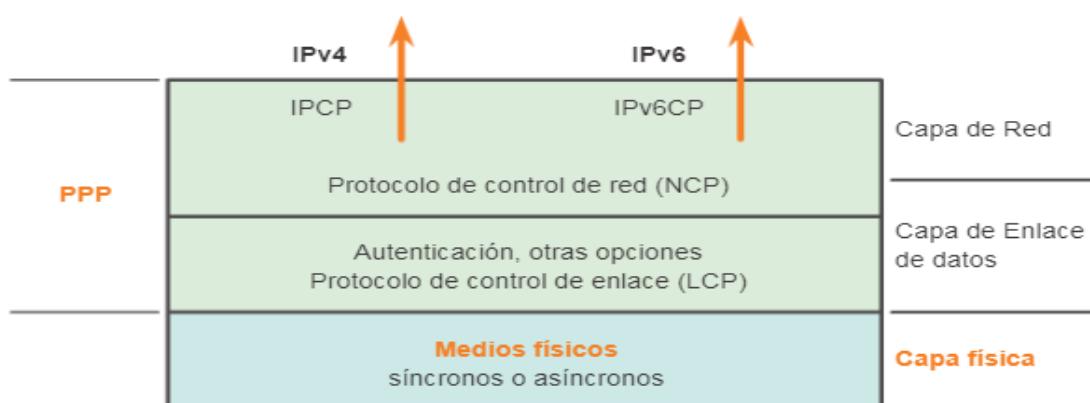
campo de protocolo, es determinada por la unidad máxima de recepción (MRU), la cual es de 1500 bytes por defecto. Mediante negociaciones, PPP puede usar otros valores para la MRU.

- A la información se le puede agregar un relleno, con un número arbitrario de bytes, hasta llegar a la MRU.

Arquitectura de capas PPP

Una arquitectura en capas es un modelo, un diseño, o un plano lógico que ayuda en la comunicación de las capas que se interconectan.

En la ilustración, se compara la arquitectura en capas de PPP con el modelo de interconexión de sistema abierto (OSI). PPP y OSI comparten la misma capa física, pero PPP distribuye las funciones de LCP y NCP de manera diferente.



En la capa física, puede configurar PPP en un rango de interfaces, incluidas las siguientes:

- Serial asíncrona
- Serial síncrona
- HSSI
- ISDN

PPP opera a través de cualquier interfaz DTE/DCE (RS-232-C, RS-422, RS-423 o V.35). El único requisito absoluto impuesto por PPP es un circuito full-duplex, ya sea dedicado o commutado, que pueda funcionar en modo de bits seriales síncrono o asíncrono, transparente para las tramas de capa de enlace PPP. PPP no impone ninguna restricción con respecto a la velocidad de transmisión además de los impuestos por la interfaz DTE/DCE específica que se utiliza.

La mayor parte del trabajo que realiza PPP lo llevan a cabo LCP y los NCP en las capas de enlace de datos y de red. LCP configura la conexión PPP y sus parámetros, los NCP manejan las configuraciones de protocolo de capa superior, y LCP finaliza la conexión PPP.

PPP busca resolver los problemas de conectividad de Internet mediante tres componentes básicos:

1. Un método para encapsular datagramas a través de enlaces seriales. PPP utiliza el Control de enlace de datos de alto nivel (HDLC) como base para encapsular datagramas a través de enlaces punto a punto.

2. Un Protocolo de control de enlace (LCP) para establecer, configurar y probar la conexión de enlace de datos.
3. Una familia de Protocolos de control de red (NCP) para establecer y configurar distintos protocolos de capa de red. PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de capa de red.

PPP se basa en el protocolo de control de enlaces LCP (Link Control Protocol), que establece, configura y pone a prueba las conexiones de enlace de datos que utiliza PPP.

El protocolo de control de red NCP (Network Control Protocol) es un conjunto de protocolos (uno por cada capa de red compatible con PPP) que establece y configura diferentes capas de red para que funcionen a través de PPP. Para IP, IPX y Apple Talk, las designaciones NCP son IPCP, IPXCP y ATALKCP, respectivamente.

Protocolo de control de enlace (LCP)

LCP funciona dentro de la capa de enlace de datos y cumple una función en el establecimiento, la configuración y la prueba de la conexión de enlace de datos.

LCP establece el enlace punto a punto. LCP también negocia y configura las opciones de control en el enlace de datos WAN, administradas por los NCP.

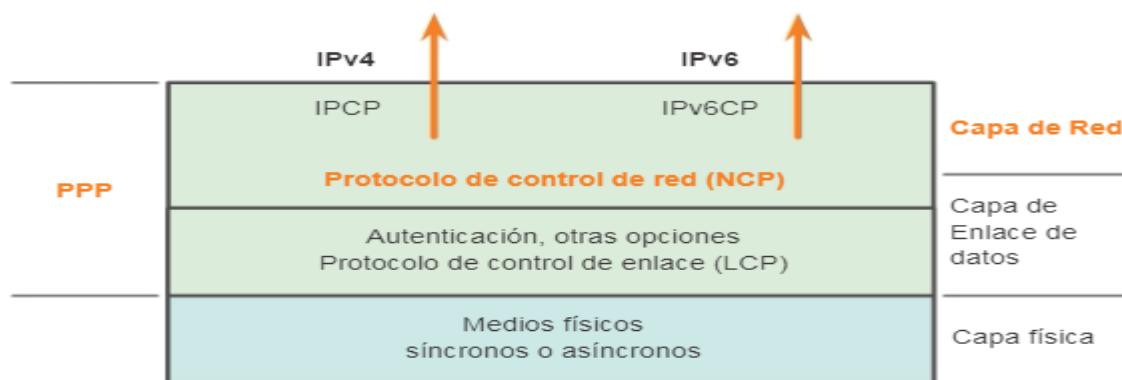
- LCP proporciona la configuración automática de las interfaces en cada extremo, incluido lo siguiente:
- Manejo de distintos límites en el tamaño de paquete
- Detección de errores comunes de configuración
- Finalización del enlace
- Determinación de cuándo un enlace funciona correctamente o cuándo falla

Una vez establecido el enlace, PPP también usa LCP para acordar automáticamente los formatos de encapsulación, como la autenticación, la compresión y la detección de errores. Establecimiento de una conexión PPP

Protocolo de control de red (NCP)

PPP permite que varios protocolos de capa de red funcionen en el mismo enlace de comunicación.

Para cada protocolo de capa de red que se usa, PPP utiliza un NCP separado, como se ve en la figura. Por ejemplo, IPv4 utiliza el protocolo de control de IP (IPCP) e IPv6 utiliza el protocolo de control de IPv6 (IPv6CP).



Los protocolos NCP incluyen campos funcionales que contienen códigos estandarizados para indicar el protocolo de capa de red que PPP encapsula.

Cada NCP administra las necesidades específicas requeridas por sus respectivos protocolos de capa de red. Los distintos componentes NCP encapsulan y negocian las opciones para varios protocolos de capa de red.

El establecimiento de una sesión PPP tiene tres fases:

1. Establecimiento del enlace: en esta fase cada dispositivo PPP envía paquetes LCP para configurar y verificar el enlace de datos.
2. Autenticación: fase opcional, una vez establecido el enlace es elegido el método de autenticación. Normalmente los métodos de autenticación son PAP y CHAP.
3. Protocolo de capa de red, en esta fase el router envía paquetes NCP para elegir y configurar uno o más protocolos de capa de red. A partir de esta fase los datagramas pueden ser enviados.



Fase 1. Establecimiento del enlace: "¿Negociamos?".



Fase 2. Determinación de la calidad del enlace: "¿Por qué no analizamos algunos detalles sobre la calidad? O no. . .".



Fase 3. Negociación del protocolo de red: "Sí, dejaré que los NCP analicen los detalles de mayor nivel".

El enlace permanece configurado para las comunicaciones hasta que las tramas LCP o NCP explícitas cierran el enlace, o hasta que ocurra algún evento externo, por ejemplo, que caduque un temporizador de inactividad o que intervenga un administrador.

LCP puede finalizar el enlace en cualquier momento. Por lo general, esto se realiza cuando uno de los routers solicita la finalización, pero puede suceder debido a un evento físico, como la pérdida de una portadora o el vencimiento de un temporizador de período inactivo.

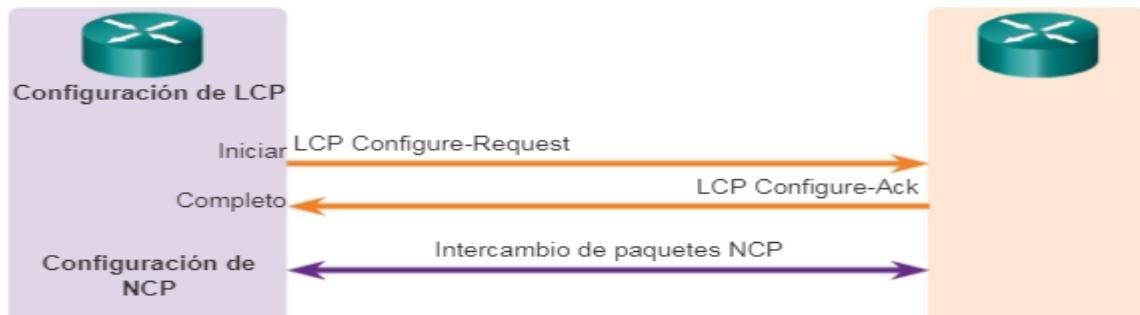
Funcionamiento de LCP

El funcionamiento de LCP incluye las disposiciones para el establecimiento, el mantenimiento y la finalización de enlaces. El funcionamiento de LCP utiliza tres clases de tramas LCP para lograr el trabajo de cada una de las fases de LCP:

- Las tramas de establecimiento de enlace establecen y configuran un enlace (solicitud de configuración, acuse de recibo de configuración, acuse de recibo negativo [NAK] de configuración y rechazo de configuración).
- Las tramas de mantenimiento de enlace administran y depuran un enlace (rechazo de código, rechazo de protocolo, solicitud de eco, respuesta de eco y solicitud de descarte).
- Las tramas de terminación de enlace terminan un enlace (solicitud de terminación y acuse de recibo de terminación).

Establecimiento del enlace

El establecimiento del enlace es la primera fase de una operación LCP, como se observa en la figura.



Esta fase se debe completar correctamente antes de que se intercambie cualquier paquete de capa de red. Durante el establecimiento del enlace, LCP abre una conexión y negocia los parámetros de configuración. El proceso de establecimiento del enlace comienza cuando el dispositivo de inicio envía una trama de solicitud de configuración al respondedor. La trama de solicitud de configuración incluye una cantidad variable de opciones de configuración necesarias para configurar en el enlace.

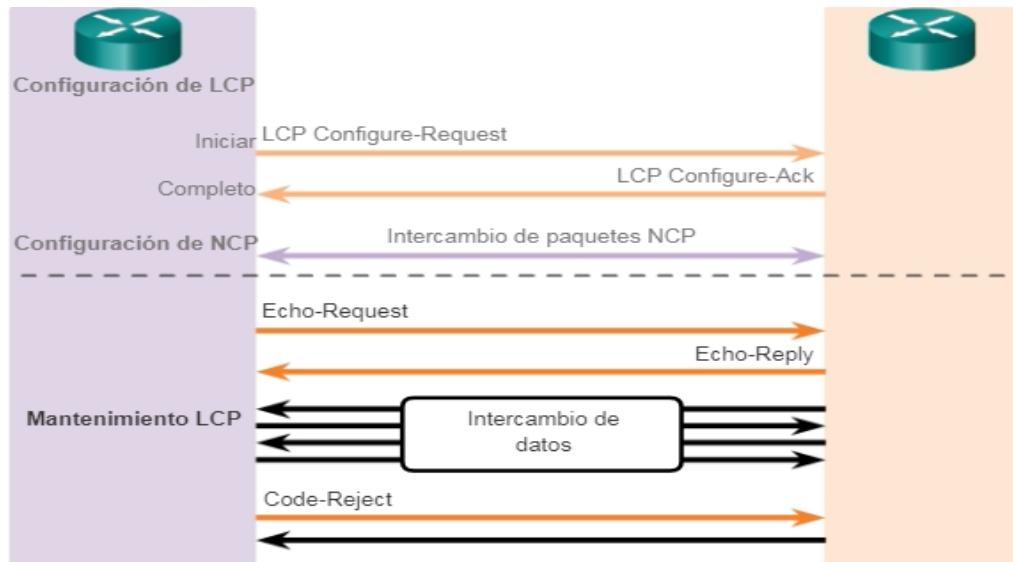
El iniciador incluye las opciones para la forma en que desea que se cree el enlace, incluidos los parámetros de protocolo o de autenticación. El respondedor procesa la solicitud:

- Si las opciones no son aceptables o no se reconocen, el respondedor envía un mensaje de NAK de configuración o de rechazo de configuración. Si esto sucede y la negociación falla, el iniciador debe reiniciar el proceso con nuevas opciones.
- Si las opciones son aceptables, el respondedor responde con un mensaje de acuse de recibo de configuración, y el proceso pasa a la fase de autenticación. La operación del enlace se entrega a NCP.

Una vez que NCP completó todas las configuraciones necesarias, incluida la validación de la autenticación si se configuró, la línea está disponible para la transferencia de datos. Durante el intercambio de datos, LCP pasa al mantenimiento del enlace.

Mantenimiento del enlace

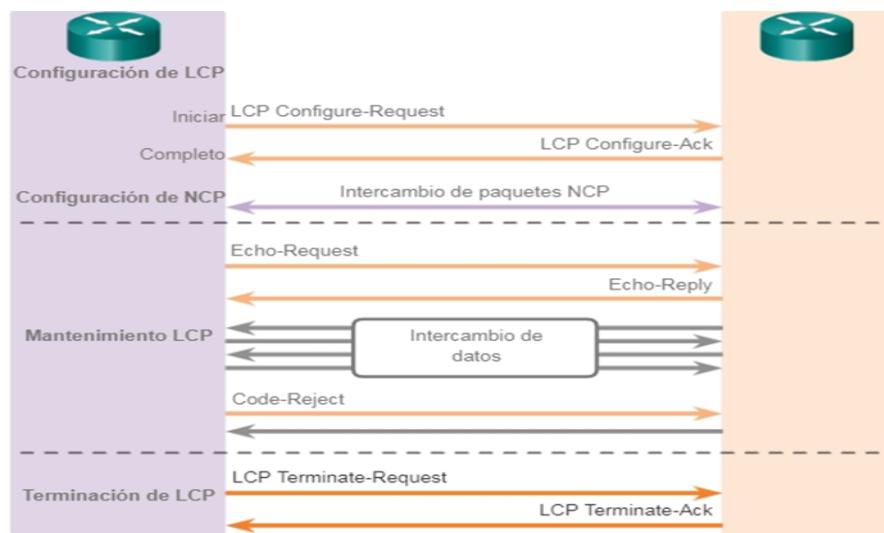
Durante el mantenimiento del enlace, LCP puede utilizar mensajes para proporcionar comentarios y probar el enlace, como se muestra en la siguiente figura.



- **Solicitud de eco, respuesta de eco y solicitud de descarte:** estas tramas se pueden utilizar para probar el enlace.
- **Rechazo de código y rechazo de protocolo:** estos tipos de tramas proporcionan comentarios cuando un dispositivo recibe una trama no válida debido a un código LCP desconocido (tipo de trama LCP) o a un identificador de protocolo defectuoso. Por ejemplo, si se recibe un paquete interpretable del peer, se envía un paquete rechazo de código en respuesta. El dispositivo emisor vuelve a enviar el paquete.

Terminación del enlace

Una vez finalizada la transferencia de datos en la capa de red, LCP termina el enlace, NCP solo termina el enlace NCP y de capa de red. El enlace permanece abierto hasta que LCP lo termina. Si LCP termina el enlace antes que NCP, también se termina la sesión NCP.

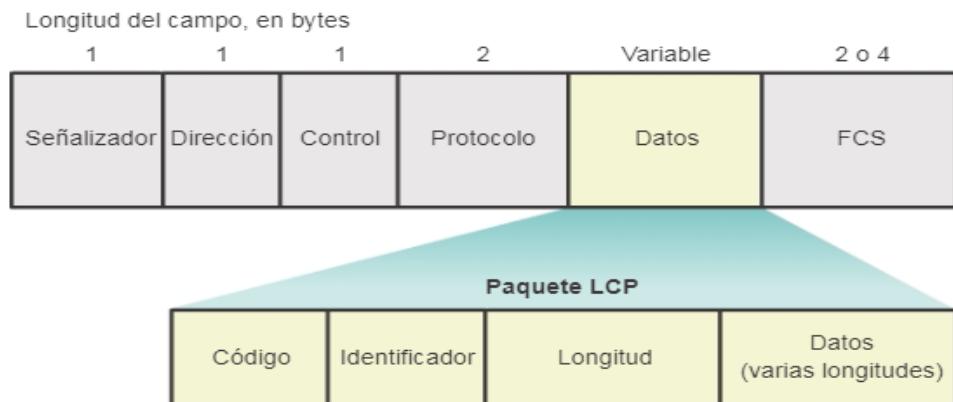


PPP puede terminar el enlace en cualquier momento. Esto podría suceder debido a la pérdida de la portadora, a un error de autenticación, a una falla de la calidad del enlace, al vencimiento de un

temporizador de período inactivo o al cierre administrativo del enlace. LCP cierra el enlace mediante el intercambio de paquetes de terminación. El dispositivo que inicia la desactivación envía un mensaje de solicitud de terminación. El otro dispositivo responde con un mensaje de acuse de recibo de terminación. Una solicitud de terminación indica que el dispositivo que la envía necesita cerrar el enlace. Cuando se cierra el enlace, PPP informa a los protocolos de capa de red para que puedan tomar las medidas adecuadas.

Paquete LCP

Los campos en un paquete LCP:



- Código:** el campo Código tiene una longitud de 1 byte e identifica el tipo de paquete LCP.
- Identificador:** el campo Identificador tiene una longitud de 1 byte y se usa para establecer coincidencias entre solicitudes y respuestas de paquetes.
- Longitud:** el campo Longitud tiene una longitud de 2 bytes e indica la longitud total (incluidos todos los campos) del paquete LCP.
- Datos:** el campo de datos consta de 0 o más bytes, según lo que indique el campo Longitud. El formato de este campo es determinado por el código.

Cada paquete LCP es un único mensaje LCP que consta de un campo Código que identifica el tipo de paquete LCP, un campo Identificador para establecer coincidencias entre solicitudes y respuestas, y un campo Longitud que indica el tamaño del paquete LCP y los datos específicos del tipo de paquete LCP.

Cada paquete LCP tiene una función específica en el intercambio de la información de configuración según el tipo de paquete. El campo Código de los paquetes LCP identifica el tipo de paquete

Clases de paquetes LCP	Tipos de paquetes LCP	Propósito
Configuración del link	Configure-Request, Configure-Ack, Configure-Nak y Configure-Reject	Se utiliza para establecer y configurar un link.
Terminación del link	Termino Request y Terminar-ACK	Utilizado para terminar un link.
Mantenimiento del link	Rechazo de código, Rechazo de protocolo, Solicitud de eco, Respuesta de eco y Solicitud de descarte.	Utilizado para administrar y depurar un link.

Proceso NCP

Una vez que se inició el enlace, LCP entrega el control al protocolo NCP correspondiente.

Si bien en los inicios se diseñó para los paquetes IP, PPP puede transportar datos de varios protocolos de capa de red mediante un enfoque modular en su implementación. El modelo modular de PPP permite que LCP configure el enlace y transfiera los detalles de un protocolo de red a un protocolo NCP específico. Cada protocolo de red tiene un NCP correspondiente, y cada NCP tiene un RFC correspondiente.

Hay NCP para IPv4, IPv6, IPX, AppleTalk y muchos otros. Los protocolos NCP usan el mismo formato de paquetes que los protocolos LCP.

Una vez que LCP configuró y autenticó el enlace básico, se invoca el protocolo NCP correspondiente para completar la configuración específica del protocolo de capa de red que se usa. Cuando NCP configuró correctamente el protocolo de capa de red, este se encuentra en estado abierto en el enlace LCP establecido. En este momento, PPP puede transportar los paquetes correspondientes del protocolo de capa de red.

Ejemplo de IPCP

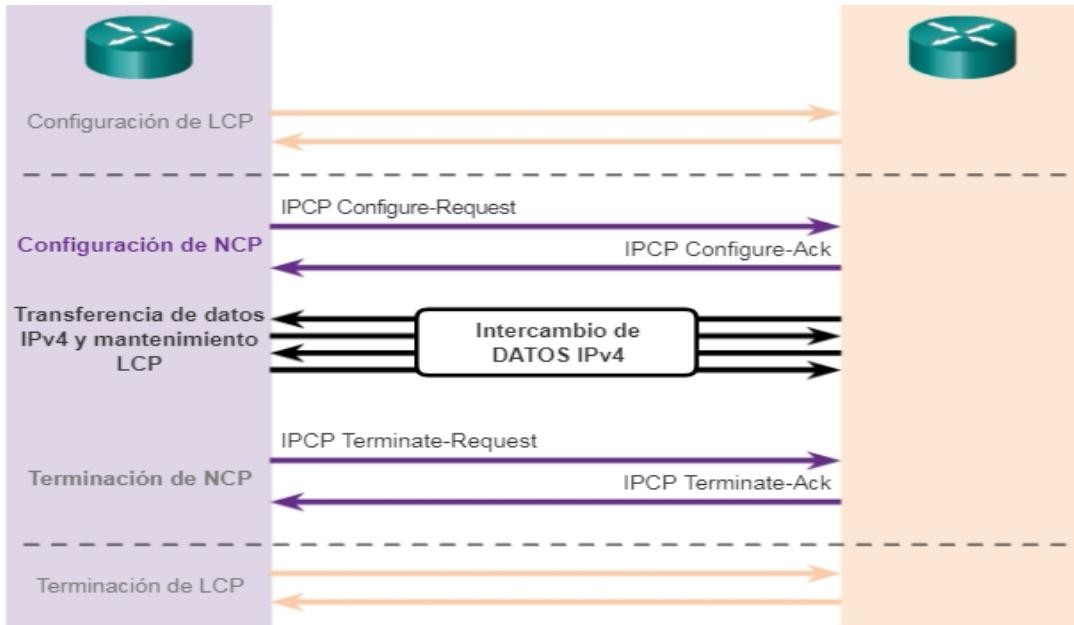
Como ejemplo de cómo funciona la capa NCP, en la ilustración se muestra la configuración NCP de IPv4, que es el protocolo de capa 3 más común. Una vez que LCP estableció el enlace, los routers intercambian mensajes IPCP para negociar opciones específicas del protocolo IPv4. IPCP es responsable de la configuración, la habilitación y la deshabilitación de los módulos IPv4 en ambos extremos del enlace. IPV6CP es un protocolo NCP con las mismas responsabilidades para IPv6.

IPCP negocia dos opciones:

- **Compresión:** permite que los dispositivos negocien un algoritmo para comprimir encabezados TCP e IP, y ahorrar ancho de banda. La compresión de encabezados TCP/IP de Van Jacobson reduce los encabezados TCP/IP a un tamaño de hasta 3 bytes. Esto puede ser unas mejoras considerables en las líneas seriales lentas, en particular para el tráfico interactivo.
- **Dirección IPv4:** permite que el dispositivo de inicio especifique una dirección IPv4 para utilizar en el routing IP a través del enlace PPP, o para solicitar una dirección IPv4 para el respondedor. Antes de la llegada de las tecnologías de banda ancha como los servicios de DSL y de cable módem, los enlaces de red de dial-up normalmente usaban la opción de dirección IPv4.

Una vez que se completa el proceso NCP, el enlace pasa al estado abierto, y LCP vuelve a tomar el control en la fase de mantenimiento del enlace.

El tráfico del enlace consta de cualquier combinación posible de paquetes LCP, NCP y de protocolo de capa de red. Cuando se completa la transferencia de datos, NCP termina el enlace del protocolo; LCP finaliza la conexión PPP.



Opciones de configuración del PPP

PPP se puede configurar para admitir diversas funciones optativas. Estas funciones optativas incluyen lo siguiente:

- **Autenticación:** los routers peers intercambian mensajes de autenticación. Las dos opciones de autenticación son: el protocolo de autenticación de contraseña (PAP, Password Authentication Protocol) y el protocolo de autenticación de intercambio de señales (CHAP, Challenge Handshake Authentication Protocol).
- **Compresión:** aumenta el rendimiento eficaz en las conexiones PPP al reducir la cantidad de datos que se deben transferir en la trama a través del enlace. El protocolo descomprime la trama al llegar a su destino. Dos protocolos de compresión disponibles en los routers Cisco son Stacker y Predictor.
- **Detección de errores:** identifica fallas. Las opciones de calidad y número mágico contribuyen a asegurar el establecimiento de un enlace de datos confiable y sin bucles. El campo de número mágico ayuda a detectar enlaces que se encuentran en una condición de loop back. Hasta que no se negocie correctamente la opción de configuración de número mágico, este se debe transmitir como cero. Los números mágicos se generan de forma aleatoria en cada extremo de la conexión.
- **Devolución de llamada PPP:** la devolución de llamada PPP se usa para mejorar la seguridad. Con esta opción de LCP, un router Cisco puede funcionar como cliente o servidor de devolución de llamada. El cliente realiza la llamada inicial, solicita que el servidor le devuelva la llamada y termina la comunicación inicial. El router de devolución de llamada responde la llamada inicial y se comunica con el cliente sobre la base de sus instrucciones de configuración. El comando es **ppp callback[accept | request]**.
- **Multienlace:** esta alternativa proporciona balanceo de carga a través de las interfaces del router que PPP utiliza. El protocolo PPP multienlace, también conocido como MP, MPPP, MLP o multienlace, proporciona un método para propagar el tráfico a través de varios enlaces WAN físicos a la vez que proporciona la fragmentación y el rearmado de paquetes, la secuenciación adecuada, la interoperabilidad con varios proveedores y el balanceo de carga del tráfico entrante y saliente.

Para negociar el uso de estas opciones de PPP, las tramas de establecimiento de enlace LCP incluyen información de la opción en el campo de datos de la trama LCP. Si no se incluye una opción de configuración en una trama LCP, se supone el valor predeterminado para esa opción de configuración.

Habilitación de PPP en una interfaz

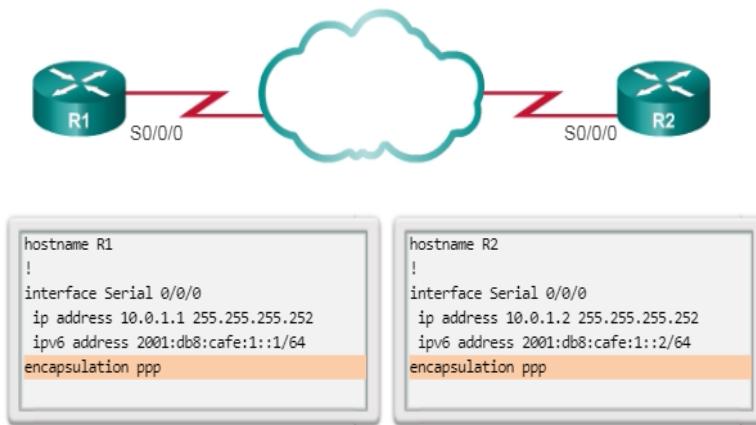
Para establecer PPP como el método de encapsulación que usa una interfaz serial, utilice el comando de configuración de interfaz **encapsulation ppp**.

El siguiente ejemplo habilita la encapsulación PPP en la interfaz serial 0/0/0:

```
R3# configure terminal  
R3(config)# interface serial 0/0/0  
R3(config-if)# encapsulation ppp
```

El comando de interfaz **encapsulation ppp** no tiene ningún argumento.

En el ejemplo se muestra que los routers R1 y R2 se configuraron con una dirección IPv4 y una dirección IPv6 en las interfaces seriales. PPP es una encapsulación de capa 2 que admite varios protocolos de capa 3, incluidos IPv4 e IPv6.



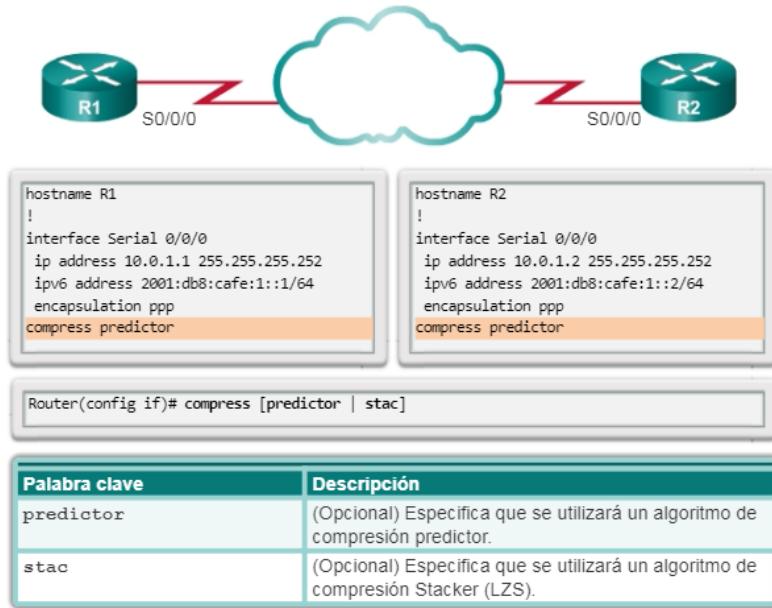
Comandos de compresión de PPP

La compresión de software de punto a punto en las interfaces seriales se puede configurar después de que se habilita la encapsulación PPP. Dado que esta opción invoca un proceso de compresión de software, puede afectar el rendimiento del sistema. Si el tráfico ya consta de archivos comprimidos, como .zip, .tar, o .mpeg, no utilice esta opción..

Para configurar la compresión a través de PPP, introduzca los siguientes comandos:

```
R3(config)# interface serial 0/0/0  
R3(config-if)# encapsulation ppp  
R3(config-if)# compress [ predictor | stac ]
```

En la ilustración, se muestra la sintaxis del comando **compress**



Comando de control de calidad del enlace PPP

Recuerde que LCP proporciona una fase optativa de determinación de la calidad del enlace. En esta fase, LCP prueba el enlace para determinar si la calidad de este es suficiente para usar protocolos de capa 3.

El comando **ppp quality percentage** asegura que el enlace cumpla con el requisito de calidad establecido; de lo contrario, el enlace queda inactivo.

Los porcentajes se calculan para las direcciones entrantes y salientes. La calidad de salida se calcula comparando la cantidad total de paquetes y bytes enviados con la cantidad total de paquetes y bytes que recibe el nodo de destino. La calidad de entrada se calcula comparando la cantidad total de paquetes y bytes recibidos con la cantidad total de paquetes y bytes que envía el nodo de destino.

Si el porcentaje de la calidad del enlace no se mantiene, el enlace se considera de baja calidad y se desactiva. El control de calidad del enlace (LQM) implementa un retraso de tiempo de modo que el enlace no rebote de un lado a otro.

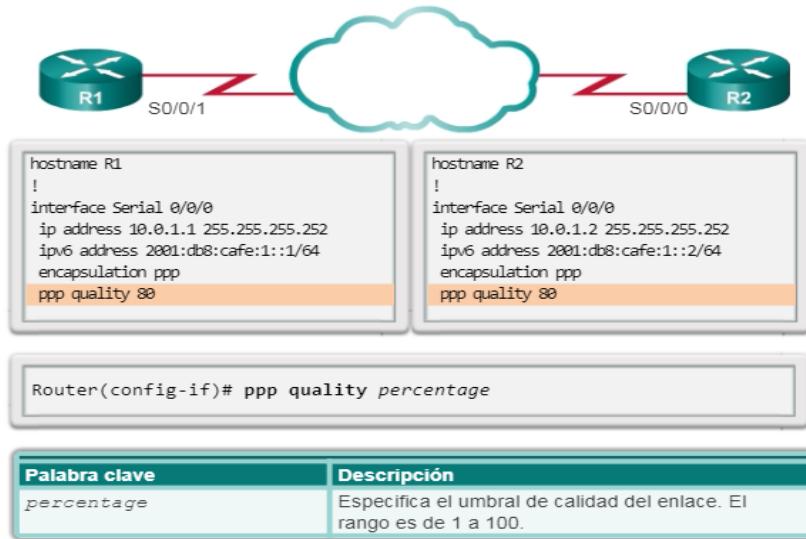
El siguiente ejemplo de configuración controla los datos descartados en el enlace y evita que las tramas formen bucles:

```

R3(config)# interface serial 0/0/0
R3(config-if)# encapsulation ppp
R3(config-if)# ppp quality 80

```

Utilice el comando **no ppp quality** para deshabilitar LQM.



Comandos de PPP multilink

El protocolo PPP multienlace (también conocido como MP, MPPP, MLP o multienlace) proporciona un método para propagar el tráfico a través de varios enlaces WAN físicos. Además, el protocolo PPP multienlace proporciona la fragmentación y el rearmado de paquetes, la secuenciación adecuada, la interoperabilidad con varios proveedores y el balanceo de carga del tráfico entrante y saliente.

MPPP permite fragmentar los paquetes y enviarlos simultáneamente a la misma dirección remota a través de varios enlaces punto a punto. Todos los enlaces físicos se activan en respuesta a un umbral de carga definido por el usuario. MPPP puede medir la carga solo en el tráfico entrante o solo en el tráfico saliente, pero no la carga combinada del tráfico entrante y saliente.

La configuración de MPPP requiere dos pasos, como se muestra en la ilustración.

Paso 1. Cree un grupo multienlace.

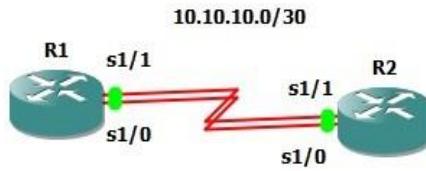
- El comando **interface multilinknumber** crea la interfaz de multienlace.
- En el modo de configuración de interfaz, se asigna una dirección IP a la interfaz de multienlace. En este ejemplo, se configuran direcciones IPv4 e IPv6 en los routers R3 y R4.
- La interfaz está habilitada para el protocolo PPP multienlace.
- Se asigna un número de grupo multienlace a la interfaz.

Paso 2. Asigne las interfaces al grupo multienlace.

Cada interfaz que forma parte del grupo multienlace tiene las siguientes características:

- Está habilitada para la encapsulación PPP.
- Está habilitada para el protocolo PPP multienlace.
- Está vinculada al grupo multienlace mediante el número de grupo multienlace configurado en el paso 1.

Para deshabilitar el protocolo PPP multienlace, use el comando **no ppp multilink**.



R1#

```
int Multilink 100
ip address 10.10.10.1 255.255.255.252
ppp multilink
ppp multilink group 100
```

```
int s1/0
encapsulotion ppp
ppp multilink
ppp multilink group 100
```

```
int s1/1
encapsulotion ppp
ppp multilink
ppp multilink group 100
```

R2#

```
int Multilink 200
ip address 10.10.10.2 255.255.255.252
ppp multilink
ppp multilink group 200
```

```
int s1/0
encapsulotion ppp
ppp multilink
ppp multilink group 200
```

```
int s1/1
encapsulotion ppp
ppp multilink
ppp multilink group 200
```

Verificación de la configuración de PPP

Utilice el comando **show interfaces serial** para verificar la configuración de la encapsulación PPP o HDLC
El comando **show ppp multilink** verifica que el protocolo PPP multienlace esté habilitado

Comando	Descripción
show interfaces	Muestra estadísticas de todas las interfaces configuradas en el router.
show interfaces serial	Muestra información sobre una interfaz serial.
show ppp multilink	Muestra información sobre una interfaz PPP multienlace.

Protocolos de autenticación PPP

PPP define un protocolo LCP extensible que permite la negociación de un protocolo de autenticación para autenticar a los peers antes de permitir que los protocolos de capa de red transmitan por el enlace. RFC 1334 define dos protocolos para la autenticación, PAP y CHAP, los cuales se muestran en la ilustración.

PAP es un proceso bidireccional muy básico. No hay cifrado. El nombre de usuario y la contraseña se envían en texto no cifrado. Si se acepta, se permite la conexión. CHAP es más seguro que PAP. Implica un intercambio de tres vías de un secreto compartido.

La fase de autenticación de una sesión PPP es optativa. Si se utiliza, se autentica el peer después de que LCP establece el enlace y elige el protocolo de autenticación. Si se utiliza, la autenticación ocurre antes de que comience la fase de configuración del protocolo de capa de red.

Las opciones de autenticación requieren que la parte del enlace que llama introduzca la información de autenticación. Esto contribuye a asegurar que el usuario tenga permiso del administrador de red para realizar la llamada. Los routers pares intercambian mensajes de autenticación.

Autenticación PAP

PAP (protocolo de autenticación de contraseña) proporciona un método de autenticación simple utilizando un intercambio de señales de dos vías. El proceso de autenticación solo se realiza durante el establecimiento de inicial del enlace.

Una vez completada la fase de establecimiento PPP, el nodo remoto envía repetidas veces al router extremo su usuario y contraseña hasta que se acepta la autenticación o se corta la conexión.

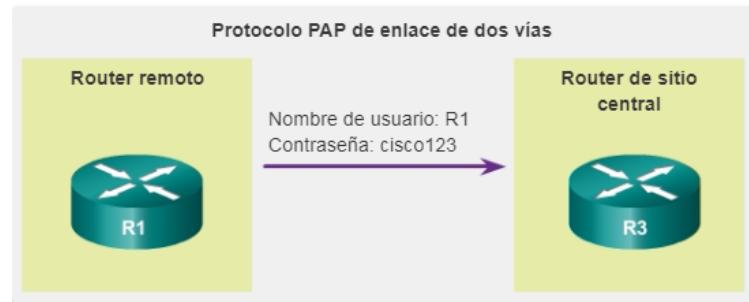
PAP no es un método de autenticación seguro, las contraseñas se envían en modo abierto y no existe protección contra el registro de las mismas o los ataques externos.

Una de las diversas características de PPP es que realiza la autenticación de capa 2 además de otras capas de autenticación, de cifrado, de control de acceso y de procedimientos de seguridad generales.

Inicio de PAP

PAP proporciona un método simple para que un nodo remoto establezca su identidad mediante un enlace bidireccional. PAP no es interactivo. Cuando se utiliza el comando `ppp authentication pap`, se envía el nombre de usuario y la contraseña como un paquete de datos LCP, en lugar de que el servidor envíe una solicitud de inicio de sesión y espere una respuesta. Una vez que PPP completa la fase de establecimiento del enlace, el nodo remoto envía repetidamente un par de nombre de usuario y contraseña a través del enlace hasta que el nodo receptor lo confirma o finaliza la conexión.

El router R1 envía su nombre de usuario y contraseña de PAP al R3.



Finalización de PAP

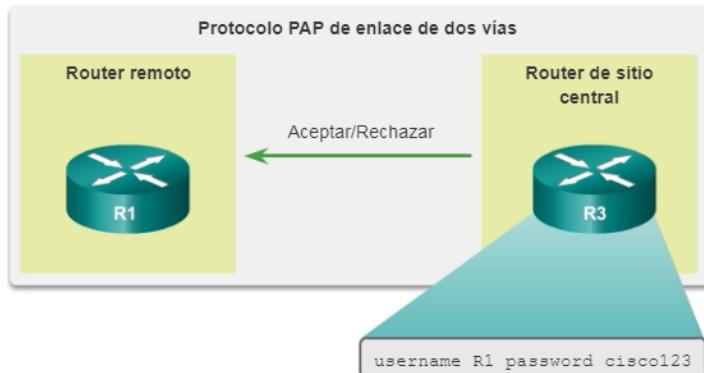
En el nodo receptor, un servidor de autenticación que permite o deniega la conexión verifica el nombre de usuario y la contraseña. Se devuelve un mensaje de aceptación o rechazo al solicitante.

PAP no es un protocolo de autenticación seguro. Mediante PAP, las contraseñas se envían a través del enlace en texto no cifrado, y no existe protección contra los ataques de reproducción o los ataques repetidos de prueba y error. El nodo remoto tiene el control de la frecuencia y la temporización de los intentos de inicio de sesión.

No obstante, hay momentos en los que se justifica el uso de PAP. Por ejemplo, a pesar de sus limitaciones, PAP se puede utilizar en los siguientes entornos:

- Una gran base instalada de aplicaciones cliente que no admiten CHAP
- Incompatibilidades entre las distintas implementaciones de CHAP de los proveedores
- Situaciones en las que una contraseña de texto no cifrado debe estar disponible para simular un inicio de sesión en el host remoto

El router R3 compara el nombre de usuario y la contraseña del R1 con su base de datos local. Si coinciden, se acepta la conexión. Si no coinciden, la conexión es denegada.

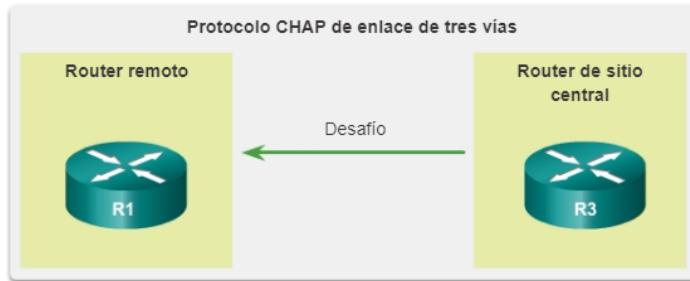


Autenticación CHAP

Una vez que se establece la autenticación con PAP, no se vuelve a autenticar. Esto deja la red vulnerable a los ataques. A diferencia de PAP, que autentica solo una vez, CHAP realiza desafíos periódicos para asegurar que el nodo remoto siga teniendo un valor de contraseña válido. El valor de contraseña varía y cambia de manera impredecible mientras existe el enlace.

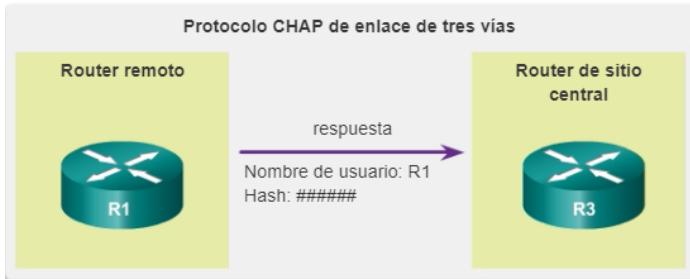
Una vez completa la fase de establecimiento del enlace PPP, el router local envía un mensaje de desafío al nodo remoto,

El router R3 inicia el protocolo de enlace de tres vías y envía un mensaje de desafío al R1.



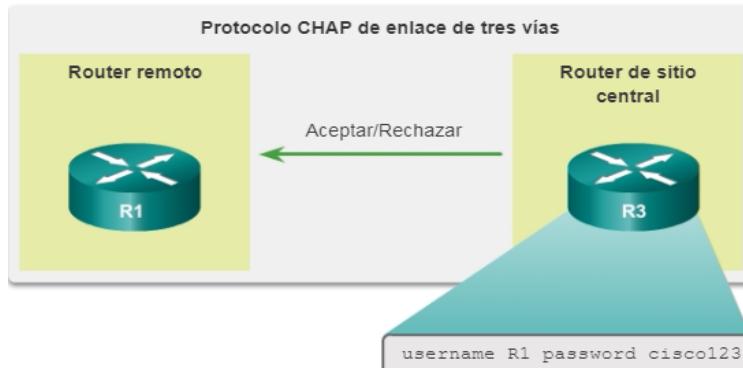
El nodo remoto responde con un valor calculado mediante una función de hash unidireccional, que suele ser la síntesis del mensaje 5 (MD5), según la contraseña y el mensaje de desafío.

El R1 responde al desafío CHAP del R3 enviando su nombre de usuario de CHAP y un valor de hash que se basa en la contraseña de CHAP.



El router local compara la respuesta con su propio cálculo del valor de hash esperado. Si los valores coinciden, el nodo de inicio reconoce la autenticación. Si el valor no coincide, el nodo de inicio finaliza la conexión de inmediato.

Con el nombre de usuario y la contraseña para el R1 en su base de datos local, el R3 compara su valor calculado de hash con el que se envió desde el R1.



CHAP proporciona protección contra los ataques de reproducción mediante el uso de un valor de desafío variable que es exclusivo e impredecible. Como la comprobación es única y aleatoria, el valor hash resultante también es único y aleatorio. El uso de comprobaciones reiteradas limita el tiempo de

exposición ante cualquier ataque. El router local o un servidor de autenticación de terceros, tiene el control de la frecuencia y la temporización de las comprobaciones.

Configuración de PPP con PAP

Defina el nombre de usuario y la contraseña que espera recibir del router remoto:

```
Router(config)#username[nombre del remoto] password[contraseña del remoto]
```

Para activar la encapsulación PPP con autenticación PAP en una interfaz se debe cambiar la encapsulación en dicha interfaz serial, el tipo de autenticación y la dirección IP:

```
Router(config-if)#encapsulation PPP  
Router(config-if)#ppp authentication pap  
Router(config-if)#ip address [dirección IP+máscara]  
Router(config-if)#no shutdown
```



Configuración de PPP con CHAP

Defina el nombre de usuario y la contraseña que espera recibir del router remoto:

```
Router(config)#username[nombre del remoto] password[contraseña del remoto]
```

Puede usar el mismo nombre de host en múltiples routers cuando quiera que el router remoto crea que está conectado a un solo router

Para activar la encapsulación PPP con autenticación CHAP en una interfaz se debe cambiar la encapsulación en dicha interfaz serial, el tipo de autenticación el nombre con el que el router remoto reconocerá el local, la contraseña con la que hará el desafío el router local y la dirección IP:

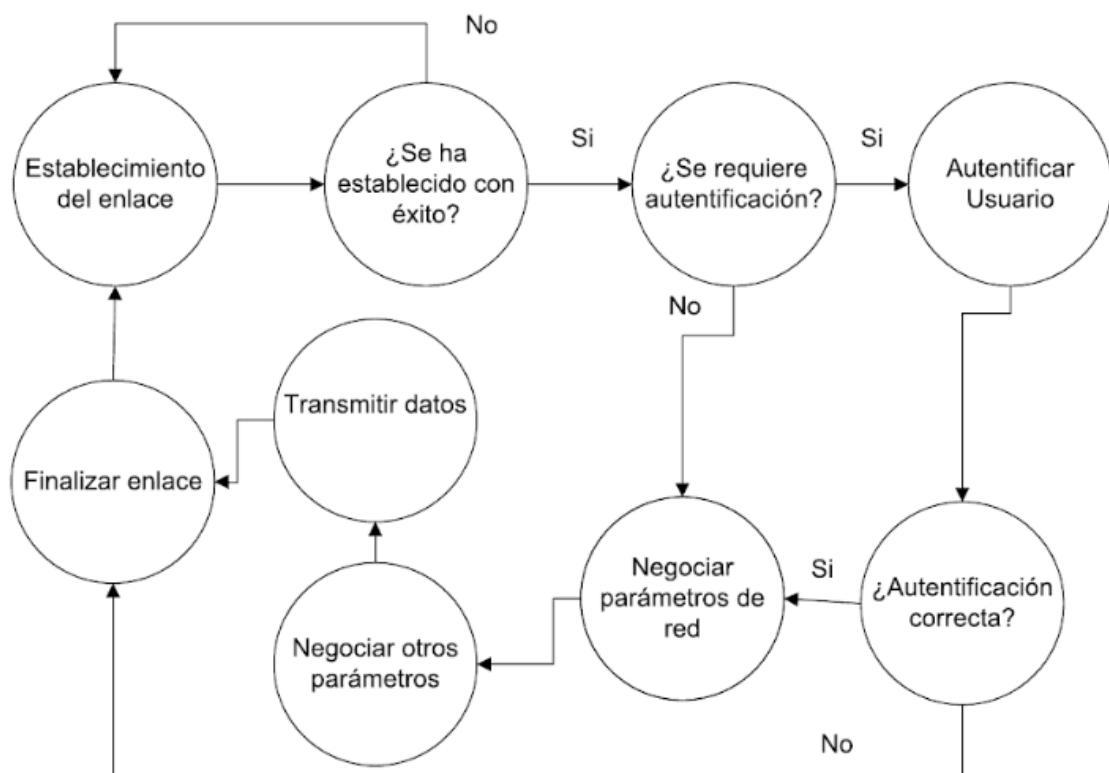
```
Router(config-if)#encapsulation PPP  
Router(config-if)#ppp authentication chap  
Router(config-if)#ip address [dirección IP+máscara]  
Router(config-if)#no shutdown
```

Para autenticarse frente a un host desconocido debe configurar en la interfaz correspondiente la contraseña que será enviada a los hosts que quieran autenticar al router. También sirve para limitar la cantidad de entradas en el router.

```
Router(config-if)#ppp chap password[contraseña]
```



El diagrama de flujo se puede utilizar para ayudar a comprender el proceso de autenticación PPP al configurar este protocolo. El diagrama de flujo proporciona un ejemplo visual de las decisiones lógicas que toma PPP.



CAPITULO 2

Redes ópticas de transporte

Estructuras de multicanalización

El desarrollo de los sistemas de transmisión digital empezó a principios de los años 70s, y fueron basados principalmente en el método de modulación PCM.

A principios de los 80s los sistemas digitales se hicieron cada vez más complejos, tratando de satisfacer las demandas de tráfico de esa época. La demanda fue tal alta que en Europa se tuvieron que aumentar las jerarquías de tasas de transmisión de 140Mbps a 565Mbps.

El problema era el alto costo del ancho de banda y de los equipos digitales. La solución era crear una técnica de modulación que permitiera la combinación gradual de tasas no síncronas (referidas como plesiocronos), lo cual derivó al término que conocemos hoy en día como PDH.

Introducción a SONET/SDH.

A partir de la introducción de la tecnología PCM hacia 1960, las redes de comunicaciones fueron pasando gradualmente a la tecnología digital en los años siguientes. Para poder soportar la demanda de mayores velocidades binarias surgió la jerarquía PDH (Plesiochronous Digital Hierarchy).

Pero como las velocidades de transmisión de esta jerarquía no son las mismas para EEUU y Japón que para Europa, las pasarelas entre redes de ambos tipos es compleja y costosa. Además si se tiene en cuenta que para poder llegar a un canal de 64Kb/s (canal de voz), habría que poner una cadena de multiplexores y demultiplexores, con el incremento de costo que esto significa.

El objetivo de la jerarquía SDH, nacida en los años 80's, era subsanar estas desventajas inherentes a los sistemas PDH, así como también normalizar las velocidades superiores a 140Mb/s que hasta el momento eran propietarias de cada compañía.. Los patrones de tráfico en los años 90's cambiaron drásticamente, ahora los datos superaban al tráfico de voz.

Las redes de alta velocidad de hoy en día son ópticas y están basadas principalmente en dos estándares conocidos como SDH y SONET, los cuales consisten de anillos de fibra óptica en los cuales la información es intercambiada electrónicamente en los nodos. Tanto SDH como SONET son las tecnologías de transporte dominantes en las redes metropolitanas de los proveedores de servicios de telecomunicaciones en la actualidad.

Definiciones importantes.

Modos de sincronización

Se distinguen cuatro modos de sincronización, a saber

- síncrono;
- seudosíncrono;
- plesiócrono;
- asíncrono.

En el modo síncrono, todos los relojes de la red se ajustan al PRC de la red. Los ajustes de puntero solamente se producirán al azar. Éste es el modo normal de funcionamiento en el dominio de un mismo operador.

En el modo seudosíncrono, no todos los relojes de la red estarán sincronizados con referencia al mismo PRC. Sin embargo, cada PRC deberá cumplir lo establecido en la Recomendación UIT-T G.811, por lo que se producirán ajustes de puntero en el elemento de red de frontera de sincronización. Éste es el modo normal de funcionamiento en la red internacional y entre operadores.

En el modo plesiócrono se inhabilitan el camino de sincronización y las alternativas de repliegue para uno o más relojes de la red. El reloj pasa al modo retención o de funcionamiento libre. Si se pierde la sincronización con respecto a un elemento de red SDH que efectúa la correspondencia asíncrona, el desplazamiento de frecuencia y la deriva del reloj harán que los ajustes de puntero persistan durante todo el periodo de conexión de la red SDH. Si se pierde la sincronización con respecto al último elemento de red de la conexión de red SDH (o al penúltimo elemento de red en el caso en que el último sea subordinado, es decir consista en un multiplexor con bucle temporizado) habrá que proceder también a ajustes de puntero a la salida de la red SDH. Sin embargo, si el fallo de la sincronización se produce en un elemento de red intermedio, ello no provocará un movimiento de puntero neto en el elemento de red de salida final, siempre que el elemento de red de entrada se mantenga sincronizado con el PRC. El movimiento del puntero en el elemento red intermedio será corregido por el elemento de red siguiente de la conexión, que se mantiene aún sincronizado.

El modo asíncrono se corresponde con la situación en la que se producen amplios desplazamientos de frecuencia. No es preciso que la red SDH mantenga tráfico con una precisión de reloj inferior a la especificada en la Recomendación UIT-T G.813. Para el envío de las AIS se requiere una precisión de reloj de 20 ppm (aplicable a los regeneradores y a cualquier otro equipo SDH en los que la pérdida de todas las señales de sincronización entrantes implique la pérdida de la totalidad del tráfico).

Qué es SONET/SDH.

SONET y SDH son un conjunto de estándares para la transmisión o transporte de datos síncronos a través de redes de fibra óptica. SONET significa por sus siglas en inglés, Synchronous Optical NETwork; SDH viene de Synchronous Digital Hierarchy. Aunque ambas tecnologías sirven para lo mismo, tienen pequeñas diferencias técnicas, de manera semejante con el T1 y el E1. SONET, por su parte, es utilizada en Estados Unidos, Canadá, Corea, Taiwán y Hong Kong; mientras que SDH es utilizada en el resto del mundo. Los estándares de SONET están definidos por la ANSI (American National Standards Institute) y los SDH por la ITU-T (International Telecommunications Union). En la tabla 2 se muestra la equivalencia entre SDH y SONET en cuestión de velocidades o tasas de bits.

La tasa de bits se refiere a la velocidad de información que es transportada a través de la fibra óptica. Una porción de estos bits sobre la línea son designados como overhead. El overhead transporta información que provee capacidades de tales como ensamblado de tramas, multicanalización, estatus de la red, rastreo, monitoreo de desempeño y funciones conocidas como OAM&P (Operations, Administration, Maintenance and Provisioning). Los bits restantes es la carga útil, es decir el ancho de banda disponible para transportar los datos de los usuarios tales como paquetes o celdas ATM (Asynchronous Transfer Mode) o cualquier otro tipo de información.

Hay que resaltar que la progresión de velocidad de datos comienza en 155 Mbit/s y aumenta en múltiplos de 4. La única excepción es OC-24, que está normalizado en ANSI T1.105, pero no es una velocidad SDH estándar de la ITU-T G.707. A veces se describen otras tasas como OC-9, OC-18, OC-36 y OC-96 y OC-1536, pero probablemente nunca han sido desplegados. Sin duda no son comunes y no son compatibles con las normas.

La siguiente velocidad de 160 GB/s OC-3072/STM-1024 no se ha normalizado todavía, debido al coste de transceptores de alta velocidad, al ser más baratos los multiplex de longitudes de onda a 10 y 40 Gbit/s.

Por otro lado, este incremento en las necesidades de ancho de banda, ha supuesto un rápido desarrollo de WDM (Wavelength Division Multiplexing); tecnología que ofrece en la actualidad la posibilidad de transportar hasta 160 canales de 10 Gbps sobre una única fibra óptica. En efecto, la red de transporte está en estos momentos pasando por un período de transición, evolucionando desde las tradicionales redes ATM y SONET/SDH basadas en la multiplexación en el tiempo con WDM utilizado estrictamente para incrementar la capacidad de la fibra óptica, hacia una red fotónica basada en la multiplexación en frecuencia óptica; realizando no sólo el transporte, sino también la multiplexación, encaminamiento, supervisión y protección en la capa óptica. Las ventajas de una red totalmente óptica son, entre otras, una menor complejidad, una mayor transparencia respecto a las señales transportadas, un mayor ancho de banda y mayores distancias de transmisión.

El modo de transferencia asíncrono o ATM (Asynchronous Transfer Mode) estandarizado por el ITU-T es una tecnología de nivel de enlace de conmutación rápida de pequeñas celdas o paquetes de longitud fija de 53 bytes, diseñada para transportar cualquier tipo de tráfico (voz, datos, imágenes o multimedia) basándose en la calidad de servicio o QoS (Quality of Service) demandada por los usuarios finales. ATM proporciona un ancho de banda escalable que va desde los 2 Mbps a los 10 Gbps; y debido a su naturaleza asíncrona, es más eficiente que las tecnologías síncronas, tales como la multiplexación por división en el tiempo o TDM (Time Division Multiplexing) en la que se basa SONET/SDH.

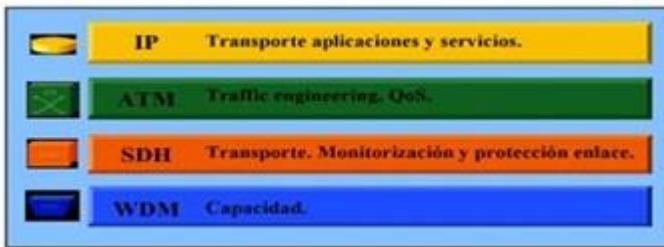
La red óptica síncrona o SONET (Synchronous Optical NETwork) estandarizada por el ANSI para Norte América y la jerarquía digital síncrona o SDH (Synchronous Digital Hierarchy) estandarizada por el ITU-T para todo el mundo y compatible en parte con SONET, son tecnologías de transmisión por fibra óptica diseñadas principalmente para la transmisión de voz

SONET/SDH apuesta por arquitecturas en anillo, constituidas por multiplexores de extracción e inserción de señales o ADMs (Add and Drop Multiplexers). Los anillos permiten conseguir redes muy flexibles, pudiendo extraer señales tributarias del tráfico agregado en cualquiera de los ADMs, además de ofrecer potentes mecanismos de protección y restauración.

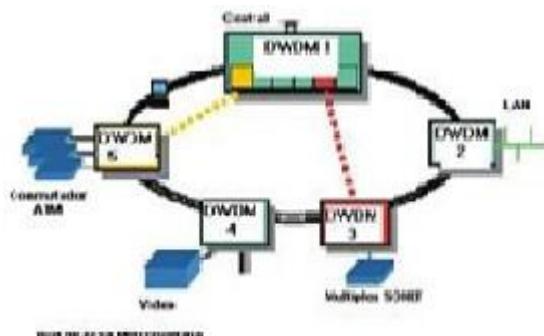
DWDM puede ayudar a la exhausta fibra, su valor se extiende más allá de esta simple ventaja, en SONET/SDH el aumento de la capacidad es la base de tirar más cable o ampliarlo, pero DWDM hace más que esto, porque lo que le da valor añadido en las redes metropolitanas, es su rápido y flexible aprovisionamiento de protocolos del DWDM, transparente en cuanto a la velocidad, centralización de datos, servicios protegidos, junto a la posibilidad de ofrecer nuevas y más altas velocidades a menor costo

Las Redes DWDM deben ser capaces de soportar la amplia gama de servicios que se implementan sobre TDM (SONET o SDH) y ATM además debe soportar conexiones de redes punto a punto, anillo, permitir la conectividad entre anillos, mallas y topología de estrella mientras provee la combinación de redes de banda ancha y transporte óptico.

Arquitectura de la Red.



La capa WDM proporciona la flexibilidad para mapear el tráfico generado en las longitudes de onda múltiple y la topología básica es un anillo de Fibra óptica que interconecta varios puntos de acceso que usan los canales ópticos.



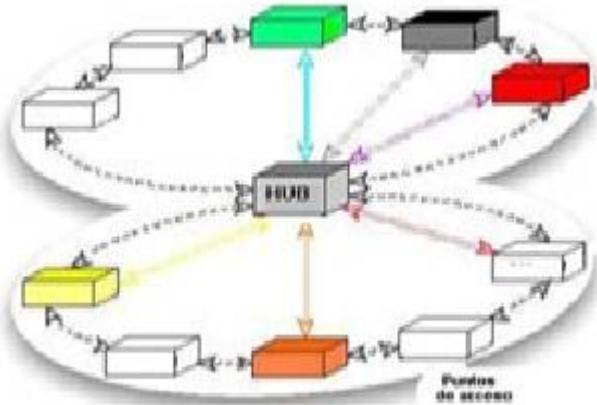
Anillo de fibra con diferentes conexiones.

En esta topología, un solo par de fibra conecta muchos elementos y les permite que transporten el tráfico entre si y hacia cada uno de ellos, la configuración en anillo es la de máxima conectividad con mínimo de ramas, permitiendo la constitución de redes gestionables flexibles además es tolerante a fallos, una estructura en anillo permite protección eficiente al establecer los canales de servicio y de protección por caminos diferentes. Cada punto de acceso ofrece un Multiplexor Add/Drop óptico que agrega y extrae canales ópticos hacia y desde el anillo, además cada punto de acceso debe procesar el tráfico según la capa y el protocolo con el tráfico asociado, como SONET, ATM, TDM, IP, etc., los canales de WDM son utilizados para conectar a los nodos en el anillo y soportar la conectividad punto a punto entre ellos y los sistemas de protección deben aplicarse para que el canal óptico se transmita en ambas direcciones en el anillo y el receptor selecciona la señal con más calidad, además si una de las trayectorias se interrumpe se conmuta la otra.

Conexión entre anillos.

La Red Óptica debe soportar la interconexión de muchos anillos para formar una red de área metropolitana multi-anillo, las opciones de topologías adicionales como son la malla y estrella también deben ser asimiladas.

Una red de anillo dual se muestra en la figura, donde pueden ser implementados canales adicionales ajenos al DWDM fuera de los anillos y pueden usarse para protección o para aumentar el ancho de banda que puede cruzar entre los anillos.



Anillo de Fibra Dual.

Estándares SDH/SONET.

Los estándares son una parte bien importante es las telecomunicaciones. Como se menciono anteriormente. ANSI coordina y aprueba los estándares de SONET mientras que los estándares de SDH son desarrollados por la ITU-T. Estándares ANSI de SONET

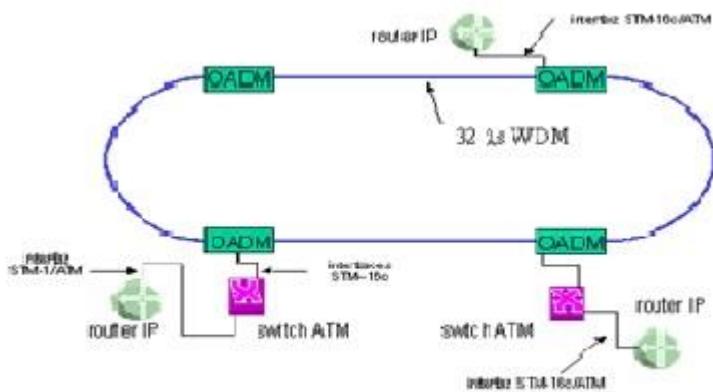
Los estándares de SONET son actualmente desarrollados por el comité T1 el cual es patrocinado por la ANSI y por la ATIS (Alliance for Telecommunications Industry Solutions).

ANSI		ITU	
Señal	Tasa de bits	Canales	Señal
DS0	64 Kbps	1 DS0	E0
DS1	1.544 Mbps	24 DS0	E1
DS2	6.312 Mbps	96 DS0	E2
DS3	44.736 Mbps	28 DS1	E3
No definido		E4	139.264 Mbps
			64 E1

Aplicaciones de SONET/SDH.

Como toda evolución, debe realizarse gradualmente. Los equipos de telefonía y de datos antiguos deben cambiarse poco a poco. La clave del SONET/SDH es que permite interfaces con fuentes asíncronas por lo que los equipos existentes pueden ser sustituidos o soportados por la red SDH. De esta forma las transiciones se pueden realizar gradualmente.

De este modo, teniendo en cuenta que IP se convertirá en la base de todos los servicios de telecomunicaciones y WDM en la tecnología de transporte más utilizada, ha habido un interés creciente en la integración de IP sobre las redes fotónica



Ejemplo de IP sobre ATM sobre encapsulación SDH para el transporte sobre una red WDM.

La tecnología SONET/SDH estaba inicialmente optimizada para el transporte de tráfico de voz, pero la aparición del estándar PoS (Packet Over SONET), estandarizado en la RFC 2615 del IETF, la ha convertido también en una alternativa muy eficiente para el tráfico de datos. El esquema de una red de este tipo puede ser el de gigarouters IP que simplemente utilizan el formato de trama SONET/SDH para entramar los paquetes IP encapsulados para su transmisión directa sobre WDM, o también es posible transportar el paquete IP entramado mediante SONET/SDH sobre una red de ADMs SONET/SDH junto a otro tipo de tráfico, que utilizará luego enlaces WDM.

En efecto, PoS proporciona un método para optimizar el transporte de paquetes de datos en tramas SONET/SDH. Para ello, primero es necesario que los paquetes IP sean encapsulados en el nivel de enlace mediante PPP (Point-to-Point Protocol) según la RFC 1662, siguiendo un entramado tipo HDLC (High-level Data Link Control) según la RFC 1661. Finalmente, las tramas HDLC son transportadas sobre la carga útil de un VC-4 o varios VC-4s concatenados según la RFC 2615.

Como SDH y SONET tienen características diferentes, ahora vamos a mencionar a cada uno de estos estándares por separado.

SDH es un estándar para redes de telecomunicaciones de "alta velocidad, y alta capacidad". Más específicamente es una jerarquía digital sincrónica. Este es un sistema de transporte digital realizado para proveer una infraestructura de redes de telecomunicaciones más simple, económica y flexible.

Estándares SDH de la ITU-T.

El sector de telecomunicaciones de la ITU (ITU-T) es el encargado de coordinar y desarrollar los estándares de SDH para el mundo. A continuación en la tabla 4 se listan los estándares más importantes de SDH, la lista completa se puede obtener en el sitio de la ITU.

Tabla 4. Estándares SDH de la ITU-T

Estándar	Descripción
ITU-T G.707	Interface del nodo de red para SDH
ITU-T G.781	Estructura de recomendaciones para SDH
ITU-T G.782	Características y tipos de equipos para SDH
ITU-T G.783	Características de bloques funcionales de SDH
ITU-T G.803	Arquitectura de redes de transporte basadas en SDH

Otros estándares importantes son el ITU-T I.432 donde se especifica la capa física Interface de red-usuario de B-ISDN (ISDN de banda ancha) o mejor conocido como ATM sobre SONET. El IETF (Internet Engineering Task Force) también ha liberado algunos RFCs (Request for Comments) que describen el protocolo punto a punto para transferir tráfico nativo IP sobre SONET o SDH, tales como:

- IETF RFC2615: PPP sobre SONET/SDH
- IETF RFC1661: PPP (Point to Point Protocol)
- IETF RFC1662: PP en tramas HDLC (High Level Data Link Control)

Componentes de una red síncrona.

Las redes SDH actuales están formadas básicamente por cuatro tipos de elementos. La topología (estructura de malla o de anillo) depende del proveedor de la red.

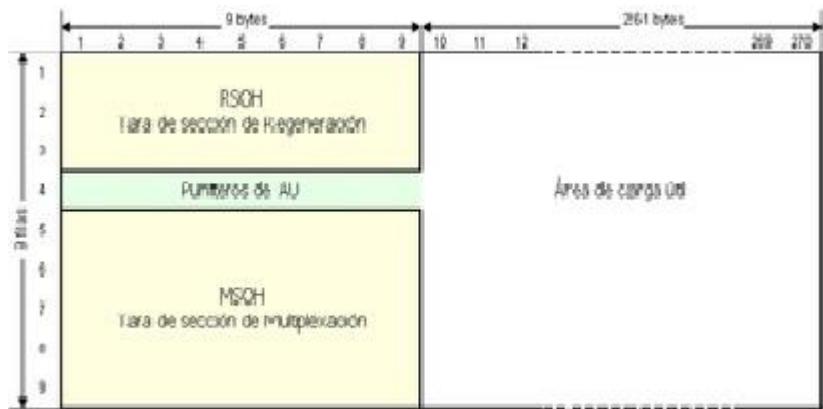
- **Regeneradores:** Se encargan de regenerar el reloj y la amplitud de las señales de datos entrantes que han sido atenuadas y distorsionadas por la dispersión y otros factores. Obtienen sus señales de reloj del propio flujo de datos entrante. Los mensajes se reciben extrayendo varios canales de 64 kbit/s de la cabecera RSOH.
- **Multiplexores:** Se emplean para combinar las señales de entrada plesioácronas y terminales síncronas en señales STM-N de mayor velocidad.
- **Multiplexores add/drop (ADM):** Permiten insertar (o extraer) señales plesioácronas y síncronas de menor velocidad binaria en el flujo de datos SDH de alta velocidad. Gracias a esta característica es posible configurar estructuras en anillo, que ofrecen la posibilidad de conmutar automáticamente a un trayecto de reserva en caso de fallo de alguno de los elementos del trayecto.
- **Transconectores digitales (DXC):** Este elemento de la red es el que más funciones tiene. Permite mapear las señales tributarias PDH en contenedores virtuales, así como conmutar múltiples contenedores, hasta VC-4 inclusive.

Gestión de los elementos de la red.

Todos los elementos SDH mencionados hasta ahora se controlan por software, lo que significa que pueden monitorizarse y controlarse desde un lugar remoto, una de las ventajas más importantes de los sistemas SDH.

La fibra óptica es el medio físico más habitual en las redes SDH. La ventaja de las fibras ópticas es que no son susceptibles a las interferencias y que pueden transportar las señales a velocidades muy elevadas (citadas anteriormente cuando hablamos del multiplexado DWDM). La desventaja es el costo relativamente alto de la fibra y su instalación. Las fibras monomodo son la opción preferida para la segunda y tercera ventana óptica (1310 y 1550 nm). Otro método posible para transmitir las señales SDH es un radio enlace o un enlace por satélite, ambos particularmente adecuados para configurar rápidamente circuitos de transmisión, o para formar parte de redes de comunicaciones móviles o en terrenos difíciles. Las desventajas en este caso son el ancho de banda limitado (actualmente hasta STM-4) y la complejidad que plantea integrar esos trayectos en el sistema de gestión de la red.

Estructura de la trama STM-1



Las tramas contienen información de cada uno de los componentes de la red: trayecto, línea y sección, además de la información de usuario. Los datos son encapsulados en contenedores específicos para cada tipo de señal tributaria.

A estos contenedores se les añade una información adicional denominada "tara de trayecto" (Path overhead), que consiste en una serie de bytes utilizados con fines de mantenimiento de red, y que dan lugar a la formación de los denominados contenedores virtuales (VC). El resultado de la multiplexación es una trama formada por 9 filas de 270 octetos cada una (270 columnas de 9 octetos). La transmisión se realiza bit a bit en el sentido de izquierda a derecha y de arriba abajo. La trama se transmite a razón de 8000 veces por segundo (cada trama se transmite en 125 µs). Por lo tanto, el régimen binario (Rb) para cada uno de los niveles es:

$$\text{STM-1} = 8000 * (270 \text{ octetos} * 9 \text{ filas} * 8 \text{ bits}) = 155 \text{ Mbps}$$

$$\text{STM-4} = 4 * 8000 * (270 \text{ octetos} * 9 \text{ filas} * 8 \text{ bits}) = 622 \text{ Mbps}$$

$$\text{STM-16} = 16 * 8000 * (270 \text{ octetos} * 9 \text{ filas} * 8 \text{ bits}) = 2.5 \text{ Gbps}$$

$$\text{STM-64} = 64 * 8000 * (270 \text{ octetos} * 9 \text{ filas} * 8 \text{ bits}) = 10 \text{ Gbps}$$

$$\text{STM-256} = 256 * 8000 * (270 \text{ octetos} * 9 \text{ filas} * 8 \text{ bits}) = 40 \text{ Gbps}$$

De las 270 columnas que forman la trama STM-1, las 9 primeras forman la denominada "tara" (overhead), independiente de la tara de trayecto de los contenedores virtuales antes mencionados, mientras que las 261 restantes constituyen la carga útil (Payload).

En la tara están contenidos bytes para alineamiento de trama, control de errores, canales de operación y mantenimiento de la red y los punteros, que indican el comienzo del primer octeto de cada contenedor virtual.

Medidas en las redes SDH:

En términos generales, los equipos de medida SDH deben ofrecer las funciones siguientes:
· Análisis de mapeado
· Alineamiento de interfaces de puertos
· Medidas con señales de prueba estructuradas
· Medidas en multiplexores add/drop
· Medidas de retardo

Prueba de los dispositivos de conmutación automática de protección (APS)
· Simulación de la actividad de los punteros
· Medidas SDH durante el servicio
· Análisis de alarmas
· Monitorización de identificadores de tramo
· Análisis de punteros
· Comprobación de los sensores integrados en el sistema inserción y extracción de canales
· Comprobación de la sincronización de la red
· Medidas en la interfaz TMN M.21 00
· Control de calidad según G.821, G.826 y
· Análisis de jitter y wander

Medida del tiempo de respuesta APS.

Cuando se produce un fallo en las redes SDH se activa un mecanismo especial de protección. El enlace defectuoso se reencamina automáticamente a través de un circuito de reserva. Esta función por ejemplo, se controla mediante los bytes K1 y K2 de la cabecera. La conmutación a la línea de protección debe efectuarse en menos de 50 ms. Para comprobar que la conmutación se efectúa correctamente y no tarda más de lo debido hay que emplear equipos de medida externos. Estos equipos miden el tiempo de respuesta (el estándar sdhs decir, la pérdida de un patrón de test específico o el disparo de una alarma preestablecida) cuando se interrumpe intencionadamente la conexión. La medida es muy importante, ya que un excesivo retardo en la respuesta puede ocasionar una considerable degradación de las prestaciones de la red e incluso el fallo total de ésta con grandes perjuicios económicos para el proveedor de la red.

Características principales de SDH.

- Velocidad básica 155Mb/s (STM-1)
· Velocidades de transmisión Los modernos sistemas SDH logran velocidades de 10 Gbit/s.
· Alta disponibilidad y grandes posibilidades de ampliación, La tecnología SDH permite a los proveedores de redes reaccionar rápida y fácilmente frente a las demandas de sus clientes.
- Función simplificada de inserción/extracción, ahora es mucho más fácil extraer o insertar canales de menor velocidad en las señales compuestas SDH de alta velocidad. Ya no hace falta demultiplexar y volver a multiplexar la estructura plesiócrona, procedimiento que en el mejor de los casos era complejo y costoso. Esto se debe a que en la jerarquía SDH todos los canales están perfectamente identificados por medio de una especie de "etiquetas" que hacen posible conocer exactamente la posición de los canales individuales.
- Fiabilidad, Las modernas redes SDH incluyen varios mecanismos automáticos de protección y recuperación ante posibles fallos del sistema.
- Plataforma a prueba de futuro, Hoy día, SDH es la plataforma ideal para multitud de servicios, desde la telefonía tradicional, las redes RDSI o la telefonía móvil hasta las comunicaciones de datos (LAN, WAN, etc.) y es igualmente adecuada para los servicios más recientes, como el video bajo demanda (VOD) o la transmisión de video digital vía ATM.
- Interconexión, Las interfaces SDH están normalizadas, lo que simplifica las combinaciones de elementos de redes de diferentes fabricantes.
- Técnica de multiplexado a través de punteros
- Estructura modular: A partir de la velocidad básica se obtienen velocidades superiores multiplexando byte por byte varias señales STM-1. Las velocidades multiplexadas, a diferencia de PDH, son múltiplos enteros de la velocidad básica..

A través del puntero, se puede acceder a cualquier canal de 2Mb/s.. Posee gran cantidad de canales de overhead que son utilizados para supervisión, gestión, y control de la red.

Desventajas de SDH.

El tráfico está cambiando, como hacer uso eficiente del ancho de banda para voz y datos.· Falta de granularidad fina para acomodar todos los flujos (Streams) de todos los clientes potenciales.· Necesidad de una gestión fácil en la Oficina Central. (CO). Siguen surgiendo problemas sobre todo cuando se combinan elementos de redes de distintos fabricantes.· Los problemas de transmisión en las pasarelas que conectan redes de operadores. Necesidad de sincronismo entre los nodos de la red SDH, se requiere que todos los servicios trabajen bajo una misma referencia de temporización.

SONET es un estándar para el transporte de telecomunicaciones ópticas formulado por la Exchange Carriers Standards Association (ECSA) para la American National Standards Institute (ANSI) para las industrias que manejan los estándares de telecomunicaciones y es básicamente una implementación de multiplexado al medio tan "ancho" como es la fibra óptica, y forma un estándar norteamericano. SONET/SDH, esperan proporcionar la infraestructura mundial en materia de telecomunicaciones por lo menos para las próximas dos o tres décadas. El incremento de la configuración flexible y su disponibilidad del ancho de banda de SONET, proporciona múltiples ventajas sobre los antiguos sistemas de telecomunicaciones.

Tabla 3. Estándares ANSI de SONET	
Estándar	Descripción
ANSI T1.105: SONET	Descripción básica incluyendo estructura de multicanalización, tasas y formatos
ANSI T1.105.01:SONET	Protección automática de Comutación
ANSI T1.105.02:SONET	Mapeos de la carga útil
ANSI T1.105.03:SONET	En las interfaces de red
ANSI T1.105.04:SONET	Protocolos y arquitecturas del canal de comunicaciones de datos
ANSI T1.105.05:SONET	Mantenimiento de conexión en cascada
ANSI T1.105.06:SONET	Especificaciones de la capa física
ANSI T1.105.07:SONET	Especificación de formatos e tasas de interfaz sub-STS
ANSI T1.105.09:SONET	Elementos de sincronización de la red
ANSI T1.119:SONET	Comunicaciones - OAM&P

Sincronización de las señales digitales

Para entender los conceptos y detalles del SONET correctamente, es importante tener claro todo lo referente a sincronía, asincronía y plesiocronía. En lo que se refiere a señales síncronas, la transición digital de estas señales ocurre exactamente al mismo tiempo. Sin embargo, esto permite tener una fase diferente entre la transición de dos señales y esto quedaría dentro de los límites especificados. Esta

diferencia de fase puede ser debido a los retrasos de propagación en el tiempo o a temblores "jitter" que se introducen en la transmisión de la red. En una red sincrónica todos los relojes están identificados con una primera referencia de reloj (PRC). Si dos señales digitales son Pleosíncronas, sus transiciones ocurren casi a la misma tasa con una variación contenida dentro de los límites. Por ejemplo, si dos redes están interconectadas, sus relojes pueden estar derivados de dos diferentes PRCs. Aunque estos relojes son extremadamente exactos, está es la diferencia entre un reloj y otro. En el caso de señales asíncronas, la transición de señales no necesariamente ocurren a la misma tasa. Asincronía en este caso significa que la diferencia entre dos relojes es mucho mayor que una diferencia plesioocrónica. Por ejemplo, si dos relojes se derivan de dos osciladores diferentes, estos pueden ser descritos como asíncronos.

Sincronización Jerárquica.

Los switches cruzados y los sistemas digitales de conexión cruzada son comúnmente empleados en las redes digitales de sincronización jerárquica. La red está organizada con una relación maestro - esclavo entre los nodos de los relojes de más alto nivel y los nodos de reloj de menor nivel. Todos los nodos pueden ser montados a la fuente de referencia primaria, un estrato 1 reloj atómico con una muy alta estabilidad y exactitud. Los relojes menos estables son adecuados para soportar nodos más bajos.

SONET Sincronizado.

El reloj interno de una terminal SONET puede derivarse de una señal de tiempo para construir un suministro de tiempo integrado (BITS) usado para sistemas de switches y otros equipos. Así, estas terminales como un maestro para otros nodos SONET proporcionando tiempos sobre las salidas de señales OC-N. Otros nodos SONET operarán como el modo de esclavos llamados "loop timing" con sus propios relojes internos para las entradas de las señales OC-N. Estándares especifican que las redes SONET deben ser capaces de derivar este tiempo para un estrato 3 o un reloj más alto.

Elementos de la Red SONET.

- Multiplexor terminal: Es el elemento que actúa como un concentrador de las señales DS-1 (1,544 Mbps) tributarias así como de otras señales derivadas de ésta y realiza la transformación de la señal eléctrica en óptica y viceversa. Dos multiplexores terminales unidos por una fibra con o sin un regenerador intermedio conforman el más simple de los enlaces de SONET.
- Regenerador: Necesitamos un regenerador cuando la distancia que separa a dos multiplexores terminales es muy grande y la señal óptica que se recibe es muy baja. El reloj del regenerador se apaga cuando se recibe la señal y a su vez el regenerador reemplaza parte de la cabecera de la trama de la señal antes de volver a retransmitirla. La información de tráfico que se encuentra en la trama no se ve alterada.
- Multiplexor Add/Drop (ADM): El multiplexor de extracción-inserción (ADM) permite extraer en un punto intermedio de una ruta parte del tráfico cursado y a su vez injectar nuevo tráfico desde ese punto. En los puntos donde tengamos un ADM, solo aquellas señales que necesitemos serán descargadas o insertadas al flujo principal de datos. El resto de señales a las que no tenemos que acceder seguirá a través de la red. Aunque los elementos de red son compatibles con el nivel OC-N, puede haber diferencias en el futuro entre distintos vendedores de distintos elementos. SONET no restringe la fabricación de los elementos de red. Por ejemplo, un vendedor puede ofrecer un ADM con acceso únicamente a señales DS-1, mientras que otro puede ofrecer acceso simultáneo a señales DS-1 (1,544 Mbps) y DS-3 (44,736 Mbps).

La señal básica de SONET.

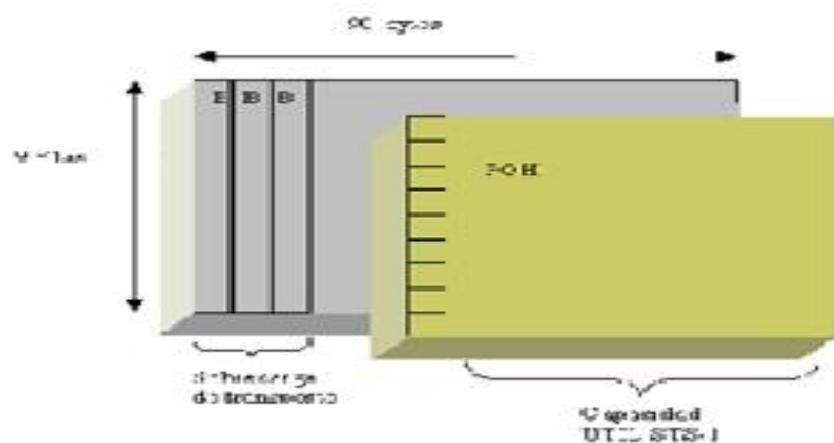
SONET define una tecnología para transportar muchas señales de diferentes capacidades a través de una jerarquía óptica síncrona y flexible. Esto se logra por medio de un esquema de multiplexado por interpolación de bytes. La interpolación de bytes simplifica la multiplexación y ofrece una administración de la red extremo a extremo.

El primer paso en el proceso de la multiplexación de SONET implica la generación de las señales del nivel inferior de la estructura de multiplexación. En SONET la señal básica la conocemos como señal de nivel 1 o también STS-1 (Synchronous Transport Signal level 1). Está formada por un conjunto de 810 bytes distribuidos en 9 filas de 90 bytes. Este conjunto es transmitido cada 125 microsegundos, correspondientes a la velocidad del canal telefónico básico de 64 Kbps, por lo que la velocidad binaria de la señal STS-1 es 51,84 Mbps.



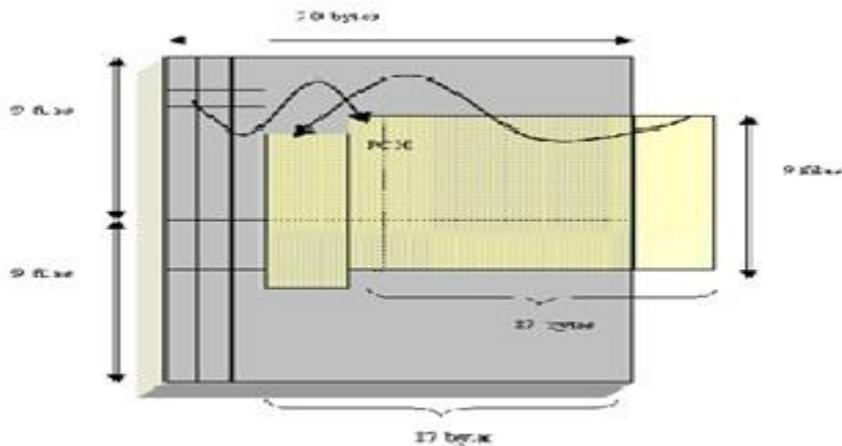
Estructura de trama de la señal STS-1

Hay 27 bytes reservados para sobrecarga del transporte. 9 para la sección y 18 para las líneas. La carga útil de la trama es de 87 columnas y 9 filas, donde la columna primera contiene 9 bytes reservados para información del servicio de trayecto (POH Path overhead), para mandar información de funciones entre el punto de origen y el de destino. Los 774 bytes restantes quedan libres para datos.



Esquema de la capacidad útil.

La carga útil puede empezar en cualquier parte de la capacidad de la trama. Típicamente comienza en una trama y termina en la siguiente aunque podría contenerse en una sola. El puntero de carga indica donde empieza. Esto se hace para lograr una buena sincronización.



Las señales de niveles más altos están formadas por la multiplexación de diversas señales de nivel 1 (STS-1), creando una familia de señales STS-N, donde la N indica el número de señales de nivel 1 que la componen. En la Tabla 1 se indican las denominaciones de las señales eléctricas y portadoras ópticas, así como sus velocidades y los puntos de coincidencia con los de la Jerarquía Digital Síncrona.

Sincronización.

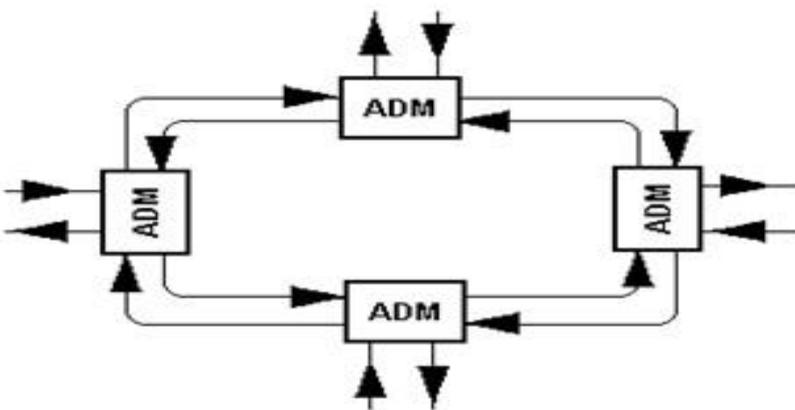
Cada señal SONET (análogo SDH) STS-1 lleva un puntero de carga útil en su sobrecarga de línea. Éste es una innovación clave de los sistemas SDH/SONET y se usa para sincronizar la multiplexación en un entorno pleosíncrono y en la alineación de señales STS-N. Muchos sistemas usan un mapeado fijo de los datos de menor velocidad en el seno de un flujo de mayor velocidad. Eso permite un acceso más sencillo a las cargas útiles transportadas, ya que no es necesario desempaquetar o analizar datos. Lo que se hace es repetir o eliminar tramas de información para corregir las diferencias de temporización. Para ello se utilizan buffers temporales de 125 ms de capacidad. Son indeseables por culpa del retardo introducido y de los posibles errores producidos al perder datos. El puntero de carga útil (payload pointer) es un número que indica en cada línea STS-1 el byte de inicio de los datos de la trama. Consecuentemente el puntero no está vinculado a la estructura de trama sino que "flota" respecto a la trama. Las pequeñas variaciones de temporización acomodan incrementando o reduciendo el valor del puntero.

Configuración de la red SONET.

- Punto a punto: La configuración de red punto a punto está formada por dos multiplexores terminales, unidos por medio de una fibra óptica, en los extremos de la conexión y con la posibilidad de un regenerador en medio del enlace si éste hiciese falta. En un futuro las conexiones punto a punto atravesarán la red en su totalidad y siempre se originarán y terminarán en un multiplexor.
- Punto a multipunto: Una arquitectura punto a multipunto incluye elementos de red ADM a lo largo de su recorrido. El ADM es el único elemento de red especialmente diseñado para esta tarea. Con esto se evitan las incomodas arquitecturas de red de demultiplexado, conectores en cruz (cross-connect), y luego volver a multiplexar. Se coloca el ADM a lo largo del enlace para facilitar el acceso a los canales en los puntos intermedios de la red.

- Red Hub: La arquitectura de red hub está preparada para los crecimientos inesperados y los cambios producidos en la red de una forma más sencilla que las redes punto a punto. Un hub concentra el tráfico en un punto central y distribuye las señales a varios circuitos.
- Arquitectura en anillo: El elemento principal en una arquitectura de anillo (Figura 2) es el ADM. Se pueden colocar varios ADM en una configuración en anillo para tráfico bidireccional o unidireccional. La principal ventaja de la topología de anillo es su seguridad; si un cable de fibra se rompe o se corta, los multiplexores tienen la inteligencia necesaria para desviar el tráfico a través de otros nodos del anillo sin ninguna interrupción.

La demanda de servicios de seguridad, diversidad de rutas en las instalaciones de fibra, flexibilidad para cambiar servicios para alternar los nodos, así como la restauración automática en pocos segundos, han hecho de la arquitectura de anillo una topología muy popular en SONET.



Arquitectura en anillo

Beneficios de la Red SONET

La clave de SONET es que permite interfaces con fuentes asíncronas por lo que los equipos existentes pueden ser sustituidos o soportados por la red SONET. De esta forma las transiciones se pueden realizar gradualmente.

Ventajas de SONET.

- ✓ La creciente flexibilidad de configuración y la disponibilidad de ancho de banda de SONET proporciona significativas ventajas frente a otros sistemas de telecomunicación más antiguos.
- ✓ Reducción de los equipos necesarios para la multiplexación y la extracción-inserción de tráfico en puntos intermedios de las grandes rutas.
- ✓ Aumento de la fiabilidad de la red, como consecuencia del menor número de equipos implicados en las conexiones.
- ✓ Proporciona bytes de cabecera que facilitan la administración de los bytes de información y el mantenimiento de los propios equipos.
- ✓ Definición de un formato síncrono de multiplexación para el transporte de señales digitales de la Jerarquía Digital Plesiócrona o PDH, en sus diversos niveles (como DS-1, DS-3) y una estructura síncrona que simplifica enormemente la interfaz de los comutadores digitales, así como los conectores y los multiplexores.
- ✓ La existencia de una gran gama de estándares genéricos que permitan la interconexión de productos de diferentes fabricantes.
- ✓ La definición de una arquitectura flexible capaz de incorporar futuras aplicaciones, con una gran variedad de velocidades de transmisión.

Futuro de las redes de transporte.

Se tiende hacia velocidades mayores, tal como en el sistema STM-64 (multiplexado por división en el tiempo, TDM de 10 Gbps), pero los costos de los elementos de ese tipo son aún muy elevados, lo que está retrasando el proceso. La alternativa es una técnica llamada DWDM (multiplexación densa por división de longitud de onda) que mejora el aprovechamiento de las fibras ópticas monomodo, utilizando varias longitudes de onda como portadoras de las señales digitales y transmitiéndolas simultáneamente por la fibra. Los sistemas actuales permiten transmitir 16 longitudes de onda, entre 1520 nm y 1580 nm, a través de una sola fibra. Se transmite un canal STM-16 por cada longitud de onda, lo que da una capacidad de unos 40 Gbit/s por fibra. Ya se ha anunciado la ampliación a 32, 64 e incluso 128 longitudes de onda. Conectada al empleo del multiplexado DWDM se observa una tendencia hacia las redes en las que todos los elementos son ópticos. Ya existen en el mercado multiplexores add/drop (inserción / extracción) ópticos y se están realizando pruebas de dispositivos ópticos de transconexión (cross-connects). En términos del modelo de capas ISO-OS, este desarrollo significa básicamente la aparición de una capa DWDN, adicional debajo de la capa SDH. Probablemente pronto veremos velocidades binarias aún más elevadas gracias a la tecnología DWDM.

SDH de nueva generación

Actualmente se siguen desarrollando extensiones al protocolo para solucionar algunos de sus inconvenientes para el transporte de datos como por ejemplo:

- GFP (Generic Framing Protocol), UIT-T G.7041 que es un protocolo que estandariza el empaquetado de datos en tramas SDH/SONET, es superior a POS. (Packet over Sonet).
- VCAT (Virtual Concatenation), es una extensión de G.707 para la concatenación de contenedores virtuales (VC) de bajo y alto nivel. (VC-12, VC-3, VC-4)
- LCAS (Link Capacity Adjustment Scheme), G.7042 un mecanismo que permite la reconfiguración dinámica de los contenedores virtuales que transportan los datos.
- La combinación LCAS y VCAT es una herramienta para el ajuste del ancho de banda en demanda.
- Especificación de la interfaz STM-256. (40Gbits/Seg)

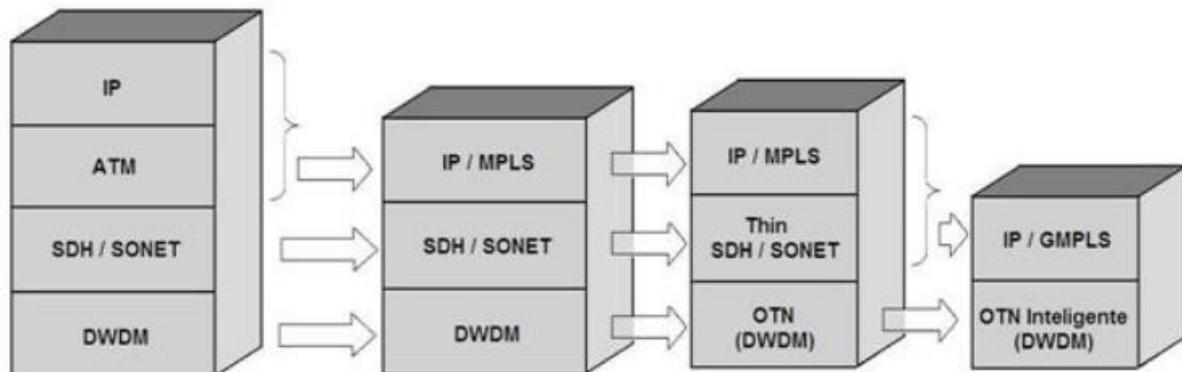
Se ha trabajado en la supresión de la capa SDH, pero simultáneamente esta tecnología evoluciona también hacia una alternativa que mejora las prestaciones en redes de datos y se mantiene en la competencia.

La mayoría de los equipos de transmisión actuales utilizan tramas SDH y SONET, las cuales están optimizadas para el tráfico de servicios de voz a 64 Kbit/s.

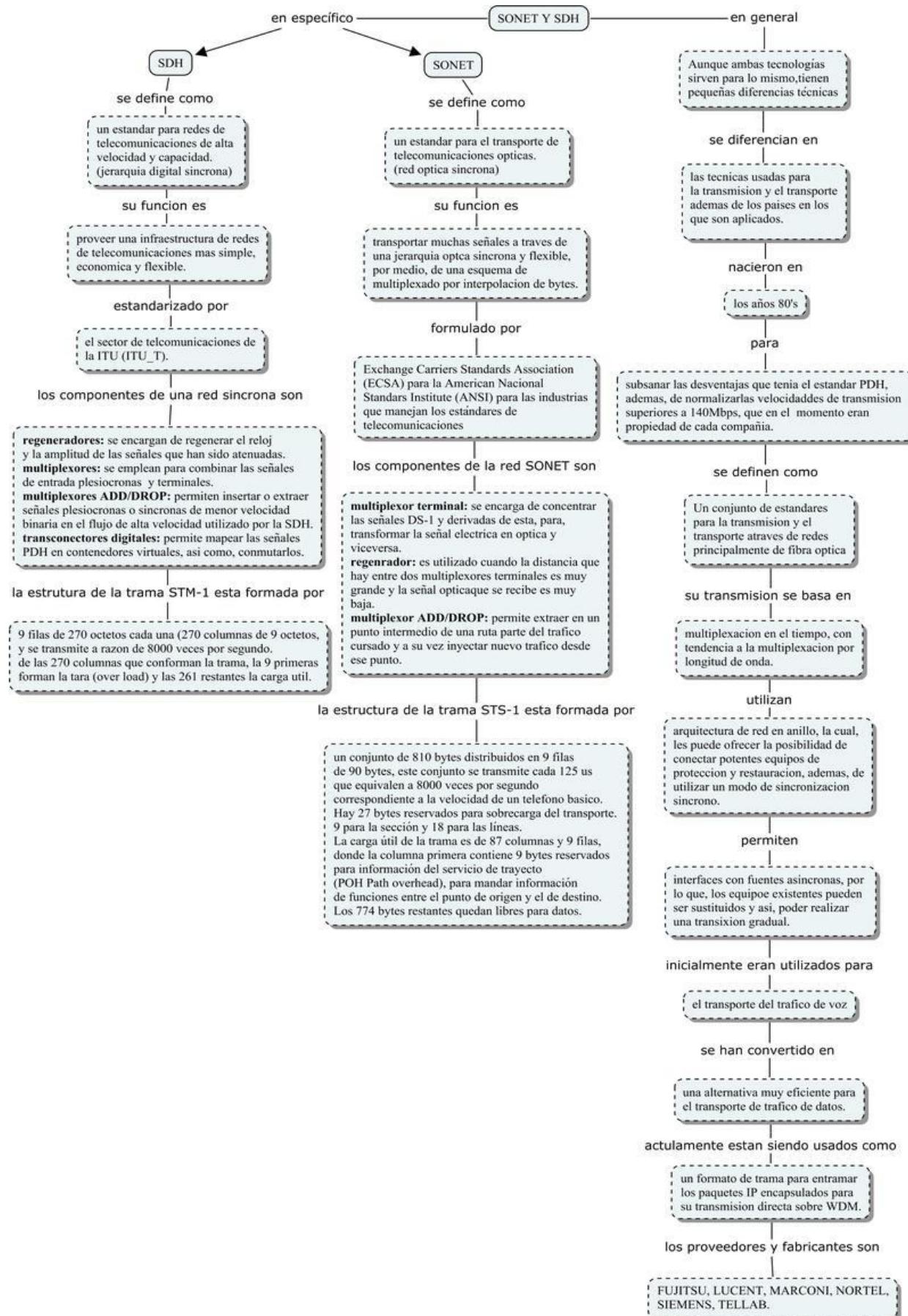
Algunas características de SONET y SDH han justificado su empleo en las Redes de Fibra Óptica durante los últimos tiempos, la más importante es que permite restaurar las conexiones punto a punto en caso de fallas en los enlaces o equipos intermedios, encontrando caminos alternativos para la transmisión.

Actualmente se desarrollan alternativas para la sustitución total de SDH.

Perspectivas de la Tecnología SDH



Evolución de la capa óptica según el modelo OSI.



DWDM(Dense Wavelength Division Multiplexing)

Multiplexación por división en longitud de onda densa)

WDM (Wavelength Division Multiplexing) es una tecnología de telecomunicaciones que transporta varias señales sobre una única fibra óptica, empleando para cada señal una longitud de onda (portadora) diferente.

Que es y motivos de invención.

Es un método de multiplexación muy similar a la multiplexación por división de frecuencias, que se utiliza en medios de transmisión electromagnéticos. Varias señales portadoras (ópticas) se transmiten por una única fibra óptica utilizando distintas longitudes de onda de un haz de luz para cada una de ellas. Cada portadora óptica forma un canal óptico que podrá ser tratado independientemente del resto de canales que comparten el medio (fibra óptica) y contener diferente tipo de tráfico. De esta manera se puede multiplicar el ancho de banda efectivo de la fibra óptica, así como facilitar comunicaciones bidireccionales. Se trata de una técnica de transmisión muy atractiva para los operadores de telecomunicaciones ya que les permite aumentar su capacidad sin tener más cables

Para transmitir mediante DWDM es necesario dos dispositivos complementarios: un multiplexor en lado del transmisor y un demultiplexor en el lado del receptor. A diferencia del CWDM, en DWDM se consigue mayor números de canales ópticos reduciendo la dispersión cromática de cada canal mediante el uso de un laser de mayor calidad, fibras de baja dispersión o mediante el uso de módulos DCM. De esta manera es posible combinar más canales reduciendo el espacio entre ellos.

Está definido para la banda de 1530 – 1610nm, espaciado entre canales de 0.8nm y 1.6nm.

Historia

El primer sistema WDM en combinar dos señales portadoras hizo su aparición alrededor de 1985. A principios del siglo XXI la tecnología permite combinar hasta 160 señales con un ancho de banda efectivo de unos 10 gbt/s por segundo. Ya las operadoras están probando los 40 gbt/s. No obstante la capacidad teórica de una sola fibra óptica se estima en 1600 Gbit/s. De manera que es posible alcanzar mayores capacidades en el futuro, a medida que avance la tecnología.

Los tempranos años 90 consideraron una segunda generación del WDM, a veces llamada narrowband WDM, en cuáles dos canales de ocho fueron utilizados. Estos canales ahora fueron espaciados en un intervalo cerca de 400 GH en la ventana 1550-nm. A mediados de los 1990s, los sistemas densos del WDM (DWDM) emergían con 16 a 40 canales y espaciaban a partir 100 a 200 GH. Por los últimos años 90 los sistemas DWDM se habían desarrollado a tal punto donde eran capaces de soportar de 64 a 160 canales paralelos, embalado denso en los intervalos de 50 o aún 25 GH.

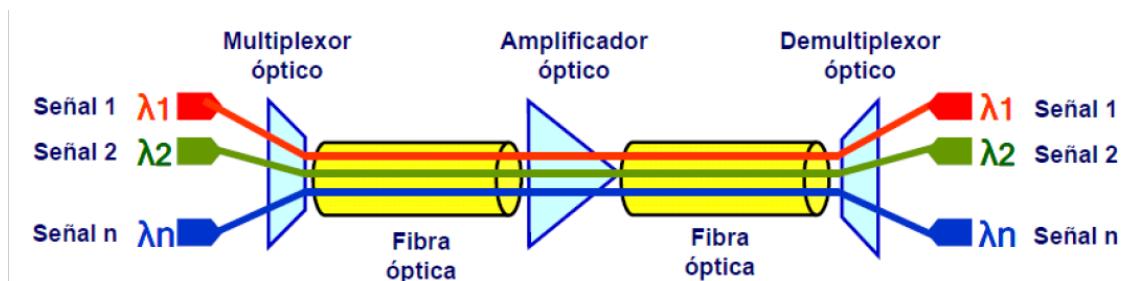
La progresión de la tecnología se puede considerar como aumento en el número de las longitudes de onda acompañadas por una disminución del espacio de las longitudes de onda. Junto con la densidad creciente de longitudes de onda, los sistemas también avanzaron en su flexibilidad de configuración, con funciones de agregar-gota, y capacidades de la administración. Los aumentos en la densidad del canal resultado de la tecnología DWDM han tenido un impacto dramático en la capacidad de carga de la fibra. En 1995, cuando los primeros sistemas 10 de Gbps fueron demostrados, el coeficiente de incremento en capacidad fue de un múltiplo lineal de cuatro cada cuatro años a cada cuatro años.

Componentes y funcionamiento

- DWDM es la base de la tecnología en una red de transporte óptica. Los componentes esenciales de DWDM se pueden clasificar por su lugar en el sistema como sigue:
- En el lado de la transmisión, láseres con precisión, longitudes de onda estables
- En el enlace, fibra óptica que exhibe bajas pérdida y funcionamiento de transmisión en los espectros relevantes de la longitud de onda, además de plano-gane los amplificadores ópticos para alzar la señal en palmos más largos
- En el lado de la recepción, foto detectores y demultiplexores ópticos usando los filtros de película fina o los elementos difractantes
- Multiplexores Ópticos add/drop y componentes cross conectores ópticos

WDM asigna las señales ópticas entrantes a frecuencias específicas de luz (longitudes de onda o lambdas) dentro de una cierta banda de frecuencias. Esta multiplexación se asemeja bastante a la manera de transmisión de estaciones de radio en diferentes longitudes de onda sin interferir con las demás (

Debido a WDM incremento la capacidad del medio físico (fibra) usando un método completamente diferente de TDM, que cada canal es transmitido a una frecuencia diferente, podemos seleccionarlo usando un sintonizador. Otra forma para pensar en WDM es que cada canal es un color de luz diferente; entonces varios canales forman un arco iris.



Las telecomunicaciones hacen un uso extensivo de las técnicas y medios ópticos.

1. Debido a la necesidad de poder transferir volúmenes grandes de información.
2. El desarrollo de la comunicación vía fibra óptica sigue creciendo a pasos agigantados.
3. La modulación de onda permite la transmisión de señales análogas o digitales de hasta unos pocos GigaHertz por segundo en una portadora de una frecuencia muy alta, típicamente de 186 a 196 GHz.

Funciones del sistema

Generación de la señal - La fuente, un láser de estado sólido, debe proporcionar la luz estable dentro de un específico, estrecha ancho de banda que transporta los datos digitales, modulado como una señal análoga.

Combinando las señales – Los sistemas Modernos de DWDM emplean los multiplexores para combinar las señales. Hay una cierta pérdida inherente asociada a la multiplexación y la demultiplexación. Esta pérdida es dependiente sobre el número de canales pero se puede ser mitigada con amplificadores ópticos, los cuales alzan todas las longitudes de onda inmediatamente sin la conversión eléctrica.

Transmitiendo las señales – Los efectos de las de la interferencia y de la degradación o de la pérdida de la señal óptica se debe contar con en la transmisión por fibra óptica. Estos efectos pueden ser reducidos al mínimo controlando variables tales como espaciamientos de canal, tolerancia de la longitud de onda, y niveles de la energía del láser. Sobre un enlace de transmisión, la señal puede necesitar ser amplificada ópticamente.

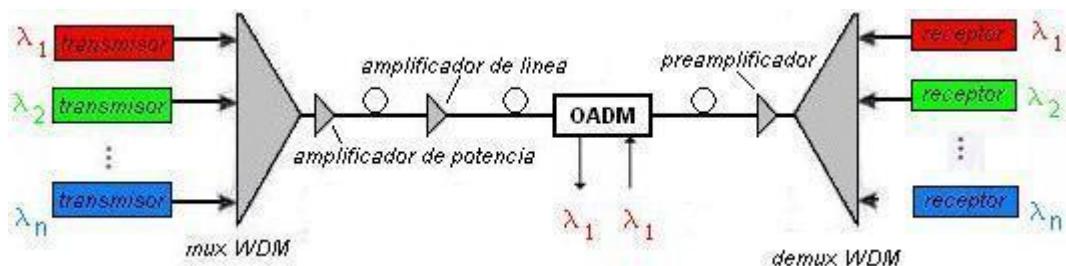
Separando las señales recibidas – Al término de la recepción, las señales multiplexadas se deben separar hacia fuera. Aunque esta tarea parecería ser simplemente lo contrario de combinar las señales, es técnicamente más difícil en la actualidad.

Recibiendo las señales - La demultiplexación de la señal es recibida por un fotodetector.

Además de estas funciones, un sistema de DWDM se debe también equipar de los interfaces del cliente-lado para recibir la señal de entrada. Esta función es realizada por los transponders.

Funcionamiento de un Transponder Basado en el Sistema DWDM

Funcionamiento del extremo-a-extremo de un sistema de DWDM unidireccional.





El transponder acepta la entrada en la forma estándar de monomodo o láser del multimodo.
La entrada

Puede venir de los diferentes medios de comunicación físicos y protocolos diferentes y tipos de tráfico.

La longitud de onda de cada señal de entrada se traza a una longitud de onda de DWDM.

Las longitudes de onda de DWDM del transponder son multiplexados en una sola señal óptica y lanzada en la fibra. El sistema también podría incluir la habilidad de aceptar los signos ópticos directos al el multiplexor; por ejemplo, los tales signos podrían venir de un nodo del satélite.

Un poste-amplificador empuja la fuerza de la señal óptica tan pronto deja el sistema (optativo).

Se usan los amplificadores ópticos a lo largo del palmo de fibra como es necesario (optativo).

Un pre-amplificador empuja el signo antes de que entre en el sistema del extremo (optativo).

La señal entrante es demultiplexada en las lambdas de DWDM individual (o longitudes de onda).

Las lambdas de DWDM individuales se trazan al tipo del rendimiento requerido (por ejemplo, OC-48 fibra del solo-modo) y mandó a través del transponder.

TRANSPONDEDOR Para Fibra Óptica / De MULTIPLEXACIÓN

100 MBPS - 4.25 GBPS

Topologías y esquemas de protección para DWDM

Las arquitecturas de red se basan en muchos factores, incluyendo tipos de aplicaciones y de protocolos, distancias, aplicaciones y patrones de acceso, y topologías de red heredadas. En el mercado metropolitano, por ejemplo, se pueden utilizar topologías punto a punto para conectar las localizaciones de la empresa, topologías de anillo para conectar las instalaciones entre oficinas (IOFs) y para el acceso residencial, y las topologías de acoplamiento se pueden utilizar para conexiones inter-POP y conexiones a lo largo del backbone transcontinental. En efecto, la capa óptica debe ser capaz de soportar muchas topologías y, debido a progresos imprevisibles en esta área, esas topologías deben ser flexibles.

Hoy, las topologías principales en despliegue son punto a punto y de anillo. Con el acoplamiento punto a punto sobre DWDM entre los grandes sitios de la empresa, necesita solamente un dispositivo de premisa del cliente para convertir el tráfico de las aplicaciones a las longitudes de onda y a la multiplexación específicas. Los portadores con topologías de anillo-lineal pueden envolver completamente a los anillos basados en OADMs. Conforme los Cross-Connect Ópticos configurables y los Switches llegan a ser más comunes, éstas redes punto a punto y de anillo serán interconectadas en los acoplamientos, transformando redes ópticas metropolitanas en plataformas completamente flexibles.

Protección Óptica

En caso de ser necesario, la salida del Multiplexor DWDM, puede beneficiarse de un sistema de Protección Óptica que garantiza la disponibilidad del servicio a través de dos rutas de fibras ópticas.

FUTURO DE DWDM

DWDM continuará proporcionando el ancho de banda para grandes cantidades de datos. De hecho, la capacidad de los sistemas crecerá conforme las tecnologías avancen y permitan un espaciamiento más cercano, y por lo tanto incrementen los números, de longitudes de onda. Pero DWDM también se está moviendo más allá del transporte para convertirse en la base del networking all-optical (totalmente óptico) con previsión de la longitud de onda y la protección basada en el acoplamiento. El cambio en la capa fotónica permitirá esta evolución, conforme los protocolos de enrutamiento permitan que las trayectorias ligeras atraviesen la red del mismo modo que lo hacen los circuitos virtuales hoy en día. Éstos y otros avances están convergiendo de manera tal que una infraestructura all-optical (totalmente óptica) puede ser prevista en la capa óptica para soportar las necesidades de la empresa, de acceso metropolitano, y de las redes metropolitanas centrales.

Ventajas DWDM

Aumenta altamente la capacidad de un punto a otro de la red de fibra óptica. Esto se debe principalmente a la posibilidad de transmitir varias señales dentro de una sola señal y a las altas tasas de transmisión que soporta.

Permite transportar cualquier formato de transmisión en cada canal óptico. Así, sin necesidad de utilizar una estructura común para la transmisión de señales, es posible utilizar diferentes longitudes de onda para enviar información síncrona y asíncrona, analógica o digital, a través de la misma fibra.

Permite utilizar la longitud de onda como una nueva dimensión, además del tiempo y el espacio, en el diseño de redes de comunicación.

Desventajas DWDM

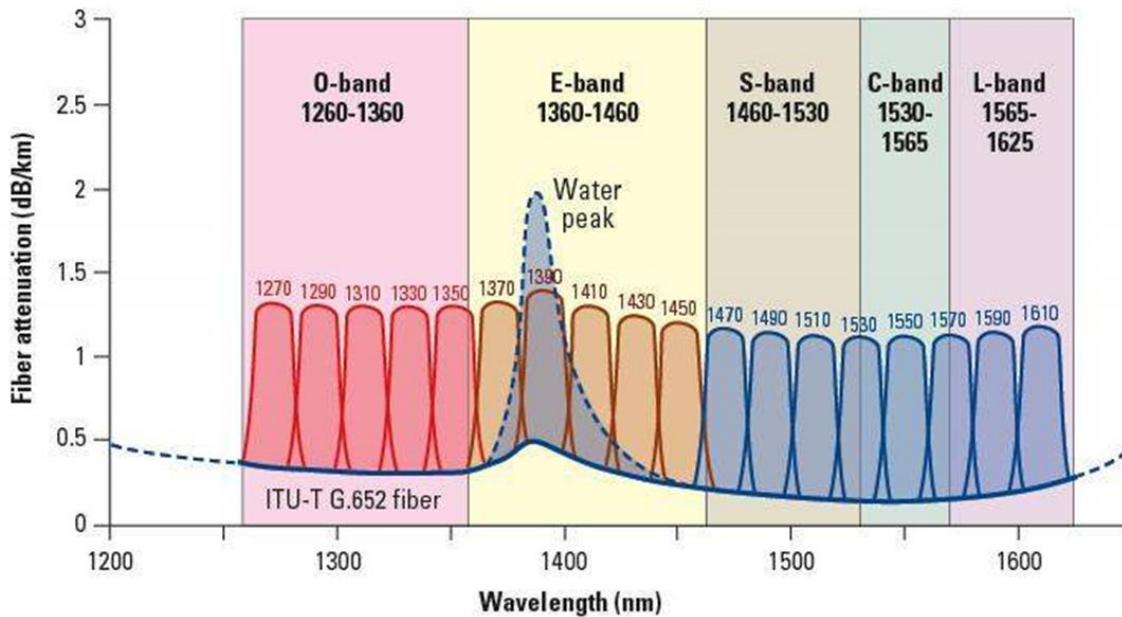
Los componentes ópticos son más caros debido a la necesidad de utilizar filtros ópticos, y láser que soporte una tolerancia a longitudes de onda compactas. Un dispositivo externo de acoplamiento es usado para acoplar la mezcla de las diferentes señales ópticas. tiene menor espacio para una tolerancia con respecto a la dispersión de las longitudes de onda.

CWDM (Coarse wavelength Division Multiplexing),

Significa Multiplexación por división en longitudes de onda ligeras. CWDM es una técnica de transmisión de señales a través de fibra óptica que pertenece a la familia de multiplexión por división de longitud de onda (WDM), se utilizó a principios de los años 80 para transportar señal de video (CATV) en conductores de fibra multimodo, fue estandarizado por la ITU-T (Internacional Telecommunication), en la recomendación de la norma G.694.2 en el año 2002.

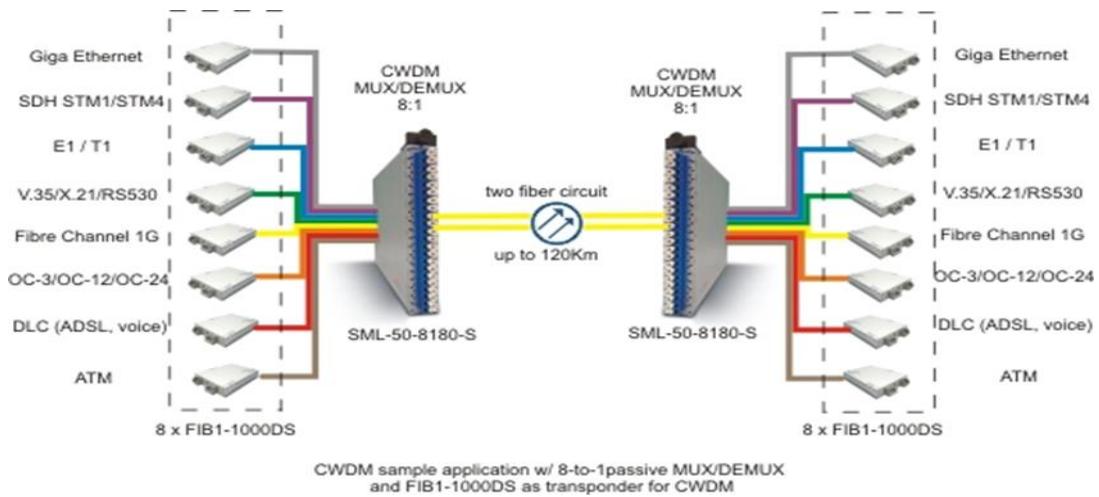
Se basa en una rejilla o separación de longitudes de onda de 20 nm (o 2.500 GHz) en el rango de 1.270 a 1.610 nm; pudiendo así transportar hasta 18 longitudes de onda en una única fibra óptica monomodo. De acuerdo con esto, se tienen dos importantes características inherentes a los sistemas CWDM que permiten emplear componentes ópticos más sencillos y, por lo tanto, también más baratos que en los sistemas DWDM:

CWDM wavelength grid as specified by ITU-T G.694.2



Al tener mayor espaciamiento de longitudes de onda, en CWDM se pueden utilizar láseres con un mayor ancho de banda espectral y no estabilizada, es decir, que la longitud de onda central puede desplazarse debido a imperfecciones de fabricación o a cambios en la temperatura a la que está sometido el láser y, aun así, estar en banda. Esto permite fabricar láseres siguiendo procesos de fabricación menos críticos que los utilizados en DWDM, y que dichos láseres no tengan sofisticados circuitos de refrigeración para corregir posibles desviaciones de la longitud de onda debidos a cambios en la temperatura a la que está sometido el chip; lo cual reduce sensiblemente el espacio ocupado por el chip y el consumo de potencia, además del coste de fabricación. Por lo general en CWDM se utilizan láseres de realimentación distribuida o DFB (Distributed Feed-Back) modulados directamente y soportando velocidades de canal de hasta 2,5 Gbps sobre distancias de hasta 80 Km en el caso de utilizar fibra óptica G.652. Por otro lado, CWDM utiliza filtros ópticos y multiplexores y demultiplexores basados en la tecnología de película delgada o TFF (Thin-Film-Filter), donde el número de capas del filtro se incrementa cuando el espaciamiento entre canales es

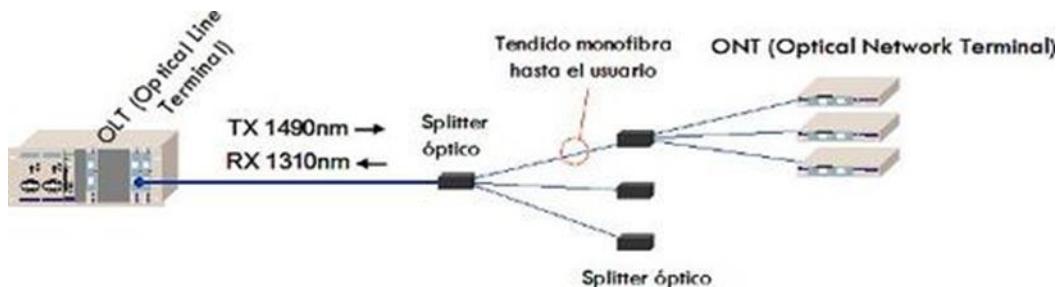
menor. Esto supone de nuevo una mayor capacidad de integración y una reducción de coste. Estos filtros CWDM de banda ancha, admiten variaciones en la longitud de onda nominal de la fuente de hasta unos $\pm 6\text{-}7$ nm y están disponibles generalmente como filtros de uno o dos canales.



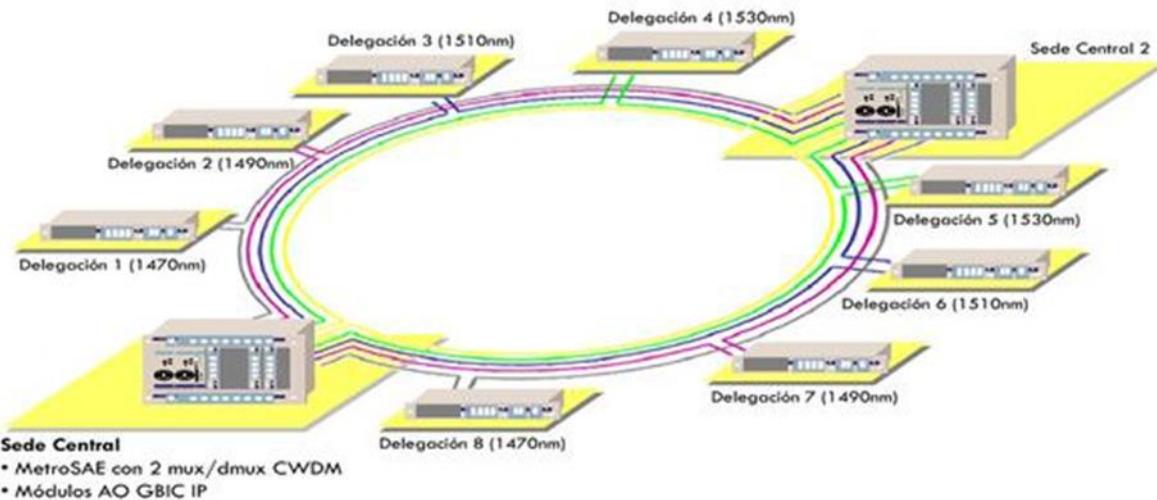
Topologías

CWDM puede admitir las siguientes topologías:

Anillos punto a punto y redes ópticas pasivas (PON, permite eliminar todos los componentes activos en la red, para introducir componentes pasivos como el divisor o splitter, y así reducir costos y mantenimiento en dicha red)



Anillos locales CWDM que se conectan con anillos metropolitanos DWDM

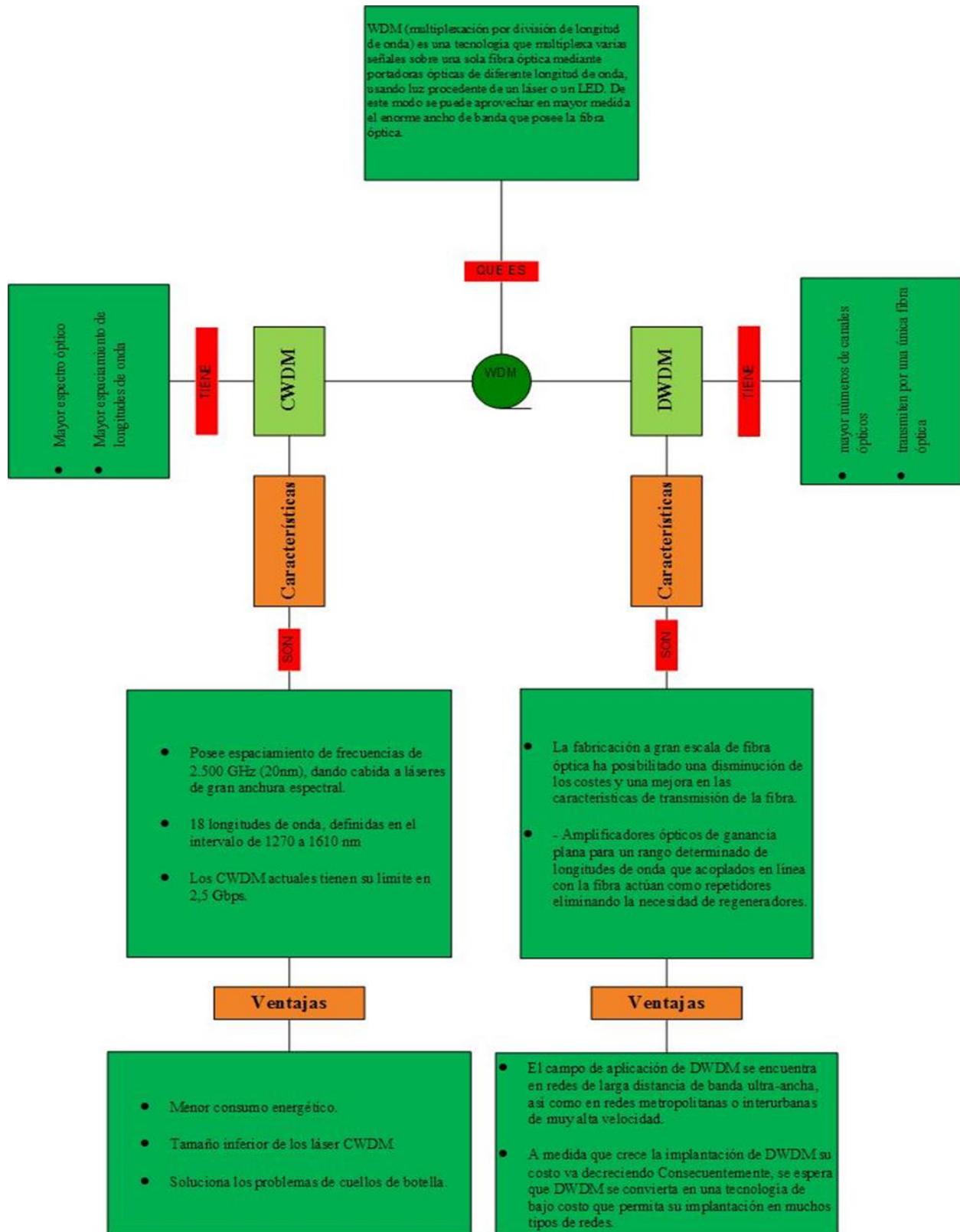


Anillos de acceso y las redes ópticas pasivas.

Ventajas

- Menor consumo energético.
- Tamaño inferior del láser CWDM.
- Soluciona los problemas de cuellos de botella.
- Hardware y costo operativo más barato referente a otras tecnologías de la misma familia.
- Anchos de banda más elevada.
- Es más sencillo referente al diseño de la red, implementación y operación.
- Mayor facilidad de instalación, configuración y mantenimiento de la red.
- Alto grado de flexibilidad y seguridad en la creación de redes ópticas metropolitanas.
- Puede transportar cualquier servicio de corto alcance como: SDH, CATV, ATM, FTTH – PON, 10Gibabit, entre otros.

Mapa mental

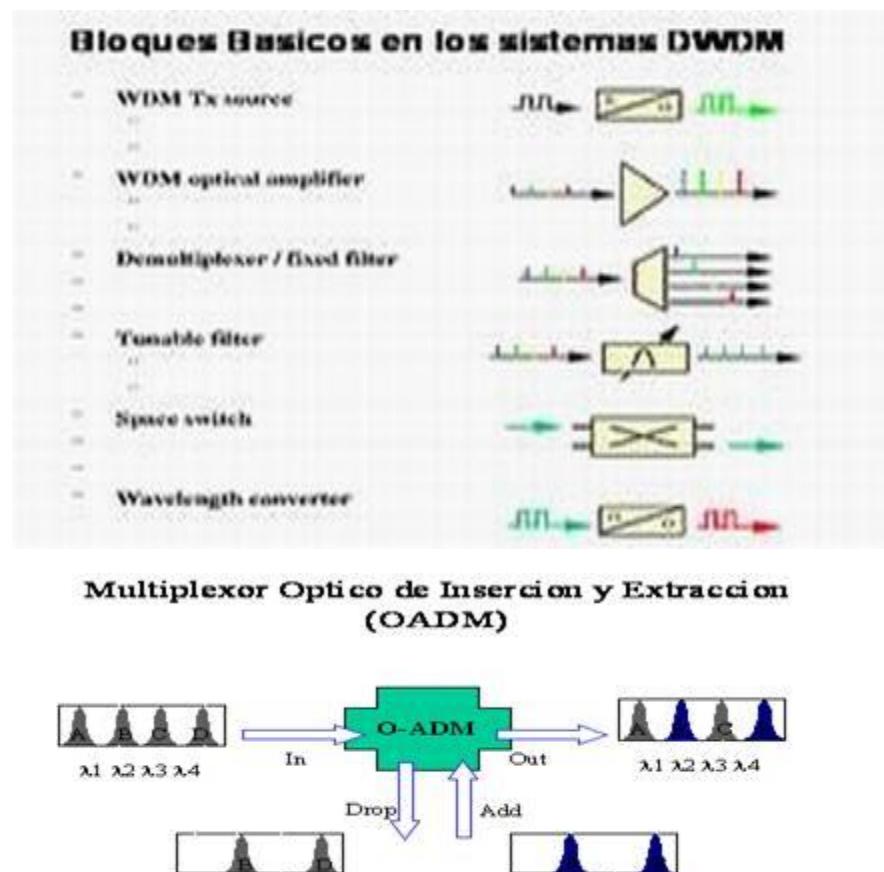


Redes Ópticas de Nueva Generación

Relacionado con las nuevas tecnologías de Telecomunicaciones sobre Fibra Óptica, en este acápite se describirá los componentes y bloques principales que integran las Redes Ópticas.

Componentes y Redes Ópticas.

Las Redes Ópticas realizan el procesamiento de la señal en el dominio óptico, en la figura 16 se muestra un conjunto de bloques básicos que resume las operaciones elementales sobre la señal.



Redes Ópticas Pasivas. (PON- Passive Optical Networks)

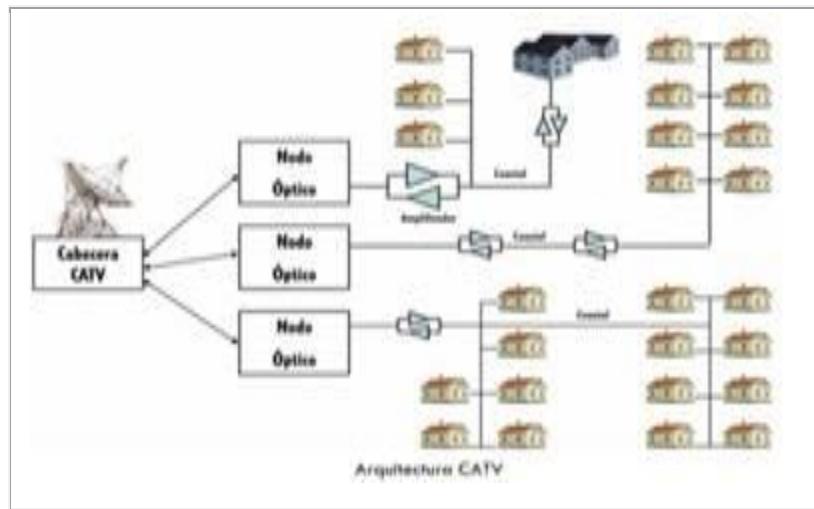
En los últimos años, la Sociedad de la Información ha experimentado un rápido desarrollo debido en gran parte a la mayor competitividad impulsada por la desregulación del mercado de las Telecomunicaciones y a la aparición de nuevos servicios de banda ancha, el resultado de estos dos factores se ha traducido en una necesidad de mejorar las redes de comunicaciones para que sean capaces de ofrecer un mayor ancho de banda a un menor coste, en la actualidad la tecnología ADSL es la estrella indiscutible en el panorama europeo, ya que es una tecnología que sigue explotando el bucle de abonado en cobre. Por otro lado, la demanda de los usuarios es cada vez mayor porque la necesidad de aumentar el ancho de banda ha hecho replantear a los operadores consolidados y emergentes sus estrategias, comenzando una carrera por la duplicación de la velocidad de sus líneas que a los ojos del profano parece no tener fin, sin embargo, ADSL cuenta con una limitación técnica importante: El máximo ancho de banda que puede

ofrecer no supera en ningún caso los 8Mbps en canal descendente y los 4Mbps en canal ascendente, además estos valores disminuyen drásticamente a medida que el usuario se aleja de la central.

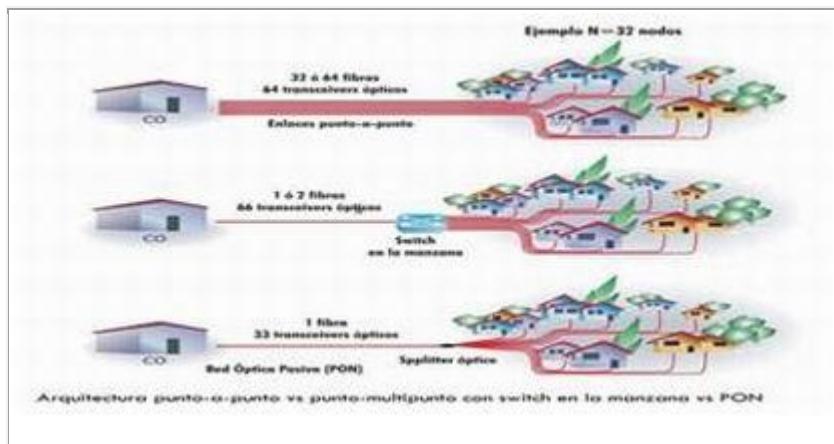
En vista a lo planteado anteriormente se dice que la tecnología de la Fibra Óptica se presenta como una firme solución al problema gracias a la robustez, a su potencial ancho de banda ilimitado y al continuo descenso de los costes asociados a los láseres y si a lo dicho anteriormente unimos que las nuevas construcciones (nuevas urbanizaciones, nuevos bloques de viviendas, centros comerciales) ya integran cableado estructurado de Fibra Óptica Monomodo por su bajo coste marginal en el proyecto, estamos hablando de un escenario completamente abonado para poder desplegar soluciones de conectividad en Fibra Óptica que directamente lleguen hasta la vivienda, y si por otro lado hablamos de arquitecturas de futuro, que son las conocidas Redes PON se postulan como una apuesta fiable, porque su costo contenido en equipamiento electroóptico y la eficiencia de las topologías árbol-rama aportan un incentivo adicional frente a los despliegues tradicionales basados en conectividad punto a punto.

Características comunes de los sistemas PON.

Las Redes Ópticas Pasivas (PON) toman su modelo de las redes CATV recicladas para ofrecer servicios de banda ancha mediante la habilitación del canal de retorno, una red CATV está compuesta por varios nodos ópticos unidos con la cabecera a través de Fibra Óptica de los cuales se derivan mediante una arquitectura compartida de cable coaxial, los accesos a los abonados, habitualmente en CATV cada nodo óptico ataca a un determinado número de usuarios (en función del ancho de banda que se quiere asignar a los usuarios) utilizando cable coaxial y Splitters (divisores) eléctricos, por ello las Redes Ópticas Pasivas sustituyen el tramo de coaxial por Fibra Óptica Monomodo y los derivadores eléctricos por divisores ópticos, para de esta manera la mayor capacidad de la fibra permite ofrecer unos anchos de banda mejorados en canal descendente y sobre todo en canal ascendente, superando la limitación típica de 36Mbps de los sistemas cable-modem DOCSIS y EURODOCSIS por nodos ópticos.



Esta nueva arquitectura es una evolución de menor coste a alternativas tradicionales como las redes punto a punto o las redes conmutadas hasta la manzana, puesto que reducen el equipamiento necesario para la conversión electroóptica y prescinden del equipamiento de red de alta densidad necesario para la conmutación.



Arquitectura punto a punto vs punto-multipunto con Switch.

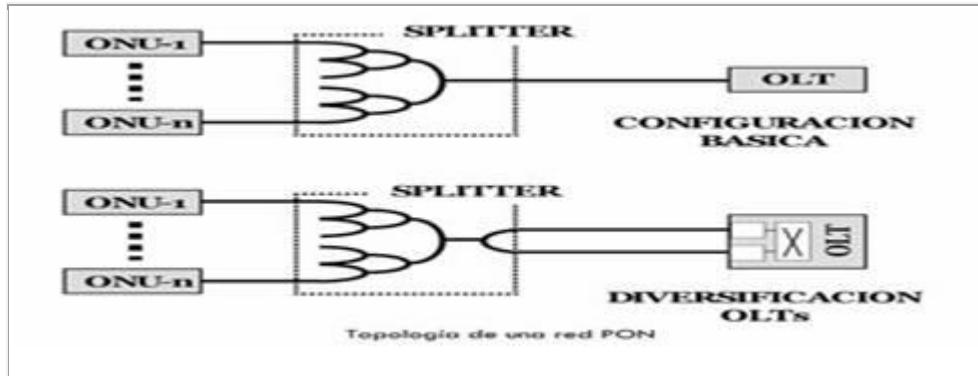
Las arquitecturas **PON** están centrando la atención de la industria de las Telecomunicaciones como una manera de atacar a la problemática de la última milla, puesto que presenta evidentes ventajas:

- Las **Redes PON** permiten atacar a usuarios localizados a distancias de hasta 20Km desde la central (O nodo óptico), dicha distancia supera con creces la máxima cobertura de las tecnologías DSL. (Máximo 5Km desde la central)
- Las **Redes PON** minimizan el despliegue de fibra en el bucle local al poder utilizar topologías árbol-rama mucho más eficientes que las topologías punto a punto, además de que este tipo de arquitecturas simplifica la densidad del equipamiento de central, reduciendo el consumo.
- Las **Redes PON** ofrecen una mayor densidad de ancho de banda por usuario debido a la mayor capacidad de la fibra para transportar información que las alternativas de cobre (xDSL y CATV)
- Como arquitectura punto-multipunto, las **Redes PON** permiten superponer una señal óptica de Televisión procedente de una cabecera CATV en otra longitud de onda sin realizar modificaciones en los equipos portadores de datos. (ver apartado: Tecnología VPON)
- Las **Redes PON** elevan la calidad del servicio y simplifican el mantenimiento de la red, al ser inmunes a ruidos electromagnéticos, no propagar las descargas eléctricas procedentes de rayos, etc.
- Las **Redes PON** permite crecer a mayores tasas de transferencia superponiendo longitudes de onda adicionales.

Breve descripción para las topologías PON.

Las Redes PON es una tecnología punto-multipunto, todas las transmisiones en una Red PON se realizan entre la unidad Óptica Terminal de Línea OLT (Optical Line Terminal), localizada en el nodo óptico o central y la Unidad Óptica de Usuario (ONU), habitualmente la unidad OLT se interconecta con una red de transporte que recoge los flujos procedentes de varias OLTs y los encamina a la cabecera de la red y la unidad ONU se ubica en domicilio de usuario configurando un esquema FTTH. (Fibra hasta el usuario Fiber To The Home)

Existen varios tipos de topologías adecuadas para el acceso a red, incluyendo topologías en anillo (no muy habituales), árbol, árbol-rama y bus óptico lineal, cada una de las bifurcaciones se consiguen encadenando divisores ópticos 1x2 o bien divisores 1xN, en algunos casos dependiendo de la criticidad del despliegue a la red de acceso puede requerir protección.



Topología de una Red PON.

Todas las topologías PON utilizan Monofibra para el despliegue y en canal descendente una PON es una red punto multipunto, donde el equipo OLT maneja la totalidad del ancho de banda que se reparte a los usuarios en intervalos temporales, en el otro canal el canal ascendente la PON es una red punto a punto donde múltiples ONUs transmiten a un único OLT, trabajando sobre Monofibra la manera de optimizar las transmisiones de los sentidos descendente y ascendente sin entremezclarse consiste en trabajar sobre longitudes de onda diferentes utilizando técnicas WDM (Wavelength Division Multiplexing), aquí la mayoría de las implementaciones superponen dos longitudes de onda, una para la transmisión en sentido descendente (1290nm) y otra para la emisión a la cabecera (1310nm) sentido ascendente, la evolución de la tecnología óptica ha permitido miniaturizar los filtros ópticos necesarios para esta separación hasta llegar a integrarlos en los transceptores ópticos de los equipos de usuario y se utilizan estas portadoras ópticas en segunda ventana (en lugar de trabajar en tercera ventana) para contener al máximo los costes de la optoelectrónica.

Al mismo tiempo las arquitecturas PON utilizan técnicas de multiplexación en tiempo TDMA para que en distintos instantes temporales determinados por el controlador de cabecera OLT, los equipos ONU puedan enviar su trama en canal ascendente, de manera equivalente el equipo de cabecera OLT también debe utilizar una técnica TDMA para enviar en diferentes slots temporales la información del canal descendente que selectivamente deberán recibir los equipos de usuario. (ONU)

Las arquitecturas PON también han tenido que resolver otro aspecto importante: La dependencia de la potencia de transmisión del equipo OLT con la distancia a la que se encuentra el equipo ONU, que como se ha detallado anteriormente, puede variar hasta un máximo de 20Km, evidentemente un equipo ONU muy cercano al OLT necesitará una menor potencia de su ráfaga para no saturar su fotodiodo y los equipos muy lejanos necesitarán que su ráfaga temporal se transmita con una mayor potencia, donde esta prestación también ha sido introducida recientemente en los transceptores ópticos PON que han simplificado notablemente la electrónica anteriormente necesaria para actuar sobre un control de ganancia externo al transceptor y la nueva óptica miniaturiza, integra y simplifica el trabajo con ráfagas de diferente nivel de potencia.

Variantes de Redes Ópticas: APON, BPON y GPON.

La transmisión en canal descendente está formada por ráfagas de celdas ATM estándar de 53bytes a las que se le añaden un identificador de tres bytes que identifican el equipo ONU generador de la ráfaga, la máxima tasa soportada en canal ascendente suponiendo una única unidad ONU es de 155Mbps, este ancho de banda se reparte en función del número de usuarios asignado al nodo óptico (Número de ONUs), en canal ascendente la trama se construye a partir de 54 celdas ATM donde se intercalan dos

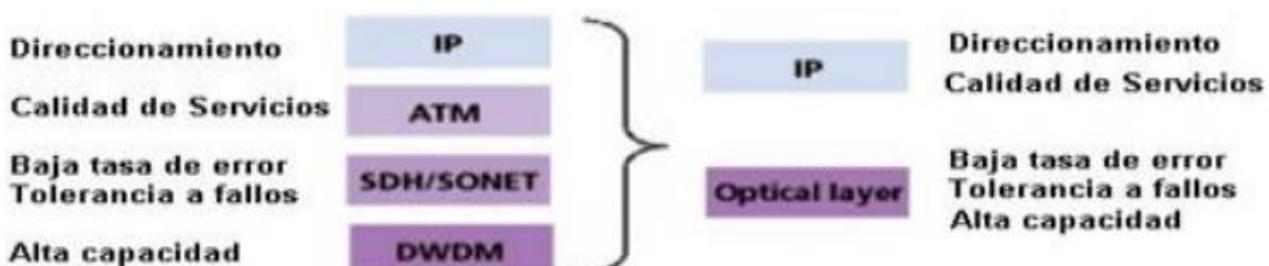
celdas PLOAM y se introduce información de los destinatarios de cada celda e información de operación y mantenimiento de la red.

GPON es un estándar muy potente pero a la vez muy complejo de implementar que ofrece:

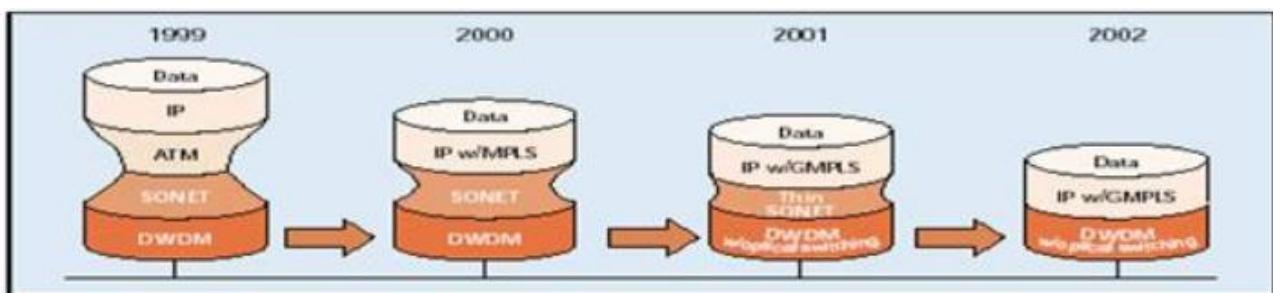
- Soporte global Multiservicio incluyendo voz (TDM, SONET, SDH), Ethernet 10/100 Base T, ATM, Frame Relay y muchas más.
- Alcance físico de 20km.
- Soporte para varias tasas de transferencia, incluyendo tráfico simétrico de 622Mbps, tráfico simétrico de 1.25Gbps y asimétrico de 2.5Gbps en sentido descendente y 1.25 en sentido ascendente.
- Importantes facilidades de gestión, operación y mantenimiento, desde la cabecera OLT al equipamiento de usuario ONU.
- Seguridad a nivel de protocolo (Encriptación) debido a la naturaleza multicast del protocolo.

Nuevo modelo para Red de Transporte

Disminución de las capas del modelo OSI hasta obtener el nivel óptico.



Proceso de evolución mostrando como se introduce el protocolo de QoS y control de tráfico, MPLS en el nivel óptico.



. Desarrollo de los niveles del modelo OSI hasta el 2002 que surge el nivel óptico.

La Red de Telecomunicaciones es tradicional se considera formada por cuatro capas: IP, ATM, SDH y DWDM, superpuestas de la forma que se ilustra en el diagrama 1 de la figura 30, esta estructura es muy robusta porque el nivel IP es portador de la inteligencia y la capa de ATM, por su parte, garantiza la calidad de servicio (QoS); SDH asegura la fiabilidad pues contiene los mecanismos para la recuperación ante fallas, mientras que DWDM añade una alta capacidad de transporte.

Sin embargo, la estructura tradicional de cuatro capas consume un mayor ancho de banda por lo que se han desarrollado un importante trabajo investigativo para simplificar este modelo, los principios en que se fundamentan las nuevas propuestas son los siguientes:

- IP se ha convertido en el protocolo unificador para todas las redes y servicios.

- Hay un aumento considerable del tráfico IP.
- Se incorporan nuevos servicios de VoIP, VPN y aumento de los servicios de banda ancha a través de ADSL.
- El protocolo MPLS de calidad de servicio y control de tráfico se incorpora al nivel óptico como GMPLS.
- Se desarrollan Routers al nivel óptico.
- Surgen alternativas de protección contra fallas al nivel óptico.
- Sobre estas premisas se ha evolucionado hacia un nuevo modelo de red basado en una estructura de dos niveles: IP directamente sobre DWDM, eliminándose las capas ATM y SDH, tal como se muestra en las secuencias 2, 3 y 4 de figura 30.
- Un aspecto a destacar en esta red es que realiza el enruteamiento de los paquetes IP completamente en el dominio óptico para lo cual varias compañías de fabricantes, especialmente en Estados Unidos y Japón han desarrollado e introducido en el mercado, equipos Routers (Routers) que operan directamente en el nivel óptico.

Estos nuevos paradigmas forman parte de las denominadas Redes de Próxima Generación las cuales presentan un conjunto de características novedosas que aquí solo se enfocan hacia los aspectos de transmisión o transporte.



FDDI Fiber Distributed Data Interface (Interfaz de Datos Distribuida por Fibra)

Es un conjunto de estándares del internet ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica. Se basa en la arquitectura token ring y permite una comunicación tipo Full Duplex. Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN). Están implementadas mediante una física de estrella (lo más normal) y lógica de anillo doble de token, uno transmitiendo en el sentido de las agujas del reloj (anillo principal) y el otro en dirección contraria (anillo de respaldo o back up).

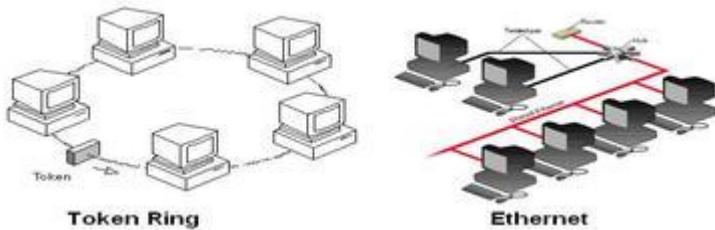
Características

- Ofrece una velocidad de 100 Mbps sobre distancias de hasta 200 metros, soportando hasta 1000 estaciones conectadas. Esta velocidad se alcanza debido a que trabaja parcialmente en las capas 1 y 2.
- FDDI se comporta de manera óptima en aquellos entornos en los cuales son esenciales la gestión de red y la recuperación de fallos.

- Utiliza técnicas de conmutación de paquetes con protocolo de paso de testigo como método de acceso

Historia

Las redes FDDI surgieron a mediados de los años ochenta para dar soporte a las estaciones de trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades.



FDDI comenzó a ser desarrollado por el comité de estándares ANSI X3T9.5 en 1983. Cada una de sus especificaciones fue diseñada y mejorada hasta culminar con SMT en 1994. La razón de su existencia fue constituir una LAN alternativa a ethernet y token ring que además ofreciese una mayor fiabilidad. En la actualidad, debido a sus superiores velocidad, coste y ubicuidad, se prefiere utilizar fast Ethernet y Gigabit Ethernet en lugar de FDDI.

Norma

El estándar FDDI ha sido desarrollado por el ANSI en el Comité X3T9.5; la norma es la ANSI X3T9.5 y ha sido adoptada por la Organización Internacional de Normalización (ISO) bajo la denominación ISO 9384.



Estructura

- PMD (Physical Media Dependent - Dependencia del medio físico).** Especifica las señales ópticas y formas de onda a circular por el cableado, incluyendo las especificaciones del mismo así como las de los conectores. Así, es la responsable de definir la distancia máxima de 2 Km. Entre estaciones FDDI y el tipo de cable multimodo con un mínimo de 500 MHz y LED's transmisores de 1300 nanómetros (nm). Estas especificaciones se cumplen en los cables de 62,5/125 micras (m m) y por la mayoría de los cables de 50/125 m m. La atenuación máxima admitida en el anillo FDDI es de 11 decibelios (dB) de extremo a extremo, típicamente referenciada a 2,5 dB por Km. ANSI aprobó la subcapa PMD en 1988, y se corresponde con la mitad inferior de la capa 1 (capa de enlace físico) en el esquema OSI. Existe también una especificación de fibra monomodo ("single-mode", SMF-PMD, 9 m m), empleando detectores/transmisores láser para distancias de hasta 60 Km. entre estaciones.

- **PHY (Physical Layer Protocol - Protocolo de la capa física).** Se encarga de la codificación y decodificación de las señales así como de la sincronización, mediante el esquema 4-bytes/5-bytes, que proporciona una eficacia del 80%, a una velocidad de señalización de 125 MHz, con paquetes de un máximo de 4.500 bytes. Proporciona la sincronización distribuida. Fue aprobada por ANSI en 1988 y se corresponde con la mitad superior de la capa 1 en el esquema OSI.
- **MAC (Media Access Control - Control de acceso al medio).** Su función es la programación y transferencia de datos hacia y desde el anillo FDDI, así como la estructuración de los paquetes, reconocimiento de direcciones de estaciones, transmisión del testigo, y generación y verificación de secuencias de control de tramas (FCS o Frame Check Sequences). Se corresponde con la mitad inferior de la capa OSI 2 (capa de enlace de datos) y fue aprobada por ANSI en 1986.
- **SMT (Station Management - Gestión de estaciones).** Se encarga de la configuración inicial del anillo FDDI, y monitorización y recuperación de errores. Incluye los servicios y funciones basados en tramas, así como la gestión de conexión (CMT o Connection Management), y la gestión del anillo (RMT o Ring Management). Se solapa con las otras 3 subcapas FDDI, y por tanto fue la de más complicada aprobación por parte de ANSI, que se realizó en 1993.

Topología Funcional

La infraestructura física es un anillo de fibra óptica de doble canal. Un canal principal para la comunicación y otro para funciones de gestión de la red y como alternativa de seguridad.



Medio de transmisión: El grupo normalizador de FDDI ha elegido el cable multimodo de fibra óptica como soporte físico, con una longitud de onda normalizada de 1.300 nm. El estándar especifica el uso de la fibra multimodo 62'5/125 μ de índice gradual. Sin embargo, pueden emplearse otros tipos de fibra (p.ej:50/125, 85/125, 100/140 μ). Para todos estos tipos de fibra se especifica un ancho de banda de al menos 500 MHz/km y una atenuación no mayor de 2.5 dB/km.

Distancia entre nodos: Para minimizar costes (dispositivos ópticos y cable), la norma FDDI especifica la utilización de trasmisores tipo LED y fibra multimodo. Con esta tecnología "barata", la distancia máxima de los enlaces es de 2 km (limitada por la dispersión modal y cromática).

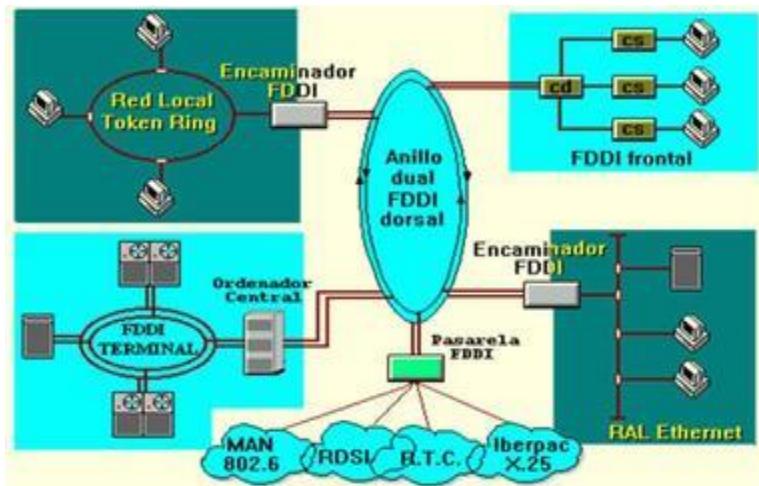
Extensión: Con estas elecciones técnicas, se pueden configurar redes de hasta 50 km de diámetro, en donde la distancia máxima entre nodos de conexión es de 2 km. Pueden conectarse a la red hasta 500 nodos; puesto que estos nodos pueden ser puentes de acceso hacia redes Ethernet y Token Ring, el número de ordenadores usuarios de una red FDDI puede alcanzar varios miles de unidades.

Tipos de nodos Las redes FDDI pueden estar configuradas con dos tipos de elementos funcionales o nodos de red y pueden conectarse al anillo de dos formas diferentes:

Tipo de Conexión	Elemento Funcional Estación	Concentrador
Doble	DAS	DAC
Simple	SAS	SAC



Arquitectura de red



- *Redes Terminales (back-end)*: Permiten la transferencia rápida de información entre la Unidad Central de Proceso (UCP) y dispositivos de almacenamiento masivo (discos ópticos, unidades de cintas) y periféricos de alta velocidad (impresoras, trazadores).
- *Redes Dorsales (backbone)*: Conectan redes de área local de velocidades menores. La velocidad de transmisión de la red de área metropolitana permite manejar una carga agregada de múltiples redes conectadas sin establecer cuellos de botella ni degradar sus respectivas prestaciones. Las redes de área local compatibles IEEE 802.X (Ethernet 802.3, Token Bus 802.4 y Token Ring 802.5) se interconectan mediante puentes o encaminadores con salida al nodo de red MAN (Red de Área Metropolitana). La red dorsal permite establecer enlaces con las redes pública de área extensa (X.25, frame relay) o con redes privadas del tipo SNA mediante pasarelas específicas.
- *Redes Frontales (front-end)*: Conectan grandes ordenadores, minis y ordenadores personales, estaciones de trabajo, terminales gráficos de alta resolución CAD/ CAM, impresoras láser, etc. Esta configuración se asemeja al entorno de red local, pero con unas prestaciones muy superiores comparada con Ethernet o Token Ring.

Aplicaciones

- Su uso más normal es como una tecnología de backbone para conectar entre sí redes LAN de cobre o computadores de alta velocidad, con expansión para redes MAN debido a que multiplica por 10 el ancho de banda disponible actualmente.
- Con este ancho de banda, una red FDDI se utiliza clusters y grupos de trabajo con aplicaciones en finanzas, ingeniería, CAD/CAM, CIM, ciencia, telemedicina, edición electrónica, multimedia y otras de requerimientos similares para las aplicaciones de la sociedad actual. La falta del ancho de banda adecuado, en estos grupos

de trabajo, es un cuello de botella que genera tiempos de espera, colisiones, reintentos y retransmisiones, y consecuentemente, la pérdida de productividad. Esto implica pérdidas económicas.

- Servicios no orientados a la conexión para tráfico síncrono y asíncrono.

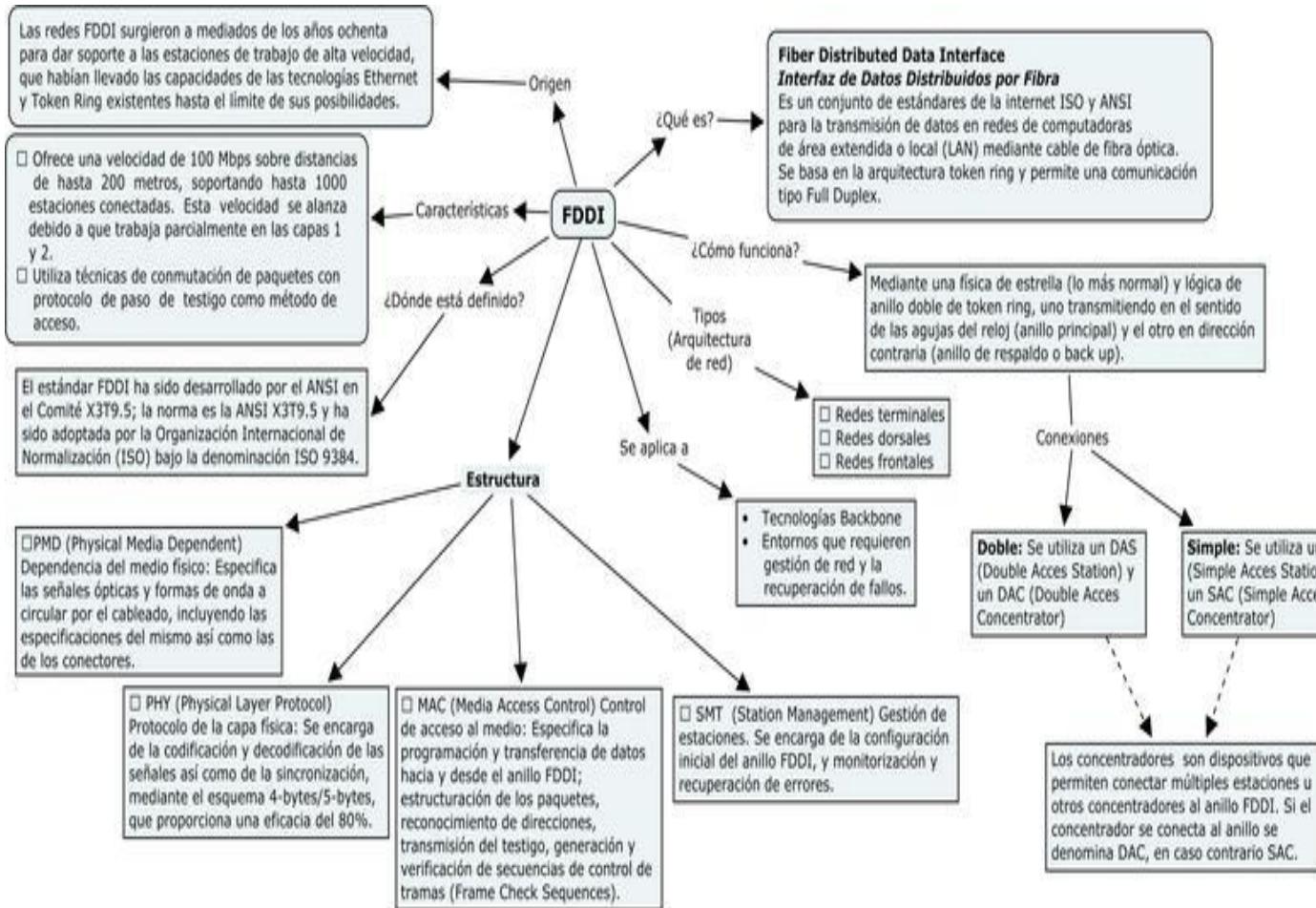
Problemas de FDDI

Existen las Tecnologías competitivas ATM, Fast Ethernet, Fibre Channel, Frame Relay, T1/E1, T3/H3, SMDS, FFOL(*FDDI Follow-on LAN*), SAFENET II y [HiPPI](#). La realidad es que la mayoría de dichos productos, competitivos o no, no están normalizados, y por tanto, los que se comercializan se hallan sujetos a incompatibilidades tras su regulación definitiva.

- Otro inconveniente son sus elevados precios, frente a las disminuciones de costes, especialmente en equipamiento TPDDI (Twisted Pair Distributed Data Interface).
- FFOL está orientada en el aspecto de plena interoperabilidad entre FDDI y ATM, y los desarrollos actuales indican que permitirá la coexistencia total entre ambas tecnologías: Posibilidad de operar sobre enlaces en redes públicas alquiladas como SONET, habilidad para servir como backbone a múltiples redes FDDI, posibilidad de proporcionar interconexiones eficientes a WAN's como ISDN (RDSI), enlaces dúplex, aislamiento frente a fallos (con mecanismos de información y recuperación de los mismos), mecanismos específicos para gestionar todos los componentes de la red (incluyendo conexiones, nodos, estaciones, y protocolos), soporte integrado para todo tipo de servicios (datos, gráficos, vídeo y audio), soporte de fibra mono y multi-modo, soporte para topologías en anillo y en árbol, y modo de acceso al medio compatibles con FDDI-II y FDDI/ATM.
- Si se decidiera sustituir el equipamiento por ATM o Fast Ethernet, la inversión en cableado TPDDI se aprovecharía al 100%.

FDDI en la actualidad

- Ha sido mejorada por la FDDI II
- Algunos operadores están empleando redes públicas FDDI como un paso previo a redes del estándar IEEE 802.6, con el fin de interconectar redes locales localizadas en distintos edificios dentro de: Campus Universitarios, Parques Tecnológicos, Complejos Industriales, etc.



CAPITULO 3

Introducción a Frame Relay

Introducción:

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI: El ITU (entonces CCITT). Sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los comutadores, en cada "salto" de la red. X.25 tiene el grave inconveniente de su importante "overhead" producido por los mecanismos de control de errores y de flujo.

Hasta hace relativamente poco tiempo, X.25 se ha venido utilizando como medio de comunicación para datos a través de redes telefónicas con infraestructuras analógicas, en las que la norma ha sido la baja calidad de los medios de transmisión, con una alta tasa de errores. Esto justificaba los abundantes controles de errores y sus redundantes mecanismos para el control de flujo, junto al pequeño tamaño de los paquetes. En resumen, se trataba de facilitar las retransmisiones para obtener una comunicación segura.

Frame Relay, por el contrario, maximiza la eficacia, aprovechándose para ello de las modernas infraestructuras, de mucha mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información.

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps., aunque nada le impide superarlas.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son comutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

Dispositivos de Frame Relay Los dispositivos conectados a una WAN Frame Relay caen dentro de una de dos categorías generales:

- **DTE (Data Terminal Equipment):** Los DTEs, en general, se consideran equipo de terminal para una red específica y, por lo general, se localizan en las instalaciones de un cliente. De hecho, pueden ser propiedad del cliente. Algunos ejemplos de los dispositivos DTE son las terminales, computadoras personales, Routers y puentes.
- **Los DCE (Data Circuit Terminating Equipment):** Los DCE son dispositivos de interconectividad de redes propiedad de la compañía de larga distancia. El propósito del equipo DCE es proporcionar los servicios de temporización y comutación en una red, que son en realidad los dispositivos que transmiten datos a través de la WAN.

En la mayoría de los casos, éstos son switches de paquetes. La conexión entre un dispositivo DTE y un DCE consta de un componente de la capa física y otro de la capa de enlace de datos. El componente físico define las especificaciones mecánicas, eléctricas y de procedimiento para la conexión entre dispositivos.

Una de las especificaciones de internase de la capa física que más se utiliza es la especificación del RS-232 (Estándar recomendado 232). El componente de la capa de enlace de datos define el protocolo que establece la conexión entre el dispositivo DTE, que puede ser un Router y el dispositivo DCE, que puede ser un switch. En este trabajo se realiza una especificación de protocolo de uso común en las interredes WAN, el protocolo Frame Relay

Circuitos Virtuales Frame Relay

Frame Relay ofrece comunicación de la capa de enlaces de datos orientada a la conexión esto significa que hay una comunicación definida entre cada par de dispositivos y que estas conexiones están asociadas con el identificador de conexión. Este servicio se implementa por medio de un circuito virtual Frame Relay, que es una conexión lógica creada entre dos DTE (Equipos Terminales de Datos) a través de una PSN (Red de Comunicación de Paquetes) de Frame Relay.

Los circuitos Virtuales ofrecen una trayectoria de comunicación bidireccional de un dispositivo DTE a otro y se identifica de manera única por medio del DLCI (Identificador de Conexiones de Enlace de Datos).

Se puede multiplexar una gran cantidad de circuitos virtuales en un solo circuito físico para transmitirlos a través de la red. Con frecuencia esta característica permite conectar múltiples dispositivos DTE con menos equipo y una red compleja. Un circuito virtual puede pasar por cualquier cantidad de dispositivos intermedios DCE (Switches) ubicados en la red Frame Relay PSN (packet switching network | Red de Comunicación de Paquetes).

Los circuitos virtuales Frame Relay caen dentro de dos categorías:

Circuitos Virtuales Comutados

- Los SVCs son conexiones temporales que se utilizan en situaciones donde se requiere solamente de una transferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un SVC consta de cuatro estados:
 1. Establecimiento de la llamada: Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.
 2. Transferencia de datos: Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
 3. Ocioso: La conexión entre los dispositivos DTE aún está activa, sin embargo no hay transferencia de datos. Si un SVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.
 4. Terminación de la llamada: Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar

Circuitos Virtuales Permanentes

Los PVCs son conexiones establecidas en forma permanente, que se utilizan en transferencia de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La comunicación a través de un PVC no requiere los estados de establecimiento de llamada y finalización que se utilizan con los SVCs. Los PVCs siempre operan en alguno de los estados siguiente:

1. Transferencia de datos: Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
2. Ociooso: Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos.

A diferencia de los SVCs los PVCs no se darán por finalizados en ninguna circunstancia ya que se encuentran en estado ocioso. Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

[Identificador de Conexión del Enlace de Datos](#)

Los circuitos virtuales de Frame Relay se identifican a través de los DLCIs (Identificadores de Conexión del Enlace de Datos). Normalmente los valores de DLCI son asignados por el proveedor de los servicios de Frame Relay (en su caso, la compañía telefónica). Los DLCIs Frame Relay tiene un significado local, lo que significa que los valores en sí mismo no son únicos en la WAN Frame Relay; por ejemplo, dos dispositivos DTE conectados a través de un circuito virtual, pueden usar un valor diferente de DLCI para hacer referencia a la misma conexión. .

[Mecanismos de control de saturación](#)

Frame Relay reduce el gasto indirecto de la red, al implementar mecanismos simples de notificación de la saturación, mas que un control de flujo explícito por cada circuito virtual. En general Frame Relay se implementa sobre medios de transmisión de red confiables para no sacrificar la integridad de los datos, ya que el control de flujo se puede realizar por medio de los protocolos de las capas superiores La tecnología Frame Relay implementa dos mecanismos de notificación de saturación:

- FECN (Notificación de la Saturación Explícita Hacia Adelante)
- BECN (Notificación de la Saturación explícita Hacia atrás)

Tanto FECN como BECN son controlados por un solo bit incluido en el encabezado de la trama Frame Relay. Este también contiene un bit DE (Elegibilidad para descarte), que se utiliza para identificar el tráfico menos importante que se puede eliminar durante períodos de saturación.

El bit FECN es parte del campo direcciones en el encabezado de la trama Frame Relay. El mecanismo FECN inicia en el momento en que un dispositivo DTE envía tramas Frame Relay a la red. Si la red está saturada, los dispositivos DCE (switches) fijan el valor de los bits FECN de las tramas en 1.

Cuando las tramas llegan al dispositivo DTE de destino, el campo de direcciones (con el bit FECN en 1) indica que la trama se saturó en su trayectoria del origen al destino. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien la indicación se puede ignorar. El bit BECN es parte del campo Direcciones del encabezado de la trama Frame Relay. Los dispositivos del DCE fijan el valor del bit BECN en 1 en las que viajan en sentido opuesto a las tramas con bit FECN igual a 1. Esto permite al dispositivo DTE receptor saber que una trayectoria específica en la red está saturada. Posteriormente el dispositivo DTE envía información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien se puede ignorar la indicación.

BIT DE

El bit DE (Elegibilidad para Descarte) se utiliza para indicar que una trama tiene una importancia menor que otras. El bit DE es parte del campo Direcciones en el Encabezado de la trama Frame Relay. Los dispositivos DTE pueden fijar el valor del bit DE de una trama en 1 para indicar que esta tiene una importancia menor respecto a las demás tramas. Al saturarse la red los dispositivos DCE descartaran las tramas con el bit DE fijado en 1 antes de descartar aquellas que no la tienen. Por lo anterior disminuye la probabilidad de que los dispositivos DCE de Frame Relay eliminen datos críticos durante el blindaje de saturación.

Verificación de errores en Frame Relay

Frame Relay utiliza un mecanismo para la verificación de errores conocido como CRC (Verificación de Redundancia cíclica). El CRC compara dos valores calculados para determinar si se ha presentado errores durante la transmisión del origen al destino. Frame Relay disminuye el gasto indirecto al implementarse la verificación de errores mas que su corrección. Frame Relay por lo general se implementa en medios confiables de transmisión de red, por lo que la integridad de los datos no se sacrifica si la corrección de un error se deja a los protocolos de las capas superiores que operan en la parte mas alta de Frame Relay.

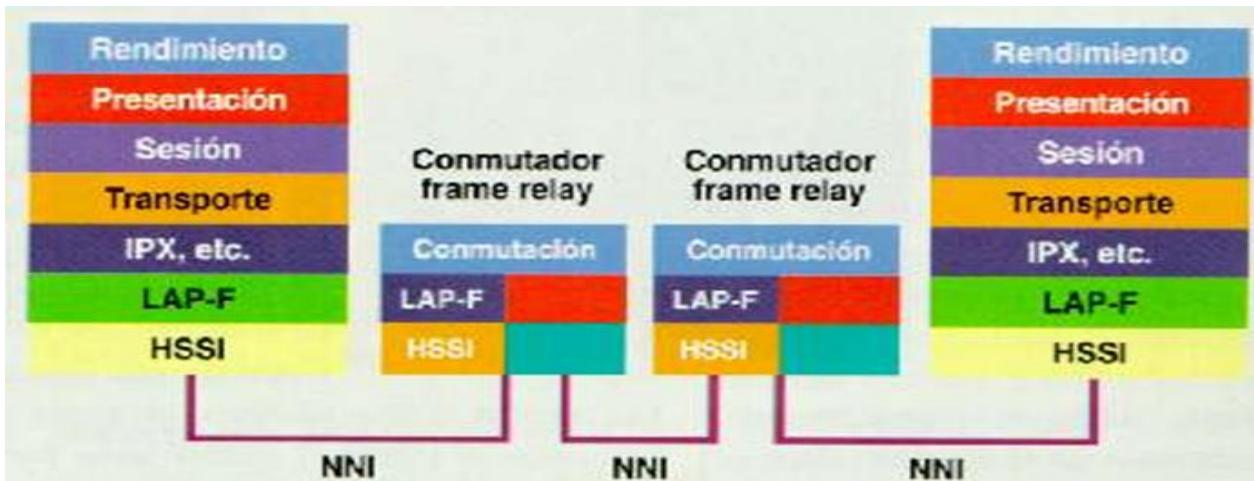
Interface LMI

LMI (Interface de la Administración Local) es un conjunto de avances en la especificación básica de Frame Relay. LMI fue desarrollada en 1990 por Cisco Systems, StrataCom, Northern Telecom y Digital Equipment Corporation. Presenta varias características (llamadas extensiones) para la administración de interredes complejas. Entre las extensiones LMI más importantes de Frame Relay están el direccionamiento Global, los mensajes de status de los circuitos virtuales y la multidifusión. La extensión de direccionamiento global LMI otorga los valores del DLCI (Identificador de la Conexión de Enlace de Datos) Frame Relay un significado global más que local. Los valores DLCI se convierten en direcciones DTE únicas en la WAN Frame Relay. La extensión global de direccionamiento agrega funcionalidad y buena administración a las interredes Frame Relay. Los mensajes de status de los circuitos virtuales LMI permiten la comunicación y sincronización entre los dispositivos DTE y DCE Frame Relay. Estos mensajes se utilizan para reportar, de manera periódica, el status de los PVCs; así se previene el envío de datos a agujeros negros (esto es, a través de los PVCs inexistentes). La extensión de LMI para multidifusión permite que se asignen grupos de multidifusión. Con la multidifusión se ahorra ancho de banda, ya que permite que los mensajes sobre la resolución de direcciones y de actualizaciones de ruteo sean enviados solamente a grupos específicos de Routers. La extensión también permite reportes sobre el status de los grupos de multidifusión de los mensajes de actualización.

Tecnología:

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que comutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red.

Estructura OSI de la red Frame Relay



Encapsulación Frame Relay

Frame Relay toma paquetes de datos de un protocolo de capa de red, como IPv4 o IPv6, los encapsula como la porción de datos de una trama Frame Relay y después pasa la trama a la capa física para la entrega en el cable. Para entender cómo funciona esto, es conveniente entender cómo se relaciona con los niveles inferiores del modelo OSI. Frame Relay encapsula los datos para el transporte y los baja a la capa física para la entrega, como se muestra en la figura 1. Primero, Frame Relay acepta un paquete de un protocolo de capa de red, como IPv4. A continuación, lo envuelve con un campo de dirección que contiene el DLCI y un valor de checksum. Se agregan campos de indicador para indicar el principio y el fin de la trama. Los campos de indicador marcan el comienzo y el fin de la trama, y siempre son los mismos.

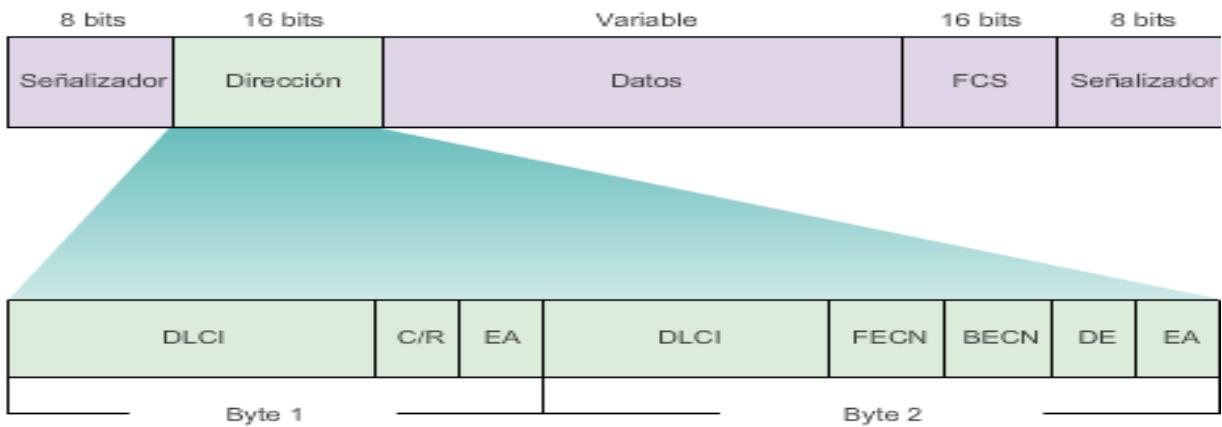
Los indicadores se representan como el número hexadecimal 7E o como el número binario 01111110. Una vez que se encapsula el paquete, Frame Relay pasa la trama a la capa física para el transporte.

El router CPE encapsula cada paquete de capa 3 dentro de un encabezado y un tráiler de Frame Relay antes de enviarlo a través del VC.

El encabezado y el tráiler se definen en la especificación de servicios portadores para el procedimiento de acceso de enlace para Frame Relay (LAPF), ITU Q.922-A.

Como se muestra en la figura, el encabezado de Frame Relay (campo de dirección) contiene específicamente lo siguiente:

Trama Frame Relay estándar



- DLCI: el DLCI de 10 bits es uno de los campos más importantes del encabezado de Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y el switch. Un DLCI exclusivo representa cada conexión virtual que se multiplexa en el canal físico. Los valores de DLCI solo tienen importancia local, lo que significa que solo son exclusivos para el canal físico en el que residen. Por lo tanto, los dispositivos de los extremos opuestos de una conexión pueden usar diferentes valores de DLCI para referirse a la misma conexión virtual.
- C/R: es el bit que sigue al byte de DLCI más importante del campo de dirección. El bit C/R no está definido actualmente.
- Dirección extendida (EA): si el valor del campo EA es 1, se determina que el byte actual es el último octeto del DLCI. Si bien todas las implementaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta capacidad permite que se usen DLCI más largos en el futuro. El octavo bit de cada byte del campo Dirección indica la EA.
- Control de congestión: consta de 3 bits de notificación de congestión de Frame Relay. Estos 3 bits se denominan específicamente “bit de notificación explícita de congestión hacia delante” (FECN), “bit de notificación explícita de congestión hacia atrás” (BECN) y “bit elegible de descarte”.

Por lo general, la capa física es EIA/TIA-232, 449 o 530, V.35 o X.21. La trama Frame Relay es un subconjunto del tipo de trama HDLC; por lo tanto, se delimita con campos de indicador. El indicador de 1 byte utiliza el patrón de bits 01111110.

La FCS determina si ocurrieron errores en el campo de dirección de capa 2 durante la transmisión. El nodo emisor calcula la FCS antes de la transmisión, y el resultado se inserta en el campo FCS. En el extremo distante, se calcula un segundo valor de FCS y se lo compara con la FCS en la trama. Si los resultados son iguales, se procesa la trama. Si existe una diferencia, se descarta la trama. Frame Relay no notifica el origen cuando se descarta una trama. El control de errores se reserva para las capas superiores del modelo OSI.

Topologías de Frame Relay

Cuando se deben conectar más de dos sitios, se debe planificar la topología o el mapa de Frame Relay de las conexiones entre los sitios. Un diseñador de red debe considerar la topología desde varios puntos de vista para comprender la red y los equipos utilizados para armarla. Las topologías completas para el diseño, la implementación, la operación y el mantenimiento incluyen mapas de descripción general, mapas de las conexiones lógicas mapas funcionales y mapas de direcciones que muestren el detalle de los equipos y los enlaces de canales.

Las redes Frame Relay enlazan decenas e incluso cientos de sitios en forma rentable. Si se considera que una red empresarial podría abarcar cualquier cantidad de proveedores de servicios e incluir redes de empresas adquiridas que difieren en el diseño básico, registrar las topologías puede ser un proceso muy complicado. Sin embargo, cada red o segmento de red puede verse como uno de tres tipos de topología: en estrella, malla completa o malla parcial.

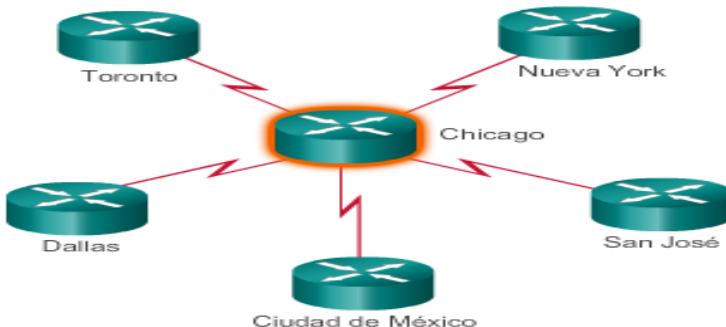
Topología en estrella (hub-and-spoke)

La topología de WAN más simple es una estrella, como la que se muestra en la figura 1. En esta topología, la empresa SPAN Ingeniería tiene un sitio central en Chicago que funciona como hub y aloja los servicios principales.

Las conexiones a cada uno de los cinco sitios remotos funcionan como spokes (que significa "rayos"). En una topología en estrella, la ubicación del hub generalmente se elige por el costo de línea arrendada más bajo. Cuando se implementa una topología en estrella con Frame Relay, cada sitio remoto tiene un enlace de acceso a la nube de Frame Relay con un único VC.

En la figura, se muestra la topología en estrella en el contexto de una nube de Frame Relay. El hub en Chicago tiene un enlace de acceso con varios VC, uno para cada sitio remoto. Las líneas que salen de la nube representan las conexiones del proveedor de servicios de Frame Relay y terminan en las instalaciones del cliente. En general, estas líneas tienen velocidades que van desde 56 kb/s hasta un T1 (1544 Mb/s) y más rápidas. Se asigna uno o más números de DLCI a cada terminal de la línea. Debido a que los costos de Frame Relay no se relacionan con la distancia, no es necesario que el hub esté en el centro geográfico de la red.

Topología en estrella (Hub and Spoke)

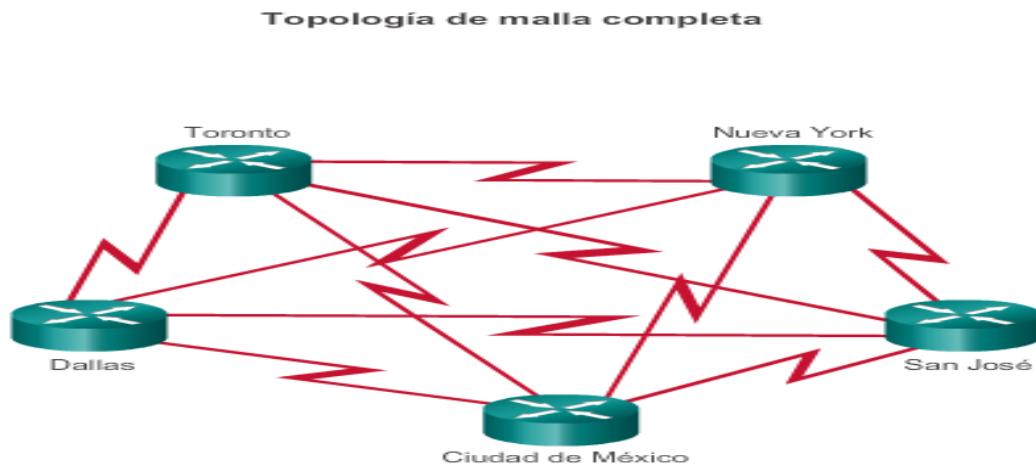


Topología en estrella: hub de Chicago con cinco enlaces físicos (spokes)

Topología de malla completa

En la figura, se muestra una topología de malla completa que usa líneas dedicadas. Una topología de malla completa se adapta a una situación en la que los servicios a los que se debe acceder están en distintas zonas geográficas y en la que se requiere un acceso altamente confiable a ellos. Una topología de malla completa conecta cada sitio a todos los demás. Si se utilizan interconexiones de línea arrendada, las líneas y las interfaces seriales adicionales agregan costos. En este ejemplo, se requieren 10 líneas dedicadas para interconectar cada sitio en una topología de malla completa.

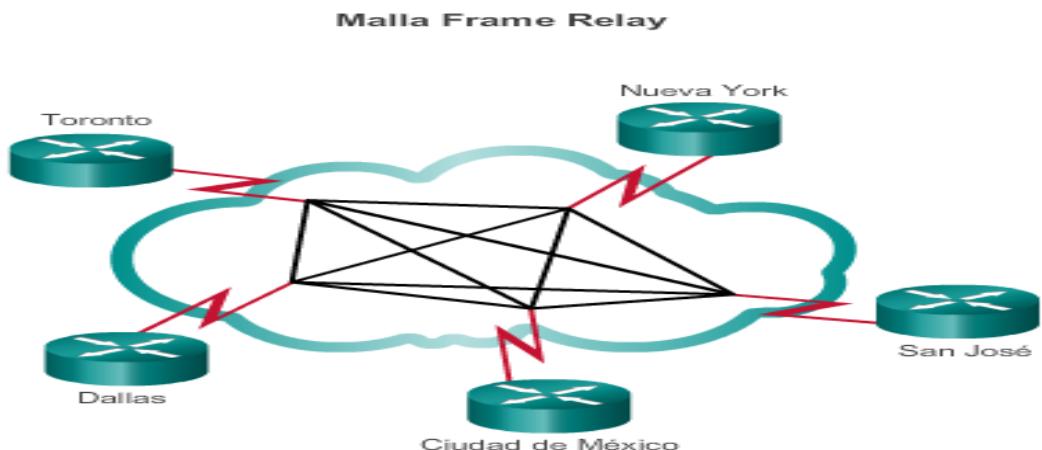
Con una malla de Frame Relay, un diseñador de red puede armar varias conexiones simplemente configurando VC adicionales en cada enlace existente, como se muestra en la figura 2. Esta actualización de software eleva la topología en estrella a una topología de malla completa sin los gastos de hardware o de líneas dedicadas adicionales. Debido a que los VC utilizan la multiplexación estadística, varios VC en un enlace de acceso usan Frame Relay mejor que los VC individuales. En la figura 2, se muestra cómo SPAN utilizó cuatro VC en cada enlace para escalar su red sin agregar nuevo hardware. Los proveedores de servicios cobran el ancho de banda adicional, pero esta solución generalmente es más rentable que usar líneas dedicadas.



Topología de malla parcial

Para las redes grandes, una topología de malla completa rara vez es accesible, porque la cantidad de enlaces necesarios aumenta exponencialmente. El problema no se debe al costo del hardware, sino a que hay un límite teórico de menos de 1000 VC por enlace. En la práctica, el límite es inferior a eso.

Por este motivo, las redes más grandes se suelen configurar en una topología de malla parcial. Con la malla parcial, existen más interconexiones que las requeridas para una configuración en estrella, pero no tantas como para una malla completa. El patrón real depende de los requisitos de flujo de datos.



Topología de malla: cada DTE tiene un enlace físico que transporta 4 VC.

Asignación de direcciones de Frame Relay

Antes de que un router Cisco pueda transmitir datos a través de Frame Relay, necesita saber qué DLCI local se asigna a la dirección de capa 3 del destino remoto. Los routers Cisco admiten todos los protocolos de capa de red mediante Frame Relay, como IPv4, IPv6, IPX y AppleTalk. Esta asignación de dirección a DLCI se puede lograr mediante la asignación estática o dinámica. En la figura 1, se muestra un ejemplo de topología con asignación de DLCI.

ARP inverso

El protocolo de resolución de direcciones (ARP) inverso es una herramienta principal de Frame Relay. Mientras que ARP traduce direcciones IPv4 de capa 3 a direcciones MAC de capa 2, ARP inverso hace lo contrario. Las direcciones IPv4 de capa 3 correspondientes deben estar disponibles antes de que se puedan utilizar los VC.

Nota: Frame Relay para IPv6 utiliza el descubrimiento inverso de vecinos (IND) para obtener una dirección IPv6 de capa 3 a partir de un DLCI de capa 2. Un router Frame Relay envía un mensaje de solicitud IND para solicitar una dirección IPv6 de capa 3 correspondiente a una dirección DLCI de capa 2 del router Frame Relay remoto. Al mismo tiempo, el mensaje de solicitud IND proporciona la dirección DLCI de capa 2 del emisor al router Frame Relay remoto.

Asignación dinámica

La asignación dinámica de direcciones depende de ARP inverso para resolver una dirección IPv4 de capa de red de siguiente salto a un valor de DLCI local. El router Frame Relay envía solicitudes de ARP inverso en su PVC para descubrir la dirección de protocolo del dispositivo remoto conectado a la red Frame Relay. El router usa las respuestas para completar una tabla de asignación de direcciones a DLCI en el router Frame Relay o en el servidor de acceso. El router arma y mantiene esta tabla de asignación, que contiene todas las solicitudes de ARP inverso resueltas, incluidas las entradas de asignación dinámica y estática.

En los routers Cisco, ARP inverso está habilitado de manera predeterminada para todos los protocolos habilitados en la interfaz física. Los paquetes de ARP inverso no se envían para los protocolos que no están habilitados en la interfaz.

Asignación estática de Frame Relay

El usuario puede elegir anular la asignación dinámica de ARP inverso mediante el suministro de un mapa estático manual para la dirección de protocolo de siguiente salto a un DLCI local. Un mapa estático funciona de manera similar a ARP inverso dinámico mediante la asociación de una dirección de protocolo de siguiente salto específica a un DLCI de Frame Relay local. No se puede utilizar ARP inverso y una instrucción de asignación para el mismo DLCI y el mismo protocolo.

Un ejemplo del uso de la asignación estática de direcciones es una situación en la cual el router en el otro lado de la red Frame Relay no admite ARP inverso dinámico para un protocolo de red específico. A fin de proporcionar conectividad, se requiere una asignación estática para completar la dirección de capa de red remota a la resolución de DLCI local.

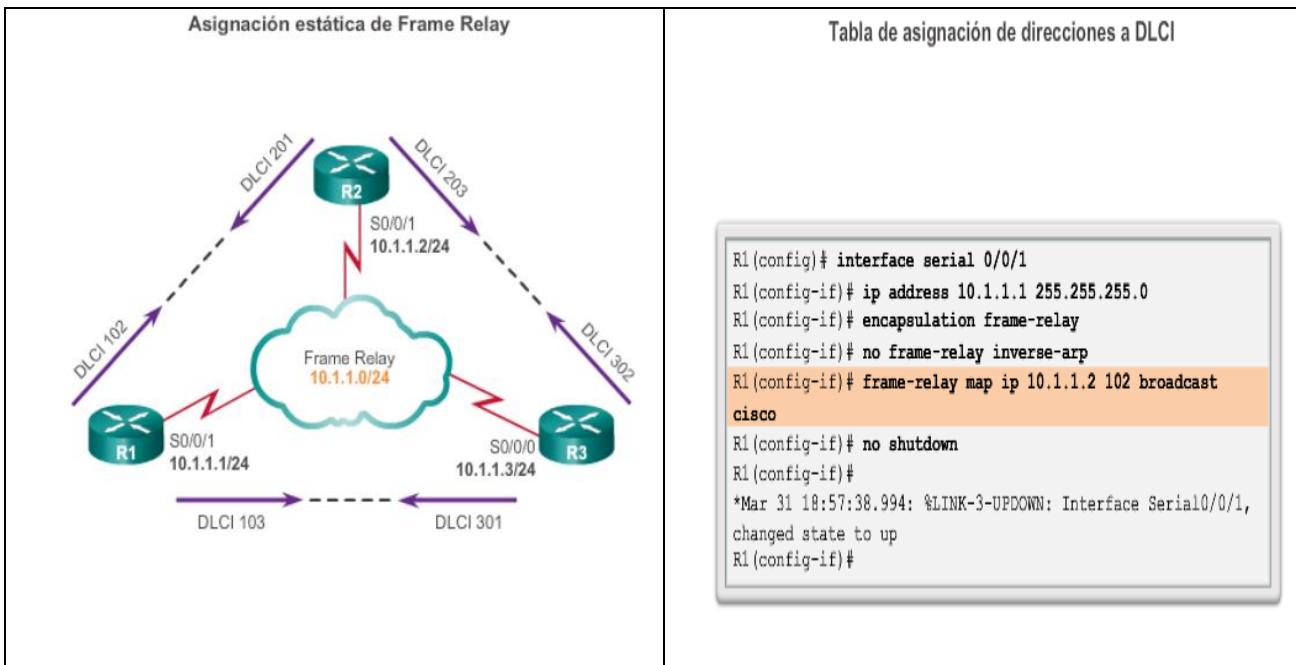
En una red Frame Relay hub-and-spoke, se da otro ejemplo. Utilice la asignación estática de direcciones en los routers spoke para proporcionar la posibilidad de conexión de spoke a spoke. Debido a que los routers spoke no tienen conectividad directa entre sí, ARP inverso dinámico no funciona entre ellos. ARP inverso dinámico depende de la presencia de una conexión punto a punto directa entre dos extremos. En este caso, ARP inverso dinámico solo funciona entre hub y spoke, y los spokes requieren asignación estática para proporcionar la posibilidad de conexión entre sí.

Configuración de la asignación estática

El establecimiento de la asignación estática depende de las necesidades de la red. Para asignar entre una dirección de protocolo de siguiente salto y una dirección de destino DLCI, utilice este comando: **frame-relay map protocol protocol-address/dci [broadcast] [ietf] [cisco]**.

Utilice la palabra clave **ietf** cuando se conecte a un router que no es de Cisco.

La configuración del protocolo OSPF (Open Shortest Path First) se puede simplificar considerablemente agregando la palabra clave optativa **broadcast** cuando se realiza esta tarea. La palabra clave **broadcast** especifica que se permite el tráfico de difusión y multidifusión en el VC. Esta configuración permite el uso de protocolos de routing dinámico en el VC.



Verificar

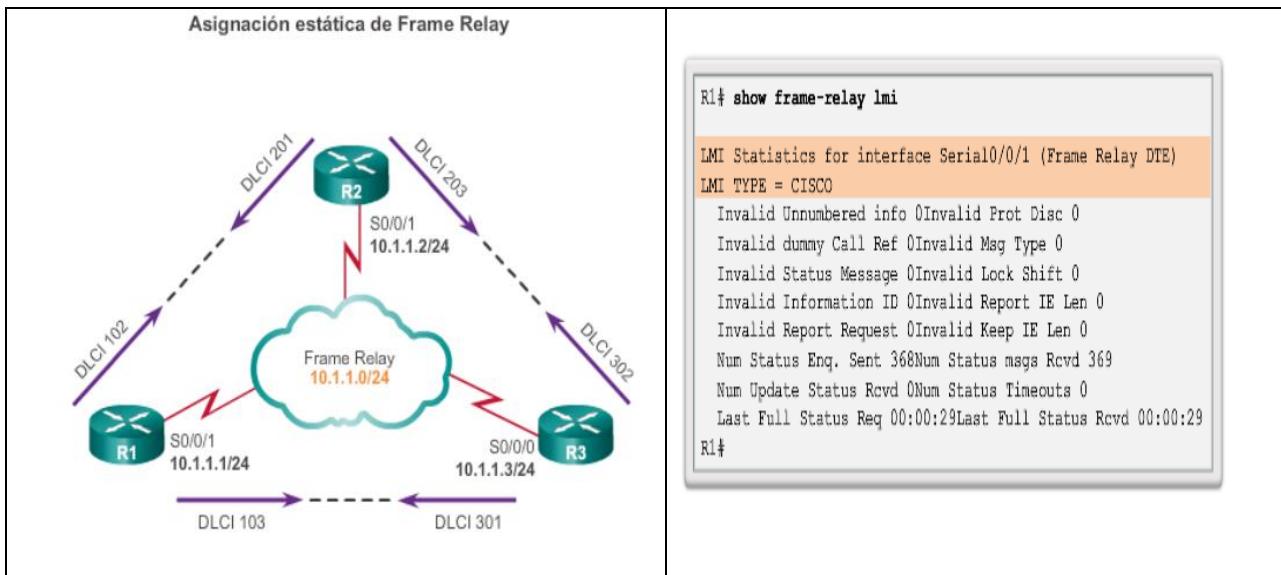
```
R1# show frame-relay map
Serial0/0/1 (up): ip 10.1.1.2 dlcii 102(0x66,0x1860), static,
                     broadcast,
                     CISCO, status defined, active
R1#
```

Interfaz de administración local (LMI)

Otro concepto importante en Frame Relay es la interfaz de administración local (LMI). El diseño de Frame Relay proporciona la transferencia de datos comutada por paquetes con retrasos mínimos de extremo a extremo. El diseño original omite cualquier cosa que pudiera ocasionar un retraso.

Cuando los proveedores implementaron Frame Relay como una tecnología independiente y no como un componente de ISDN, decidieron que los DTE debían adquirir dinámicamente la información sobre el estado de la red. Sin embargo, el diseño original no incluía esta característica. Un consorcio de Cisco, Digital Equipment Corporation (DEC), Northern Telecom y StrataCom amplió el protocolo Frame Relay a fin de proporcionar capacidades adicionales para los entornos complejos de internetworking. Estas ampliaciones se conocen colectivamente como la LMI.

Es fácil confundir la LMI y la encapsulación. La LMI es una definición de los mensajes que se usan entre el DTE (el R1) y el DCE (el switch Frame Relay que pertenece al proveedor de servicios). La encapsulación define los encabezados que utiliza un DTE para comunicar información al DTE en el otro extremo de un VC. Al switch y al router conectado a él les interesa utilizar el mismo LMI. Al switch no le interesa la encapsulación. A los routers terminales (DTE) sí les interesa la encapsulación.



Existen varios tipos de LMI, y cada uno es incompatible con los demás. El tipo de LMI configurado en el router debe coincidir con el tipo que utiliza el proveedor de servicios. Los routers Cisco admiten tres tipos de LMI:

- CISCO: extensión original de LMI
- ANSI: correspondiente al estándar ANSI T1.617, anexo D
- Q933A: correspondiente al estándar ITU Q933, anexo A

Para mostrar la información de los mensajes de LMI y los números de DLCI asociados, use el comando **show interfaces [tipo número]**, como se muestra en la figura 2. Cisco utiliza el DLCI 1023 para identificar los mensajes de LMI que se usan para la administración de enlaces Frame Relay

Como se muestra en la figura 3, los mensajes de estado de LMI son similares a la trama Frame Relay. En lugar del campo Dirección de una trama Frame Relay que se utiliza para la transmisión de datos, hay un campo DLCI de LMI. A continuación del campo DLCI están los campos Control, Discriminador de protocolo y Referencia de llamada. Estos son los mismos que en la trama de datos de Frame Relay estándar.

Identificadores LMI		Visualización
Identificadores de VC	Tipos de VC	
0	Administración de enlace LMI (ANSI, ITU)	
1 a 15	Se reserva para uso futuro	
16 a 991	Disponible para la asignación de terminal de VC	
992 a 1007	Información de administración de capa2 optativa	
1008 a 1018	Se reserva para uso futuro (ANSI, UIT)	
1019 a 1022	Multidifusión de LMI	
1023	Administración de enlace LMI (Cisco)	

Verificación del funcionamiento de Frame Relay: operaciones de LMI

El siguiente paso es analizar algunas estadísticas de LMI mediante el comando **show frame-relay lmi**. En la ilustración, se muestra un resultado de ejemplo que indica la cantidad de mensajes de estado intercambiados entre el router local y el switch Frame Relay local. Asegúrese de que los contadores entre los mensajes de estado enviados y recibidos aumenten. Esto valida que existe comunicación activa entre el DTE y el DCE.

También busque elementos Invalid distintos de cero. Esto ayuda a aislar el problema de comunicaciones de Frame Relay entre el switch de la prestadora de servicios y el router cliente.

```
R1# show frame-relay lmi

LMI Statistics for interface          (Frame Relay DTE) LMI TYPE = CISCO
Serial0/0/1

  Invalid Unnumbered info 0           Invalid Prot Disc 0
  Invalid dummy Call Ref 0          Invalid Msg Type 0
  Invalid Status Message 0          Invalid Lock Shift 0
  Invalid Information ID 0          Invalid Report IE Len 0
  Invalid Report Request 0          Invalid Keep IE Len 0
  Num Status Enq. Sent 578          Num Status msgs Rcvd 579
  Num Update Status Rcvd 0          Num Status Timeouts 0
  Last Full Status Req 00:00:28     Last Full Status Rcvd 00:00:28

R1#
```

Verificación del funcionamiento de Frame Relay: estado de PVC

Utilice el comando **show frame-relay pvc [interface interfaz] [dci]** para ver las estadísticas de tráfico y PVC. Este comando además resulta útil para ver la cantidad de paquetes de BECN y FECN que recibe el router. El estado de PVC puede ser activo, inactivo o eliminado.

El comando **show frame-relay PVC** muestra el estado de todos los PVC configurados en el router. También puede especificar un PVC en particular.

Después de recopilar las estadísticas, utilice el comando **clear counters** para restablecer los contadores de estadísticas. Después de borrar los contadores, espere 5 o 10 minutos antes de volver a emitir los comandos **show**. Observe cualquier error adicional. Si necesita comunicarse con la prestadora de servicios, estas estadísticas contribuyen a resolver los problemas.

```
R1# show frame-relay pvc 102
PVC statistics for interface Serial0/0/1 (Frame Relay DTE)
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/1.102

  input pkts 1230      output pkts 1243      in bytes 103826
  out bytes 105929     dropped pkts 0       in pkts dropped 0
  out pkts dropped 0   out bytes dropped 0
  in FECN pkts 0      in BECN pkts 0       out FECN pkts 0
  out BECN pkts 0      in DE pkts 0        out DE pkts 0
  out bcast pkts 1228  out bcast bytes 104952
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 01:38:29, last time pvc status changed 01:26:19
R1#
```

Verificación del funcionamiento de Frame Relay: ARP inverso

Para borrar mapas de Frame Relay creados dinámicamente mediante ARP inverso, utilice el comando **clear frame-relay inarp**, como se muestra en la figura 1.

La última tarea es confirmar si el comando **frame-relay inverse-arp** resolvió una dirección IPv4 remota a un DLCI local. Utilice el comando **show frame-relay map** para mostrar las entradas de mapa actuales y la información sobre las conexiones.

Cuando se realiza una solicitud de ARP inverso, el router actualiza su tabla de mapa con tres estados posibles de conexión LMI. Estos estados son los siguientes:

- **ACTIVE**: indica un circuito de extremo a extremo (DTE a DTE) correcto.
- **INACTIVE**: indica una conexión correcta al switch (DTE a DCE) sin que se detecte un DTE en el otro extremo del PVC. Esto puede ocurrir debido a una configuración incorrecta en el switch.
- **DELETED**: indica que el DTE está configurado para un DLCI que el switch no reconoce como válido para esa interfaz.

```
R1# clear frame-relay inarp
R1# show frame-relay map
Serial0/0/1.102 (up): point-to-point dlci, dlci 102(0x66,0x1860),
broadcast status defined, active
Serial0/0/1.103 (up): point-to-point dlci, dlci 103(0x67,0x1870),
broadcast status defined, active
R1#
```

```
R2# clear frame-relay inarp
R2# show frame-relay map
Serial0/0/1.201 (up): point-to-point dlci, dlci 201(0xC9,0x3090),
broadcast status defined, active
Serial0/0/1.203 (up): point-to-point dlci, dlci 203(0xCB,0x30B0),
broadcast status defined, active
R2#
```

La contratación:

A la hora de contratar un enlace Frame Relay, hay que tener en cuenta varios parámetros. Por supuesto, el primero de ellos es la velocidad máxima del acceso (V_t), que dependerá de la calidad o tipo de línea empleada.

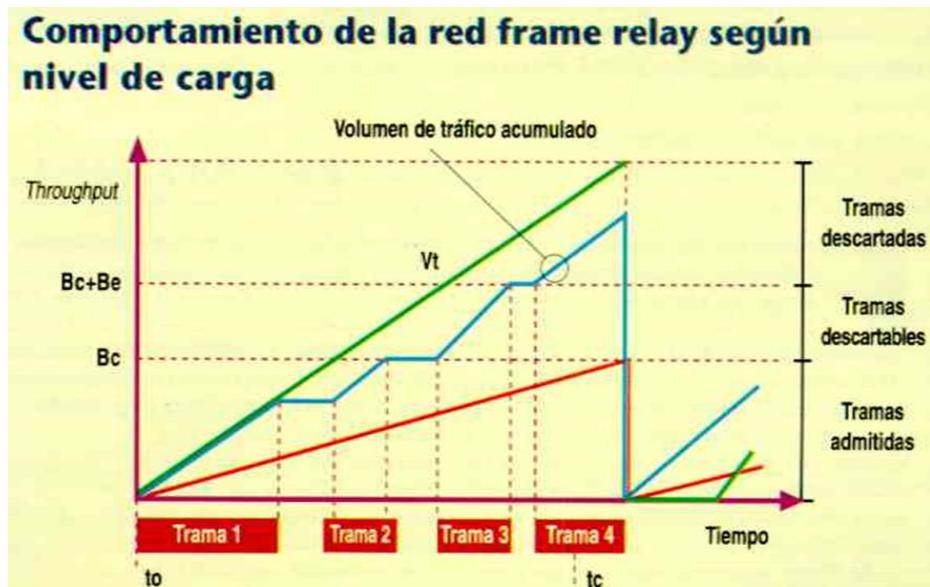
Pero hay un parámetro más importante: se trata del CIR (velocidad media de transmisión o Committed Information Rate). Es la velocidad que la red se compromete a servir como mínimo. Se contrata un CIR para cada PVC o bien se negocia dinámicamente en el caso de SVC's.

El Committed Burst Size (B_c) es el volumen de tráfico alcanzable transmitiendo a la velocidad media (CIR). Por último la ráfaga máxima o Excess Burst Size (B_e) es el volumen de tráfico adicional sobre el volumen alcanzable.

Para el control de todos estos parámetros se fija un intervalo de referencia (t_c). Así, cuando el usuario transmite tramas, dentro del intervalo t_c , a la velocidad máxima (V_t), el volumen de tráfico se acumula y la red lo acepta siempre que este por debajo de B_c . Pero si se continúa transmitiendo hasta superar B_c , las tramas empezarán a ser marcadas mediante el bit DE (serán consideradas como desecharables).

Por ello, si se continúa transmitiendo superando el nivel marcado por B_c+B_e , la red no admitirá ninguna trama más.

Por supuesto la tarificación dentro de cada volumen (B_c/B_e) no es igual, puesto que en el caso de B_e , existe la posibilidad de que las tramas sean descartadas.



Velocidad de acceso y velocidad de información comprometida

Los proveedores de servicios arman las redes Frame Relay con switches muy grandes y potentes, pero los dispositivos solo ven la interfaz del switch del proveedor de servicios. En general, los clientes no están expuestos al funcionamiento interno de la red, que se puede armar con tecnologías de muy alta velocidad, como SONET o SDH.

Desde el punto de vista de un cliente, Frame Relay es una interfaz única configurada con uno o más PVC. Los clientes adquieren los servicios de Frame Relay de un proveedor de servicios.

- **Velocidad de acceso:** la velocidad de acceso se refiere a la velocidad del puerto. Desde el punto de vista de un cliente, el proveedor de servicios proporciona una conexión serial o un enlace de

acceso a la red Frame Relay a través de una línea arrendada. La velocidad de acceso es la velocidad a la que sus circuitos de acceso se unen a la red Frame Relay. Estos pueden ser de 56 kb/s, T1 (1544 Mb/s) o T1 fraccionada (un múltiplo de 56 kb/s o de 64 kb/s). Las velocidades de acceso se miden en el switch Frame Relay. No es posible enviar datos a mayor velocidad que la velocidad de acceso.

- **Velocidad de información comprometida (CIR):** los clientes negocian las CIR con los proveedores de servicios para cada PVC. La CIR es la cantidad de datos que la red recibe del circuito de acceso. El proveedor de servicios garantiza que el cliente pueda enviar datos a la CIR. Todas las tramas recibidas a la CIR o por debajo de esta se aceptan.

La CIR especifica la velocidad de datos máxima promedio que la red se compromete a entregar en condiciones normales. Al suscribirse a un servicio de Frame Relay, se especifica la velocidad de acceso local, por ejemplo, 56 kb/s o T1. Normalmente, el proveedor solicita que el cliente especifique una CIR para cada DLCI.

Si el cliente envía la información más rápido que la CIR en un DLCI determinado, la red marca algunas tramas con un bit de elegibilidad de descarte (DE). La red hace lo mejor para entregar todos los paquetes; sin embargo, descarta primero los paquetes DE si hay congestión.

Independientemente de cualquier costo de CPE, el cliente paga por tres componentes de los costos de Frame Relay siguientes:

- **Velocidad de acceso:** el costo de la línea de acceso desde el DTE hasta el DCE (del cliente al proveedor de servicios). Esta línea se cobra sobre la base de la velocidad del puerto que se negoció y se instaló.
- **PVC:** este componente de los costos se basa en los PVC. Después de establecer un PVC, el costo adicional para aumentar la CIR suele ser bajo y se puede hacer en pequeños incrementos (4 kb/s).
- **CIR:** en general, los clientes eligen una CIR inferior a la velocidad de acceso. Esto les permite aprovechar las ráfagas.

Sobresuscripción

En ocasiones, los proveedores de servicios venden más capacidad de la que tienen, con la suposición de que no todos exigen la capacidad que tienen permitida todo el tiempo. Esta sobresuscripción es similar a que las aerolíneas vendan más asientos de los que tienen con la expectativa de que algunos de los clientes reservados no se presenten. Debido a la sobresuscripción, hay situaciones en las que la suma de las CIR de varios PVC a una ubicación dada es superior a la velocidad del puerto o del canal de acceso. Esto puede causar congestión y descarte de tráfico

Ráfaga

Una gran ventaja de Frame Relay es que cualquier capacidad de red que no se utilice queda a disposición de todos los clientes o se comparte con ellos, generalmente sin cargo adicional. Esto permite que los clientes excedan la CIR a modo de bonificación.

Con el ejemplo anterior, en la figura 1 se muestra que la velocidad de acceso en el puerto serie S0/0/1 del router R1 es de 64 kb/s. Esto supera la combinación de las CIR de los dos PVC. En circunstancias normales, los dos PVC no deben transmitir más de 32 kb/s y 16 kb/s, respectivamente. Mientras la cantidad de datos que envían los dos PVC no excede la CIR, debería atravesar la red.

Debido a que los circuitos físicos de la red Frame Relay se comparten entre los suscriptores, suele haber momentos en los que hay un exceso de ancho de banda disponible. Frame Relay puede permitir que los clientes accedan de forma dinámica a este ancho de banda adicional y que excedan la CIR sin costo.

Las ráfagas permiten que los dispositivos que necesitan ancho de banda adicional temporalmente puedan tomarlo prestado de otros dispositivos que no lo utilizan, sin costo adicional.

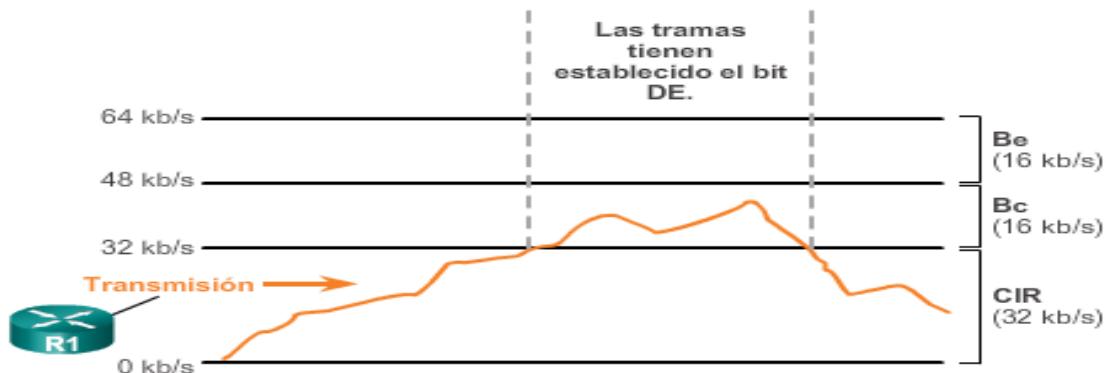
Se utilizan varios términos para describir las velocidades de ráfaga, incluidos “tamaño de ráfaga comprometida” (Bc) y “tamaño de ráfaga en exceso” (Be).

El Bc es una velocidad negociada por encima de la CIR que el cliente puede usar para transmitir durante una ráfaga breve y que representa el tráfico máximo permitido en condiciones de funcionamiento normales. Permite que el tráfico se transmita en ráfaga a velocidades más altas, tanto como el ancho de banda disponible de la red lo permita. Sin embargo, no puede exceder la velocidad de acceso del enlace. Un dispositivo puede llegar hasta el Bc y aun así esperar que los datos pasen. Si persisten las ráfagas largas, se debe adquirir una CIR más alta.

Las tramas por encima de la CIR tienen el bit DE establecido en 1, lo que las marca como elegibles para descarte si se congestionada la red. Las tramas que se envían en el nivel de Bc se marcan como elegibles para descarte (DE) en el encabezado de la trama, pero es muy probable que se reenvíen.

El Be describe el ancho de banda disponible por encima de la CIR hasta la velocidad de acceso del enlace. A diferencia del Bc, no se negocia. Las tramas se pueden transmitir en este nivel, pero es muy probable que se descarten.

Ejemplo de ráfaga de Frame Relay



Comandos de configuración básica de Frame Relay

Paso 1. Establezca la dirección IP en la interfaz

En un router Cisco, Frame Relay se admite generalmente en las interfaces seriales síncronas.

Utilice el comando **ip address** para establecer la dirección IPv4 de la interfaz.

Con el comando **ipv6 address**, los routers se configuran con direcciones IPv6:

Paso 2. Configure la encapsulación

El comando de configuración de interfaz **encapsulation frame-relay [cisco | ietf]** habilita la encapsulación de Frame Relay y permite el procesamiento de Frame Relay en la interfaz admitida. Existen dos opciones de encapsulación para escoger: cisco e ietf.

El tipo de encapsulación ietf cumple con RFC 1490 y RFC 2427.

Paso 3. Establezca el ancho de banda

Utilice el comando **bandwidth** para establecer el ancho de banda de la interfaz serial. Especifique el ancho de banda en kb/s. Este comando notifica al protocolo de routing que el ancho de banda se configuró estáticamente en el enlace

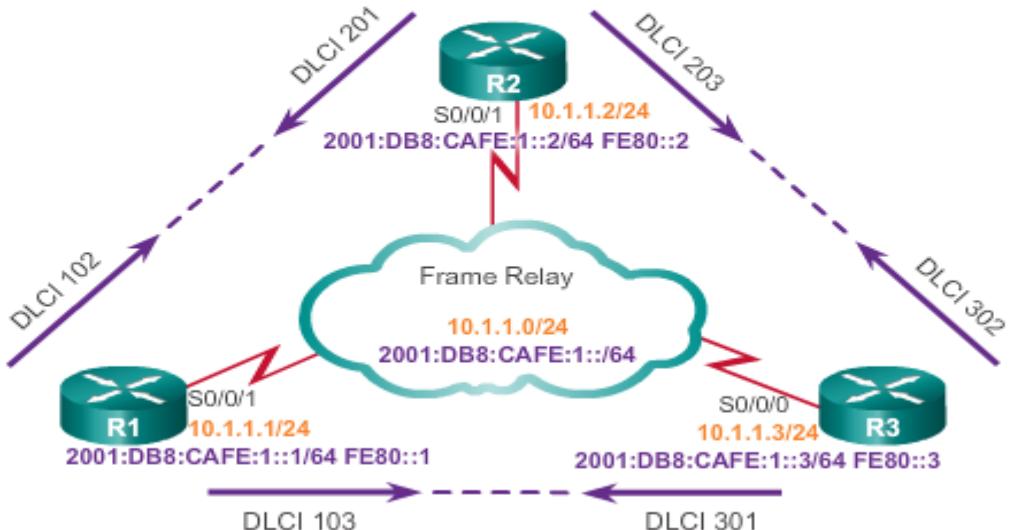
Paso 4. Establezca el tipo de LMI (optativo)

La configuración manual del tipo de LMI es optativa, ya que los routers Cisco detectan automáticamente el tipo de LMI de manera predeterminada. Recuerde que Cisco admite tres tipos de LMI: cisco, ANSI anexo D y Q933-A anexo A.

El comando **show interfaces serial** verifica la configuración, incluida la encapsulación de capa 2 de Frame Relay y el tipo de LMI. Este comando muestra la dirección IPv4, pero no incluye ninguna de las direcciones IPv6. Utilice el comando **show ipv6 interface** o el comando **show ipv6 interface brief** para verificar IPv6.

Ejemplo

Topología de Frame Relay



```
R1(config)# interface Serial0/0/1
R1(config-if)# bandwidth 64
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# encapsulation frame-relay
```

```
R2(config)# interface Serial0/0/1
R2(config-if)# bandwidth 64
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# ipv6 address 2001:db8:cafe:1::2/64
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# encapsulation frame-relay
```

Configuración de un mapa estático Frame Relay

La asignación de dirección a DLCI se logra mediante la asignación de direcciones dinámica o estática.

La asignación dinámica la realiza la característica de ARP inverso. Debido a que ARP inverso está habilitado de manera predeterminada, no se requiere ningún comando adicional para configurar la asignación dinámica en una interfaz.

La asignación estática se configura manualmente en un router. El establecimiento de la asignación estática depende de las necesidades de la red. Para asignar entre una dirección de protocolo de siguiente salto y una dirección de destino DLCI, utilice el comando **frame-relay map protocol protocol-address dlci [broadcast]**

Las redes NBMA solo permiten la transferencia de datos de una computadora a otra a través de un VC o de un dispositivo de switching. Las redes NBMA no admiten el tráfico de multidifusión y de difusión, por lo que un paquete individual no puede llegar a todos los destinos. Esto requiere que reproduzca los paquetes manualmente a todos los destinos. El uso de la palabra clave **broadcast** es una forma simplificada de reenviar las actualizaciones de routing

Verificación de un mapa estático de Frame Relay

Para verificar la asignación de Frame Relay, utilice el comando **show frame-relay map**

```
R1# show frame-relay map
Serial0/0/1 (up) : ipv6 2001:DB8:CAFE:1::2 dlci 102(0x66,0x1860),
                     static, CISCO, status defined, active
Serial0/0/1 (up) : ipv6 FE80::2 dlci 102(0x66,0x1860), static,
                     broadcast, CISCO, status defined, active
Serial0/0/1 (up) : ip 10.1.1.2 dlci 102(0x66,0x1860), static,
                     broadcast, CISCO, status defined, active
R1#
```

Configuración de las subinterfaces punto a punto

Las subinterfaces se ocupan de las limitaciones de las redes Frame Relay al proporcionar una manera de subdividir una red Frame Relay de malla parcial en una cantidad de subredes más pequeñas de malla completa o punto a punto. A cada subred se le asigna su propio número de red y aparece ante los protocolos como si se pudiera llegar a ella mediante una interfaz diferente.

Para crear una subinterfaz, utilice el comando **interface serial** en el modo de configuración global seguido del número de puerto físico, un punto (.) y el número de subinterfaz. Para simplificar la resolución de problemas, utilice el DLCI como número de subinterfaz. También debe especificar si la interfaz es punto a multipunto o punto a punto con la palabra clave **multipoint o point-to-point**, ya que no hay un valor predeterminado

El siguiente comando crea una subinterfaz punto a punto para el PVC 103

```
R1(config-if)# interface serial 0/0/0.103 point-to-point
```

Si la subinterfaz se configura como punto a punto, también se debe configurar el DLCI local de la subinterfaz para distinguirlo de la interfaz física. El DLCI también se requiere para las subinterfaces multipunto con ARP inverso habilitado para IPv4. No se requiere para las subinterfaces multipunto configuradas con mapas de rutas estáticas.

El proveedor de servicios de Frame Relay asigna los números de DLCI. Estos números van del 16 al 992 y, en general, solo tienen importancia local. El intervalo varía según la LMI que se utilice.

El comando **frame-relay interface-dlci** configura el DLCI local en la subinterfaz

```
R1(config-subif)# frame-relay interface-dlci 103
```

```
router(config-if)# interface serial number.subinterface-number  
[multipoint | point-to-point]
```

Configuración de las subinterfaces punto a punto

En la figura, se muestra la topología anterior, pero con subinterfaces punto a punto. Cada PVC es una subred distinta. Las interfaces físicas del router se dividen en subinterfaces, con cada subinterfaz en una subred distinta.

En la 2da figura, el R1 tiene dos subinterfaces punto a punto. La subinterfaz s0/0/1.102 se conecta al R2, y la subinterfaz s0/0/1.103 se conecta al R3. Cada subinterfaz está en una subred diferente.

Para configurar subinterfaces en una interfaz física, se requieren los siguientes pasos:

Paso 1. Elimine cualquier dirección de capa de red asignada a la interfaz física. Si la interfaz física tiene una dirección, las subinterfaces locales no reciben las tramas.

Paso 2. Configure la encapsulación de Frame Relay en la interfaz física mediante el comando **encapsulation frame-relay**.

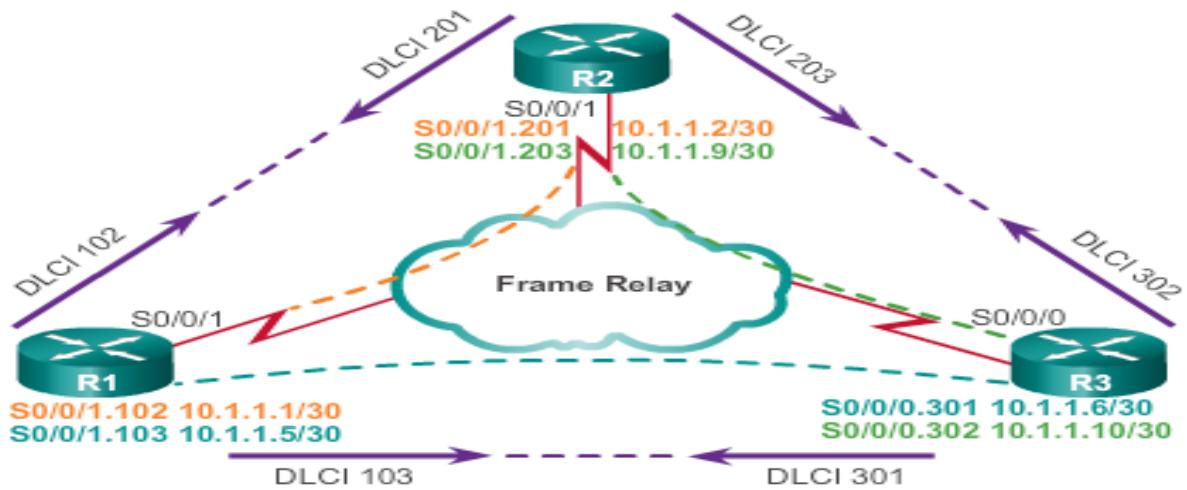
Paso 3. Cree una subinterfaz lógica para cada uno de los PVC definidos. Especifique el número de puerto, seguido de un punto (.) y el número de subinterfaz. Para simplificar la resolución de problemas, se sugiere que el número de subinterfaz coincida con el número de DLCI.

Paso 4. Configure una dirección IP para la interfaz y establezca el ancho de banda.

Paso 5. Configure el DLCI local en la subinterfaz mediante el comando **frame-relay interface-dlci**. Recuerde que el proveedor de servicios de Frame Relay asigna los números de DLCI.

Utilice el verificador de sintaxis de la figura 3 para configurar la interfaz física del router R2 en subinterfaces punto a punto con la configuración de Frame Relay correspondiente.

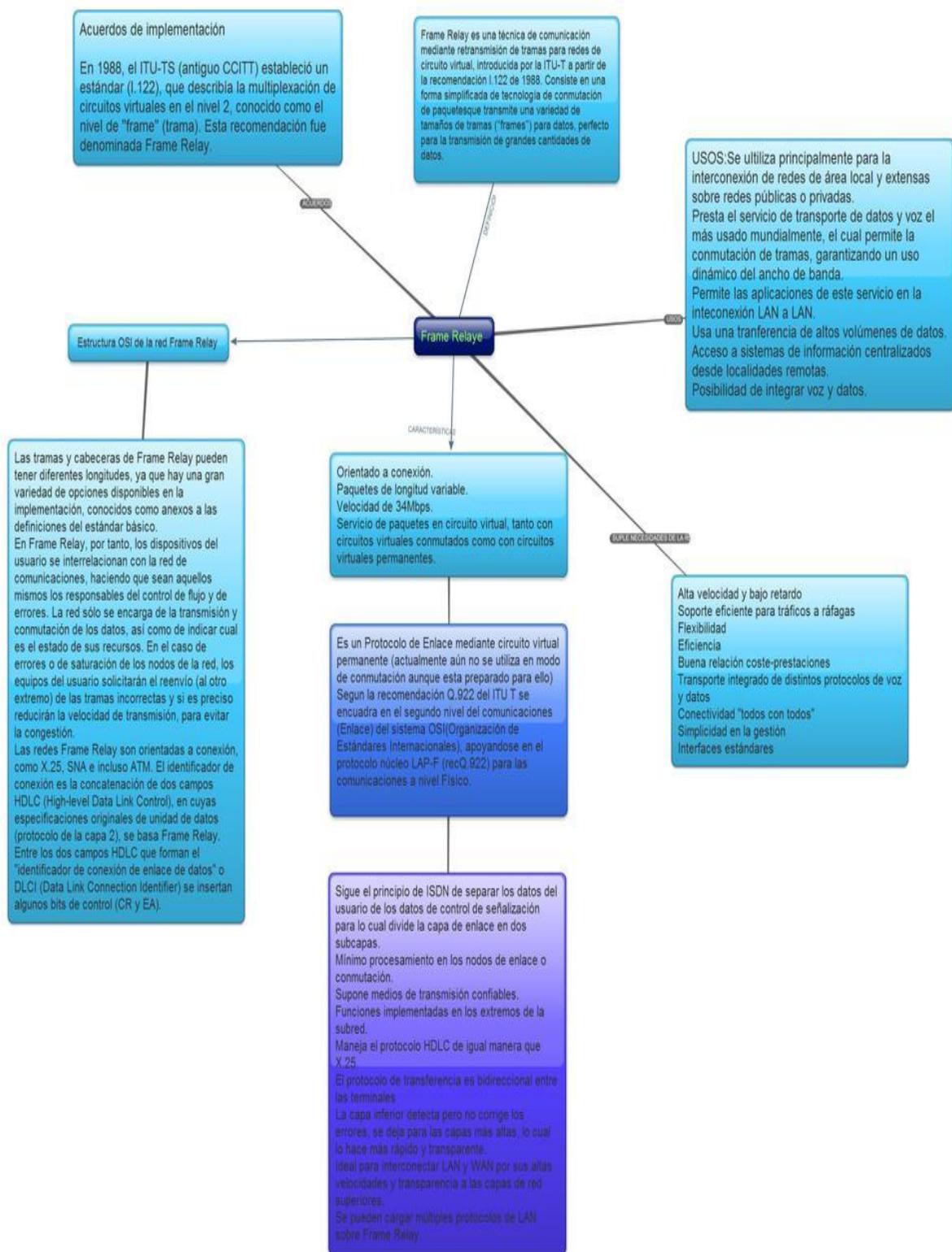
Topología de Frame Relay con Subinterfaces



Configuración de subinterfaces punto a punto en el R1

```
R1(config)# interface serial 0/0/1
R1(config-if)# encapsulation frame-relay
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/1.102 point-to-point
R1(config-subif)# ip address 10.1.1.1 255.255.255.252
R1(config-subif)# bandwidth 64
R1(config-subif)# frame-relay interface-dlci 102
R1(config-fr-dlci)# exit
R1(config-subif)# exit
R1(config)# interface serial 0/0/1.103 point-to-point
R1(config-subif)# ip address 10.1.1.5 255.255.255.252
R1(config-subif)# bandwidth 64
R1(config-subif)# frame-relay interface-dlci 103
R1(config-fr-dlci)#
```

Mapa mental



CAPITULO 4

Introducción a VPN

La seguridad es un motivo de preocupación cuando se utiliza Internet pública para realizar negocios. Las redes virtuales privadas (VPN) se utilizan para garantizar la seguridad de los datos a través de Internet. Una VPN se utiliza para crear un túnel privado a través de una red pública. Se puede proporcionar seguridad a los datos mediante el uso de cifrado en este túnel a través de Internet y con autenticación para proteger los datos contra el acceso no autorizado.

Aspectos básicos de las VPN

Las organizaciones necesitan redes seguras, confiables y rentables para interconectar varias redes, por ejemplo, para permitir que las sucursales y los proveedores se conecten a la red de la oficina central de una empresa. Además, con el aumento en la cantidad de trabajadores a distancia, hay una creciente necesidad de las empresas de contar con formas seguras, confiables y rentables para que los empleados que trabajan en oficinas pequeñas y oficinas domésticas (SOHO), y en otras ubicaciones remotas se conecten a los recursos en sitios empresariales.

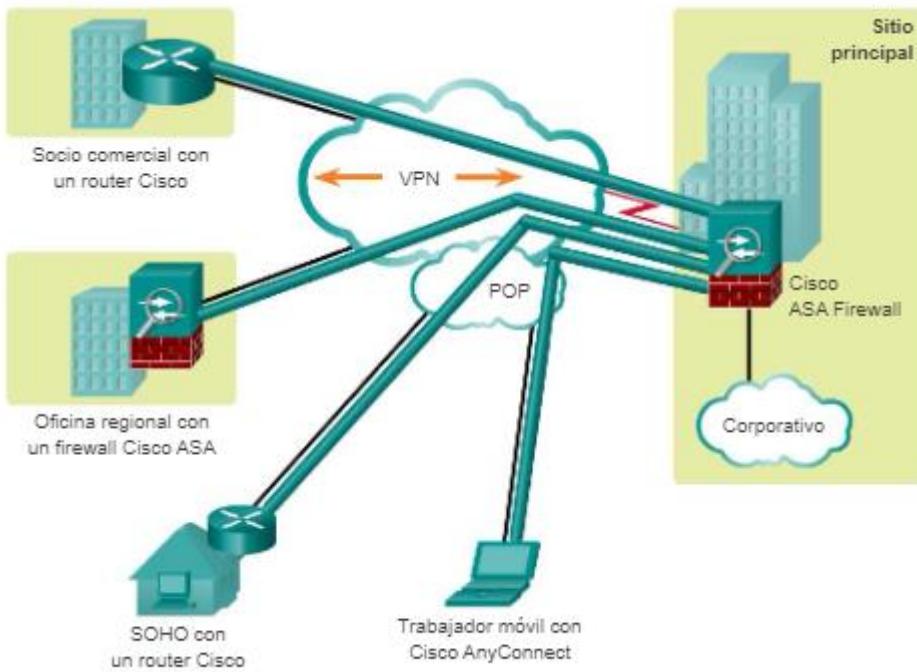
En la ilustración, se muestran las topologías que utilizan las redes modernas para conectar ubicaciones remotas. En algunos casos, las ubicaciones remotas se conectan solo a la oficina central, mientras que en otros casos, las ubicaciones remotas se conectan a sitios adicionales.

Las organizaciones utilizan las VPN para crear una conexión de red privada de extremo a extremo a través de redes externas como Internet o las extranets. El túnel elimina la barrera de distancia y permite que los usuarios remotos accedan a los recursos de red del sitio central. Una VPN es una red privada creada mediante tunneling a través de una red pública, generalmente Internet. Una VPN es un entorno de comunicaciones en el que el acceso se controla de forma estricta para permitir las conexiones de peers dentro de una comunidad de interés definida.

Las primeras VPN eran exclusivamente túneles IP que no incluían la autenticación o el cifrado de los datos. Por ejemplo, la encapsulación de routing genérico (GRE) es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolo de capa de red dentro de los túneles IP. Esto crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP.

En la actualidad, las redes privadas virtuales generalmente se refieren a la implementación segura de VPN con cifrado, como las VPN con IPsec.

Para implementar las VPN, se necesita un gateway VPN. El gateway VPN puede ser un router, un firewall o un dispositivo de seguridad adaptable (ASA) de Cisco. Un ASA es un dispositivo de firewall independiente que combina la funcionalidad de firewall, concentrador VPN y prevención de intrusiones en una imagen de software.

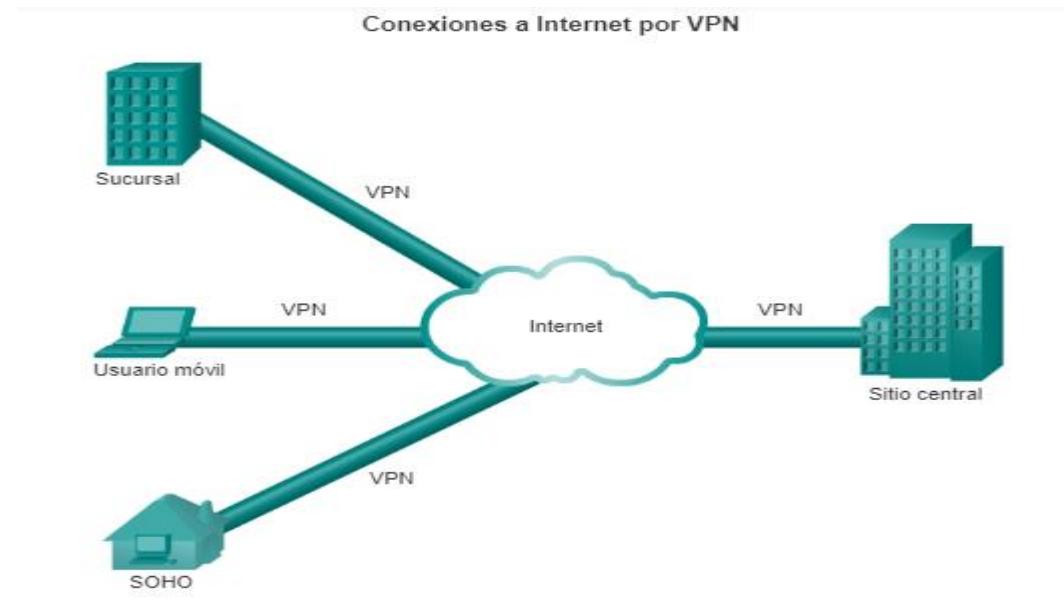


Beneficios de las VPN

Como se muestra en la ilustración, una VPN utiliza conexiones virtuales que se enrutan a través de Internet desde la red privada de una organización hasta el sitio remoto o el host del empleado. La información de una red privada se transporta de manera segura a través de la red pública para formar una red virtual.

Los beneficios de una VPN incluyen lo siguiente:

- Ahorro de costos: las VPN permiten que las organizaciones utilicen un transporte externo de Internet rentable para conectar oficinas remotas y usuarios remotos al sitio principal; por lo tanto, se eliminan los costosos enlaces WAN dedicados y los bancos de módem. Además, con la llegada de las tecnologías rentables de ancho de banda alto, como DSL, las organizaciones pueden utilizar VPN para reducir los costos de conectividad y, al mismo tiempo, aumentar el ancho de banda de la conexión remota.
- Escalabilidad: las VPN permiten que las organizaciones utilicen la infraestructura de Internet dentro de los ISP y los dispositivos, lo que facilita la tarea de agregar nuevos usuarios. Por lo tanto, las organizaciones pueden agregar una gran cantidad de capacidad sin necesidad de aumentar considerablemente la infraestructura.
- Compatibilidad con la tecnología de banda ancha: las redes VPN permiten que los trabajadores móviles y los empleados a distancia aprovechen la conectividad por banda ancha de alta velocidad, como DSL y cable, para acceder a las redes de sus organizaciones. La conectividad por banda ancha proporciona flexibilidad y eficacia. Las conexiones por banda ancha de alta velocidad también proporcionan una solución rentable para conectar oficinas remotas.
- Seguridad: las VPN pueden incluir mecanismos de seguridad que proporcionan el máximo nivel de seguridad mediante protocolos de cifrado y autenticación avanzados que protegen los datos contra el acceso no autorizado.



Tipos de VPNs

Existen dos tipos de redes VPN:

1. Sitio a sitio
2. Acceso remoto

VPN de sitio a sitio

Una VPN de sitio a sitio se crea cuando los dispositivos en ambos lados de la conexión VPN conocen la configuración de VPN con anticipación, como se muestra en la ilustración. La VPN permanece estática, y los hosts internos no saben que existe una VPN. En una VPN de sitio a sitio, los hosts terminales envían y reciben tráfico TCP/IP normal a través de un “gateway” VPN. El gateway VPN es el responsable de encapsular y cifrar el tráfico saliente para todo el tráfico de un sitio en particular. Después, el gateway VPN lo envía por un túnel VPN a través de Internet a un gateway VPN de peer en el sitio de destino. Al recibirlo, el gateway VPN de peer elimina los encabezados, descifra el contenido y transmite el paquete hacia el host de destino dentro de su red privada.

Una VPN de sitio a sitio es una extensión de una red WAN clásica. Las VPN de sitio a sitio conectan redes enteras entre sí, por ejemplo, pueden conectar la red de una sucursal a la red de la oficina central de una empresa. En el pasado, se requería una conexión de línea arrendada o de Frame Relay para conectar sitios, pero dado que en la actualidad la mayoría de las empresas tienen acceso a Internet, estas conexiones se pueden reemplazar por VPN de sitio a sitio.

VPN de sitio a sitio

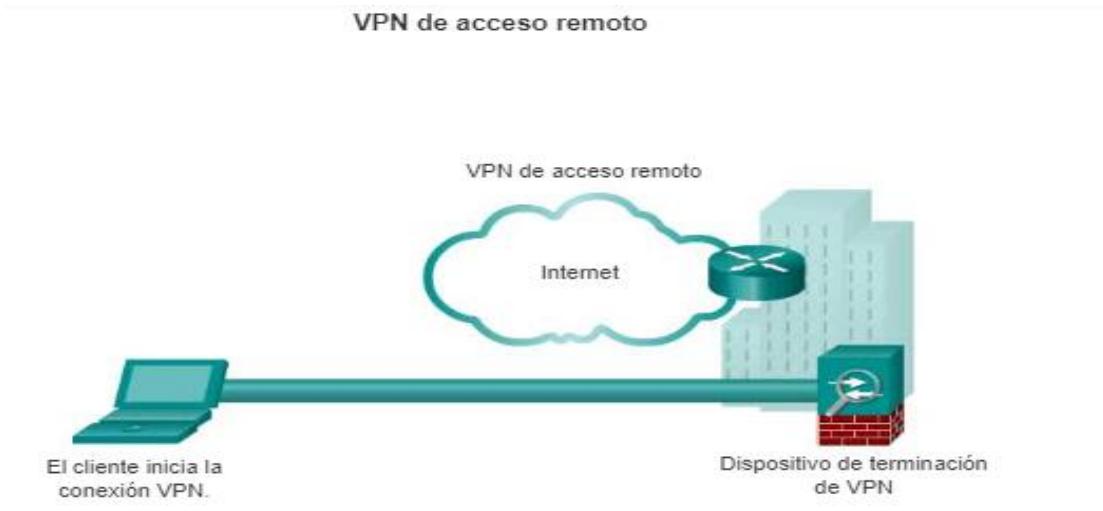


VPN de acceso remoto

Si se utiliza una VPN de sitio a sitio para conectar redes enteras, la VPN de acceso remoto admite las necesidades de los empleados a distancia, de los usuarios móviles y del tráfico de extranet de cliente a empresa. Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite el intercambio dinámico de información y se puede habilitar y deshabilitar. Las VPN de acceso remoto admiten una arquitectura cliente/servidor, en la que el cliente VPN (host remoto) obtiene acceso seguro a la red empresarial mediante un dispositivo del servidor VPN en el perímetro de la red.

Las VPN de acceso remoto se utilizan para conectar hosts individuales que deben acceder a la red de su empresa de forma segura a través de Internet. La conectividad a Internet que utilizan los trabajadores a distancia suele ser una conexión por banda ancha, DSL, cable o inalámbrica, como se indica en la ilustración.

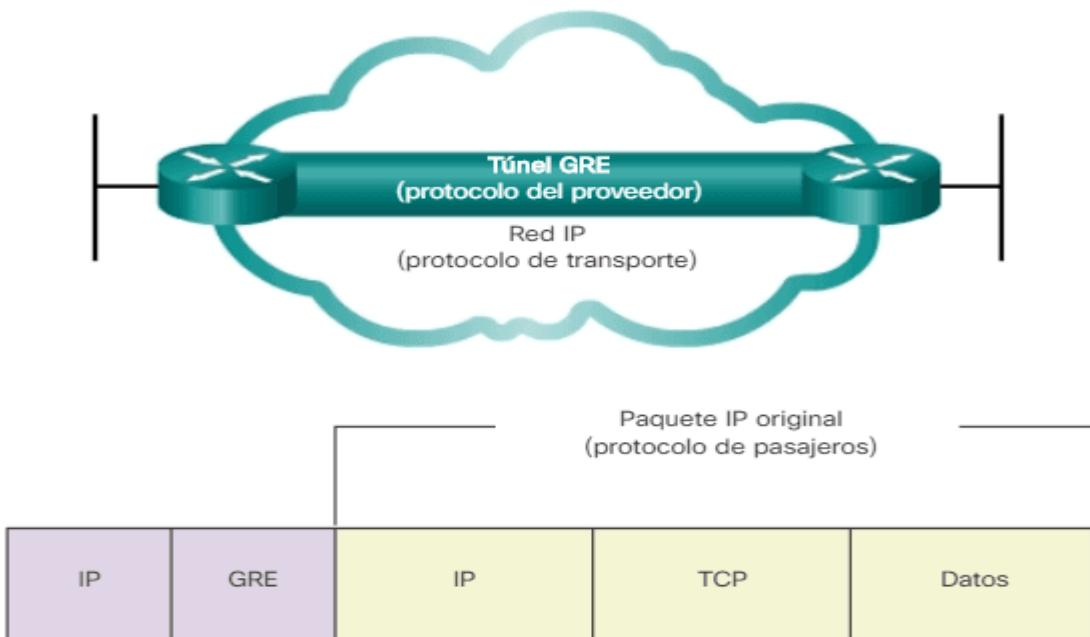
Es posible que se deba instalar un software de cliente VPN en la terminal del usuario móvil; por ejemplo, cada host puede tener el software Cisco AnyConnect Secure Mobility Client instalado. Cuando el host intenta enviar cualquier tipo de tráfico, el software Cisco AnyConnect VPN Client encapsula y cifra este tráfico. Después, los datos cifrados se envían por Internet al gateway VPN en el perímetro de la red de destino. Al recibirlas, el gateway VPN se comporta como lo hace para las VPN de sitio a sitio.



Qué es GRE

La encapsulación de routing genérico (GRE) es un ejemplo de un protocolo de tunneling de VPN de sitio a sitio básico y no seguro. GRE es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquete de protocolo dentro de túneles IP, lo que crea un enlace punto a punto virtual a los routers Cisco en puntos remotos a través de una internetwork IP.

GRE está diseñada para administrar el transporte del tráfico multiprotocolo y de multidifusión IP entre dos o más sitios, que probablemente solo tengan conectividad IP. Puede encapsular varios tipos de paquete de protocolo dentro de un túnel IP.



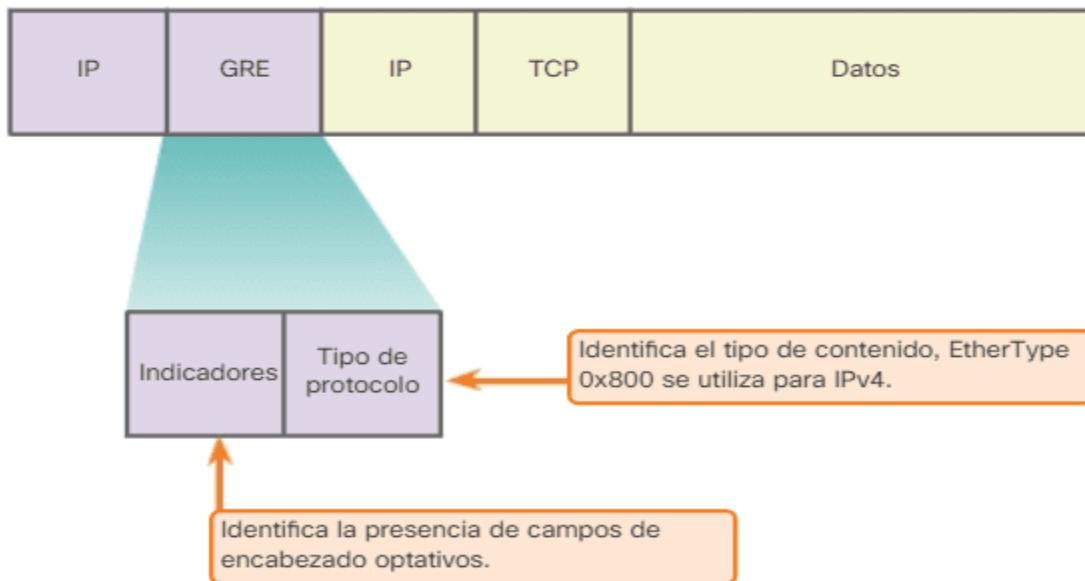
Encapsulación de enrutamiento genérico (GRE)

Como se muestra en la ilustración, una interfaz de túnel admite un encabezado para cada uno de los siguientes protocolos:

- Un protocolo encapsulado (o protocolo de pasajeros), como IPv4, IPv6, AppleTalk, DECnet o IPX
- Un protocolo de encapsulación (o portadora), como GRE
- Un protocolo de entrega de transporte, como IP, que es el protocolo que transporta al protocolo encapsulado

Características de GRE

El tunneling IP que utiliza GRE habilita la expansión de la red a través de un entorno de backbone de protocolo único. Esto se logra mediante la conexión de subredes multiprotocolo en un entorno de backbone de protocolo único.



Las características de GRE son las siguientes:

GRE se define como un estándar IETF (RFC 2784).

- En el encabezado IP externo, se utiliza el número 47 en el campo de protocolo para indicar que lo que sigue es un encabezado GRE.
- La encapsulación de GRE utiliza un campo de tipo de protocolo en el encabezado GRE para admitir la encapsulación de cualquier protocolo de capa 3 del modelo OSI. Los tipos de protocolo se definen en RFC 1700 como "EtherTypes".
- GRE en sí misma no tiene estado; de manera predeterminada, no incluye ningún mecanismo de control de flujo.
- GRE no incluye ningún mecanismo de seguridad sólido para proteger su contenido.
- El encabezado GRE, junto con el encabezado de tunneling IP que se indica en la ilustración, crea por lo menos 24 bytes de sobrecarga adicional para los paquetes que se envían por túnel.

Configuración de túneles GRE

GRE se utiliza para crear un túnel VPN entre dos sitios, como se muestra en la figura 1. Para implementar un túnel GRE, el administrador de red primero debe descubrir las direcciones IP de las terminales.



Para implementar un túnel GRE, el administrador de red primero debe descubrir las direcciones IP de las terminales. Después, se deben seguir cinco pasos para configurar un túnel GRE:

- *Paso 1. Cree una interfaz de túnel con el comando `interface tunnel number`.*
- *Paso 2. Especifique la dirección IP de origen del túnel.*
- *Paso 3. Especifique la dirección IP de destino del túnel.*
- *Paso 4. Configure una dirección IP para la interfaz de túnel.*
- *Paso 5. (Optativo) Especifique el modo de túnel GRE como modo de interfaz de túnel. El modo de túnel GRE es el modo predeterminado de interfaz de túnel para el software IOS de Cisco.*

Comandos de configuración de túneles GRE

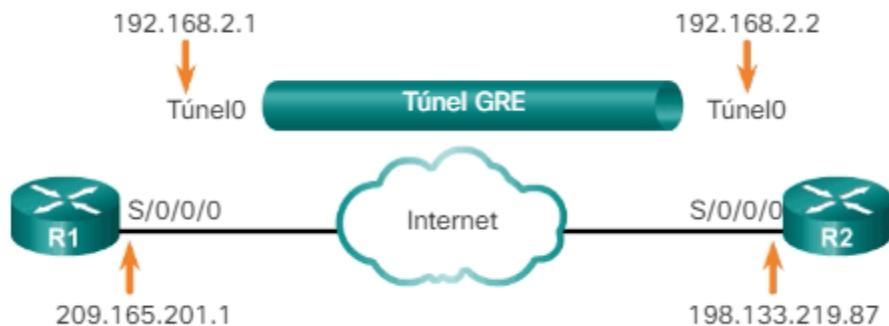


Imagen 4: Comandos de configuración de túneles GRE

Se detalla una configuración básica de túnel GRE para el router R1:

- `R1(config)# interface Tunnel0`
- `R1(config-if)# tunnel mode gre ip`
- `R1(config-if)# ip address 192.168.2.1 255.255.255.0`
- `R1(config-if)# tunnel source 209.165.201.1`
- `R1(config-if)# tunnel destination 198.133.219.87`
- `R1(config-if)# router ospf 1`
- `R1(config-router)# network 192.168.2.0 0.0.0.255 area 0`

La configuración del R2 refleja la configuración del R1:

- **R2(config)# interface Tunnel0**
- **R2(config-if)# tunnel mode gre ip**
- **R2(config-if)# ip address 192.168.2.2 255.255.255.0**
- **R2(config-if)# tunnel source 198.133.219.87**
- **R2(config-if)# tunnel destination 209.165.201.1**
- **R2(config-if)# router ospf 1**
- **R2(config-router)# network 192.168.2.0 0.0.0.255 area 0**

La configuración mínima requiere la especificación de las direcciones de origen y destino del túnel. También se debe configurar la subred IP para proporcionar conectividad IP a través del enlace de túnel.

Ambas interfaces de túnel tienen el origen del túnel establecido en la interfaz serial local S0/0/0 y el destino del túnel establecido en la interfaz serial S0/0/0 del router peer. La dirección IP se asigna a las interfaces de túnel en ambos routers. También se configuró OSPF para intercambiar rutas a través del túnel GRE.

Descripción de los comandos

Las descripciones de los comandos individuales de túnel GRE se muestran en la figura 4.

Tabla de Comandos de túnel GRE.	
Comando	Descripción
tunnel mode gre ip	Especifica que el modo de la interfaz de túnel es GRE por IP.
tunnel source <i>ip_address</i>	Especifica la dirección de origen del túnel.
tunnel destination <i>ip_address</i>	Especifica la dirección de destino del túnel.
ip address <i>ip_address mask</i>	Especifica la dirección IP de la interfaz de túnel.

Nota: cuando se configuran los túneles GRE, puede ser difícil recordar cuáles son las redes IP asociadas a las interfaces físicas y cuáles son las redes IP asociadas a las interfaces de túnel. Recuerde que antes de que se cree un túnel GRE, ya se configuraron las interfaces físicas.

Los comandos tunnel source y tunnel destination se refieren a las direcciones IP de las interfaces físicas configuradas previamente. El comando ip address en las interfaces de túnel se refiere a una red IP especialmente diseñada para los propósitos del túnel GRE.

Verificación del túnel GRE

Existen varios comandos que se pueden utilizar para controlar los túneles GRE y resolver los problemas relacionados. Para determinar si la interfaz de túnel está activa o inactiva, utilice el comando **show ip interface brief**.

```
R1# show ip interface brief | include Tunnel
```

Tunnel0	192.168.2.1	YES manual	up	up
---------	-------------	------------	----	----

Para verificar el estado de un túnel GRE, utilice el comando **show interface tunnel**.

```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 192.168.2.1/24
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 209.165.201.1, destination 209.165.201.2
Tunnel protocol/transport GRE/IP
<se omite el resultado>
```

Verificar que la interfaz de tunel esté activa

El protocolo de línea en una interfaz de túnel GRE permanece activo mientras haya una ruta al destino del túnel. Antes de implementar un túnel GRE, la conectividad IP ya debe estar operativa entre las direcciones IP de las interfaces físicas en extremos opuestos del túnel GRE potencial. El protocolo de transporte de túnel se muestra en el resultado.

Si también se configuró OSPF para intercambiar rutas a través del túnel GRE, verifique que se haya establecido una adyacencia OSPF a través de la interfaz de túnel con el comando **show ip ospf neighbor**, observe que la dirección de interconexión para el vecino OSPF está en la red IP creada para el túnel GRE.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
209.165.201.2	0	FULL/ -	00:00:37	192.168.2.2	Tunnel0

IPsec

Seguridad de protocolo de Internet

Las VPN con IPsec ofrecen conectividad flexible y escalable. Las conexiones de sitio a sitio pueden proporcionar una conexión remota segura, rápida y confiable. Con una VPN con IPsec, la información de una red privada se transporta de manera segura a través de una red pública. Esto forma una red virtual en lugar de usar una conexión dedicada de capa 2, como se muestra en la ilustración. Para que siga siendo privado, el tráfico se cifra a fin de mantener la confidencialidad de los datos.

IPsec es un estándar IETF que define la forma en que se puede configurar una VPN de manera segura mediante el protocolo de Internet.

IPsec es un marco de estándares abiertos que detalla las reglas para las comunicaciones seguras. IPsec no se limita a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de creación de claves. En realidad, IPsec depende de algoritmos existentes para implementar comunicaciones seguras. IPsec permite que se implementen nuevos y mejores algoritmos sin modificar los estándares existentes de IPsec.

IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes, también conocidos como "peers". IPsec protege una ruta entre un par de gateways, un par de hosts o un gateway y un host. Como resultado, IPsec puede proteger prácticamente todo el tráfico de una aplicación, dado que la protección se puede implementar desde la capa 4 hasta la capa 7.

Todas las implementaciones de IPsec tienen un encabezado de capa 3 de texto no cifrado, de modo que no hay problemas de routing. IPsec funciona en todos los protocolos de capa 2, como Ethernet, ATM o Frame Relay.

Las características de IPsec se pueden resumir de la siguiente manera:

- IPsec es un marco de estándares abiertos que no depende de algoritmos.
- IPsec proporciona confidencialidad e integridad de datos, y autenticación del origen.
- IPsec funciona en la capa de red, por lo que protege y autentica paquetes IP.

Seguridad de protocolo de Internet

Los servicios de seguridad IPsec proporcionan cuatro funciones fundamentales, las cuales se muestran en la ilustración:

- **Confidencialidad (cifrado):** en una implementación de VPN, los datos privados se transfieren a través de una red pública. Por este motivo, la confidencialidad de los datos es fundamental. Esto se puede lograr mediante el cifrado de los datos antes de transmitirlos a través de la red. Este es el proceso de tomar todos los datos que una computadora envía a otra y codificarlos de una manera que solo la otra computadora pueda decodificar. Si se intercepta la comunicación, el pirata informático no puede leer los datos. IPsec proporciona características de seguridad mejoradas, como algoritmos de cifrado seguros.
- **Integridad de datos:** el receptor puede verificar que los datos se hayan transmitido a través de Internet sin sufrir ningún tipo de modificaciones ni alteraciones. Si bien es importante que los datos a través de una red pública estén cifrados, también es importante verificar que no se hayan modificado cuando estaban en tránsito. IPsec cuenta con un mecanismo para asegurarse de que la

porción cifrada del paquete, o todo el encabezado y la porción de datos del paquete, no se haya modificado. IPsec asegura la integridad de los datos mediante checksums, que es una comprobación de redundancia simple. Si se detecta una alteración, el paquete se descarta.

- **Autenticación:** verifica la identidad del origen de los datos que se envían. Esto es necesario para la protección contra distintos ataques que dependen de la suplantación de identidad del emisor. La autenticación asegura que se cree una conexión con el compañero de comunicación deseado. El receptor puede autenticar el origen del paquete mediante la certificación del origen de la información. IPsec utiliza el intercambio de claves de Internet (IKE) para autenticar a los usuarios y dispositivos que pueden llevar a cabo la comunicación de manera independiente. IKE utiliza varios tipos de autenticación, por ejemplo, nombre de usuario y contraseña, contraseña por única vez, biometría, clave previamente compartida (PSK) y certificados digitales.
- **Protección antirreproducción:** es la capacidad de detectar y rechazar los paquetes reproducidos, y ayuda a prevenir la suplantación de identidad. La protección antirreproducción verifica que cada paquete sea único y no esté duplicado. Los paquetes IPsec se protegen mediante la comparación del número de secuencia de los paquetes recibidos con una ventana deslizante en el host de destino o el gateway de seguridad. Se considera que un paquete que tiene un número de secuencia anterior a la ventana deslizante tiene un retraso o está duplicado. Los paquetes duplicados y con retraso se descartan.

El acrónimo CIA se suele utilizar para ayudar a recordar las iniciales de estas tres funciones: confidencialidad, integridad y autenticación

Estructura IPsec

Confidencialidad

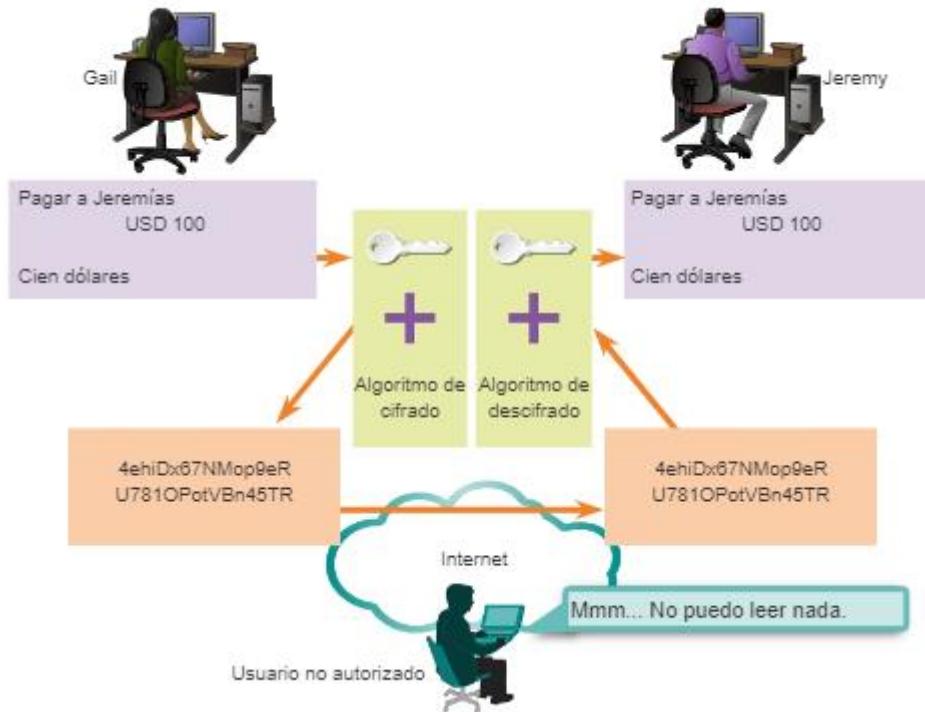
El tráfico VPN se mantiene confidencial con el cifrado. Los datos de texto no cifrado que se transportan a través de Internet pueden interceptarse y leerse. Cifre la fecha para que se mantenga privada. El cifrado digital de los datos hace que estos sean ilegibles hasta que el receptor autorizado los descifre.

Para que la comunicación cifrada funcione, el emisor y el receptor deben conocer las reglas que se utilizan para transformar el mensaje original a su forma cifrada. Las reglas se basan en algoritmos y claves asociadas. En el contexto del cifrado, un algoritmo es una secuencia matemática de pasos que combina un mensaje, texto, dígitos o las tres cosas con una cadena de dígitos denominada “clave”. El resultado es una cadena de cifrado ilegible. El algoritmo de cifrado también especifica cómo se descifra un mensaje cifrado. El descifrado es extremadamente difícil o imposible sin la clave correcta.

En la ilustración, Gail desea enviar una transferencia electrónica de fondos (EFT) a Jeremías a través de Internet. En el extremo local, el documento se combina con una clave y se procesa con un algoritmo de cifrado. El resultado es un texto cifrado. El texto cifrado se envía a través de Internet. En el extremo remoto, el mensaje se vuelve a combinar con una clave y se devuelve a través del algoritmo de cifrado. El resultado es el documento financiero original.

La confidencialidad se logra con el cifrado del tráfico mientras viaja por una VPN. El grado de seguridad depende de la longitud de la clave del algoritmo de cifrado y la sofisticación del algoritmo. Si un pirata informático intenta descifrar la clave mediante un ataque por fuerza bruta, la cantidad de intentos posibles es una función de la longitud de la clave. El tiempo para procesar todas las posibilidades es una función de la potencia de la computadora del dispositivo atacante. Cuanto más corta sea la clave, más fácil será descifrarla. Por ejemplo, una computadora relativamente sofisticada puede tardar aproximadamente un año para descifrar una clave de 64 bits, mientras que descifrar una clave de 128 bits puede llevarle de 10 a 19 años.

Confidencialidad con cifrado



El grado de seguridad depende de la longitud de la clave del algoritmo de cifrado. Cuanto más larga es la clave, se torna más difícil descifrarla. Sin embargo, una clave más larga requiere más recursos de procesador para cifrar y descifrar datos.

DES y 3DES ya no se consideran seguros; por lo tanto, se recomienda utilizar AES para el cifrado de IPSec. La mejor seguridad para el cifrado de IPSec de las VPN entre dispositivos de Cisco la proporciona la opción de 256 bits de AES. Además, dado que se descifraron claves de Rivest, Shamir y Adleman (RSA) de 512 bits y 768 bits, Cisco recomienda utilizar claves de 2048 bits con la opción RSA si se la utilizó durante la fase de autenticación de IKE.

Cifrado simétrico

Los algoritmos de cifrado, como AES, requieren una clave secreta compartida para el cifrado y el descifrado. Cada uno de los dos dispositivos de red debe conocer la clave para decodificar la información. Con el cifrado de clave simétrica, también denominado "cifrado de la clave secreta", cada dispositivo cifra la información antes de enviarla a través de la red al otro dispositivo. El cifrado de clave simétrica requiere saber qué dispositivos se comunican entre sí para poder configurar la misma clave en cada dispositivo, como se ilustra en la figura 1.

Por ejemplo, un emisor crea un mensaje cifrado en el que cada letra se reemplaza por otra letra que está dos lugares más adelante en el abecedario: A se convierte en C, B se convierte en D y así sucesivamente. En este caso, la palabra SECRET se convierte en UGETGV. El emisor ya le dijo al destinatario que la clave secreta se corre dos letras. Cuando el destinatario recibe el mensaje UGETGV, la computadora del destinatario decodifica el mensaje corriendo dos letras hacia atrás y calcula la palabra SECRET. Cualquier

persona que ve el mensaje solo ve el mensaje cifrado, que parece no tener sentido, a menos que la persona conozca la clave secreta.

A continuación, se muestra una sinopsis para los algoritmos simétricos:

- Utilizan criptografía de clave simétrica.
- El cifrado y el descifrado utilizan la misma clave.
- Por lo general, se utilizan para cifrar el contenido del mensaje.
- Ejemplos: DES, 3DES y AES

¿Cómo es que los dispositivos de cifrado y descifrado tienen una clave secreta compartida? Para enviar las claves secretas compartidas a los administradores de los dispositivos, se podría utilizar el correo electrónico, el servicio de mensajería común o de entrega urgente. Otro método más seguro es el cifrado asimétrico.



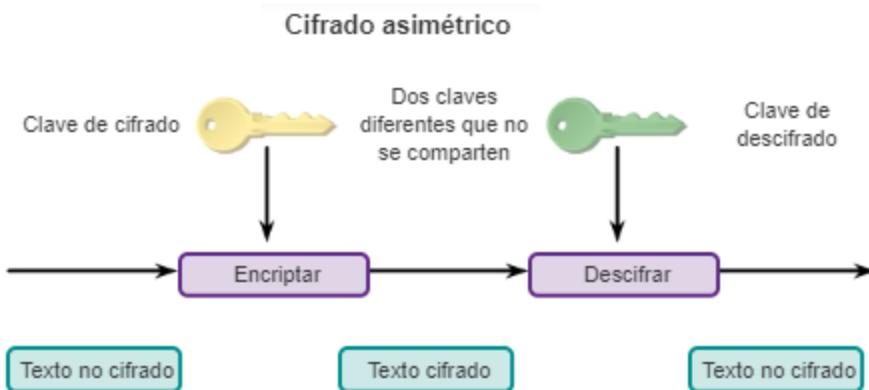
Cifrado asimétrico

El cifrado asimétrico utiliza claves diferentes para el cifrado y el descifrado. Aunque conozca una de las claves, un pirata informático no puede deducir la segunda clave y decodificar la información. Una clave cifra el mensaje, mientras que una segunda clave descifra el mensaje, como se ilustra en la figura 2. No es posible cifrar y descifrar con la misma clave.

El cifrado de clave pública es una variante del cifrado asimétrico que utiliza una combinación de una clave privada y una pública. El destinatario brinda una clave pública a cualquier emisor con el que desee comunicarse. El emisor utiliza una clave privada que se combina con la clave pública del destinatario para cifrar el mensaje. Además, el emisor debe compartir su clave pública con el destinatario. Para descifrar un mensaje, el destinatario utiliza la clave pública del emisor con su propia clave privada.

A continuación, se muestra una sinopsis para los algoritmos asimétricos:

- Utilizan criptografía de clave pública.
- El cifrado y el descifrado utilizan claves diferentes.
- Por lo general, se usan en la certificación digital y la administración de claves.
- Ejemplos: RSA



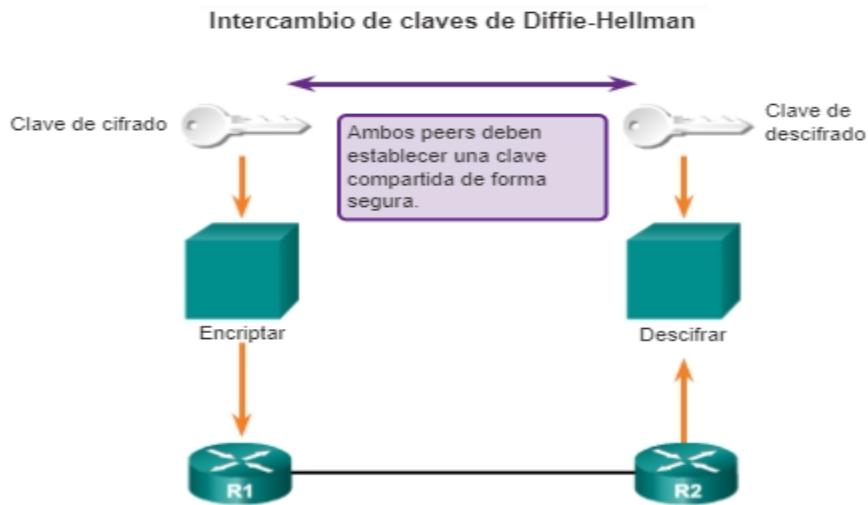
Integridad de datos

Diffie-Hellman (DH) no es un mecanismo de cifrado y no se suele utilizar para cifrar datos. En cambio, es un método para intercambiar con seguridad las claves que cifran datos. Los algoritmos (DH) permiten que dos partes establezcan la clave secreta compartida que usan el cifrado y los algoritmos de hash.

DH, presentado por Whitfield Diffie y Martin Hellman en 1976, fue el primer sistema en utilizar la clave pública o las claves criptográficas asimétricas. En la actualidad, DH forma parte del estándar IPsec. Además, un protocolo denominado OAKLEY utiliza un algoritmo DH. OAKLEY es un protocolo utilizado por el protocolo IKE, que forma parte del marco general denominado “protocolo de administración de claves y de asociación de seguridad de Internet”.

Los algoritmos de cifrado, como DES, 3DES y AES, así como los algoritmos de hash MD5 y SHA-1, requieren una clave secreta compartida simétrica para realizar el cifrado y el descifrado. ¿Cómo obtienen la clave secreta compartida los dispositivos de cifrado y descifrado? El método más sencillo de intercambio de claves es un método de intercambio de clave pública entre dispositivos de cifrado y descifrado.

El algoritmo DH especifica un método de intercambio de clave pública que proporciona una manera para que dos peers establezcan una clave secreta compartida que solo ellos conozcan, aunque se comuniquen a través de un canal inseguro. Como todos los algoritmos criptográficos, el intercambio de claves DH se basa en una secuencia matemática de pasos.



Los algoritmos de hash manejan la integridad y la autenticación del tráfico VPN. Los hashes proporcionan integridad y autenticación de datos al asegurar que las personas no autorizadas no alteren los mensajes transmitidos. Un hash, también denominado “síntesis del mensaje”, es un número que se genera a partir de una cadena de texto. El hash es más corto que el texto en sí. Se genera mediante el uso de una fórmula, de tal manera que es muy poco probable que otro texto produzca el mismo valor de hash.

El emisor original genera un hash del mensaje y lo envía con el mensaje propiamente dicho. El destinatario analiza el mensaje y el hash, produce otro hash a partir del mensaje recibido y compara ambos hashes. Si son iguales, el destinatario puede estar lo suficientemente seguro de la integridad del mensaje original.

En la ilustración, Gail le envió a Alex un EFT de USD 100. Jeremías interceptó y alteró este EFT para mostrarse como el destinatario y que la cantidad sea USD 1000. En este caso, si se utilizara un algoritmo de integridad de datos, los hashes no coincidirían, y la transacción no sería válida.

Los datos VPN se transportan por Internet pública. Como se muestra, existe la posibilidad de que se intercepten y se modifiquen estos datos. Para protegerlos contra esta amenaza, los hosts pueden agregar un hash al mensaje. Si el hash transmitido coincide con el hash recibido, se preservó la integridad del mensaje. Sin embargo, si no hay una coincidencia, el mensaje se alteró.

Las VPN utilizan un código de autenticación de mensajes para verificar la integridad y la autenticidad de un mensaje, sin utilizar ningún mecanismo adicional.

El código de autenticación de mensajes basado en hash (HMAC) es un mecanismo para la autenticación de mensajes mediante funciones de hash. Un HMAC con clave es un algoritmo de integridad de datos que garantiza la integridad de un mensaje. Un HMAC tiene dos parámetros: una entrada de mensaje y una clave secreta que solo conocen el autor del mensaje y los destinatarios previstos. El emisor del mensaje utiliza una función HMAC para producir un valor (el código de autenticación de mensajes) que se forma mediante la compresión de la clave secreta y la entrada de mensaje. El código de autenticación de mensajes se envía junto con el mensaje. El receptor calcula el código de autenticación de mensajes en el mensaje recibido con la misma clave y la misma función HMAC que utilizó el emisor. A continuación, el receptor compara el resultado que se calculó con el código de autenticación de mensajes que se recibió. Si los dos valores coinciden, el mensaje se recibió correctamente y el receptor se asegura de que el emisor

forma parte de la comunidad de usuarios que comparten la clave. La fortaleza criptográfica del HMAC depende de la fortaleza criptográfica de la función de hash subyacente, del tamaño y la calidad de la clave, y del tamaño de la longitud del resultado del hash en bits.

Hay dos algoritmos HMAC comunes:

MD5: utiliza una clave secreta compartida de 128 bits. El mensaje de longitud variable y la clave secreta compartida de 128 bits se combinan y se procesan con el algoritmo de hash HMAC-MD5. El resultado es un hash de 128 bit. El hash se adjunta al mensaje original y se envía al extremo remoto.

SHA: SHA-1 utiliza una clave secreta de 160 bits. El mensaje de longitud variable y la clave secreta compartida de 160 bits se combinan y se procesan con el algoritmo de hash HMAC-SHA1. El resultado es un hash de 160 bits. El hash se adjunta al mensaje original y se envía al extremo remoto.

Nota: el IOS de Cisco también admite implementaciones de SHA de 256 bits, 384 bits y 512 bits.

Algoritmos de hash



Autenticación

Las VPN con IPsec admiten la autenticación. Al realizar negocios a larga distancia, es necesario saber quién está del otro lado del teléfono, del correo electrónico o del fax. Lo mismo sucede con las redes VPN. El dispositivo en el otro extremo del túnel VPN se debe autenticar para que la ruta de comunicación se considere segura, como se indica en la ilustración. Existen dos métodos de autenticación de peers:

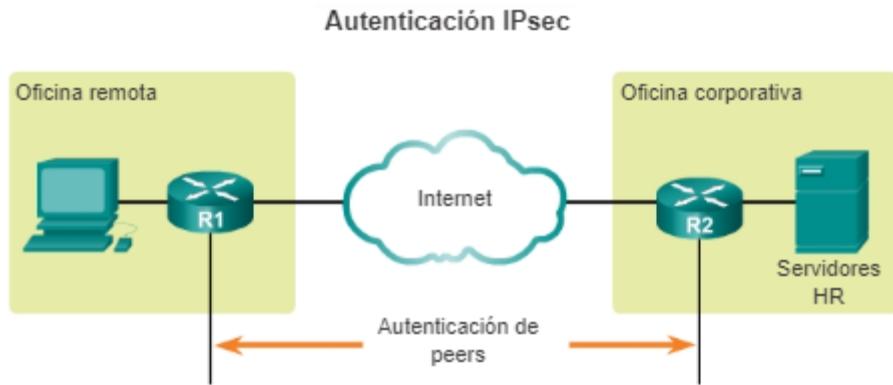
PSK: es una clave secreta que se comparte entre las dos partes que utilizan un canal seguro antes de que se necesite utilizarla. Las claves previamente compartidas (PSK) utilizan algoritmos criptográficos de clave simétrica. Se introduce una PSK en cada peer de forma manual y se la utiliza para autenticar el peer. En cada extremo, la PSK se combina con otra información para formar la clave de autenticación.

Firmas RSA: se intercambian certificados digitales para autenticar los peers. El dispositivo local deriva un hash y lo cifra con su clave privada. El hash cifrado, o la firma digital, se vincula al mensaje y se reenvía hacia el extremo remoto. En el extremo remoto, se descifra el hash cifrado con la clave pública del extremo local. Si el hash descifrado coincide con el hash recalculado, la firma es genuina.

IPsec utiliza RSA (sistema criptográfico de claves públicas) para la autenticación en el contexto de IKE. El método de firmas RSA utiliza una configuración de firma digital en la que cada dispositivo firma un conjunto de datos de forma digital y lo envía a la otra parte. Las firmas RSA usan una entidad de

certificación (CA) para generar un certificado digital de identidad exclusiva que se asigna a cada peer para la autenticación. El certificado digital de identidad tiene una función similar a la de una PSK, pero proporciona una seguridad mucho más sólida. Las personas que originan una sesión IKE y que responden a ella con firmas RSA envían su propio valor de ID, su certificado digital de identidad y un valor de firma RSA que consta de una serie de valores IKE, cifrados con el método de cifrado IKE negociado (como AES).

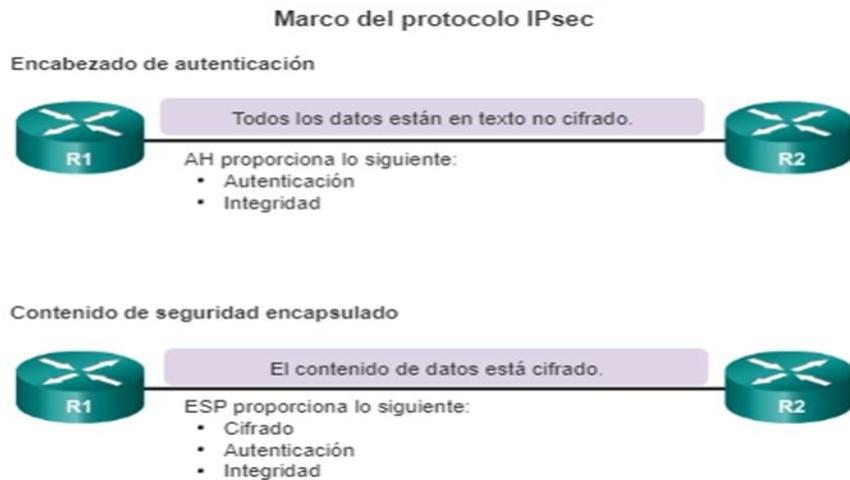
El algoritmo de firma digital (DSA) es otra opción para la autenticación.



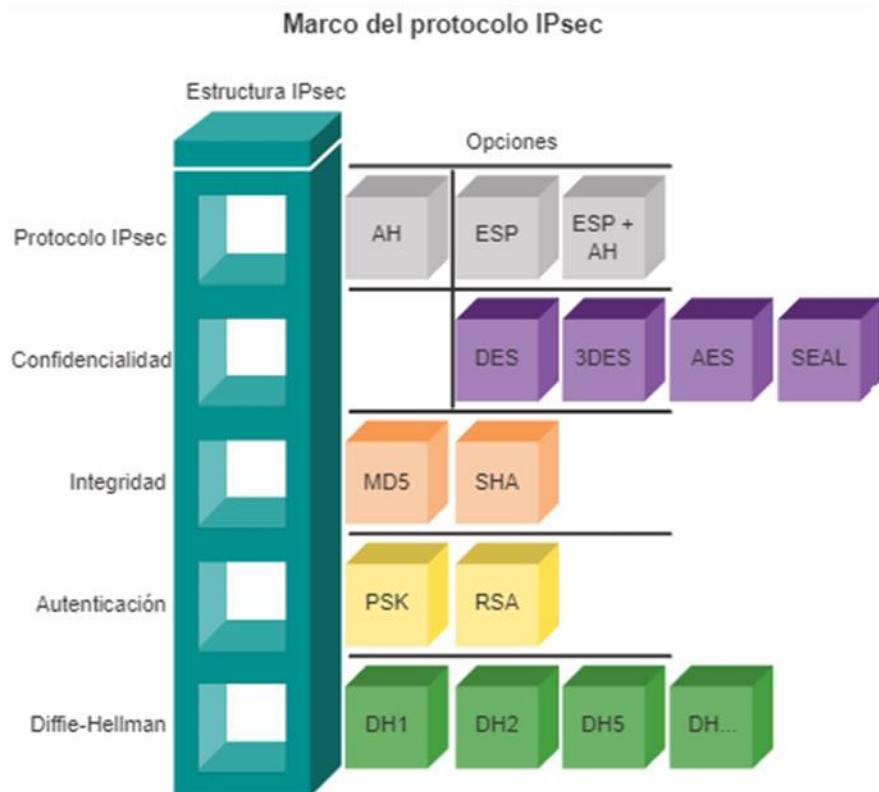
Como se mencionó anteriormente, el marco del protocolo IPSec describe la mensajería para proteger las comunicaciones, pero depende de los algoritmos existentes.

En la figura 1, se describen dos protocolos IPSec principales:

- **Encabezado de autenticación (AH):** AH es el protocolo que se debe utilizar cuando no se requiere o no se permite la confidencialidad. Proporciona la autenticación y la integridad de datos para los paquetes IP que se transmiten entre dos sistemas. Sin embargo, AH no proporciona la confidencialidad (el cifrado) de datos de los paquetes. Todo el texto se transporta como texto no cifrado. Cuando se utiliza solo, el protocolo AH proporciona una protección poco eficaz.
- **Contenido de seguridad encapsulado (ESP):** es un protocolo de seguridad que proporciona confidencialidad y autenticación mediante el cifrado del paquete IP. El cifrado de paquetes IP oculta los datos y las identidades del origen y el destino. ESP autentica el paquete IP y el encabezado ESP internos. La autenticación proporciona la autenticación del origen de los datos y la integridad de los datos. Si bien el cifrado y la autenticación son optativos en ESP, se debe seleccionar, como mínimo, uno de ellos.



En la figura 2, se muestran los componentes de la configuración de IPsec. Se deben seleccionar cuatro componentes básicos del marco de IPsec.



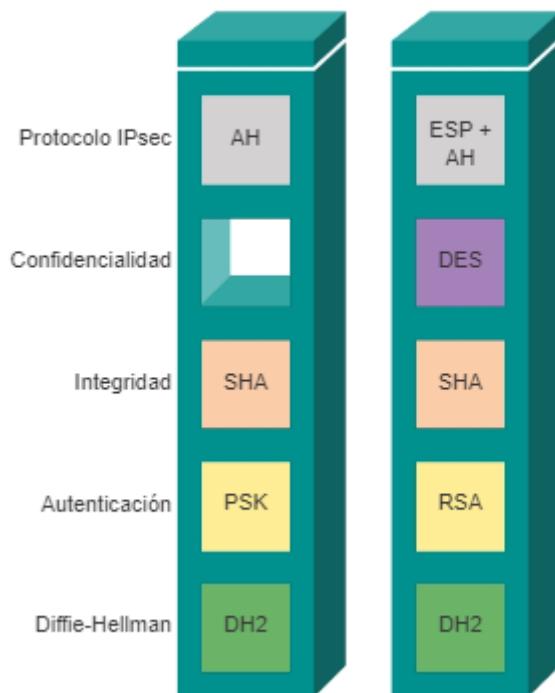
- **Protocolo del marco de IPsec:** al configurar un gateway IPsec para proporcionar servicios de seguridad, se debe seleccionar un protocolo IPsec. Las opciones son una combinación de ESP y AH. En realidad, las opciones de ESP o ESP+AH casi siempre se seleccionan porque AH en sí mismo no proporciona el cifrado, como se muestra en la figura 3.
- **Confidencialidad (si se implementa IPsec con ESP):** el algoritmo de cifrado elegido se debe ajustar al nivel deseado de seguridad (DES, 3DES o AES). Se recomienda AES, ya que AES-GCM proporciona la mayor seguridad.

- **Integridad:** garantiza que el contenido no se haya alterado en tránsito. Se implementa mediante el uso de algoritmos de hash. Entre las opciones se incluye MD5 y SHA.
- **Autenticación:** representa la forma en que se autentican los dispositivos en cualquiera de los extremos del túnel VPN. Los dos métodos son PSK o RSA.
- **Grupo de algoritmos DH:** representa la forma en que se establece una clave secreta compartida entre los peers. Existen varias opciones, pero DH24 proporciona la mayor seguridad.

La combinación de estos componentes es la que proporciona las opciones de confidencialidad, integridad y autenticación para las VPN con IPsec.

Nota: en esta sección, se presentó IPsec para proporcionar una comprensión de cómo IPsec protege los túneles VPN. La configuración de VPN con IPsec excede el ámbito de este curso.

Implementación de IPsec



Tipos de VPN de acceso remoto

Las VPN se convirtieron en la solución lógica para la conectividad de acceso remoto por muchos motivos. Las VPN proporcionan comunicaciones seguras con derechos de acceso hechos a la medida de los usuarios individuales, como empleados, contratistas y socios. También aumentan la productividad mediante la extensión de la red y las aplicaciones empresariales de forma segura, a la vez que reducen los costos de comunicación y aumentan la flexibilidad.

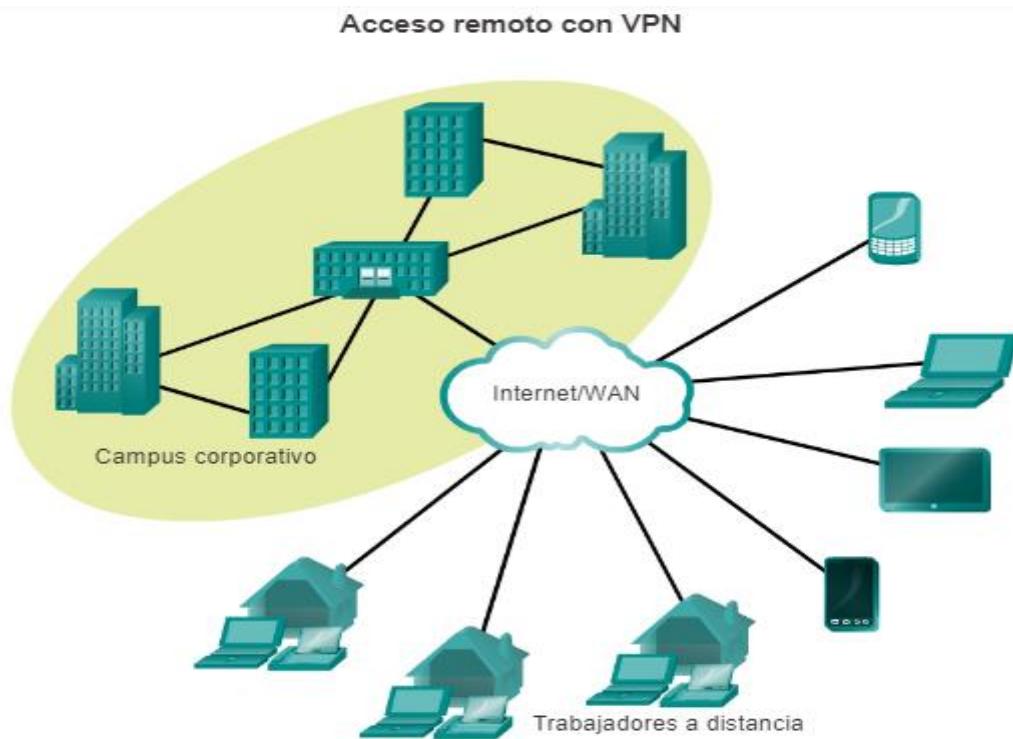
Básicamente, con la tecnología VPN, los empleados pueden llevar la oficina con ellos, incluido el acceso al correo electrónico y las aplicaciones de red. Las VPN también permiten que los contratistas y socios tengan acceso limitado a los servidores, a las páginas web o a los archivos específicos requeridos. Este acceso de red les permite contribuir a la productividad de la empresa sin comprometer la seguridad de la red.

Existen dos métodos principales para implementar VPN de acceso remoto:

- Capa de sockets seguros (SSL)
- Seguridad IP (IPsec)

El tipo de método VPN implementado se basa en los requisitos de acceso de los usuarios y en los procesos de TI de la organización.

Tanto la tecnología de VPN con SSL como la de VPN con IPsec ofrecen acceso a prácticamente cualquier aplicación o recurso de red. Las VPN con SSL ofrecen características como una fácil conectividad desde las computadoras de escritorio que no administra la empresa, un escaso o nulo mantenimiento del software de escritorio y portales web personalizados por el usuario al iniciar sesión.



VPN de acceso remoto con IPsec

Tanto la tecnología de VPN con SSL como la de IPsec ofrecen acceso a prácticamente cualquier aplicación o recurso de red, como se muestra en la ilustración. Las VPN con SSL ofrecen características como una fácil conectividad desde las computadoras de escritorio que no administra la empresa, un escaso o nulo mantenimiento del software de escritorio y portales web personalizados por el usuario al iniciar sesión.

IPsec supera a SSL en muchas formas importantes:

- La cantidad de aplicaciones que admite
- La solidez del cifrado
- La solidez de la autenticación
- La seguridad general

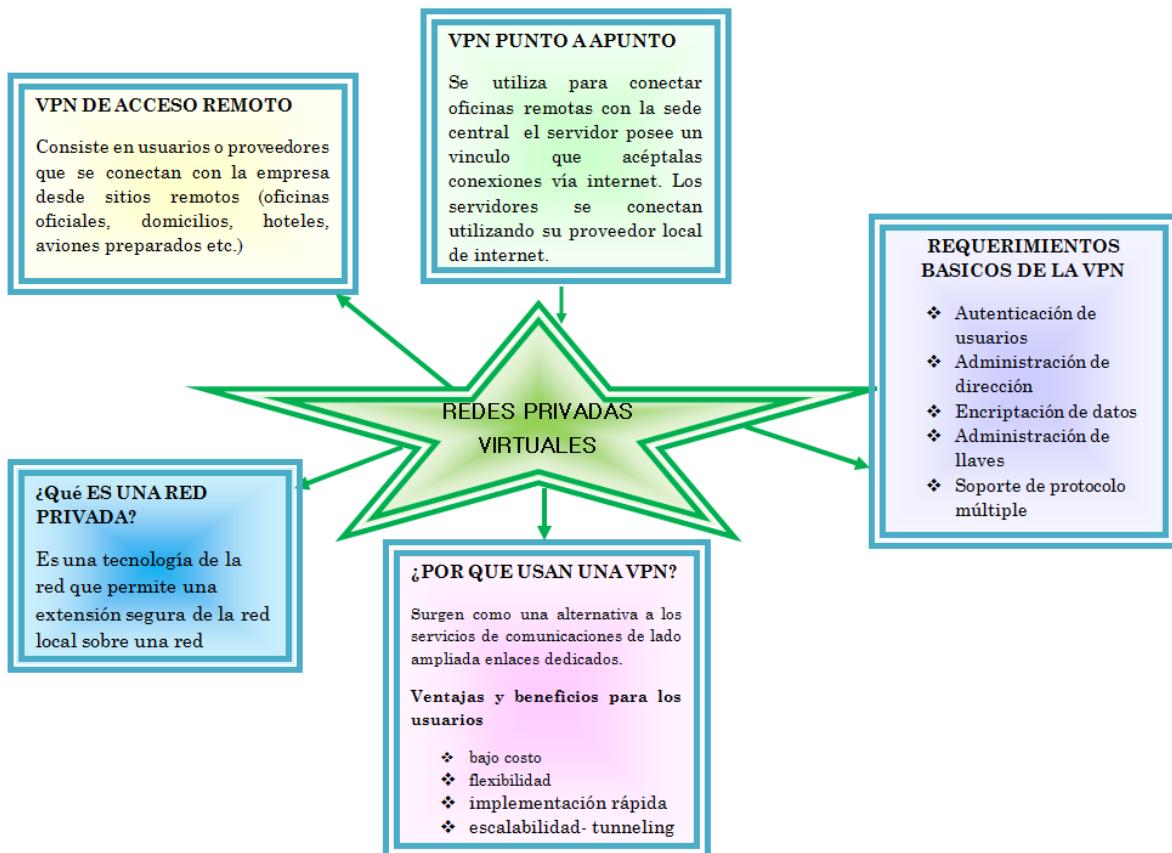
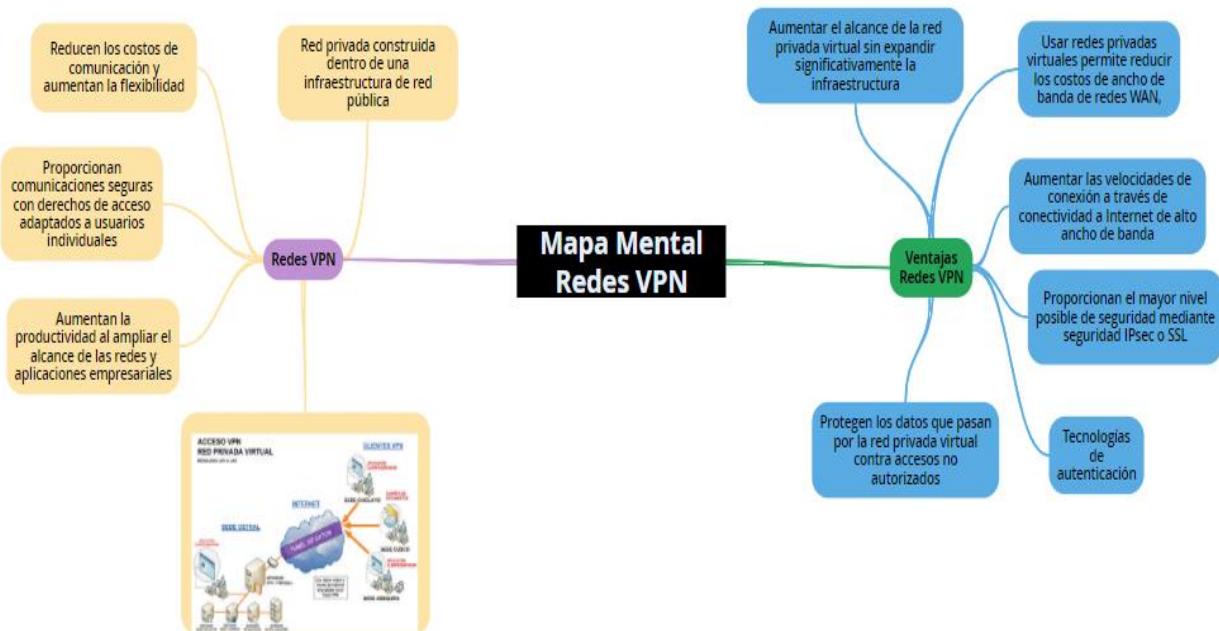
Cuando la seguridad representa un problema, IPsec es la mejor opción. Si el soporte y la facilidad de implementación son los principales problemas, considere utilizar SSL.

IPsec y las VPN con SSL se complementan porque resuelven diferentes problemas. Según las necesidades, una organización puede implementar una o ambas. Este enfoque complementario permite que un único dispositivo, como un router ISR o un dispositivo de firewall ASA, puedan satisfacer todos los requisitos de los usuarios de acceso remoto. Si bien muchas soluciones ofrecen IPsec o SSL, las soluciones de VPN de acceso remoto de Cisco ofrecen ambas tecnologías integradas en una única plataforma con administración unificada. Si se ofrece tanto la tecnología IPsec como SSL, las organizaciones pueden personalizar su VPN de acceso remoto sin ningún hardware adicional ni complejidad de administración.

Comparación de IPsec y SSL

	SSL	IPsec
Aplicaciones	Aplicaciones habilitadas para Web, uso compartido de archivos, correo electrónico	Todas las aplicaciones basadas en IP
Cifrado	Moderado a seguro Longitudes de clave de 40 bits a 256 bits	Seguro Longitudes de clave de 56 bits a 256 bits
Autenticación	Moderada Autenticación unidireccional o bidireccional	Segura Autenticación bidireccional mediante secretos compartidos o certificados digitales
Complejidad de conexión	Baja Solo se requiere un navegador web.	Media Puede resultar difícil para usuarios sin conocimientos técnicos.
Opciones de conexión	Cualquier dispositivo se puede conectar.	Solo se pueden conectar dispositivos específicos con una configuración específica.

Mapa Conceptual



IPsec

IPsec es un marco de estándares abiertos que detalla las reglas para las comunicaciones seguras.

Servicios

- Confidencialidad**, Cifrado de los datos antes de transmitirlos a través de la red.
- Integridad de datos**, IPsec cuenta con un mecanismo para asegurarse de que el paquete no se haya modificado.
- Autenticación**, IPsec utiliza el intercambio de claves de Internet (IKE) para tener una comunicación de manera independiente.
- Protección antireproducción**, Los paquetes IPsec se protegen mediante la comparación del número de secuencia.

Características

- IPsec es un marco de estándares abiertos que no depende de algoritmos.
- IPsec proporciona confidencialidad e integridad de datos, y autenticación del origen.
- IPsec funciona en la capa de red, por lo que protege y autentica paquetes IP.

TÚNELES GRE

Protocolo de tunneling desarrollado por Cisco que puede encapsular varios tipos de paquete de protocolo dentro de túneles IP.

Funcionamiento

GRE crea un enlace virtual punto a puntos a los routers Cisco en puntos remotos a través de una internetwork IP. Diseñada para administrar el transporte del tráfico multiprotocolo y de multidifusión IP.

Características

- Se define como un estándar RFC 2784.
- En el encabezado IP utiliza el número 47 para indicar que es GRE.
- Admite la encapsulación de cualquier protocolo de capa 3 del modelo OSI.
- No incluye ningún mecanismo de control de flujo.
- No incluye un mecanismo de seguridad.
- Crea por los menos 24 bytes de sobrecarga adicional para los paquetes que se envían por túnel.

Configuración

Crear una interfaz de túnel con el comando **interface tunnel number**. Especificar la dirección IP de origen del túnel. Especificar la dirección IP de destino del túnel. Configurar una dirección IP para la interfaz del túnel. (Opcional) Especificar el modo de túnel GRE como modo de interfaz de túnel.

CAPITULO 5

Protocolo BGP

Border Gateway Protocol (BGP) es el protocolo de enrutamiento utilizado en internet por los ISPs para interconectar distintos sistemas autónomos y sus redes. Su objetivo es proveer un enrutamiento entre sistemas autónomos libre de bucles. Soporta VLSM y CIDR, lo cual ayuda en gran medida a reducir el tamaño de grandes tablas de enrutamiento. BGP no requiere una arquitectura jerárquica y posee la capacidad de soportar múltiples conexiones, acompañándolas con excelentes políticas de control de rutas.

Existen protocolos vector distancia como RIP y estado enlace como OSPF, a BGP se le conoce como un protocolo vector distancia mejorado, o también como protocolo **Vector Path**, siendo su métrica **Path Vectors** (Atributos). BGP busca el camino más estable hacia el destino, a diferencia de los otros protocolos de enrutamiento. Además este camino se basa en políticas de enrutamiento, lo cual permite controlar el flujo de tráfico entre los sistemas autónomos.

Debido a que en cada AS se utiliza un protocolo IGP con una definición distinta para el coste de los enlaces, es imposible encontrar el camino más corto hacia cada destino. Por ello, una vez se han aplicado las restricciones sobre las rutas, BGP utiliza un algoritmo similar al tipo vector de distancia, llamado *path-vector*, para seleccionar aquellas rutas que impliquen el mínimo número de AS a atravesar.

BGP Versión 4 (BGP-4) es la última versión de BGP y es definida en la RFC 4271, además existe una extensión de esta última versión llamada BGP4+, la cual soporta múltiples protocolos, incluyendo IPV6, estas son definidas en la RFC 4760.

Las tablas de encaminamiento de BGP almacenan rutas para alcanzar redes (indicadas mediante prefijos). Las rutas están formadas por una secuencia de números de sistemas autónomos que se deben seguir para alcanzar el prefijo indicado. El último número de AS de la ruta se corresponde con la organización que tiene registrado el prefijo, es decir, el AS donde se encuentra el destino. El principal motivo para almacenar la ruta completa es la detección y eliminación de bucles (loops) para evitar que los paquetes se envíen de forma infinita pasando varias veces por un mismo AS.

BGP usa TCP como protocolo de transporte, lo cual significa que es orientado a la conexión. Por lo tanto BGP envía la información dentro de segmentos, usando el puerto 179 y el número de protocolo 6,

Para entender el funcionamiento de BGP primero se deben tener conocimiento de los siguientes conceptos:

- **Sistema Autónomo:** Hace referencia a una red o grupo de redes administradas de manera independiente, donde se puede gestionar todo tráfico que pasa por ella.
- Los números de Sistemas Autónomos(AS) poseen 16 bits, es decir desde 1 – 65535 definidos en la RFC 1930, donde desde el 64512-65534 son privados. Actualmente existen sistemas autónomos de 32 bits.
- **IGP:** Interior gateway protocol, son los protocolos de enrutamiento de interior, es decir protocolos que corren dentro de un sistema autónomo, como por ejemplo RIP, EIGRP, OSPF, IS-IS.
- **EGP:** Exterior gateway protocol, son los protocolos que intercambian información de enrutamiento entre diferentes sistemas autónomos, como por ejemplo BGP.

BGP es un protocolo normalmente utilizado por los ISPs, ya que logra administrar un gran flujo de información de enrutamiento que existe en todo internet. Por lo tanto para entender de mejor forma como funciona BGP y cómo influye este protocolo en la red de una empresa o un ISP debemos entender como son interconectados.

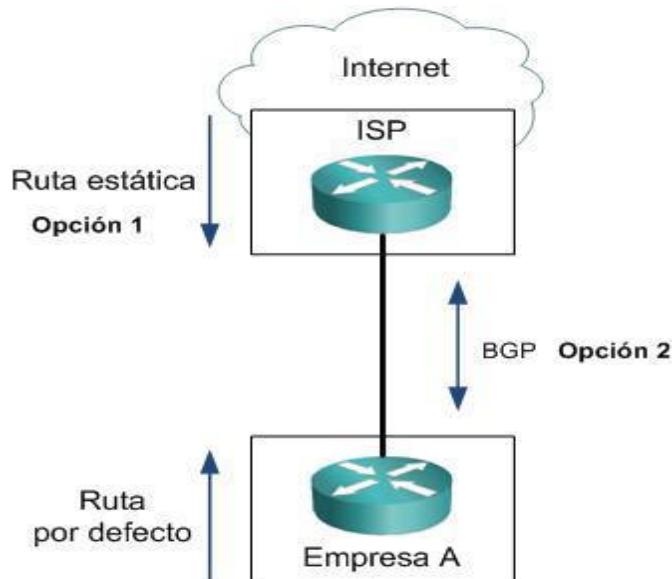
Tipos de conexiones a ISPs

Singlehommed ISP Connectivity.

Este tipo de conexión solo posee un enlace al ISP, por lo tanto no es tolerante a fallas. Existen dos formas de conectarse a Internet:

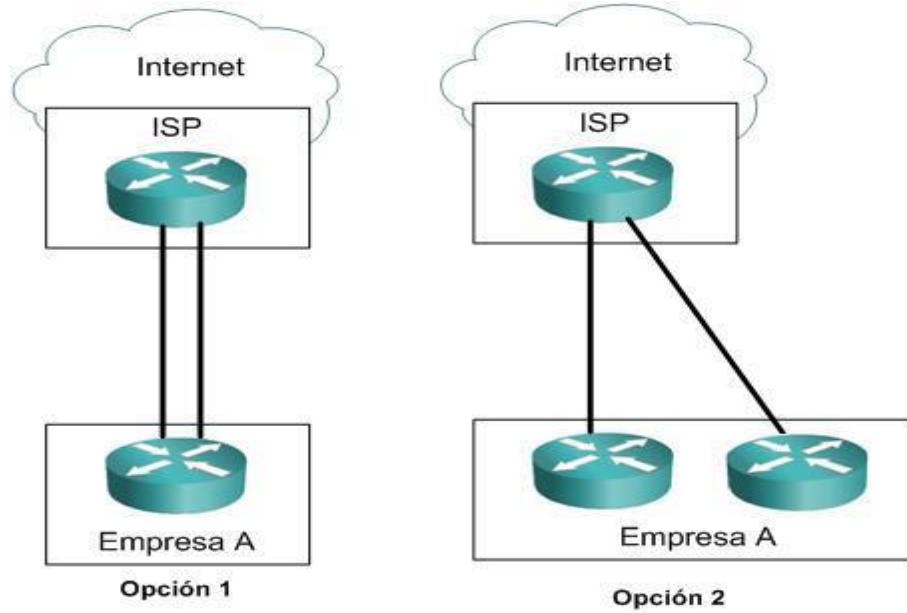
La primera opción es generando una ruta por defecto hacia el ISP, y a su vez el ISP genera una ruta estática hacia la red de la empresa. Esta opción no es la mejor, ya que el ISP debe estar configurando y realizando modificaciones en sus redes manualmente cada vez que la empresa decida realizar nuevos cambios. Además les toma demasiado tiempo a los equipos del ISP aprender esta nueva red. Por lo tanto la mejor opción es la 2.

La opción 2 utiliza BGP como protocolo de enrutamiento entre el ISP y la empresa, esto genera en el ISP una mejor forma de conexión, ya que las nuevas rutas pueden ser anunciadas directamente desde la empresa hacia el ISP, y gracias a BGP estas nuevas redes son aprendidas muy rápidamente.



Dual-Homed ISP Connectivity

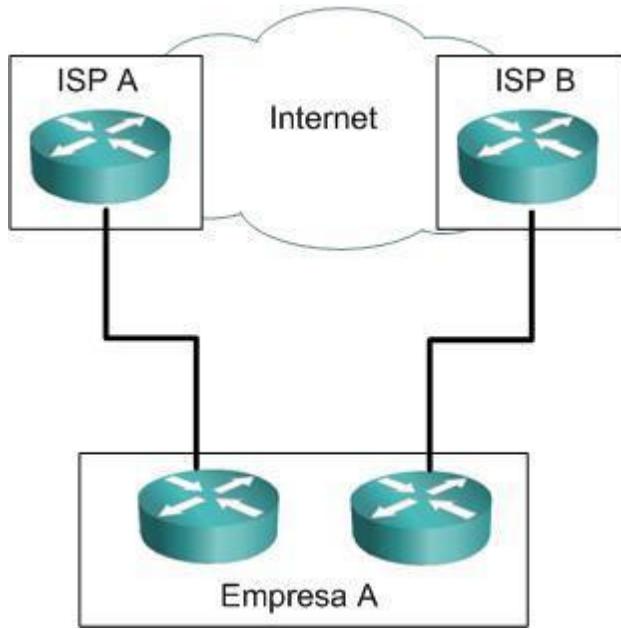
Este tipo de conexión provee un enlace redundante, por lo tanto ante la falla del primer enlace, siempre estará disponible un segundo. También gracias al doble enlace se puede realizar balanceo de carga. En la opción 1 si el router borde falla se pierde la conectividad hacia internet, a pesar de que posea un doble enlace. La opción 2 posee una mayor resistencia a fallas, ya que si ocurre un problema en uno de los equipos siempre existe la posibilidad de utilizar el router Backup.



Multihomed ISP Connectivity.

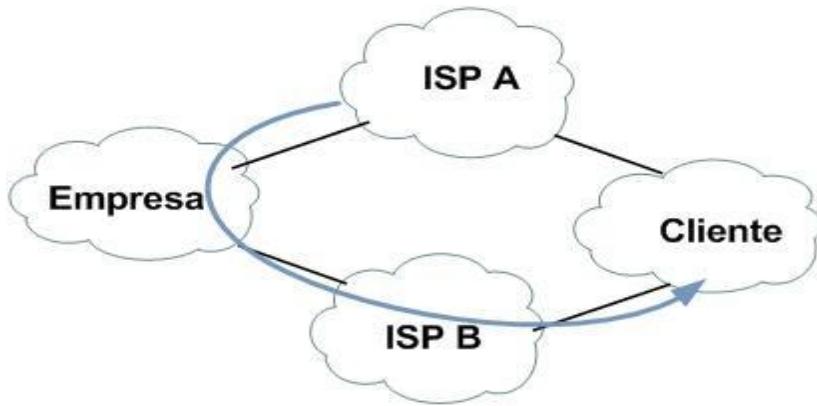
Hace referencia a la conexión de una empresa hacia dos ISP distintos. Si los enlaces hacia las empresas son redundantes se le llama dual Multihomed.

Proveer Multihomed genera una red escalable, resistente a fallas, que permite realizar balanceo de carga entre los diferentes ISP, ya que posee más de una conexión a internet.



Sistema Autónomo de transito

Al utilizar Multihomed se debe tener la precaución de definir como serán anunciadas las rutas hacia los ISP, ya que nuestra red podría ser utilizada por uno de los ISP como transito para alcanzar otros sistemas autónomos.



Cuando se decide implementar Multihomed existen 3 principales formas de realizar la conexión con el ISP.

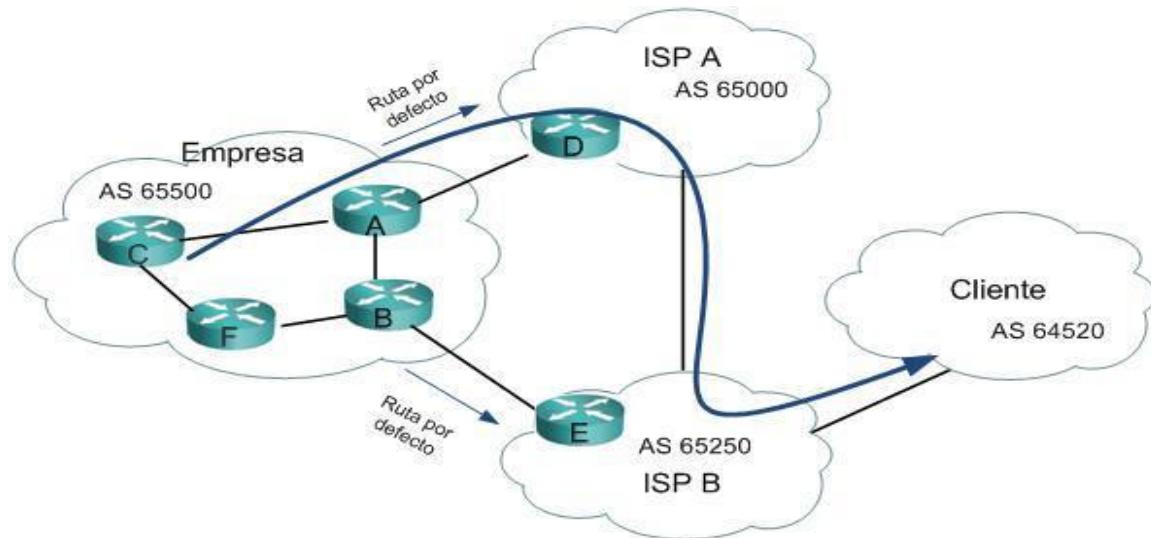
- 1) Se crea en los routers borde una ruta por defecto hacia el ISP, donde el uso de la CPU será menor y la tabla de enrutamiento más pequeña.
- 2) Se construye una ruta por defecto hacia el ISP y éste nos envía algunas rutas específicas. Donde el uso de CPU será medio y la tabla de enrutamiento no será sobrecargada.
- 3) El ISP nos envía todas las rutas de las redes, donde el uso del CPU será extremo y la tabla de enrutamiento será demasiado grande. Normalmente los ISP utilizan esta opción.

Entre más redes anunciadas por el ISP, más precisa será la decisión de enrutamiento.

Multihomed mejor ruta

Dentro de un sistema autónomo los IGP son los encargados de seleccionar el mejor camino, cuando se decide redistribuir una ruta por defecto en un IGP puede suceder que no siempre se seleccione el mejor camino para alcanzar el destino fuera de la red.

Por ejemplo, la red de la Empresa en el sistema autónomo 65500 desea conectarse con la red del Cliente perteneciente al sistema autónomo 64520. Si se decide redistribuir una ruta por defecto en router A y router B dentro de un IGP como RIP, router C elegiría la ruta más corta dentro de su sistema autónomo, por lo tanto decidiría el camino por router A, debido que existen menos saltos.

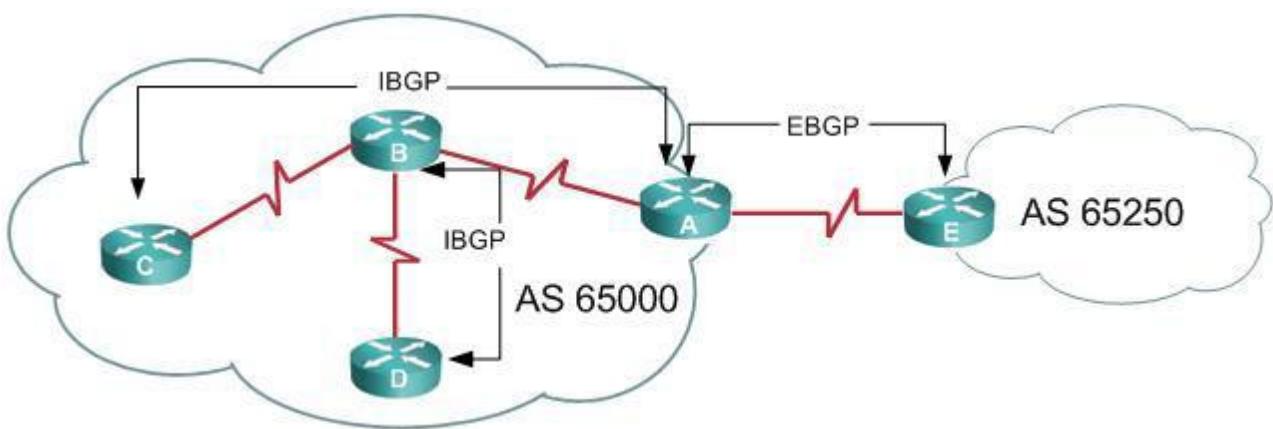


Router A decidiría utilizar la ruta por defecto hacia ISP A perteneciente al sistema autónomo 65000.

Este camino no es el más óptimo para llegar a la red destino del Cliente, ya que fue influenciado por el IGP de la red de la Empresa. La solución para este problema está en aplicar BGP, utilizando sus políticas y atributos, para influenciar el tráfico por el camino más óptimo para alcanzar las redes deseadas.

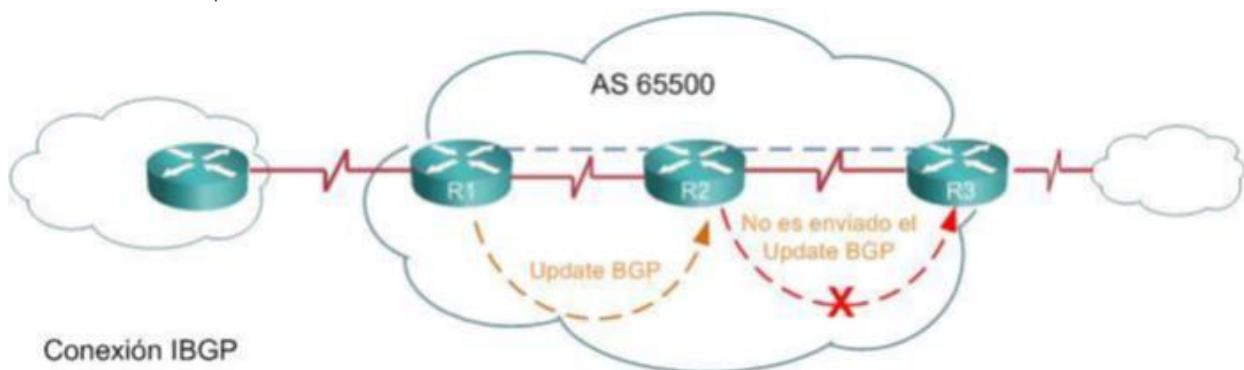
IBGP y EBGP

IBGP hace referencia a la conexión entre dos routers que corren BGP dentro de un mismo sistema autónomo, como por ejemplo, Router A, B, C y D son IBGP dentro del SA 65000. EBGP son los Routers borde que interconectan los distintos SA, como por ejemplo Router A del SA 65000 y Router E del SA 65250



Los mensajes BGP entre peers EBGP, se envian con un TTL de 1, por lo tanto solo se puede generar adyacencia EBGP entre routers borde, ya que no permite mas de un salto. El TTL entre routers IBGP siempre es mayor a 1, (En Dynagen es 255), lo que permite generar adyacencia entre vecinos que no se encuentran directamente conectados.

Problemas de Update



Según la regla de BGP split horizon especifica que las rutas aprendidas vía IBGP nunca son propagadas a otros IBGP peers.

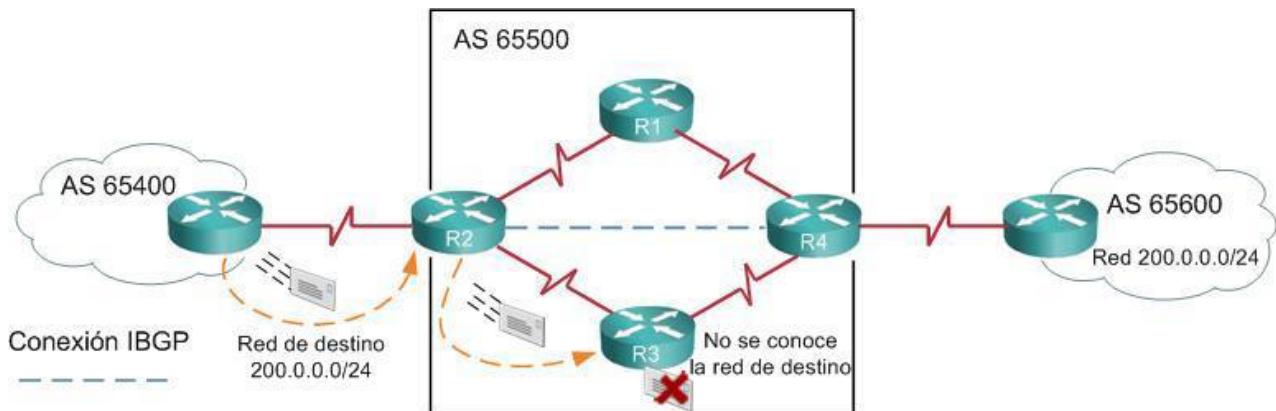
Tipos de Sistemas Autónomos

Sistema autónomo de transito

Un AS de transito es el encargado de transportar tráfico entre sistemas autónomos, como por ejemplo el tráfico entre distintos ISPs o sucursales.

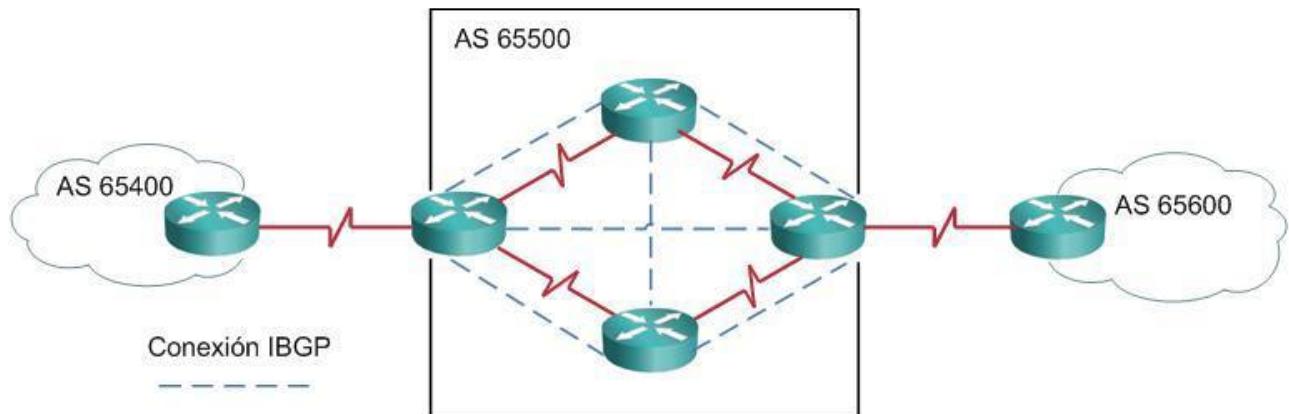
En un sistema autónomo de tránsito todos los routers deben tener completo conocimiento de las rutas externas. Una opción para lograr esto es redistribuyendo todas las rutas en el IGP que corre dentro del sistema autónomo, sin embargo esto puede provocar problemas.

Al redistribuir las rutas dentro de un IGP las tablas de enrutamiento serán gigantescas y protocolos como Ospf o Eigrp no podrán soportarlas.



Otra opción es correr IBGP solo en los routers borde, pero esto generará otro problema. Al momento de anunciar redes externas, éstas serán informadas solo a los routers borde IBGP, y al momento de que el tráfico atravesie el sistema autónomo de tránsito existirán routers que no tengan un destino hacia esa red (como R1 y R3 de la figura 3.1), ya que no las aprendieron vía BGP y no poseen un camino vía IGP. Por lo tanto estos paquetes serán descartados.

La solución es correr IBGP en todos los routers dentro del sistema autónomo de tránsito, realizando un full mesh entre routers que corren BGP. Ejemplo full-mesh



Sistema Autónomo de no tránsito

En un sistema autónomo Multihomed se aconseja correr IBGP en los routers borde. Los routers que hablarán IBGP solo pasaran las rutas a su vecino IBGP, y estos vecinos no pasaran estas rutas a otros. De esta forma se asegura BGP de evitar bucles de enrutamiento, pero esto a su vez es un problema en sistemas autónomos de tránsito.

Cuando el sistema autónomo no es de tránsito, las decisiones de salida pueden ser tomadas por el IGP, evitando correr IBGP en todos los routers del sistema autónomo. Por ejemplo se puede redistribuir una ruta por defecto dentro de IGP en cada router borde, pero como existen dos salidas, puede que esta decisión no sea la mejor, ya que la mejor salida será influenciada por el IGP.

Por lo tanto para seleccionar el mejor camino se debe correr IBGP en todos los routers, ya que él será el encargado de decidir cuál será la mejor salida. Cabe recordar que las redes que serán aprendidas por los IBGP no necesariamente serán todas las existentes en Internet, por lo tanto la empresa puede tomar la decisión de aprender solo las redes necesarias, a las que le interesa escoger el mejor camino, y para todas las demás, tomar la ruta por defecto redistribuida.

¿Cuándo usar BGP?

Se debe utilizar BGP cuando se tiene un buen entendimiento de su funcionamiento y además se cumple una de las siguientes condiciones:

- El sistema autónomo será utilizado como transito para alcanzar otros sistemas autónomos. Por ejemplo un ISP.
- Cuando un sistema autónomo posee más de una conexión a otros sistemas autónomos.
- Cuando se desea aplicar políticas de enrutamiento sobre el tráfico que entra y sale del sistema autónomo

Normalmente no es necesario usar BGP cuando se posee una sola salida en la red, por lo tanto en estos casos solo con una ruta estática o ruta por defecto bastaría.

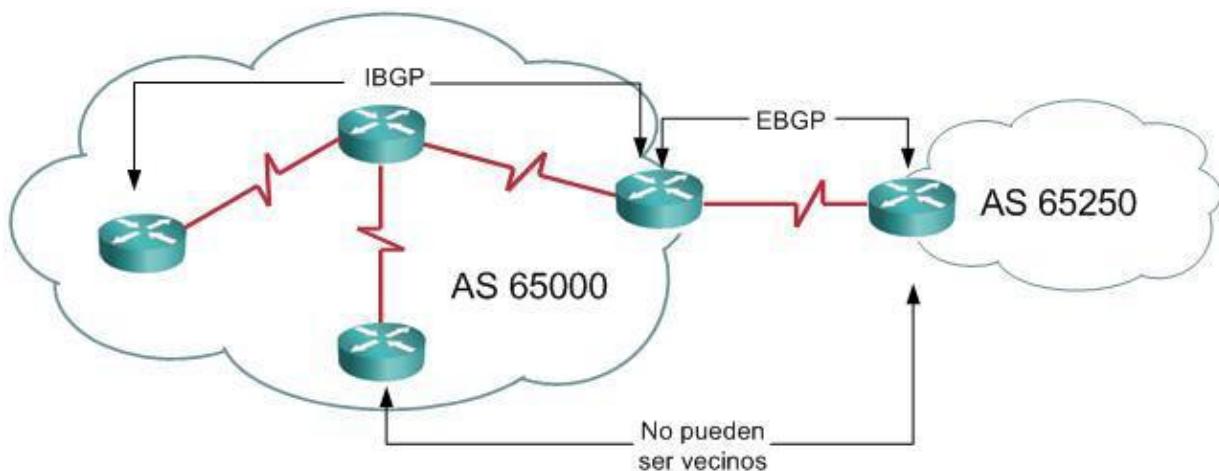
No se debe usar BGP cuando existen las siguientes condiciones:

- Existe solo una conexión a Internet o a un sistema autónomo.
- Pocos recursos de hardware, cuando existe muy poca memoria en el router o el procesador no soporta constantes actualizaciones de BGP.
- Cuando se posee limitado conocimiento sobre el proceso de selección de rutas de BGP.

Configuración de vecinos

BGP no funciona igual que los otros protocolos de enrutamiento IGP, y exige primero identificar quiénes serán sus vecinos.

Ya que la vecindad no necesita ser directa, también existen restricciones respecto a las vecindades. Por ejemplo, dentro de un sistema autónomo se pueden generar Neighbors, a pesar de que estos no se encuentren directamente conectados (IBGP), pero solo el router borde puede generar vecindad con el router perteneciente al otro sistema autónomo (EBGP).



Un Router EBGP intentará conversar con su neighbor, por lo tanto éste debe poder ser alcanzado, y ya que esta directamente conectado, no necesita de otro protocolo (como un IGP).

Cuando se inicia la conversación entre los EBGP se genera un three-way handshake, por la sesión TCP entre ambos. Por lo tanto al declarar un vecino con el comando **Neighbor** éste debe ser alcanzable.

Ya que no es necesario que los vecinos estén directamente conectados, normalmente se decide usar interfaces **loopbacks** para el establecimiento de la sesión TCP entre los routers, esto permite que cuando existan caminos redundantes hacia un vecino, la caída de una interfaz física no afecte la adyacencia.

[Regla de sincronización de BGP](#)

La regla de sincronización de BGP indica que en un sistema autónomo de transito, encargado de transportar tráfico entre redes, BGP nunca debería anunciar las redes antes de que el IGP aprenda las rutas. Por lo tanto ambos deberían ser sincronizados. Esto ayuda a que no ocurran problemas dentro del sistema autónomo cuando se utiliza como transito, ya que siempre poseerá un camino dentro de la red de la empresa, y no generará un Black Hole.

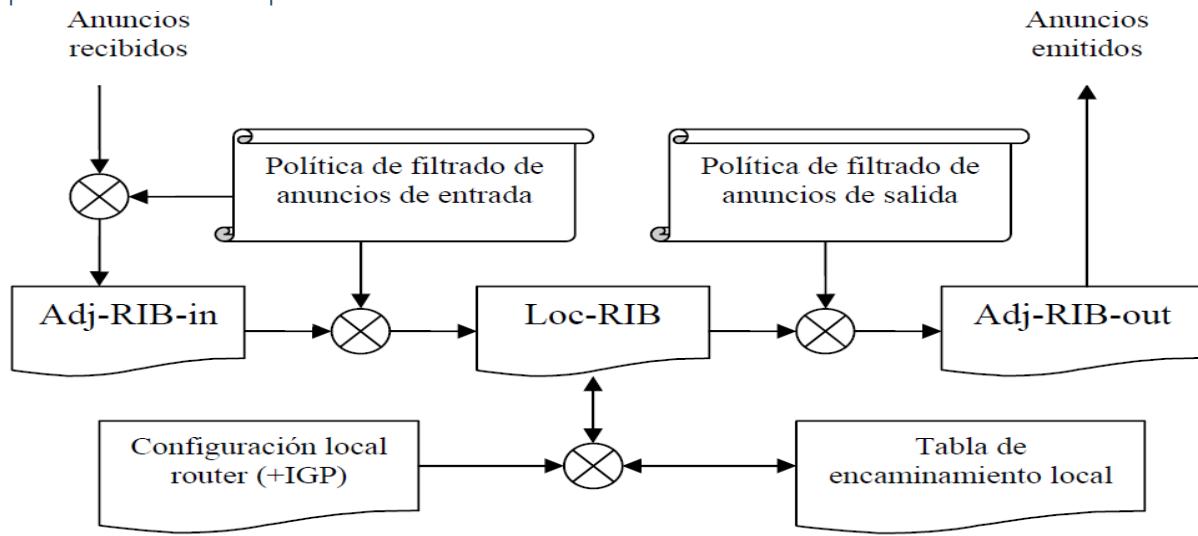
Funcionamiento del proceso BGP

Cuando un router anuncia un prefijo a uno de sus vecinos BGP, esa información es considerada válida hasta que el primer router explícitamente anuncia que la información ya no es válida o hasta que la sesión BGP se pierde. Esto significa que BGP no requiere que la información de routing se refresque periódicamente. De este modo, en un principio existirá un alto flujo de mensajes cuando se establece la sesión BGP, pero transcurrido un tiempo de estabilización los routers sólo necesitarán informar de los cambios que han ocurrido. Por ejemplo, en un AS tipo *backbone* el intercambio es del orden de 50.000 prefijos inicialmente.

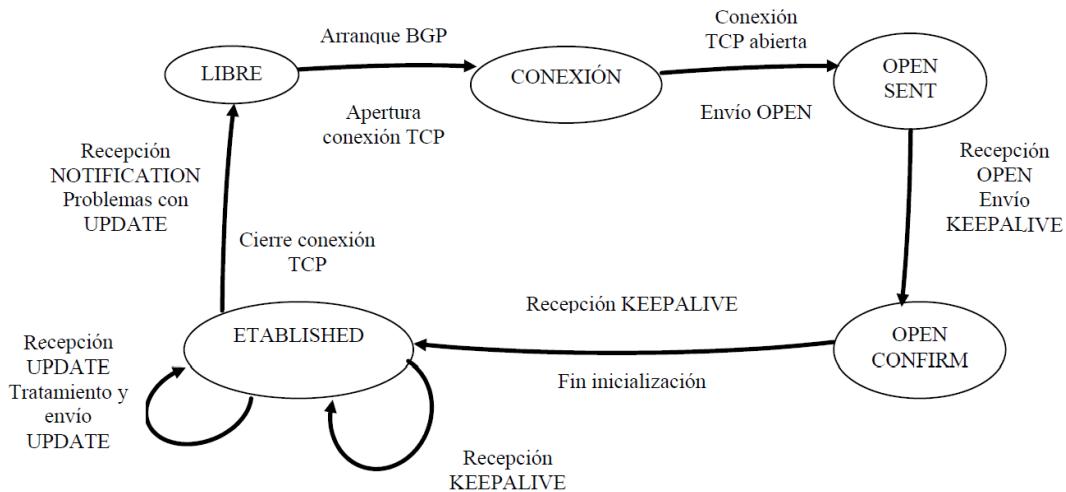
Para almacenar información de encaminamiento, el protocolo BGP necesita un conjunto de tablas de datos denominadas RIBs (*Routing Information Bases*). Éstas son las siguientes:

- **Adj-RIB-in:** En esta tabla se almacenan prefijos aprendidos de un vecino particular. Hay tantas tablas de este tipo como pares BGP.
- **Loc-RIB:** Almacena las mejores rutas seleccionadas (prefijos + longitud máscara) que conoce el proceso BGP bien porque las ha obtenido de la tabla de encaminamiento (comandos network, agrégate-address y redistribute), o bien porque se han aprendido por BGP (I-BGP o E-BGP), tras pasar los filtros de entrada. Estas rutas pueden ser anunciadas si la política de encaminamiento a la salida lo permite. Hay sólo uno por cada sistema autónomo.
- **Adj-RIB-out:** Almacena prefijos para ser anunciados a otros vecinos. Esta tabla se construye a partir de las informaciones de la tabla Loc-RIB que han sido filtrados y cuyos atributos han sido modificados según configuración. Se tiene una tabla de este tipo por cada par BGP.

Esquema funcional del proceso BGP:



El proceso BGP consiste en un autómata de 6 estados con 13 eventos posibles. La interacción con otros procesos BGP se lleva a cabo intercambiando mensajes. Los mensajes intercambiados en una sesión BGP sirven para informar sobre el conocimiento de nuevas rutas activas, para suprimir rutas que ya no están activas, para indicar la viabilidad actual de la conexión o para informar sobre la existencia de condiciones inusuales en la conexión TCP. El siguiente esquema muestra los estados y los mensajes del proceso BGP:



Estados de un Neighbor BGP.

Los routers para generar adyacencia pasan por los siguientes estados:

- Idle
- Connect
- Active
- Open sent
- Open Confirm
- Established

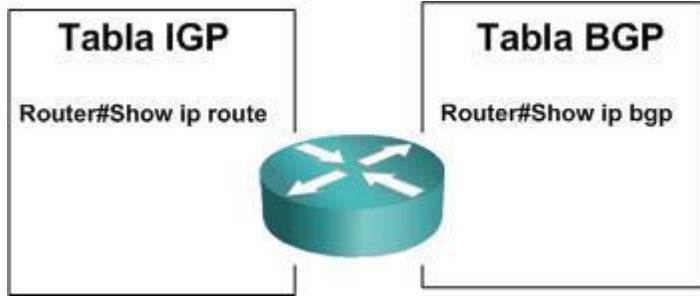
Cuando se encuentra en el estado Established, los mensajes OPEN, NOTIFICATION Y KEEPALIVE son intercambiados.

Tablas de BGP

BGP mantiene su tabla de enrutamiento separada de la tabla de IGP, y ofrece las mejores rutas a la tabla de enrutamiento IGP. También pueden ser redistribuidas las rutas de la tabla de BGP a la tabla de enrutamiento IP del IGP.

La tabla de información de BGP se conoce con varios nombres:

- BGP table
- BGP topology table
- BGP topology database
- BGP routing table
- BGP forwarding database



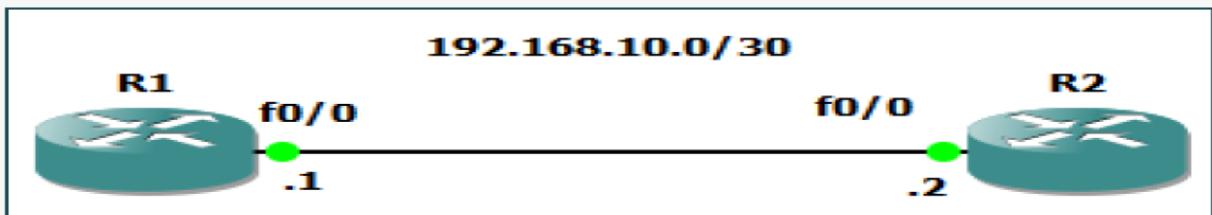
Las redes aprendidas por EBGP poseen una distancia administrativa de 20, y las IBGP poseen una distancia administrativa de 200. Por lo tanto solo pasan a la tabla de enrutamiento las rutas con menor distancia administrativa, en comparación con las rutas de los protocolos IGP.

BGP también mantiene una Neighbors Table, la cual contiene una lista de sus vecinos con los cuales posee conexión. Para que BGP genere adyacencia debe ser asignado explícitamente el vecino con el comando **Neighbor**. Luego de establecer adyacencia, Bgp mantiene esta relación con mensajes BGP/TCP keepalive, los cuales son enviados siempre cada 60 segundos.

Ejemplo de adyacencia con comando Neighbor

```
R1(config)#router bgp 65000
R1(config-router)#neighbor 192.168.10.2 remote-as 65000
R1(config-router)#
*Mar 1 00:09:05.671: %BGP-5-ADJCHANGE: neighbor 192.168.10.2 Up

R2(config)#router bgp 65000
R2(config-router)#neighbor 192.168.10.1 remote-as 65000
R2(config-router)#
*Mar 1 00:09:07.235: %BGP-5-ADJCHANGE: neighbor 192.168.10.1 Up
```



Tipos de mensajes de BGP

Cuando la sesión TCP se establece el primer mensaje en enviarse es el OPEN, si se logra establecer la conexión, se responde con un mensaje Keepalive.

Cuando la conexión ya ha sido establecida se intercambian los mensajes Update, keepalive y Notification. Los mensajes Update se utilizan para intercambiar sus tablas de enrutamiento, los keepalive se encargan de mantener la conexión arriba y los notification avisan algún error o condición especial.

Mensajes

- Open (19 – 4096 bytes)
- Keepalive (19 bytes)
- Update (19 – 4096 bytes)
- Notification (19 – 4096 bytes)

Mensaje Update, intercambio de tabla de enrutamiento.

Estos mensajes envían información sobre los Path, cada Path requiere de un mensaje update. Cada update posee los atributos respecto al path, y las redes que pueden ser alcanzadas por este path. Por lo tanto cada Update posee las Rutas con sus respectivos atributos (as-path, origin, local-preference, etc.).

Parámetros de los paquetes BGP

- **Version** : Identifica la versión que corre BGP, posee 8 bit y actualmente es versión 4.
- **Sistema Autónomo** : Identifica el sistema autónomo, posee 16 bit.
- **Hold-time** : Tiempo de espera máximo entre los mensajes keepalive, posee 6 bit y por defecto son 180 segundos.
- **Optional Parameters.**

Estados de un Neighbor BGP.

Los routers para generar adyacencia pasan por los siguientes estados:

- Idle
- Connect
- Active
- Open sent
- Open Confirm
- Established

Cuando se encuentra en el estado Established, los mensajes OPEN, NOTIFICATION Y KEEPALIVE son intercambiados.

Verificación rápida de estado de vecinos

Un comando muy útil, cuando ya se encuentran configurados los neighbors es el #**show ip bgp summary**, con este comando se puede verificar el estado de un vecino, y determinar si existe algún problema en la adyacencia. También se puede verificar el sistema autónomo perteneciente a ese vecino, y el tiempo transcurrido desde que se generó la adyacencia.

```
R1#show ip bgp summary
Neighbor      V   AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.10.1  4 65000       12      13       4    0     0 00:08:16      0
```

Atributos BGP

Los routers BGP envían mensajes update sobre redes, con sus respectivos prefijos y atributos. Estos prefijos y atributos se utilizan para seleccionar el mejor camino hacia una red.

Los atributos pueden ser:

- Well-known / optional
- Mandatory / discretionary
- Transitive / nontransitive

Los atributos de ruta se dividen en cuatro categorías:

- Well-known mandatory
- Well-known discretionary
- Optional transitive
- Optional nontransitive

Los atributos Well-known son los que deben ser obligatoriamente reconocidos por todos sus vecinos. Existen dos tipos, “mandatory”, los cuales deben ir obligatoriamente en todos los mensajes update de BGP y los Well-known discretionary, los cuales no necesariamente debe estar presente en todos los mensajes actualizaciones, pero si deben ser reconocidos por los routers BGP.

Los atributos opcionales, no necesitan ser necesariamente reconocidos por los routers BGP. Existen dos tipos, Optional transitive, a pesar de que el router no implementan el atributo, lo debe pasar a otros routers, y los Optional nontransitive los cuales no implementan el atributo lo eliminan y no lo pasan a otros routers.

Los atributos definidos por BGP son los siguientes:

Well-know mandatory attributes	Optional transitive attributes
AS-path	Aggregator
Next hop	Community
Origin	
Well-know discretionary attributes	Optional nontransitive attribute
Local preference	Multiexit-discriminator
Atomic aggregate	

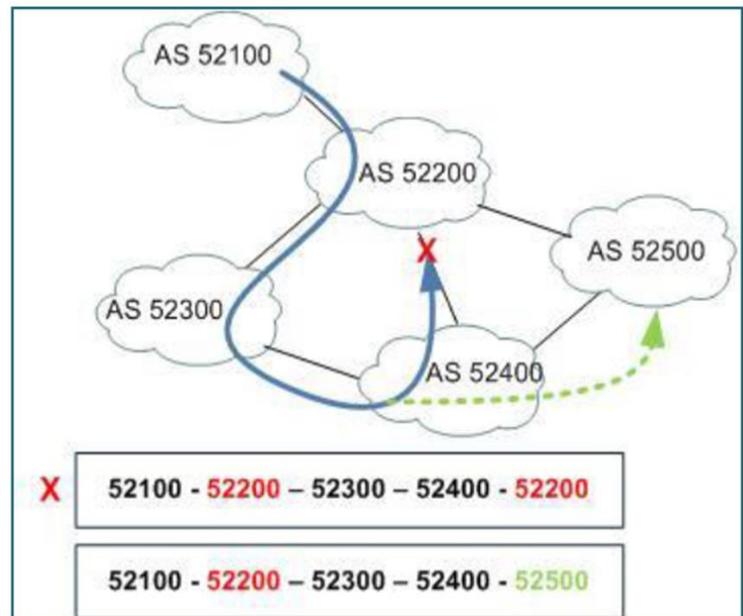
Además Cisco define un atributo llamado weight el cual es configurado localmente y no es propagado a los vecinos.

Atributo AS-PATH

Lista los sistemas autónomos por los que pasa la ruta para llegar a la red, se utiliza para asegurar un camino libre de bucles, ya que el router no aceptará una ruta que posea un sistema autónomo por el cual ya atravesó.

Además este atributo es **well-known mandatory**.

Por ejemplo si el paquete viaja desde el AS 52100 al AS52500 y toma el camino 52100 – 52200 – 52300 – 52400, al momento de decir el camino, nunca lo enviará al 52200, ya que por este ya pasó



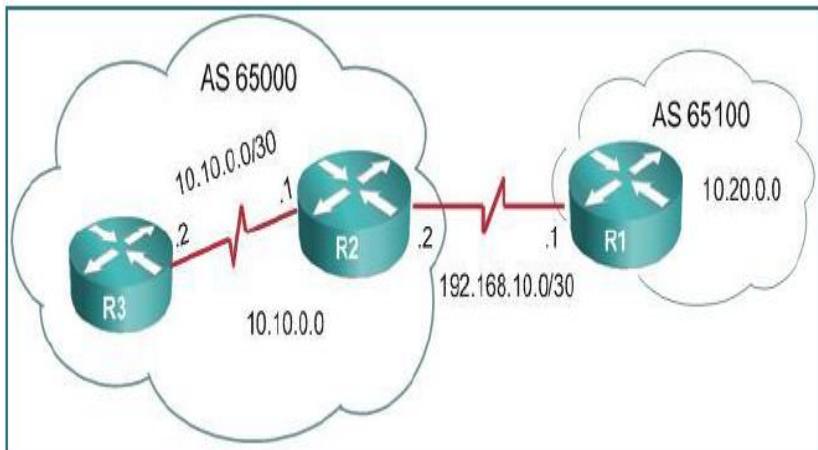
Atributo Next-hop

Este atributo indica la dirección IP del siguiente salto para alcanzar la red destino.

El siguiente salto no necesariamente debe estar directamente conectado, sino que más bien es la dirección IP del router quien anunció la red.

Este atributo es **well-known mandatory**.

Por ejemplo, router R3 tiene como Next-hop de la red 10.20.0.0 la dirección IP 192.168.10.1 del router R1.



Atributo Origin

Indica cómo fue aprendida la ruta, si fue aprendida a partir de un IGP utilizando el comando network, se marca una “l” en la tabla de BGP. Si la ruta fue aprendida por un EGP se marca con una “e”. Incomplete, es cuando el origen es desconocido, normalmente ocurre cuando una ruta es distribuida en BGP y es marcada con un signo “?”.

Este atributo además es **well-known mandatory**

Atributo Local Preference

Se utiliza para determinar cuál es la salida preferida en el sistema autónomo. Cuando el Local Preference es más alto, posee mayor prioridad, por lo tanto es mejor.

Este atributo es enviado solo entre peers IBGP dentro del mismo sistema autónomo local y no es enviado entre peers EBGPs. Para routers Cisco el local preference por defecto es 100. Además este es un atributo **well-known discretionary**.

Atributo MED

Este atributo informa a los vecinos externos por cuál de las salidas del sistema autónomo local se prefiere que sean alcanzadas las redes locales, en otras palabras cual es la entrada preferida a la red. El menor valor MED es el preferido, por lo tanto posee mayor prioridad. Este atributo es enviado entre los vecinos EBGP y por defecto es 0. Este atributo es **optional nontransitive attribute**.

Atributo WEIGHT

Este atributo es utilizado en el proceso de selección de ruta, tiene significancia local, por lo tanto no es propagado hacia los vecinos. Cuando existen múltiples rutas hacia un camino, la ruta con weight más alto será la preferida.

Selección de la mejor ruta:

Un router pasa la mejor ruta a tabla de enrutamiento, pero cuando existe más de una ruta para una red específica, sigue los siguientes criterios:

- 1) Los routers cisco prefieren las rutas que posean mayor weight.
- 2) Si aun así existe más de una ruta, se selecciona la ruta con mayor local preference.
- 3) Si las rutas poseen igual Local preference, se selecciona la ruta que fue generada localmente vía comando Network o aggregate-address.
- 4) Si las rutas no fueron originadas localmente por el router, se prefiere la ruta con menor as-path.
- 5) Si el tamaño del as-path es el mismo, se prefieren las rutas menórricamente originadas según el siguiente código: IGP<EGP<Incomplete.
- 6) Si las rutas poseen el mismo código origin, se prefieren las rutas con menor MED. La comparación del MED solo ocurre cuando el comando bgp-always-compare-med es habilitado.
- 7) Si poseen el mismo MED, se prefieren los caminos EBGP sobre los IBGP.
- 8) Si no hay neighbors EBGP y solo existen vecinos IBG, además de que la sincronización se encuentra deshabilitada, se prefiere el camino con menor métrica respecto del IGP existente en relación a la dirección del siguiente salto.
- 9) Cuando las rutas son aprendidas vía EBGP, se prefiere la ruta que fue recibida primero, es decir la más antigua. Este paso es saltado si el comando router-id es configurado en el router.
- 10) Se prefiere el camino con menor router-id del vecino.
- 11) Si las direcciones IP son iguales, se prefiere la dirección del router del vecino más baja.

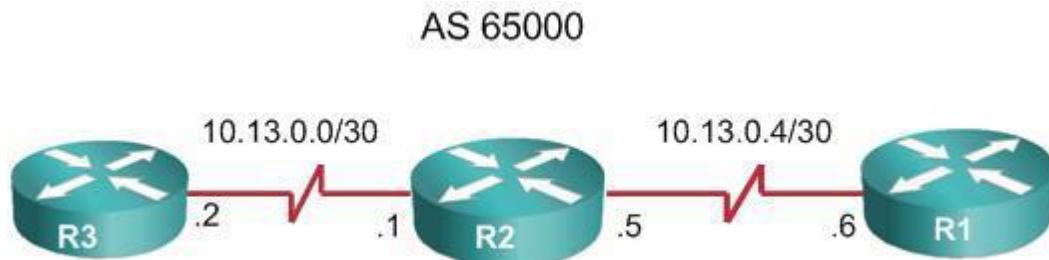
Configurando BGP

Para empezar a configurar se debe iniciar el proceso de BGP con el siguiente comando en modo configuración global:

#router bgp numero de sistema autónomo Solo se permite un proceso de BGP, por lo tanto si ya se ingresó un número de sistema autónomo y se intenta ingresar otro proceso, el Router notificará el número ya configurado.

Luego con el comando Neighbor dentro de la configuración de BGP se define el vecino:

#neighbor dirección IP remote-as número del sistema autónomo del router vecino.



R1(config)#router bgp 65000

R1(config-router)#neighbor 10.13.0.5 remote-as 65000

R2(config)#router bgp 65000

R2(config-router)#neighbor 10.13.0.2 remote-as 65000

R2(config-router)#neighbor 10.13.0.6 remote-as 65000

R3(config)#router bgp 65000

R3(config-router)#neighbor 10.13.0.1 remote-as 65000

Luego se puede comprobar que la adyacencia se ha generado ingresando el comando **#show ip bgp summary**, con esto verificamos el estado de los vecinos (State/PfxRcd), y si se ha logrado generar adyacencia entre ellos.

```
R2#show ip bgp summary
BGP router identifier 192.168.10.2, local AS number 65000
BGP table version is 1, main routing table version 1
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.13.0.2	4	65000	8	8	1	0	0	00:05:28	0
10.13.0.6	4	65000	8	8	1	0	0	00:04:17	0

Anunciando redes

Para anunciar redes se debe usar el comando:

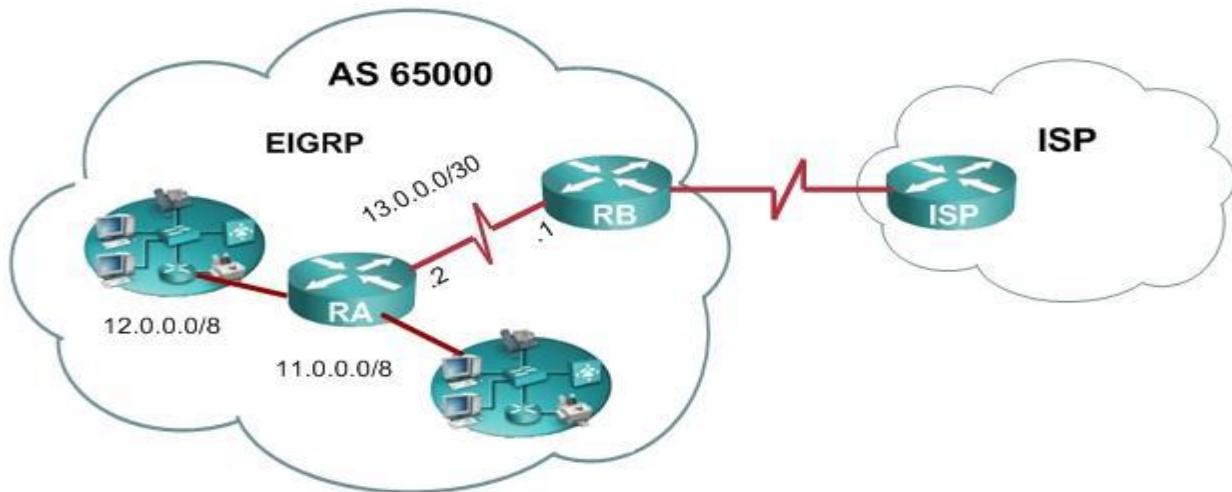
#Network dirección de red mask máscara de la red

Este comando se debe ingresar en la configuración de BGP y se debe escribir exactamente la dirección de red y mascara, sino arrojará aviso de error. Esto normalmente ocurre cuando se ingresa una dirección de host.

También se debe tomar en cuenta que los routers borde son los encargados de anunciar las redes que se encuentran dentro del sistema autónomo, y ese router borde debe conocer todas las redes para poder anunciarlas. El router por ejemplo puede conocer las redes por un protocolo de enrutamiento como EIGRP y anunciar con el comando network dentro BGP las redes conocidas por este protocolo. Por lo tanto NO ES NECESARIO que las redes que se ingresen con el comando network se encuentren directamente conectadas al router borde, solo es necesario que las conozca por un protocolo de enrutamiento o ruta estática.

Ejemplo

Router RB puede anunciar a ISP con el comando network las redes 11.0.0.0/8 y 12.0.0.0/8 a pesar de que no las tenga directamente conectadas, ya que estas redes las conoce por EIGRP. Es muy importante que las conozca porque si no, no podrán ser anunciadas.



Ejemplo Adyacencia con loopbacks.

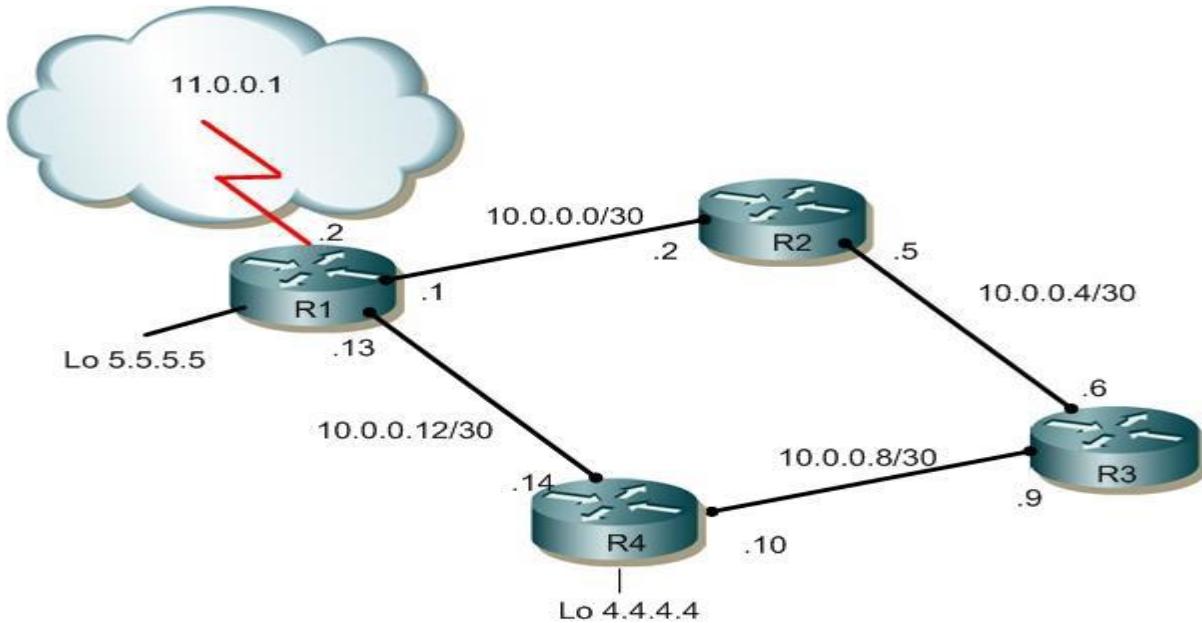
En esta topología los 4 Routers pertenecen al mismo sistema autónomo (100), y todos corren EIGRP conociendo así todas las redes. La configuración de los neighbors debe ser hacia el Router borde (R1), en consecuencia los routers podrían ser configurados de la siguiente manera.

```
R2-R3 (config-router)#Neighbor 10.0.0.1 remote-as 100
```

```
R4 (config-router) #Neighbor 10.0.0.13 remote-as 100
```

Por lo tanto NO ES NECESARIO que se configuren R4-R3 como neighbors ni R3 con R2. También hay que destacar la dirección IP de neighbor puede ser cualquier IP configurada en el router a la que se pueda alcanzar vía protocolo de enrutamiento IGP o ruta estática. Por lo tanto R4 puede configurar como vecino a R1 con el comando

```
R4(config-router)#Neighbor 5.5.5.5 remote-as 100
```



Ya que puede alcanzar la dirección IP 5.5.5.5 por EIGRP. BGP identifica como origen la dirección IP de la interfaz de salida, por lo tanto en R4 se debe configurar como origen la dirección IP 4.4.4.4 con el siguiente comando:

```
(config-router)#Neighbor 5.5.5.5 update-source loopback 0
```

Se aconseja utilizar las loopbacks para los neighbors cuando se tiene más de un camino hacia el otro Neighbor, para así no generar vecindad con la dirección de la interfaz de salida, ya que podría fallar y al momento de seleccionar el otro camino hacia el neighbor cambiaría las direcciones IP y por lo tanto no se generaría vecindad

Actualizar políticas aplicadas a rutas.

Al momento de aplicar nuevas políticas a las rutas, estas deben ser actualizadas, existen 3 caminos para actualizar las rutas:

Hard reset:

Se puede realizar con el comando **clear ip bgp *** o **clear ip bgp dirección_vecino**. Esto permitirá que se reinicie completamente la sesión TCP entre todos los vecinos (*) o un vecino específico. El restablecimiento de la sesión toma entre 30 a 60 segundos y genera que se reenvíen todas las tablas de BGP, actualizando así las nuevas políticas aplicadas.

Soft reset:

Utiliza gran parte de la memoria, ya que almacena todos los updates sin modificación en una tabla. Luego cuando se aplica el filtro, los cambios son calculados a partir de esta tabla. El comando es **clear ip bgp soft**.

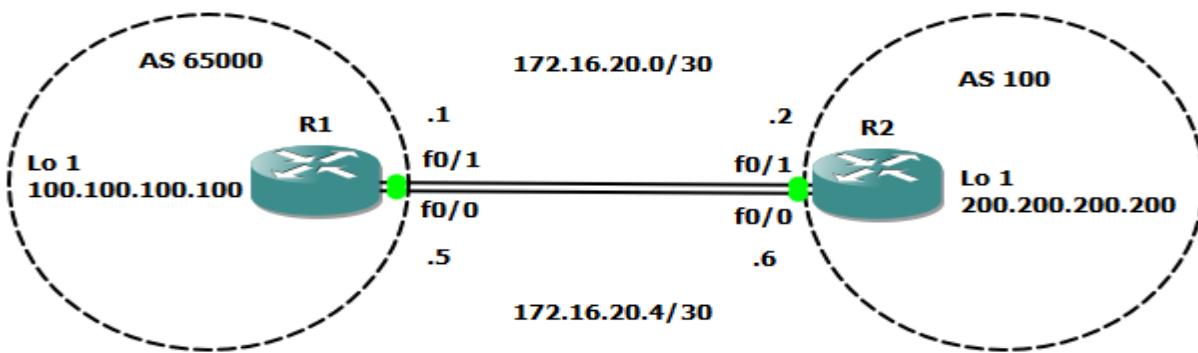
Route refresh:

Solicita al peer el reenvío de toda la información, esto utiliza menos memoria, y permite al router aplicar las políticas de entrada. El comando es **clear ip bgp {* | address | peer-group -name} in**. Para poder

utilizar route refresh, los routers deben soportar esta capacidad, esto se puede verificar con el comando `show ip bgp neighbors`.

EBGP Multihop

Si poseemos dual homed para alcanzar un sistema autónomo, podríamos preferir que el tráfico fuera balanceado entre los enlaces. Esto permitiría aprovechar el ancho de banda de los enlaces para enviar el tráfico fuera de nuestra red, y que además exista un enlace de Backup. Para lograr esto, tenemos que generar adyacencia con loopbacks entre vecinos EBGP. Sin embargo los paquetes enviados entre vecinos EBGP poseen un TTL en 1, y para utilizar loopback necesitamos como mínimo dos saltos, por lo tanto debemos aplicar el comando `ebgp-multihop` como veremos a continuación.



Se debe aplicar el comando `neighbor dirección_IP ebgp-multihop 2` para permitir que los mensajes de EBGP posean un TTL de 2, esto permitirá la adyacencia entre vecinos EBGP usando loopbacks.

```
R1(config)#router bgp 65000
R1(config-router)#neighbor 200.200.200.200 remote-as 100
R1(config-router)#neighbor 200.200.200.200 ebgp-multihop 2
R1(config-router)#neighbor 200.200.200.200 update-source loopback 1
R1(config-router)#exit
R1(config)#ip route 200.200.200.200 255.255.255.255 172.16.20.2
R1(config)#ip route 200.200.200.200 255.255.255.255 172.16.20.6
```

También se deben crear dos rutas estáticas hacia la dirección de loopback que generará la adyacencia, para que realicen un balanceo de carga entre los enlaces.

```
R2(config)#router bgp 100
R2(config-router)#neighbor 100.100.100.100 remote-as 65000
R2(config-router)#neighbor 100.100.100.100 ebgp-multihop 2
R2(config-router)#neighbor 100.100.100.100 update-source loopback 1
R2(config-router)#exit
R2(config)#ip route 100.100.100.100 255.255.255.255 172.16.20.1
R2(config)#ip route 100.100.100.100 255.255.255.255 172.16.20.5
```

Dirección del próximo salto

BGP anuncia las redes con la dirección del próximo salto, es decir las redes que conozca el router de borde vía BGP las anunciara a sus vecinos DENTRO de su sistema autónomo con la dirección IP del

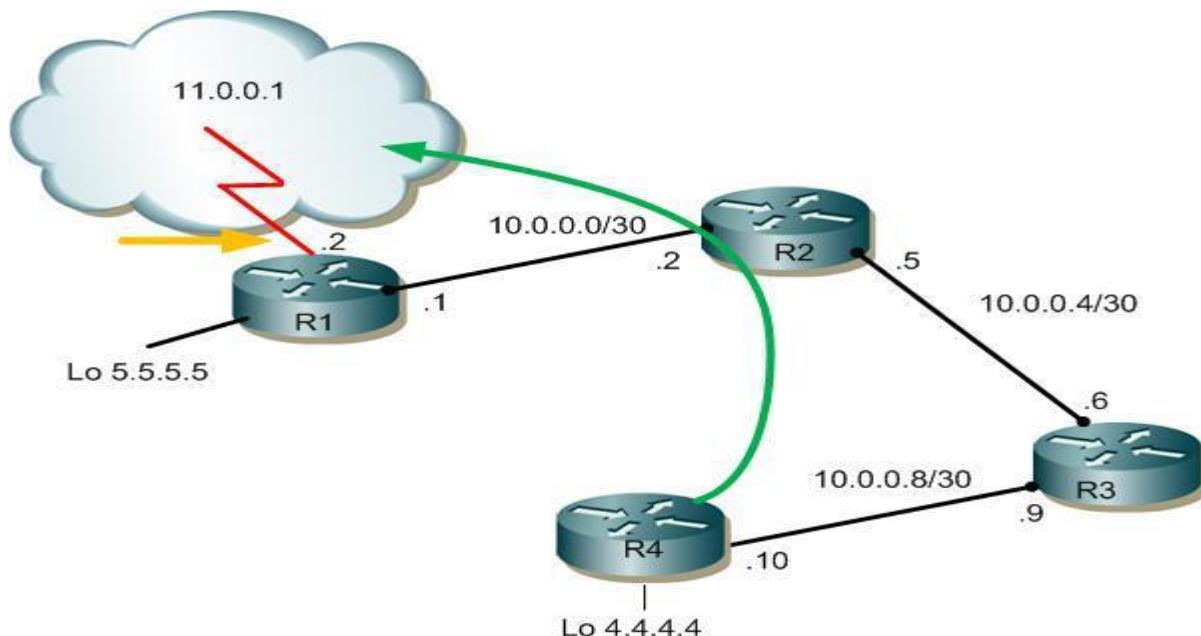
neighbor externo, por lo tanto todos los routers dentro del sistema autónomo deben saber cómo poder alcanzar esa dirección. Esto es muy importante, ya que puede ocurrir que los routers conozcan todas las redes de los sistemas autónomos externos y aun así no pueda llegar a ella, ya que no saben cómo alcanzar la dirección IP del próximo salto.

Ejemplo:

A R1 se le informan las redes desde el Router fuera de su red. Para que R1 pueda alcanzar las redes tiene que dirigir el tráfico hacia la dirección 11.0.0.1, por lo tanto R1 puede llegar ya que se muestra en su tabla de enrutamiento como directamente conectada.

R1 le informa vía IBGP a R4 las redes de los AS fuera de su red. Entonces R4 para poder alcanzar esas redes debe dirigir el tráfico a 11.0.0.1, y como R4 no la posee directamente conectada como R1, debe tratar de alcanzarla utilizando un protocolo de enrutamiento interno como EIGRP, OSPF, RIP o ruta estática.

Hay que tomar atención al momento de configurar el protocolo de enrutamiento IGP, ya que debe ser anunciada la red 11.0.0.0 y finalmente aplicar passive interface, ya que no es parte del sistema autónomo



También si no se desea utilizar un protocolo de enrutamiento para que los routers conozcan la dirección 11.0.0.1 se puede configurar el comando **#Neighbor dirección IP next-hop-self** en el router de borde. En dirección IP ingresamos la IP de los vecinos que poseemos conectados.

Es decir R1 le anuncia R4 que él será el próximo salto para alcanzar las redes anunciadas desde el router borde.

Next Hop para rutas directamente conectadas o redistribuidas

Cuando una red es conocida vía un IGP o se encuentra directamente conectada se muestra con next-hop 0.0.0.0, como vemos en el siguiente ejemplo:

```

R4(config-router)#do show ip bgp
BGP table version is 10, local router ID is 172.16.24.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop        Metric   LocPrf  Weight  Path
*-> 10.0.0.4/30    172.16.20.6    332800
*-> 10.0.0.8/30    0.0.0.0          0
*->i100.0.0.0/24   10.0.0.6          0
*-> 172.16.20.0/30 172.16.20.6    307200
*-> 172.16.20.4/30 0.0.0.0          0
*->i172.16.23.0/24 172.16.20.1    0
*-> 172.16.24.0/24 0.0.0.0          0
*->i172.16.25.0/24 172.16.20.6    0
*-> 200.0.0.0       10.0.0.10        0
                                         100      0      32768  ?      100 i
                                         0      100      0      32768  ?      200 i
R4(config-router)#

```

Peer groups

Se pueden crear peer groups para agrupar los vecinos que poseen iguales políticas, esto permite no tener que ingresar un comando por cada vecino al momento de aplicar las políticas.

Para configurarlo primero se debe crear el peer group, el nombre asignado al peer group tiene significancia local y no es enviado otros routers.

El comando para crear el peer group es:

```
Router(config-router)#neighbor peer-group-name peer-group
```

Asignar vecinos al grupo:

```
Router(config-router)#neighbor ip-address peer-group peer-group-name
```

Si se desea resetear las conexiones de vecinos en el grupo se debe ingresar el comando:

```
Router(config-router)#clear ip bgp peer-group peer-group-name
```

Si deseamos terminar la sesión para un vecino podemos aplicar el comando neighbor shutdown

Autenticación

BGP soporta Message digest 5 para la autenticación de sus vecinos. MD5 envía un hash el cual es creado usando la llave y un mensaje. El Hash es enviado envés de la llave, por lo tanto la llave nunca viaja por la red.

Para autenticar BGP, ambos vecinos deben poseer la misma configuración (contraseña) y su respectiva dirección IP del vecino.

Para autenticar un vecino se debe ingresar la siguiente configuración en BGP:

Ejemplo

```
#Neighbor dirección ip password contraseña
```

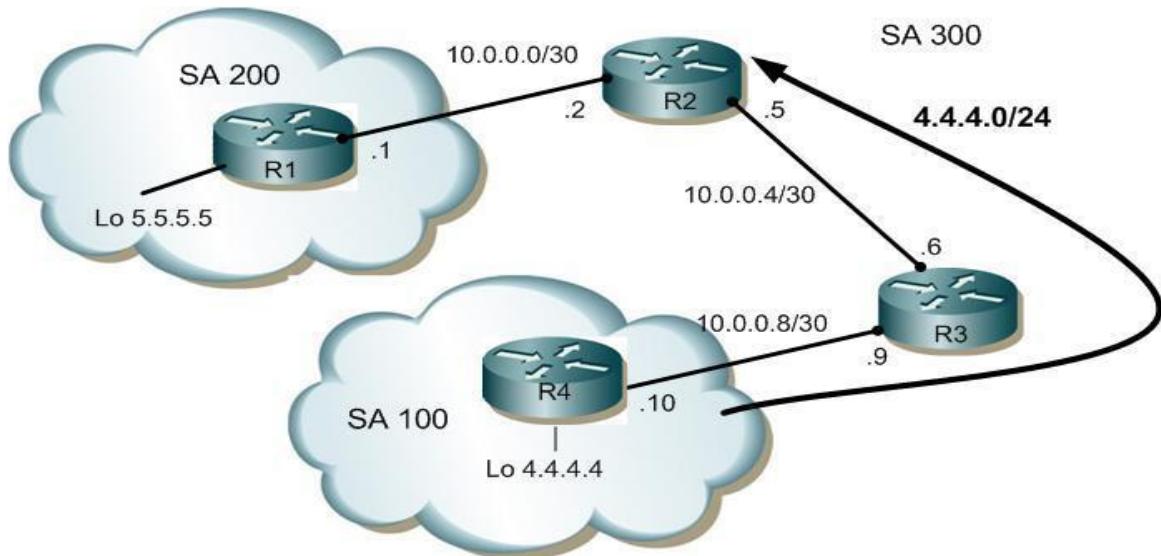
Dirección IP del vecino que se desea autenticar y contraseña

Filtro de rutas con lista de distribución

Los filtros de rutas se utilizan para evitar enviar redes a lugares que no se desean. Por ejemplo evitar enviar una red fuera del sistema autónomo de la Empresa.

Ejemplo

Primero se debe crear una Access list que indique las direcciones de las redes que se desean permitir o que se desean denegar. Por ejemplo:



Configuración Filtro con lista de distribución

Access list, deniega la red

R(config)#Access-list 1 deny red wildcard

R(config)#Access-list 1 permit any

Aplicar el filtro

R(config-router)#Neighbor IP_neighor distribute-list 1 out

Si R2 desea filtrar la red 4.4.4.0/24 para que no sea aprendida por R1 se debe configurar lo siguiente:

#Access-list 1 deny 4.4.4.0 0.0.0.255 ← Para denegar la red

#Access-list 1 permit any ← Para permitir todas las demás redes y así no denegarlas todas.

Aplicar el filtro

#Neighbor 10.0.0.1 distribute-list 1 out ← Dirección del vecino que no se desea que aprenda las redes.
Se aplica la lista de distribución de salida (out).

Comandos de verificación de BGP

Identificando atributos

Para identificar los atributos de las rutas aprendidas vía BGP, utilizamos el comando **show ip bgp**.

```
R3#show ip bgp
```

```
BGP table version is 6, local router ID is 172.16.20.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
* i10.0.0.0/30	10.0.0.10	0	100	0	200 i
*>i	10.0.0.6	0	100	0	100 i

Se pueden identificar:

Origin code
Next-Hop
Metrica
Local Preference
Weight
AS-PATH

Identificar la mejor ruta:

El signo > identifica cual es la mejor ruta cuando se posee más de un camino.
I= via comando network origin code
?= redistribucion origin code

Comprobando mejor ruta

El comando **show ip bgp dirección_de_red** nos permite identificar los valores de los atributos, para la sección de la mejor ruta, cuando existe más de un camino hacia el destino. A continuación veremos un ejemplo para la red 10.0.0.0 de la topología de ejemplo.

```
R3#show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/30, version 6
Paths: (2 available, best #2, table Default-IP-Routing-Table)
Flag: 0x820
    Not advertised to any peer
    200
        10.0.0.10 (metric 307200) from 172.16.20.5 (172.16.20.5)
            Origin IGP, metric 0, localpref 100, valid, internal
    100
        10.0.0.6 (metric 307200) from 172.16.20.1 (172.16.20.1)
            Origin IGP, metric 0, localpref 100, valid, internal, best
```

CAPITULO 6

Introducción a MPLS

MPLS (MultiProtocol Label Switching) es un protocolo de conmutación por etiquetas definido para funcionar sobre múltiples protocolos como Sonet, Frame Relay, ATM, Ethernet o cualquiera sobre el que pueda funcionar PPP. Las principales motivaciones para su desarrollo son la ingeniería de tráfico, la diferenciación de clases de servicio, y las redes privadas virtuales (VPN). En un principio, también proporcionaba una mayor velocidad puesto que los routers sólo deben mirar la etiqueta para conmutar y no leer la cabecera de la capa 3 para después decidir por dónde enrutar en función del destino y/u otros parámetros. Sin embargo, hay tecnologías que han conseguido aumentar la velocidad de los routers para consultar las tablas de enrutamiento (como ASIC).

Las ventajas que llevaron a desarrollar ATM: uso de conmutadores ATM más rápidos porque funcionaban con etiquetas, el poder ofrecer ingeniería de tráfico mediante circuitos virtuales... llevan a desarrollar MPLS unos años más tarde, basándose en la idea de las etiquetas, pero reduciendo la complejidad de las redes IP sobre ATM y mejorando la funcionalidad en algunos casos. IP sobre ATM conseguía aprovecharse de la velocidad que proporcionaban los conmutadores ATM para unir los routers IP, pero seguían siendo dos redes separadas (complejo de gestionar), y el número de circuitos virtuales aumenta mucho con el tamaño de la red. Varios fabricantes intentaron mejorar esto proponiendo soluciones mediante etiquetas que separasen las funciones de routing (encaminamiento, control de por dónde se envían los paquetes) de las de forwarding (reenvío en sí). El problema ahora es que eran incompatibles entre sí. MPLS es un intento de estandarizar estas soluciones.

MPLS aprovecha lo mejor de la capa 2, la rápida conmutación, sin perder de vista la capa 3, para no perder sus posibilidades. Esto se consigue separando de verdad la función de conmutación de la de enrutamiento. MPLS hace más viable la ingeniería de tráfico, permite enrutamiento rápido (porque en realidad hace conmutación, pero con información de enrutado), permite que los equipos de reenvío sean más baratos si sólo deben entender paquetes etiquetados, permite ofrecer QoS basándose en diferentes CoS (clases de servicio), hace más fáciles y flexibles las VPN (redes privadas virtuales), y además parece el primer paso para conseguir redes totalmente ópticas (ya que decidimos por dónde enviar el paquete según lo que diga la etiqueta y no hace falta procesar la cabecera de orden 3; es decir, aunque las decisiones del enrutado sean en el dominio eléctrico, la conmutación podría ser óptica).

MPLS utiliza los campos para etiquetas de ATM o Frame Relay, o añade una cabecera para el resto de protocolos entre la del nivel 3 y la del nivel 2. La diferencia con IP sobre ATM es que no tenemos una red diferente que nos proporciona conexión entre routers IP, sino que los niveles están integrados, y las funciones de encaminamiento y reenvío separadas pero coordinadas. Hay una parte de control, que se encarga de las decisiones de encaminamiento, pero no construye una tabla en la que consultar la dirección IP de los paquetes que lleguen, sino que informa a la parte de reenvío, que construye una tabla con etiquetas; así no es necesario mirar la cabecera de la capa 3, y decidir para cada paquete, porque la decisión ya está tomada para cada etiqueta. El único router que tiene que hacer funciones de enrutamiento es el primero, que tiene que decidir qué etiqueta coloca a cada paquete. Todos los paquetes que llevan la misma etiqueta forman un grupo que se denomina Forwarding Equivalent Class (FEC).

En los últimos años se han desarrollado diferentes tecnologías y se han puesto al servicio de las empresas para que éstas puedan mezclar la alta velocidad de operación de ATM basada en Comutación con el proceso de enrutamiento IP de Internet de la capa de Red. Estas tecnologías son:

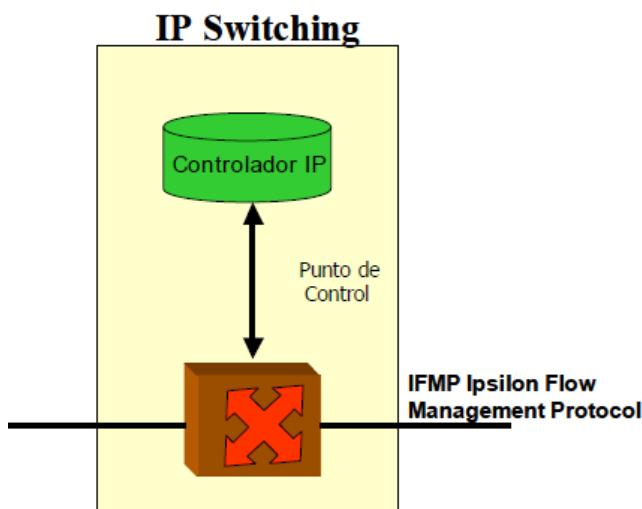
CELL SWITCHING ROUTER (CSR).

Fue desarrollado por Toshiba y presentado a la **IETF (Internet Engineering Task Force)** en 1994. “Esta tecnología se fundamenta en la utilización de los protocolos de encaminamiento IP para controlar infraestructura ATM. CSR se ha desarrollado en redes comerciales y académicas en Japón

IP SWITCHING.

Desarrollado por Ípsilon Networks en 1996, el objetivo básico de IP Switching fue el de integrar comutadores ATM de una manera eficiente (eliminando el plano de control ATM), es decir la idea fue eliminar el software ATM orientado a conexión e implementar el ruteo IP sin conexión sobre el Hardware ATM basado en la clasificación de flujo”.

Un Switch IP es simplemente un enrutador IP encadenado con un Switch ATM, un software IP de ruteo, un controlador del hardware del Switch y clasificador de flujo el cual se encarga de decidir en qué momento se debe conmutar el flujo.

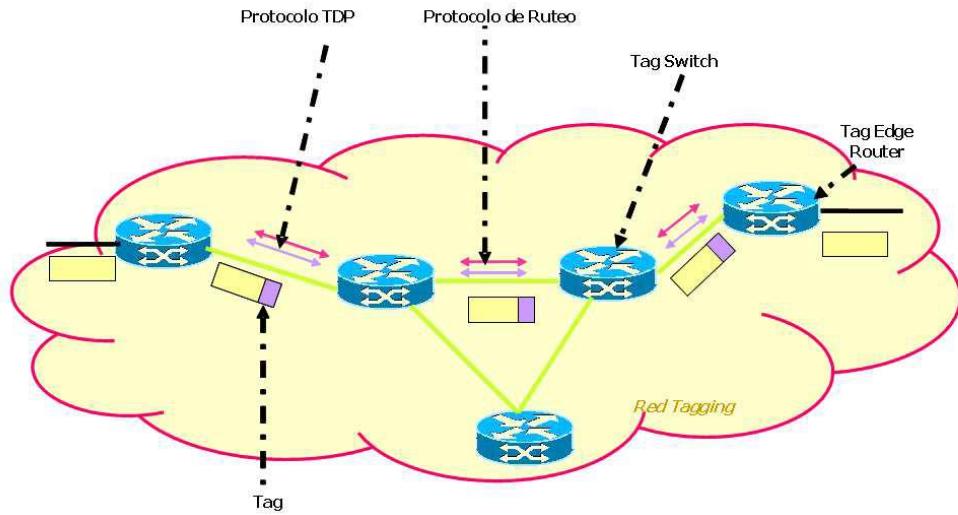


TAG SWITCHING.

Es la tecnología de conmutación de etiquetas desarrollada por Cisco System. A diferencia de las dos soluciones anteriores, Tag Switching es una técnica que no requiere de flujo de tráfico para la creación de tablas de etiqueta en un enrutador, en lugar de ésto utiliza protocolos de enrutamiento IP para determinar el siguiente salto.

Para Cisco el término etiqueta es identificado como Tag, es decir, no se utiliza el término Label. Este tipo de tecnología cuenta con los siguientes elementos:

- Tag Edge Routers: Estos Routers son los que aplican los “Tag” (Etiquetas) a los paquetes en el borde de la Red.
- Tag Switches: Comutan paquetes o celdas basados en “Tags” (Etiquetas).
- Tag Distribution Protocol (TDP): Éste es el protocolo encargado de la distribución de la información de etiquetas en la red.



Esta tecnología basa su enrutamiento en protocolos de ruteo estándares como lo son OSPF, IS-IS, para indicar las rutas de red, las cuales al ser encontradas se les asigna una etiqueta igual que al paquete y se distribuye a todos los nodos con el protocolo de distribución TDP.

Cuando un paquete llega a un Tag Edge Router se analiza el encabezado de la capa de red, aplica los servicios de red (seguridad, QoS), selecciona una ruta de sus tablas y aplica una etiqueta al paquete para ser enviado al siguiente Tag Switch, este Tag Switch recibe el paquete y lo conmuta en función de la etiqueta sin analizar el encabezado de capa 3, finalmente el paquete llega al Tag Router de salida, donde se elimina la etiqueta y se envía el paquete a su destino final.

Estructuras

Los routers que conmutan mediante etiquetas se llaman LabelSwitching Router (LSR). Estos contienen una relación en la que a una etiqueta entrante se asigna una etiqueta saliente y un interfaz de salida. En realidad, ésta información está dividida en dos estructuras:

- Incoming Label Map (ILM): Contiene en cada entrada la etiqueta, un código para saber el tratamiento que tiene que recibir el paquete y la FEC a la que pertenece. Cuando llega un paquete, se extrae su etiqueta y se mira en la lista qué hay que hacer con él.
- Next Hop Label Forwarding Entry (NHLFE): Contiene la etiqueta y el interfaz de salida e información sobre el siguiente salto. Cuando tenemos un paquete en el router que hay que enviar, se crea la nueva cabecera con la nueva etiqueta y se envía al siguiente salto por el interfaz de salida.
- Hay una tercera estructura que sólo se encuentra en el router de entrada a la red MPLS, que relaciona cada FEC con una etiqueta (hace las veces del ILM para el primer router, pero al primer LSR los paquetes le llegan sin etiquetar), se llama FEC to NHLFE (FTN). Contiene FEC y entrada NHLFE. Cuando llega un paquete hay que decidir a qué FEC pertenece, y enviarlo a la entrada NHLFE correspondiente.

MPLS e IP

Es importante comprender las diferencias entre la manera en que MPLS y el enrutamiento IP envían datos a través de una red. El envío de paquetes IP tradicional usa la dirección IP destino ubicado en la cabecera del paquete para realizar una decisión de envío independiente en cada Router de la red. Estas decisiones salto a salto son basadas en protocolos de enrutamiento de capa red, tales como OSPF o BGP, los mismos que buscan la ruta más corta a través de la red para llegar al destino. MPLS crea un modelo overlay basado en conexión dentro de las tradicionales redes enrutadas IP no orientadas a conexión. Esta

arquitectura orientada a conexión da apertura a nuevas posibilidades de administración de tráfico en una red IP

ARQUITECTURA MPLS

La arquitectura MPLS describe los mecanismos para realizar la conmutación de etiquetas, que combina los beneficios del envío de paquetes basados en la conmutación de Capa 2 con los beneficios del enrutamiento de Capa 3.

En el envío de paquetes tradicional, con los ambientes de red no orientados a conexión típicos del protocolo IP, el enrutamiento de cada paquete se analiza salto por salto, se chequea su encabezamiento de capa 3, y se toma una decisión de envío independiente basada en la información extraída desde algoritmos de enrutamiento de la capa de red. En MPLS, al ser una arquitectura orientada a conexión, la transmisión de los datos ocurre en las trayectorias establecidas por la operación de intercambio de etiquetas denominadas caminos de etiquetas conmutados (LSPs, Label Switched Path)

Para distribuir las etiquetas en una red que emplee MPLS se emplea el protocolo de distribución de etiqueta (LDP, Label Distribution Protocol) o el protocolo de reserva de recursos (RSVP, Resource Reservation Protocol). Cada paquete encapsula y porta las etiquetas durante su transporte dentro de esta red.

Es posible alcanzar altas velocidades en la conmutación de datos porque las etiquetas, que poseen una longitud fija, son insertadas al comienzo del paquete o celda y son usadas para la conmutación y reenvío con acciones exclusivas de la capa 2, que en caso de ATM son ejecutadas por hardware. MPLS realiza las siguientes funciones:

- Especifica mecanismos para administrar flujos de diferentes tráficos entre diferentes hardwares, máquinas, o flujos entre diferentes aplicaciones.
- Mantiene independientes los protocolos de la capa 2 y de la capa 3.
- Provee un medio para relacionar direcciones IP con simples etiquetas de longitud fija usadas por diferentes tecnologías de conmutación y enrutamiento de paquetes.
- Relaciona protocolos existentes (como RSVP y OSPF).
- Establece la transferencia de datagramas IP sobre cualquier tecnología o estándar de transporte desde Frame Relay a 10 Gigabit Ethernet.

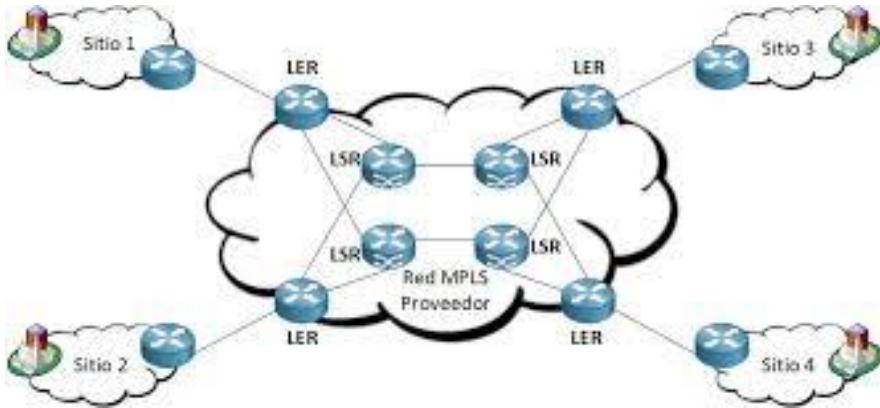
Componentes.

Cuando se diseña una red con arquitectura MPLS se debe tener en cuenta que como sistema comprende tres conceptos fundamentales:

1. Enrutador de Conmutación de Etiquetas (LSR, Label Switching Router)
2. Trayectoria de Conmutación de Etiqueta (LSP, Label Switched Path)
3. Paquetes Etiquetados (LP, Labeled Packets).

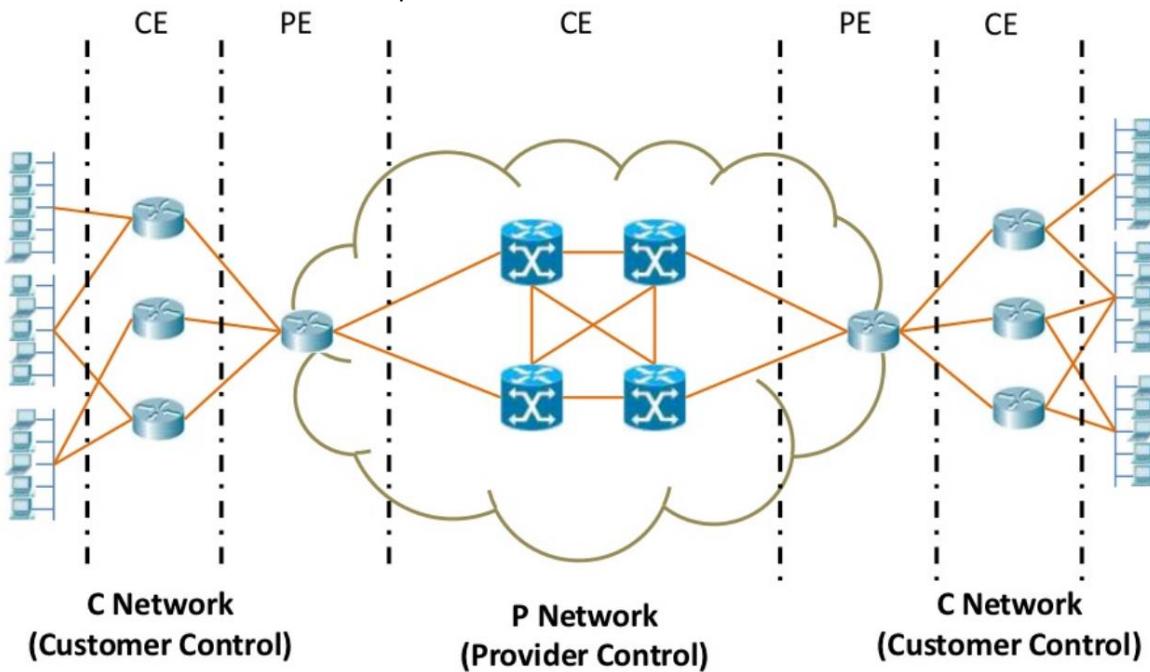
En su forma más simple un sistema MPLS es un conjunto de LSR que envían paquetes etiquetados a través de los LSP. Los Routers de Conmutación de Etiquetas (LSR) y los Routers de Etiqueta de Borde (LER) son los nodos principales que componen una red MPLS. Los dos son físicamente el mismo dispositivo, un Router o un switch de red troncal que incorpora el software MPLS, siendo el administrador el que lo configura para cualquiera de los dos modos de trabajo.

Haciendo referencia a la Figura, se realiza la descripción de los conceptos y componentes que integran la arquitectura MPLS.



Desde el punto de vista del proveedor de servicios se puede definir los componentes como

- C Network. Redes del cliente
- P Network Backbone del proveedor



Dominio MPLS: Es la porción de la red donde los procedimientos de enruteamiento y de envío están acorde al protocolo MPLS.

Enrutador de commutación de etiquetas (LSR, Label Switched Router): Es un enrutador de alta velocidad en el corazón de la red MPLS, el cual debe soportar los protocolos de enruteamiento IP y participa en el establecimiento de las trayectorias de intercambio de etiquetas (LSP, Label Switched Paths) utilizando el protocolo de señalización de etiquetas adecuado. Permite commutación de tráfico de datos a alta velocidad basado en las trayectorias establecidas. Además, los enrutadores LSR en MPLS se clasifican en base a la dirección del flujo de datos, como enrutadores ascendentes upstream o descendentes downstream. También se conoce como enrutador del interior del Dominio MPLS

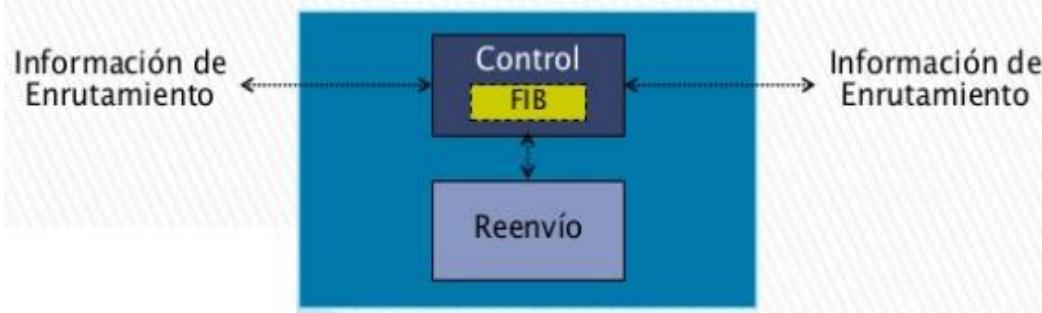
Enrutador de borde, de entrada o salida (LER, Label Edge Router): Es un dispositivo que opera en la periferia de la red de acceso y la red MPLS, el cual se encarga de insertar las etiquetas en base a la información de enruteamiento. Como otro elemento básico aparece la Clase de Equivalencia de Reenvío (FEC Forward Equivalent Class) que define un conjunto de paquetes que comparten los mismos atributos y reciben el mismo tratamiento durante su transporte, aun cuando el destino final de cada paquete sea

diferente. La asignación de un paquete a una FEC en particular se realiza una sola vez, en el momento que el paquete entra a la red.

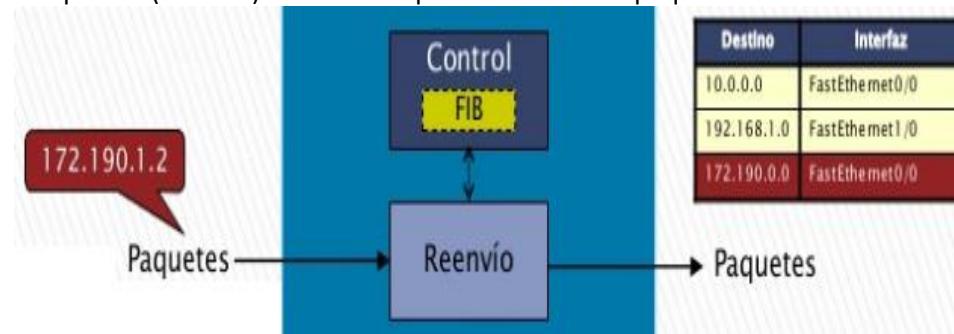
Componentes de Envío y Control:

La arquitectura MPLS se divide en dos componentes separados:

- **Componente de Control.**- También denominado plano de Control. Es el responsable de la creación y mantenimiento de la información de envío de etiquetas (denominadas también enlaces) entre un grupo de switches de etiquetas interconectados. Es donde se realiza el intercambio de la información de control (llevado a cabo por protocolos de enrutamiento (por ejemplo OSPF o IS-IS)) funcionando en conjunto con procedimientos MPLS de asignación y distribución de etiquetas entre un grupo de LSR interconectados

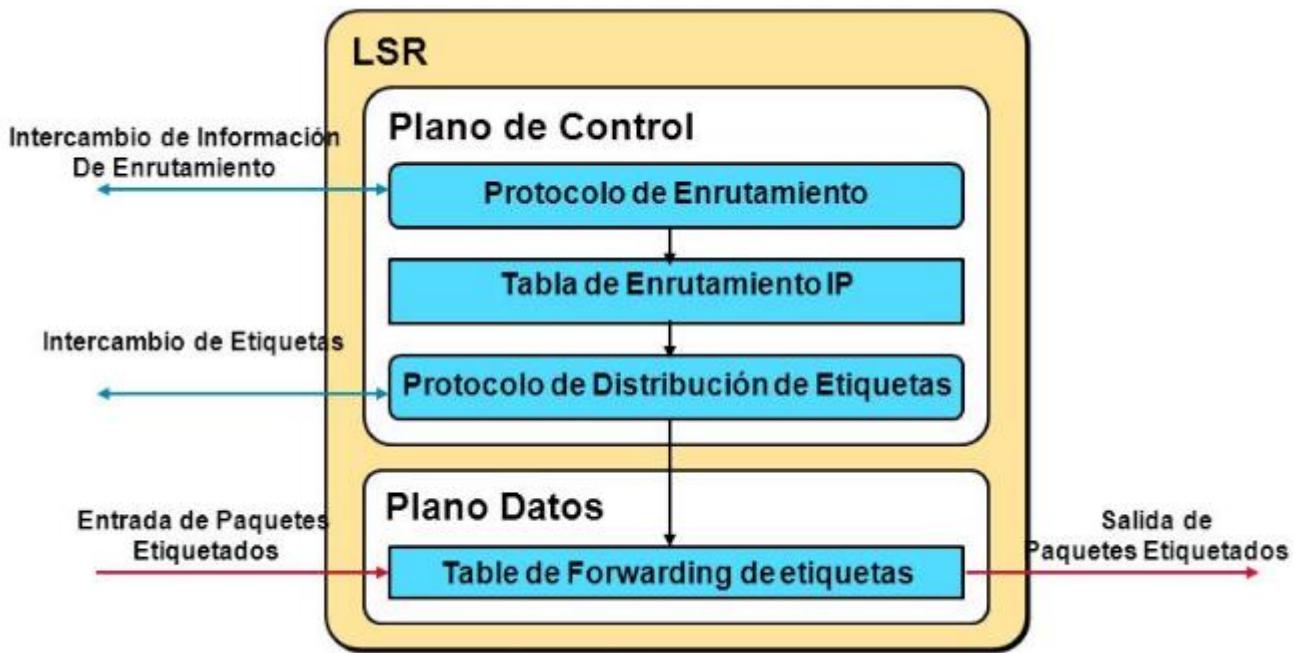


- **Componente de envío (Forwarding) .-** También denominado plano de datos, emplea una base de datos de envío de etiquetas mantenida por una comutación de etiquetas, para ejecutar el envío de paquetes de datos basándose en las etiquetas transportadas por los paquetes.
 - El componente de envío utiliza la información de la componente de control para la construcción de las tablas de envío de etiquetas, en las cuales se realiza el envío de los paquetes.
 - Extrae la cabecera del paquete IP de destino.
 - Usa el algoritmo de emparejamiento del prefijo más largo para encontrar un prefijo en la FIB que corresponda a la dirección IP destino. Obtiene de la FIB el puerto (Interfaz) de salida al que debe enviar el paquete

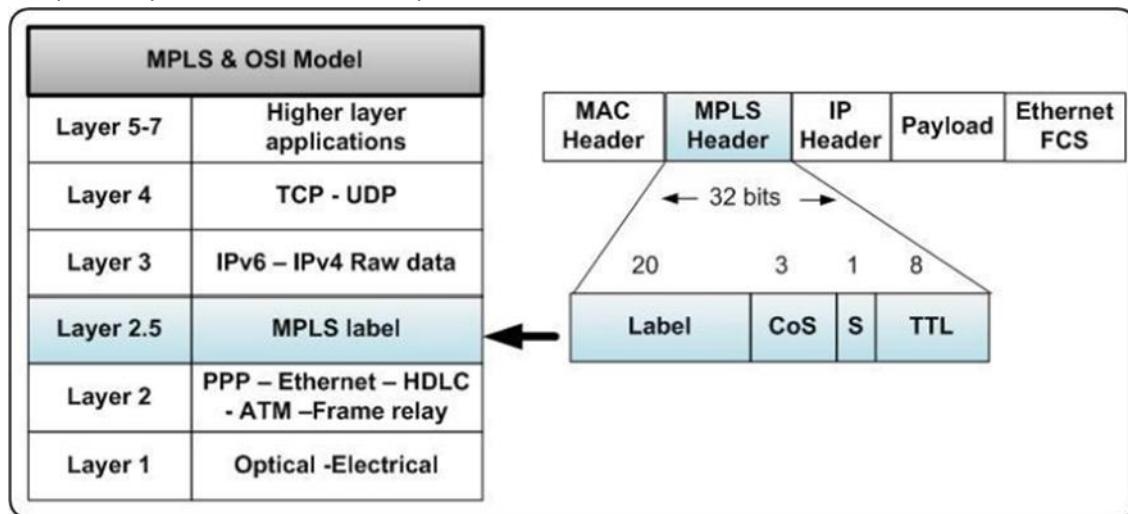


En cada nodo MPLS se deben ejecutar uno o varios protocolos de enrutamiento IP para intercambiar la información de enrutamiento IP con otros nodos MPLS de la red.

En este sentido, cada nodo MPLS es un router IP en el plano de control



Etiquetas y Asociación de Etiquetas.



Una etiqueta es un identificador corto de longitud fija de 4 octetos (32 bits) y de significado local el cual es utilizado para identificar un FEC.

Un FEC es el conjunto de las direcciones IP que corresponden al mismo prefijo. Los paquetes IP que pertenecen a la misma FEC tienen el mismo puerto (Interface) de salida.

La etiqueta que se coloca en un paquete particular representa a dicho FEC al cual el paquete es asignado.

Una etiqueta, en su forma simple, identifica la trayectoria que debe seguir un paquete por el dominio MPLS.

En una red IP, la asignación de un paquete a una FEC se hace en cada router buscando su dirección en la tabla de enrutamiento.

Formato genérico de la etiqueta MPLS.

Bits →	20	3	1	8
	Etiqueta	Exp	S	TTL

La distribución de los 4 Octetos (32 bits) de la cabecera MPLS es la siguiente:

- Los primeros 20bits son el valor de la etiqueta. Sin embargo, los primeros 16 valores están exentos del uso normal, es decir, que tienen un significado especial.
- Le siguen 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS, Class of Service), puede emplearse para marcar paquetes para diferenciar el tratamiento en el envío, quizás basado en el marcado de Diff-Serv en paquetes IP entrantes.
- A continuación 1 bit de stack para poder agrupar etiquetas de forma jerárquica (S).
- Y por último 8 bits utilizados para Tiempo de Vida (TTL). Este TTL tiene la misma función que el TTL en el encabezado IP.

Las especificaciones del (IETF, Internet Engineering Task Force) definen que MPLS funciona sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc.

Por ello, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (por ejemplo, enlaces PPP o LAN) se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del nivel 3 como se observa en la Figura siguiente.

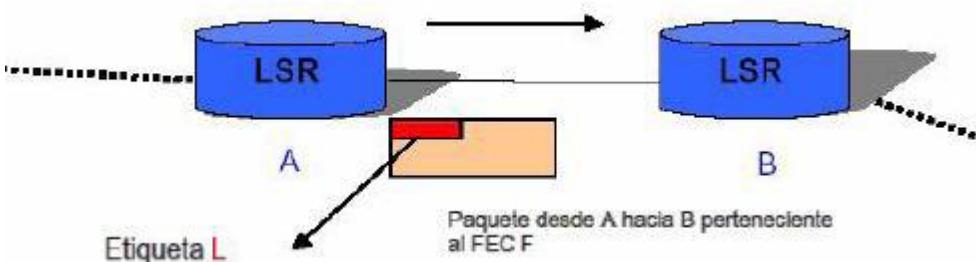
Sin embargo, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos para las etiquetas

De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP en el momento de extender su red

A partir de que el paquete ha sido clasificado dentro de un nuevo FEC o un FEC existente, se le asigna una etiqueta a este paquete. Comúnmente un paquete es asignado a un FEC basado (completamente o parcialmente) en su dirección de destino de la capa de red, y es importante señalar que la etiqueta nunca es una codificación de esa dirección.

Los paquetes entonces se envían basados en sus valores de etiquetas. El enrutador que lo recibe examina el paquete para ver el contenido de la etiqueta y determina el próximo salto y este paquete será procesado de esta forma hasta que el paquete abandona el dominio MPLS, es decir, el envío de este paquete se basa en el intercambio de etiquetas.

De esta forma, si se tienen dos LSR uno A y otro B como se muestra a continuación, ambos enrutadores estarán de acuerdo en que, cuando A transmite un paquete hacia B, el enrutador A etiquetará el paquete con una etiqueta con el valor L si y solo si el paquete es miembro de la FEC F (Caso particular para este ejemplo).



Por lo que ambos estarán de acuerdo en asociar la etiqueta L y el FEC F para paquetes que se mueven de A hacia B. Con este acuerdo, L se convierte en la etiqueta de salida de A representando el FEC F y L se convierte en la etiqueta de entrada que representa el FEC F en B.

Se debe notar que L no necesariamente representa el FEC F para todos los paquetes sino, para los que han sido enviados desde A hacia B, por lo que L es un valor arbitrario en el cual su asociación con F es local entre A y B. **Las etiquetas MPLS tienen un significado local.**

Dentro de la red NO es necesario analizar la cabecera del paquete. En cada router la etiqueta es usada como un índice en una tabla (**LFIB Label Forward Information Base**) que indica el próximo salto y la nueva etiqueta

Las tablas de enrutamiento de etiquetas LFIB han sido configuradas mediante protocolos de distribución de etiquetas

Durante la asignación de la etiqueta se emplea uno de los siguientes criterios de transporte:

- Destino de enrutamiento Unicast (punto-punto).
- Destino de enrutamiento Multicast (punto-multipunto).
- Ingeniería de Tráfico
- Calidad de Servicio (QoS)
- Red Privada Virtual (VPN).

Ventajas del reenvío basada en etiquetas

Puede realizarse con switch de baja capacidad

La asignación del FEC puede realizarse basada en cualquier información disponible sobre el paquete, incluso si no está en la cabecera

Los criterios para asignar la FEC pueden llegar a ser muy complejos sin afectar los routers

La etiqueta puede ser usada para indicar la ruta que debe seguir el paquete cuando pesa debe ser determinada a prior por razones de políticas o ingeniería de tráfico

Tablas de enrutamiento y envío.

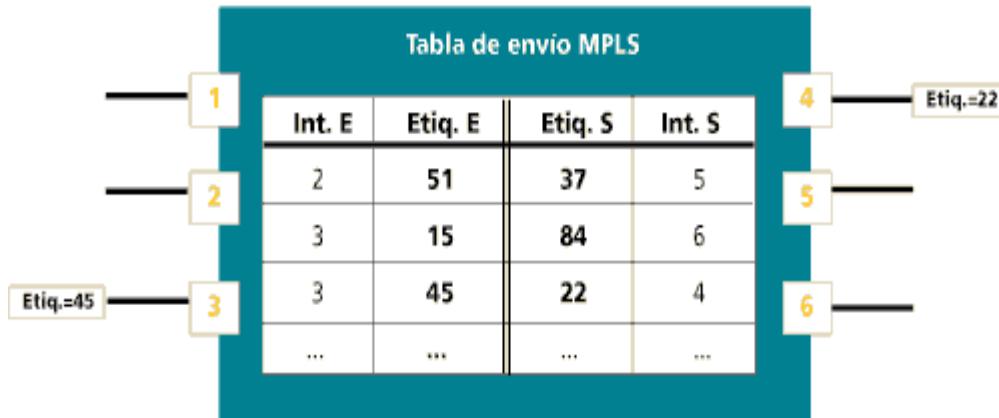
En la arquitectura MPLS en cada LSR se crean dos tablas, las cuales toman información relevante para la componente de envío. La primera, se conoce como base de información de etiqueta (LIB, Label Information Base). Esta tabla contiene todas las etiquetas asignadas por este LSR y los enlaces de estas etiquetas a etiquetas recibidas desde cualquier LSR vecino.

Estos enlaces son utilizados para construir las entradas a la base de información de envío (FIB). En la Figura se muestra como ejemplo una tabla de la base de datos de etiquetas.

No todas las etiquetas dentro de la tabla LIB se necesitan utilizar para el envío del paquete, ya que múltiples LSR vecinos pueden enviar etiquetas para el mismo prefijo IP, pero puede que el salto IP real no se encuentre en uso en la tabla de enrutamiento hacia el destino.

La segunda tabla conocida como base de información de envío de etiqueta (FLIB, Forward Label Information Base), se emplea durante el envío de paquetes y contiene sólo las etiquetas que están siendo utilizadas por la componente de envío de MPLS. FLIB es el equivalente MPLS de la matriz de conmutación de un conmutador ATM

LSR



Creación y clasificación de etiquetas.

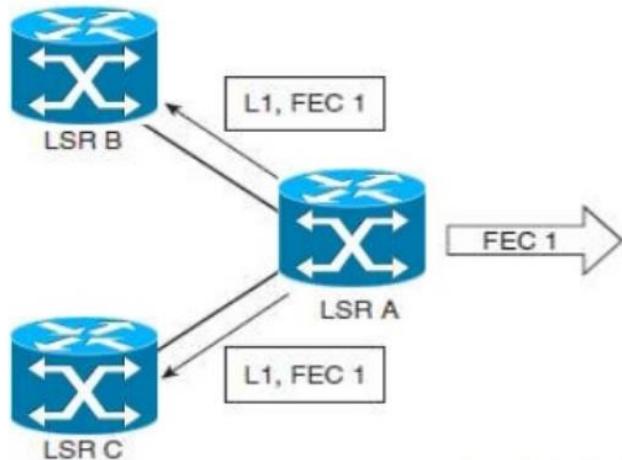
En la creación de etiquetas se pueden emplear los siguientes métodos:

- **Método basado en la topología:** utiliza el procesamiento normal de los protocolos de enrutamiento (tales como OSPF y BGP) (J.M, 2006, Aziz et al., 2002).
- **Método basado en solicitud:** utiliza el procesamiento de control de tráfico basado en solicitud (tal como RSVP) (Aziz et al., 2002).
- **Método basado en tráfico:** utiliza la recepción de un paquete para activar la asignación y distribución de etiqueta.

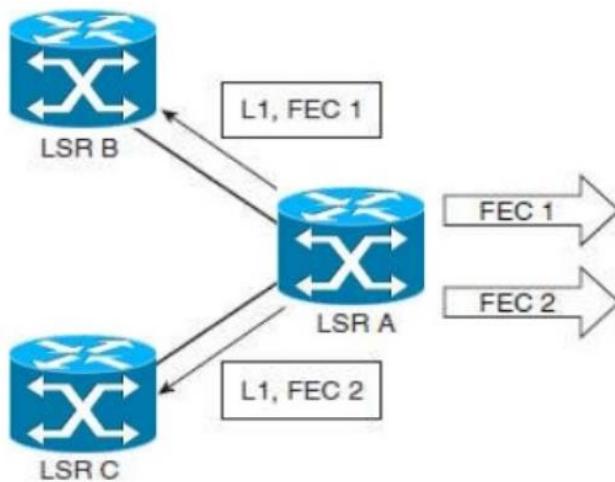
Clasificación de etiquetas:

Las etiquetas utilizadas por un LSR para la unión del FEC se clasifican de la siguiente forma:

Por plataforma: los valores empleados son únicos dentro de todo el LSR. Las etiquetas son asignadas de una fuente común, no hay dos etiquetas distribuidas en interfaces diferentes que se repitan.



Por interfaz: los rangos de etiqueta están asociados con interfaces y las etiquetas suministradas a estas interfaces son asignadas por fuentes diferentes. Los valores de etiquetas suministrados a interfaces diferentes pueden ser los mismos.



Distribución de etiquetas.

La arquitectura MPLS permite varios métodos de distribución de señalización de etiqueta. Los protocolos de enrutamiento existentes como BGP han sido mejorados para portar la información de etiqueta dentro del contenido del protocolo.

El RSVP se extendió para soportar el intercambio de etiquetas. Además el (IETF: *Internet Engineering Task Force*) también definió un nuevo protocolo conocido como Protocolo de Distribución de Etiquetas (*LDP, Label Distribution Protocol*) para señalización explícita e intercambio de espacio de etiqueta. Para soportar enrutamiento explícito basado en los requisitos de QoS y CoS se definieron extensiones del protocolo base LDP. Estas extensiones están comprendidas en la definición del protocolo LDP en el enrutamiento basado en la necesidad (*CR-LDP, Constraint-Based Routing Label Distribution Protocol*).

Existen dos modos para la distribución de etiquetas en MPLS:

- **Distribución de etiqueta en demanda hacia atrás:** en este modo, los enlaces de etiquetas se entregan al LSR anterior solo si ha ocurrido una solicitud.
- **Distribución de etiqueta no solicitada hacia atrás:** en este modo, los enlaces de etiqueta se entregan sin considerar si los otros LSR necesitan la etiqueta. Esto puede realizarse al menos una vez durante el tiempo de vida de una relación entre LSRs adyacentes.

Según los esquemas que existen en la distribución de etiquetas se pueden resumir como sigue:

- LDP, enlaza distintos IP *unicast* a etiquetas
- RSVP y CR-LDP, se emplea para ingeniería de tráfico y reserva de recursos.
- Protocolo independiente *multicast* (*PIM, Protocol Independent Multicast*), se utiliza para enlazar etiquetas a estados *multicast*.
- BGP, se emplea para etiquetas externas (VPN).

El modo de Distribución de etiquetas es utilizado dependiendo de la interfaz y aplicación. **Asignación de etiquetas.**

MPLS define dos modos para la asignación de etiquetas a LSR vecinos:

- **Modo Independiente:** en este modo un LSR reconoce un FEC particular y toma la decisión de asociar una etiqueta a un FEC y de distribuir esta asociación a sus pares de distribución de etiqueta.

- **Modo Ordenado:** en este modo un LSR asocia una etiqueta a un FEC particular si y solo si es el enrutador de salida o si ha recibido una asociación de etiqueta para el FEC de su siguiente salto (LSR).

En MPLS se definen de dos modos el tratamiento para ataduras de etiquetas recibidas de diferentes LSR:

- **Modo Conservativo:** En este modo las asociaciones entre un FEC y una etiqueta recibidas de un LSR que no son el próximo salto para un FEC dado son descartadas. Este modo requiere que el LSR mantenga pocas etiquetas. Este modo es recomendado para ATM-LSR y hace un mejor uso de la memoria disponible del router.
- **Modo Liberal:** En este modo se retienen las asociaciones entre una etiqueta y un FEC recibidas de LSR que no son el próximo salto para un FEC determinado.

Este modo permite una adaptación más rápida a los cambios en la topología y permite el envío de tráfico a diferentes LSP en caso de cambios.

En la arquitectura MPLS la decisión de asociar una etiqueta particular a un FEC particular es tomada por el LSR que es descendente con respecto a esta asociación. El enrutador descendente debe informar al enrutador ascendente de dicha asociación, por lo que la asociación es distribuida en la dirección “descendente-ascendente” donde el enrutador A es ascendente con relación al enrutador B. Además cuando un enrutador recibe un paquete etiquetado con una etiqueta particular de entrada, pero no tiene ninguna asociación para esta etiqueta, este paquete debe ser descartado.

[Unión de etiquetas.](#)

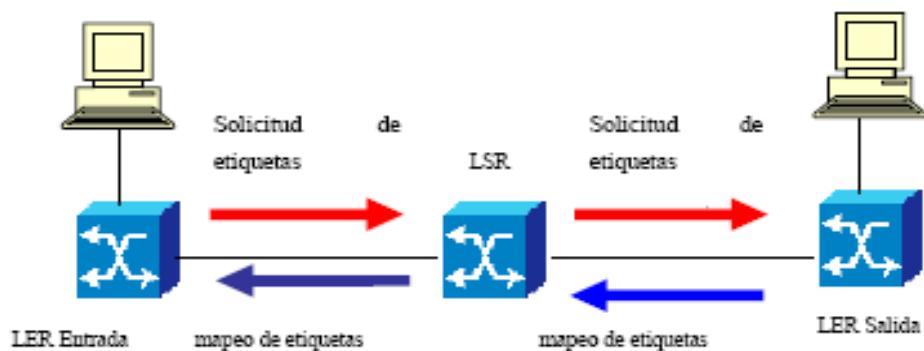
El flujo de tráfico entrante de diferentes interfaces puede ser fusionado y conmutado utilizando una etiqueta común, si su viaje por la red es hacia el mismo destino y comparten los mismos requisitos para su transporte a esto se le conoce como fusión de cadenas o agregación de flujo.

[Pila de etiquetas.](#)

El mecanismo de pila de etiqueta permite operaciones jerárquicas en el dominio MPLS. Es la combinación de dos o más encabezamientos de etiquetas asociados a un simple paquete. Este mecanismo permite que MPLS se emplee simultáneamente para enrutamiento multinivel donde cada nivel en una pila de etiquetas pertenece a algún nivel jerárquico, lo cual facilita el modo de operación de túnel en MPLS.

[Mecanismos de señalización.](#)

- **Solicitud de etiqueta:** Es el mecanismo que utiliza un LSR para que su LSR vecino le asigne una etiqueta, de esta forma él puede asociar esta etiqueta a un FEC específico. Este mecanismo se utiliza desde que el paquete entra por el LSR de entrada al dominio MPLS hasta que lo abandona por el LSR de salida.
- **Mapeo de etiqueta:** Como respuesta a la solicitud de etiqueta, un LSR enviará una etiqueta al LSR que la solicitó utilizando el mecanismo de mapeo. Los mecanismos de solicitud y mapeo de etiqueta se muestran en la siguiente figura



- **Protocolo de distribución de etiqueta (LDP):** Nuevo protocolo que adoptó el (*IETF: Internet Engineering Task Force*) en enero del 2001 (RFC 3036) y no es más que un conjunto de procedimientos con los cuales un LSR informa a otro de las asociaciones FEC-etiqueta que ha hecho. Para lograr estas asociaciones es necesaria la creación de los LSP. Las parejas de LSRs utilizando LDP, intercambian los tipos de mensajes siguientes:
 - **mensajes de descubrimiento:** anuncia y mantiene la presencia de un LSR en una red.
 - **mensajes de sesión:** establece, mantiene, y termina las sesiones entre LDP iguales.
 - **mensajes de advertencia:** crea, cambia, y borra enlaces de etiquetas para FECs.
 - **mensajes de notificación:** provee información de consulta e información de señal de error.

Imposición de etiquetas en el contorno de la red MPLS

La imposición de etiquetas es el acto de adición de una etiqueta a un paquete, cuando éste entra en el dominio MPLS. Se trata de una función de frontera o contorno, lo que quiere decir que los paquetes se etiquetan antes de enviarse al dominio MPLS.

Para desempeñar esta función, un LSR de contorno debe comprender dónde se ha encabezado el paquete y qué etiqueta, o pila de etiquetas, se debería asignar al paquete. En un envío de etiqueta de Capa 3 convencional, cada salto en la red realiza una consulta en la tabla de envíos IP para la dirección de destino IP almacenada en la cabecera de Capa 3 del paquete, selecciona una dirección IP de siguiente salto para el paquete en cada iteración de la consulta y, eventualmente, envía el paquete fuera de una interfaz hacia su destino final.

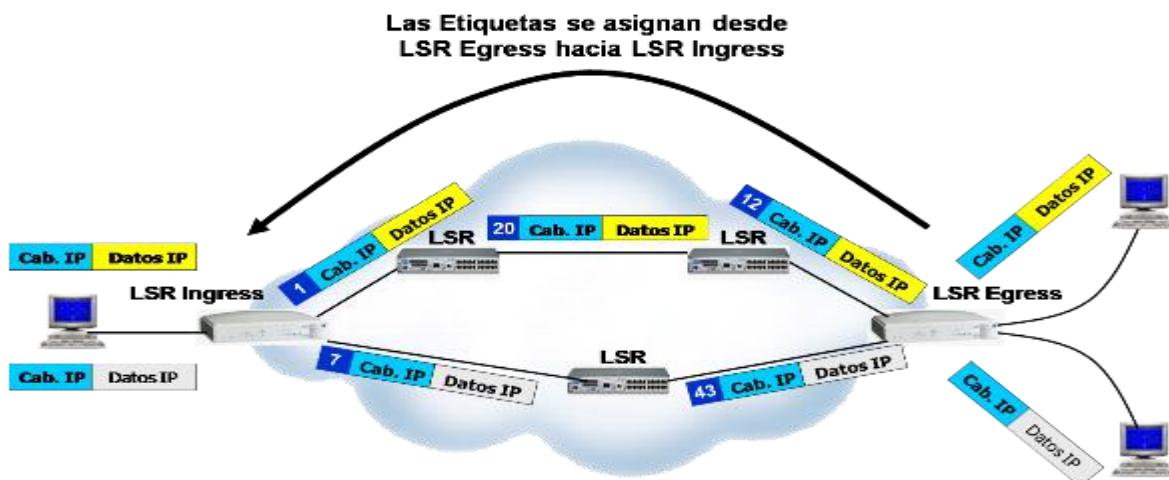
La elección para el siguiente salto del paquete IP es una combinación de dos funciones. La primera función separa el conjunto de paquetes posibles en un conjunto de prefijos de destino IP. La segunda función efectúa la asignación de cada prefijo de destino IP a una dirección IP del siguiente salto. Esto significa que cada destino en la red se alcanza mediante una ruta respecto al flujo de tráfico que va desde un dispositivo de entrada hasta el dispositivo de salida de destino (podrían habilitarse múltiples rutas si el equilibrado de la carga se realiza utilizando rutas de costo equivalente o rutas de costo desigual, como ocurre con algunos protocolos IGP, como, por ejemplo, OSPF, IS-IS, EIGRP).

Clases equivalentes de envío (FEC).-

En la arquitectura MPLS, los resultados de la primera función se conocen como **clases equivalentes de envío**, éstas vendrían a ser como un conjunto de paquetes IP que se envían de la misma manera, por la misma ruta y con idéntico tratamiento.

Una clase equivalente de envío podría corresponder a una subred de destino, pero también podría corresponder a cualquier clase de tráfico que un LSR de contorno considere significativa. Por ejemplo, todo el tráfico interactivo hacia un cierto destino o todo tráfico con un cierto valor de precedencia IP podría constituir una FEC. Otro ejemplo; una FEC puede ser un subconjunto de la tabla BGP, incluyendo todos los prefijos de destino alcanzables a través del mismo punto de salida.

Con el envío IP convencional, el procesamiento de paquetes se efectúa en cada salto en la red. No obstante, cuando se introduce MPLS, se asigna un paquete particular a una FEC particular una sola vez, y esto tiene lugar en el dispositivo de contorno a medida que el paquete entra en la red. La FEC a la que se asigna el paquete se codifica entonces como un identificador corto de longitud fija, conocido como etiqueta. Es decir la FEC a la que se asigna el paquete se codifica como un identificador fijo de corta longitud, conocido como una etiqueta. En la figura siguiente se ilustra el proceso de imposición de etiqueta



Enrutamiento MPLS

Todos los paquetes que entran a una red MPLS lo hacen por medio de un LSR de entrada y salen de la misma forma por medio de un LSR de salida. Este mecanismo crea una ruta comutada por etiqueta (LSP), que es esencialmente el conjunto de LSR que atraviesa el paquete desde el LSR de entrada hasta llegar al LSR de salida para una FEC particular. Esta LSP es unidireccional, lo que quiere decir que el tráfico de retorno desde una FEC determinada utilizará otra LSP.

La creación de la LSP es un esquema orientado a conexión porque la ruta se establece antes que cualquier flujo de tráfico. Sin embargo, el establecimiento de esta conexión se basa en información topológica más que en la necesidad de un flujo de tráfico. Esto significa que la ruta se crea independientemente de si en ese momento hay tráfico esperando a pasar por la ruta hacia un conjunto particular de FEC.

A medida que el paquete atraviesa la red MPLS, cada LSR intercambia la etiqueta entrante por otra de salida, parecido al mecanismo utilizado actualmente en ATM, donde el VPIA/CI se intercambia por un par VPIA/CI diferente cuando sale del switch ATM. El proceso es repetido hasta llegar al último LSR denominado LSR de salida.

El equivalente MPLS de la matriz de conmutación de un Switch ATM es la base de información de envío de etiquetas. La información relacionada con el componente de envío se almacena en dos tablas, cada LSR mantiene estas dos tablas.

La primera, es la **Base de información de etiquetas LIB en términos MPLS estándar**, mantiene todas las etiquetas asignadas por este LSR y las asignaciones de estas etiquetas a las etiquetas recibidas de cualquiera de los vecinos. Estas asignaciones de las etiquetas se distribuyen mediante el uso de protocolos de distribución de etiquetas.

Así como varios vecinos pueden enviar etiquetas para un mismo prefijo IP aunque pudiera no ser el siguiente salto IP actualmente en uso en la tabla de enrutamiento para el destino, no todas las etiquetas de la TIB/LIB deben utilizarse para el envío de paquetes.

La segunda tabla, conocida como **Base de información de envío de etiquetas LFIB en términos MPLS estándar**, se utiliza durante el envío de paquetes y almacena sólo las etiquetas que en ese momento está usando el componente de envío MPLS.

Las figuras a y b muestran un LSR de contorno en términos MPLS estándar y en términos del IOS de cisco y de la terminología del Envío expreso de Cisco (CEF) (se eligió un LSR de contorno ya que su función es un superconjunto de un LSR que no es de contorno).

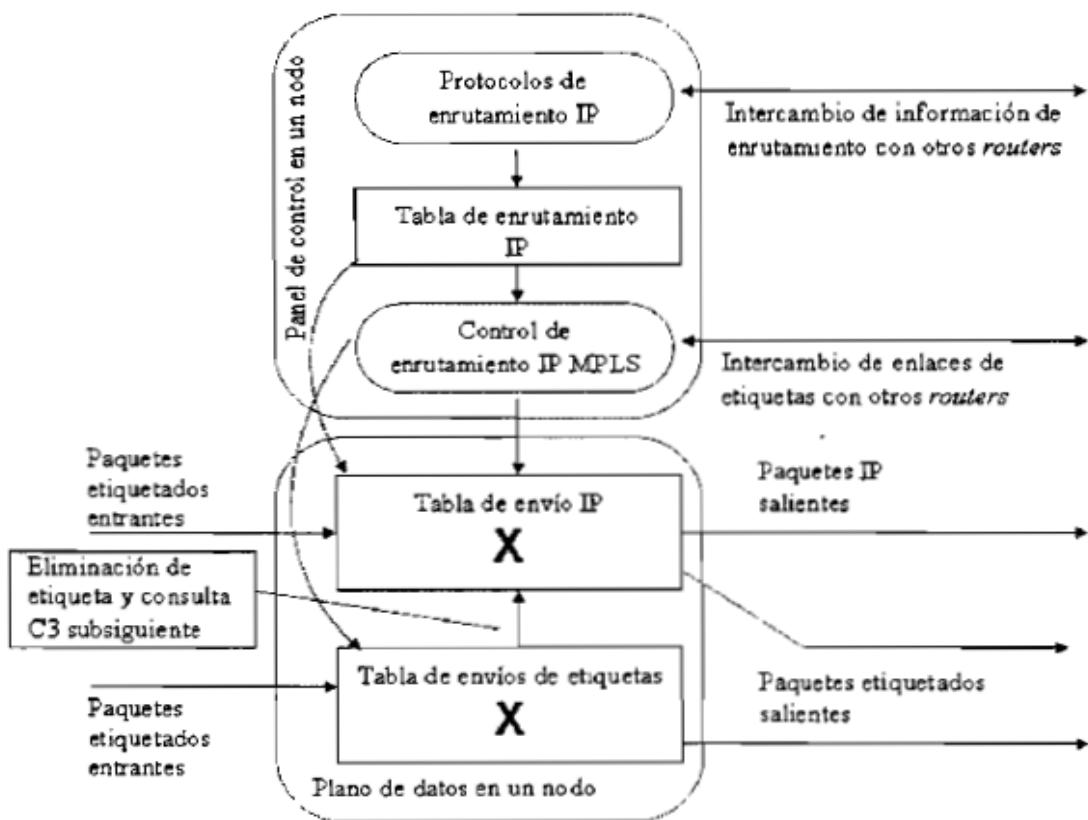


Figura a

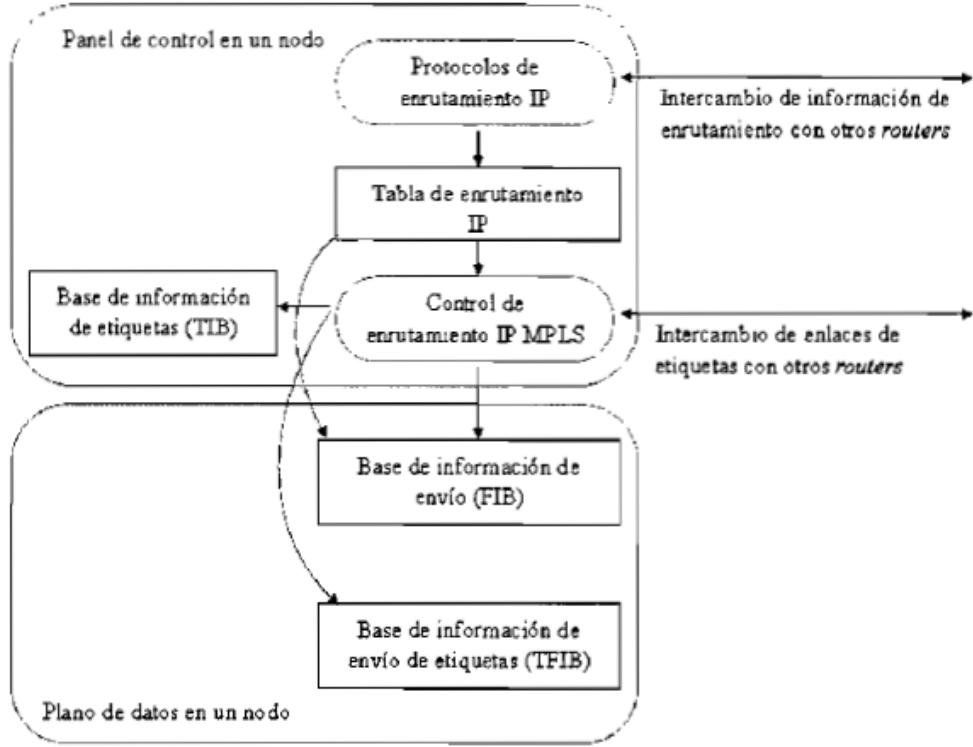


FIGURA B

Descripción del proceso LDP entre dos LSR

Al iniciarse una sesión LDP un enrutador crea la estructura de la base de información de etiqueta (LIB). El enrutador trata también de descubrir otros LSR en las interfaces que están corriendo MPLS a través de paquetes *hello*. Estos paquetes se envían como paquetes UDP *multicast* o *broadcast*, realizándose así el descubrimiento automático de LSR vecinos. Después que un paquete *hello* descubre un LDP vecino, se establece una sesión LDP mediante TCP, para asegurar confiabilidad en la entrega de la información. Inmediatamente después de creada la tabla LIB se asigna una etiqueta a cada FEC y se almacena este enlace en la tabla. La LIB se mantiene siempre sincronizada con la tabla de enrutamiento IP, es decir tan pronto como aparezca una ruta nueva en la tabla de enrutamiento, una etiqueta nueva se asigna y se enlaza a la nueva ruta.

Trayectorias comutadas de etiquetas (LSP):

Dentro de un dominio MPLS, la trayectoria sobre la cual debe viajar un paquete basado en un FEC particular en el dominio MPLS, desde el LSR de entrada hasta el LSR de salida, se conoce como LSP y la creación del LSP está basada en un esquema orientado a conexión, puesto que el camino se establece antes de cualquier flujo de datos. El establecimiento de un LSP para un FEC es en un solo sentido, lo cual significa que para el tráfico de retorno se emplea otro LSP diferente.

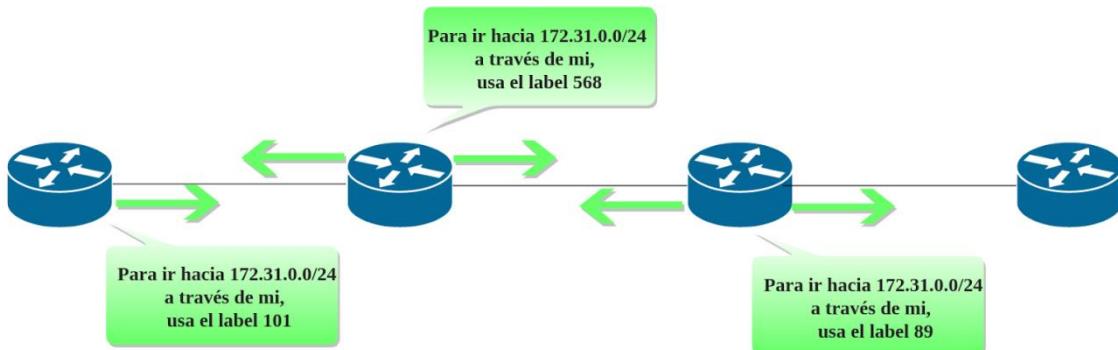
MPLS para establecer un LSP provee las opciones siguientes:

- **Enrutamiento salto a salto:** cada LSR puede seleccionar el próximo salto, para un FEC dado, que se empleará para el envío de paquetes hacia el destino utilizando su cálculo interno de ruta. El LSR usa cualquier protocolo de enrutamiento tal como OSPF, interfaz red a red privada ATM (PNNI), etc.

- **Enrutamiento explícito:** El LSR de ingreso especifica la lista de nodos que atraviesa el LSP. Este camino puede que no sea el óptimo. A lo largo del camino los recursos pueden ser reservados para asegurar QoS al tráfico de datos. Esto facilita la aplicación de ingeniería de tráfico a lo largo de la red y de servicios diferenciados utilizando flujos basados en políticas o métodos de administración de redes.
- **Enrutamiento basado en restricciones (CR, Constraint-based routing):** El enrutamiento basado en restricciones (CR) toma en cuenta parámetros, tales como características de enlace (ancho de banda, retardo, etc.), cantidad de saltos, y calidad de servicio (QoS, Quality of Service). Los LSP establecidos basados en restricciones se denominan CR-LSP. Las restricciones pueden ser saltos explícitos o requisitos de QoS. Los saltos explícitos se refieren a qué camino debe ser tomado. Los requisitos de QoS dictan qué enlaces y qué mecanismos de formación de colas de espera y planificación se emplearán para el flujo.
- Utilizando CR para establecer un LSP, el camino a seguir no siempre es el que implica menor “costo”, así por ejemplo en una aplicación de régimen de tráfico se pudiera establecer un LSP con mayor costo pero menor nivel de congestión. CR incrementa la complejidad de los cálculos de enrutamiento cuando el camino a seleccionar debe satisfacer los requisitos de QoS.

Descripción Funcional de las operaciones MPLS.

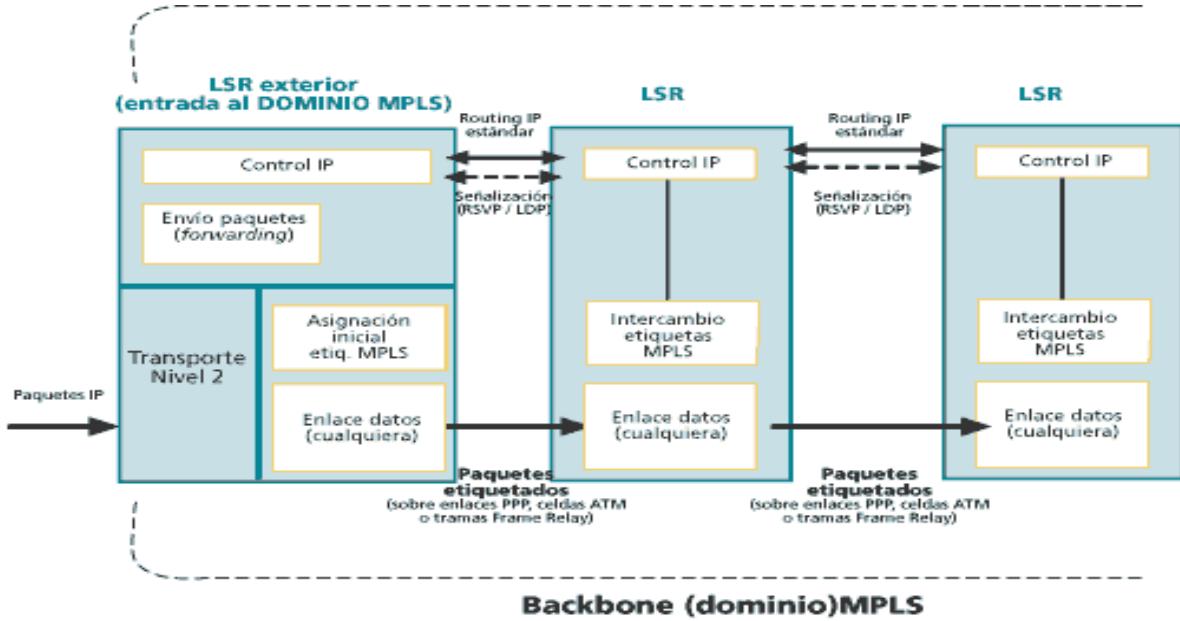
Se debe recordar que el funcionamiento en la Arquitectura MPLS se basa en la separación de los componentes de envío (*forwarding*) y control (*routing*) y su relación estrecha entre sí.



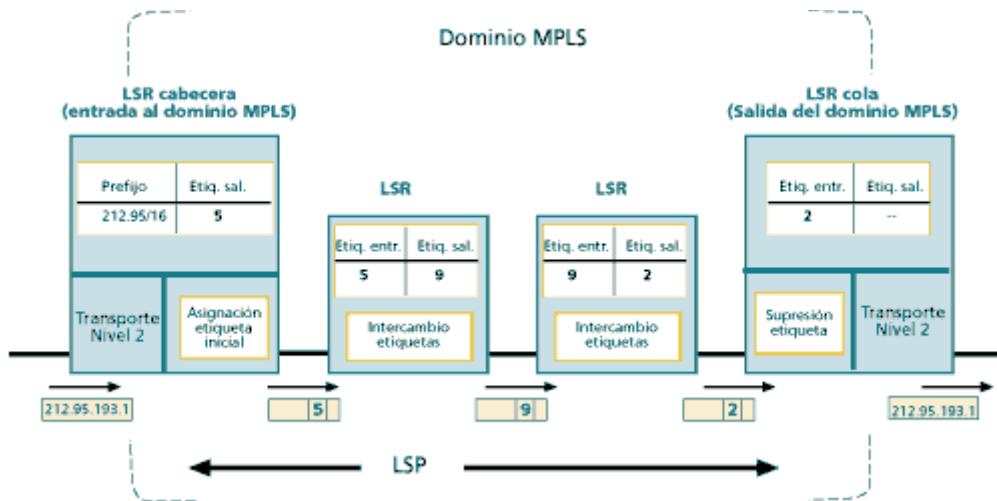
Funcionamiento del envío de paquetes en MPLS.

MPLS separa las dos componentes funcionales de control y de envío igual que en las soluciones de conmutación IP, como ya se ha explicado anteriormente. De igual manera el envío se implementa mediante el intercambio de etiquetas en los LSP. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el Forum ATM; sino que utiliza el protocolo LDP o el RSVP. Pero de acuerdo con los requisitos del (IETF, Internet Engineering Task Force), el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es más sencilla de gestionar que la solución clásica IP/ATM. Con esta variante no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM. Esto lo resuelve el procedimiento de intercambio de etiquetas MPLS.

En la siguiente Figura se muestra el esquema funcional de un LSR de frontera y los enlaces que puede establecer con otros elementos del Dominio MPLS y no con el entorno MPLS. (



El mecanismo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para realizar la asignación por el LSR de entrada o LER.



Componente de control en MPLS.

La componente de control en MPLS es la que establece los caminos de envío de etiqueta a lo largo de rutas IP y de la distribución de las uniones de etiquetas a los LSR. Además, mantiene la fiabilidad de los caminos debido a que pueden ocurrir cambios topológicos. Para poder realizar estas funciones se basa en dos aspectos fundamentales:

- Generación de las tablas de envío que establecen los LSP.
- Distribución de la información sobre las etiquetas a los LSR.

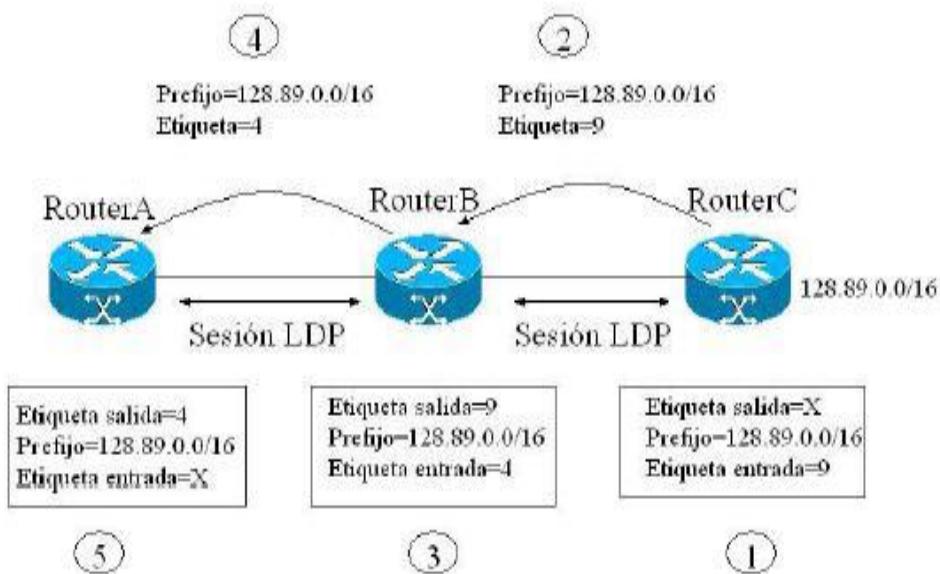
Las tablas de encaminamiento que establecen los LSP se generan a partir de la información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP, etc.) y para la distribución de

etiquetas no solo utiliza un único protocolo de distribución de etiquetas (de hecho se han estandarizando algunos existentes, con las correspondientes extensiones) este es el caso del protocolo RSVP del Modelo de Servicios Integrados del (IETF: *Internet Engineering Task Force*); además se definió el LDP específicamente para la distribución de etiquetas.

En la figura se muestra cómo trabaja LDP en un esquema de asignación de etiquetas hacia atrás:

- El LSR asigna una etiqueta para cada ruta en su tabla de enrutamiento, y crea una entrada en su FLIB con esta etiqueta como etiqueta de entrada.
- El LSR entonces advierte una relación entre la etiqueta que creó (etiqueta de entrada) y la ruta a otros LSR adyacentes.
- Cuando un LSR recibe información de asociación de etiqueta con una ruta y esta información fue originada por el próximo salto para esta ruta, el LSR coloca la etiqueta en la posición de la etiqueta de salida de la tabla FLIB asociada con la ruta.

Este mecanismo crea la unión entre la etiqueta de salida y la ruta. Este proceso se repite desde el LER de salida hasta el LER de entrada.

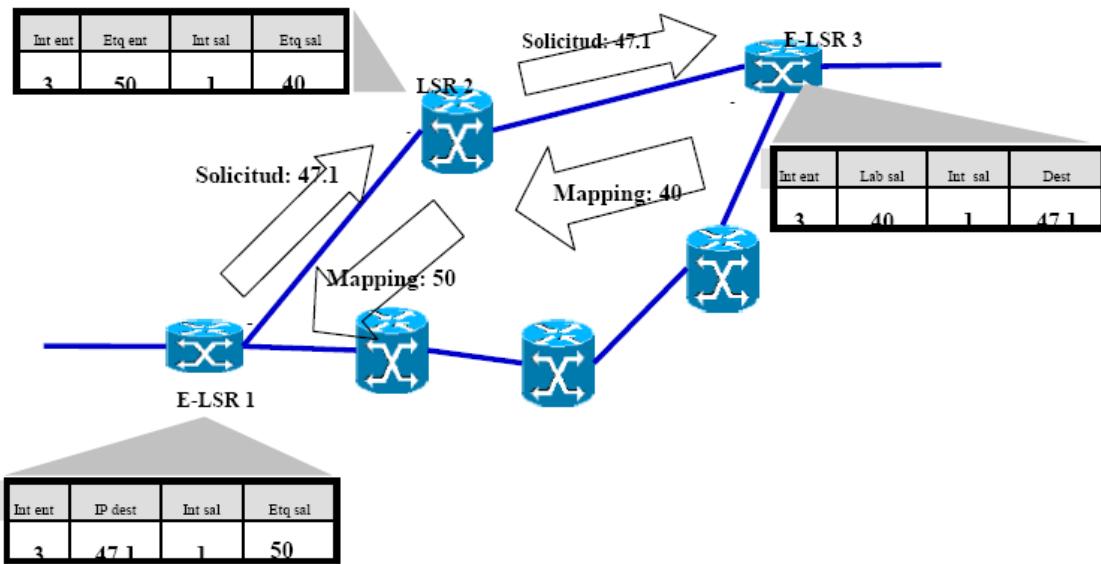


Ejemplo: Envío de un paquete IP.

Envío de un paquete entre una fuente y un destino con dirección IP 47.1.0.0/24. La figura muestra un ejemplo de envío de paquete donde se emplea como elemento de decisión la IP destino:

- Un paquete no etiquetado con destino 47.1 arriba al enrutador LSR1.
- LSR1 chequea su tabla FLIB y según su destino asigna el paquete a la clase FEC definida para el prefijo 47.1.
- El paquete es etiquetado con la etiqueta de salida 50 y se envía hacia su próximo salto LSR2.
- LSR2 recibe el paquete con la etiqueta de llegada 50 la cual se emplea como índice a la tabla FLIB.
- La etiqueta de llegada 50 se reemplaza por la etiqueta de salida 40.

6. LSR3 recibe el paquete con la etiqueta de llegada 40 la cual se emplea como índice a la tabla FLIB.
7. El paquete se envía por la interfaz de salida 1 con la adecuada información de capa 2 (tal como dirección MAC) de acuerdo a la tabla FLIB. (Note que LSR3 no tiene que hacer ninguna búsqueda de prefijo IP basado en el destino como fue hecha por E-LSR1).
8. Cuando el paquete arriba a E-LSR3, éste remueve la etiqueta desde el paquete y lo envía como un paquete IP no etiquetado.



Funcionamiento de MPLS en modo Trama

Comutación de etiquetas en MPLS en modo trama

Un router IOS adecuado y que está operando como un LSR MPLS en un dominio MPLS y en modo trama, puede realizar varias acciones sobre el paquete etiqueta. A continuación listamos estas acciones:

- **Acción pop de etiqueta (omisión de la etiqueta).** Elimina la etiqueta superior de la pila de etiquetas MPLS y propaga la sobrecarga restante, ya sea como un paquete etiquetado (si el bit de la parte inferior de la pila es cero) o como un paquete IP sin etiquetar (el campo Tag Stack de la FIB está vacío).
- **Intercambiar la etiqueta.** Sustituye la etiqueta superior de la pila de etiquetas MPLS por otro valor (el campo Tag Stack de la LIB es una etiqueta larga).
- **Acción push de etiqueta.** Sustituye la etiqueta superior de la pila de etiquetas MPLS por un conjunto de etiquetas (el campo Tag Stack de la LFIB contiene varias etiquetas).
- **Agregar.** Elimina la etiqueta superior de la pila de etiquetas MPLS y hace una búsqueda de Capa 3 en el paquete IP subyacente. La etiqueta eliminada es la etiqueta de la parte inferior de la pila de etiquetas MPLS; de lo contrario, se descarta el datagrama.
- **Desetiquetar.** Elimina la etiqueta superior de la pila de etiquetas MPLS y envía el paquete IP subyacente al siguiente salto IP especificado. La etiqueta eliminada es la etiqueta de la parte inferior de la pila de etiquetas MPLS; de lo contrario, se descarta el datagrama.

Convergencia en una red MPLS

Un aspecto importante de las redes MPLS es el tiempo de convergencia de la red. Algunas aplicaciones MPLS (ejemplo: diseño MPLSA/PN o BGP basado en MPLS) no operan correctamente a menos que se pueda enviar un paquete etiquetado a lo largo de todo el trayecto, desde el LSR de contorno de entrada hasta el LSR de contorno de salida. En estas aplicaciones, el tiempo de convergencia necesario para el Protocolo de Gateway Interior (IGP) para converger en torno a un fallo en la red principal puede aumentarse retrasando la propagación de la etiqueta.

En una red MPLS en modo trama, si se utiliza el modo de retención liberal, en combinación con el control de etiqueta independiente y la distribución de etiquetas de flujo descendente no solicitada, se minimiza el retraso de convergencia TDP/LDP. Cada router que emplea el modo de retención liberal, normalmente tiene asignaciones de etiqueta para un prefijo dado desde todos sus vecinos TDP/LDP, de manera que siempre puedan encontrar una etiqueta de salida apropiada siguiendo la convergencia de la tabla de enrutamiento sin preguntar a su nuevo router de siguiente salto acerca de la asignación de etiqueta.

Interacción de MPLS con el Protocolo de Gateway Fronterizo

En la tabla de enrutamiento IP de un router que actúa como LSR se asigna una etiqueta a cada prefijo IP, siendo la única excepción las rutas aprendidas a través del Protocolo de gateway fronterizo (BGP). A estas rutas no se les asignan etiquetas y el LSR de contorno de entrada utiliza la etiqueta asignada al siguiente salto BGP para etiquetar los paquetes enviados hacia los destinos BGP.

La interacción entre MPLS, IGP y BGP brinda al diseñador de redes una perspectiva completamente nueva del diseño de redes. De acuerdo con el funcionamiento tradicional, BGP se tiene que ejecutar en cada router del núcleo de la red del proveedor de servicios para permitir el envío correcto de paquetes.

Aplicaciones.

Las principales aplicaciones que tiene MPLS son:

- Permite realizar Ingeniería de tráfico.
- Puede garantizar la Calidad de Servicio (QoS) a través de la diferenciación de niveles de servicio mediante clases
- Puede brindar servicio de redes privadas virtuales (VPN)

Ingeniería de tráfico.

Ingeniería de tráfico: Con MPLS el análisis de los paquetes se realiza no solo a los paquetes individuales, sino a los flujos de paquetes, en el que cada flujo posee ciertos requisitos de QoS y demanda de tráfico previsibles. Con MPLS, es posible establecer rutas, basadas en estos flujos individuales, o sea, dos flujos diferentes entre los mismos puntos finales pueden seguir distintas rutas. Además, cuando está presente la congestión, las rutas MPLS pueden ser reconfiguradas inteligentemente. Un uso efectivo de la ingeniería de tráfico puede aumentar substancialmente la capacidad utilizable de la red.

Diferenciación de niveles de servicio mediante clases (CoS).

Diferenciación de niveles de servicio mediante clases (CoS): MPLS está diseñado para cursar servicios diferenciados, según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo Tipo de Servicio ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a

la red. MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

[Servicios de Redes Privadas Virtuales \(VPN\).](#)

Servicios de Redes Privadas Virtuales (VPN): Con la utilización de la arquitectura MPLS se tienen mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP, debido a que la red del proveedor no pierde la visibilidad IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios. Para mayor seguridad se puede cifrar la información, pero se limitan las opciones de QoS. Además la operación de túneles de nivel 2 está condicionada a un único protocolo de éste nivel casi siempre definido por el proveedor. La flexibilidad que MPLS brinda a las VPN y las facilidades de gestión, configuración y crecimiento permiten a esta arquitectura imponerse en este mundo.

CAPITULO 7

Introducción a los servicios Metroethernet

Introducción

Metroethernet es un término usado para describir una red de la tecnología de Ethernet en un área metropolitana y ha tenido en los últimos años un crecimiento increíble desde que la tecnología fue inventada en 1973 por Bob Metcalfe en Xerox Corp's en California. Este estándar comenzó conociéndose como Ethernet DIX, en referencia a los nombres de los creadores. Metroethernet ofrece una amplia gama del servicio de una manera simple, escalable, y flexible, es utilizado para la conectividad a Internet público, y la conectividad entre los sitios corporativos que se encuentran separados geográficamente.

La red metro Ethernet es una arquitectura que suministra la conectividad con banda ancha a la red metropolitana soportando grandes servicios, aplicaciones y tráfico en tiempo real; tomando cuenta que las actualizaciones, el rendimiento, la disponibilidad, la fiabilidad y un proceso integrado de seguridad que en toda empresa exige

Metro Ethernet realiza una conexión de acceso a la banda ancha y de los diferentes servicios de los cuales son necesarios y beneficiosos para las empresas en la red metropolitana, todo ello con una conexión de punto a punto con una banda con un bajo costo tanto en una red pública como privada

Es una arquitectura tecnológica que tiene como propósito suministrar los diferentes servicios de la conexión en una red MAN/WAN de nivel 2. Esta red es la encargada de soportar múltiples servicios, aplicaciones y algunos mecanismos q nos ayuda a soportar y controlar el tráfico en tiempo real, este tráfico puede ser el registro de un servicio de telefonía IP que es sensible a retardo y al jitter.

Es considerado un servicio de banda ancha que utiliza el protocolo IP utilizada para entrelazar redes de área local a través de las redes metropolitanas, permitiendo la conformación de redes IP VPN (redes virtuales IP) que pueden estar aislados (EPL L1: Ethernet Private Line Layer 1), concentrados en un solo origen (EPL L2: Ethernet Private Line Layer 2) o intercomunicados de forma total hacia múltiples destinos EPN: Ethernet Private Network L2). Además de permitir Clases de Servicio (CoS), por medio de la implementación de IP MPLS, ofrece calidad de servicio (QoS) y discrimina tráficos prioritarios del cliente, optimizando el canal de comunicaciones contratado

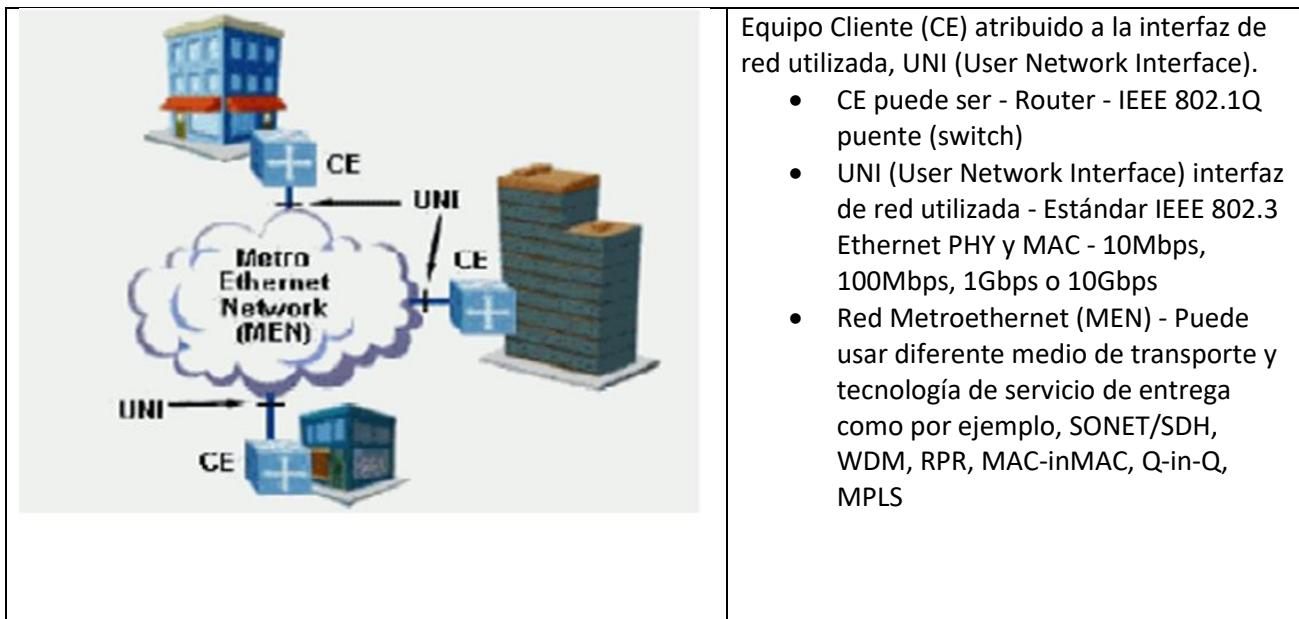
Entre sus principales servicios se encuentra la intercomunicación entre redes IP con aplicaciones en las cuales el cliente requiera altas tasas de transferencia de información y una clasificación de su tráfico, garantizando calidad de servicio. Algunas de las características técnicas se encuentran:

Realiza conexiones desde 256 Kbps hasta Fast Ethernet (FE).

- Enlaces por fibra óptica o cobre.
- Interfaz para conexión directa a redes LAN (Ethernet) o a routers (V.35)
- Creación de redes virtuales (VPN)
- Clasificación de tráfico (CoS)
- Calidad de Servicio (QoS)
- Gestión centralizada de la operación del canal

Topología de la red

Metroethernet es esencialmente un "campo de tecnología", ya que es usado como un backbone en una red, también puede ser usado entre routers, switches y concentradores o hub. Además puede ser usado para conectar servidores, granja de servidores y estaciones de alto poder. Hoy en día Metroethernet necesita el soporte de las topologías de anillo y de malla. Esto es de vital importancia porque mientras que la topología típica de red de Ethernet usada en una empresa es la topología en árbol, los portadores requieren otras topologías, incluyendo los anillos y malla. Ethernet tradicional no es capaz del despliegue de estas topologías, particularmente porque no puede haber ciclos en la red de la capa 2. Todos los servicios de Metroethernet comparten algunos atributos en común, pero estos son diferentes. El modelo básico para el servicio de Metroethernet según Metroethernet Forum (MEF), quien es una organización no lucrativa encargada de estandarizar los servicios de Metroethernet en todo el mundo, se muestra a continuación en la figura



¿Qué es un servicio ethernet?

Una red Metroethernet manejada por servicios es aquella donde “el proveedor de servicio examina detalladamente la amplitud y profundidad de su portafolio actual y futuro antes de diseñar una infraestructura”.

Es importante pensar “primero en los servicios”. En el pasado, los proveedores de servicio construían su infraestructura de red basados en cierta tecnología o conjunto de productos puntuales y luego miraban qué servicios podían desplegar sobre esa infraestructura. Esto puede ser extremadamente limitante y puede resultar en SLAs y ofrecimientos de servicio tipo “lo mejor disponible”.

Los proveedores ahora están examinando sus ofertas de servicio más cuidadosamente y están casi siempre buscando lo que necesitan para construir arquitecturas flexibles que utilicen un rango de tecnologías y características inteligentes.

Conexión de Ethernet Virtual (EVC)

El EVC es una asociación de dos o más UNIs, donde el UNI es la interfaz estándar Ethernet y el punto de demarcación entre el equipo cliente y el proveedor de servicio Metroethernet Network MEN. Una conexión de Ethernet Virtual (EVC) tiene dos funciones:

- Conectar dos o más sitios (UNIs) habilitando la transferencia de tramas Ethernet entre ellos.
- Impedir la transferencia de datos entre usuarios que no son parte del mismo EVC, permitiendo privacidad y : seguridad

Basada en estas características, Un EVC puede ser usado para construir Virtual Private Network (VPN) de nivel 2. El MEF (Metroethernet Forum) ha definido dos tipos de EVC:

- Punto a Punto (E-Line)
- Multipunto a Multipunto (E-LAN)

Definición Servicio Ethernet

Para ayudar a los suscriptores a entender mejor la variedad entre los servicios Ethernet, y a crear un portafolio de conectividad y de servicios de valor añadido al usar Metro Ethernet; El foro Metroethernet MEF ha definido dos modelos de la conectividad, descritos en la siguiente tabla

Tipo de Servicio (Modelo Conectividad de Red)	Tipo de Conectividad	Ejemplo de servicio en uso
Servicio Ethernet LAN	Completamente mallado (any-to-any), conectividad de múltiples puntos; interconecta LANs separado a través de un área metropolitana	Servicio transparente del LAN Ethernet Privado en Red de Anillo
Servicio Línea de Ethernet	Conexión punto a punto	Línea de Ethernet Privada

De acuerdo con estos modelos, los proveedores de servicio pueden utilizar Ethernet como el método de acceso para una gran variedad de servicios de conectividad de servicio de capa 1 y capa 2 y capa 3, tales como IP VPN e Internet dedicado.

También MEF ha desarrollado la definición de servicio Ethernet. Las metas para este marco son:

9. Definición y nombre común de los tipo de servicio Ethernet
10. Defina los atributos y parámetros de asociación usado para definir un específico servicio Ethernet.



El MEF ha definido dos tipos de conexiones del servicio Ethernet:

- Ethernet Line (E-Line) service Type: Punto a Punto.
- Ethernet LAN (E-LAN) service Type: Multipunto a Multipunto

Los tipos de servicio son realmente categorías "umbrella", esos atributos pueden ser agrupados en las siguientes categorías:

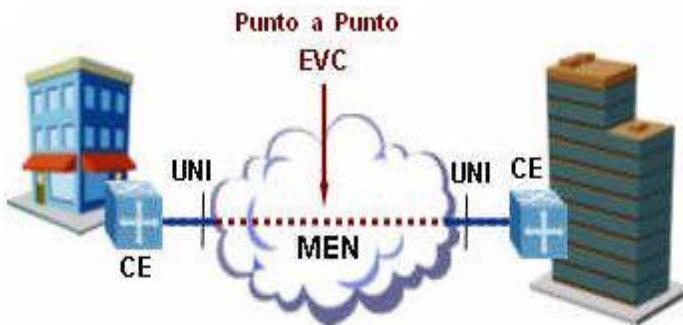
- Interfaz física Ethernet
- Parámetros de tráfico
- Parámetros de desempeño
- Clase de servicio
- Service Frame Delivery
- Soporte de etiqueta (Tag) VLAN
- Servicio de Multiplexación
- Bundling
- Seguridad

Tipos de servicio Ethernet

El MEF ha definido dos tipos de servicios básicos que a continuación se expondrán, y otro tipo que puede ser definido en el futuro.

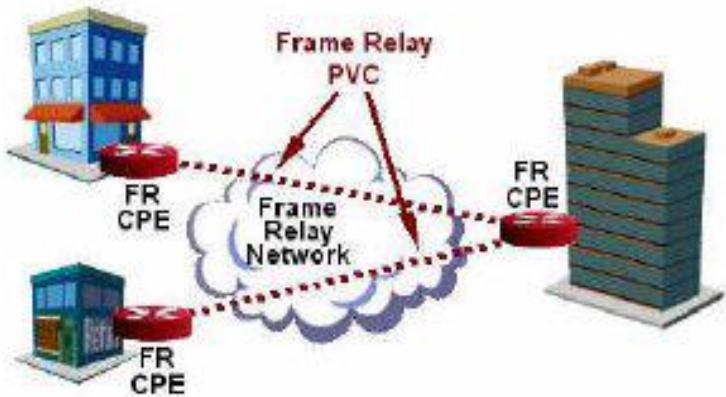
Tipo de Servicio Línea de Ethernet _ Punto a punto

El tipo de Servicio Línea de Ethernet (E-Line Service) provee una conexión de Ethernet virtual (Ethernet Virtual Connection _ EVC) punto a punto entre dos UNIs. Este tipo de conexión se muestra a continuación.

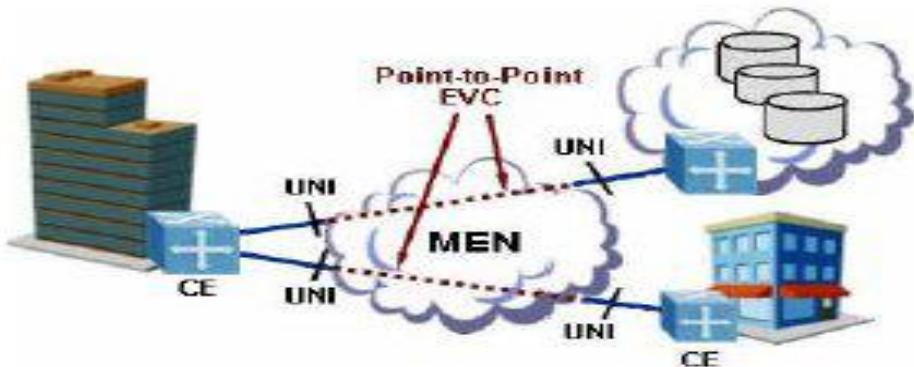


Un E-Line Service provee ancho de banda simétrico para envío de datos en ambas direcciones, sin asegurar desempeño. Un E-Line service, provee un CIR (Committed Information Rate), un CBS (Committed Burst Size), un EIR (Excess Information Rate) y un EBS (Excess Burst Size) dependiendo del proveedor de servicio. Estas características del servicio están relacionadas con las demoras, jitter y la seguridad entre las diferentes velocidades de las UNIs.

Un servicio E_Line puede proveer conexión punto a punto EVCs entre UNIs análogas para usar Frame Relay PVCs para interconectar sitios como lo ilustra la figura.

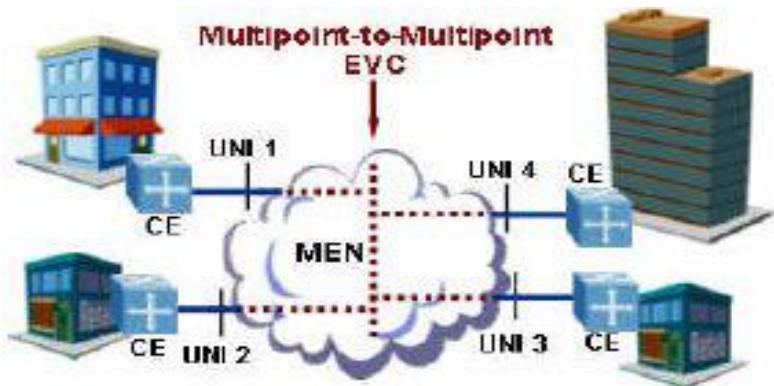


Un servicio E_Line puede también proveer conexión punto a punto entre UNIs análogas hacia un TDM (línea de servicio privada). Este servicio interconecta dos UNIs y provee una completa transparencia para servicios de trama entre UNIs. La figura ilustra este tipo de conexión.



Tipo de Servicio LAN de Ethernet _ Multipunto a Multipunto

El tipo de servicio LAN de Ethernet provee conectividad multipunto, conectando dos o más UNIs como se ilustra en la figura. Un usuario envía datos de una UNI y puede recibir uno o más de otros UNIs. Cada sitio (UNI) es conectada a un EVC multipunto, al agregar usuarios, que son conectados a un mismo EVC multipunto, simplificando el aprovisionamiento y la activación del servicio.



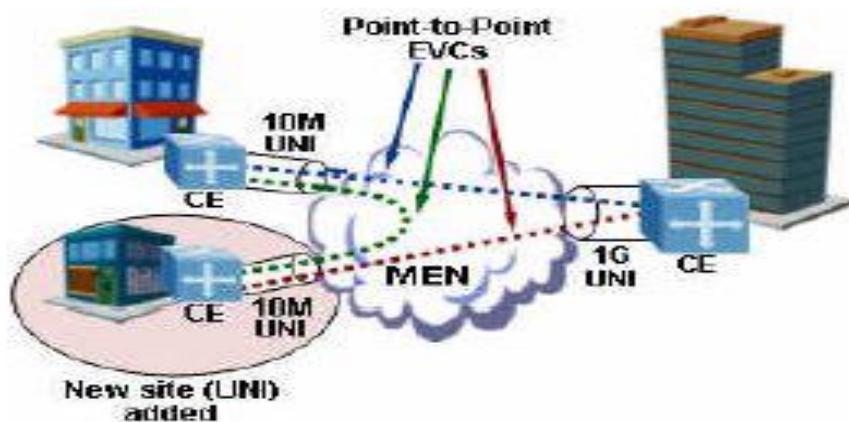
Una E-LAN puede ser usada para crear un amplio rango de servicios, mostrando un mejor desempeño para los servicios ofrecidos. La E-LAN se usa para interconectar varios usuarios, mientras E-LINE normalmente es usada para conectarse a Internet.

Una E-LAN define el CIR, CBS, EIR y EBS. La velocidad de cada puerto UNI puede ser diferente, por ejemplo, en la figura de arriba, los UNI 1, 2 y 3 tienen 100Mbps con un CIR de 10Mbps, el UNI 4 posee 1Gbps con 40Mbps de CIR.

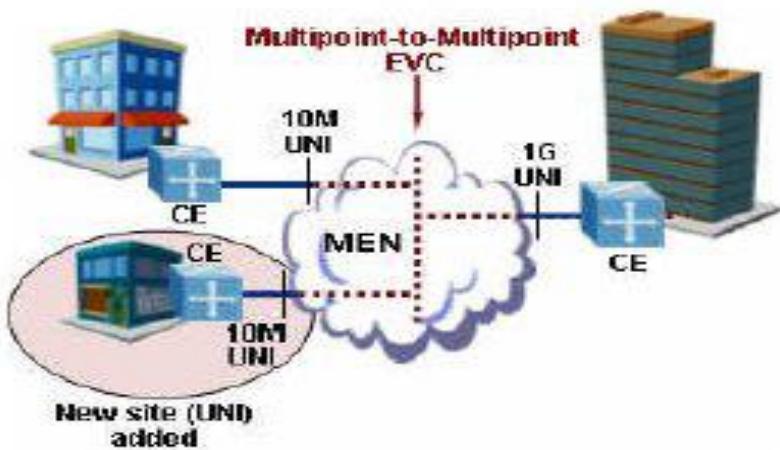
Configuración Punto a Punto en E-LAN

Un E-LAN puede ser usado para conectar solo dos UNIs, aunque parece similar a E-Line, hay algunas diferencias.

Con un E-Line, cuando un nuevo UNI es agregado, es necesario adicionar un nuevo EVC para conectar este nuevo usuario a uno de los UNIs existentes. En la figura, un nuevo punto de red es adicionado y por consiguiente un nuevo EVC es creado para conectar todos los puntos de la red.



Con un nuevo punto de red (UNI), solo es necesario agregarlo al EVC multipunto existente, no se necesitan EVC adicionales. Un E-LAN permite al nuevo sitio comunicarse con todos los otros UNI. Los servicios E-LAN pueden ser creados a partir de la conformación de VPNs en la red switcheada.



Interface física de Ethernet

Los atributos se definen como las capacidades de los diferentes tipos de servicio. Algunos atributos aplican a los puntos de acceso (UNI), mientras que otros a los canales virtuales (Conexión Ethernet Virtual EVC).

Para los puntos de acceso (UNI) aplican los siguientes atributos:

- **Medio físico:** son los especificados en el estándar 802.3 – 2000. Ejemplos de medios físicos incluye 10BaseT, 100BaseT, 1000BaseSX.
- **Velocidad:** las velocidades son las especificadas en el estándar Ethernet: 10Mbps, 100Mbps, 1Gb/s y 10Gb/s.
- **Modo:** un enlace puede soportar full o half duplex o auto negociación.
- **Capa MAC:** las especificadas en IEEE 802.3 – 2000.

Características del ancho de banda

El Foro MetroEthernet MEF ha definido los servicios de ancho de banda como atributos que pueden aplicarse a una UNIs o para una Conexión Ethernet Virtual EVC. Una característica del ancho de banda es un límite promedio en que la trama Ethernet puede atravesar la UNI.

Esta puede separar la característica del ancho de banda para la entrada de tramas dentro de la red y salida de tramas de la red. El Comité promedio de información (Committed Information Rate CIR) para un Frame Relay PVC es un ejemplo de una característica de ancho de banda. MetroEthernet ha definido los siguientes tres características de ancho de banda para los atributos del servicio:

- Ingreso perfil de ancho de banda por ingreso UNI.
- Ingreso perfil de ancho de banda para un Conexión Ethernet Virtual EVC.
- Ingreso perfil de ancho de banda para identificar Clase del servicio CoS.

Parámetros

Una característica para un servicio MetroEthernet consiste de los siguientes parámetros:

- **CIR (Committed Information Rate):** es la cantidad promedio de información que se ha transmitido, teniendo en cuenta los retardos, pérdidas.
- **CBS (Committed Burst Size):** es el tamaño de la información utilizado para obtener el CIR respectivo.
- **EIR (Excess Information Rate):** especifica la cantidad de información mayor o igual que el CIR, hasta el cual las tramas son transmitidas sin pérdidas.
- **EBS (Excess Burst Size):** es el tamaño de información que se necesita para obtener el EIR determinado.”

Servicio Color De La Trama

El “color” del servicio de la trama es usado para determinar el ancho de banda conformado por un servicio particular de la trama. Un servicio puede tener dos otros colores, dependiendo de la configuración de los parámetros de la trama.

Un servicio de trama es marcada como “Verde” si este esta conformado con CIR y CBS en la característica de ancho de banda., por ejemplo el promedio del servicio de una promedio de trama y máximo tamaño del servicio de trama es menos o igual a el CIR y CBS, respectivamente. Esto es referente ha como conformar CIR.

Un servicio de trama es marcada como “Amarillo” si este no esta conformado con CIR pero esta conformada con EIR y EBS en la característica de ancho de banda., por ejemplo el promedio del servicio de trama es mas grande que la CIR pero menos que la EIR y el máximo tamaño de servicio trama es menor que la EBS. Esto es referente ha como conformar EIR.

Un servicio de trama es marcada como “Rojo” y es descartada si este no esta conformado con CIR ni esta conformada con EIR.

El comité técnico de MEF está trabajando actualmente en qué colores están marcados en las tramas del servicio.

CIR y CBS

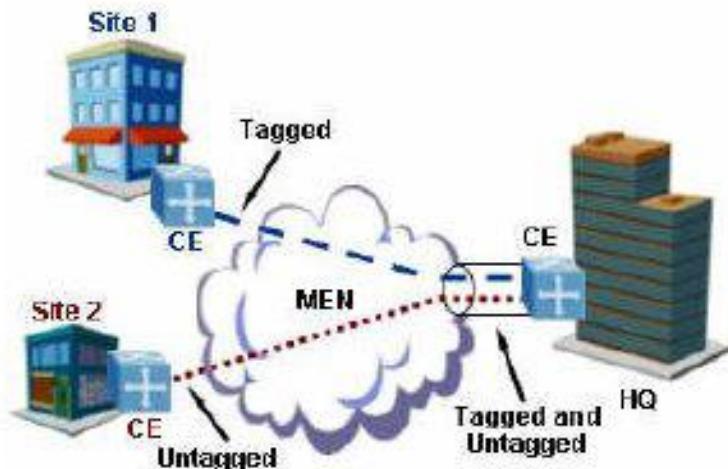
- CIR (Committed Information Rate): es la cantidad promedio de información que se ha transmitido, teniendo en cuenta los retardos, pérdidas, etc.
- CBS (Committed Burst Size): es el tamaño de la información utilizado para obtener el CIR respectivo.

EIR y EBS

- EIR (Excess Information Rate): especifica la cantidad de información mayor igual que el CIR, hasta el cual las tramas son transmitidas sin pérdidas.
- EBS (Excess Burst Size): es el tamaño de información que se necesita para obtener el EIR determinado.

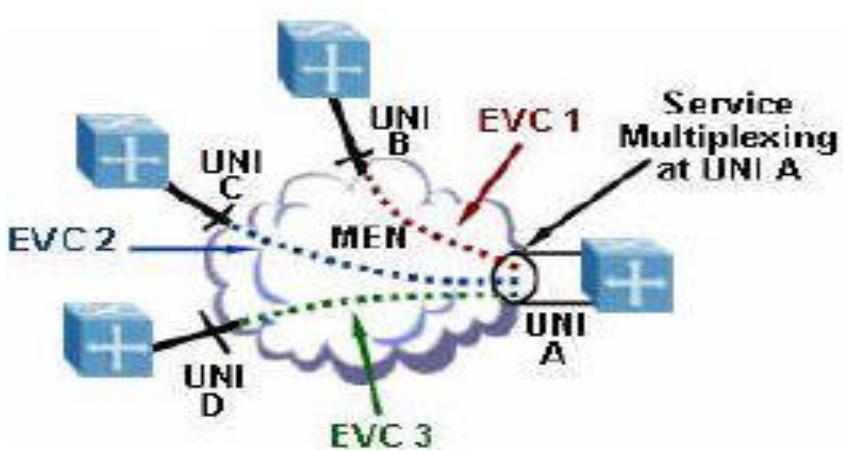
SOPORTE VLAN TAG

Las VLAN proveen el soporte de un importante set de capacidades que afectan el servicio de entrega de trama y su funcionamiento. El servicio de trama Ethernet puede soportar 802.1Q tagged (etiquetado) o Untagged (No etiquetado), esto es importante para entender que sucede en ambas tramas. Las VLAN soportan una variedad de servicios Ethernet. Un UNI puede soportar tagged (etiquetado) o Untagged (No etiquetado).



Servicio de multiplexación

Este servicio es usado para soportar varios canales virtuales (Conexión Ethernet Virtual EVC) de diferentes velocidades simultáneamente en un solo enlace de conexión (UNI) esto lo observamos en la figura. Usando multiplexación se elimina la necesidad de tener diferentes interfaces físicas para tener enlaces a diferentes velocidades.



Beneficios Del Servicio de Multiplexación

El servicio permite a un UNI soportar múltiples Conexiones Ethernet Virtuales EVCs, comparado con la alternativa de separar las interfaces físicas para cada Conexión Ethernet Virtual EVC, se presentan varios beneficios:

- Costo bajo de los equipos, ya que se minimiza el número de routers y switch y maximiza la densidad de utilización puerto/slot.

- Minimiza espacio, potencia y cableado. Comparado con m\xf3ltiplex UNI no multiplexada, el servicio de multiplexi\xf3n UNIs reduce la cantidad de espacio de rack, la potencia requerida para el suscriptor y reduce el n\xfamero de equipos conectadas entre estos.
- Simplifica la activaci\xf3n de nuevos servicios. El servicio de multiplexi\xf3n permite nuevas conexiones ethernet virtuales EVCs para ser establecido sin tener la necesidad de visitar un sitio para la instalaci\xf3n del los equipos, conexiones cruzadas o parcheo de cables.

CAPITULO 8

Introducción a las redes de acceso residencial

El bucle de abonado y las tecnologías dsl

ADSL pertenece a un conjunto de tecnologías que se agrupan bajo la denominación genérica de xDSL (any Digital Susbscriber Line). Este conjunto de tecnologías gracias al uso de un tipo de códigos de línea adecuados permiten la transferencia de regímenes binarios de alta velocidad sobre el par trenzado telefónico. La tecnología xDSL, suministra el ancho de banda suficiente para numerosas aplicaciones, incluyendo además un rápido acceso a Internet utilizando las líneas telefónicas; acceso

De los diferentes medios de transmisión que existen, el más antiguo y abundante es el par de hilo de cobre.

La red telefónica conmutada, RTC, se diseñó para permitir las conexiones de voz y el bucle de abonado, formado por pares de hilo de cobre, proporciona el medio físico de acceso a la red, uniendo el teléfono de una casa con la central telefónica.

Aunque se diseñó para soportar señales vocales, que necesitan un ancho de banda pequeño, entre 300 Hz y 3400 Hz, en la actualidad han evolucionado permitiendo ofrecer sobre ellos servicios de banda ancha de alta velocidad.

Las tecnologías xDSL utilizan el par de cobre trenzado, twisted copper pair en inglés, de una distancia máxima determinada que varía en función de la tecnología usada (HDSL, ADSL, VDSL, etc).

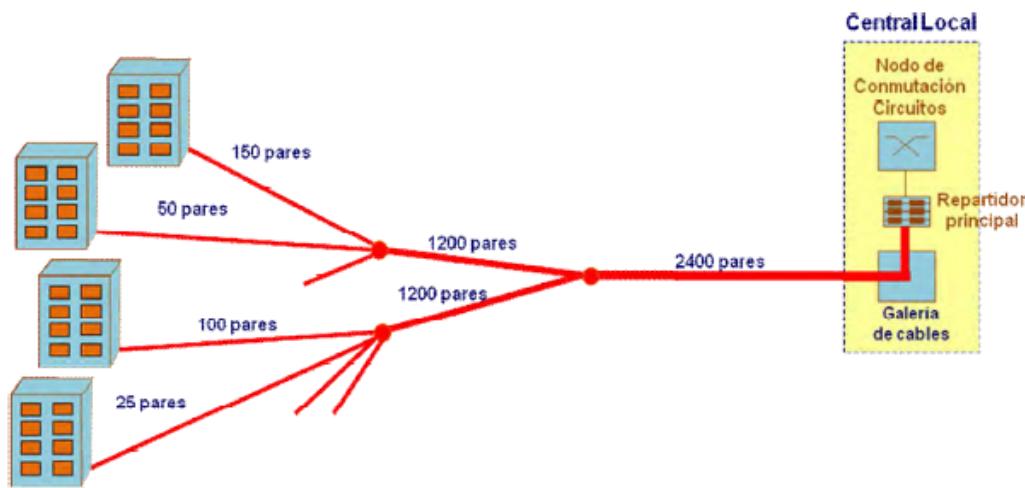
Desde el punto de vista técnico, el bucle de abonado puede considerarse una tecnología obsoleta, pero no se considera como tal debido al número de ellos que existen en el mundo.

Características del bucle

El par de cobre es un medio de transmisión de los llamados guiados, donde las ondas electromagnéticas van encaminadas por el medio físico. Es full-dúplex, consiste en dos hilos de conductores de cobre, aislados con material plástico, y se emplea tanto para la transmisión como para la recepción. Los estándares son de 0,5 o 0,4mm cada uno.

Para minimizar las posibles interferencias electromagnéticas y la diafonía entre pares, los hilos, en lugar de ir paralelos, van trenzados. Esto no es así en el interior de las casas, donde los pares van paralelos, ya que la pequeña distancia que tiene que recorrer unido a que no hay posibilidad de cruzarse con otro circuito, minimizan la posibilidad de interferencias.

Además de esto, a lo largo del camino hasta la central se van cambiando de orden, técnica llamada transposición, para que la inducción que pueda haber no se dé siempre sobre el mismo par. Varios pares se van uniendo en grupos de cables más gruesos, formando cables mayores, a lo que se denomina mazos de cables.



La planta instalada de par de cobre presenta ciertos inconvenientes como pueden ser los siguientes:

- Ramas laterales. Las ramas laterales son consecuencia de la reutilización de los mismos pares para diferentes usuarios. Al producirse altas y bajas de usuarios de las compañías telefónicas sobre el mismo par, quedan ramas. Estas ramas laterales solo afectan a servicios de datos, transportados por señales de alta frecuencia. El servicio de voz no se ve afectado por estas ramas.
- Bobinas. El par trenzado, por su disposición física, presenta un carácter intrínsecamente capacitivo. Este efecto se compensa en parte por el trenzado. No obstante, cuando las distancias son grandes, este carácter capacitivo se impone, resultando en una degradación de las frecuencias altas en la banda vocal. En estos casos se instala una bobina que compensa el efecto capacitivo. Esto resulta en un aplanamiento del espectro en la banda vocal, pero a la vez aparece una frecuencia de corte poco más allá de la frecuencia vocal por lo que no se pueden transmitir señales DSL

Atenuación

Cuando una señal sufre una pérdida de potencia al transitar por un medio de transmisión decimos que ha sufrido una atenuación.

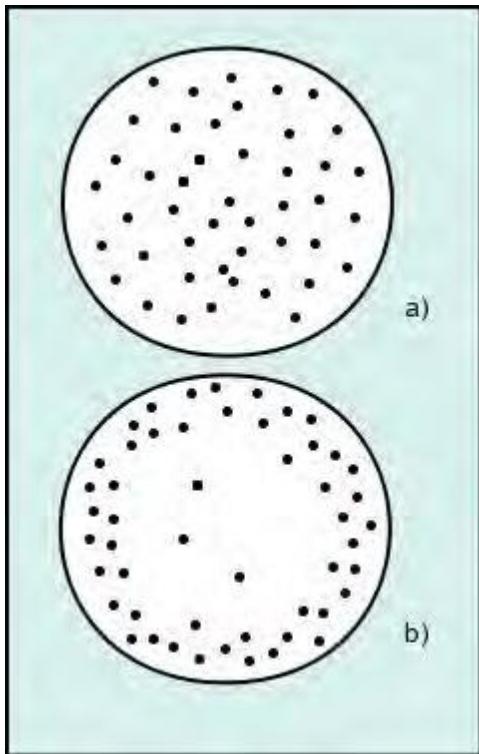
La atenuación es la diferencia entre la potencia de la señal transmitida y la potencia de la señal recibida en el otro extremo, expresada en decibelios.

La atenuación es uno de los factores más importantes a la hora de determinar la distancia a la cual podemos hacer llegar una señal, y crece con la longitud del cable y la frecuencia.

Efecto pelicular (Skin effect)

En los pares trenzados aparece el efecto pelicular, o skin effect, por el cual se observa, para corrientes de alta frecuencia, mayor densidad de corriente en la superficie del conductor. Al disminuir la superficie a través de la que fluye, resulta en un aumento de la atenuación a altas frecuencias.

El efecto pelicular se debe a que la variación del campo magnético es mayor en el centro del conductor, lo que da lugar a una reactancia inductiva mayor, y por ello, una intensidad menor.



En la primera imagen a) se muestra la distribución de la densidad de corriente en un conductor cuando es recorrido por una corriente continua.

En la segunda imagen b) se muestra la distribución de la densidad de corriente en un conductor cuando es recorrido por una corriente alterna.

Ruido

Podemos definir el ruido como una forma no deseada de energía que tiende a dificultar la emisión y recepción de señales deseadas.

El ruido siempre está presente en los sistemas electrónicos, influyendo en el rendimiento.

Los sistemas de transmisión basados en cobre deben salvar una serie de obstáculos debidos a factores tanto intrínsecos como extrínsecos.

Los factores intrínsecos son aquellos relacionados con las características del propio medio de transmisión, como el ruido térmico, el eco, las reflexiones y las interferencias cruzadas. Los factores extrínsecos son los debidos a causas externas al sistema, como el ruido impulsivo o las interferencias de otros sistemas.

Capacidad máxima del canal: Teorema de Shannon – Hartley

En los servicios de telecomunicación en los que la señal es digital, la velocidad de transmisión que se puede alcanzar sobre un determinado circuito se define como el número máximo de bits que se transmiten por segundo (bit/s) y su límite viene dado por el ancho de banda de dicho circuito, así como por la relación señal/ruido que presente.

Según el teorema postulado por el científico Shannon en los años 40, la capacidad de un sistema afectado por ruido blanco es función de la relación entre el nivel de la señal útil y del ruido presente en la línea y del ancho de banda del canal.

$$C = B \log_2 (1 + S/N)$$

Dónde:

- C representa la capacidad de transferencia máxima del canal expresada en bit/s
- B representa el ancho del canal en Hz
- S/N (Signal/Noise) es la relación entre el nivel de la señal útil y del ruido presente en la línea.

Teóricamente es posible transmitir información por un canal a cualquier velocidad siempre que esta sea menor que la capacidad C con una probabilidad de error arbitrariamente pequeña usando un esquema de codificación suficientemente complicado. Para una velocidad superior a la capacidad C no es posible encontrar un esquema de codificación que conduzca a una probabilidad de error arbitrariamente pequeña.

Shannon demostró que la tasa de transmisión no puede crecer sin límite a medida que el ancho de banda crece sin límite, estableciendo un valor mínimo de relación señal a ruido (límite de Shannon) por debajo del cual no es posible llevar a cabo comunicaciones libres de error de bit.

Como el SNR no puede reducirse infinitamente, la tasa de transmisión tampoco puede crecer sin límite con el ancho de banda, sino que llega hasta un valor para el cual se alcanza el límite de Shannon a partir del cual R no puede aumentar más.

Tecnologías xDSL

La Red Telefónica Pública Comutada, RTPC, fue concebida para el transporte de señales de voz y es adecuada para el transporte de señales analógicas dentro de la banda de frecuencias comprendida entre 300 y 3400 Hz. Fue después, con la aparición de las comunicaciones de datos cuando se planteó la necesidad de enviar este tipo de tráfico sobre la red telefónica para lo que había que adaptar las líneas para la prestación de servicios de banda ancha.

Aunque el bucle de abonado a priori tiene serias limitaciones para soportar servicios que requieran un gran ancho de banda, mediante la instalación de módems en ambos extremos del canal de comunicación, las tecnologías DSL permiten multiplicar la capacidad de la línea.

El principal inconveniente es que la velocidad de transmisión depende en gran medida de la atenuación presente en la línea, derivada principalmente de la longitud de la misma, es decir, de la distancia entre ambos módems que es la distancia desde el usuario hasta la central telefónica. De esta forma, a mayor distancia, menor es el caudal soportado por el sistema.

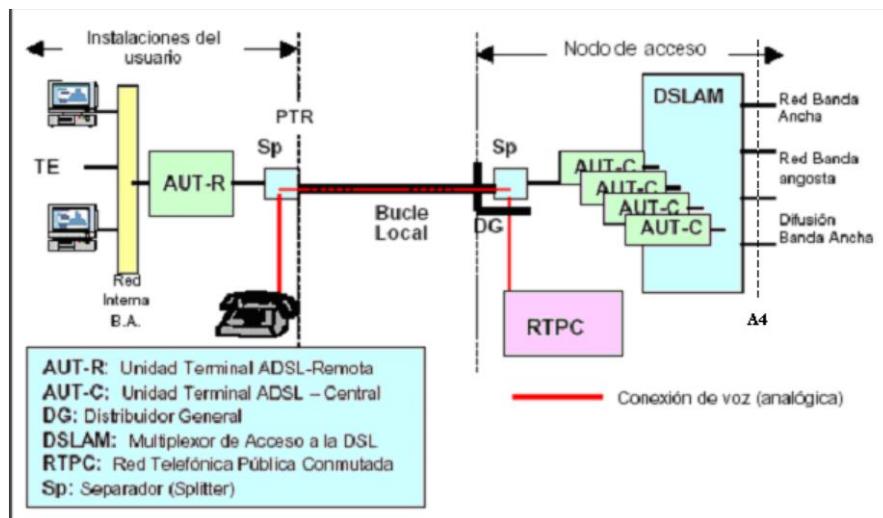
Para trabajar con xDSL, en la central de telefonía local tiene que haber instalado un servidor DSLAM que traduce las señales DSL. La señal se transmite desde casa del usuario por la línea telefónica hasta el DSLAM.

xDSL comparte el par de cobre con el servicio telefónico tradicional POTS (*Plain Old Telephone Service*), por lo que utiliza las frecuencias por encima del ancho de banda telefónico, que va de 300 Hz a 3400 Hz.

El envío y recepción de datos, en casa del cliente, se realiza a través de un módem. Para separar las señales de voz y datos, que viajan por la misma línea, se usan divisores o *splitters*, elementos que se colocan delante del módem del usuario y del DSLAM y que están formados por dos filtros, uno paso bajo para las señales de voz, que residen en la banda base, por debajo de los 4 KHz, y otro paso alto para los datos que residen en frecuencias más altas.

Actualmente, para facilitar la instalación, en el lado del usuario únicamente se colocan microfiltros (filtros paso bajo) en los teléfonos, ya que el modem ADSL del usuario lleva el filtro paso alto incorporado

De esta forma, los proveedores de servicio pueden proporcionar velocidades de datos de varios Mbps dejando intactos los servicios de voz que viajan por la misma línea.



Línea de abonado digital de alta velocidad (HDSL)

Esta tecnología, High Data Rate Digital Subscriber Line, es una mejora de las normas T1, en Estados Unidos y Japón que siguen la normativa ANSI, y E1 en prácticamente el resto del mundo donde se sigue la normativa ETSI.

Estos enlaces alcanzaban velocidades de 1,544 Mbps en el caso de los T1 y 2,048 Mbps en el caso de los E1.

Los enlaces de este tipo para servicios de uso residencial presentaban una serie de inconvenientes, entre los que estaba la necesidad del uso de repetidores, que se colocaban cada kilómetro aproximadamente, lo que hacía que estas líneas resultaran demasiado caras.

Los problemas forzaron la eliminación del uso de repetidores, y fue así como, a mediados de los años 80 se desarrolló HDSL.

Alcanza hasta 2,048 Mbps en ambos sentidos en una distancia máxima hasta 5 Km dependiendo del estado de los pares.

Línea de abonado digital simétrica (SDSL)

Con esta tecnología, *Symmetric Digital Subscriber Line*, que es una evolución del HDSL se consigue las mismas velocidades, también simétricas, que con HDSL, pero usando un único par de cobre. Usa el mismo código de línea, 2B1Q,

La ventaja respecto a HDSL es el uso de un único par, no superándolo ni en velocidad ni en distancia alcanzada.

Línea de abonado digital de alta velocidad simétrica (G.SHDSL)

El diseño de SHDSL, *Single-pair High-speed Digital Subscriber Line*, pretende solventar los inconvenientes que el HDSL y SDSL presentaban.

El G.SHDSL proporciona un servicio simétrico de hasta 2,3 Mbps empleando únicamente un par de abonado y ofrece la posibilidad de obtener el doble de velocidad sobre cuatro hilos en lugar de dos, usando dos pares de abonado, llegando de esta forma a velocidades de 4,624 Mbps.

Las distancias que alcanza están entre los tres y los seis kilómetros, sobre cables de 0,4 mm de sección.

De las ventajas que presenta respecto al HDSL y el SDSL, además de ofrecer mayor velocidad y mayor cobertura, es la mayor normalización, lo que permite la interoperabilidad de productos de distintos fabricantes.

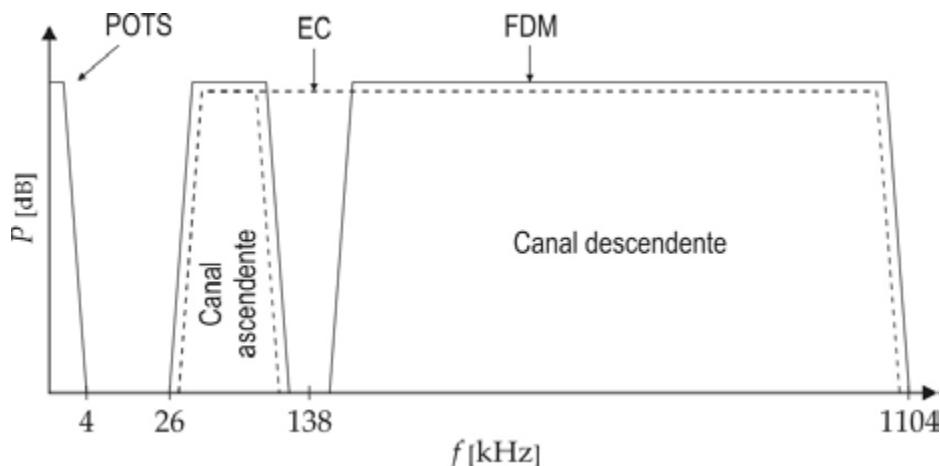
No puede compartir la línea con el servicio de voz tradicional, pero permite el transporte de voz a través de VoIP o de sistemas de VoDSL.

Línea de abonado digital asimétrica (ADSL)

El ADSL, Asymmetric Digital Subscriber Line, y las posteriores versiones mejoradas, es la más extendida en el mercado residencial de todas las tecnologías DSL.

Es una tecnología asimétrica que proporciona mucho más caudal en el canal descendente, de la red hacia el usuario, que en ascendente, del usuario a la red. Esto se realiza dividiendo el ancho de banda del par de cobre en tres secciones, usando técnicas de multiplexación por división en frecuencia, una para el servicio telefónico, otra para el canal ascendente y otra para el canal descendente.

Ofrece una capacidad hacia el usuario (*downstream*) de hasta 8 Mbps, y desde el usuario hacia la red (*upstream*) de hasta 1 Mbps, usando un solo par de cobre de hasta 4 Km.



Línea de abonado digital asimétrica (ADSL2)

Las novedades en ADSL2 respecto al ADSL están destinadas a mejorar el rendimiento y la interoperabilidad. Entre los cambios hay mejoras en la velocidad máxima que ofrece, las distancias alcanzadas, la adaptación de la velocidad y el consumo.

Línea de abonado digital asimétrica (ADSL2+)

Con ADSL2+ se dobla la velocidad que se puede alcanzar con ADSL, llegando a los 20 Mbps en bajada.

Las mejoras en la velocidad tanto del ADSL2 como del ADSL2+ se deben a la utilización de un mayor ancho de banda para la transmisión. El margen de frecuencias en el que operan los módems ADSL va desde los 25 KHz hasta 1,1 MHz, en ADSL2+ el margen superior se amplía hasta los 2,2 MHz.

Línea de abonado digital de muy alta velocidad (VDSL)

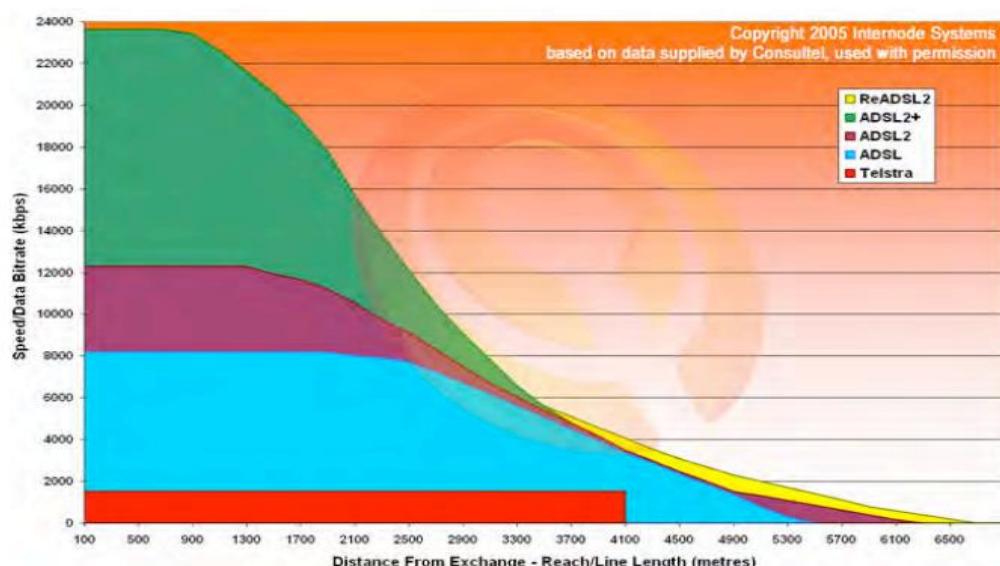
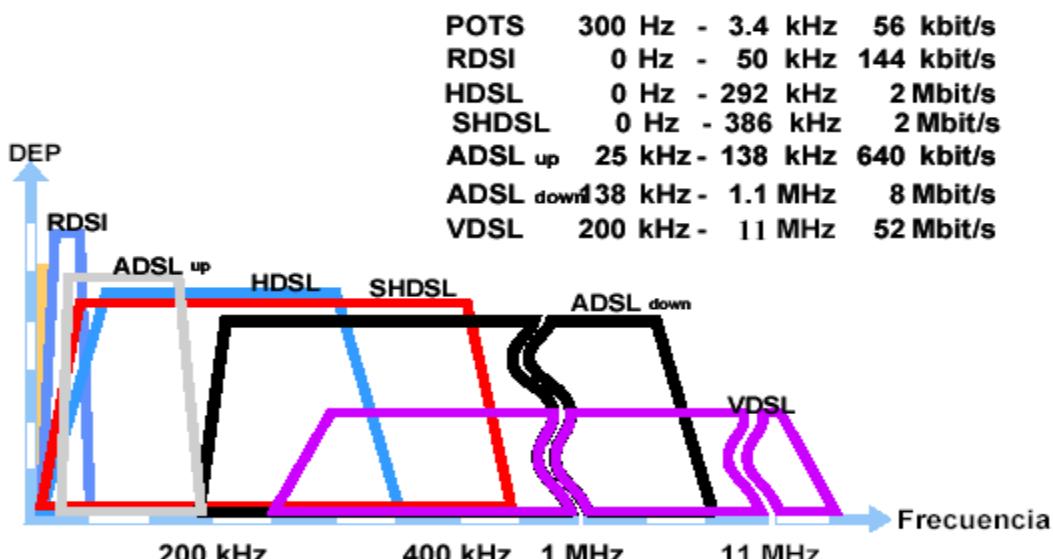
Esta tecnología, *Very High Speed Digital Subscriber Line*, transmite datos de alta velocidad sobre pares de corto alcance.

Existe tanto en versión simétrica como asimétrica, siendo las velocidades conseguidas en su versión simétrica sensiblemente menores que en la asimétrica.

Con VDSL se consigue la transmisión de datos a velocidades de hasta varias decenas de Mbps, pero a distancias de únicamente cientos de metros de la central.

Línea de abonado digital de muy alta velocidad 2 (VDSL2)

El VDSL2, *Very High Speed Digital Subscriber Line 2*, es la norma de comunicaciones DSL más reciente. Diseñado para soportar servicios con necesidad de gran ancho de banda, como aquello que incluyen voz, datos y video, televisión de alta definición o juegos, alcanza velocidades superiores a los 100 Mbps. Permite la transmisión simétrica o asimétrica de datos.



Alcance

La atenuación en la línea crece con la longitud del cable y la frecuencia , y decrece al aumentar el diámetro del cable

Esto explica que el caudal máximo que se puede conseguir mediante los módems ADSL varíe en función de la longitud del bucle y las características del mismo.

Las velocidades de transmisión dependen de la longitud y diámetro del cable, pero también influyen:

- Presencia de tramas multiplexadas.
- Estado de conservación del bucle.
- Acoplamiento de ruido.
- Diafonía introducida por otros servicios (xDSL).

La capacidad de transmisión decrece al aumentar la longitud del bucle. Al disminuir el diámetro del bucle también decrece la longitud máxima de alcance

La presencia de ruido externo provoca la reducción de la relación Señal/Ruido con la que trabaja cada una de las subportadoras, y esa disminución se traduce, como habíamos visto al hablar de la modulación, en una reducción del caudal de datos que modula a cada subportadora, lo que a su vez implica una reducción del caudal total que se puede transmitir a través del enlace entre el ATU-R y el ATU-C

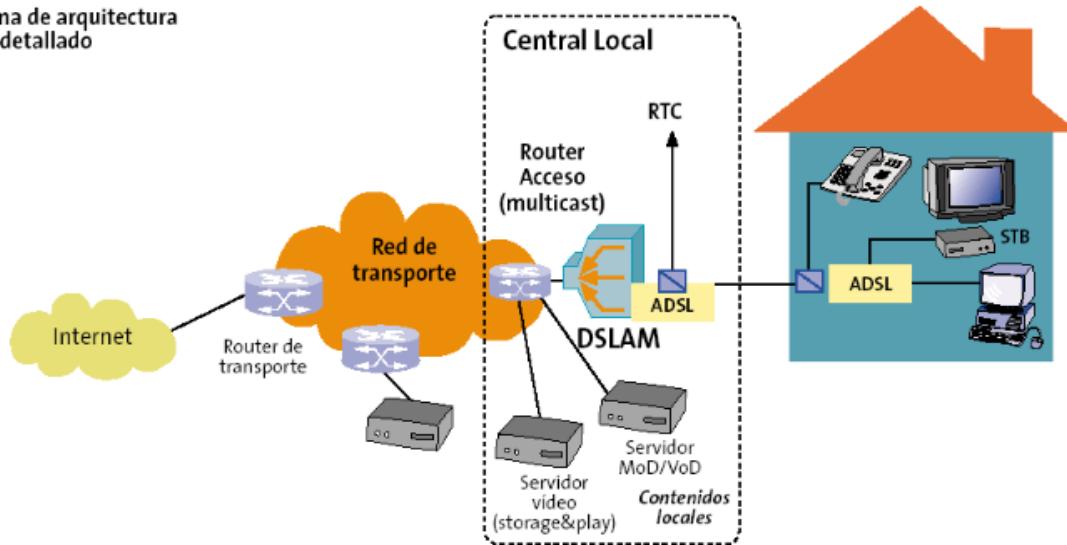
Arquitecturas de Red

El común denominador de todas las tecnologías xDSL, entre ellas el ADSL, es que funcionan sobre bucle de abonado local. Como consecuencia de ello las redes de acceso

xDSL se han visto impulsadas por las operadoras clásicas de telefonía, como tecnología que permitiera el acceso al servicio de banda ancha sobre los pares de cobre, que daban servicio a la telefonía. Esta tecnología se basa fundamentalmente en la utilización por parte de las compañías proveedoras del par trenzado que llega hasta cada teléfono (en caso de particulares) o centralitas (empresas u otros). Gracias a esto la tecnología no requiere de la implantación de ninguna red, o coste alguno, exceptuando los equipos que se encargan de transmitir y adaptar la información que va a ser enviada desde el origen.

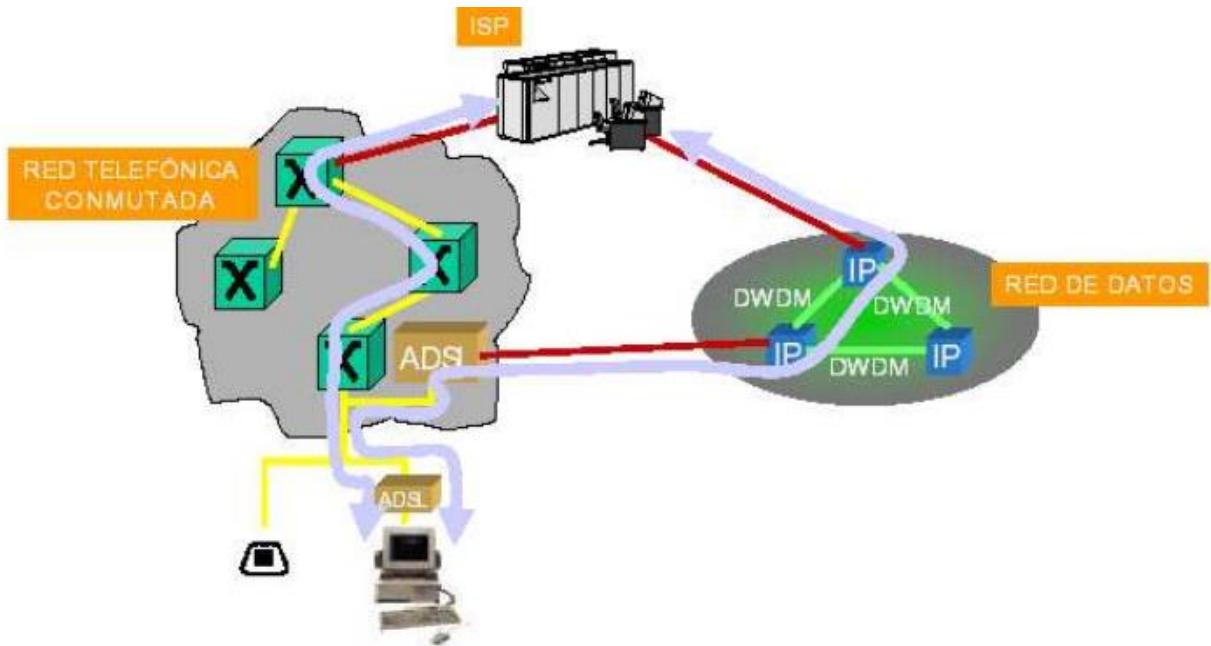
La arquitectura fundamental de las tecnologías xDSL, y en particular de ADSL, se basa en la existencia de una pareja de módems situados a ambos extremos del par de cobre. Las diversas modulaciones empleadas no pueden transportarse a gran distancia ni sobre cualquier categoría de cable ni tampoco la señal proveniente del enlace ascendente puede atravesar los equipos de conmutación de circuitos de la RTB, por lo tanto estos enlaces de datos solo pueden establecerse entre el usuario y la central

Esquema de arquitectura de red detallado



Las arquitecturas de las redes xDSL, y ADSL, son configuraciones de enlace punto a punto, desde el cliente del servicio y la central de conmutación más cercana. Esto hace que los enlaces desde y hasta los usuarios sean dedicados y no compartidos por más de un usuario. Esta es sin duda una de las características más destacadas, ya que el resto de las tecnologías (HFC, LMDS, WLAN, Satélite) son medios netamente compartidos por los usuarios del servicio. A partir de la central, generalmente la arquitectura de los sistemas ADSL se basa en redes de transmisión y multiplexación ATM, y en redes de datos basadas en IP. De esta manera, la transmisión es transparente para los usuarios, ya que desde la central es función del operador como se da salida a los datos.

Las centrales que soportan esas tecnologías deben disponer de los equipos de agregación de la parte reservada a la red (bucles de abonado), para combinar el tráfico de datos de cada uno de los usuarios, y que este se pueda redirigir hacia la red troncal (backbone desde el que se da servicio). Los equipos destinados a este fin se denominan DSLAM (DSL Access Multiplexer) y terminan el enlace físico que soporta las modulaciones de ADSL. Así los flujos bidireccionales de datos correspondientes a cada par de cobre, se injetan hacia el troncal, en norma general, sobre una jerarquía de conmutación de paquetes ATM.

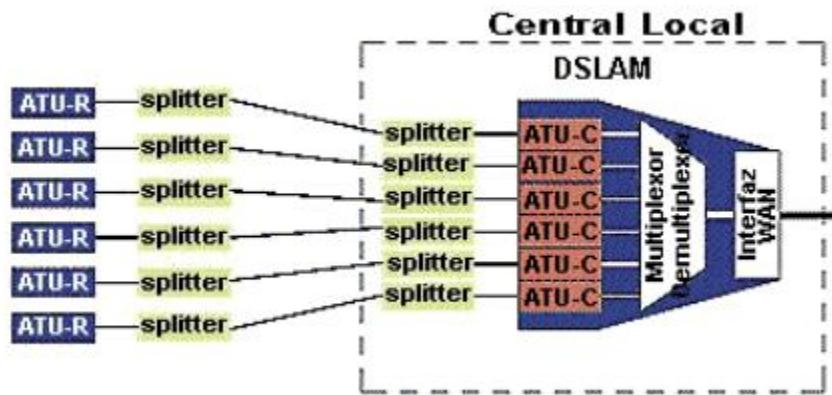


-Arquitectura clásica de acceso a Internet por ADSL

DSLAM

El ADSL necesita una pareja de módems por cada usuario: uno en el domicilio del usuario (ATU-R) y otro (ATU-C) en la central local a la que llega el bucle de ese usuario. Esto complica el despliegue de esta tecnología de acceso en las centrales. Para solucionar este problema surgió el DSLAM ("Digital Subscriber Line Access Multiplexer"): un chasis que agrupa gran número de tarjetas, cada una de las cuales consta de varios módems ATU-C, y que además realiza las siguientes funciones:

- Concentra en un mismo chasis los módems de central de varios usuarios.
- Concentra (Multiplexa/demultiplexa) el tráfico de todos los enlaces ADSL hacia una red WAN.
- Realiza funciones de nivel de enlace (protocolo ATM sobre ADSL) entre el módem de usuario y el de central



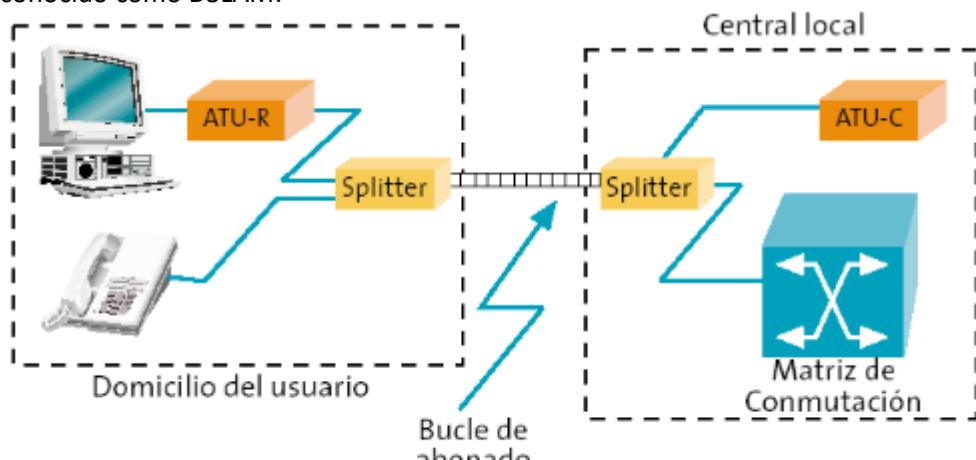
Elementos de la red

Módem ADSL o ATU-C (ADSL Terminal Unit Central). Módem ADSL, que reside en el nodo de acceso y cuya función principal es lade modular la información digital para así, adaptarla bucle de abonado.

Microfiltros o Splitters. Ambos se encargan de separar la voz de los datos transmitidos, de manera que la voz vaya desde el teléfono de abonado hasta la PSTN (Red Telefónica Conmutada Pública) y los datos desde el equipo terminal hasta la red de acceso al servicio.

Bucle. Por el que se envían las señales de voz y datos. La modulación evita que interfieran las bandas de ambos.

ATU-R (ADSL Terminal Unit Remote). Módem ADSL que reside en las dependencias del abonado. Convierte la información digital de la red de usuario en celdas ATM y la modula para que pueda enviarse por el bucle de abonado. En algunos casos, también puede hacer funciones de encaminamiento de red de usuario. Los DSLAM (Digital Subscriber Line Access Multiplexer) se ubican en la central remota y son un banco de módems encargados de recibir la información proveniente de las ATU-C, decodificarla y multiplexarla digitalmente, para poder a continuación transportarla al destino deseado. multiplexor digital DSL, conocido como DSLAM:



Arquitectura ADSL.

Modulación en ADSL

Una de las claves que permiten el acceso de banda ancha en el par de cobre esta sin duda en las modulaciones empleadas en ADSL. El objetivo de los sistemas ADSL es llegar a la mayor parte de los usuarios dentro del Área de servicio, que no es más que la zona geográfica en la que la central de conmutación puede dar servicio a los usuarios. Existen grandes limitaciones que no permiten la implantación de las tecnologías ADSL en algunos lugares. Sin duda si la distancia a la central de conmutación supera la distancia máxima, el servicio es inviable. Además el estado de los pares es fundamental para determinar la calidad y la distancia máxima donde el servicio es operativo. En cuanto a la velocidad que se puede alcanzar en función del tipo de par trenzado ADSL verifica (de forma teórica):

1. Velocidades de datos de 1,5 ó 2 Mbps; par 0,5 mm, distancia 5,5 km
2. Velocidades de datos de 1,5 ó 2Mbps; par 0,4 mm,distancia 4,6 km
3. Velocidad de datos de 6,1 Mbps; par 0,5 mm, distancia 3,7 km
4. Velocidad de datos de 6,1 Mbps; par 0,4 mm, distancia 2,7 km

Vemos como en un par de cobre la atenuación por unidad de longitud aumenta a medida que se incrementa la frecuencia de las señales transmitidas y disminuye cuando se incrementa el diámetro del hilo. Y cuanto mayor es la longitud del bucle, tanto mayor es la atenuación total que sufren las señales transmitidas. Ambas cosas explican que la tasa máxima que se puede conseguir mediante los módems ADSL varíe en función de la longitud del bucle de abonado.

Las técnicas de modulación usadas para xDSL son 2B1Q, 2Bit 1 Quaternary, CAP, Carrierless Amplitude Phase Modulation, y DMT, Discrete Multitone Modulation, aunque es la técnica DMT, estandarizada por ANSI, ETSI y la UIT la que domina actualmente.

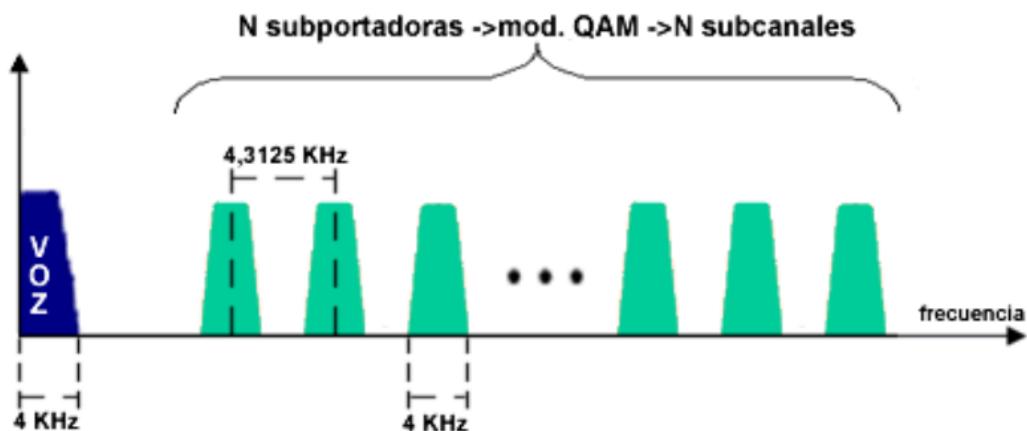
La modulación DMT es un método basado en el uso de múltiples portadoras. El rango de frecuencias usadas es dividido en bandas de frecuencias o canales, separadas entre sí 4,3125 KHz. Cada portadora ocupa 4 KHz. Dividiendo el espectro de frecuencias en múltiples canales DMT se consigue un mejor funcionamiento ante las presencia de fuentes interferentes, el reparto del flujo de datos se hace en función de la relación señal a ruido estimada en cada una de las portadoras.

DMT presenta algunas ventajas sobre CAP derivadas del uso de múltiples portadoras. Cada uno de los canales se modula en amplitud y fase, adaptando la tasa de bit en cada uno de ellos a su capacidad real. DMT realiza un chequeo constante sobre cada portadora, lo que permite ajustar la tasa de bit a ganancias diferentes según la frecuencia, incluso eliminando portadoras afectadas por el ruido. De esta forma los sistemas DMT son capaces de aproximarse más al límite teórico del canal, proporcionando más velocidad y mayor alcance

Básicamente consiste en el empleo de múltiples portadoras y no sólo una, que es lo que se hace en los módems de banda vocal.

Cada una de estas portadoras (denominadas subportadoras) es modulada en cuadratura (modulación QAM) por una parte del flujo total de datos que se van a transmitir.

Estas subportadoras están separadas entre sí 4,3125 KHz, y el ancho de banda que ocupa cada subportadora modulada es de 4 KHz.



El reparto del flujo de datos entre subportadoras se hace en función de la estimación de la relación Señal/Ruido en la banda asignada a cada una de ellas.

Cuanto mayor es esta relación, tanto mayor es el caudal que puede transmitir por una subportadora.

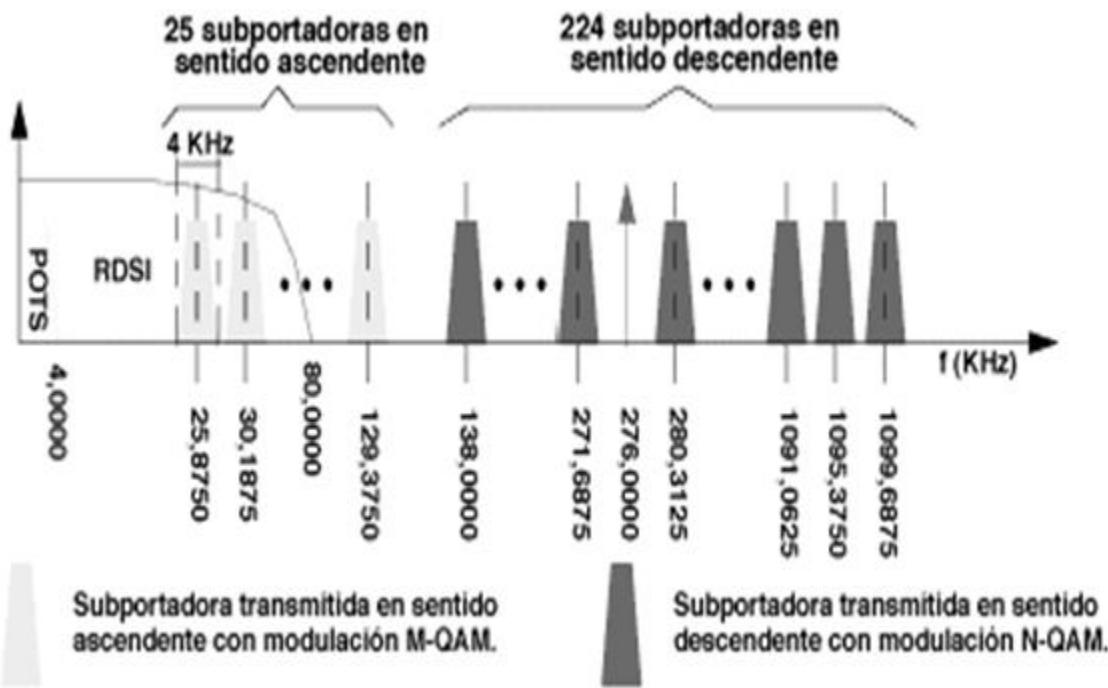
Esta estimación de la relación Señal/Ruido se hace al comienzo, cuando se establece el enlace entre el ATU-R y el ATU-C, por medio de una secuencia de entrenamiento predefinida.

La técnica de modulación usada es la misma tanto en el ATU-R como en el ATU-C. La única diferencia estriba en que el ATU-C dispone de hasta 512 subportadoras, mientras que el ATU-R sólo puede disponer como máximo de 64.



Sea cual sea la técnica de modulación utilizada, el estándar ANSI T1.413 especifica que ADSL debe utilizar Multiplexación por División en la Frecuencia (FDM) o Cancelación de Eco para conseguir una comunicación full-duplex. Ambas técnicas reservan los subcanales más bajos para la voz analógica.

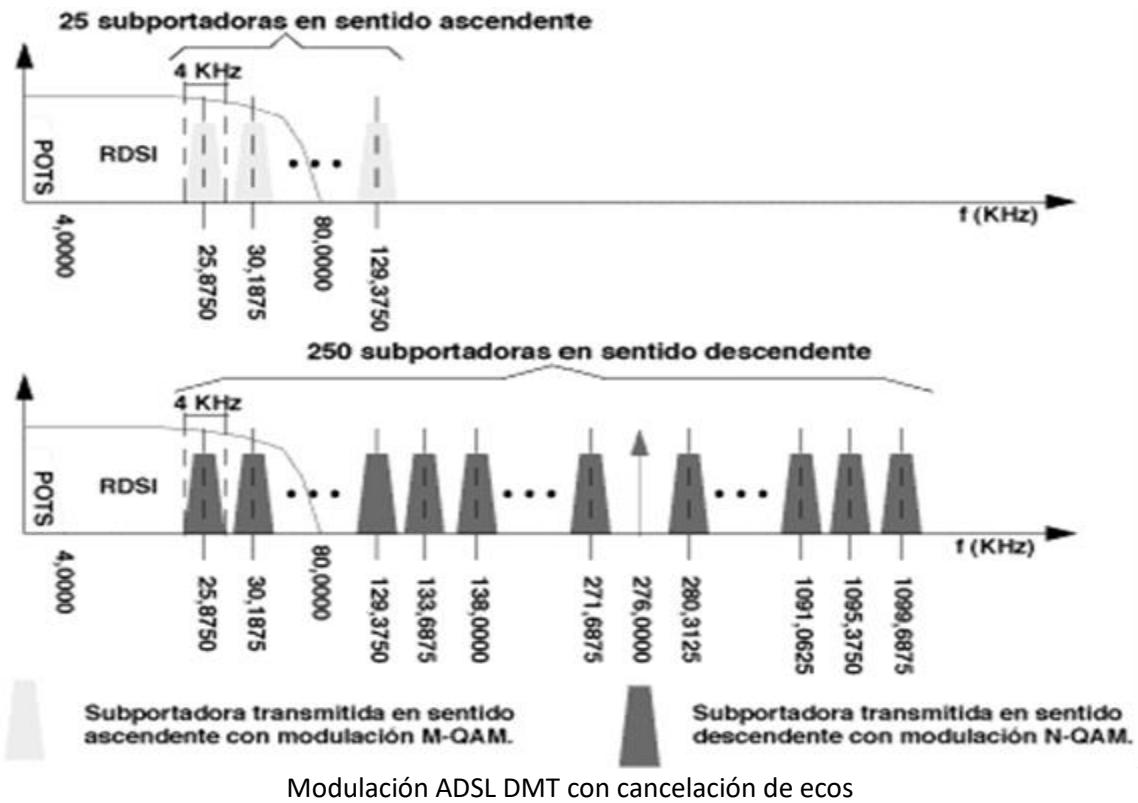
El estándar ANSI T1.413 ha adoptado DMT (Discrete Multitone -Multitonos Discretos) como la técnica de modulación en ADSL. DMT demuestra mayor inmunidad al ruido, mayor flexibilidad en la velocidad de transmisión y mayor facilidad para adaptarse a las características de la línea que otros métodos. Todo ello se traduce en fiabilidad en largas distancias de línea. La multiplexación por División en la Frecuencia (FDM) divide el rango de frecuencias en dos bandas, una de upstream (sentido ascendente) y otra de downstream (sentido descendente), lo que simplifica el diseño de los módems, aunque reduce la capacidad de transmisión en sentido descendente, no tanto por el menor número de subportadoras disponibles como por el hecho de que las de menor frecuencia, aquéllas para las que la atenuación del par de cobre es menor, no están disponibles



Modulación ADSL DMT con FDM

La Cancelación de Eco elimina la posibilidad de que la señal en una dirección sea interpretada como "una señal producida por una persona" en la dirección opuesta, y por tanto devuelta en forma de eco hacia el origen.

Por tanto separa de las señales correspondientes a los dos sentidos de transmisión, permitiendo mayores caudales a costa de una mayor complejidad en el diseño de los módems



Modulación ADSL DMT con cancelación de ecos

Como se puede comprobar, la modulación DMT empleada parece y realmente es bastante complicada, pero el algoritmo de modulación se traduce en una IFFT en el modulador, y en una FFT en el demodulador situado al otro lado del bucle.

Estas operaciones se pueden efectuar fácilmente si el núcleo del módem se desarrolla sobre un DSP.

- El modulador del ATU-C, hace una IFFT de 512 muestras sobre el flujo de datos que se ha de enviar en sentido descendente.
- El modulador del ATU-R, hace una IFFT de 64 muestras sobre el flujo de datos que se ha de enviar en sentido ascendente.
- El demodulador del ATU-C, hace una FFT de 64 muestras tomadas de la señal "upstream" que recibe.
- El demodulador del ATU-R, hace una FFT, sobre 512 muestras de la señal ascendente recibida.

En las dos figuras anteriores se han presentado las dos modalidades dentro del ADSL con modulación DMT: FDM y cancelación de ecos.

En la primera, los espectros de las señales ascendente y descendente no se solapan, lo que simplifica el diseño de los módems, aunque reduce la capacidad de transmisión en sentido descendente, no tanto por el menor número de subportadoras disponibles como por el hecho de que las de menor frecuencia, aquéllas para las que la atenuación del par de cobre es menor, no están disponibles.

La segunda modalidad, basada en un cancelador de ecos para la separación de las señales correspondientes a los dos sentidos de transmisión, permite mayores caudales a costa de una mayor complejidad en el diseño.

En un par de cobre la atenuación por unidad de longitud aumenta a medida que se incrementa la frecuencia de las señales transmitidas. Y cuanto mayor es la longitud del bucle, tanto mayor es la atenuación total que sufren las señales transmitidas.

Ambas cosas explican que el caudal máximo que se puede conseguir mediante los módems ADSL varíe en función de la longitud del bucle de abonado.

La presencia de ruido externo provoca la reducción de la relación Señal/Ruido con la que trabaja cada una de las subportadoras, y esa disminución se traduce en una reducción del caudal de datos que modula a cada subportadora, lo que a su vez implica una reducción del caudal total que se puede transmitir a través del enlace entre el ATU-R y el ATU-C.

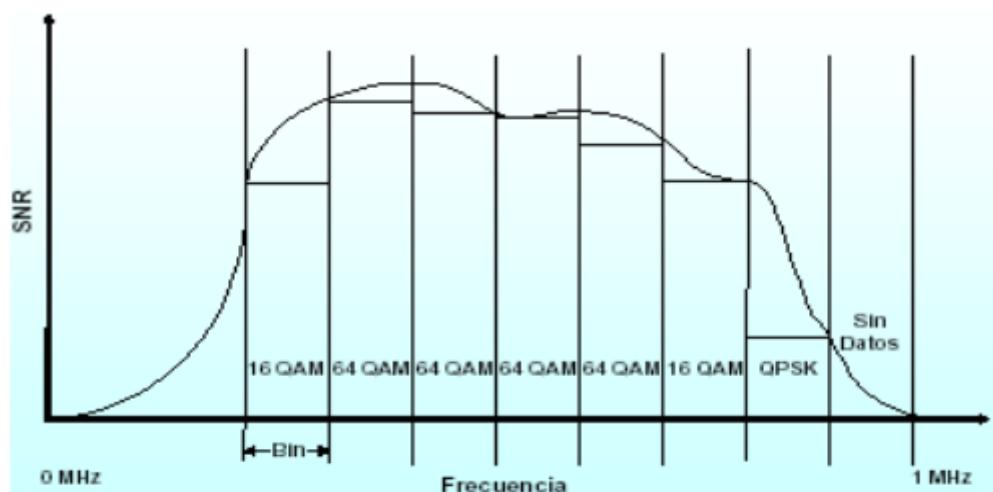
Hasta una distancia de 2,6 Km de la central, en presencia de ruido (caso peor), se obtiene un caudal de 2 Mbps en sentido descendente y 0,9 Mbps en sentido ascendente.

Esto supone que en la práctica, teniendo en cuenta la longitud media del bucle de abonado en las zonas urbanas, la mayor parte de los usuarios están en condiciones de recibir por medio del ADSL un caudal superior a los 2 Mbps.

Este caudal es suficiente para muchos servicios de banda ancha, y desde luego puede satisfacer las necesidades de cualquier internauta, teletrabajador así como de muchas empresas pequeñas y medianas.

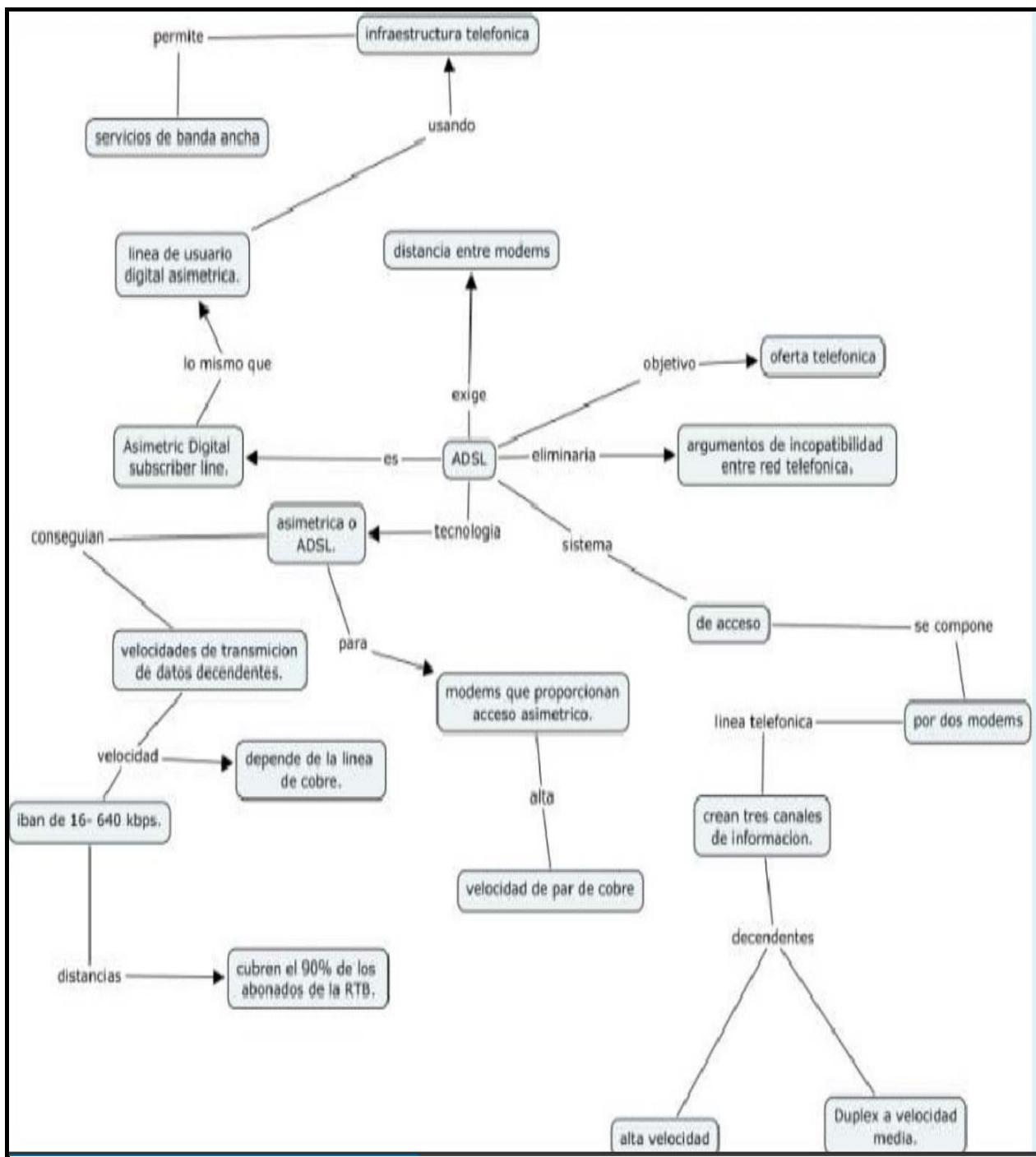
Existe una variante de DTM, denominada DWMT (Discrete Wavelet Multi-Tone) que es algo más compleja pero ofrece aún mayor rendimiento al crear mayor aislamiento entre los 256 subcanales, mediante el uso de transformadas Wavelet (algoritmo para descomponer una señal en elementos más simples). La transformada Wavelet produce armónicos de energía más bajo, lo cual hace de esto una tarea más simple para detectar la señal decodificada en la recepción. Esta variante podría ser el protocolo estándar para transmisiones ADSL a larga distancia y donde existan entornos con un alto nivel de interferencias

Cada portadoras de DMT (denominadas subportadoras) es modulada en cuadratura (modulación QAM) por una parte del flujo total de datos que se van a transmitir. Estas subportadoras están separadas entre sí 4,3125 KHz, y el ancho de banda que ocupa cada subportadora modulada es de 4 KHz. El reparto del flujo de datos entre subportadoras se hace en función de la estimación de la relación Señal/Ruido en la banda asignada a cada una de ellas. Cuanto mayor es esta relación, tanto mayor es el caudal que puede transmitir por una subportadora. Esta estimación de la SNR se hace al comienzo, cuando se establece el enlace entre el ATU-R y el ATU-C, por medio de una secuencia de datos predefinida



- Asignación de la tasa transmisión en función de SNR.

Mapa Conceptual

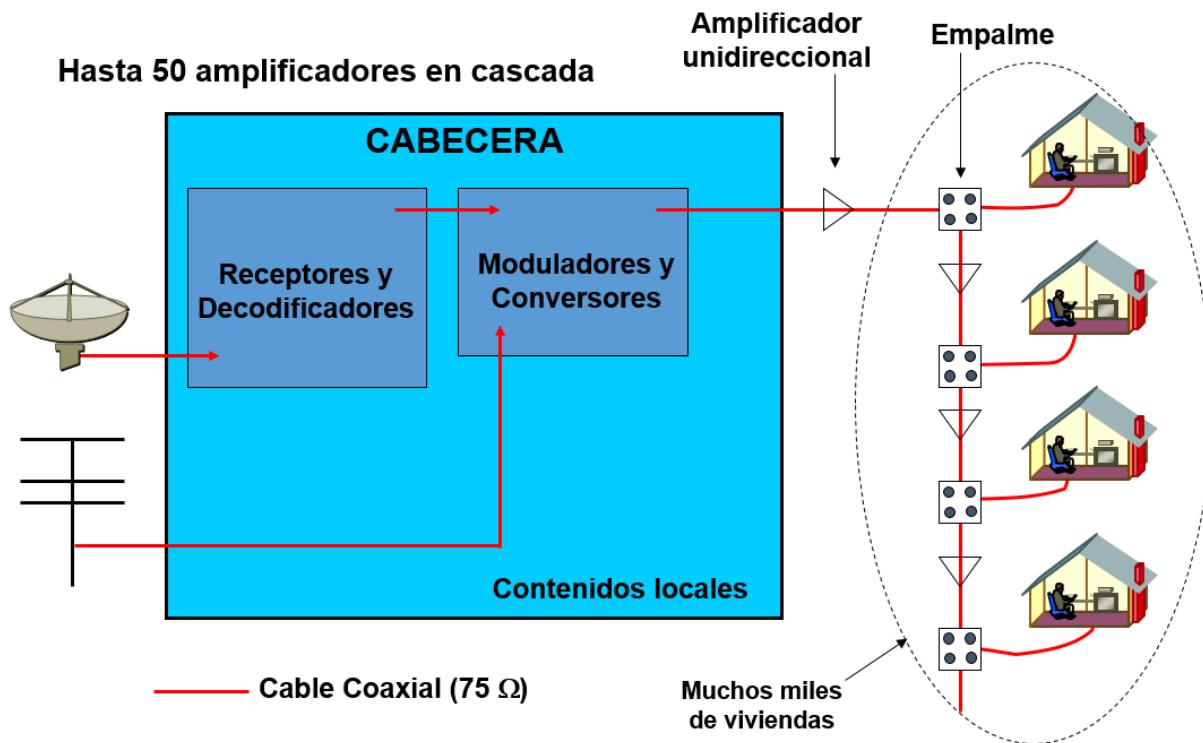


Redes CATV

RED HFC (Hibrid fiber-coaxial)

Introducción

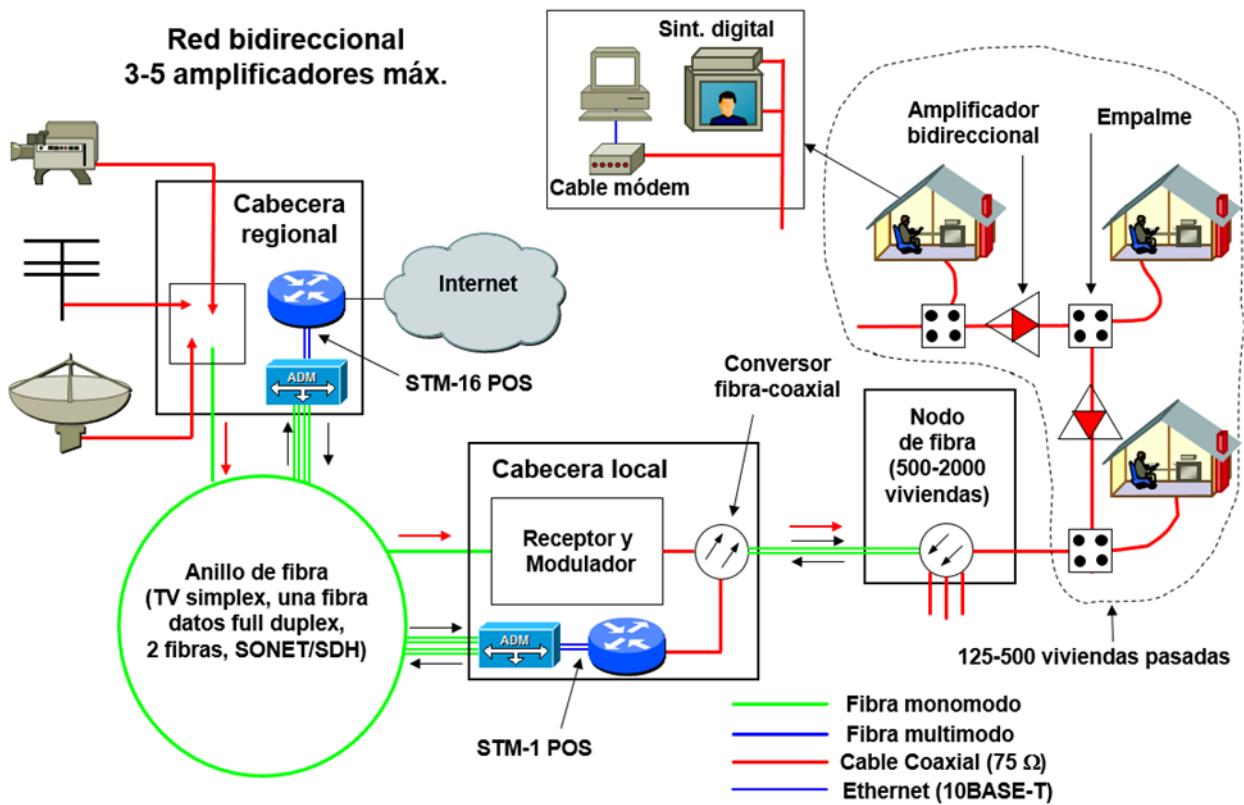
Las redes híbridas de fibra óptica y cable coaxial, HFC, fueron implementadas en un principio por operadores de TV Cable o *televisión de antena comunitaria*. Esta consta de dividir las zonas de servicios en grupos de entre 500 a 2000 viviendas llamados nodos, la señal llega a cada nodo por cables de fibra y esta es repartida dentro de los nodos por cable coaxial, los que posteriormente incluyeron servicios como Video on Demand, Pay Per View, etc. Con el avance de la tecnología, las redes de TV Cable fueron capaces de ofrecer otros servicios multimedia como telefonía y acceso a Internet de Banda Ancha. Para esto, modificaron las mismas redes existentes, transformándose en *Operadores Multi-Servicio*, MSO. La red sufrió modificaciones importantes, pasando de ser una red prácticamente unidireccional a ser una red bidireccional desbalanceada.



En la discusión actual sobre telecomunicaciones se encuentran habitualmente términos como convergencia IMS (IP Multimedia Subsystem) y Redes de Nueva Generación, NGN (Next Generation Networking). HFC representa un bloque fundamental en la comprensión de estos conceptos. Un factor clave para el éxito de los operadores de cable que pretenden adecuar sus redes para la próxima generación de arquitecturas de comunicaciones, será la capacidad del personal técnico para evaluar las diversas opciones disponibles. Por otro lado, los MSO, se enfrentan a otras consideraciones como el manejo de la compatibilidad de las diversas normas de próxima generación con las arquitecturas existentes y cómo determinar el momento óptimo para realizar este cambio.

La estandarización de las redes HFC se ha hecho mediante el estándar DOCSIS.

DOCSIS son las siglas de Especificación de Interfaz de Servicios de Datos Por Cable (Data Over Cable Service Interface Specification), es un estándar internacional, no comercial, que define los requerimientos de la interfaz de soporte de comunicaciones y operaciones para los sistemas de datos por cable, lo cual permite añadir transferencias de datos de alta velocidad a un sistema CATV sobre una infraestructura Híbrida-FibraCoaxial (HFC) existente.



¿Qué es una red HFC?

Una red HFC es una red de telecomunicaciones por cable que combina la fibra óptica y el cable coaxial como soportes de la transmisión de las señales. Se compone básicamente de cuatro partes claramente diferenciadas: la cabecera, la red troncal, la red de distribución, y la red de acometida de los abonados.

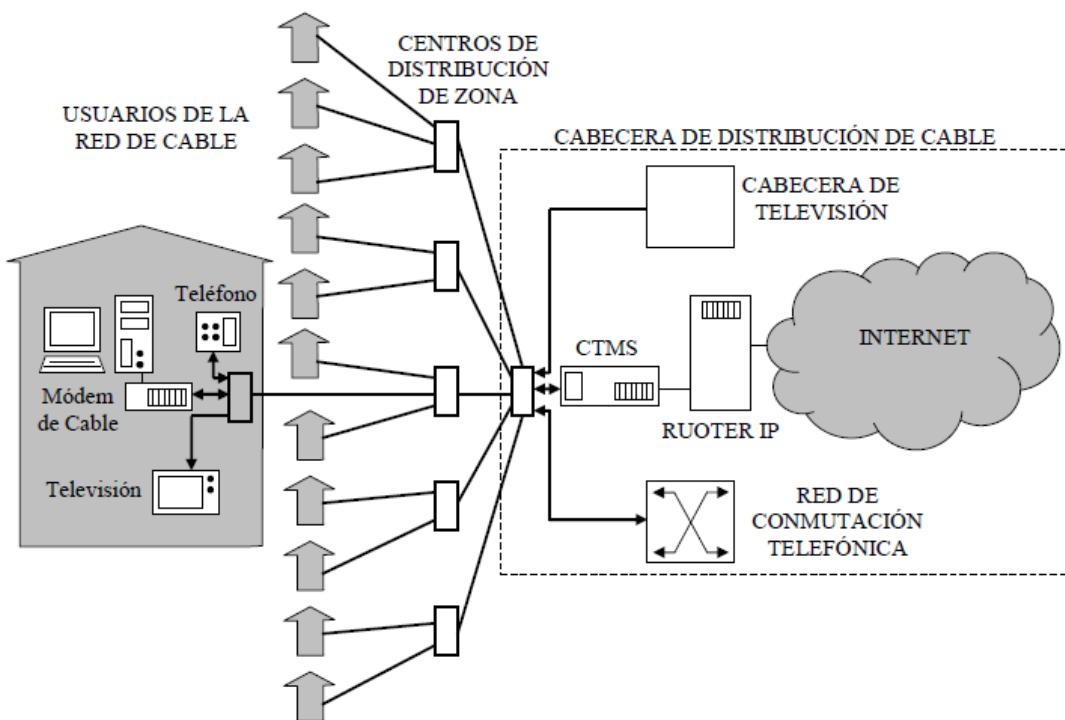
La cabecera es el centro desde el que se gobierna todo el sistema. Su complejidad depende de los servicios que ha de prestar la red. Por ejemplo, para el servicio básico de distribución de señales unidireccionales de televisión (analógicas y digitales) dispone de una serie de equipos de recepción de televisión terrenal, vía satélite y de microondas, así como de enlaces con otras cabeceras o estudios de producción. Las señales analógicas se acondicionan para su transmisión por el medio cable y se multiplexan en frecuencia en la banda comprendida entre los 86 y los 606 MHz.. Las señales digitales de vídeo, audio y datos que forman los canales de televisión digital se multiplexarán para formar el flujo de transporte MPEG (Motion Picture Experts Group).

Una vez añadida la codificación para corrección de errores y realizada una intercalación de los bits para evitar las ráfagas de errores, se utiliza un modulador QAM (modulación de amplitud en cuadratura) para transmitir la información hasta el equipo terminal de abonado (set-top-box).

Los canales digitales de televisión y otros servicios digitales se ubican en la banda comprendida entre 606y 862 MHz.

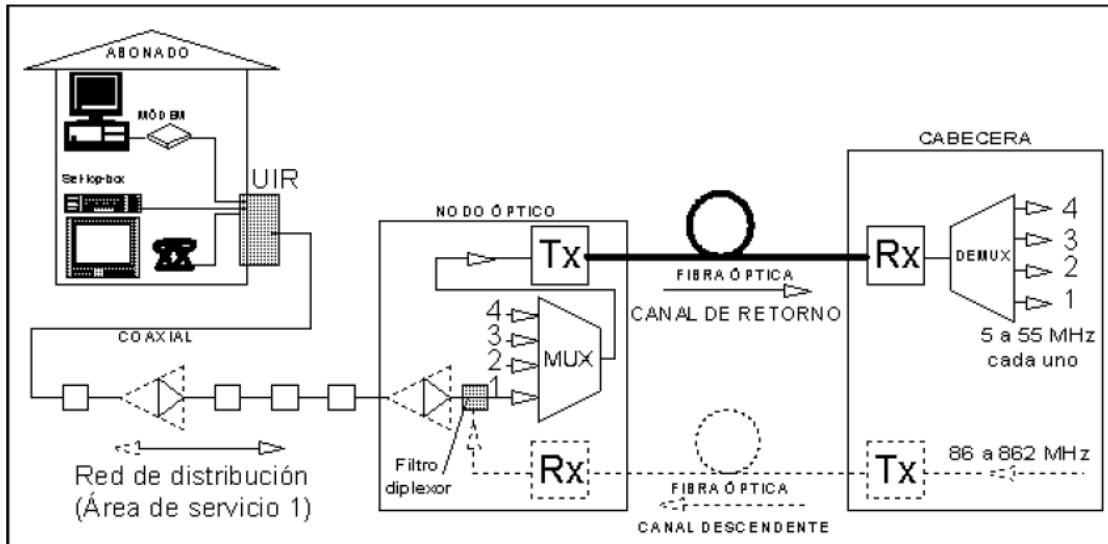
La cabecera es también la encargada de monitorizar la red y supervisar su correcto funcionamiento. El monitorizado se está convirtiendo rápidamente en un requerimiento básico de las redes de cable, debido a la actual complejidad de las nuevas arquitecturas y a la sofisticación de los nuevos servicios que transportan, que exigen de la red una fiabilidad muy alta. En la cabecera se realizan además todo tipo de funciones de tarificación y de control de los servicios prestados a los abonados.

La red troncal suele presentar una estructura en forma de anillos redundantes de fibra óptica que une a un conjunto de nodos primarios. Esta estructura emplea habitualmente tecnología PDH o SDH (Jerarquía Digital Plesiócrona y Síncrona, respectivamente), que permite construir redes basadas en ATM (Modo de Transferencia Asíncrono). Los nodos primarios alimentan a otros nodos (secundarios) mediante enlaces punto a punto o bien mediante anillos. En éstos nodos secundarios las señales ópticas se convierten a señales eléctricas y se distribuyen a los hogares de los abonados a través de una estructura tipo bus de coaxial, la red de distribución. Cada nodo sirve a unos pocos cientos de hogares (500 es un tamaño habitual en las redes HFC), lo cual permite emplear cascadas de 2 ó 3 amplificadores de banda ancha como máximo. Con esto se consiguen unos buenos niveles de ruido y distorsión en el canal descendente (de la cabecera al abonado). La red de acometida salva el último tramo del recorrido de las señales descendentes, desde la última derivación hasta la base de conexión de abonado.



Canal de retorno:

Las modernas redes de telecomunicaciones por cable híbridas fibra óptica-coaxial han de estar preparadas para poder ofrecer un amplio abanico de aplicaciones y servicios a sus abonados. La mayoría de estos servicios requieren de la red la capacidad de establecer comunicaciones bidireccionales entre la cabecera y los equipos terminales de abonado, y por tanto exigen la existencia de un canal de comunicaciones para la vía ascendente o de retorno, del abonado a la cabecera.



El canal de retorno ocupa en las redes HFC el espectro comprendido entre 5 y 55 MHz. Este ancho de banda lo comparten todos los hogares servidos por un nodo óptico. Los retornos de distintos nodos llegan a la cabecera por distintas vías o multiplexados a distintas frecuencias y/o longitudes de onda. Una señal generada por el equipo terminal de un abonado recorre la red de distribución en sentido ascendente, pasando por amplificadores bidireccionales hasta llegar al nodo óptico. Allí convergen las señales de retorno de todos los abonados, que se convierten en señales ópticas en el láser de retorno, el cual las transmite hacia la cabecera.

El cable MODEM:

Las redes HFC, mediante el uso de módems especialmente diseñados para las comunicaciones digitales en redes de cable, tienen capacidad para ofrecer servicios de acceso a redes de datos como Internet a velocidades cientos de veces superiores a las que el usuario medio está acostumbrado (hasta 33.6 Kbps desde casa, a través de la red telefónica). Los módems de cable están convirtiendo las redes de CATV en verdaderos proveedores de servicios de telecomunicación de vídeo, voz, y datos.

Un módem de cable típico tiene las siguientes características: Es un módem asimétrico. Recibe datos a velocidades de hasta 30 Mbps. y transmite hasta 10 Mbps. (valores más normales son 10 y alrededor de 1 Mbps., descendente y ascendente, respectivamente).

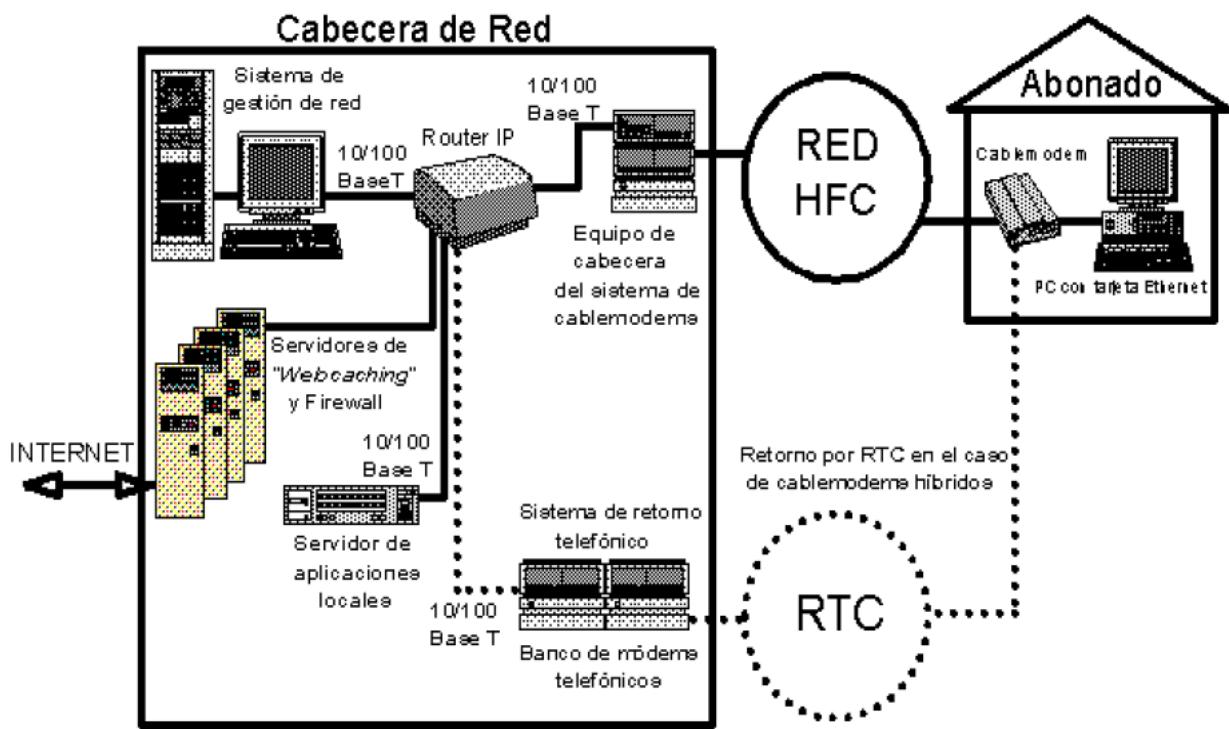
Se conecta a la red HFC mediante un conector de cable coaxial tipo F, y al PC del abonado a través de una tarjeta Ethernet 10BaseT que éste debe incorporar. La recepción de datos se realiza por un canal de entre 6 y 8 MHz. del espectro descendente (entre 50 y 860 MHz.) con modulación digital 64-QAM (Quadrature Amplitude Modulation).

El módem de cable demodula la señal recibida y encapsula el flujo de bits en paquetes Ethernet. El PC del abonado ve la red HFC como una enorme red local Ethernet. En sentido ascendente, el módem de cable descompone los paquetes Ethernet que recibe del PC y los convierte en celdas ATM o en tramas con otro formato propietario. Utiliza un canal de unos 2 MHz. Del espectro de retorno (entre 5 y 55 MHz.) con modulación digital QPSK (Quaternary Phase Shift Keying).

La cabecera ha de disponer de unos equipos que realicen funciones de router y switch, y que adapten el tráfico de datos de la red HFC al protocolo IP. Además, debe existir un sistema de gestión de red y de

abonados, pudiendo también existir un servidor que realice funciones de caching de información y actúe como Firewall.

La transmisión de datos en redes HFC se realiza a través de un medio de acceso compartido, en el que un grupo más o menos grande de usuarios comparte un ancho de banda generalmente grande, un canal de 6 MHz., por ejemplo, con una capacidad de entre 10 y 30 Mbps.



Topologías y elementos de las redes HFC

Veamos una breve descripción de los elementos físicos que componen topología de una red HFC típica.

Cabecera

La principal función de las Cabeceras es combinar distintas fuentes de información para introducirlas en la red. En el caso de la televisión por cable, la Cabecera es la encargada de combinar las señales provenientes de distintos lugares y medios físicos e incluso tipos de información y formas de codificación.

Antiguamente los operadores de cable combinaban señales provenientes de satélites, cables e incluso antenas radioeléctricas. En la actualidad, los nuevos operadores de cable son, en su mayoría, Operadores Multi-Servicio, proporcionando telefonía e Internet de alta velocidad. Esto se consigue utilizando técnicas de división por frecuencia.

Para proporcionar telefonía, las Cabeceras incorporan un nodo de acceso denominado Host Digital Terminal para controlar la asignación dinámica de los canales del cable a los abonados, cuando se producen llamadas entrantes y salientes.

Para la conexión a Internet, es necesaria una comunicación bidireccional y ésta es obtenida asignando una parte relativamente pequeña del ancho de banda, con una tasa de datos de 500 kbps a 1,5 Mbps que se conoce como Upstream de comunicación de datos del suscriptor al operador

Por otro lado, el ancho de banda de descarga suele ser más grande, con una tasa de datos de hasta 35 Mbps, que se conoce como comunicación de datos de Downstream del operador al suscriptor. En esta técnica se utilizan dos módems: uno en el extremo del usuario conocidos como Cable módems, CM y otro en la Cabecera del operador, conocido como Sistema de Terminación de Cable módems, CMTS. El operador conecta su Cabecera a un Proveedor de Servicios de Internet, ISP. Los CMTS pueden manejar la conexión a Internet de entre 4000 y 30000 usuarios. Una Cabecera puede tener más de un CMTS.

Este dispositivo realiza la codificación, modulación y gestión de acceso al medio compartido por los CM, proporcionando una interfaz Ethernet. En la Cabecera se encuentran, además otros equipos como el Switch Ethernet, un servidor AAA (Authentication, Authorization and Accounting), para control de acceso y tarificación y un servidor de contenidos locales y de caching para las páginas más visitadas.

Los proveedores de cable también tendrán servidores para la contabilidad y registro,

Protocolo de Configuración de Anfitrión Dinámico, DHCP para asignar y administrar las direcciones IP de todos los usuarios de sistema del cable y control de los servidores.

CMTS

CMTS son las siglas de Cable Modem Termination System (Sistema de Terminación de Cablemódems).

Es un equipo que se encuentra normalmente en la cabecera de la compañía de cable y se utiliza para proporcionar servicios de datos de alta velocidad, como Internet por cable o Voz sobre IP, a los abonados.

Para proporcionar dichos servicios de alta velocidad, la compañía conecta su cabecera a Internet mediante enlaces de datos de alta capacidad a un proveedor de servicios de red. En la parte de abonado de la cabecera, el CMTS habilita la comunicación con los cablemódems de los abonados. Dependiendo del CMTS, el número de cablemódems que puede manejar varía entre 4.000 y 150.000 o incluso más. Una determinada cabecera puede tener entre media docena y una docena de CMTS (a veces más) para dar servicio al conjunto de cablemódems que dependen de esa cabecera.

Para entender lo que es un CMTS se puede pensar en un router con conexiones Ethernet en un extremo y conexiones RF (radiofrecuencia) coaxiales en el otro. La interfaz RF transporta las señales de RF hacia y desde el cablemódem del abonado.

De hecho, la mayoría de CMTS tienen tanto conexiones Ethernet (u otras interfaces de alta velocidad más tradicionales) como a interfaces RF. De esta forma, el tráfico que llega de Internet puede ser enrutado (o puenteado) mediante la interfaz Ethernet, a través del CMTS y después a las interfaces RF que están conectadas a la red HFC de la compañía de cable. El tráfico viaja por la red HFC para acabar en el cablemódem del domicilio del abonado. Obviamente, el tráfico que sale del domicilio del abonado pasará por el cablemódem y saldrá a Internet siguiendo el camino contrario.

Los CMTS normalmente solo manejan tráfico IP. El tráfico destinado al cablemódem enviado desde Internet, conocido como tráfico de bajada (downstream), se transporta encapsulado en paquetes MPEG. Estos paquetes MPEG se transportan en flujos de datos que normalmente se modulan en señales QAM.

El tráfico de subida (upstream, datos del cablemódem hacia la cabecera o Internet) se transporta en tramas Ethernet, típicamente en señales QPSK.

Un CMTS típico, permite al ordenador del abonado obtener una dirección IP mediante un servidor DHCP. Además, aparte de la IP, también suele asignar la puerta de enlace, servidores DNS, etc.

El CMTS también puede incorporar un filtrado básico como protección contra usuarios no autorizados y ciertos ataques. Se suele utilizar la regulación de tráfico para restringir las velocidades de transferencia de los usuarios finales. Un CMTS puede actuar como bridge o router.

El cablemódem de un abonado no puede comunicarse directamente con otros módems en la misma línea. En general, el tráfico del cablemódem se enruta a otros cablemódems o a Internet a través de una serie de CMTS y routers. Evidentemente una determinada ruta podría pasar por un único CMTS.

Un CMTS proporciona casi las mismas funciones que el DSLAM en sistemas DSL.

Fibra Óptica

La fibra óptica se utiliza para transmitir a lo largo de la red señales seleccionadas de todos los tipos y comúnmente en formato digital. Las interconexiones de fibra proveen en las redes HFC la conectividad entre el punto donde se genera el espectro FDM y el punto central de distribución coaxial. También es utilizada para comunicar las Cabeceras y con proveedores externos de información como Broadcasts y proveedores de Internet.

Las conexiones básicas propias de la red HFC son: Estrella, Anillo Cubierto, Anillo Cubierto Analógico y Anillo Digital de Repetición.

Nodos de Fibra

Los nodos de fibra son básicamente la interconexión entre una línea de fibra óptica y la red de distribución coaxial. Un nodo está compuesto básicamente de un receptor óptico que alimenta a un amplificador de Downstream y opcionalmente, puede contener un transmisor de Upstream, también conectado a la red coaxial.

Algunos nodos tienen la opción de tener múltiples entradas de fibras para Downstream que son alimentadas por receptores ópticos diferentes cuyas salidas son combinadas en un filtro duplex. Con esto se tienen dos opciones: mejorar la calidad de la señal y flexibilidad de la red.

Red de distribución Coaxial

El parámetro más elemental en una red coaxial es el Ancho de Banda, el cual es determinado por los equipos de amplificación que son utilizados en dicha red. Algunos operadores de redes HFC sugieren emplear redes coaxiales pequeñas para evitar el uso de amplificadores entre la parte óptica y el usuario.

El segundo parámetro importante a considerar en una red HFC es el tamaño del área de la red coaxial. Todos los usuarios conectados a la misma red coaxial comparten el ancho de banda.

El suministro eléctrico presenta niveles de confiabilidad, por lo general, levemente inferiores a los esperados para los requerimientos de las redes HFC. Por esto se emplea una estrategia para minimizar los efectos de los cortes de suministro

Equipos Terminales

Los equipos terminales proveen la interfaz entre los dispositivos de aplicaciones del usuario final y el sistema de distribución compartido. Dependiendo del servicio, los equipos terminales pueden realizar funciones como: transformación de formatos de los datos de la red, testeo y otras funciones de

seguridad. Por lo general, son la cara más visible de la red y proveer a los usuarios de estos equipos representa una gran inversión debido principalmente al alto número de equipos que puede tener una red.

Los equipos más importantes son: Equipos In-Home, que se encuentran al interior de los hogares conectados directamente a la red o como equipos intermedios entre el Drop y el receptor del subscriptor; Equipos Punto-de-entrada, que proporcionan medios para aislar las redes de cable direccionales de las señales generadas al interior de los hogares, este equipo puede manejar un canal de Ethernet; y Equipos Terminales Compartidos con multipuertos para ser compartidos por más de un usuario.

Telefonía

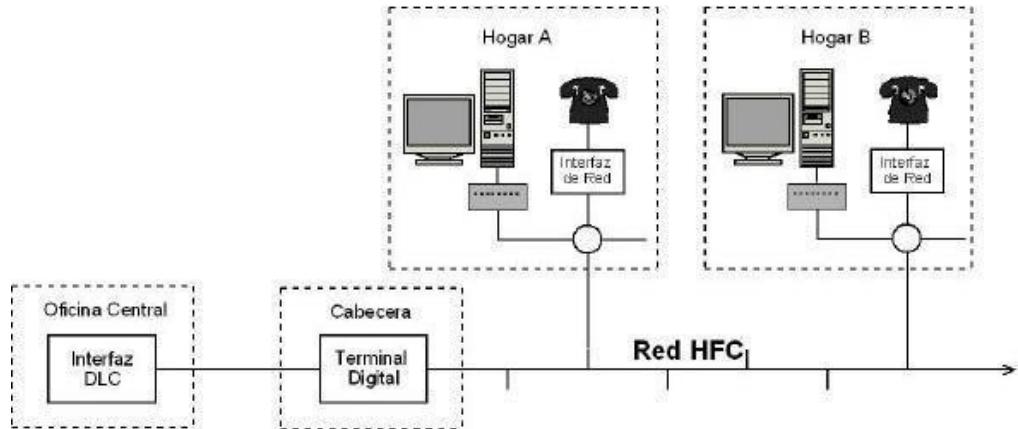
El Servicio de Telefonía o servicios de voz, también se puede integrar en las redes HFC. Requieren sistemas bidireccionales, tiempo real y ancho de banda constante mientras dure la transmisión. La alimentación eléctrica de los equipos que permitan la transmisión de voz puede ser local o remota a partir de los centros de distribución.

El usuario dispone de un dispositivo conocido como Puerto de Voz que convierte las señales telefónicas a señales de Radiofrecuencia, RF para transmitirlas a la red HFC. En la Cabecera existe un módem que modula y remodula, utilizando QPSK el tráfico ascendente y descendente entre el puerto de voz y la Cabecera.

Las redes HFC se adaptan a los servicios de voz con las mismas funcionalidades de las redes de conmutación de circuitos, pero la tendencia de todos los fabricantes es dar voz sobre IP. El Usuario de un teléfono o Equipo Terminal se conecta a la Oficina Central, la que se encuentra habitualmente en un punto central del área a la que sirve. Las líneas que conectan un abonado a la Oficina Central se llaman Líneas de Abonado y las líneas que unen oficinas centrales se les conocen como Troncales. Las oficinas centrales se pueden conectar con Oficinas Tandem, que son las encargadas de las comunicaciones de larga distancia entre dos redes Troncales.

Los instrumentos telefónicos no son conectados directamente a los Switch al interior de las oficinas centrales, existe un equipo que conecta un grupo de teléfonos ubicados geográficamente cerca y que se conecta a la oficina central. A este equipo se le llama Concentrador DLC (Digital Loop Carrier) y mejora la eficiencia de la utilización de cable cuando un grupo de usuarios no se encuentra cerca de la Oficina Central. En la oficina central se requiere de una Interfaz DLC, que es un equipo que sirve de interfaz entre el Switch y los Concentradores DLC.

Cuando el servicio de telefonía es soportado por redes HFC, aparecen variaciones en la arquitectura. Primero desaparece el Colector DLC y es reemplazado por un Terminal Digital HDT, que en lugar de estar en el área donde se ubican los DLC, se encuentra en la Cabecera. Se requiere adicionalmente un Dispositivo de Interfaz de Red, NID en cada hogar entre el teléfono analógico y el equipo que se conecta a la red HFC, tal como se muestra en la Figura



Lógicamente, el primer paso en la transmisión de voz por un sistema de telefonía digital corresponde al proceso de digitalización. La digitalización se realiza sobre componentes de frecuencias en el rango audible para el ser humano. La tasa de muestreo en telefonía es de 8000 muestras por segundo, obteniéndose mediante el teorema de Nyquist un ancho de banda de 4 kHz. Luego del muestreo, la señal es convertida en formato digital de 8 bits por muestra. Con esto se obtiene 64 kbps. Para la utilización del medio de manera más eficiente, se utiliza la Multiplexión por División de Tiempo para transmitir más de un canal.

DOCSIS

DOCSIS es un estándar creado por CableLabs que permite: "introducir un sistema de datos sobre cable abierto que facilite la rápida definición, diseño, desarrollo e implementación de servicios". En la actualidad DOCSIS es el estándar más difundido a nivel mundial para redes de HFC.

DOCSIS es un estándar no comercial que define los requisitos de la interfaz de comunicaciones y operaciones para los datos sobre sistemas de cable, lo que permite añadir transferencias de datos a un sistema de televisión por cable existente.

El estándar DOCSIS se encuentra actualmente en la versión 2.0. La versión europea de DOCSIS se denomina EuroDOCSIS. También existen otras variantes de DOCSIS que se emplean en Japón.

En la actualidad existen especificaciones finales del DOCSIS 3.0, cuya principal novedad reside en el soporte para IPv6 y el "channel bonding", que permite utilizar varios canales simultáneamente, tanto de subida como de bajada, por lo que la velocidad podrá sobrepasar los 100 Mbps en ambos sentidos.

FTTx ¿Qué es?

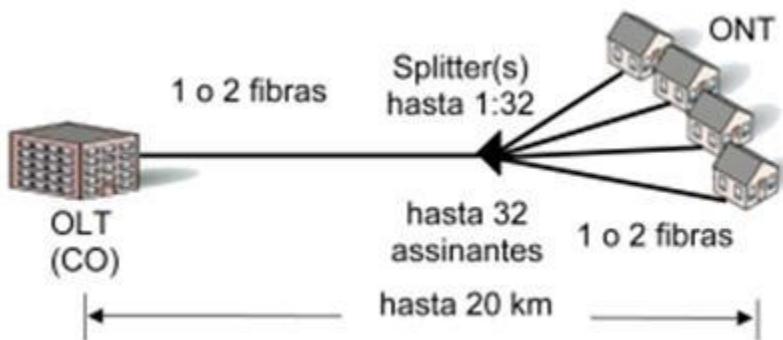
FTTx es una expresión genérica para asignar arquitecturas de redes de transmisión de alto desempeño, basada en tecnología óptica. Son redes totalmente pasivas.

El acrónimo FTTx es conocido ampliamente como Fibre-to-the-x, donde x puede denotar distintos destinos

Funcionamiento:

En la CO/Central Office (o Sala de Equipos) la señal es transmitida por una red óptica donde en una región próxima a los suscriptores, la señal se divide y es transmitida a las ONTs (Optical Network Terminal) - localizada en los respectivos abonados.

En la figura 1 se muestra el procedimiento que sigue la FTTx:



A mediados de los años 90, un grupo internacional de proveedores de servicios de red se reunieron para desarrollar unos documentos de referencia que finalmente definirían la nueva red óptica pasiva FTTX (Fiber-to-the-x).

Permitiría ofrecer conexiones rentables a los abonados, abrir un nuevo mercado, y ayudar a los proveedores de servicios pertinentes para mejorar la competencia en el mercado desarrollando equipamiento estandarizado.

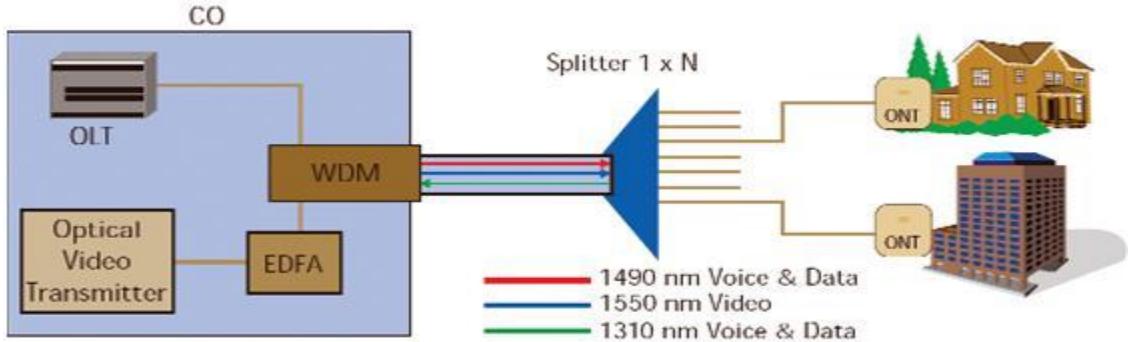
El grupo creó la red de acceso multiservicio (full-service access network, FSAN). Además, la legislatura de los Estados Unidos firmó el decreto de las telecomunicaciones en 1996 para "promover y reducir la regulación con el objetivo de asegurar precios más bajos y servicios de alta calidad para los consumidores americanos de telecomunicaciones y fomentar el rápido despliegue de la nueva tecnología de telecomunicaciones".

El sector de normalización de las telecomunicaciones (ITU-T) convirtió las especificaciones de la FSAN en recomendaciones. La especificación de la FSAN para el PON basado en modo de transferencia asíncrona (ATM) se convirtió en la recomendación G.983.1 de la ITU-T en 1998.

En 2001 se creó el consejo del FTTH para promover el FTTH en Norte América y asesorar la legislatura americana. Esto desembocó en el tratado de acceso a internet de banda ancha en 2001, que proporciona incentivos en los impuestos de las compañías que invierten en infraestructura de banda ancha de nueva generación.

En 2003, la comisión federal de comunicación (FCC) eliminó los requerimientos de facturación para las redes FTTH, liberando a las compañías locales del grupo "Bell" (RBOCs) de su obligación de ofrecer el uso de sus infraestructuras de redes al grupo local de la competencia (CLECs), y de este modo hacer la tecnología más atractiva para las grandes empresas. Esto significa que la RBOCs puede ahora invertir en infraestructura de fibra óptica sin tener que compartirlo con la competencia, lo que debería ser un importante incentivo para el desarrollo de redes FTTH.

[Retorno](#)

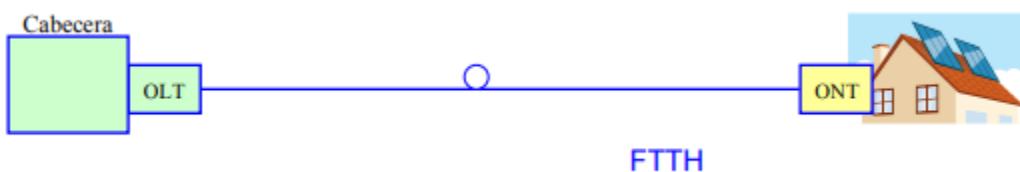


Un enlace FTTx consiste en un sistema que enlaza la Central (dispositivo OLT) con el abonado (ONT). El esquema de la figura anterior nos muestra la solución adoptada para la transmisión bidireccional: La transmisión de voz y datos utiliza las lambdas de 1310 nm (hacia el usuario) y 1490 nm (retorno). En el caso de incorporar TV interactiva al circuito, esta circula a 1550 nm. La señal resultante es dividida en términos de potencia por los splitters, hasta conectar con todas las ONT con ello queda definida una arquitectura pasiva, capaz por tanto de soportar cualquier tipo de red, a definir por los equipos activos incorporados en su cabecera. En conclusión el retorno de la topología FTTx se realiza por medio del Splitter, pero sobre otro hilo de F.O de retorno.

Las arquitecturas FTTX más importantes son:

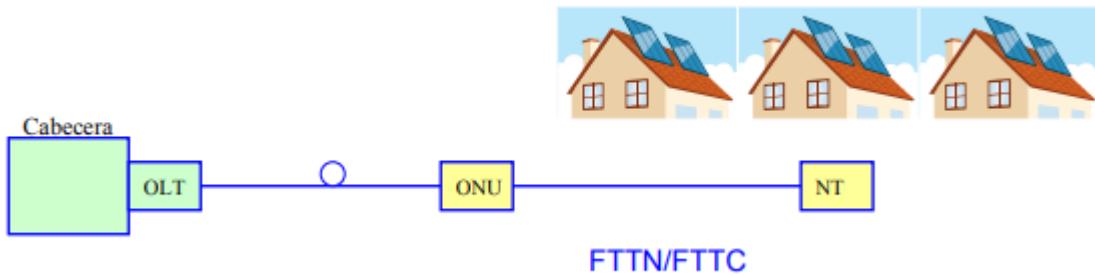
FTTH (home).

FTTH es la fibra hasta el hogar, es decir la fibra óptica llega al domicilio u oficina del usuario. El cliente no comparte recursos con otros usuarios. Es la alternativa más costosa al momento de implementarla. Una ventaja adicional al gran ancho de banda que ofrece consiste en que es una red pasiva, por consiguiente no emplea elementos activos como: amplificadores, regeneradores, etc.



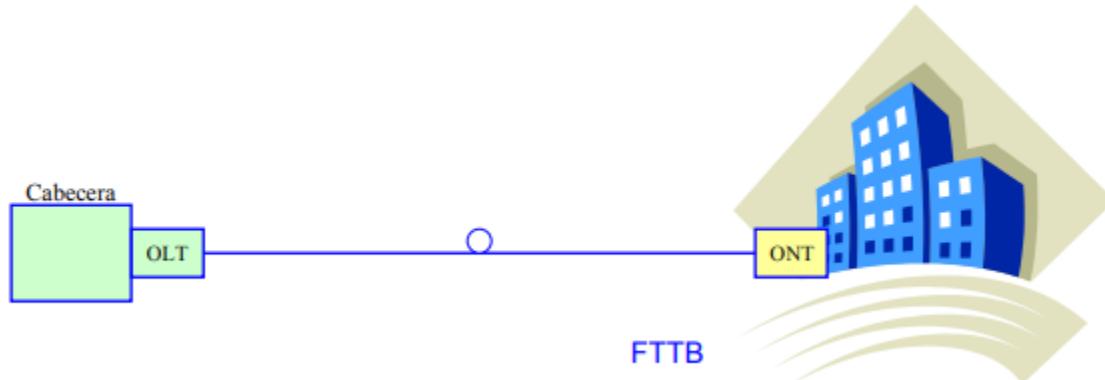
FTTC (Fiber To The Curb):

FTTC es la fibra hasta la acera, en este caso la fibra llega generalmente hasta un armario ubicado en la calle desde donde se distribuirá al usuario por medio de cobre o cable coaxial. Tiene como una de sus principales desventajas que se necesita mayor inversión que FTTH en lo que se refiere a equipos de multiplexación e interfaces de red. La tecnología FTTC compensa costos haciéndola más económica en relación a FTTH, debido a que este último emplea mayor longitud de fibra óptica en relación al primero y principalmente tomando en consideración que los equipos terminales de usuario con interfaz óptico son costosos. FTTC es capaz de ofrecer servicios de gran ancho banda.



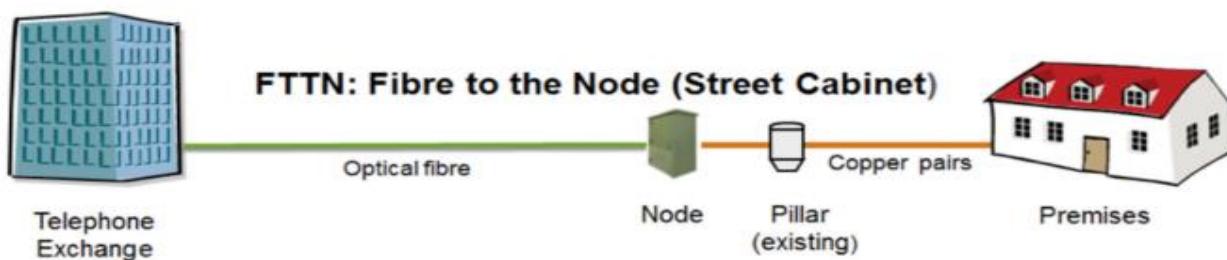
FTTB (building).

En FTTB o fibra hasta el edificio, la fibra termina antes, típicamente en un punto de distribución intermedio en el interior o inmediaciones del edificio de los abonados. Desde este punto de distribución intermedio, se accede a los abonados finales del edificio o de la casa. La red de acceso con FTTC se considera híbrida en el sentido de que utiliza fibra óptica hasta el punto dónde termina la instalación óptica y a partir de allí hasta el usuario se llega con cobre o cable coaxial.

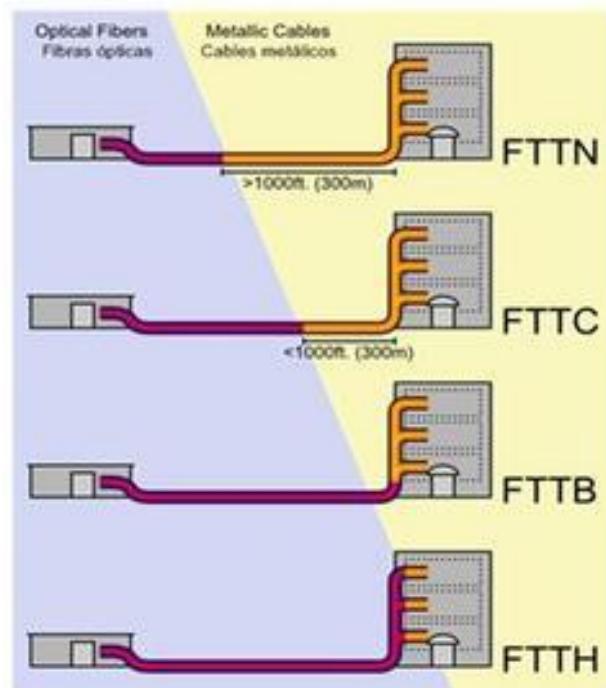


FTTN (node o neighborhood).

FTTN, fibra hasta el vecindario, también es similar a FTTC, la fibra óptica llega hasta un lugar de un barrio o vecindario para desde allí llegar a los usuarios por un medio de transmisión más económico como el cobre.



Las diferentes arquitecturas



Una red FTTx se puede dividir en tres partes principales: la sala de equipos o central, la red de distribución óptica (ODN) y la conexión/equipos en los locales de los usuarios.

La sala de equipos (equipment room), cabecera (head end) o oficina central (central office) como se quiera llamar dispone de los equipos necesarios para transmitir y recibir la información de los abonados y de los suministradores de contenidos, por lo tanto debe disponer de equipos receptores de voz, video y datos, para después redistribuirlos entre los usuarios utilizando un Terminal Óptico de Red (OLT).

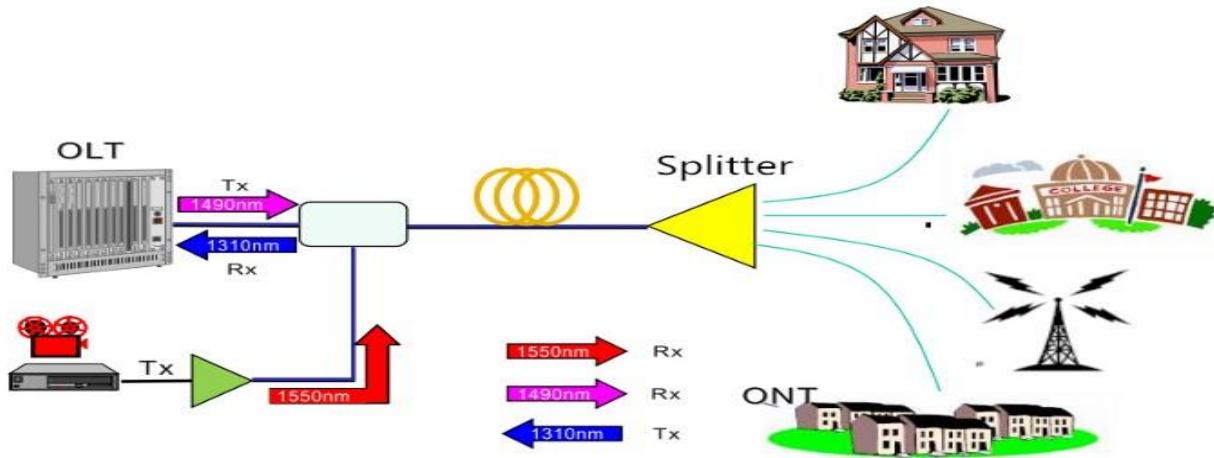
La ODN proporciona los medios ópticos de transmisión desde la OLT hacia el usuario, y viceversa.

La ODN es una parte crítica en las redes FTTx, ya que las cabeceras y los equipos de los usuarios se pueden actualizar fácilmente, durante períodos de 20, 30 o más años y utilizarán la misma ODN, por lo tanto la instalación de debe realizar de forma fiable para poder resistir el paso del tiempo. Mapa Mental xPON – FTTx

Una visión general de la red de acceso FTTH con GPON

La red de acceso FTTH basada en la red óptica pasiva (PON, por sus siglas en inglés) es una arquitectura de red de punto a multipunto de fibra hasta instalaciones en la que se utilizan divisores ópticos sin alimentación para permitir que una única fibra óptica sirva para varias instalaciones, de 32 a 128. La red FTTH utiliza la baja atenuación y el alto ancho de banda de la fibra monomodo para proporcionar un ancho de banda mucho mayor que el disponible actualmente con las tecnologías de banda ancha existentes.

La terminal de línea óptica, los divisores ópticos y la terminal de red óptica son los tres componentes de la red de acceso FTTH con GPON.



OLT (Terminal de línea óptica)

La terminal de línea óptica es el elemento principal de la red, ya que es el motor que impulsa el sistema FTTH. Esta generalmente se instala en la oficina central, encargándose de la programación del tráfico, el control del búfer y la asignación de ancho de banda entre otras funciones. Por lo general, la OLT funciona con alimentación de CC redundante y tiene al menos 1 tarjeta de línea para Internet entrante, 1 tarjeta de sistema para la configuración a bordo y 1 o varias tarjetas GPON: siendo estas una serie de puertos GPON.

Splitter óptico

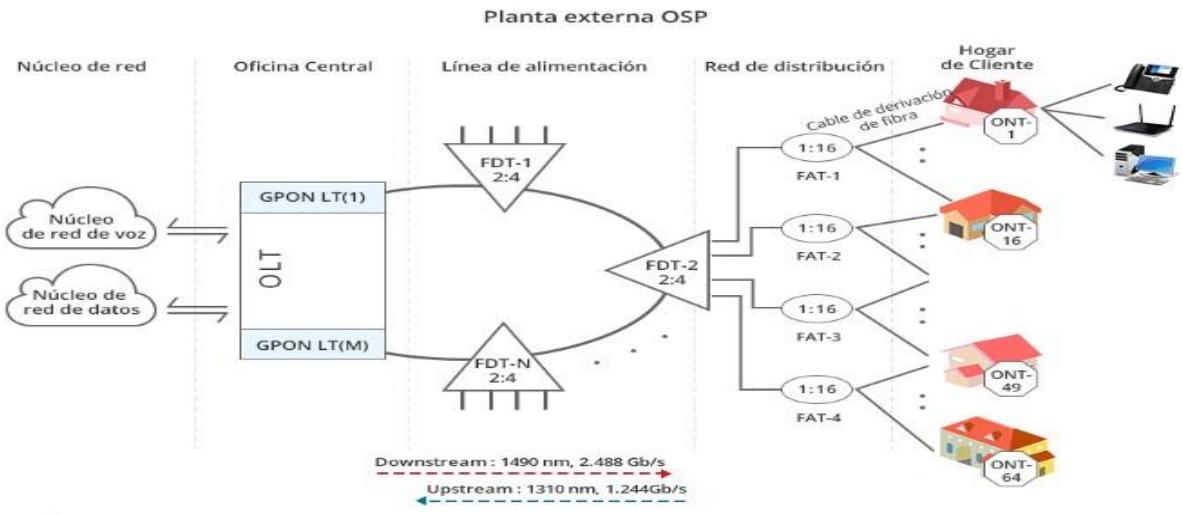
El splitter óptico divide la potencia de la señal. Es decir, cada enlace de fibra que entra al splitter puede dividirse en un número dado de fibras a su salida. Normalmente, tres o más niveles de fibras corresponden a dos o más niveles de splitters, permitiendo así que muchos usuarios comparten cada fibra. El splitter óptico pasivo tiene un amplio rango de longitud de onda de operación, baja pérdida y uniformidad de inserción, dimensiones mínimas, alta fiabilidad y una política de protección y supervivencia de red compatible.

ONT (Terminal de red óptica)

La ONT es la utilizada en las instalaciones del cliente. Esta está conectada a la OLT por medio de fibra óptica y no tiene elementos activos presentes en el enlace. En GPON, el transceptor en la ONT es la conexión física entre las instalaciones del cliente y la oficina central OLT.

Arquitectura de la red de acceso FTTH con GPON

Con una topología de árbol, GPON maximiza la cobertura con un mínimo de divisiones de red, reduciendo así la potencia óptica. Una red de acceso FTTH consta de cinco áreas: un área de red central, una de la oficina central, una de alimentación, una de distribución y un área de usuario.



Núcleo de red

El núcleo de red incluye el equipo ISP del proveedor de servicios de Internet, PSTN, red telefónica commutada por sus siglas en inglés, (comunicación de paquetes o la comunicación heredada de circuitos) y el equipo del proveedor de televisión por cable.

Oficina central

La función principal de la oficina central es alojar las OLT y ODF (marcos de distribución óptica) y proporcionar la alimentación necesaria. A veces, esta incluso puede incluir algunos de los componentes del núcleo de red.

Red de alimentación

La red de alimentación se extiende desde la ODF, en la oficina central, hasta los puntos de distribución. En estos puntos, que normalmente se tratan de cajas para empalme y derivación situadas en la calle, llamadas marcos de interrupción de la fibra, FDT por sus siglas en inglés, es en donde se suelen situar los divisores de nivel 1. El cable de alimentación generalmente se conecta como una topología de anillo a partir de un puerto GPON y con una terminación en otro puerto GPON para así poder proporcionar protección de tipo B , tal y como se muestra en la imagen de arriba.

Red de distribución

El cable de distribución conecta el switch de nivel 1 (dentro de la caja de distribución, FDT por sus siglas en inglés) con el divisor de nivel 2. El divisor de nivel 2 se encuentra normalmente en una caja terminal para fibra óptica, CTO, montada en un poste y normalmente situada en la entrada del vecindario.

Área de usuario

En el área del usuario, los cables de derivación se utilizan para conectar el splitter de nivel 2, que se encuentra dentro de la caja terminal, a las instalaciones del suscriptor. Para facilitar el mantenimiento, por lo general, el cable de derivación aéreo termina en la entrada de la casa del suscriptor en una caja terminal (TB por sus siglas en inglés). A partir de ahí se utilizaría un cable de derivación de interior que conectaría esta caja terminal con la caja terminal de acceso (ATB por sus siglas en inglés) instalada dentro de la casa. Para finalizar, un cable de conexión conectaría la ONT con la ATB.

La arquitectura FTTB

FTTB, de las siglas en inglés Fiber To The Building (fibra hasta el edificio), permite la transmisión de información a altas velocidades aprovechando las ventajas de la fibra óptica y los sistemas de distribución ópticos. Este tipo de arquitectura se está empezando a implementar en la actualidad y puede tener

buenos resultados puesto que es más económica que arquitecturas similares como FTTH (fibra hasta el hogar) debido a que en este caso se llega con fibra óptica hasta el hogar o domicilio donde se encuentra el abonado, razón por la cual los costos se incrementan.

Con FTTB en cambio, llega una sola terminal de red óptica (ONT) hasta el edificio y es compartida por todos los abonados en el edificio. Desde la terminal de red óptica hasta el abonado o usuario se tiene cobre con tecnología que puede ser del tipo xDSL y que para el caso concreto de este proyecto de titulación será VDSL2.

FTTH vs FTTB

La adopción de la tecnología FTTH (fibra hasta el hogar) o FTTB (fibra hasta el edificio)/FTTN (fibra hasta el nodo o inmediaciones del edificio) por parte del operador depende de muchos factores: entorno regulatorio, capacidad de inversión, capacidad de realizar nuevas acometidas sobre el edificio, calidad del par de cobre instalado, etc. Generalmente FTTH es la opción ideal para nuevos edificios y FTTB para edificios existentes.

FTTB en vez de una ONT (Optical Network Terminator) en casa del abonado emplea una MDU (Multi-Drawing Unit) en el edificio. En ambos casos, la conexión con el equipo OLT en la central (Optical Line Terminal) se realiza por fibra óptica, pero cambian las interfaces hacia el abonado: GbE (datos y vídeo) y RJ-11 (voz) en la ONT y VDSL2 en la MDU (se trata de un mini-DSLAM).

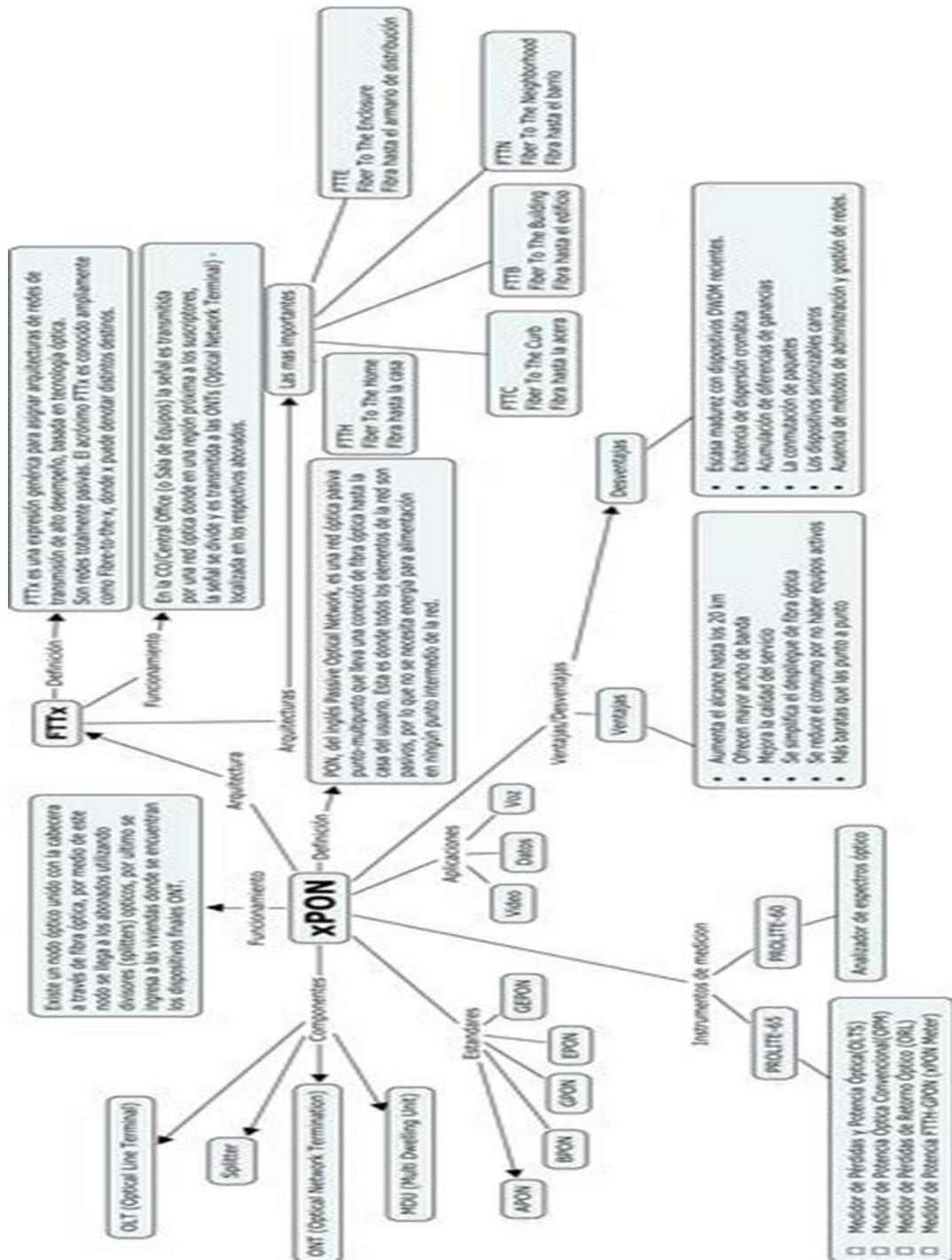
Ventajas de FTTB/FTTN respecto a FTTH:

- Tiempo de despliegue menor para ofrecer servicios que demandan más ancho de banda y distancias que ADSL2+. El operador no necesita negociar el despliegue de fibra dentro del edificio hasta las casas de los clientes.
- Inversión inicial menor, debido a la reutilización de la infraestructura de cobre existente. Hay un ahorro en coste de tramitación de licencias, coste de mano de obra de ingeniería e instalación y coste de fibra óptica.

Desventajas de FTTB/FTTN respecto a FTTH:

- Si en vez de FTTB se emplea una arquitectura FTTN, los anchos de banda soportados por VDSL2 no podrían ser ofrecido a todos los clientes.
- El coste operacional es mayor debido a la existencia de más protocolos y dispositivos, que suponen más puntos de fallos y una mayor complejidad en la monitorización de la red.

Mapa Conceptual



REDES HFC

es

problemas

*Dadas las señales ascendentes convergen en un único punto, así como también las señales indeseadas, ruido e interferencias sumando sus patencias y contribuyendo a la degradación de la señal a ruido (S/N) en el enlace digital de subida.
+HFC usa un medio compartido sin conmutación ni enrutamiento. Cualquier información que se ponga en el cable puede ser retransmitida por cualquier suscriptor sin mayores trámites, esto hace que los servicios de los operadores HFC necesiten transmitir codinas cifradas, de modo que los clientes que no hayan pagado una película no puedan verla.

Una red HFC es una red de cable que combina en su estructura el uso de la fibra óptica y el cable coaxial. Este tipo de redes representa la evolución natural de las redes clásicas de televisión por cable (CATV). Una red de CATV está compuesta básicamente por una cabecera de red, la red troncal, la red de distribución, y el último tramo de acoplamiento al hogar del abonado.

CATV está compuesta básicamente

por una cabecera de red, la red troncal,

la red de distribución, y el último tramo de acoplamiento al hogar del abonado.

F.O. fibra óptica:
La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos, un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado (y se propaga por el interior de la fibra con un ángulo de reflexión par dentro del ángulo límite de reflexión total), en función de la ley de Snell. La fuente de luz puede ser láser o un LED.

tipos de cables utilizados

coaxial:

Es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores coaxiales, uno central (americano vivo) encargado de llevar la información, y uno exterior de aspecto tubular, llamado mala o blindaje, que sirve como referencia de tierra y retorno de los corrientes. Entre ambos se encuentra una capa aislante llamada dielectrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.

la red troncal:

Es la encargada de repartir la señal compuesta generada por la cabecera a todas las zonas de distribución que abarca la red de cable, la red troncal se ha convertido, por ejemplo, en una estructura con anillos redundantes que unen nodos ópticos entre sí.

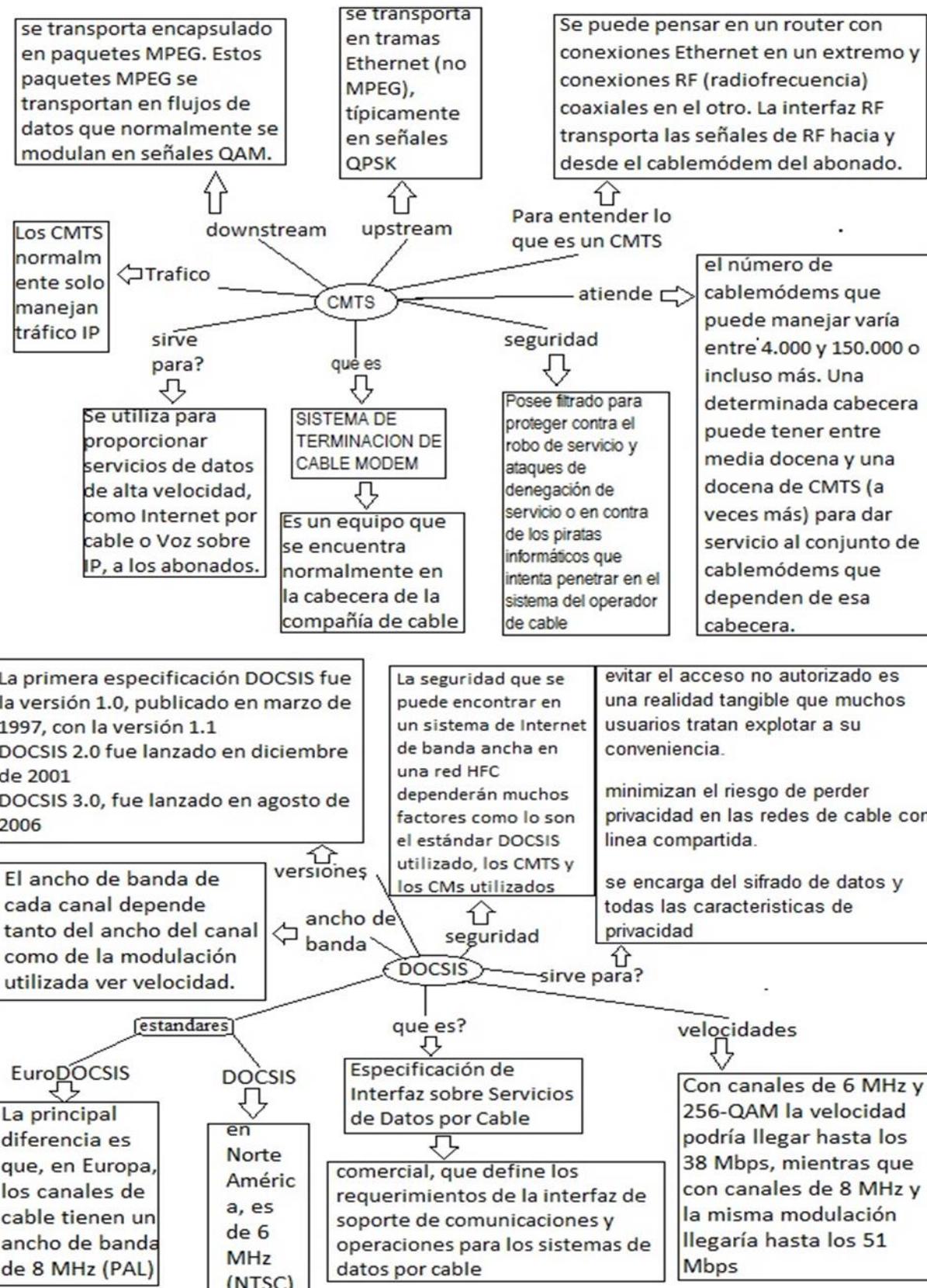
frecuencias trabajadas

- Desde los 5 a los 420 MHz aproximadamente encontramos los datos ascendentes
-después de los 420MHz hasta los 500MHz no se tiene hasta el momento un conocimiento que certifique que los utilizan para algún uso en especial,
-desde los 500MHz a los 550MHz aproximadamente encontramos divididos en canales de 6MHz la TV analógica que va aproximadamente hasta el canal 70 ocupando los 499 MHz.
-Después de los 500MHz a los 750 MHz aproximadamente encontramos la TV digital
-Después de los 750 MHz a los 860 MHz aproximadamente encontramos los datos Descendentes

red de distribución:

Está compuesta por una estructura tipo bus de coaxial que lleva las señales descendentes hasta la última分歧ion antes del hogar del abonado. En el caso de la red HFC normalmente la red de distribución contiene un máximo de 2 ó 3 amplificadores de banda ancha y abarca grupos de unas 500 viviendas.

En estos casos la fibra óptica llega hasta el piso de un edificio, de allí sale por la fachada del mismo para alimentar un nodo óptico que se instala en la azotea, y de este parte el coaxial hacia el grupo de edificios (o que alimenta (para servicios de datos y telefonía suelen utilizarse cables de pares trenzados para llegar directamente hasta el abonado, desde el nodo óptico).



CAPITULO 9

Introducción a las redes Wireless Wan

Introducción

Una WWAN a menudo difiere de la red de área local inalámbrica (WLAN) al usar tecnologías de red celular de telecomunicaciones móviles como LTE, WiMAX (a menudo llamada red de área metropolitana inalámbrica o WMAN), UMTS, CDMA2000, GSM, datos de paquetes digitales celulares (CDPD) y Mobitex para transferir los datos. También puede usar el Servicio de distribución local multipunto (LMDS) o Wi-Fi para proporcionar acceso a Internet. Estas tecnologías se ofrecen a nivel regional, nacional o incluso global y las proporciona un proveedor de servicios inalámbricos.

La conectividad WWAN le permite a un usuario con una computadora portátil y una tarjeta WWAN navegar en la web, consultar el correo electrónico o conectarse a una red privada virtual (VPN) desde cualquier lugar dentro de los límites regionales del servicio celular. Varias computadoras pueden tener capacidades integradas de WWAN.

Las tecnologías principales son:

- GSM (Global System for Mobile Communication)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System)

Motivos de desarrollo

Históricamente las comunicaciones en entornos rurales han supuesto un “handicap” para los operadores que no han conseguido encontrar un modelo de negocio viable en dichos entornos por diversas razones y sobre todo para la población de dichas zonas, que requiere comunicaciones competitivas, pero éstas no se han logrado y en bastantes casos aún no llegan a sus ubicaciones. Tecnologías como el LMDS, o WiFi en combinación con el satélite parecían muy prometedoras pero no hay modelos generalizados de éxito en entornos rurales, de hecho, siguen existiendo muchos pueblos con comunicaciones deficientes que contrastan con entornos urbanos donde se dispone de fibra, comunicaciones móviles, etc. En este entorno, surge una tecnología llamada WIMAX que parece poder aportar soluciones prometedoras al problema de las comunicaciones en entornos rurales

GSM

En la conferencia de telecomunicaciones CEPT del año 1982 fue creado el grupo de trabajo Groupe Spécial Mobile o GSM, cuya tarea era desarrollar un estándar europeo de telefonía móvil digital.

El estándar GSM fue desarrollado a partir de ese año. En el grupo GSM participaron 26 compañías europeas de telecomunicaciones. En 1990 se especificó el primer estándar GSM-900, al que siguió DCS-1800 un año más tarde.

En 1992 las primeras redes europeas de GSM-900 iniciaron su actividad, y el mismo año fueron introducidos al mercado los primeros teléfonos móviles GSM, siendo el primero el Nokia 1011 en noviembre de este año. En los años siguientes, el GSM compitió con otros estándares digitales, pero se terminó imponiendo también en América Latina y Asia. GSM se considera, un estándar de segunda generación (2G), por su velocidad de transmisión y otras características.

Arquitectura del GSM

Es importante describir la arquitectura del GSM pues ella es el punto de partida de la arquitectura base del IMS

Radio base o BS. / Controlador de estaciones base o BSC

Al emplear celdas el estándar GSM introduce una novedad de los sistemas anteriores el controlador de estaciones base, o BSC, (Base Station Controller) que actúa de intermediario entre el “core” de la red y las antenas, y se encarga del reparto de frecuencias y el control de potencia de terminales y estaciones base. El conjunto de estaciones base coordinadas por un BSC proporcionan el enlace entre el terminal del usuario y la siguiente capa de red, ya la principal, que veremos más adelante. Como capa de red, el conjunto de BSs + BSC se denomina subsistema de estaciones base, o BSS . Además, normalmente varias estaciones base al mismo tiempo pueden recibir la señal de un terminal y medir su potencia. De este modo, el controlador de estaciones base o BSC puede detectar si el usuario va a salir de una celda y entrar en otra, y avisa a ambas MSCs y al terminal para el proceso de salto de una BS a otra: es el proceso conocido como handover o traspaso entre celdas, una de las tres labores del BSC, que permite hablar aunque el usuario se desplace.

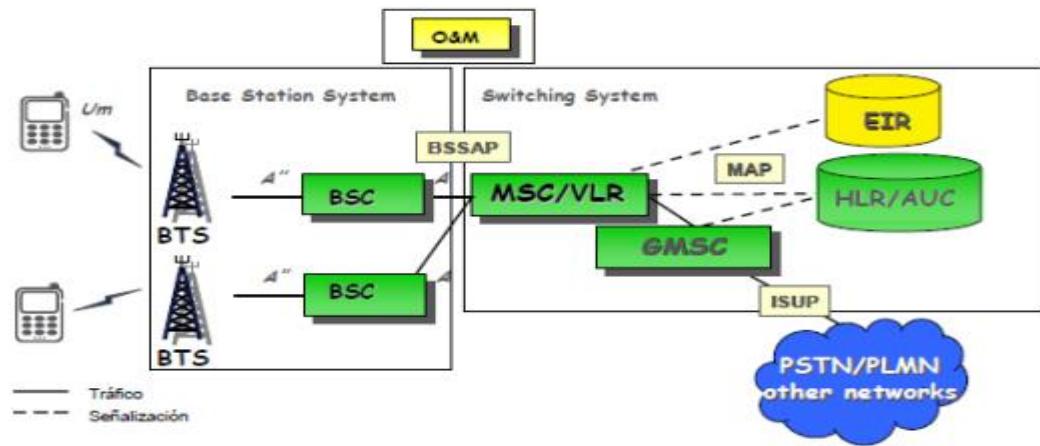
Central de conmutación móvil o MSC.

La central de conmutación móvil o MSC se encarga de iniciar, terminar y canalizar las llamadas a través del BSC y BS correspondientes al abonado llamado. Es similar a una centralita telefónica de red fija. El MSC está conectado a los BSCs de su área de influencia, pero también a su VLR, y debe tener acceso a los HLRs de los distintos operadores e interconexión con las redes de telefonía de otros operadores.

Registros de ubicación base y visitante (HLR y VLR).

El HLR es una base de datos de los usuarios dentro de la red, si está conectado o no y las características de su abono (servicios que puede y no puede usar, tipo de terminal, servicios, etc.). Es de carácter permanente; cada número de teléfono móvil está adscrito a un HLR determinado y único, que administra su operador móvil.

Al recibir una llamada, el MSC pregunta al HLR correspondiente al número llamado si está disponible y dónde está (es decir, a qué BSC hay que pedir que le avise) y enruta la llamada o da un mensaje de error. El VLR es una base de datos volátil que almacena, para el área de cubertura de un MSC, posee los datos de todos los usuarios activos en ese momento y en ese tramo de la red. Cuando un usuario se registra en la red, el VLR del tramo al que está conectado el usuario se pone en contacto con el HLR de origen del usuario y verifica si puede o no hacer llamadas según su tipo de abono. Esta información permanece almacenada en el VLR mientras el terminal de usuario está encendido y se refresca periódicamente para evitar fraudes (por ejemplo, si un usuario de prepago se queda sin saldo y su VLR no lo sabe, podría permitirle realizar llamadas).



3G

3G es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS. Las redes 2G se construyeron principalmente para transmisiones de voz y la transmisión de datos era lenta. Dados los cambios rápidos en las expectativas de los usuarios, no cumplían las necesidades inalámbricas en crecimiento. La evolución del 2G al 3G se realizó en etapas.

3G proporciona una velocidad de transferencia de información de al menos 200 kbit / s. Esto asegura que se puede aplicar a la telefonía inalámbrica de voz, acceso a Internet móvil, conexión a Internet inalámbrica fija, llamadas de video y tecnologías de TV móvil.

4G (LTE)

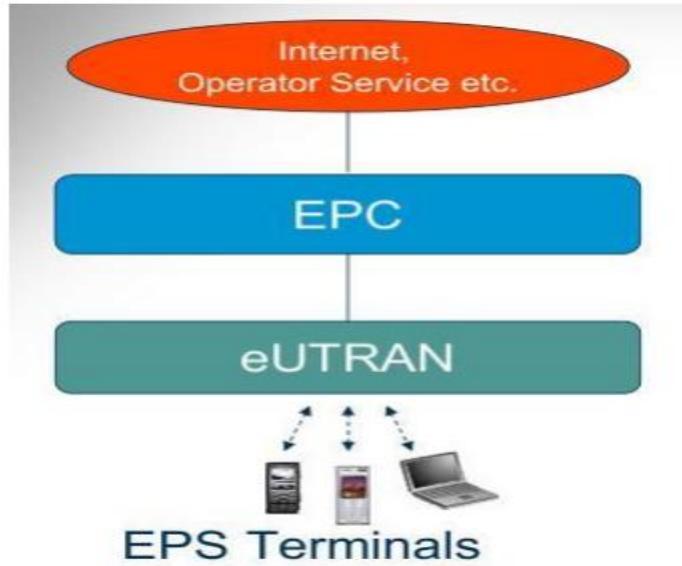
Ante el aumento del uso de datos móviles y la aparición de nuevas aplicaciones y servicios como televisión móvil, web 2.0, flujo de datos de contenidos han sido las motivaciones por las que 3GPP desarrolle el proyecto LTE. Alrededor del 2010, las redes UMTS llegan al 85% de los abonados de móviles.

Es por eso que LTE 3GPP quiere garantizar la ventaja competitiva sobre otras tecnologías móviles. De esta manera, se diseña un sistema capaz de mejorar significativamente la experiencia del usuario con total movilidad, que utilice el protocolo de Internet (IP) para realizar cualquier tipo de tráfico de datos de extremo a extremo con una buena calidad de servicio (QoS) y, de igual forma el tráfico de voz, apoyado en Voz sobre IP (VoIP) que permite una mejor integración con otros servicios multimedia.

Así, con LTE se espera soportar diferentes tipos de servicios incluyendo la navegación web, FTP, video streaming, voz sobre IP, juegos en línea, video en tiempo real, pulsa y habla (push-to-talk) y pulsar para ver (push-to-view, PTV). Arquitectura de 4G La arquitectura de esta nueva tecnología se denominada "System Architecture Evolution" (SAE) o también EPC . La arquitectura SAE presenta varias ventajas con respecto a las tecnologías que se han desarrollado anteriormente para redes celulares, mejorando la capacidad de la red especialmente en el núcleo, donde presenta simplicidad en la arquitectura optimizando el tráfico de los servicios, los cuales son totalmente basados en IP.

La arquitectura LTE consta de dos partes la EPC y la EUTRAN . La EUTRAN es la encargada de todas la funciones relacionadas a la interfaz de radio y el control de los móviles, por otro lado, la EPC brinda

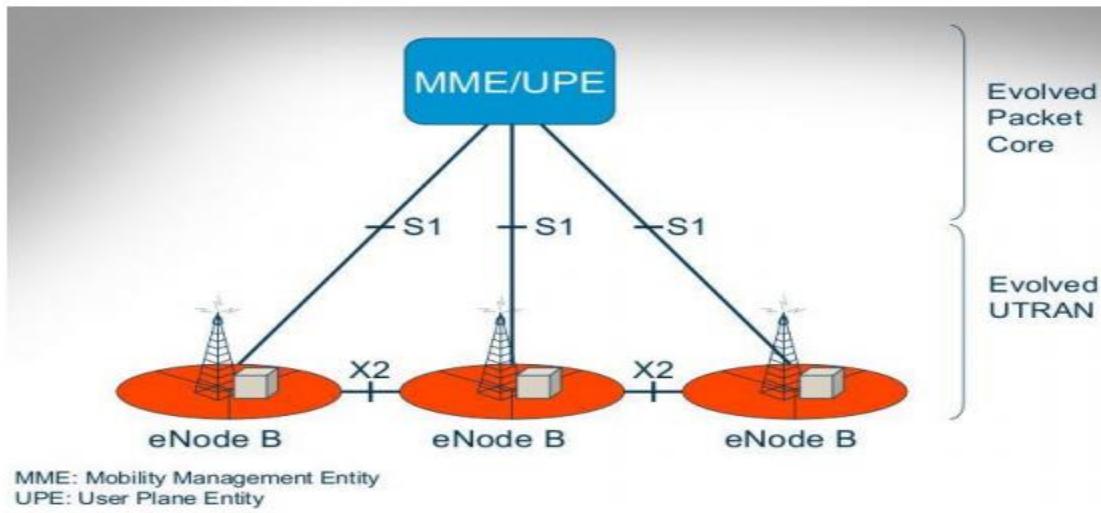
acceso a otras redes de paquetes IP y donde se gestiona los aspectos relacionados a la seguridad, calidad de servicio, gestión de recursos y movilidad.



La eUTRAN está compuesta por los eNodosB que interactúan con la EPC por medio de los MME para el control de la movilidad, gestión y otros aspectos.

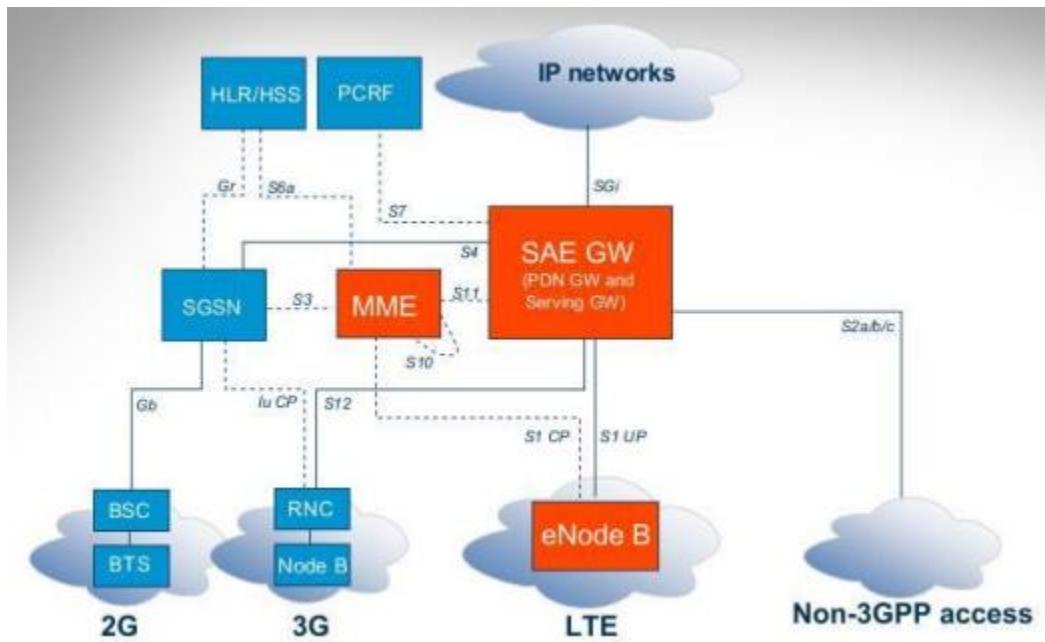
Algunas de las funciones del eNodeB son:

- Funciones de gestión de recursos de radio como conexión, control de admisión de radio, control de movilidad en el plano de usuario.
- Compresión de encabezados IP y encripción de datos de usuario.
- Enrutamiento en el plano de usuario.
- Transmisión de información broadcast.
- Reportes de configuración para movilidad. Las funciones de la MME son:
 - Proveer señalización, seguridad y control de la seguridad.
 - Proveer señalización entre los nodos para gestionar la movilidad entre nodos.
 - Es el encargado de administrar tarifas para cobros.
 - Gestiona la movilidad entre otras redes como 2G y 3G.



En una visión más amplia de la arquitectura planteada por LTE se aprecia la interacción con diversos tipos de redes como GSM, UMTS, IP y otras.

En color naranja se presenta los bloques funcionales que representan los elementos que conforman la SAE, los cuales son: los eNodosB, MME y SAE GW (también denominado SWG, "Serving Gateway"), en este último bloque se han incluido el PGW (PDN Gateway, "Public Data Network Gateway"). El dicha figura las líneas continuas representan el flujo de datos por medio de las interfaces correspondientes y con líneas discontinuas se representa la señalización entre los diferentes bloques funcionales o equipos.



El MME obtiene información del abonado a través de la información almacenada en el HSS para autorizar al usuario a los servicios a los que tiene acceso. El MME autentica, autoriza y selecciona el PDN (Public Data Network) apropiado para establecer el enlace entre el EUTRAN a las redes o servicios externos, al mismo tiempo gestiona la movilidad y obtiene información de cobro.

El MME proporciona conectividad entre el eNodeB y una red GSM o UMTS a través del SGSN (Serving GPRS Support Node). En general se puede decir que MME tiene toda la responsabilidad por las operaciones concernientes al plano de control, además, es el primer contacto de LTE con GSM o UMTS.

El SGW es controlado por el MME, es un punto donde se monitorizan las políticas de conexión y servicio establecidas en el PCRF(Policy and Charging Rules Function) para poder administrar QoS, además, es responsable de la organización del tráfico y los buffers para almacenamiento de paquetes.

El PGW gestiona la asignación de direcciones IP a los UE (“User Equipment”), tiene que ver con todo lo relacionada a la inspección de paquete IP y realiza las funciones que en GSM realizaba el GGSN (Gateway GPRS Support Node) pero además tiene la función de control de la movilidad. Por otro lado, el HSS almacena y administra todo lo relativo a los datos de suscripciones de los usuarios.

Movilidad y Portabilidad

Movilidad: El host se traslada de una red origen a una red destino. Se requiere que la conexión se mantenga en todo momento mientras el host se mueve.

Portabilidad: Se requiere conexión en la red origen y en la red destino, pero la conexión puede perderse durante el cambio de una red a otra.

En ambos casos se requiere una cierta transparencia del usuario respecto al cambio de ubicación

IP Móvil

Introducción

Dada la creciente población de dispositivos móviles con conexión a Internet, como laptops, palmtops, y posteriormente smartphones. Se hace evidente el problema de recepción de paquetes cuando se está cambiando constantemente el punto de acceso a Internet. Por lo que es necesario establecer un protocolo para mantener conectado a Internet el dispositivo cuando éste está en movimiento.

Con la llegada de IPv6 y sobre todo su uso en los terminales móviles esta tecnología ha comenzado a tener una mayor relevancia. De hecho se presenta como la principal opción (prácticamente la única que se considera) a la hora de implementar movilidad IP en una red.

¿Qué es IP móvil?

Mecanismo a nivel de red diseñado para permitir la movilidad de un host en Internet de forma que se mantenga en todo momento su dirección IP original, así como las conexiones o sesiones que tuviera establecidas

El cambio de router se produce dinámicamente y de forma transparente a los niveles superiores. Las sesiones se mantienen incluso durante el cambio de router, siempre y cuando la comunicación se mantenga en todo momento, aunque la velocidad de movimiento puede influir en este factor

IP móvil está diseñado para resolver el problema de la ‘macro’ movilidad, o sea entre redes diferentes. La ‘micro’ movilidad (entre células en una red inalámbrica) se resuelve mejor con mecanismos a nivel de enlace.

Protocolo de IP Móvil es un protocolo creado por la IETF (Internet Engineering Task Force) que permite mantener una IP fija mientras el dispositivo está cambiando de una red a otra mientras se mueve.

Conceptos básicos

Mobile IP basa su funcionamiento en la existencia de tres agentes:

- **El nodo móvil:** es aquel que varía su posición respecto a la jerarquía de direcciones IP. En otras palabras, cambia de red a la que está conectado.
- **El agenteo nodo origen** (home agent): router situado en la red IP a la que pertenece el nodo móvil y que conoce en todo momento la situación de éste.
- **El agente remoto** (correspondent agent): router situado en la red IP donde está conectado el nodo móvil en un momento determinado.

Mobile IP requiere que los nodos móviles dispongan de dos direcciones. Más adelante se describe porqué son necesarias y como se obtiene cada una, por ahora resulta suficiente definirlas como:

- **home address:** dirección permanente asociada a una localización física (home network) a la que pertenece el nodo móvil.
- **care-of address:** dirección variable en función de la red en la que se encuentre conectado el nodo en cada instante de tiempo.

Una vez se tienen claros estos conceptos podemos empezar a profundizar en el funcionamiento de Mobile IP.

Descripción general

Mobile IP define dos nuevas entidades conocidas genéricamente como agentes: el Home Agent (HA) y el Foreign Agent (FA), que no son más que dos encaminadores, uno en la red de origen del nodo móvil y otro en la que visita y que realizan funciones de gestión de datos similares a las del HLR (Home Location Register) y del VLR (Visitor Location Register) de las red celular GSM (Global System for Mobile Communications).

El funcionamiento es simple. Cuando un nodo móvil se mueve hasta otra red recibe un aviso del FA de la red visitada para que se registre. De esta manera detecta su cambio de localización, ya sea respecto al HA o a un FA anterior. Entonces adquiere la dirección del FA (care of address) que queda registrada en su HA. A partir de aquí cualquier datagrama enviada al nodo móvil pasa por su HA que lo envía al FA mediante un túnel, que se encarga de hacerlo llegar al nodo móvil.

En sentido contrario, el nodo móvil envía directamente los datagramas a su nodo destino.

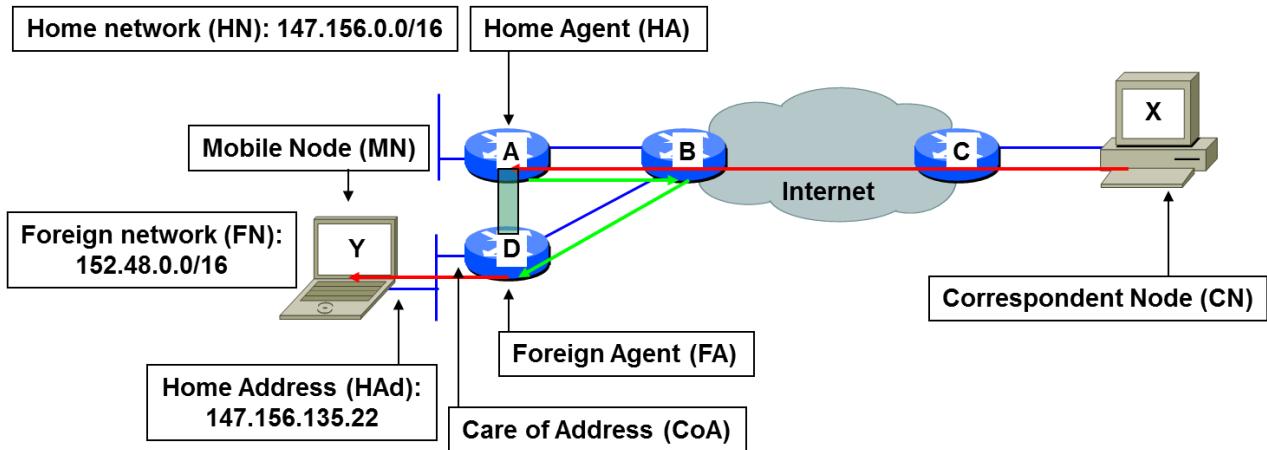
La simplicidad del protocolo Mobile IP tiene su precio: el soporte de la micro movilidad. En entornos de alta movilidad como los celulares en los que el nodo móvil cambia de punto de acceso con gran frecuencia el rendimiento del protocolo puede no ser el adecuado según el tipo de servicio que se quiera soportar. Cada cambio, aunque sea dentro de una misma red, requiere de un intercambio de señalización con el HA lo que ralentiza el proceso de actualización con la posterior pérdida de paquetes que esto supone

Integración de los protocolos del IETF en 3G

Las aproximaciones realizadas por los dos grupos de 3G para integrar los protocolos desarrollados por el IETF están siendo diametralmente opuestas. Por un lado el 3GPP2 cuenta ya desde hace más de un año con un estándar de lo que ellos denominan Wireless IP. En este documento se describen los requerimientos para soportar redes de paquetes inalámbricas en las redes de 3G basadas en cdma2000; diferenciando dos alternativas: Simple IP, basado en el protocolo PPP (Point to Point Protocol); y Mobile IP basado en el protocolo del mismo nombre.

El documento también propone la utilización de servidores RADIUS (Remote Authentication Dial In User Service) para labores de AAA y la utilización de Diffserv para ofrecer calidad de servicio.

Terminología de IP móvil



La ‘Care of Address’ es la dirección IP donde se termina el túnel (en este caso la de la interfaz ethernet del router D)

Esta figura muestra la terminología utilizada en IP móvil:

- **Mobile Node (MN):** Es el host que se mueve de una red a otra.
- **Correspondent Node (CN):** es el host que envía datagramas al MN
- **Home Network (HN):** La red a la que pertenece el host móvil y en la que se encuentra inicialmente. Está definida por un prefijo.
- **Foreign Network (FN):** la red en la que se encuentra el MN de forma transitoria
- **Home Agent (HA):** El agente (normalmente un router) encargado de las labores de mantenimiento asociadas a IP móvil en la HN. Entre otras cosas se encarga de crear el túnel con el FA
- **Foreign Agent (FA):** El agente (normalmente un router) que se encarga de las labores de mantenimiento asociadas a IP móvil en la FN. Entre otras cosas se encarga de mantener el túnel con el HA
- **Care of Address (CoA):** la dirección IP que tiene el túnel de IP móvil en el lado del FA. El FA es normalmente un router con varias interfaces y el túnel puede terminar en cualquiera de ellas, por lo que la CoA puede ser cualquiera.
- **Home Address (Had):** la dirección IP del MN en la HN

Ventajas de IP móvil

Sólo el HA (Home Agent) y el FA (Foreign Agent) necesitan saber la ubicación del host móvil. Los demás routers realizan encaminamiento de paquetes de la manera normal.

Solo los routers y los hosts móviles necesitan nuevo software. Transparente al resto de la red

Escalable. Solo el HA y el FA almacenan información de estado

El host móvil siempre está accesible en la misma dirección IP.

Se produce ineficiencia por:

- Encapsulado (cabecera IP adicional)
- Ruta no óptima (problema de triangulación) como consecuencia del túnel (sólo en el sentido CN→MN)

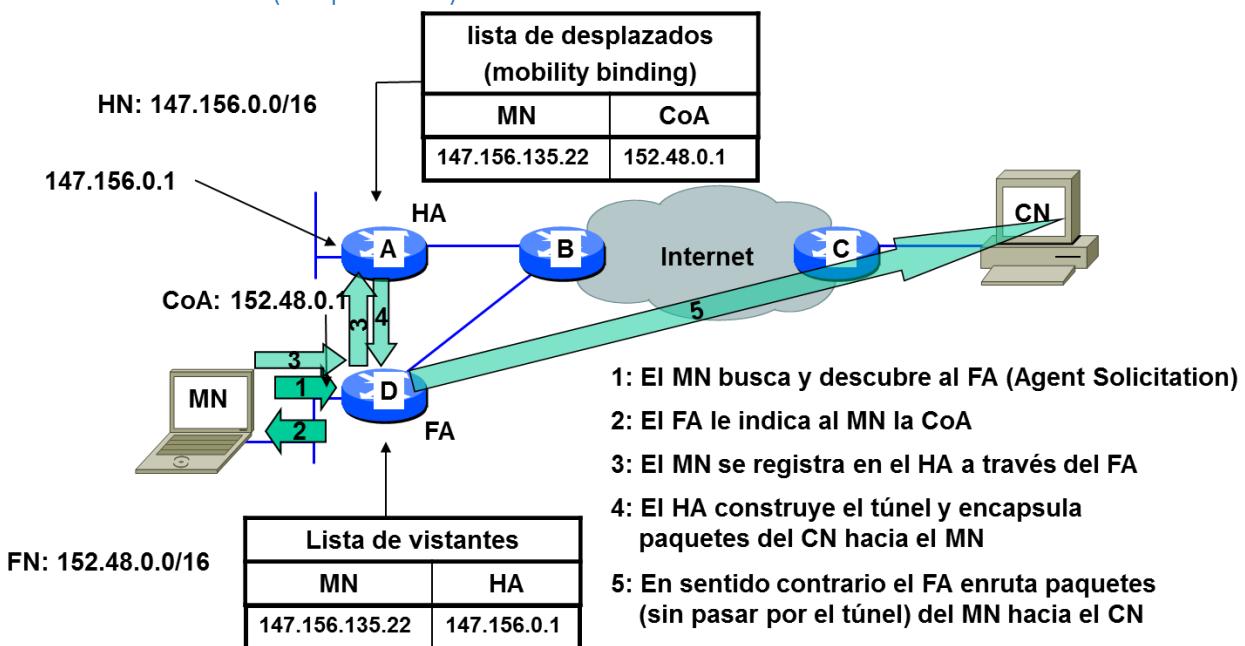
Funcionamiento de IP móvil

Para el funcionamiento de IP móvil es fundamental que el MN localice a su FA. Esto se hace por medio de extensiones al mecanismo de Router Discovery (RFC 1256) que usa mensajes ICMP (Agent Solicitation y Agent Advertisement). El MN emite a intervalos regulares mensajes de búsqueda de agentes (Agent Solicitation). Si recibe respuesta del HA deduce que está 'en su casa' (su HN) y no usa los servicios de IP móvil

Si el MN recibe respuesta de un FA inspecciona el prefijo de red; si se trata de una red extraña pide la CoA y envía un mensaje de registro a su HA para que construya el túnel. Por otro lado los agentes (HA y FA) se anuncian periódicamente en el ámbito de su LAN (TTL = 1) e indican cuales son sus posibilidades (actuar como HA, como FA o como ambos)

Si el MN recibe un Agent Advertisement de un FA nuevo deduce que ha cambiado de zona (quizá se está moviendo); entonces pide una nueva CoA y se reregistra en su HA.

Proceso de IP móvil (simplificado)



Si el MN se mueve y se conecta a través de otro FA el proceso se repite.

La nueva entrada del MN en la tabla del HA (con otra CoA) borra la anterior. Esto permite el cambio de FA ('roaming') sin perder la comunicación.

Esta figura muestra de forma simplificada el proceso que se sigue para el funcionamiento de IP móvil.

En primer lugar el MN busca un agente en su red. Si encuentra un FA y ve que el prefijo de red no coincide con el suyo deduce que se encuentra en una red extraña y debe por tanto iniciar el proceso de IP móvil.

Para ello pide en primer lugar la CoA al FA y envía un mensaje de registro hacia su HA, cuya dirección conoce por configuración. El mensaje de registro (que viaja en un datagrama UDP) no lo envía directamente al HA sino que lo hace a través del FA. Esto permite al FA actualizar su 'lista de visitantes' con una entrada que identifica al MN que acaba de llegar y al HA del que depende. Cuando el mensaje de registro llega al HA este actualiza su lista de desplazados o 'mobility binding' con una entrada que identifica al MN y a la CoA que le asignó el FA (la CoA viene indicada en el mensaje de registro). A continuación el HA construye el túnel IP con el FA y envía a través de él encapsulados los datagramas que recibe dirigidos al MN.

Para la comunicación en sentido contrario (del MN al CN) se utilizan las tablas de rutas normales, sin túneles. Así pues las rutas no son simétricas.

El MN envía periódicamente mensajes Agent Solicitation. De esta forma descubrirá cuando dependa de otro FA debido a un cambio de ubicación o cualquier otra circunstancia; en ese caso se repetirá el proceso de registro sustituyéndose la nueva CoA en la entrada correspondiente al MN en la lista de desplazados. Cuando el MN vuelva a casa dicha entrada desaparecerá

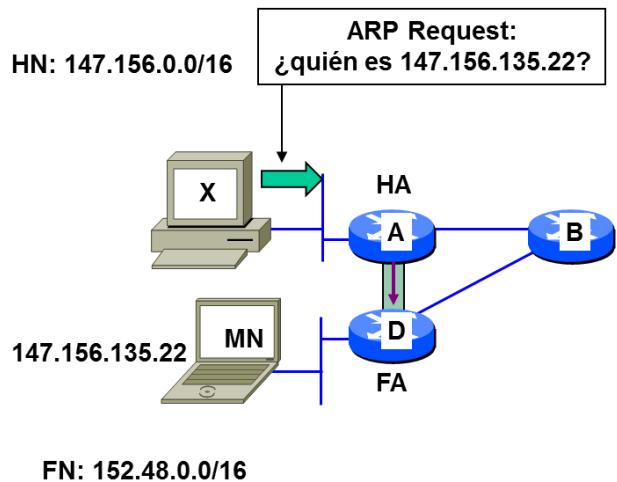
[Comunicación de hosts de la HN con el MN](#)

IP móvil plantea un problema interesante en la comunicación entre el MN y los hosts de su Home Network. Supongamos en la figura una comunicación entre el MN y el host X, situado en su Home Network. Los datagramas de MN hacia X llegan sin problemas puesto que siguen la ruta normal, que pasa por D-B-A.

Sin embargo los datagramas enviados por X hacia el MN no llegarán. La razón es que X, al ver que el host de destino pertenece a su misma red, le buscará en su LAN mediante un ARP Request y MN no recibirá dicho mensaje pues no se encuentra en esa LAN.

La solución a este problema es que el HA suplante a efectos de ARP el papel del MN y responda a los ARP Request como si el mismo fuera el MN. A efectos del host X la dirección del MN será la de la interfaz Ethernet del HA. Este mecanismo se conoce como 'Proxy ARP'. El HA empieza a funcionar como Proxy ARP para el MN en cuanto este se registra desde un FA, es decir cuando se crea una mobility binding para él.

Pero queda por resolver un problema. Cuando el MN se marcha de la HN la ARP cache de X contiene la dirección MAC de MN y no enviará una ARP Request hasta después de varios minutos. Para forzar la rápida actualización de la ARP Cache en X cuando el HA realiza una mobility binding para el MN envía un mensaje ARP broadcast anunciando la nueva dirección MAC de MN. Esto provoca la inmediata actualización de todas las ARP caches que tuvieran una entrada para la IP del MN. Este mecanismo de envío de mensajes ARP no solicitados se conoce como 'Gratuitous ARP'.



1: Un datagrama de MN a X (que está en la HN) llega sin problemas usando las rutas estándar (D-B-A).

2: Pero un datagrama de X a MN no llega: X lanza una ARP Request (buscando la MAC de MN) que no es respondida. X no sabe que MN está fuera de su red.

3: Para evitarlo se utiliza el Proxy ARP: el HA ‘suplanta’ al MN y responde en su lugar a la ARP Request, anunciando su propia MAC para la IP del MN.

- 4: Para asegurar la rápida actualización de las ARP caches, cuando el MN se va de la HN el HA manda un mensaje ARP anunciando su dirección MAC para la IP del MN, sin esperar ningún ARP Request.
Esto se conoce como 'Gratuitous ARP'.

El MN y el FA deben tener comunicación a nivel de enlace, sin routers intermedios. El túnel es unidireccional, los datagramas de vuelta (desde el MN al CN) siguen la ruta normal estándar, sin túneles (salvo que el CN sea también un MN).

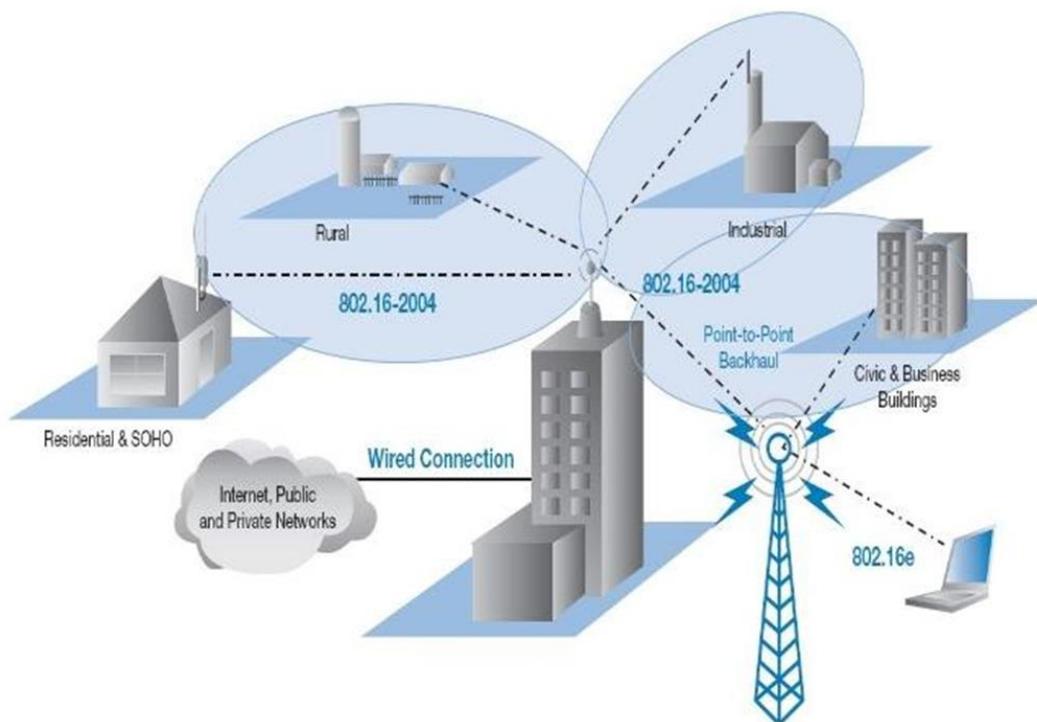
Pero si los routers tienen filtros rechazarán datagramas que vengan de la FN (Foreign Network) con dirección de origen HA (Home Address); en ese caso hay que hacer el túnel bidireccional (camino de vuelta a través del HA).

Que es WIMAX?

Basado en el estándar IEEE 802.16 o WIMAX (Worldwide Interoperability for Microwave Access), es una potente solución a las necesidades de redes de acceso inalámbricas de banda ancha, de amplia cobertura y elevadas prestaciones. Ofrece una gran capacidad (hasta 75 Mbps por cada canal de 20 MHz), e incorpora mecanismos para la gestión de la calidad de servicio (QoS). WIMAX permite amplias coberturas tanto con línea de visión entre los puntos a conectar (LOS) como sin línea de visión (NLOS) en bandas de frecuencias de uso común o licenciadas.

WIMAX asegura la interoperabilidad con el estándar para redes de área metropolitana inalámbricas o WMAN desarrollado por la ETSI (European Telecommunications Standards Institute) y conocido como HiperMAN (High Performance Radio Metropolitan Area Network), de objetivos muy similares a WIMAX. En junio de 2001 se constituyó el llamado WIMAX Forum promovido por fabricantes de equipos de la industria inalámbrica y de comunicaciones con el objetivo de definir y promover el estándar IEEE 802.16. Esta organización sin ánimo de lucro busca dar soporte a los grupos de trabajo del IEEE 802.16, certificar y asegurar la interoperabilidad entre los equipos de distintos fabricantes.

Las aplicaciones típicas de la tecnología WIMAX son el backhaul inalámbrico de otras redes (como puede ser el caso de las estaciones base de telefonía móvil o los hot spots), la “última milla” de la red de acceso a Internet alta velocidad tanto en segmento doméstico como en el profesional (especialmente indicado en aquellas zonas sin cobertura de banda ancha) y soluciones nómadas, que en conexión con otras redes permiten lo que se ha venido a llamar como “Alway Best Connected”, esto es, la conexión a un WISP (Wireless Internet Service Provider) a través de la red óptima en cada momento.

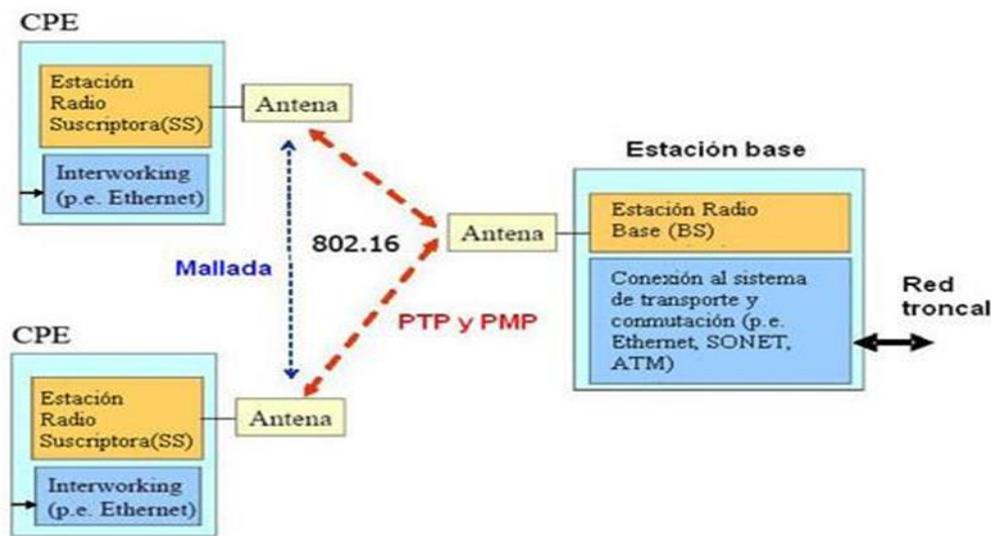


Componentes de una red WiMAX

Básicamente se pueden mencionar los dos tipos de elementos que forman las redes 802.16:

- El equipo de usuario o CPE (Customer Premises Equipment). Este es el equipo que incorpora las funciones de las SS (Subscriber Station) identificadas en el funcionamiento de las redes Broadband Wireless Acces (BWA). Este equipo proporciona la conectividad vía radio con la estación base (BS).
- La estación base con las funciones de BS (Base Station). Además de proporcionar conectividad con las SS también proporciona los mecanismos de control y gestión de los equipos SS. La estación base tiene los elementos necesarios para conectarse con el sistema de distribución.

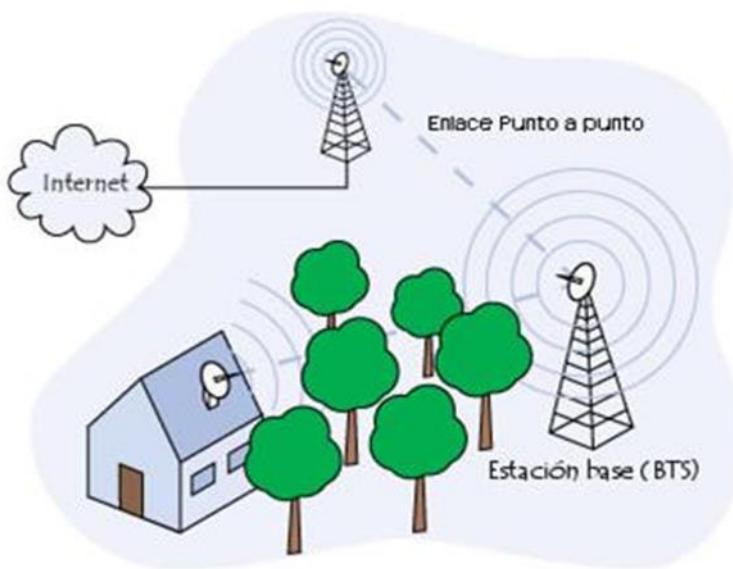
En la figura se identifican estos dos elementos así como las posibles configuraciones de conectividad entre ellas. De forma general, una red WiMAX posee una arquitectura similar a las redes celulares tradicionales ya que se basa en una distribución estratégica de una serie de emplazamientos en donde se ubicarán las estaciones base (BS). Cada estación base utiliza una configuración punto-multipunto (PMP) o punto-punto (PTP) para enlazar los equipos de los clientes. También existe la posibilidad de que las estaciones clientes se enlacen entre ellas en una configuración mallada.



Topología de red

Existen varias topologías de despliegue de red que pueden ser soportadas en las redes WiMAX. Es posible desplegar una red cableada dedicada a la interconexión de estaciones base, o bien realizar estas conexiones en base a circuitos radio Punto – punto en la banda de microondas, o inclusive emplear WiMAX para estos circuitos Punto – punto entre estaciones.

Las estaciones base son capaces de soportar su propia interconexión, dividiendo el ancho de banda disponible entre el dedicado a las comunicaciones de usuarios y el dedicado a la interconexión de las diferentes estaciones base.



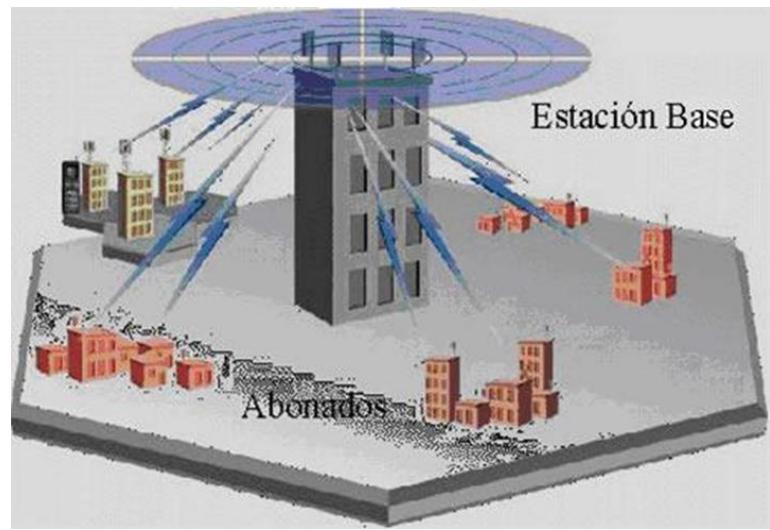
Arquitectura Punto-Multipunto (PMP).

En las configuraciones punto-multipunto (PMP) un enlace WiMAX se realiza a partir de una estación base (BS) central con antenas sectoriales, que consisten en un conjunto de antenas direccionales distribuidas alrededor de un mástil central. En estas redes pueden haber estaciones con 2 sectores (a 180º), 4 sectores (a 90º) u 8 sectores (a 45º) todo depende del tipo de antena que se utilice y de la zona que se pretende dar cobertura. Dentro de un sector y para una determinada frecuencia (canal) todas las estaciones (BS) reciben la misma potencia o partes de la misma.

Cada antena define un sector, un área donde la frecuencia puede ser rehusada. Los sectores también pueden ser desarrollados en base a arrays de antenas, donde un conjunto de dipolos son combinados y se consiguen lóbulos direccionales para variar las relaciones de fase de las señales de cada una de las antenas. Las relaciones de fase son modificadas electrónicamente y, en el caso de antenas adaptativas, el sistema es capaz de ajustar la anchura y dirección del lóbulo para facilitar la mejor conexión con un determinado usuario. Son las conocidas antenas inteligentes.

Para esta topología de red, el downlink se maneja mediante una estación base (BS) centralizada y una antena sectorizada que es capaz de manejar varias zonas simultáneamente. Dentro de un canal de frecuencia y un sector de antenas dado, sólo existe una BS transmitiendo, de manera que no se tiene que coordinar con las demás BS, excepto en la multiplexación de tiempo. Las transmisiones en el enlace de bajada (downlink, DL) suelen ser broadcast, de forma que todas las estaciones de usuario reciben toda la información y escogen la que vaya dirigida a ellos. En el enlace de subida (uplink, UL) las estaciones de usuario comparten el canal mediante mecanismos de gestión de demanda.

En este sentido, un enlace Punto-multipunto, comparte un determinado nodo (en el lado uplink), que se caracteriza por tener una antena onmidireccional (o con varios sectores) y puntos de terminación (o repetidores) con antenas direccionales con una ganancia elevada. Este tipo de red es más sencillo de implementar que las redes punto a punto, ya que el hecho de añadir un subscriptor sólo requiere incorporar equipamiento del lado del cliente, no teniendo que variar nada en la estación base. Aunque, cada sitio remoto debe encontrarse dentro del radio de cobertura de la señal, que en el caso de WiMAX (a diferencia de la tecnología LMDS) no requerirá que se sitúe en puntos con visión directa.

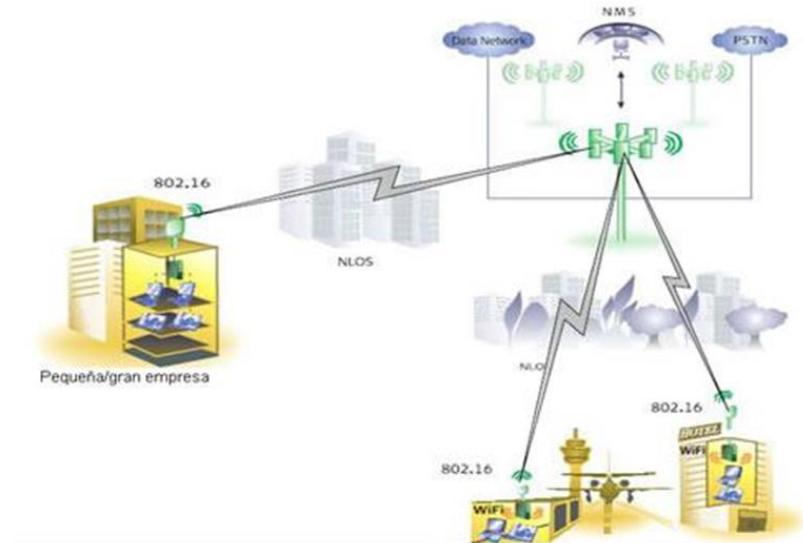


En síntesis, existe una Estación Base que controla la red, donde:

- Los usuarios se conectan a la Estación Base.
- La transmisión se divide en tramas de uplink y downlink por TDD o FDD
- El downlink es dividido para los usuarios. El uplink se accede por TDMA/TDM.

Por otra parte, la capa MAC es orientada a la conexión. Para propósitos de relacionar los servicios a las SS y asociarlos a los diferentes niveles de calidad de servicio (QoS), todas las comunicaciones de datos están en el contexto de una conexión. El flujo de servicio debe ser suministrado en el momento en el que la SS se instala en el sistema y justo después de que se registra; las conexiones se deben asociar a ese flujo de servicio para tener una referencia al hacer las peticiones de ancho de banda. El flujo de servicio define los parámetros de QoS de los packet data units (PDU) que se intercambian durante la conexión.

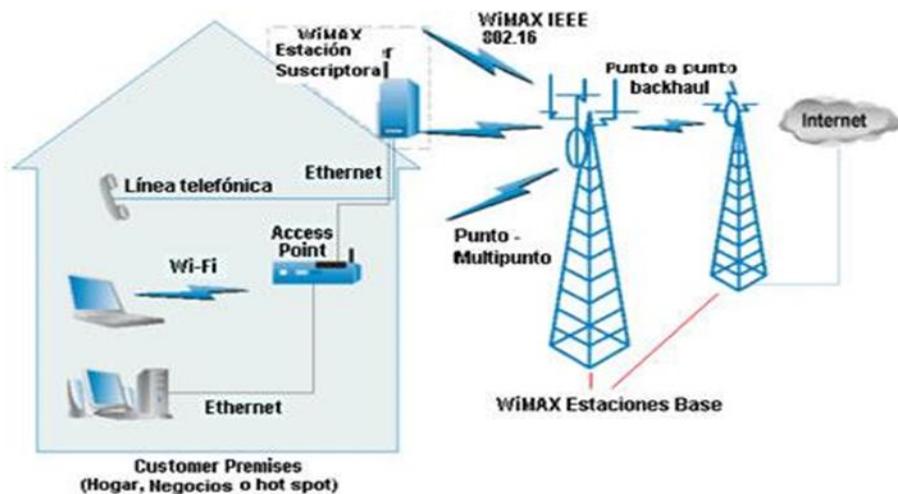
En adición, el 802.16 provee una tecnología inalámbrica ideal para conectar WLAN's 802.11 y hotspots comerciales con Internet, como se puede apreciar en la siguiente figura



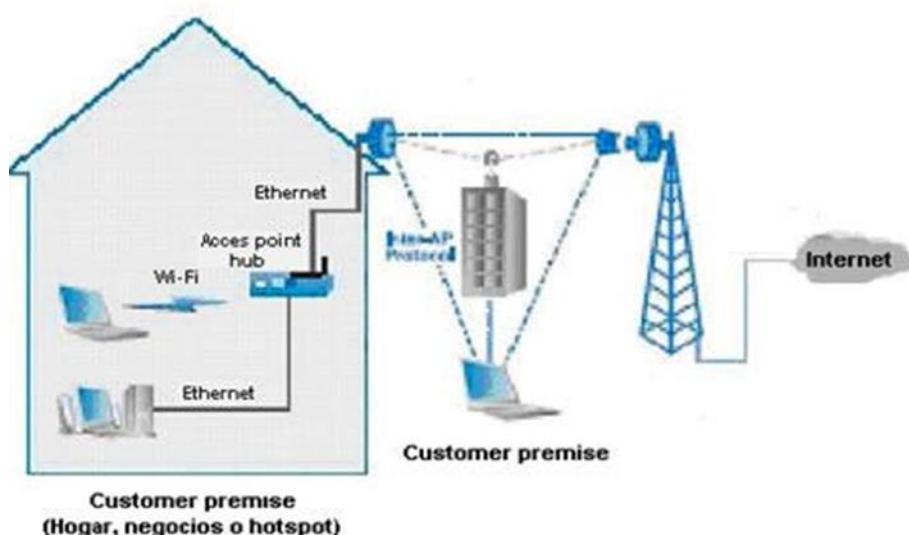
La arquitectura Punto - Multipunto representa la arquitectura más extendida que permite al operador de red alcanzar el mayor número de usuarios al menor coste y limita el número de routers y switches necesarios para operar la red.

Esta topología ha sido recomendada en ocasiones también para su uso en bandas milimétricas. El problema radica en la topografía de la mayor parte de las ciudades, que podrían ser los principales mercados para este tipo de servicios.

En la siguiente imagen se pueden observar los dos tipos de topologías de WiMAX:

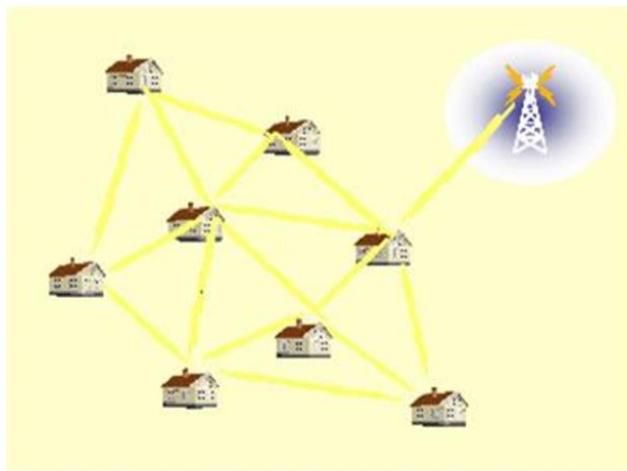


Redes Enmalladas (Mesh). Las redes enmalladas son aquellas en las que la comunicación se puede hacer entre los diferentes nodos y no sólo entre nodo y estación base.



Para este tipo de redes, se pueden realizar las operaciones de dos maneras diferentes: distribuida ó centralizada: para la distribuida, todos los nodos deben coordinar con los demás la manera de transmitir para evitar colisiones con los datos y realizar el control de tráfico, y además deben enviar por difusión

(broadcast) su respectivo estado (recursos disponibles, peticiones y concesiones) a todos sus vecinos; para la centralizada, los recursos se asignan de una manera más concentrada, ya que la estación base Mesh, recopila varias peticiones de un determinado sector y otorga los respectivos recursos para cada enlace, tanto para el downlink como para el uplink, al mismo tiempo que comunica estas decisiones a las demás estaciones del sector.



En una red mesh cada terminal de usuario es capaz de establecer varios enlaces con usuarios adyacentes. De esta forma, existen una serie de alternativas antes de llegar al punto origen de la red. Algoritmos especiales de encaminamiento son capaces de direccionar las comunicaciones por el camino más adecuado en cada momento; si un equipo de cliente deja de funcionar, la red sigue funcionando por caminos alternativos.

En este sentido, una red modo mesh se caracteriza por:

- No se requiere una entidad centralizada de coordinación.
- Los usuarios se conectan unos con otros.
- Las tramas se dividen en minislots.
- No hay división entre uplink o downlink, la transmisión va en las dos direcciones por TDD.

[Dispositivos usados para establecer una conexión por WiMAX.](#)

Estos son algunos de los dispositivos usados por esta tecnología:

CPE

El CPE (Customer Premises Equipment) es un aparato conectado a nuestro computador (De escritorio o Laptop) que nos permite crear una red WiMAX dentro de nuestra casa. También podemos conectar nuestro teléfono para realizar llamadas VoIP de bajo costo. Al igual que las tarjetas WiMAX este se puede llevar a todas partes que queramos y conectarnos inalámbricamente donde sea a una alta velocidad.

Tarjeta WiMAX

Tarjeta de red portátil usada para hacer conexiones de red usando el estándar 802.16x(WiMAX). Esta es usada en laptops. Solo la conectamos, instalamos el driver y configuramos la conexión de modo que podremos salir a la calle y nuestra conexión WiMAX estará accesible a donde quiera que vayamos sin necesidad de buscar un router o punto de acceso (HotSpot).

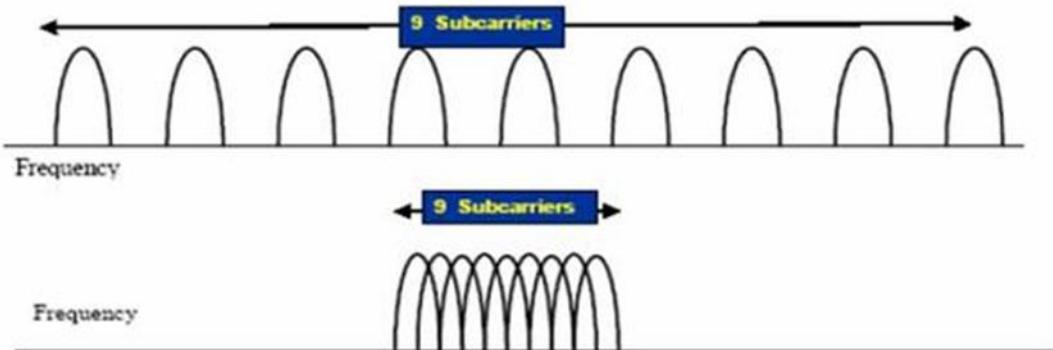
Equipos para Terminales del Abonado:



1. Conexión de la mini-antena
2. Conexión adaptador de energía
3. Conexión de Red
4. RSI: Intensidad de la señal
5. DATA: Transmisión de datos
6. LINK: Cable de red conectado
7. STATUS: Estado
8. POWER: Indicador de Energía

CARACTERISTICAS TECNICAS: OFDM

- Técnica de transmisión multiportadora OFDM (Orthogonal Frequency Division Multiplexing).
- Divide el ancho de banda disponible en diferentes subportadoras de banda estrecha (FDM).



Se denomina multi-discreto tono de modulación porque, en lugar de un solo transportista está modulada, un gran número de espaciarse subcarriers son moduladas a través de algunos m-aria de QAM. Se trata de una propagación de espectro técnica que aumenta la eficiencia de las comunicaciones de datos mediante el incremento de datos porque hay más compañías aéreas que modulan. Además, los problemas con multi-ruta de señal y cancelación de interferencia espectral se reducen de forma selectiva la modulación de la "clara" o hacer caso omiso de los transportistas con los transportistas de alta velocidad binaria errores.

Al igual que FDM, OFDM también se utiliza múltiples sub-transportistas, pero el sub-los transportistas están poco espaciados entre sí, sin causar interferencia, la supresión de guardia entre bandas adyacentes sub-portadoras. Esto es posible porque las frecuencias (sub-aéreas) son ortogonales, es decir, el pico de una sub-portadora coincide con la nula adyacente de un sub-carrier.

En un sistema OFDM, una muy alta tasa de flujo de datos se divide en múltiples paralelas baja tasa de flujos de datos. Cada menor flujo de datos es entonces asignada a los datos individuales sub-portadora y

modulada a través de algunos tipos de PSK (Phase Shift Keying) o QAM (modulación de amplitud de cuadratura). es decir, BPSK, QPSK, 16-QAM, 64-QAM.

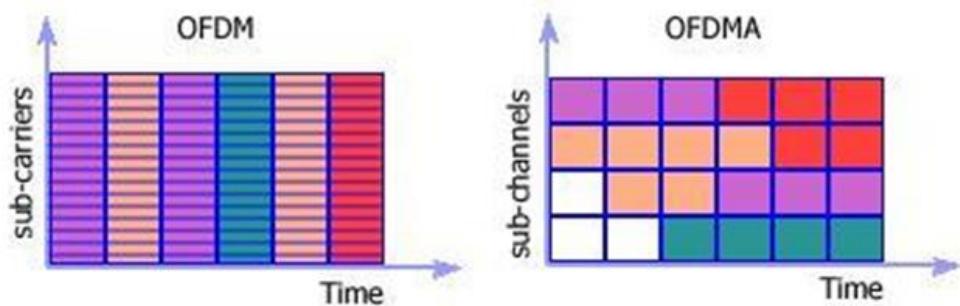
OFDM necesita menos ancho de banda que FDM para transportar la misma cantidad de información lo que se traduce en mayor eficiencia espectral. Además de una alta eficiencia espectral, un sistema de OFDM como WiMAX es más resistente a RNE medio ambiente. Puede ser eficiente y superar las interferencias de frecuencia selectiva desvanecimiento causado por múltiples porque la igualación se hace en un subconjunto de sub-compañías aéreas en lugar de una sola compañía aérea más amplia. El efecto del ISI (Inter Symbol Interference) se suprime en virtud de un período más largo símbolo del paralelo OFDM sub-portadoras de un único sistema de soporte y el uso de un prefijo cíclico (CP).

El OFDM propagación de espectro sistema se utiliza para muchas aplicaciones ampliamente utilizadas, incluida la televisión digital en Alemania, Australia, Japón y Europa; radiodifusión sonora digital en Europa; Línea de abonado digital asíncrona (ADSL), módems y las redes inalámbricas en todo el mundo (IEEE 802.11a / g).

OFDMA

Emplea múltiples poco espaciados sub-transportistas, pero los sub-los transportistas están divididos en grupos de sub-portadoras. Cada grupo se llama un sub-canal. Los sub-aéreas que forman un sub-canal no tienen por qué ser adyacentes. En la bajada, un sub-canal pueden ser destinados a diferentes receptores. En el enlace ascendente, un transmisor se le puede asignar uno o varios sub-canales.

Subchannelization define sub-canales que pueden ser asignados a las estaciones de abonado (SSS) en función de su canal de condiciones y requisitos de datos. El uso de subchannelization, en el mismo horario a Mobile WiMAX Base Station (BS) puede asignar más poder transmitir a los dispositivos de usuario (SSS), con menor relación S / R (señal-ruido), y menos poder para los usuarios de dispositivos con una mayor relación señal ruido. Subchannelization también permite a la BS de asignar mayor poder a sub-canales asignados al interior SSS lo mejor en el fomento de la cobertura.



Subchannelization en el enlace ascendente puede guardar un dispositivo de usuario transmitir el poder ya que puede concentrar el poder sólo en determinados sub-canal (s) que le han sido asignados. Este ahorro de energía característica es especialmente útil para de baterías usuario dispositivos, el probable caso en Mobile WiMAX.

Funcionamiento

En una punta esta la Estación Base, elemento que se identifica normalmente con un operador de comunicaciones, en donde existen una o varias antenas con las que se retransmite la señal. Este elemento puede ser una torre como tal en donde se anclan las antenas o puede tratarse de una pequeña edificación en algún lugar elevado, como otro edificio o un altozano. Las antenas que se ubican en este extremo

pueden ser omnidireccionales, de muchas direcciones, sectoriales, que cubren sectores específicos del territorio de cobertura, o antenas de panel, para conexiones punto a punto, cuando se quiere cubrir una gran distancia y se necesita una tasa de transferencia alta.

En el otro extremo de la conexión, está el usuario final, que puede ser residencial o corporativo, se encuentra instalado el CPE (Customer Premises Equipment, Equipo Local de Cliente), que constituye el último eslabón de este tipo de redes y en donde acaba el flujo de transferencia de datos entre operador y el cliente final. Por las características de la señal transmitida en WiMax, el CPE no resulta aparatoso. Se trata de un pequeño dispositivo, como una mínima caja en la que asoma una antena, cuando la señal se pretende distribuir en una red LAN o se da servicio a varios puestos. Se instala en el exterior o interior del edificio y se conecta al punto de distribución. Por su tamaño y aspecto, en cualquier caso, resulta un elemento poco llamativo para el observador. Pero puede ser perfectamente una tarjeta PCMCIA, PCI o módulo USB que se inserte llanamente en el ordenador, cuando se trata de conexiones directas de equipos individuales. Es posible, incluso, encontrar portátiles que lo llevan integrado en su circuitería.

Estación Base

En una Torre o Estación Base, pueden coincidir distintos tipos de antenas, con las que atender distintas necesidades y oferta de servicio para abonados. Un mismo enlace de WiMax, tiene capacidad para proporcionar varios canales por conexión física y atender a múltiples suscriptores, cada uno de ellos tratados privadamente, con protocolos y nivel de servicio diferenciados para cada uno de ellos, según lo que puedan contratar individualmente. En la segunda parte de este artículo, veremos la cómo funciona la conexión de los dos puntos. La torre, y el usuario final.

Como conectar la Torre base y el CPE

Existen dos formas de poder lograrlo. Cuando se plantea un enlace LOS, esto quiere decir que, entre la Torre Base y los CPE de usuario, no hay obstáculo alguno, que se interponga en el intercambio de señal, existe visibilidad y una comunicación directa. Éste es el mejor de los casos y la comunicación se produce en las frecuencias altas, entre 12 y 66 GHz, consiguiendo un radio de cobertura muy alto, y donde las conexiones pueden alcanzar las mayores tasas de transmisión de estas especificaciones. Si los enlaces son del tipo NLOS, la comunicación se produce sin contacto visual directo entre los extremos. La señal debe sortear obstáculos constructivos y para evitar los problemas de interferencia que estos pueden introducir en la señal, se opera en las frecuencias más bajas, entre 2 y 11 GHz, lo que provoca que las velocidades de operación de los enlaces sea menor y la cobertura tenga una extensión mucho más reducida, situándose su alcance en una extensión similar a la que cubren las células de telefonía móvil. Pero eso sí, NLOS es superior a Wi-Fi.

Transmisión de dos puntos

Para este cometido, se utiliza la modulación OFDM (Orthogonal Frequency División Multiplexing), con 256 portadoras y OFDMA (Orthogonal Frequency División Multiple Access), con 2.048 portadoras. Una modulación que es apropiada para las transmisiones de flujo sostenido como para aquellas otras que se producen a ráfagas, lo que este tipo de conexión está capacitado para llevar datos de cualquier tipo de servicio en IP, voz, datos y también vídeo. Para establecer el mejor enlace posible, el estándar define mecanismos de modulación adaptativa, que permite que la estación base y los equipos receptores de usuario negocien las condiciones de la modulación a emplear, según las características de cada enlace de radio. Una facilidad que se refuerza con el empleo de antenas mejoradas, que incrementan la eficiencia y cobertura de la comunicación, aprovechando la experiencia tecnológica de la telefonía móvil 3G para este componente.

CERTIFICACIONES Y ESTANDARES

WiMAX Forum

El WiMAX Forum¹ es una organización sin fines de lucro, impulsada por el sector de las comunicaciones radio, que fue creada con el objeto de promover y certificar la interoperabilidad de los productos inalámbricos de banda ancha de conformidad con los estándares IEEE 802.16 y ETSI HyperMAN. El objetivo de esta institución es acelerar las implementaciones mundiales y expandir el mercado de soluciones de acceso inalámbrico de banda ancha interoperables y basadas en estándares.

El foro está trabajando con las empresas asociadas a fin de desarrollar perfiles estandarizados y productos WiMAX interoperables en torno a bandas concretas del espectro de frecuencia de radio, fundamentalmente 2.3GHz, 2.5GHz, 3.5GHz y 5.8GHz. Son miembros del WiMAX Fórum numerosas empresas y proveedores de servicios.

Estándar 802.16 (WiMAX)

WiMAX (Worldwide Interoperability for Microwave Access), es la denominación de una marca de referencia para productos que pasan la conformidad y los test de interoperatividad de los estándares 802.16. IEEE802.16 es el grupo de trabajo del IEEE especializado en acceso punto a multipunto de banda ancha. El estándar original WiMAX, el IEEE 802.16, especifica la tecnología para el rango de 10-66 GHz. Posteriormente, 802.16a añadió soporte para el rango de 2 a 11 GHz, donde algunas bandas no requieren licencia, o sólo precisan una simple autorización.

Los esfuerzos se están centrando en esta variación del estándar. La ventaja principal se centra en la posibilidad de realizar comunicaciones sin disponer de línea de vista, haciendo un uso eficiente de las tecnologías existentes, pero sin desafiar a las leyes de la física.

Una característica importante del estándar es que define una capa MAC que soporta múltiples especificaciones físicas (PHY). Esto es vital a la hora de permitir a los fabricantes su diferenciación respecto a la competencia y por lo que se considera el estándar como un marco de trabajo para la evolución de tecnologías inalámbricas. WiMAX puede ser descrito como el intento de mezclar muchas tecnologías para cubrir varias necesidades en un espectro amplio, con la diferencia de que a este foco vago se le están sacando rentabilidades prácticas.

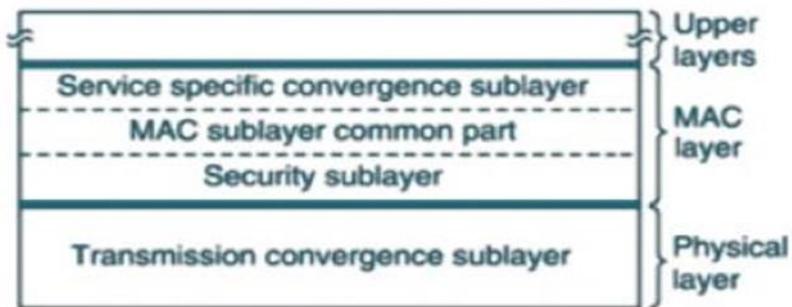
WiMAX se basa principalmente en dos subestándares del IEEE, 802.16-2004 para el acceso fijo, y 802.16e para el acceso portable o móvil. Las diferentes versiones de especificaciones de cada subestándar se presentan en sucesivas Wave, que se corresponden con los diferentes perfiles de sistema (WiMAX Forum System Profiles) definidos para su certificación. Actualmente se han definido el perfil de WiMAX fijo, y el de WiMAX móvil. Para el WiMAX Fijo, las normas de certificación están completamente definidas, manteniendo las características del subestándar ya mencionadas, pero especialmente para WiMAX Móvil se están definiendo sucesivas versiones o releases, y dentro de cada una de ellas, sucesivas fases (waves) que van marcando las novedades en la definición del proceso de certificación (Certification Profiles).

Seguridad

Como cualquier otra red de comunicación al servicio de empresas y usuarios individuales que desean mantener su información segura, los sistemas WiMAX necesitan aplicar medidas para asegurar la privacidad de sus usuarios finales y prevenir del acceso a información confidencial o sensible a personas que no están autorizadas.

Desde que los sistemas WiMAX utilizan el interface radio como medio de transmisión, la pregunta que conviene hacerse es cómo prevenir que los intrusos no intercepten información sensible y confidencial transmitida por ondas hertzianas ya sea en banda libre o banda licenciada.

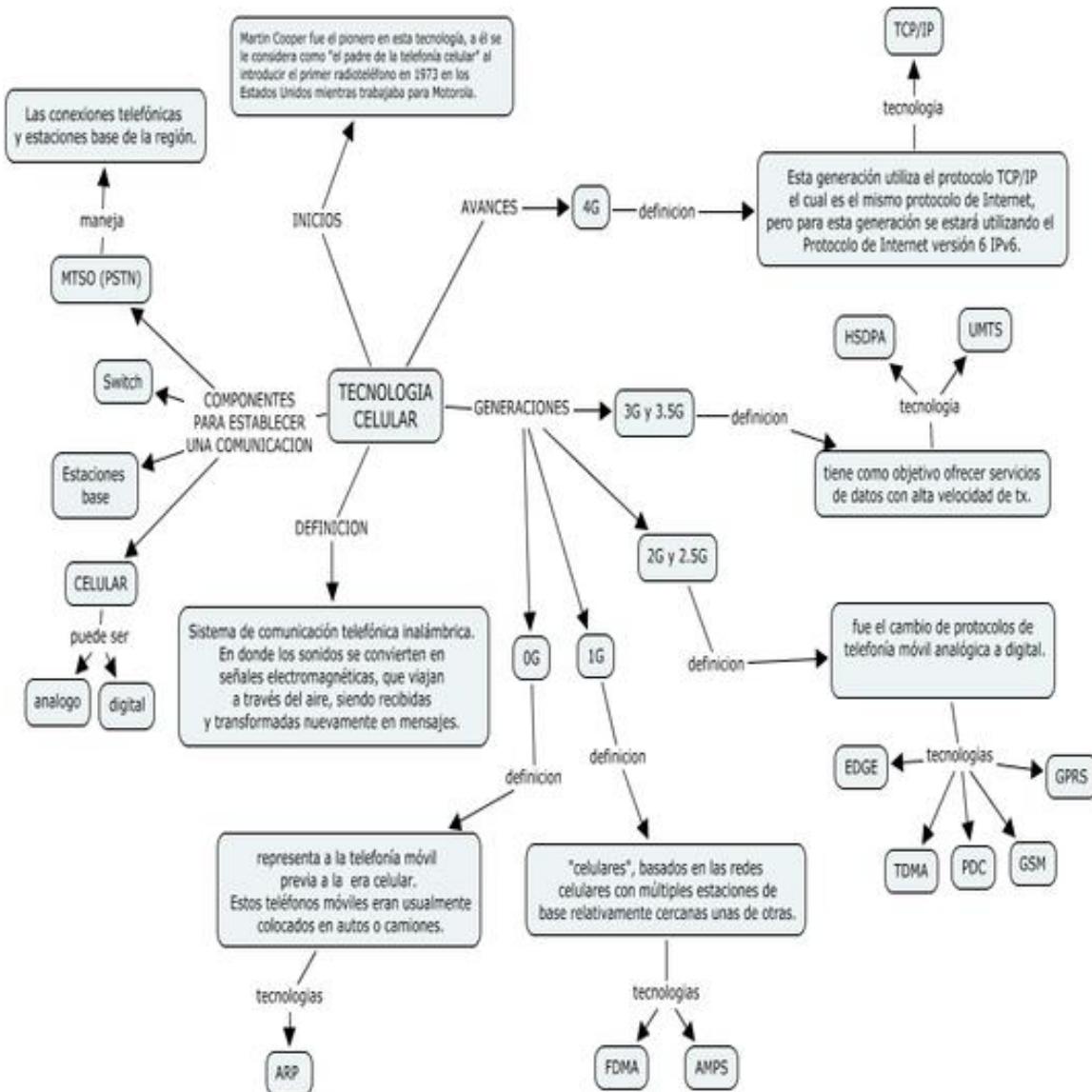
Tanto los clientes como los operadores deberían sentirse protegidos y confiar en que su sistema es privado y seguro, y que las medidas apropiadas están disponibles para minimizar los riesgos de seguridad, incluyendo:



Escuchas/espionaje: interceptar información de forma intencional cuando se está transmitiendo.

- Privacidad: Asegurarse de que la información transmitida es solamente leída por los destinatarios a los que va dirigida.
- MAC Spoofing: evitar que un atacante copie las direcciones MAC de CPE legítimas con el fin de conseguir el acceso a la red.
- Robo del Servicio: prevenir que los agresores puedan acceder a Internet u otros servicios utilizando CPE robadas y advirtiendo a los usuarios legítimos de obtener los servicios de forma gratuita.

Mapa Conceptual



CAPITULO 10

REDES DE NUEVA GENERACION (NGN)

Se denomina NGN Red de Siguiente Generación a la evolución de redes de telecomunicación y acceso telefónico clásico con el objetivo de lograr la convergencia tecnológica de los nuevos servicios multimedia (voz, datos, video...).

La idea principal que se esconde debajo de este tipo de redes es el transporte de paquetes encapsulados de información a través de Internet. Estas nuevas redes son construidas a partir del protocolo IP (Internet Protocol), siendo el término "all-IP" comúnmente utilizado para describir dicha evolución.

Según la ITU-T: Una Red de próxima Generación es una red basada en la transmisión de paquetes capaz de proveer servicios integrados, incluyendo los tradicionales telefónicos, y capaz de explotar al máximo el ancho de banda del canal haciendo uso de las Tecnologías de Calidad del Servicio (QoS) de modo que el transporte sea totalmente independiente de la infraestructura de red utilizada.

Además, ofrece acceso libre para usuarios de diferentes compañías telefónicas y apoya la movilidad que permite acceso multipunto a los usuarios.

La NGN se caracteriza por los siguientes aspectos fundamentales:

- Transferencia basada en paquetes
- La separación de las funciones de control entre las capacidades portadoras, llamada / sesión, y aplicación / servicio
- Separación entre la prestación de servicios de red, y la provisión de interfaces abiertas
- Soporte para una amplia gama de servicios, aplicaciones y mecanismos basado en módulos de servicios (incluyendo / servicios en tiempo no real tiempo real / transmisión y multimedia)
- capacidades de banda ancha con calidad de servicio y la transparencia de extremo a extremo
- Interfuncionamiento con redes heredadas a través de interfaces abiertas
- movilidad generalizada
- El acceso no restringido a los usuarios de diferentes proveedores de servicios
- Una variedad de esquemas de identificación que puede ser resuelta a las direcciones IP para los propósitos de enrutamiento en redes IP
- características de los servicios unificados para el mismo servicio que percibe el usuario
- servicios de convergencia entre fijo / móvil
- Independencia de las funciones relacionadas con los servicios de tecnologías de transporte subyacentes
- Cumple con todos los requisitos reglamentarios, por ejemplo relativas a las comunicaciones de emergencia y seguridad / privacidad, etc.

Concepto IMS

IMS (IP Multimedia Subsystem) es una manera completamente nueva de distribuir multimedia (voz, video, datos, etc.) independiente del dispositivo (teléfono, móvil, o fijo, IPTV, notebook, etc.) o de medio de acceso (3G / EDGE / GPRS, Wi-Fi, banda ancha, línea telefónica, etc.).

La industria de telecomunicaciones está actualmente migrando hacia sistemas *all-IP*, impulsada por la necesidad fundamental de reducir costos, crear nuevos servicios que generen lucro y proteger el modelo

de negocios de operadora. Esas son las metas tanto de comunicación fija y móvil. IMS permite la convergencia de las tecnologías de datos, voz y redes sobre una infraestructura basada en IP.

Para los usuarios, servicios basados en IMS permitirán comunicaciones en varios modos inclusive voz, texto, fotos y video, o cualquier combinación de esas de una forma altamente personal y segura. Eso permite que las operadoras ofrezcan servicios nuevos e innovadores que son esperados por los usuarios finales.

La Plataforma IMS, es más que un sistema técnico, es un modelo para viabilizar de forma consistente una visión integradora de convergencia de servicios de comunicación, tecnologías de redes, de acceso, contenido, ingreso y control. Con eso generando nuevas amplias y concretas posibilidades de negocios y atractivas perspectivas de ROI (*Return on Investment*), sea para proveedores de plataforma así como para las empresas operadoras, proveedores de contenido y prestadoras de servicios, que tendrán a su disposición un nuevo y amplio abanico de posibilidades de negocios.

[¿Porque IMS?](#)

Históricamente cada vez se desplego un nuevo servicio, se creó una red específica con sus correspondientes protocolos y plataformas, tal como vimos durante los otros capítulos. Muchas redes, prácticamente inconexas y dificultosamente interconectadas.

Todas las tecnologías que se utilizan en telecomunicaciones ingresaron en distintos momentos en el tiempo, por lo tanto son soportadas por redes y plataformas específicas para cada una de ellas, de acuerdo con la tecnología que existente al momento del surgimiento de cada uno de los medios de comunicación.

Las arquitecturas tecnológicas que soportan cada una de las redes de comunicación están separadas, y utilizan protocolos distintos. Por ejemplo, la televisión usa altas frecuencias y ultra altas frecuencias, los teléfonos móviles usan GSM y los computadores personales internet (a través del protocolo TCP/IP en la mayoría de los casos). Sin embargo los equipos de acceso a estas redes incorporan cada vez más tecnología que permite obtener diversos contenidos multimedia. Los teléfonos móviles comenzaron a incorporar imágenes, música y video. Además existe un desafío en poder mantener las sesiones de los teléfonos móviles cuando cambiaban de red, ya sea a otra del mismo proveedor u otro diferente a través de Roaming. Por ejemplo llegar a mi casa y continuar en el teléfono fijo, la comunicación que había iniciado en el teléfono móvil y viceversa.

Con la intención de unificar todas la redes, el grupo 3rd Generation Partnership Project se planteó crear el IMS que pretende ser una arquitectura que soporte el tráfico de voz, datos y multimedia mediante la conmutación de paquetes a direcciones IP con independencia del medio de acceso ya sean teléfonos móviles, fijos; computadores personales; y todo dispositivo que pueda tener una dirección IP en la red. Sólo requiere que los equipos utilicen el protocolo de sesión SIP32 que permite la señalización y administración de sesiones.

Además, dada la necesidad de reducir costos y al mismo tiempo aumentar coberturas y servicios, ha hecho que cada vez más la industria de telecomunicaciones migre hacia sistemas operados casi totalmente en infraestructura IP, esto explica porque miran con interés ideas integradas de convergencia de datos y voz sobre infraestructuras basada en IP, como IMS.

El IMS es más que un sistema técnico, es un modelo para realizar una integración convergente de servicios de comunicación, tecnologías de redes, de acceso, contenido, ingreso y control. Generando así

nuevas amplias y concretas posibilidades de negocios ya sea para proveedores de plataforma así como para las empresas operadoras, proveedores de contenido y prestadoras de servicios, que tendrán a su disposición un nuevo y amplio abanico de posibilidades de negocios.

IMS no solamente sirve para proporcionar nuevos servicios. Lo que realmente pretende es servir para todo tipo de servicios, tanto actuales como futuros, que se puedan prestar por Internet. IMS permitirá que los operadores puedan controlar y facturar cada uno de los servicios.

IMS hace que cuando los usuarios se desplacen puedan utilizar todos los servicios que disponen cuando están en ubicaciones fijas. Dicho en otras palabras. No importa el acceso ni el dispositivo utilizado, el servicio siempre puede ser brindado con calidad.

Para conseguirlo, utiliza protocolos estandar, aprobados por IETF33. De modo que una sesión multimedia entre dos usuarios IMS, un usuario IMS y otro que esté en Internet, o entre dos usuarios que estén en internet se efectúa usando los mismos protocolos. Además, los que desarrollen aplicaciones o servicios también lo harán sobre el protocolo IP. De este modo IMS realmente hace que el mundo IP de Internet sea el elemento convergente de las distintas redes de telecomunicaciones.

¿Qué es IMS?

IMS o IP Multimedia Subsystem es un conjunto de especificaciones que describen la arquitectura de red capaz de soportar telefonía y servicios multimedia a través de IP. Define una arquitectura para tráfico de voz, datos, video, servicios e imágenes conjuntamente a través de infraestructura basada en el ruteo de paquetes a través de direcciones IP. Esto permite incorporar en una red todo tipo de servicios de voz, multimedia y datos accesibles a través de cualquier medio con conexión a internet, ya sea fija, o móvil. Sólo requiere que los equipos utilicen el protocolo de sesión SIP (Session Initiation Protocol) que permite la señalización de sesiones.

Este concepto necesita que cada dispositivo conectado a la red que requiera sesiones multimedia, de voz y de datos, posea una dirección IP.

Arquitectura del IMS

La arquitectura IMS (IP Multimedia Subsystem) está concebida en niveles o capas, teniendo cada capa sus elementos de red y funcionalidades.

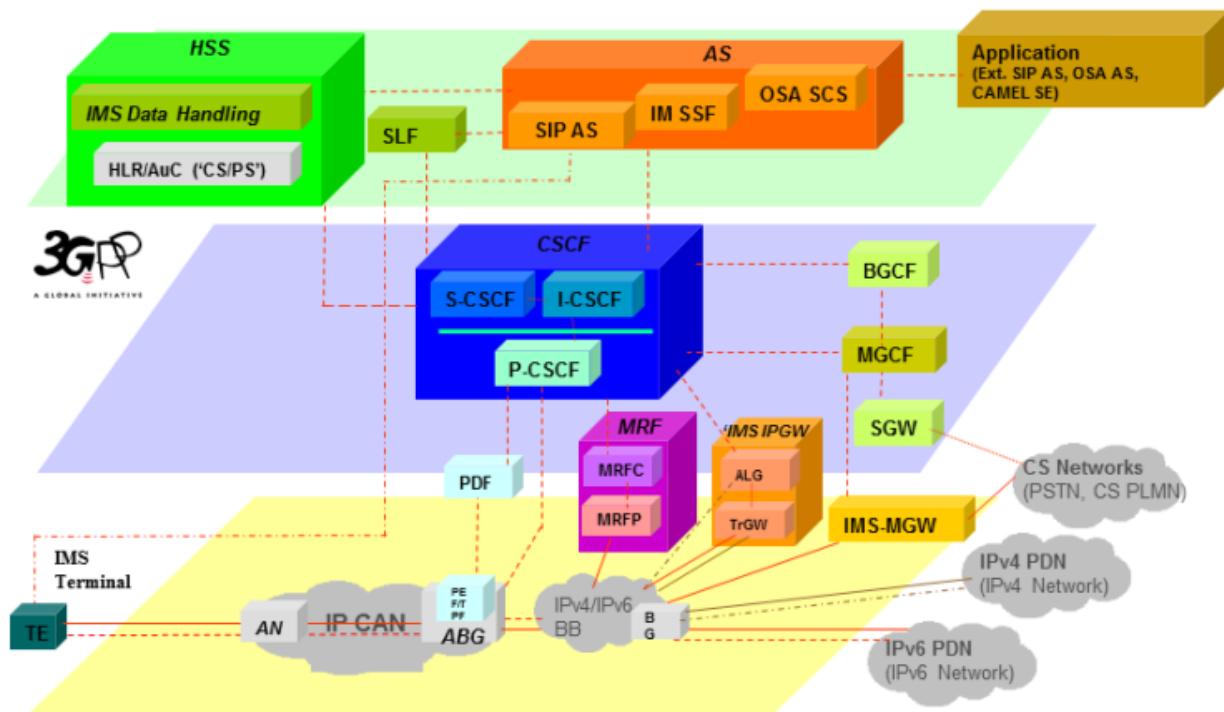
El gran logro del IMS y su estratificación es el hacer que el servicio sea agnóstico del acceso. Eso quiere decir que son importar cuál sea el acceso, el usuario puede tener la misma experiencia del servicio.

Las capas se describen a continuación:

- **Capa de Acceso** La capa de acceso puede representar todo acceso de alta velocidad, tal como: xDSL (x Digital Subscriber Line), Redes de Cable, Wi-Fi (Wireless Fidelity), Wi-Max, LTE (Long Term Evolution), etc.
- **Capa de Transporte** La capa de transporte representa una red IP. Esta red podrá integrar mecanismos de calidad de servicio con MPLS34, DiffServ35, RSVP36, entre otros tantos. La capa de transporte está compuesta por routers (“edge routers” para el acceso y “core routers” para el tránsito), conectados a través de una red de transmisión.
- **Capa de Control** Está formada por diversos controladores de sesión (Session Controllers) responsables del encaminamiento de la señalización entre usuarios y de la invocación de los servicios. Estos nodos se llaman “Call Session Control Function” o CSCF. También aquí se encuentra la Base de Datos (HSS) y el “Multimedia Resource Function” (o “MRF”) que los

proveedores llaman Servidores de Media IP (“IP Media Server” o “IP MS”). El MRF se divide en dos partes, el MRFC (MRF Control), ubicado en la Capa de Control, y el MRFP (MRF Processor), ubicado en la Capa de Transporte. La interconexión entre ambos es a través del protocolo H.248. Podemos hacer una analogía (bastante forzada pero a los fines del entendimiento) y decir que esta capa cumple las funciones similares a una central de conmutación o a un Service Swiching de una red inteligente.

- **Capa de Aplicación** La capa de aplicación introduce las aplicaciones (servicios de valor agregado) propuestas a los usuarios. Gracias a su capa de control, El operador puede posicionarse como integrador de servicios ofrecidos por él mismo o bien por terceros. Esta capa está formada por servidores de aplicación (“Application Server” o “AS”). En esta capa residen TODOS los servicios. Aquellos que alguna vez estuvieron integrados junto con el control en las redes monolíticas, hoy están a disposición de cualquier usuario sin importar cuál es su acceso



Arquitectura de IMS.

En la arquitectura genérica de una red IMS, la entidad funcional clave es el nodo CSCF (Call State Control Function), que integra, a su vez, tres subsistemas -P-CSCF (Proxy CSCF), S-CSCF (Serving CSCF) y I-CSCF (Interrogating CSCF)-, encargados, básicamente, de procesar y encaminar la señalización, controlar los recursos del subsistema de transporte, realizar el registro y autenticación de los usuarios, aprovisionar los servicios IMS mediante el desvío de la señalización a los servidores de aplicación en cuestión, y generar los registros de tarificación. IMS dispone también de una base de datos o HSS (Home Subscriber System) que describe a cada cliente, sus terminales y sus derechos de acceso a las distintas aplicaciones. Los nodos MGCF (Media Gateway Control Function) e IM-MGW (IP Multimedia Gateway) permiten el interfuncionamiento de IMS con las redes de conmutación de circuitos (RTB, RDSI, GSM, etc.), implementando los planes de control y usuario, respectivamente. Finalmente, nos encontramos con los servidores de aplicación y las pasarelas con destino al plano de servicios, que son los que ofrecen aplicaciones a los usuarios.

Identificador de recursos universal

IMS no define las aplicaciones que pueden ser ofrecidas al usuario final, sino la infraestructura y capacidades del servicio que los operadores pueden emplear para construir su propia oferta de servicios. El operador IMS puede elegir ofrecer los servicios de forma independiente, combinada o en multitud de variantes, pero todos ellos tendrán una infraestructura común, reduciendo su ciclo de desarrollo y los costes de equipamiento y operación. Los servicios finales pueden ser los servicios tradicionales (las llamadas básicas de voz por conmutación de circuitos, el correo electrónico, la mensajería de texto, la mensajería multimedia, etc.) o bien servicios multimedia avanzados (videoconferencia convencional o adaptada para personas con algún tipo de discapacidad, difusión de radio, difusión de TV, video bajo de demanda, mensajería instantánea, chat multimedia, videojuegos en red interactivos, localización o guiado, PTT, etc.).

La identificación de los usuarios, servicios y nodos se realiza mediante un URI (Universal Resource Identifier), que evita que el usuario deba memorizar números de teléfono, pues se trata de nombres al estilo de servicios Internet.

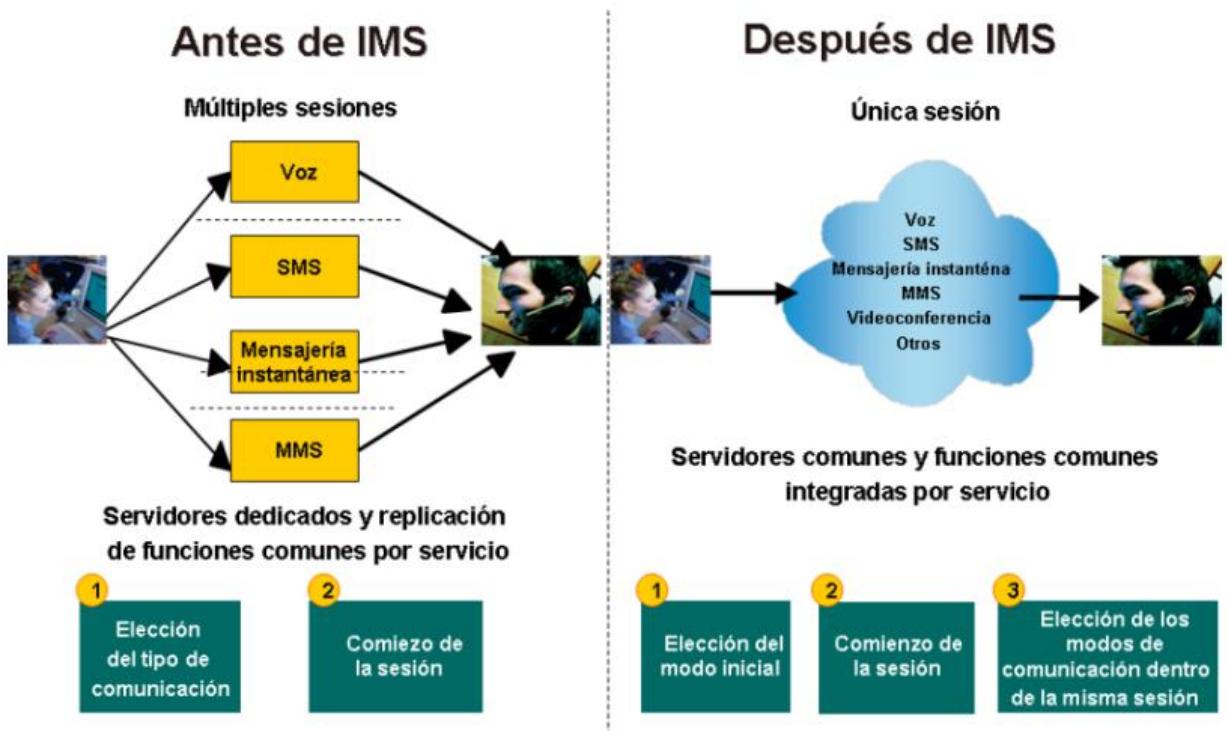
De esta forma, IMS ofrece para el acceso a otros usuarios o contenidos una interfaz gráfica similar a los actuales programas de mensajería instantánea , con la ventaja de que integrara la telefonía fija y móvil multimedia, los accesos inalámbricos y cualquier sistema de comunicaciones que se implemente en el futuro. Es decir, una persona podrá ver desde su teléfono móvil que contactos de su agenda están conectados, incluso donde están en ese momento, y a través de que medios es posible comunicarse con ellos. Tras elegir uno o varios destinatarios, se podrá iniciar una conversación por mensajes, voz o videoconferencia y pasar de un modo a otro cuando desee, o compartir archivos mientras navega por Internet o ve la televisión. Si está llegando a casa, podrá pasar instantáneamente a su teléfono fijo o red de banda ancha particular a través de Wi-Fi o Bluetooth. Además, todo dentro de una misma sesión y sin interrumpir la comunicación en ningún momento

Funcionalidad, precio y calidad

En la estructura de red tradicional, las funcionalidades comunes de cada servicio (facturación, presencia, gestión de grupos y listas de contactos, encaminamiento, provisión, etc.) están implementadas por separado, en una estructura replicada a lo largo de toda la red. IMS, por el contrario, proporciona una serie de funciones comunes que son genéricas en su estructura e implementación, y que todos los servicios de la red pueden reutilizar. Por ejemplo, el sistema de facturación IMS registra los datos relacionados con la sesión IMS, tales como los usuarios implicados, la duración, los componentes multimedia empleados y la QoS autorizada; y permite facturar cualquier tipo de servicio tanto en pospago como en prepago, según su duración, contenidos, volumen de datos, destino de la sesión o las diferentes combinaciones de los anteriores. Esto además facilita y acelera el proceso de creación y suministro de servicios, y la reutilización de infraestructura de transporte de red y de servidores de aplicaciones, y minimiza el inmovilizado fijo y la necesidad de personal técnico en todas las áreas (provisión, operación y mantenimiento, facturación, etc.). La posibilidad de ofrecer paquetes de servicios es muy importante para reforzar la posición competitiva de los operadores de telecomunicación. Por ejemplo, la ventaja tradicional de las operadoras de cable frente a los antiguos ex monopolios telefónicos era la posibilidad de ofrecer una oferta integrada de telefonía, Internet y televisión. Ahora la amenaza procede de los nuevos proveedores de servicios capaces de ofrecer aplicaciones gratuitas o a bajo coste sobre su infraestructura de red. De esta forma, empresas como Skype pueden ofrecer VoIP de bajo coste a sus usuarios empleando una arquitectura P2P, sin tener que pagar al proveedor de acceso a Internet por

suministrar dicho servicio y sin tener que asumir el mantenimiento de ninguna infraestructura de red, pues tan solo es necesario disponer de unos pocos servidores.

Sin embargo, estas empresas no son capaces de ofrecer el catálogo de servicios que podría ofertar un operador con IMS. Además, las operadoras podrán, gracias a esta nueva tecnología, ir entrando en el mundo de los servicios informáticos, permitiendo a sus clientes empresariales disfrutar de muchas de sus aplicaciones actuales bajo el modelo de pago por uso, sin tener que realizar constantes inversiones en hardware y software, ya que será más rentable y eficiente distribuirlas en red,



Principios tecnológicos

- El control de la sesión se realiza mediante el protocolo de control de llamada IMS, basado en SIP y SDP. La señalización de IMS se realiza mediante el protocolo SIP (Session Initiation Protocol), diseñado originariamente por el IETF para la gestión de sesiones multimedia en Internet. SIP aporta las funciones para el registro, establecimiento, modificación y finalización de las sesiones IMS entre dispositivos diversos. Puesto que no todos los dispositivos son capaces de soportar los mismos servicios, al establecer la sesión se negocian las características de esta mediante el protocolo SDP (Session Description Protocol), también diseñado por el IETF. Mediante SDP, los extremos de una sesión pueden indicar sus capacidades multimedia y definir el tipo de sesión que desean mantener. En este intercambio de señalización se negocia también la QoS, tanto durante el establecimiento como durante la sesión en curso. Por ello, y puesto que con IMS es posible monitorizar en todo momento la calidad del servicio en términos de latencia, ancho de banda y seguridad, la QoS en IMS es mucho más dinámica que en las tradicionales redes de telecomunicación.

- **El transporte de red es realizado mediante IPv6 en vez de IPv4.** La razón es que IPv6 está siendo paulatinamente desplegado en Internet y existen muchas empresas e instituciones que ya lo emplean internamente. De este modo, el 3GPP prefirió dar compatibilidad hacia atrás en lugar de hacia delante y partir de la situación más avanzada técnicamente. Entre las ventajas de IPv6 cabe destacar la QoS y seguridad integradas, la auto configuración, un mayor espacio de direccionamiento, y que el tráfico en el piano de usuario se transfiere directamente entre terminales siguiendo el modelo P2P.
- **La provisión de servicios multimedia se lleva a cabo por medio de protocolos del IETF .** Además de SIP/SDP e IPv6, IMS emplea otros protocolos estándar de Internet para la provisión de servicios multimedia, como RTP (Real Time Protocol) y RTCP (Real Time Control Protocol) para el transporte de flujos IP multimedia en el piano de usuario, RSVP (Resource Reservation Protocol) y DiffServ para asegurar la QoS extremo a extremo

CAPITULO 11

Redes Definidas Mediante Software (SDN)

Aunque la idea de redes programables existe desde hace tiempo, no ha sido hasta hace pocos años que se ha empezado a trabajar seriamente con ellas gracias a su gran potencial de innovación.

Las redes definidas mediante software, conocidas mundialmente en inglés como Software-Defined Networking y abreviadas como SDN, son un paradigma de red emergente que da esperanzas para solventar las limitaciones que tienen las actuales infraestructuras de red.

La característica principal de este tipo de redes es que rompen la integración en vertical, separando toda la lógica de control de la red (el plano de control) de los subyacentes routers y switches que retransmiten el tráfico (el plano de datos).

Una vez realizada esta separación, tanto routers como switches pasan a convertirse en simples dispositivos de retransmisión de datos y toda su lógica de control pasa a ser implementada dentro un controlador lógicamente centralizado.

La separación entre el plano de datos y de control se consigue por medio de una interfaz de programación de aplicaciones (API) que permite a los controladores SDN ejercer control directo sobre los elementos del planos de datos.

El ejemplo más conocido de éste tipo de API es OpenFlow. Los switch que trabajan con OpenFlow tienen una o más tablas, conocidas como flow tables, donde se definen todas las reglas de encaminamiento del dispositivo. Cada una de estas reglas define por un lado a un subconjunto del tráfico y por el otro establece las acciones que deben aplicarse a éste (drop, forward, modify, etc).

Esta separación del plano de control, permite a los administradores de red, aplicar políticas dinámicas desde una perspectiva más alejada y global, y sin la complicación de tener que configurar cada dispositivo de red de forma individual, sino que es el propio controlador quien se encarga de instalar las reglas necesarias en cada uno de éstos de forma automática y dinámica. Se acelera también la capacidad de innovación, ya que el control lógico no está atado al hardware, y aumenta la flexibilidad de la red, dado que permite introducir nuevos servicios más fácilmente.

Redes Definidas por Software (SDN)

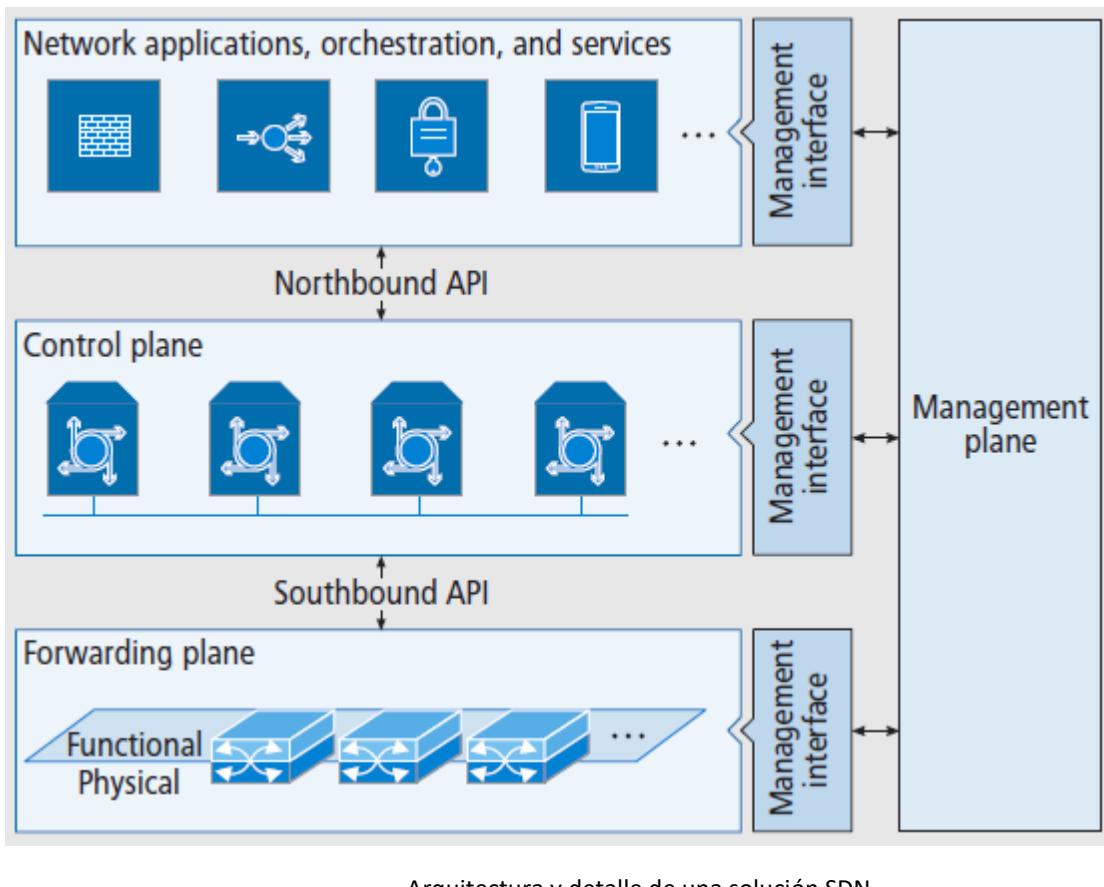
Las redes SDN virtualizan la infraestructura de red, separando el plano de control del plano de distribución o forwarding. Esto favorece una arquitectura centralizada: dinámica, automatizada, y rentable. Esta nueva arquitectura, surge para cubrir los requerimientos del plano de control implementándolo a través de software.

En las redes de datos se cuenta con dos recursos: el plano de control que utiliza información de la señalización para tomar decisiones de control, mientras el plano de datos está encargado de la transmisión de datos a los usuarios.

Cómo funciona SDN?

Las redes definidas por software tienen definido un plano de control centralizado a través de un controlador que dispone de recursos para gestionar las interfaces físicas a través del API Southbound y protocolos como OpenFlow, que permiten separar el plano de control del plano del plano de forwarding,

o distribución. A nivel de aplicación el plano de control se comunica a través de un API Northbound que mejora la administración de los datos, como aparece en la figura.



El ONF aclara que la arquitectura SDN está compuesta por tres diferentes capas accesibles a través de API.

- The Application Layer (Network Applications, Orchestration and Services): en esta capa, se encuentran las aplicaciones del usuario final, las cuales reciben e interactúan con el negocio; en la capa de aplicación están los servicios.
- The Control Layer: proporciona el control lógico centralizado, con la función de supervisar el reenvío de paquetes a través de una interfaz activa.
- The Infrastructure Layer: lo componen los elementos de la red y los dispositivos que proporcionan la commutación y reenvío de paquetes [5].

La comunicación entre las capas se realiza a través de los recursos proporcionados por las API, a nivel superior entre el control y la aplicación interviene el API Northbound; y para comunicar el control con el forwarding (distribución) se utiliza el API Southbound [7].

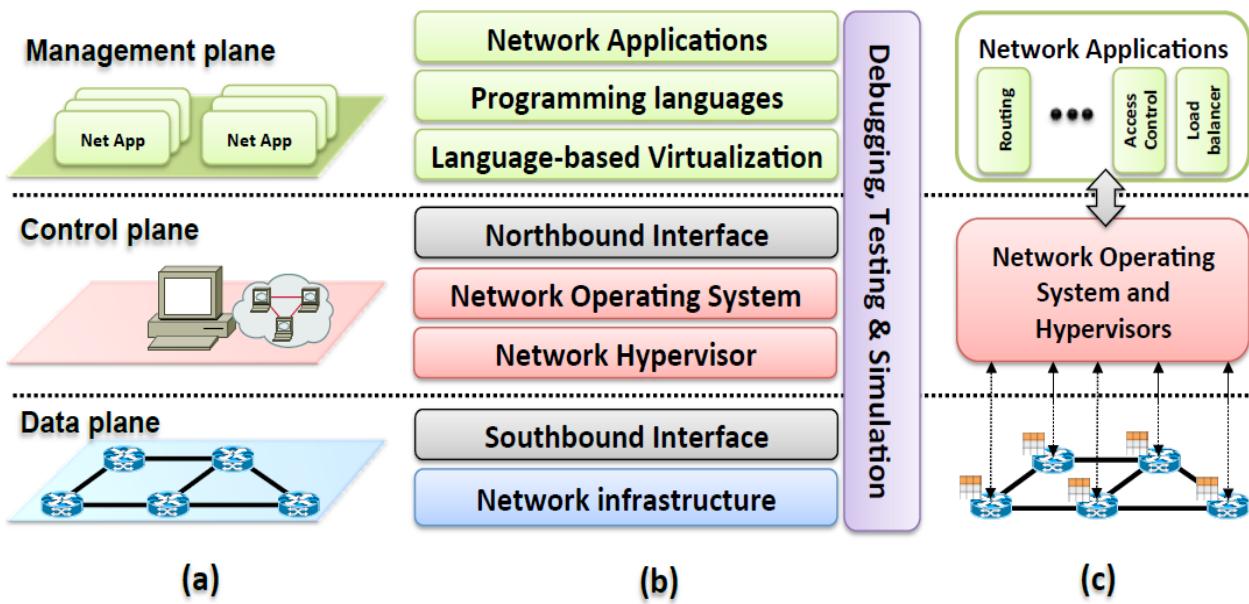
Arquitectura SDN

La arquitectura de las redes definidas mediante software se caracteriza por la división entre el plano de datos y el de control. Esto implica tener tecnologías distintas en cada plano, ya que en el de datos tendremos tecnologías propias de las telecomunicaciones y el ámbito de redes, mientras que en el plano

de control, tendremos tecnologías propias de los sistemas de software, que nos permiten gestionar dinámicamente la información con la que se trabaja.

Adicionalmente, aparece un tercer plano, el de gestión, que se encuentra por encima del plano de control y que tiene un ámbito de actuación mucho más abstracto. El objetivo principal del plano de gestión es el de informar al plano de control de eventos que suceden ajenos a lo que ocurre dentro de la red en ese momento; por ejemplo advertir a un controlador de la presencia de servidores web infectados para que luego el controlador se encargue de realizar las acciones pertinentes como podría ser aislar esos servidores.

En cada uno de los tres planos se identifican diferentes capas en función del tipo de tareas que realizan, tal y como se muestra en la figura. A continuación se explican en profundidad cada uno de los planos.



Arquitectura de las SDN vista por (a) planos, (b) capas y (c) diseño del sistema.

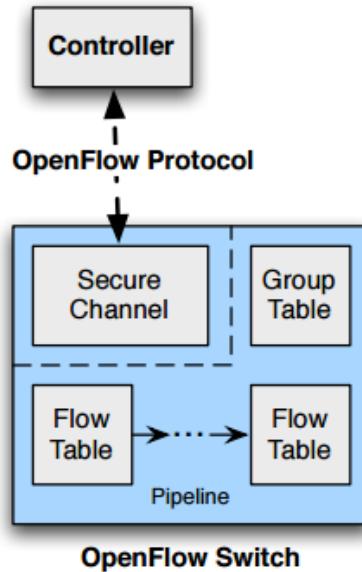
Plano de datos

El plano de datos es el plano de más bajo nivel, pegado a los dispositivos y encargado del envío y transmisión de paquetes.

Comúnmente la infraestructura de este plano está compuesta por routers, switches y middleboxes (como firewalls o balanceadores de carga), pero en las redes SDN todos ellos se reducen a simples dispositivos de transmisión de paquetes.

Toda la lógica operacional es removida y centralizada en dispositivos de más alto nivel con los que este plano mantendrá una comunicación persistente.

Una vez eliminada la lógica de los dispositivos, se precisa de algún tipo de interfaz que permita a entidades externas gestionar su comportamiento. Para ello OpenFlow introduce las Flow Tables y Group Tables, que consisten en una serie de tablas de enrutamiento que contemplan diferentes acciones, juntamente con un protocolo propio de red para comunicarse con el controlador correspondiente.



En un switch OpenFlow hay varias *flow tables*, formadas por un conjunto de entradas llamadas *flow entries*. Cada entrada (o fila) de la tabla contiene tres campos (o columnas) como se muestra en la FIGURA

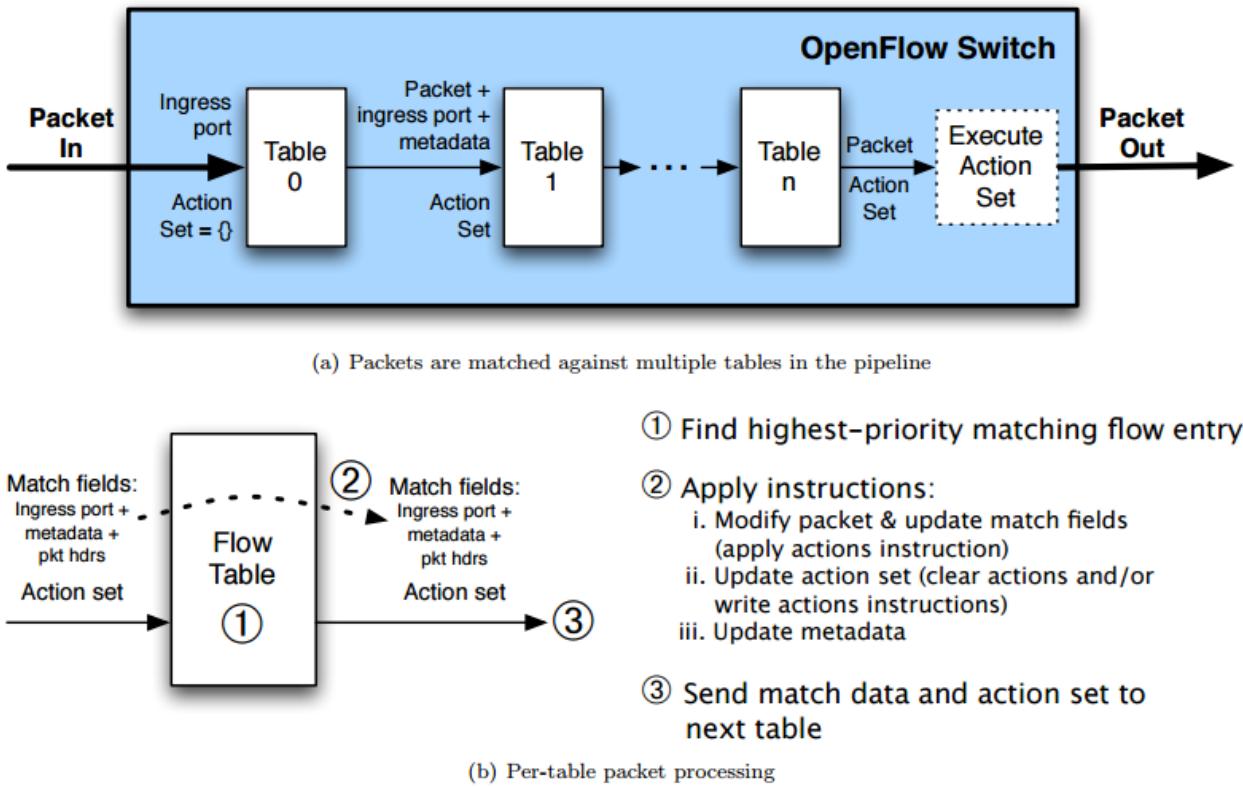
Rule (match fields)	Action (instructions)	Stats (counters)									
		Packet + byte counters									
		1. Forward packets to port(s). 2. Encapsulate and forward to controller. 3. Drop packet. 4. Send to normal processing pipeline.									
Switch Port	VLAN ID	VLAN pcp	MAC src	MAC dst	Eth type	IP Src	IP Dst	IP ToS	IP Prot	L4 sport	L4 dport

Campos de cada entrada de una flow table

1. **Match fields:** donde encontramos los campos que deben encajar. Consiste en el puerto de entrada juntamente con las cabeceras del paquete al que le queremos aplicar una acción específica.
2. **Instrucciones:** el tipo de acción que queremos aplicar al paquete (drop, modificar algún campo de la cabecera, etc.).
3. **Contadores:** información estadística que se almacena sobre los paquetes que han encajado.

La gestión de las *flow tables* se hace a través de una pipeline entre las diferentes tablas tal y como se muestra en la siguiente figura. Cada tabla está numerada secuencialmente, empezando desde el 0. La

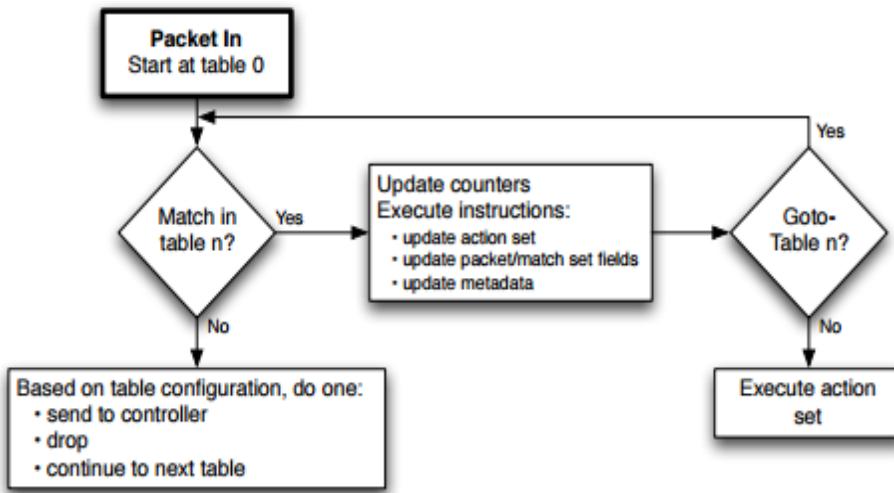
pipeline se procesa empezando desde la primera *flow table*, comprobando si el paquete encaja con alguna entrada de esta tabla y en función del resultado se usan o no el resto de tablas.



Recorrido de un paquete a través de la pipeline de procesamiento de paquetes

El procedimiento estándar de los switches OpenFlow por cada paquete entrante es el siguiente: primero se debe comprobar si existe alguna entrada en las flow tables que encaje con el paquete.

En caso de no existir ninguna entrada que encaje, por lo general existe una regla al final que manda el paquete al controlador para que sea éste quien decida, aunque se podría optar por descartarlo directamente sin ningún problema. En el caso contrario, si el dispositivo encuentra una entrada que encaja con el paquete, le aplicará la acción especificada en el campo de instrucciones. En la próxima figura se puede ver el diagrama de flujo completo con las posibilidades que se ofrecen.



Plano de control

En el plano de control queda centralizada toda la lógica de la red y por tanto es donde se define el comportamiento de la misma. Para ello se usan controladores que procesan los datos, definen las estrategias y toman las decisiones pertinentes.

Es importante remarcar que hablar de control lógicamente centralizado, no significa que exista un único controlador físico encargado de gestionar el comportamiento de la red, ya que éste puede estar perfectamente distribuido.

Existen varios controladores SDN actualmente, algunos de ellos muy focalizados a ofrecer métricas concretas (Tabla 1). Entre los más conocidos se encuentran: **NOX**, escrito en C++ y centrado en ofrecer rendimientos altos; **POX**, escrito en Python y centrado únicamente en el desarrollo rápido de módulos; **Floodlight**, escrito en Java es un controlador muy completo, con soporte para distribuir la lógica en múltiples controladores, integra una API REST en su interface *Northbound* y presenta una muy buena documentación y comunidad, aunque su principal problema es que tiene una curva de aprendizaje muy abrupta; por último, **OpenDaylight** es un controlador muy usado en la industria, escrito en Java, también muy completo y robusto, pero con los mismos problemas de aprendizaje que Floodlight.

Para el presente proyecto se escoge POX porque presenta una curva de aprendizaje rápida, tiene buena documentación y permite desarrollar los módulos muy ágil y rápidamente

	NOX	POX	Floodlight	OpenDaylight
<i>Lenguaje</i>	C++	Python	Java	Java
<i>Rendimiento</i>	Rápido	Lento	Rápido	Rápido
<i>Distribuido</i>	No	No	Si	Si
<i>OpenFlow</i>	1.0 (CPqD: 1.1, 1.2, 1.3)	1.0	1.0	1.0, 1.3
<i>Curva de aprendizaje</i>	Moderada	Fácil	Difícil	Difícil

Tabla 1: Comparación entre los controladores SDN más conocidos

La manera más recomendable de implementar un controlador es mediante módulos programados como objetos. Cada módulo es programado para un propósito concreto, como por ejemplo el aprendizaje de direcciones de nivel 2 o nivel 3, o aplicar el protocolo de *spanning tree*, o protocolos para obtener información de la red. De esta manera, sólo se debe implementar un nuevo módulo, que llame en el orden deseado a los diferentes módulos y gestione su interacción. Las ventajas de este tipo de implementación es que escala muy bien, favorece el reutilización de código y si además permite que puedan adaptarse a la perfección a través de la herencia.

Cada módulo es responsable de hacer cumplir las políticas de red que se le han definido en función de los diferentes inputs que recibe el controlador, así como traducir estas políticas y las decisiones tomadas a reglas en forma de entradas en las *flow tables* de cada switch de la red.

En referencia a los inputs, hay 3 tipos de informaciones conceptualmente diferentes que el controlador debe procesar y que le llegan desde interfaces diferentes. Dividido por interfaces encontramos:

- **Southbound**, es la interfaz de unión entre el plano de datos y el de control, a través de la cual switches y controlador intercambian información. Vía esta interfaz los switches avisan al controlador cuando son puestos en marcha, o cuando llega un paquete que no coincide con ninguna entrada. Y de forma inversa, usando esta interfaz, el controlador puede enviar mensajes a cualquier switch para que añada una entrada a una de sus *flow tables*.
- **Eastbound** y **Westbound**, son interfaces pensadas para comunicar múltiples controladores de un mismo proveedor de red, generalmente para hacer posible la distribución de la lógica del sistema de manera horizontal en múltiples controladores. Estas interfaces son propias y específicas del controlador SDN que se utiliza y no todos los controladores ofrecen soporte para arquitecturas de control distribuidas.
- **Northbound**, permite al controlador comunicarse con el exterior. Esta funcionalidad es especialmente importante y potente en la aplicación de políticas dinámicas de red. Los controladores son ahora los que realizan las tareas de los antiguos firewalls o平衡adores de carga, y éstos no definen su comportamiento en función de eventos de red, sino de gestión. Mediante esta interfaz se pueden habilitar políticas como por ejemplo deshabilitar un servidor conflictivo dinámicamente, o mandar al controlador que aplique una calidad de servicio (QoS) específica para un determinado cliente.

Plano de gestión

Finalmente el plano de gestión, visto como el cerebro de la red, es donde se acumula la mayor parte de la lógica de gestión de la red. Este plano tiene la visión más amplia y general del estado de la red, y cuenta con la posibilidad de intercambiar información con redes vecinas para conocer información relevante de ellas. Debe tenerse en cuenta, además, que en redes existen muchas funcionalidades en las que su gestión está estrechamente relacionada con la gestión de otras redes, como por ejemplo el cómputo de rutas extremo a extremo con el balanceo de carga de la red.

No hay que olvidar que las tareas de gestión de redes implican una carga computacional muy grande, sobre todo cuanto más compleja es la red. En el plano de gestión esto no es un problema, ya que se pueden asignar tanto recursos como sean necesarios.

Tipos de Switch OpenFlow

Un switch híbrido puede conectar el tráfico de OpenFlow con Ethernet a través de los puertos reservados. El hardware del switch OpenFlow puede ser virtualizado, para soportar múltiples instancias de conmutación.

En los switches que sólo hablan OpenFlow se reciben el procesamiento de los paquetes enviados de otros switches OpenFlow; mientras que en los switches híbridos se soporta la operación OpenFlow y de forma normal la conmutación IP.

El Canal OpenFlow

Esta interfaz conecta a cada switch OpenFlow con el controlador; para configurar, administrar el switch, recibir eventos y coordinar los flujos de paquetes.

En la comunicación, se establece un canal OpenFlow; el cual es usualmente encriptado utilizando Transport Layer Security (TLS) aunque corre directamente sobre TCP/IP. Si falla la conexión, es detectada por los valores TCP y se aplican los tiempos de espera de la sesión TLS.

El puerto de transporte para comunicarse en OpenFlow 1.0 es el #6633; mientras en la versión 1.3 utiliza el puerto 6653. Esta comunicación en OpenFlow inicia la negociación con la versión más alta, y en su defecto toma la más baja.

Encripción TLS

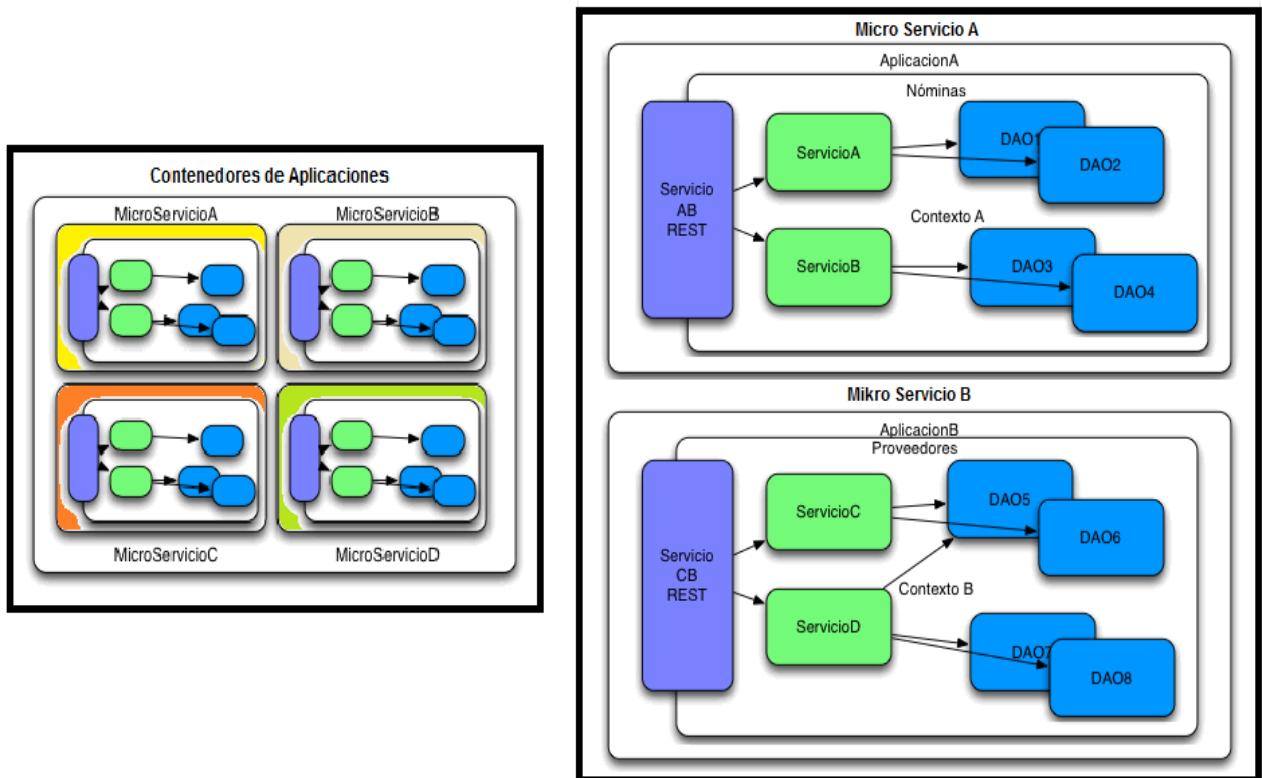
Transport Layer Security es el modo seguro por defecto en OpenFlow, para el cual la versión 1.2 de TLS o superior, proporciona autenticación y cifrado de la conexión para que se conecte el switch con el controlador por el puerto 6633; quedando el controlador en modo escucha del puerto predeterminado.

Otra alternativa es utilizar TCP plano, e implementar un túnel IPSec o VPN para definir una red física separada sin conexiones URI y TCP válidos, entre otras medidas para mantener la privacidad e integridad del controlador, evitando su suplantación u otros tipos de ataques al canal OpenFlow

Para hablar de los componentes de OpenDayLight es necesario contextualizar cómo funcionan y qué son los micro-servicios. En todos los desarrollos de software hay una capa de servicios, soportada por otros recursos de apoyo. Generalmente los servicios se agrupan compartiendo el mismo contexto, después pueden aislarse mejorando su funcionalidad la cual es publicada a través de REST.(Representación del estado de transferencia) .

Al estar REST publicando los servicios, se convierten en aplicaciones independientes, con lo cual se aíslan en un contenedor independiente, que separa esta aplicación de las otras.

Con esta arquitectura se consigue facilitar el despliegue de aplicaciones, que se reducen a micro-servicios, los cuales son alcanzables desde todo tipo de dispositivos ya que es publicado vía REST, como aparece en la figura.

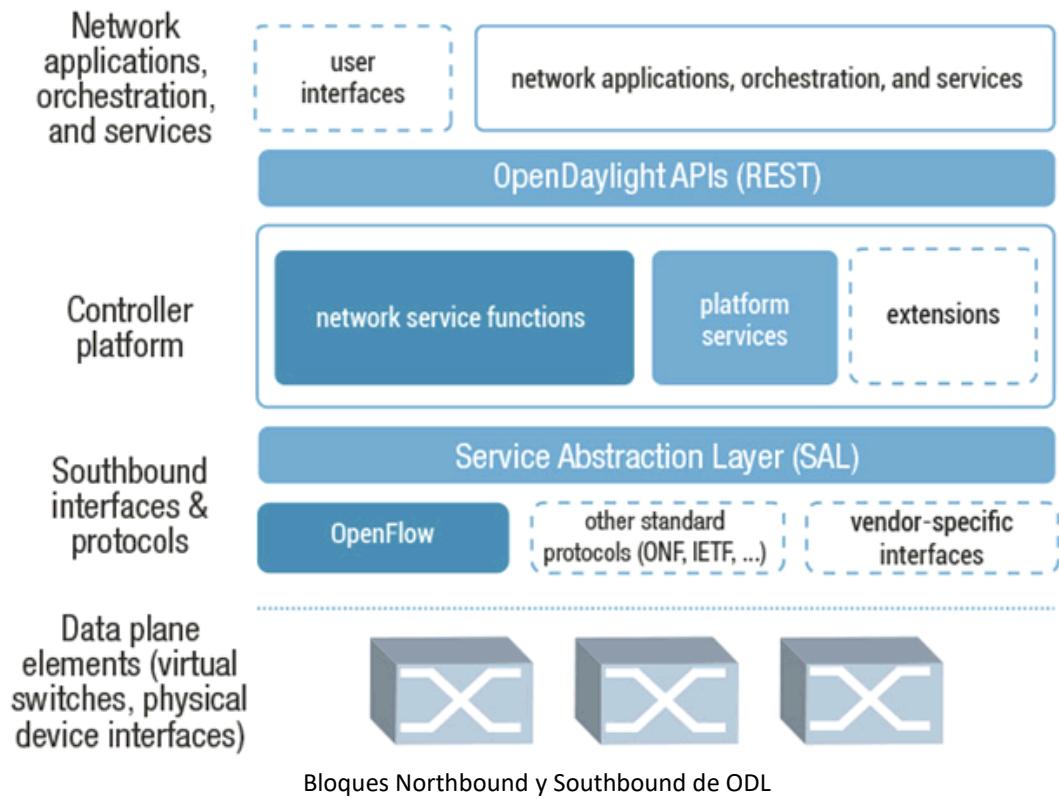


Jerarquía: contenedor, micro-servicio, aplicación, servicio, grupo de servicios, aplicaciones y recursos comunes.

El Controlador SDN OpenDayLight

El controlador de red SDN ODL es una plataforma modular que reutiliza servicios e interfaces comunes para construir y ejecutar aplicaciones, aprovechando las funcionalidades de otros paquetes, exportando servicios a través de interfaces Java. Muchos de estos servicios funcionan bajo el modelo proveedor-consumidor a través de una capa de adaptación llamada MD-SAL.

Desde allí MD-SAL (la capa de abstracción del servicio) interactúa a nivel superior con el API REST, que conecta directamente el control con la capa de aplicación a través del API Northbound, y de igual forma comunica el control con la capa de Forwarding a través de MD-SAL, junto con el API Southbound y protocolos como OpenFlow como aparece en la figura.

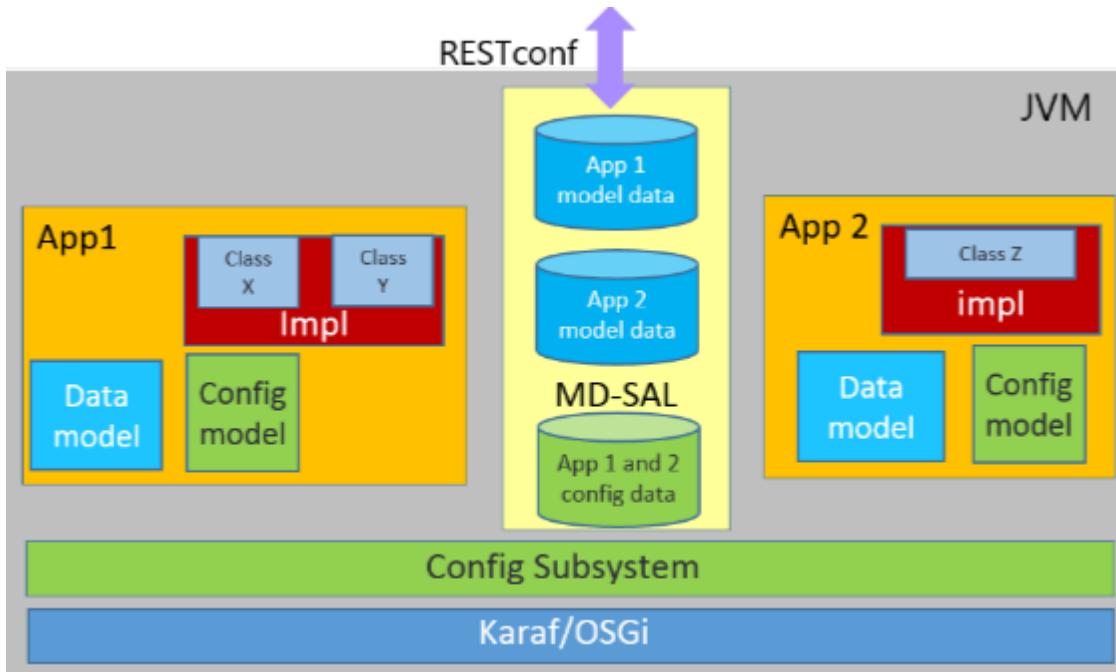


OpenDayLight utiliza a Maven POM.xml (Project Object Model), una herramienta de Java, para poder generar dependencias entre otros módulos y componentes externos. Maven está construido con una arquitectura basada en plugins que permite utilizar cualquier aplicación a través de una entrada estándar

Módulos de OpenDayLight

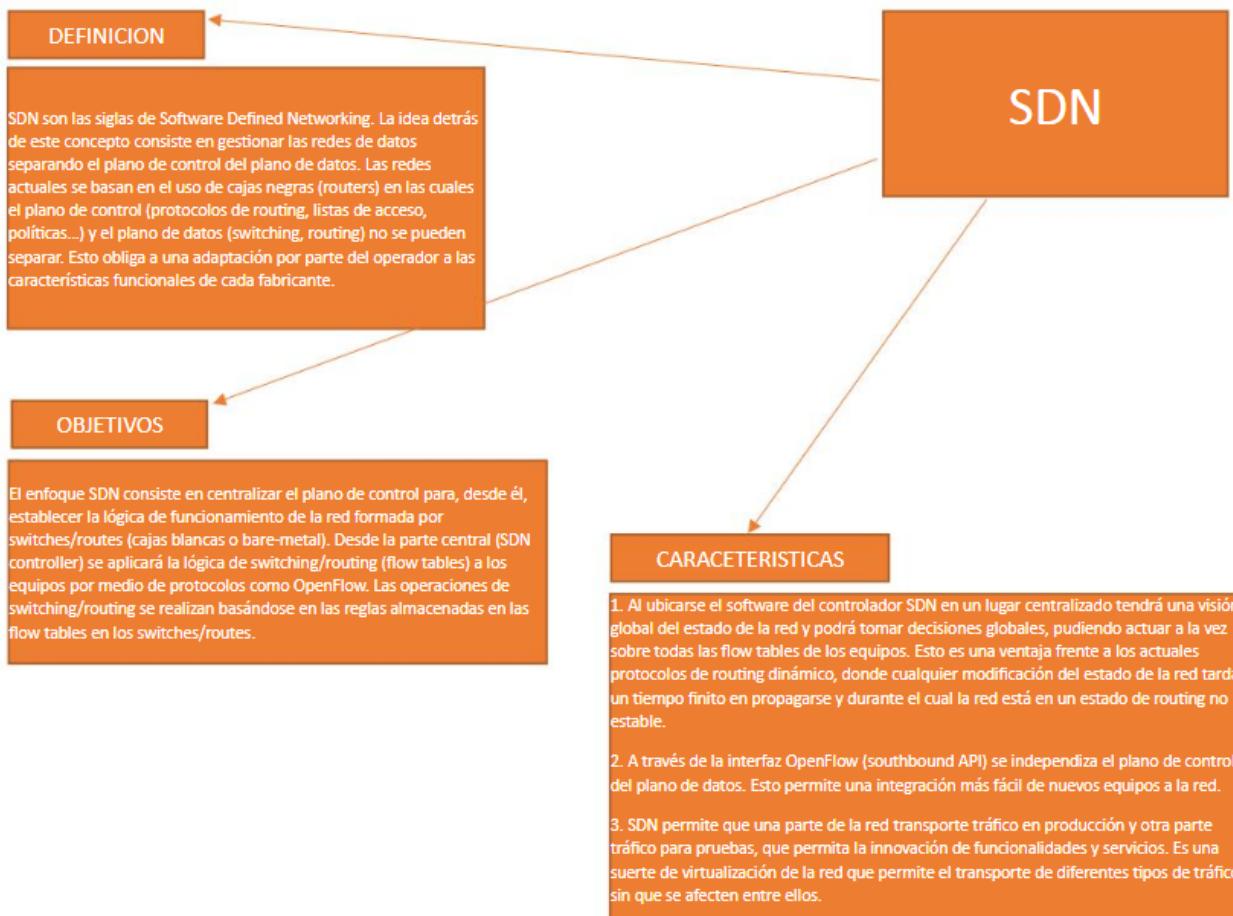
ODL es una plataforma en la cual sus módulos reutilizan servicios e interfaces comunes a través de Java. Muchos de estos servicios están construidos en un modelo proveedor-consumidor, a través de la capa de adaptación de servicio MD-SAL, que reúne las funcionalidades de muchas aplicaciones, las cuales prestan sus servicios, para que desarrolle las tareas del controlador SDN.

El core de la plataforma es una librería de almacenamiento que conserva dos grupos: los datos de configuración (que mantienen el estado de la red deseada) y los datos de funcionamiento (que representan el estado real de la red sobre la base de datos de los elementos de red gestionados). De esta forma, todas las llamadas generadas por eventos y datos van de “Proveedor” a un “Consumidor” a través de este almacén utilizando la lógica de MD-SAL



Un usuario puede publicar datos a través de MD-SAL o REST, almacenando los objetos individuales con la jerarquía padre-hijo, los cuales son accesibles a través de la instancia Yang. Para este fin OpenFlow 1.1 los conecta como protocolo que se guarda en el almacén de datos. Accediendo a los detalles del nodo conector, a través del identificador de nodo mediante Yang o utilizando la URL de la configuración del flujo de datos a través de Rest-Conf, se puede consultar, crear o modificar los flujos a partir de nuevas tablas de flujo

Mapa Conceptual



ANEXOS DE CONFIGURACION

10 comandos a configurar en un dispositivo nuevo

Dependiendo de las implementaciones y del mismo Administrador, siempre hay una lista de cosas que "siempre hay que hacer": claves, nombres de dispositivos... etc. Esta es una lista posible de "10 cosas que siempre hay que configurar" en los dispositivos de una red:

1. Configurar cuentas de acceso a los dispositivos.
2. Configurar un hostname que lo identifique.
3. Configurar una clave de acceso al modo privilegiado.
4. Encriptar las claves.
5. Deshabilitar el acceso vía http.
6. Configurar un servicio de traducción de nombres.
7. Configurar commandos alias.
8. Configurar el reloj de los dispositivos.
9. Evitar que los mensajes logging molesten durante las tareas de configuración.
10. Configurar el servicio de logs.

Configuración de cuentas de acceso a los dispositivos

Router(config)#username [usuario] secret [clave]

Luego de configurado usuario y clave, es necesario aplicarlo a cada una de las líneas de acceso:

Router(config)#line con 0

Router(config-line)#login local

Router(config)#line aux 0

Router(config-line)#login local

Router(config)# line vty 0 4

Router(config-line)# login local

Configurar un hostname

Router(config)#hostname [nombre]

Adicionalmente, Cisco IOS permite configurar un nombre de dominio de modo que el dispositivo "conozca" en qué dominio DNS se encuentra:

Router(config)#ip domain name [dominio]

Configurar una clave de acceso al modo privilegiado

Router(config)#enable secret [clave]

No todas las claves configuradas en dispositivos Cisco IOS están encriptadas por defecto Active el servicio de encriptación de claves que ofrece IOS:

Router(config)#service password-encryption

Deshabilitar el acceso vía http

Router(config)#no ip http server

Configurar un servicio de traducción de nombres

Router(config)#no ip domain-lookup

Otra opción, es configurar un servidor DNS real para que el dispositivo pueda hacer las búsquedas que sean necesarias:

Router(config)#ip name-server [IP]

Configurar comandos alias

Router(config)#alias [modo] [abreviado] [comando]

Router(config)#alias exec s show running-config

Configurar el reloj de los dispositivos

En principio este requisito se puede cubrir configurando, además de fecha y hora en el reloj, el uso horario:

Router#clock set [hh]:[mm]:[ss] [mmm] [dd] [aaaa]

Router#configure terminal

Router(config)#clock timezone [huso] [GMT]

En el caso de países o regiones que modifican el uso horario de acuerdo a la estación:

Router(config)#clock summer-time [huso] recurring

Ahora bien, en redes con numerosos dispositivos, es conveniente configurar el acceso a un servidor NTP

Router(config)#ntp server [IP]

Evitar que los mensajes logging molesten

Router(config)#no logging console

El que quizás es el mejor modo (porque nos permite seguir recibiendo estos mensajes de estado, que son de gran importancia), es sincronizar estos mensajes con el ingreso de comandos en el prompt del sistema operativo:

Router(config)#line con 0

```
Router(config-line)#logging synchronous  
Router(config)#line aux 0  
Router(config-line)#logging synchronous  
Router(config)#line vty 0 4  
Router(config-line)#logging synchronous
```

Configurar el servicio de log

```
Router(config)# logging buffered [tamaño]
```