SUPER-PDF

Yo

[NOMBRE DE LA EMPRESA] [Dirección de la compañía]

Contenido

Trabajo Práctico: **BGP** Border Gateway Protocol 10
1. BGP – Border Gateway Protocol 13
1.1 Tipos de puntos de tráfico 13
Tier 1 13
Tier 2 13
Tier 3 13
1.2 Definiciones 14
Ruteo 14
Ruta 14
Tránsito 14
Peering 14
Default 14
Exchange points (IXP) 14
2. Tipos de acuerdo 15
2.1 Acuerdos Bilaterales 15
2.2 Acuerdos Multilaterales 15
2.3. Tipos de IXP 16
2.3.1 Modelo de capa 3 16
2.3.2 Modelo solo capa 2 16
3. Sistemas Autónomos (AS – Autonomous System) 17
3. 1 Tipos de AS 17
4. IANA - Internet Assigned Numbers Authority 17
5. Redundancia 19
6. Protocolos de ruteo 20
6.1 IGP 20
6.2 EGP 20
7. Características de BGP 21
7.1 Ventajas de BGP 21
7.2 Características del vector distancia 21
7.3 Atributos de BGP 22
7.4 EBGP y IBGP 23
8. Tipos de mensajes BGP 26
8.1 Open Message 27
8.2 Update Message 27
8.3 Notification Message 27
8.4 KeepAlive Message 27
9. Máquina de estado BGP 28
9.1 Idle State 28

9.2 Connect State 28
9.3 Activate State 28
9.4 Open Sent State 29
9.5 Open Confirm 29
9.6 Established State 29
10. Configuración de BGP 30
10.1 Habilitar enrutamiento BGP 31
10.2 Definir los vecinos BGP 31
10.3 Definición de grupo de pares 31
10.4 Asignar vecinos al grupo peer 32
10.5 Deshabilitar un vecino BGP 33
10.6 Problema de la dirección IP de origen IBGP 33
11. Identificar las redes BGP 34
12. Ejemplo de configuración de BGP 36
12.1 Ejemplo sin peer group 37
12.2 Ejemplo de IBGP y EBGP 37
12.3 Verificación y solución de problemas BGP 37
X25 41
RED FRAME RELAY 44
Características de Frame Relay 44
Cómo funciona Frame Relay 44
Rendimiento de Frame Relay 45
Problemas con Frame Relay 46
ATM 47
HISTORIA. 47
INTRODUCCIÓN. 47
MULTIPLEXACIÓN ASÍNCRONA. 48
ESTRUCTURA BÁSICA DE LA CELDA 48
ENCABEZADO DE LA CELDA 49
RUTAS Y CANALES VIRTUALES: 50
NIVELES DE ATM 50
APLICACIONES TÍPICAS 51
Preguntas: 53
¿Que capas del modelo OSI utiliza X25? 53
¿Cual es la maxima cantidad de datos a transferir en X25? 53
Enumere 3 ventajas de X25 53
¿Cuáles son los dos circuitos virtuales de X25? 53
Enumere 3 ventajas de PAD. 53
¿Qué tipos de circuitos presentan las redes ATM? 53

¿Cómo es la estructura de una celda ATM? 53
Mencione tres aplicaciones de ATM. 0
¿Qué ventajas presenta ATM sobre X.25? 0
¿Cómo está formada una red ATM? 0
¿Para qué se utiliza frame relay? 0
¿Cuál es el rango de ancho de banda de frame relay? 0
¿Cuál es el tamaño máximo de paquete? 0
¿En qué capa se encuentra el modelo OSI? 0
¿Qué indica el principio y final de la trama en frame relay? 0
VPN y FDDI 1
FDDI 2
¿Qué es FDDI? 2
Historia de FDDI 2
Generalidades de FDDI 2
Composición de FDDI 2
Trama de Datos de FDDI 4
Tipos de Tráfico de FDDI 5
Especificaciones de FDDI 6
Método de Acceso de FDDI 6
Conclusión de FDDI 7
VPN 7
¿Qué es y cómo funciona una VPN? 7
Historia de la VPN 8
Ventajas de VPN 9
Desventajas de las VPN 10
Tipos de VPN 10
Protocolos de VPN 11
Arquitectura de las VPN 11
Ejemplos de Aplicación 12
Noticias 13
Conclusiones de VPN 13
VOIP +h323 + sip 17
Consigna 17
Desarrollo de la actividad 17
VOIP 17
VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS. 18
VoIP Retardo. 18
CAUSAS DEL DELAY. 18
Jitter 19

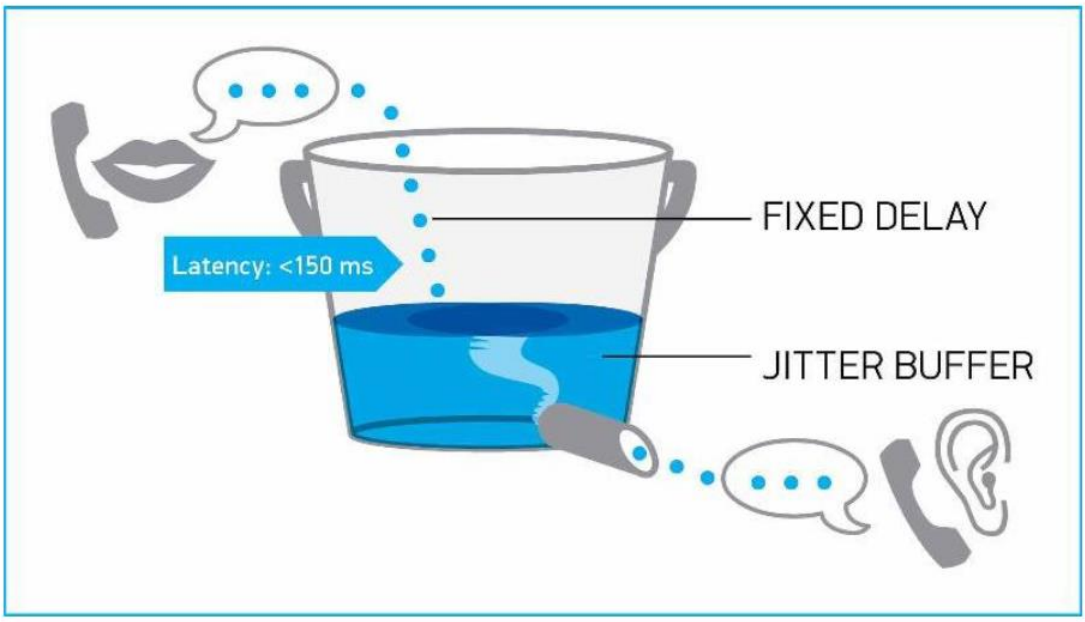


Ilustración 3 Buffer anti jitter

.....19
JITTER: BUFFER ADAPTATIVO.....19
Pérdida de Paquetes.....20
CODIFICACIÓN DE LA VOZ: OTROS ASPECTOS. 20
LATENCIA. 20
PARÁMETROS DE LA VOZ. 21
Calidad de la Voz VSQ. 21
PROTOCOLOS VOIP......22
TRANSPORTE DE INFORMACIÓN EN TELEFONÍA IP. 23
REAL TIME TRANSPORT PROTOCOL 24
PROTOCOLO RTCP (REAL TIME CONTROL PROTOCOL). 26
SEÑALIZACIÓN Y CONTROL DE LLAMADA H.323 y SIP 27
PROTOCOLO DE SEÑALIZACIÓN H.323 28
EL ESTABLECIMIENTO DE LLAMADAS EN H.323.....31
PROTOCOLO DE SEÑALIZACIÓN SIP 32
SERVIDORES DE REDIRECCIÓN. 33
SERVIDORES PROXY. 34
SERVIDORES DE REGISTRO.....34
Redes por software (SDN) y Metro Ethernet.....38
Redes por software 40
¿Que son las redes por software?.....40
¿Como funcionan las SDN?.....40
Openflow 41
Arquitectura.....42
Ventajas de las redes definidas por software.....43

En qué se diferencian las SDN de las redes tradicionales?....44
Aplicaciones y servicios que pueden sacar provecho de las redes definidas por software (SDN) 44
Metro Ethernet: 45
Servicios de Metro Ethernet....46
Beneficios de Metro Ethernet....47
Metro Ethernet en comparación con Frame Relay y ATM 47
Estándares....48
Estándares de Ethernet Sobre Fibra Óptica 49
Trama Ethernet 49
802.Q/P Encabezado de Encapsulación. 50
Prioridad del usuario 51
IEEE 802.1P 51
CFI 51
VID- VLAN ID....51
Ethernet SLA....51
Bandwith profile.....51
Clases de Servicio. 51
Servicios 52
Tecnologías....53
Evolución de Ethernet 53
Parámetros de tráfico....55
PARÁMETROS DE PERFORMANCE 58
Frame delay (Retardo de trama)....58
Frame Jitter 58
Frame loss (Pérdida de trama)....58
Categorías de los servicios....58
Atributos: 59
SERVICIO DE 59
MULTIPLEXACIÓN....59
BUNDLING 60
SECURITY FILTERS 60
Servicios Ofrecidos 60
1 Acceso a Internet dedicado 60
2 Intranet extranet L2 VPN 61
3 Extencion de Lan....61
Preguntas 62
Redes por software 62
METRO 63

MPLS CATV ADSL FTTX 64
ADSL 66
Características: 66
Modulación en ADSL 67
Ventajas ADSL 67
CATV 69
¿Qué es CATV? 69
Redes modernas 69
Cable Modem 70
FTTX 71
FTTH - Fiber-to-the-home 71
FTTO - Fiber-to-the-office 71
FTTB - Fiber-to-the-basement 71
FTTP - Fiber-to-the-premises 71
FTTN - Fiber-to-the-node 71
FTTA - Fiber-to-the-antenna 72
Tecnología FTTx 72
Diseño y planificación de redes 72
¿FTTH (fibra óptica hasta la casa) O HFC (híbrido de fibra coaxial)? 72
Ventajas de FTTH 72
Ventajas de HFC 72
Instalación 72
Transmisión **de** datos 73
Velocidad 73
Ancho de banda 73
Precio 73
MPLS 74
¿Qué es? 74
¿Cómo funciona una red MPLS? 74
Partes importantes en MPLS 75
La etiqueta: 75
Bits experimentales 75
Parte inferior de la pila: 75
Tiempo de vida 75
Beneficios de una red MPLS 75
- Mayor rendimiento en la interconexión de sedes 75
- Optimiza el presupuesto 75
- Es adaptable a cualquier empresa 76
- Mejor experiencia de usuario 76

Conclusión 76
Preguntas 76
Wifi, Wimax y Telefonía Móvil 78
WIFI 79
Tipos de Wifi 80
Estándares que certifica la Alianza Wi-Fi 80
Dispositivos 81
Tipos de seguridad en conexiones WiFi 81
Ventajas e inconvenientes redes WiFi 82
WIMAX 83
Características 84
Tipos de WiMax 85
Dispositivos y funcionamiento WiMax 85
Estándares WIMAX 86
Ventajas tecnología Wimax 87
Desventajas tecnología Wimax 87
Diferencias entre WiFi y WiMax 87
GSM 88
Objetivos 88
Tipos de Servicios 89
Radios de frecuencia 89
Codificación de la voz 89
Celdas GSM 89
Arquitectura 90
Roaming 90
GPRS 91
¿Por qué el GPRS trajo tantos cambios? 91
Importantes mejoras 92
Características de GPRS 92
Diferencias entre GSM y GPRS 93
Ventajas 93
Desventajas 93
UMTS 95
Cómo funciona la red 3G 95
Ventajas y desventajas de la red 3G 96
4G LTE 97
Ventajas y desventajas de la tecnología móvil 4G 98
Ventajas 98
Desventajas 98

4G EN ARGENTINA 98
Bibliografía..... 101
Preguntas y Respuestas..... 102

UNIVERSIDAD ABIERTA INTERAMERICANA

FACULTAD DE TECNOLOGÍA INFORMÁTICA

CARRERA: **Ingeniería en Sistemas Informáticos**

ALUMNO: **Acosta, Agustin; Destito, Juan; Lastra, Julián; Morales, Juan**

MATERIA: **Redes Administrativas**

Trabajo Práctico: BGP Border Gateway Protocol

DOCENTE: **Milio, Claudio**

AÑO: **2022**

Contents

1. BGP – Border Gateway Protocol 13
1.1 Tipos de puntos de tráfico 13
Tier 1 13
Tier 2 13
Tier 3 13
1.2 Definiciones 14
Ruteo 14
Ruta 14
Tránsito 14
Peering 14
Default 14
Exchange points (IXP) 14
2. Tipos de acuerdo 15
2.1 Acuerdos Bilaterales 15
2.2 Acuerdos Multilaterales 15
2.3. Tipos de IXP 16
2.3.1 Modelo de capa 3 16
2.3.2 Modelo solo capa 2 16
3. Sistemas Autónomos (AS – Autonomous System) 17
3. 1 Tipos de AS 17
4. IANA - Internet Assigned Numbers Authority 17
5. Redundancia 19
6. Protocolos de ruteo 20
6.1 IGP 20
6.2 EGP 20
7. Características de BGP 21
7.1 Ventajas de BGP 21
7.2 Características del vector distancia 21
7.3 Atributos de BGP 22
7.4 EBGP y IBGP 23
8. Tipos de mensajes BGP 26
8.1 Open Message 27
8.2 Update Message 27
8.3 Notification Message 27
8.4 KeepAlive Message 27
9. Máquina de estado BGP 28
9.1 Idle State 28
9.2 Connect State 28

9.3 Activate State 28
9.4 Open Sent State 29
9.5 Open Confirm 29
9.6 Established State 29
10. Configuración de BGP 30
10.1 Habilitar enrutamiento BGP 31
10.2 Definir los vecinos BGP 31
10.3 Definición de grupo de pares 31
10.4 Asignar vecinos al grupo peer 32
10.5 Deshabilitar un vecino BGP 33
10.6 Problema de la dirección IP de origen IBGP 33
11. Identificar las redes BGP 34
12. Ejemplo de configuración de BGP 36
12.1 Ejemplo sin peer group 37
12.2 Ejemplo de IBGP y EBGP 37
12.3 Verificación y solución de problemas BGP 37

1. BGP – Border Gateway Protocol

Border Gateway Protocol (BGP) es un protocolo de enrutamiento usado para intercambiar información de enrutamiento entre diferentes redes. Este realiza el intercambio de información con los routers de dominio.

¿Qué es lo que debe de soportar un protocolo de enrutamiento de internet?

Debe poder:

- Trabajar con topologías complejas
- Contar con políticas de ruteo complejas para soportar políticas administrativas de cada ISP
- Escalar anuncios a cientos de miles de rutas.
- Intercambio confiable de información
- Poseer escalabilidad
- Poseer estabilidad
- Poseer capacidad de adaptación a los cambios
- Poseer capacidad de convergencia
- Contar con un tráfico de Control inmanejable
- Necesidad de políticas de enrutamiento

BGPv4 cumple con los requisitos mencionados.

La topología de internet cuenta con un esquema de proveedores de servicios (ISP) de distintos niveles (tiers).

Estos ISPs pueden ser locales, regionales o globales.

La topología de internet es cada vez más semejable a lo que es un grafo. Esta tiene unos requerimientos de tránsito más complejos debido a que cada vez hay más dispositivos que se conectan a internet.

1.1 Tipos de puntos de tráfico

Existen diferentes tipos de puntos de tráfico. Contamos con los niveles de tier 1, 2 y 3.

Tier 1

Tienen redes que pueden alcanzar otras redes sin comprar tráfico IP.

Tienen tránsito libre para peering con otras redes Tier1.

Hay aproximadamente 14 en el mundo.

Tier 2

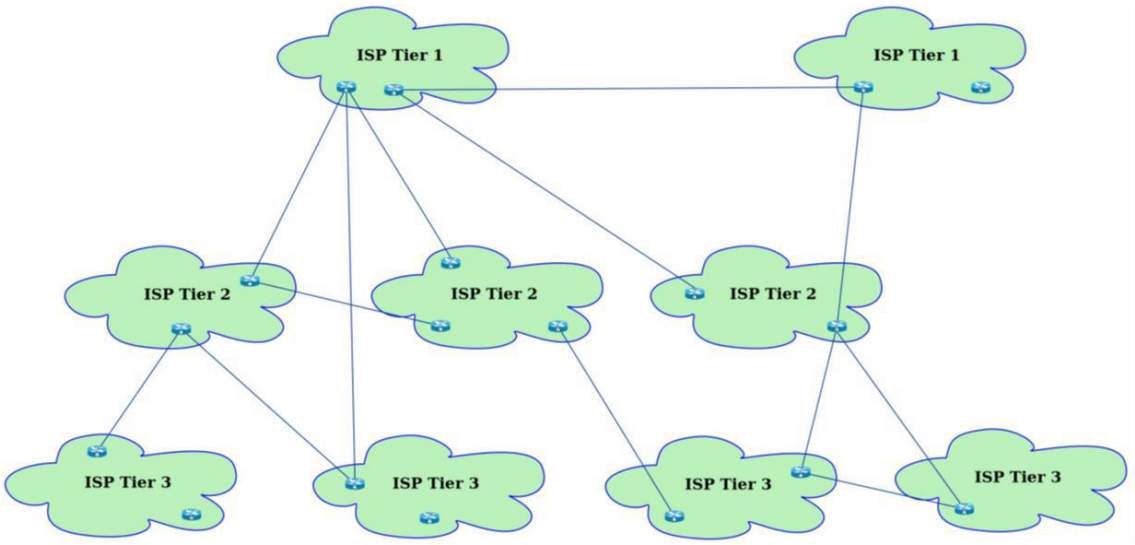
Tienen redes de peering las cuales necesitan comprar tráfico para alcanzar otras redes en internet.

Tier 3

Estos únicamente compran tránsito a otras redes.

Entre ellos existen grandes volúmenes de intercambios de tabla de BGP, los cuales son más de 500.000 rutas.

En el siguiente gráfico se puede visualizar los diferentes tier de los ISP y la topología que estos forman.



1.2 Definiciones

Ruteo

Es el proceso que se ejecuta en un equipo de computación el cual analiza los posibles destinos a los cuales puede dirigirse un paquete de datos.

Estos destinos forman las llamadas rutas.

Ruta

Una ruta permite que un paquete de datos pueda viajar desde un origen a un destino. Este paquete toma un camino determinado para poder alcanzar el destino, pasando por uno o más puntos intermedios hasta llegar.

Tránsito

Transmisión de tráfico a través de una red, la cual regularmente tiene un costo

Peering

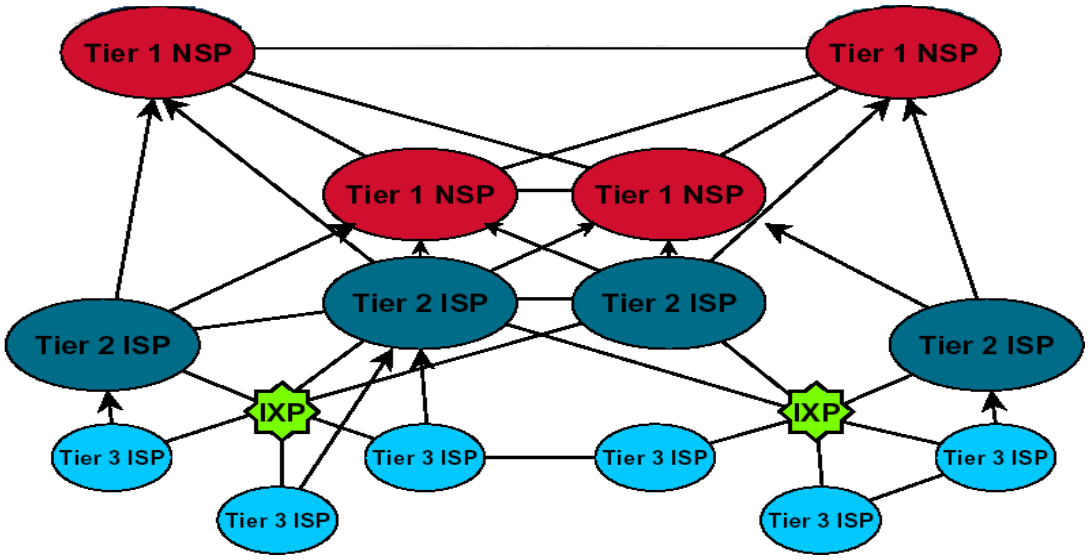
Es el intercambio de información de enrutamiento y tráfico

Default

Hacia dónde enviar el tráfico cuando no existe una ruta específica en la tabla de enrutamiento por un costo

Exchange points (IXP)

Punto en común donde varios sistemas autónomos intercambia información de ruteo y tráfico



2. Tipos de acuerdo

Existen dos tipos de acuerdo:

2.1 Acuerdos Bilaterales

Cada proveedor establece la relación que necesite con otros proveedores en el IXP

Los enrutadores de borde los ISP establecen sesiones de BGP con los enrutadores de borde de otros proveedores

2.2 Acuerdos Multilaterales

Cada proveedor establece sesiones con el concentrador

Los enrutadores de borde de los ISP tienen como vecino al IXP

2.3. Tipos de IXP

Los diferentes tipos son los siguientes:

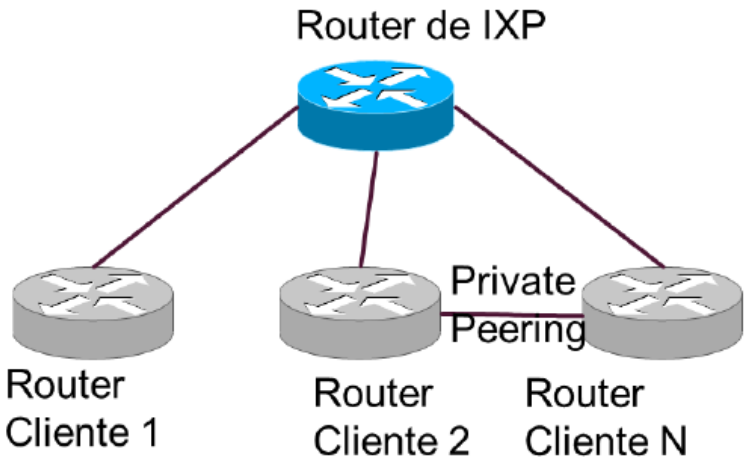
Modelo de capa 3, modelo de solo capa 2, y modelo capa 2 + route server

2.3.1 Modelo de capa 3

El router de IXP hace sesiones de BGP con cada uno de los participantes

Los participantes pueden también interconectarse, pero no a través del router del IXP

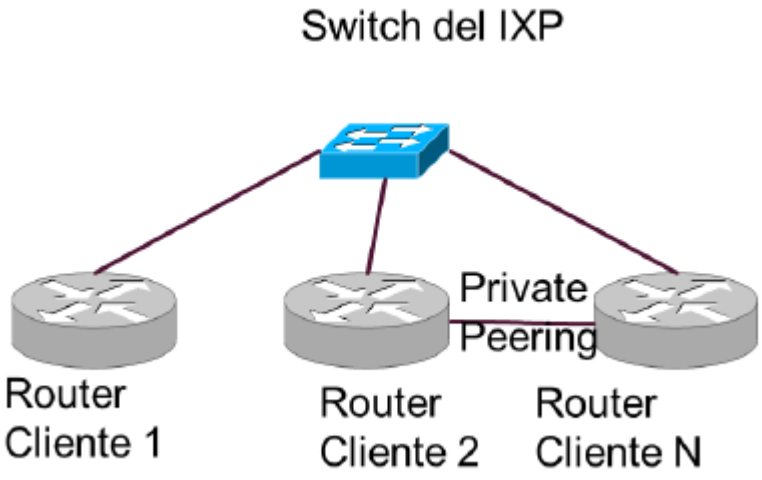
En la siguiente imagen se muestra un modelo de capa 3



2.3.2 Modelo solo capa 2

Cada participante hace sesiones de BGP con cada uno de los participantes

Los participantes pueden también interconectarse a través del IXP o no



3. Sistemas Autónomos (AS – Autonomous System)

Un sistema autónomo es un conjunto de redes IP administradas en las que se utiliza una misma política de enrutamiento, con un mismo protocolo de enrutamiento

Cada sistema autónomo está identificado por un único número entero de 32 bits, conocido como número de sistema autónomo (ASN)

Un AS normalmente pertenece a una organización, se pueden utilizar uno o varios IGP (Interior Gateway Protocol) en cada AS

Cada AS es visto por el resto del mundo como una sola entidad

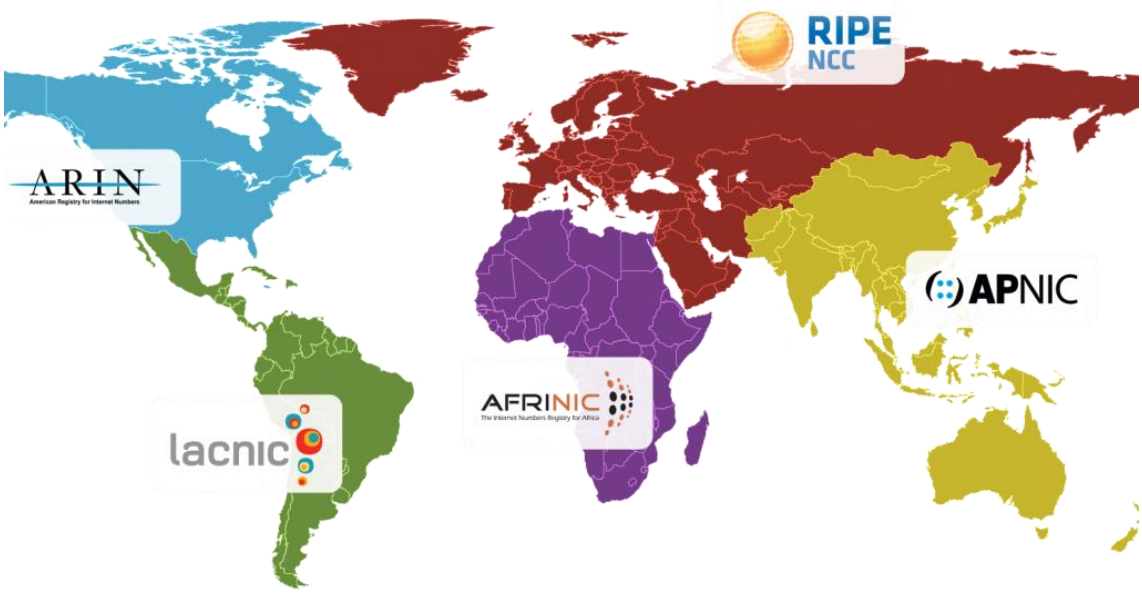
Cuando un AS se conecta a internet utilizando un EGP (External Gateway Protocol) como BGP, se le debe asignar un único número de AS el cual es administrado por el Internet Assigned Numbers Authority (IANA)

3. 1 Tipos de AS

- Stub: Tiene conexión con un solo AS, y solo transporta tráfico con fuente o destino en el AS (tráfico local)
- Transit: Tiene conexión con más de 1 AS y transporta trafico que pasa a través del AS, no es fuente o destino (tráfico de tránsito)
- Multihomed: Tiene conexión con más de 1 AS, pero no transporta tráfico de tránsito.

4. IANA - Internet Assigned Numbers Authority

La IANA se encarga de asignar los números de AS a través de cinco Registros Regionales de Internet (RIR – Regional Internet Register)



Los números AS pueden estar entre 1 y 65.535, los RIRs administran los números de AS entre 1 y 64.512.

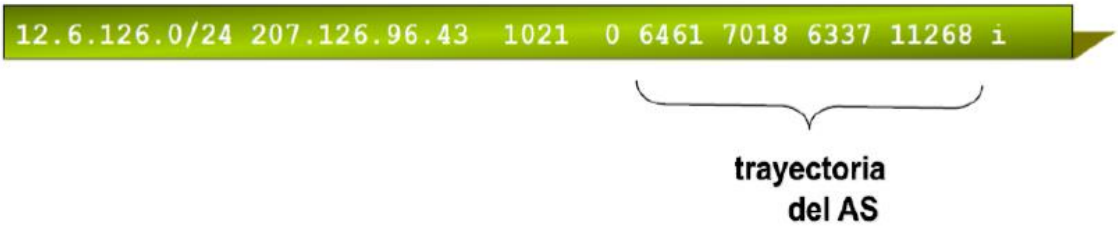
Los números 64.515 hasta 65.535 están reservados para uso privado.

La IANA hace cumplir una política para que las organizaciones que se conectan a un único proveedor utilicen un número de AS del Pool privado.

Con el lanzamiento del RFC 4893 y RFC 5398 se extendieron los campos de dos octetos (16 bits) a campos de cuatro octetos (32 bits), aumentando el tamaño del conjunto de 65.536 a 4.294.967.296 valores disponibles.

Los Internal Routing Protocols anuncian una lista de las redes y las métricas para llegar a cada red. Mientras que los Routers BGP intercambian información de accesibilidad, llamados **path vectors**, formada por **path atributes**.

Entre la información de los path vectors se incluye una lista de la ruta completa de BGP con la cantidad de AS necesarios para llegar a una red de destino, como así también incluyen la dirección IP para llegar al siguiente AS y cuál fue el origen del recorrido



5. Redundancia

La redundancia se puede lograr mediante la implementación de enlaces redundantes, la implementación de dispositivos redundantes, y el uso de componentes redundantes en un router.

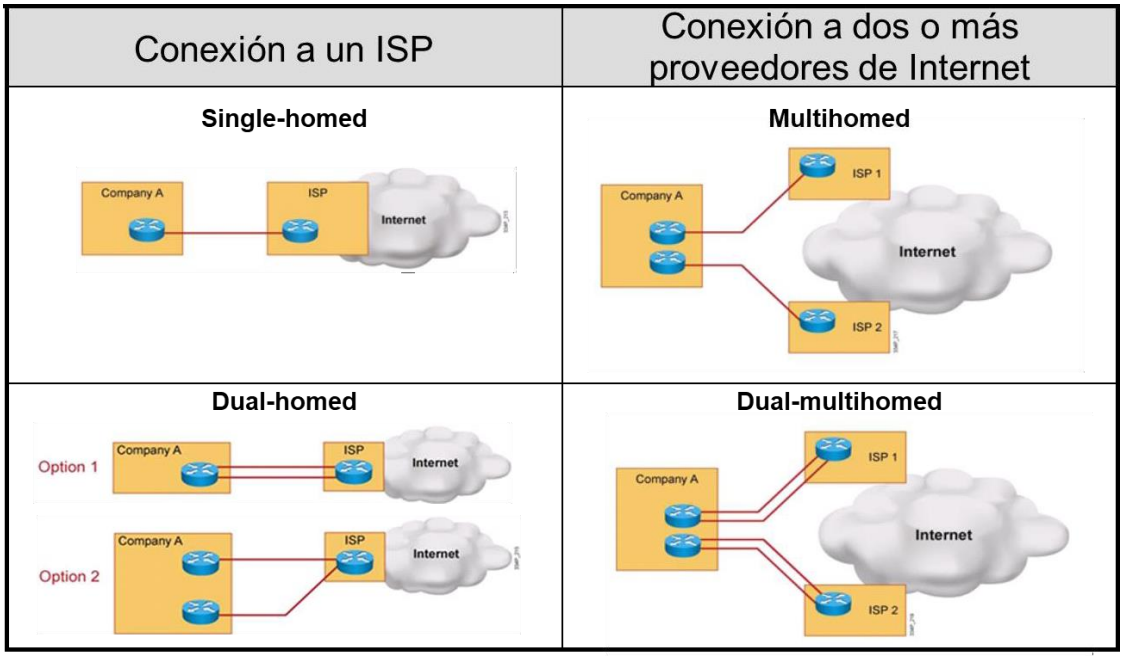
La conexión del ISP también puede ser redundante.

Cuando un cliente se conecta a un solo ISP la conexión se conoce como single-homed o dual-homed. Si la red ISP falla, la conectividad a Internet se interrumpe.

En cambio, cuando un cliente está conectado a múltiples ISPs la conexión se denomina multihomed o dual-multihomed.

Con conexiones a múltiples ISPs, la redundancia se construye en el diseño.

Con una conexión a un solo ISP, la redundancia se puede lograr si dos enlaces hacia el mismo ISP se utilizan eficazmente. Esto se llama ser base dual.



6. Protocolos de ruteo

PROTOCOLO	USO	TIPO	JERARQUÍA	MÉTRICA
RIP	Interior	Distance vector	✗	Hop count
OSPF	Interior	Link state	✓	Cost
IS-IS	Interior	Link state	✓	Metric
EIGRP	Interior	Advanced distance vector	✗	Composite
BGP	**Exterior**	**Path vector**	✗	**Patch vectors**

6.1 IGP

IGP - Internal Gateway Protocol

Es un protocolo de ruteo usado para Intercambiar información de rutas DENTRO de un SA

Entre ellos tenemos a los protocolos RIP, EIGRP, OSPF, etc.

6.2 EGP

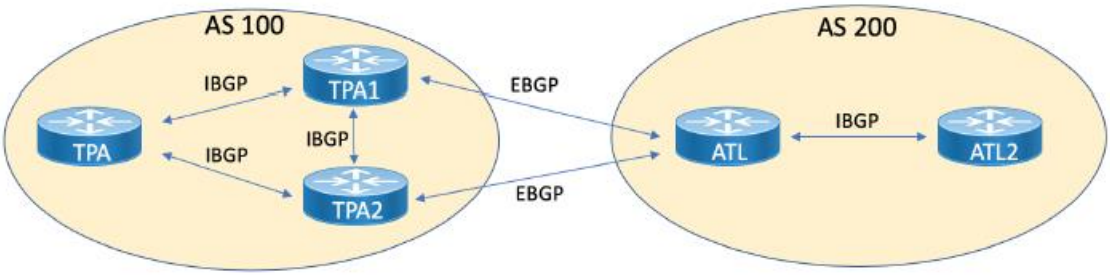
EGP - Exterior Gateway Protocol

Protocolo de ruteo usado para intercambiar información de rutas ENTRE SA

BGP Border Gateway Protocol

Es un protocolo de ruteo externo

La tabla de ruteo mantiene una lista de SA que son atravesados para alcanzar a otros SA



7. Características de BGP

7.1 Ventajas de BGP

- **ESCALABILIDAD**: Diseñado para manejar grandes tablas de rutas (full-routing implica del orden de 400.000 prefijos). Y no requiere excesivo control de tráfico.
- **ESTABILIDAD**: Se adapta a los cambios de manera facil y rápida
- **SENCILLEZ**: Es de la familia de los protocolos de vector distancia (no requiere estructura jerárquica ni conocimiento de la topología de red).

7.2 Características del vector distancia

Usa TCP como protocolo de transporte utilizando el puerto 179

Para que un router sepa hacia donde dirigir un paquete, alguien le tiene que decir por dónde tiene que encaminarlo, es decir, aprende.

De la misma forma, si se quiere que alguien llegue hasta nuestras redes le tenemos que comunicar que están disponibles, es decir, se anuncia.

Un router BGP forma una relación de vecino directa con un número limitado de otros routers BGP. A través de estos vecinos BGP, un router aprender las rutas BGP a través de internet para así poder llegar a cualquier red publicada. Cualquier router que ejecuta BGP se conoce como un speaker BGP

Cada speaker BGP tiene un número limitado de vecinos BGP con los cuales se forma y mantiene una relación entre peers basada en TCP. Estos peers, también conocidos como neighbors BGP, pueden ser internos o externos al AS.

Los vecinos BGP primero establecen una conexión, para el intercambio de todas las rutas candidatas BGP.

Después de este primer intercambio, actualizaciones incrementales se enviarán como cambios en la información de la red.

Las actualizaciones incrementales son más eficientes que actualizaciones completas de tablas.

7.3 Atributos de BGP

BGP utiliza atributos para seleccionar el mejor camino. Podemos decir que los atributos son la métrica de BGP.

Las variables describen características o atributos del camino al destino.

Los atributos se dividen dos categorías, según la importancia de la información transportada en los mensajes.

▪ **Well-known**: Atributos cuya utilización es obligatoria

▪ **Optional**: Atributos opcionales.

Estas categorías se dividen permitiendo así una mayor granularidad.

Los atributos Well-known se dividen en:

▪ **Mandatory**: Estos atributos son requeridos y deben ser reconocidos por todas las implementaciones de BGP.

▪ **Discretionary**: Estos atributos no son requeridos, pero en el caso de estar presentes todos los routers que ejecuten BGP tiene que reconocerlos y actuar en la información que contienen.

Los atributos opcionales se dividen en:

▪ **Transitive**: El router no debe de reconocer estos atributos, pero si este es el caso, marcará la actualización como parcial y enviará la actualización completa con los atributos, al siguiente router. Los atributos atraviesan el router sin ser cambiados, si no son reconocidos.

▪ **Nontransitive**: Estos atributos son eliminados si caen en un router que no entiende o reconoce los atributos. Estos atributos no serán propagados al peer BGP.

Los atributos se envían en los mensajes de Update usando el formato TLV. El campo Tipo tiene 2 Bytes, conteniendo los Bits:

- Bit Opcional (Optional Bit - Bit 0)

0 - Atributo Well-Known. Debe ser reconocido por todas las implementaciones de BGP

Discrecional (Discretionary) - Pueden no estar en una ruta en particular

Obligatorio (Mandatory) - Deben estar en todas las rutas

1 - Atributo Opcional. Pueden o no ser reconocidos por otras implementaciones

- Bit Transitivo (Transitive Bit - 1).

Los Atributos Opcionales pueden ser

0 - No transitivos. Pueden ser descartados por aquellas implementaciones que no los reconozcan

1 - Transitivos - Aunque no sean reconocidos por otras implementaciones deben ser Re advertidos por las mismas

- Bit Parcial (Partial Bit - 2)

Sólo para atributos opcionales, el valor 1 indica que al menos un router BGP en el camino no reconoció el atributo

- Bit de Longitud Extendida (Extended Length Bit - 3)

El valor 0 implica que el campo Longitud del TLV tiene 1 Octeto, El valor 1 indica que el campo longitud tiene 2 octetos

- Bits No Usados (Unused Bits – 4-7).

El código de tipo (8-15). Se codifica el tipo de atributo.

Attribute Code	Type
1 — ORIGIN	Well-known mandatory
3 — NEXT_HOP	Well-known mandatory
2 — AS_PATH	Well-known mandatory
4 — MULTI_EXIT_DISC	Optional nontransitive
5 — LOCAL_PREF	Well-known discretionary
6 — ATOMIC_AGGREGATE	Well-known discretionary
7 — AGGREGATOR	Well-known discretionary
8 — COMMUNITY	Optional transitive (Cisco)
9 — ORIGINATOR_ID	Optional nontransitive (Cisco)
10 — Cluster List	Optional nontransitive (Cisco)
11 — Destination Preference	(MCI)
12 — Advertiser	(Baynet)
13 — rcid_path	(Baynet)
255 — Reserved	—

7.4 EBGP y IBGP

Cuando BGP se ejecuta entre routers en diferentes sistemas autónomos, se llama EBGP.

Por defecto, los routers que ejecutan BGP están conectados directamente entre sí.

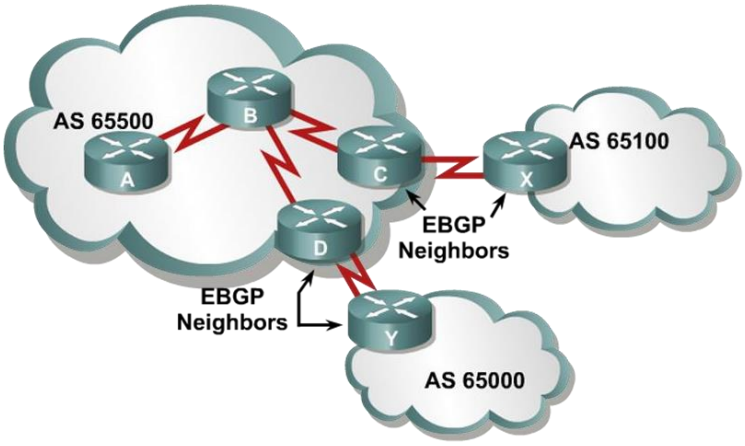
Un vecino **EBGP** es un router fuera de este sistema autónomo; un IGP no se ejecuta entre los vecinos EBGP.

También existe el **IBGP** y se utiliza para enviar la información dentro de un AS, utilizado como área de tránsito para otro AS.

IBGP necesita que sus routers estén en una topología totalmente mallada, aunque no es necesario que estén directamente conectados.

EBGP hace que dos routers puedan intercambiar actualizaciones de enrutamiento BGP, en cada lado se deberá superar con éxito el saludo de tres vías TCP antes de que la sesión BGP se pueda establecer.

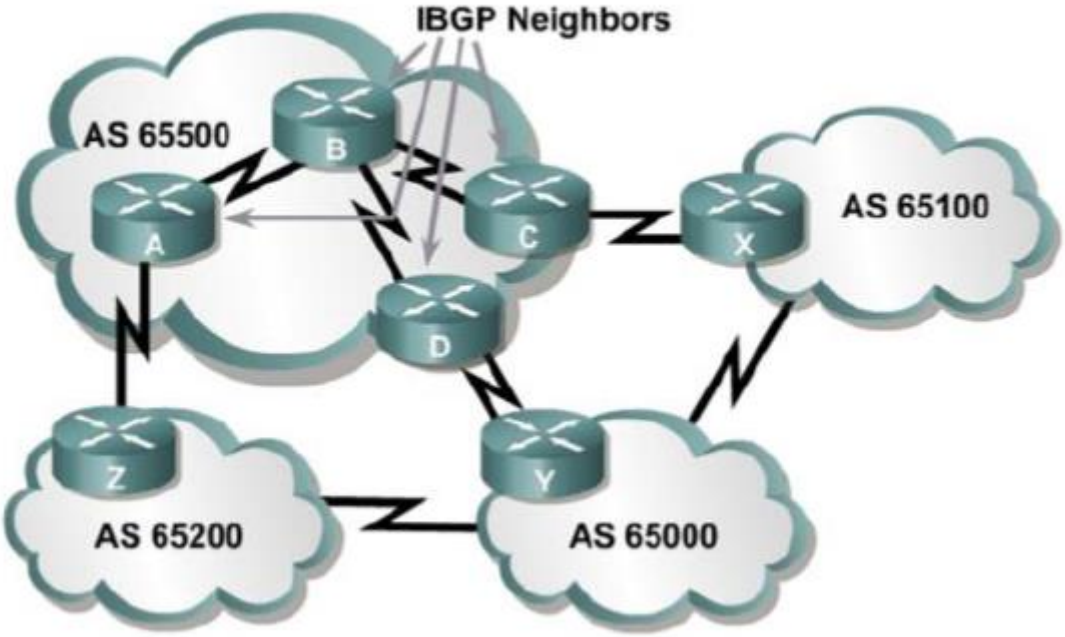
La dirección IP utilizada en el comando BGP neighbor debe ser accesible sin el uso de un IGP, para que de estar forma pueda ser accedido a través de una red conectada directamente o mediante el uso de rutas estáticas a esa dirección IP.



Los requisitos para la relación de vecinos de EBGP son:

- Se deben de definir los vecinos
- Luego se establece una sesión TCP de tres vías antes de iniciar el intercambio de actualización de enrutamiento BGP
- Finalmente los vecinos EBGP suelen conectarse directamente y estos tienen diferentes números de AS.

Los vecinos de IBGP están en los mismos sistemas autónomos y estos no necesitan estar conectados directamente.



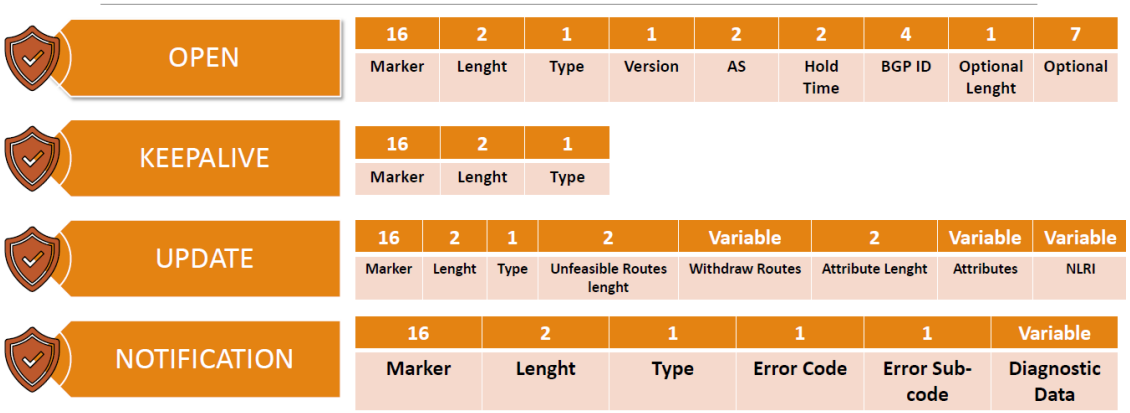
Los requisitos para la relación de vecinos de IBGP son:

- Definir los vecinos, a través de una sesión TCP de tres vías. Esta sesión se debe establecer antes de iniciar el intercambio de actualización de enrutamiento BGP.
- Ser alcanzables, estos vecinos IBGP deben encontrarse disponibles.
- Mismo numero de AS, los vecinos IBGP deben tener el mismo número de Sistema Autónomo.

8. Tipos de mensajes BGP

BGP define una variedad de tipos de mensajes:

- Open
  - Este incluye el holdtime y el router ID de BGP
  - Se utiliza para establecer conexiones con los routers BGP peers
- Keepalive
  - Se envían periódicamente entre routers peers con el objeto de evitar que expiren los timers de espera y mantener las conexiones
- Update
  - Incluye los atributos del path y las redes. Estos contienen información referida a únicamente una ruta
- Notification
  - Se genera cuando se detecta un error, se cierra la conexión BGP luego de enviarse un mensaje de notification.



Los mensajes pueden tener entre 19 y 4096 bytes de longitud.

El campo de marcador (16 bytes): se usa para autenticar mensajes BGP o para detectar pérdida de sincronización entre dos pares BGP

El campo de longitud (2 bytes): indica la longitud total del mensaje BGP, incluido el encabezado.

El campo de tipo (1 byte): corresponde a uno de los cuatro tipos de mensajes BGP.

8.1 Open Message

Una vez que una conexión TCP se ha establecido, el mensaje Open es enviado e incluye una serie de parámetros que deben ser acordados antes de una adyacencia total BGP pueda establecerse.

Una vez que ambos peers BGP hayan acordado sus capacidades, pueden empezar a intercambiar información de enrutamiento a través de Update messages de BGP.

8.2 Update Message

El mensaje UPDATE facilita dos tipos de información:

La información sobre una ruta particular a través del conjunto de redes.

Esa información se puede incorporar a la base de datos de cada dispositivo de enrutamiento que la recibe.

Una lista de rutas previamente anunciadas por este dispositivo de enrutamiento que van a ser eliminadas.

8.3 Notification Message

Estos mensajes se envían cuando se detecta algún tipo de error.

La conexión BGP se cierra inmediatamente después que este es enviado.

Los mensajes de notificación poseen un código de error, un subcódigo de error, y datos para describir el error.

8.4 KeepAlive Message

Se envían mensajes Keepalive entre pares cada 60 segundos (por defecto) para mantener las conexiones.

Cada mensaje Mensaje consiste solamente en un encabezado de mensaje (19 bytes).

Hold time tiene tres veces el temporizador KEEPALIVE de 60 segundos.

Si el temporizador periódico = 0, no se envían mensajes de actividad.

El intervalo recomendado keepalive es un tercio del intervalo de tiempo de mantenimiento.

9. Máquina de estado BGP

BGP es una máquina de estado que toma un router a través de los siguientes estados con sus vecinos:

Idle, Connect, Open sent, Open confirm, Established

El estado Idle comenzará una vez que el comando neighbor es configurado.

9.1 Idle State

El router está buscando en la tabla de enrutamiento para ver si existe una ruta para llegar al vecino.

Si un router permanece en este estado entonces el router es:

En espera de una ruta estática a la red o dirección IP que desea configurar.

Esperando el IGP para aprender acerca de esta red de otro router.

9.2 Connect State

El router encontró una ruta al vecino y ha completado el protocolo de enlace de tres vías TCP.

9.3 Activate State

BGP está tratando de adquirir un peer para iniciar una conexión TCP.

Si tiene éxito, éste pase al OpenSent de lo contrario el estado vuelve al estado Idle.

Si el router queda es este estado significa que el router no ha recibido una respuesta (paquete abierto confirmar) atrás del vecino.

Las razones para esto pueden ser que falten declaración del vecino p en número de AS es incorrecto.

9.4 Open Sent State

Un mensaje open fue enviado, con los parámetros para la sesión BGP.

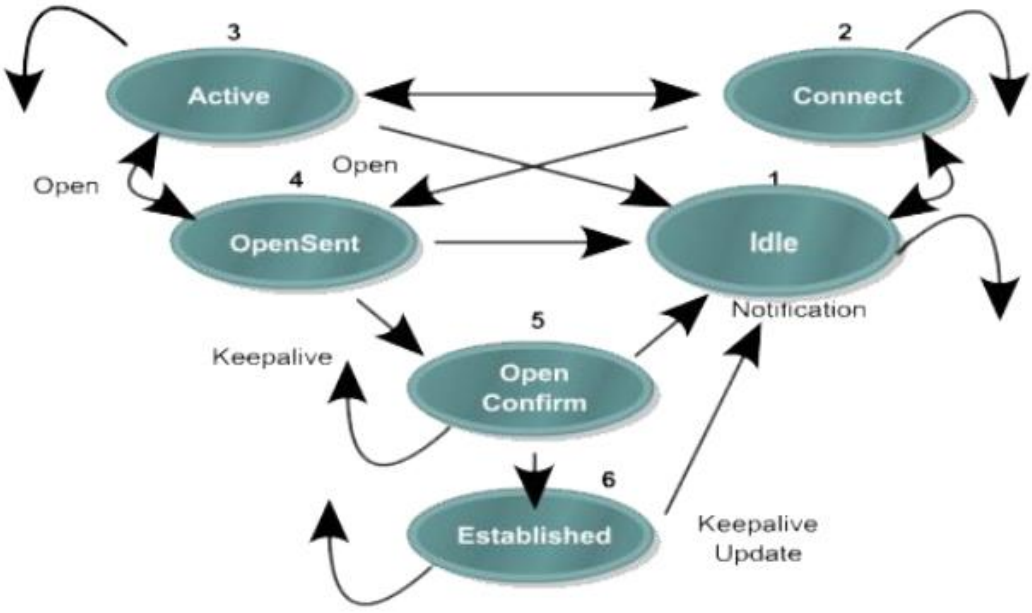
9.5 Open Confirm

El router recibe un acuerdo sobre los parámetros para establecer una sesión.

9.6 Established State

Este es el estado deseado para una relación de vecino.

Significa que están establecidos como peering y comienza el enrutamiento.



10. Configuración de BGP

Antes de implementar una solución de enrutamiento BGP, debe ser considerado lo siguiente:

▪ Plan de direccionamiento IP

▪ La topología de red

▪ BGP relación con un proveedor de servicio

Una vez que los requisitos se han evaluado, se puede crear el plan de aplicación.

La información necesaria para implementar enrutamiento BGP incluye lo siguiente:

▪ El número AS de empresa y el proveedor de servicios

▪ Las direcciones IP de todos los vecinos (peers) involucrados

▪ Las redes que son anunciadas dentro de BGP

En el plan de ejecución, las tareas básicas de BGP son las siguientes:

▪ Definir el proceso de BGP

▪ Establecer las relaciones de vecindad

▪ Anuncia las redes en BGP

Tras la implementación de BGP, la verificación debe confirmar la correcta instalación en cada router.

Tareas de verificación incluyen la verificación de:

▪ Verificar que las correspondientes relaciones BGP vecino y adyacencias se establecen.

▪ Verificación de que la tabla BGP se completa con la información necesaria.

▪ Verificar que haya conectividad de la red entre los routers y otros dispositivos.

▪ Verificación de que BGP comporta como se espera en un caso de un cambio topológico, mediante pruebas de fallo de enlace y eventos de fallo de router.

Después de una exitosa implementación de BGP, el proceso de solución y verificación y los resultados deben ser documentados para referencia futura.

La documentación debe incluir:

▪ Un mapa de la topología

▪ El plan de direccionamiento IP

▪ La jerarquía del sistema autónomo

▪ Las redes e interfaces incluidos en cada router en BGP

▪ El valor por defecto y los parámetros configurados especiales

▪ Los resultados de la verificación.

10.1 Habilitar enrutamiento BGP

Router bgp Autonomous-system

El valor autonomous-system es un número generado internamente (si no se conecta a una red de proveedor) u obtenerse a partir de un ISP o RIR. Es un parámetro necesario.

Puede ser cualquier número entero positivo en el rango de 1 a 65535.

Sólo una instancia de BGP se puede configurar en el router de una sola vez.

10.2 Definir los vecinos BGP

Identificar enrutador del mismo nivel para establecer una sesión BGP con.

neighbor {ip-address | peer-group-name} remote-as autonomous-system

La ip-address es la dirección de destino del BGP peer.

Esta dirección debe ser alcanzable antes de intentar establecer la relación BGP.

El autonomous-system se utiliza para determinar si la sesión es con peers BGP internos (IBGP) o con pares BGP externo (EBGP).

Si el valor es el mismo que el AS del router, a continuación, se intenta una sesión IBGP.

Si el valor no es el mismo que AS del router, entonces se intenta una sesión de EBGP.

10.3 Definición de grupo de pares

En BGP, los vecinos se han configurado con las mismas políticas de actualización.

Para simplificar la configuración y la actualización más eficiente, los vecinos con las mismas políticas de actualización se pueden agrupar en peer groups.

Los miembros del peer group heredarán todas las opciones de configuración del grupo de pares.

Sólo las opciones que afectan a las actualizaciones entrantes se pueden anular.

Crear un peer group sobre el router local.

Router(config-router)#

neighbor peer-group-name **peer-group**

peer-group-name es el nombre del grupo de pares BGP que se creará.

El nombre es local en el router en el que está configurado y no se transmite a cualquier otro router.

10.4 Asignar vecinos al grupo peer

Asignar vecinos como parte del grupo de pares.

```
Router(config-router)#

neighbor ip-address peer-group peer-group-name
```

- ip-address es la dirección IP del vecino que ha de ser asignado como un miembro del peer group.
- peer-group-name debe existir.

10.5 Deshabilitar un vecino BGP

Para deshabilitar un vecino BGP existente o una relación grupo de pares.

Router(config-router)#

neighbor {ip-address | peer-group-name} **shutdown**

- Es indicado para hacer grandes cambios de política a un router vecino.
- El comando no sólo termina la sesión, sino que también elimina todos los datos relacionados de enrutamiento.
- Para volver a habilitar el vecino anteponer la palabra clave no al comando.

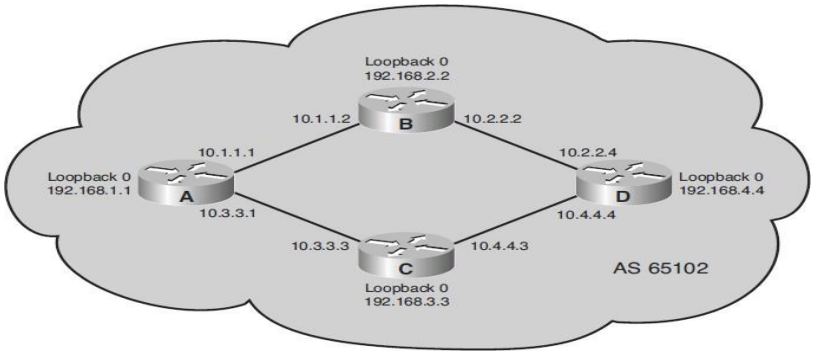
10.6 Problema de la dirección IP de origen IBGP

BGP no acepta cambios solicitados. Debe ser consciente de cada router vecino y tener una declaración de vecino para ello.

Por ejemplo, cuando un router crea y envía un paquete, la dirección IP del interfaz de salida se utiliza como dirección de origen de paquetes por defecto.

Para los paquetes BGP, esta dirección IP de origen debe coincidir con la dirección en la declaración del vecino correspondiente en el otro router o los routers no establecerá la sesión BGP.

Esto no es un problema para los vecinos EBGP, ya que típicamente están directamente conectados.



Cuando existen varias rutas entre los vecinos IBGP, la dirección de origen BGP puede causar problemas:

El Router D utiliza el comando neighbor10.3.3.1 remote-as 65102 para establecer una relación con A.

Sin embargo, el router A envía paquetes BGP a través de D B por lo tanto la dirección IP origen de los paquetes es 10.1.1.1.

La sesión IBGP entre A y D no se puede establecer porque D no reconoce 10.1.1.1 como un vecino BGP.

Establezca la sesión IBGP utilizando una interfaz loopback

Router(config-router)#

neighbor {ip-address | peer-group-name} **update-source** loopback interface-number

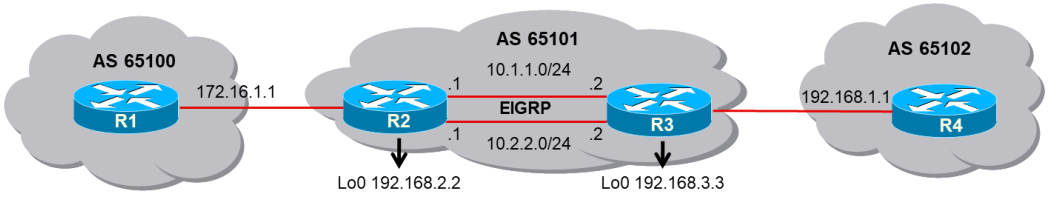
- El comando update-source informa al router para utilizar una dirección de la interfaz loopback para todos los paquetes BGP.
- El comando anula la dirección IP origen por defecto para los paquetes BGP únicamente, utilizado en sesiones IBGP.
- Como ventaja adicional, las interfaces físicas pueden fallar por cualquier número de razones, pero loopbacks nunca fallan.

Configure el router como siguiente salto para un BGP-speaking peer.

Router(config-router)#

neighbor {ip-address | peer-group-name} **next-hop-self**

- El comando fuerza BGP anunciarse a sí mismo como el origen de las rutas
- ip-address identifica el peer router para el que se enviará los anuncios, este router sera identificado como el next hop.
- Este comando es útil en redes unmeshed (tales como Frame Relay) donde los vecinos BGP no pueden tener acceso directo a todos los otros vecinos en la misma subred IP.



- R2 usa el comando neighbor next-hop-self para cambiar la configuración predeterminada del siguiente salto de BGP
- Después de configurar este comando, R2 anuncia un siguiente salto de 192.168.2.2 (la dirección IP de su interfaz loopback) a su vecino IBGP porque esa es la dirección IP de origen de la actualización de enrutamiento a su vecino IBGP (establecido con el comando neighbor update-source).

```
R2(config)# router bgp 65101
R2(config-router)# neighbor 172.16.1.1 remote-as 65100
R2(config-router)# neighbor 192.168.3.3 remote-as 65101
R2(config-router)# neighbor 192.168.3.3 update-source loopback0
R2(config-router)# neighbor 192.168.3.3 next-hop-self
R2(config-router)# exit
R2(config)# router eigrp 1
R2(config-router)# network 10.0.0.0
R2(config-router)# network 192.168.2.0
R2(config-router)#
```

11. Identificar las redes BGP

Habilitar BGP para anunciar una red si está presente.

Router(config-router)#

network network-number [**mask** network-mask] [**route-map** map-tag]

El comando BGP network determina qué redes este router anuncia.

- A diferencia de los IGPs, el comando no inicia BGP en interfaces específicas.
- El parámetro mask indica que BGP-4 soporta subredes y superredes.
- Si la máscara no se especifica, este comando sólo anuncia la red con clase

También es importante observar que el prefijo debe coincidir exactamente con (dirección y máscara) una entrada en la tabla de enrutamiento IP.

Es importante entender que cualquier red (tanto dirección y máscara) debe existir en la tabla de enrutamiento para la red que se anuncian en BGP.

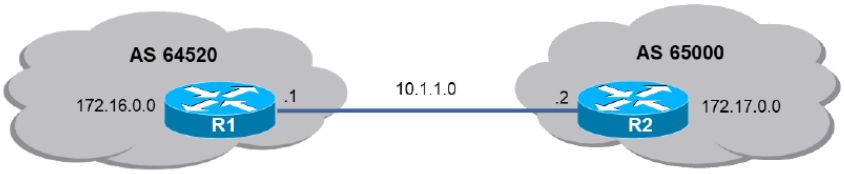
Por ejemplo, para resumir muchas redes y anunciar un bloque CIDR 192.168.0.0/16, configurar:

- network 192.168.0.0 mask 255.255.0.0
- ip route 192.168.0.0 255.255.0.0 null0

Ahora BGP puede encontrar una coincidencia exacta en la tabla de enrutamiento y anunciar la red 192.168.0.0/16 a sus vecinos.

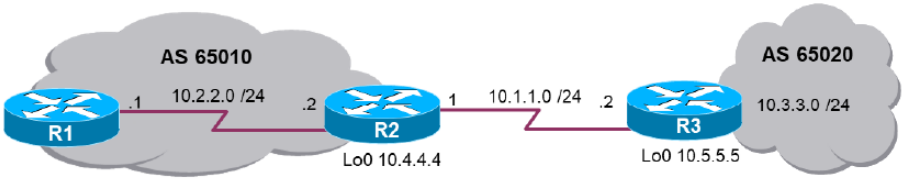
La ruta estática se anuncia en realidad nunca se utilizaría desde BGP contendría longer prefix matching routes en su tabla de enrutamiento.

12. Ejemplo de configuración de BGP



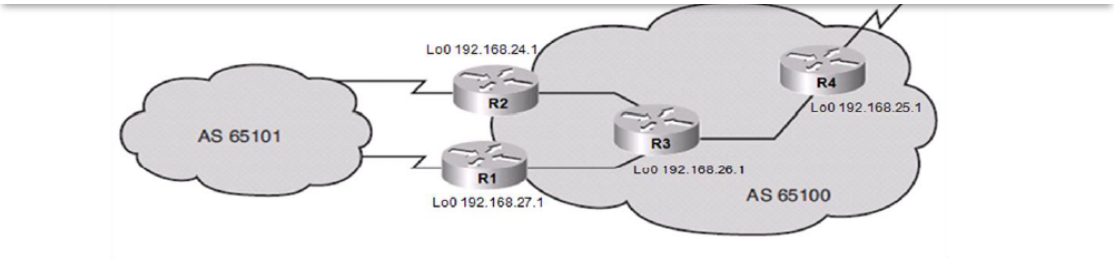

```
R1(config)# router bgp 64520
R1(config-router)# neighbor 10.1.1.2 remote-as 65000
R1(config-router)# network 172.16.0.0
R1(config-router)#
```

```
R2(config)# router bgp 65500
R2(config-router)# neighbor 10.1.1.1 remote-as 64520
R2(config-router)# network 172.17.0.0
R2(config-router)#
```



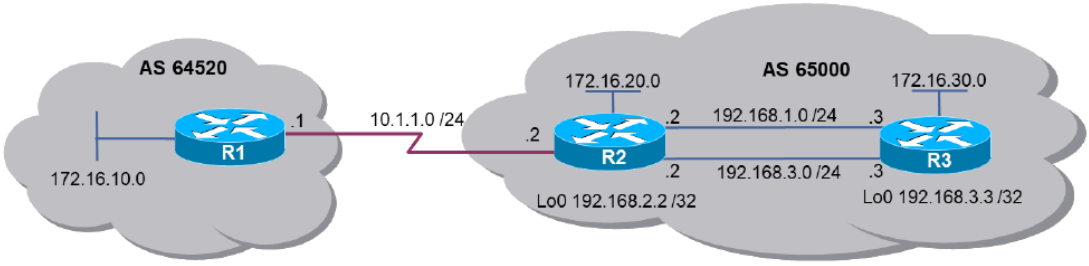

```
R2(config)# router bgp 65010
R2(config-router)# neighbor 10.1.1.2 remote-as 65020
R2(config-router)# network 10.2.2.0 mask 255.255.255.0
R2(config-router)# network 10.4.4.0 mask 255.255.255.0
R2(config-router)#
```

12.1 Ejemplo sin peer group




```
R1(config)# router bgp 65100
R1(config-router)# neighbor 192.168.24.1 remote-as 65100
R1(config-router)# neighbor 192.168.24.1 update-source loopback 0
R1(config-router)# neighbor 192.168.24.1 next-hop-self
R1(config-router)# neighbor 192.168.24.1 distribute-list 20 out
R1(config-router)#
R1(config-router)# neighbor 192.168.25.1 remote-as 65100
R1(config-router)# neighbor 192.168.25.1 update-source loopback 0
R1(config-router)# neighbor 192.168.25.1 next-hop-self
R1(config-router)# neighbor 192.168.25.1 distribute-list 20 out
R1(config-router)#
R1(config-router)# neighbor 192.168.26.1 remote-as 65100
R1(config-router)# neighbor 192.168.26.1 update-source loopback 0
R1(config-router)# neighbor 192.168.26.1 next-hop-self
R1(config-router)# neighbor 192.168.26.1 distribute-list 20 out
R1(config-router)#
```

12.2 Ejemplo de IBGP y EBGP




```
R2(config)# router bgp 65000
R2(config-router)# neighbor 10.1.1.1 remote-as 64520
R2(config-router)# neighbor 192.168.3.3 remote-as 65000
R2(config-router)# neighbor 192.168.3.3 update-source loopback 0
R2(config-router)# neighbor 192.168.3.3 next-hop-self
R2(config-router)# network 172.16.20.0 mask 255.255.255.0
R2(config-router)# network 192.168.1.0
R2(config-router)# network 192.168.3.0
R2(config-router)# no synchronization
R2(config-router)#
```

12.3 Verificación y solución de problemas BGP

Command	Description
show ip bgp	Muestra las entradas en la tabla BGP. Especifique un número de red para obtener información más específica sobre una red en particular..
show ip bgp neighbors	Muestra información detallada sobre las conexiones TCP y BGP con los vecinos.
show ip bgp summary	Muestra el estado de todas las conexiones BGP.
show ip bgp rib-failure	Muestra todas las rutas BGP anunciadas a los vecinos.
debug ip bgp [dampening | events | keepalives | updates]	

1. ¿Qué entiende por protocolo BGP?
   Border Gateway Protocol (BGP) es un protocolo de enrutamiento usado para intercambiar información de enrutamiento entre diferentes redes. Este realiza el intercambio de información con los routers de dominio

2. ¿Cuáles son los tipos de acuerdo presentes en el protocolo?

   A. Acuerdos Bilaterales Cada proveedor establece la relación que necesite con otros proveedores en el IXP Los enrutadores de borde los ISP establecen sesiones de BGP con los enrutadores de borde de otros proveedores

   B. Acuerdos Multilaterales Cada proveedor establece sesiones con el concentrador Los enrutadores de borde de los ISP tienen como vecino al IXP

3. ¿Qué entiende por sistema autónomo?

   Un sistema autónomo es un conjunto de redes IP administradas en las que se utiliza una misma política de enrutamiento, con un mismo protocolo de enrutamiento Cada sistema autónomo está identificado por un único número entero de 32 bits, conocido como número de sistema autónomo (ASN) Un AS normalmente pertenece a una organización, se pueden utilizar uno o varios IGP (Interior Gateway Protocol) en cada AS Cada AS es visto por el resto del mundo como una sola entidad

4. Cual es la función del IANA?

   La IANA se encarga de asignar los números de AS a través de cinco Registros Regionales de Internet (RIR – Regional Internet Register) Los números AS pueden estar entre 1 y 65.535, los RIRs administran los números de AS entre 1 y 64.512. Los números 64.515 hasta 65.535 están reservados para uso privado. La IANA hace cumplir una política para que las organizaciones que se conectan a un único proveedor utilicen un número de AS del Pool privado. Con el lanzamiento del RFC 4893 y RFC 5398 se extendieron los campos de dos octetos (16 bits) a campos de cuatro octetos (32 bits), aumentando el tamaño del conjunto de 65.536 a 4.294.967.296 valores disponibles.

5. Que entiende por redundancia?

   La redundancia se puede lograr mediante la implementación de enlaces redundantes, la implementación de dispositivos redundantes, y el uso de componentes redundantes en un router. La conexión del ISP también puede ser redundante. Cuando un cliente se conecta a un solo ISP la conexión se conoce como single-homed o dual-homed. Si la red ISP falla, la conectividad a Internet se interrumpe. En cambio, cuando un cliente está conectado a múltiples ISPs la conexión se denomina multihomed o dual-multihomed. Con conexiones a múltiples ISPs, la redundancia se construye en el diseño.

6. Enumere los diferentes protocolos de ruteo.

   A. IGP Es un protocolo de ruteo usado para Intercambiar información de rutas DENTRO de un SA Entre ellos tenemos a los protocolos RIP, EIGRP, OSPF, etc.

   B. EGP EGP - Exterior Gateway Protocol Protocolo de ruteo usado para intercambiar información de rutas ENTRE SA

   C. BGP Es un protocolo de ruteo externo La tabla de ruteo mantiene una lista de SA que son atravesados para alcanzar a otros SA

7. Cuales son las ventajas mas importantes de BGP ¿

   • ESCALABILIDAD: Diseñado para manejar grandes tablas de rutas (full-routing implica del orden de 400.000 prefijos). Y no requiere excesivo control de tráfico.

   • ESTABILIDAD: Se adapta a los cambios de manera fácil y rápida

   • SENCILLEZ: Es de la familia de los protocolos de vector distancia (no requiere estructura jerárquica ni conocimiento de la topología de red)

8. Enumere los tipos de mensajes del protocolo BGP
   • Open ◦ Este incluye el holdtime y el router ID de BGP ◦ Se utiliza para establecer conexiones con los routers BGP peers
   • Keepalive ◦ Se envían periódicamente entre routers peers con el objeto de evitar que expiren los timers de espera y mantener las conexiones
   • Update ◦ Incluye los atributos del path y las redes. Estos contienen información referida a únicamente una ruta
   • Notification ◦ Se genera cuando se detecta un error, se cierra la conexión BGP luego de enviarse un mensaje de notification.

9. ¿Cuáles son los estados posibles del protocolo BGP?

   A. Idle State El router está buscando en la tabla de enrutamiento para ver si existe una ruta para llegar al vecino. Si un router permanece en este estado entonces el router es: En espera de una ruta estática a la red o dirección IP que desea configurar. Esperando el IGP para aprender acerca de esta red de otro router.

   B. Connect State El router encontró una ruta al vecino y ha completado el protocolo de enlace de tres vías TCP.

   C. Activate State BGP está tratando de adquirir un peer para iniciar una conexión TCP. Si tiene éxito, éste pase al OpenSent de lo contrario el estado vuelve al estado Idle. Si el router queda es este estado significa que el router no ha recibido una respuesta (paquete abierto confirmar) atrás del vecino. Las razones para esto pueden ser que falten declaración del vecino p en número de AS es incorrecto.

   D. Open Sent State Un mensaje open fue enviado, con los parámetros para la sesión BGP.

   E. Open Confirm El router recibe un acuerdo sobre los parámetros para establecer una sesión.

F. Established State Este es el estado deseado para una relación de vecino. Significa que están establecidos como peering y comienza el enrutamiento

10. Que es lo que debe de ser considerado para poder implementar el protocolo BGP?

    Antes de implementar una solución de enrutamiento BGP, debe ser considerado lo siguiente: ▪ Plan de direccionamiento IP ▪ La topología de red ▪ BGP relación con un proveedor de servicio

PRESENTACIÓN X25, ATM, FRAME RELAY

REDES ADMINISTRATIVAS

Integrantes: • CHMELIK, Lucas •DUCLOS, Tomas •MATUTE, Leonel • PATIÑO, Florencia

X25

Es un protocolo estándar ITU-T para la comunicación en una WAN, define como deben ser establecer y mantener las conexiones entre los dispositivos del usuario y los dispositivos de la red. Está diseñado para operar efectivamente sin importar los tipos de sistemas conectados a la red. Se utiliza en las redes de conmutación de paquetes.

Utiliza las tres capas inferiores del modelo OSI y el conjunto de protocolos X25 sólo tiene significado local. Especifica sólo la interfaz.

Es el conjunto de estándares que gobiernan la interfaz entre los DTE (Data Terminal Equipment) y los DCE (Data Communication Equipment).

Características generales:

- Diseñado para medios físicos poco confiables.
- No apto para trafico en tiempo real.
- Paquetes de hasta 128 bytes.
- Servicio orientado a la conexión.
- Costo proporcional al tiempo y al tráfico.
- Velocidades de 9,6 a 64 Kbps.

Ventajas:

- Confiable.
- Segura.
- Gran capacidad de transmisión.
- Se pueden realizar varias conexiones lógicas sobre una física.

Desventajas:

- Es un protocolo complejo.
- Ancho de banda limitado.
- Lentitud de transmisiones grandes y variables.

Utiliza las tres capas inferiores del modelo OSI:

- Capa Física: especifica la interfaz eléctrica, mecánica, procedimental y funcional entre DTE y DCE. Hace referencia a los estándares X21 (digital) y X21bis (analogico). Los circuitos se definen en X24.
- Capa de Enlace de Datos: proporciona a la capa de Paquete un recurso de transporte confiable. No conoce de Circuitos Virtuales y utiliza los protocolos LAP y LAPB.

- Capa de Red: se ofrecen servicios mediante Primitivas (se intercambian parametros).

  Maneja QoS (calidad del servicio) que tiene los valores mínimos y los valores deseables con respecto al retardo de transito, la probabilidad de error, la prioridad, el costo y la ruta.

Servicios de X25

PVC (Circuitos virtuales permanentes): es el equivalente a una linea delicada, que esta definido de manera estática y siempre esta disponible, mientras que la red lo este. Equivale a líneas privadas.

SVC (Circuitos virtuales conmutados): es el equivalente a una llamada. La red establece una conexión en un circuito virtual, transfiere paquetes y libera la conexión. Equivale a las llamadas telefónicas.

Circuitos Virtuales

Define la existencia de un camino lógico y bidireccional de un DTE a otro a través de la red X25. Físicamente la conexión puede pasar por muchos nodos intermedios como DCE y PSE. Varios circuitos virtuales pueden ser multiplexados en un solo circuito físico.

Transferencia de datos

La máxima cantidad de datos para transferir es de 128 octetos para dar rapidez y en algunos casos puede producir fragmentación.

Control de flujo: los paquetes se transmiten gracias a la capa de enlace, es confiable.

Algoritmos de Asignacion

A la llamada entrante por el DCE se le asigna el numero mas bajo disponible.

A la llamada saliente por el DTE se le asigna el numero mas alto disponible.

Limitaciones de X25

- Es una implementación incompleta del modelo OSI, solo define interface.
- No se preveen rutas alternativas en caso de error, solo se retransmite.
- No tolera empaquetado de voz, tiene alto delay potencial.

Pad

Es un dispositivo muy común en las redes X25. Se utilizan cuando el dispositivo DTE es muy simple como para implementar todas las funcionalidades de X25.

Sus tres funciones primarias son:

- Buffering: almacena los datos hasta que el dispositivo esta lista para transmitir.
- Ensambla paquetes: forma paquetes con los datos para enviarlso hacia el DCE.
- Desensambla paquetes: los paquetes de entrada los desensambla antes de enviarlos al DTE.

RED FRAME RELAY

Frame Relay es una tecnología de protocolo de red de conmutación de paquetes digital de capa de enlace de datos diseñada para conectar redes de área local (LAN) y transferir datos a través de redes de área amplia (WAN). Frame Relay comparte parte de la misma tecnología subyacente que X.25 y alcanzó cierta popularidad en los Estados Unidos como la infraestructura subyacente para servicios de red digital de servicios integrados (ISDN) vendidos a clientes comerciales.

Se basa en la tecnología de conmutación de paquetes X.25 más antigua que fue diseñada para transmitir datos analógicos como conversaciones de voz. A diferencia de X.25, que fue diseñado para señales analógicas, Frame Relay es una tecnología de paquetes rápida, lo que significa que el protocolo no intenta corregir errores. A menudo se usa para conectar LAN con backbones principales, así como en redes de área amplia públicas y también en entornos de redes privadas con líneas T-1 arrendadas. Requiere una conexión dedicada durante el período de transmisión y no es ideal para voz o video, que requieren un flujo constante de transmisiones.

Frame Relay, también considerada como red X.25 de segunda generación, opera a través de líneas de fibra óptica o RDSI y admite diferentes protocolos de red de nivel superior, incluido el protocolo de Internet (IP).

Características de Frame Relay

Frame Relay es un servicio sin conexión, lo que significa que cada paquete de datos que pasa por la red contiene información de dirección.

Frame Relay es un servicio que se proporciona con una variedad de velocidades desde 56Kbps hasta 25 Mbps. Aunque las velocidades más utilizadas para el servicio son actualmente 56 Kbps y 1.544 Mbps

Las tramas son de longitud variable y va hasta 4,096 bytes

Frame Relay se considera un servicio ISDN de banda ancha

Opera a alta velocidad (1.544 Mbps a 44.376 Mbps).

Opera solo en las capas físicas y de enlace de datos. Por lo tanto, se puede usar fácilmente en Internet.

Tiene un gran tamaño de trama de 9000 bytes. Por lo tanto, puede acomodar todos los tamaños de trama de red de área local.

Frame Relay solo puede detectar errores (en la capa de enlace de datos). Pero no hay control de flujo o control de errores.

Cómo funciona Frame Relay

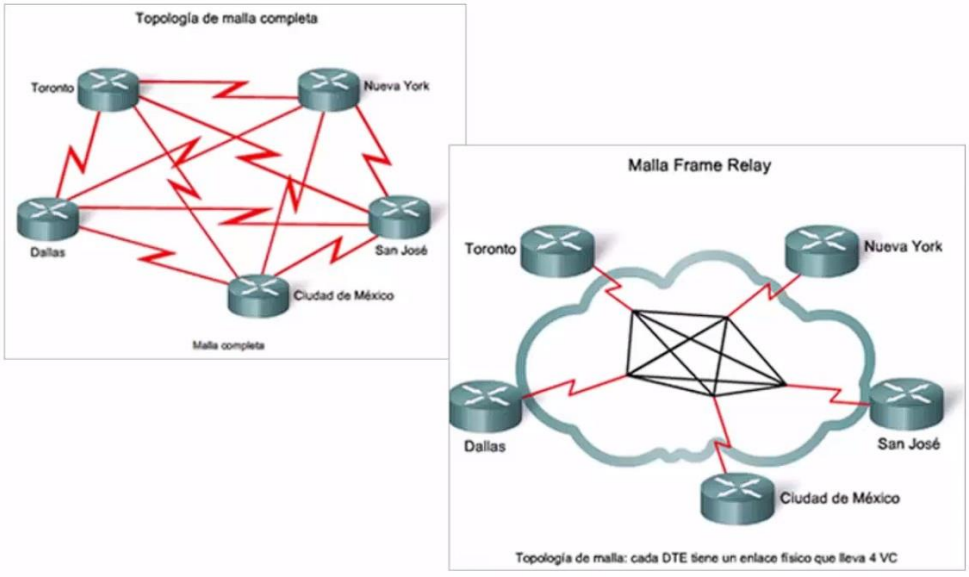
Frame Relay admite la multiplexación del tráfico desde múltiples conexiones a través de un enlace físico compartido. Utiliza componentes de hardware que incluyen tramas de router, bridges, y switches para empaquetar datos en mensajes de retransmisión de trama individuales. Cada conexión utiliza un identificador de conexión de enlace de datos de 10 bits (DLCI) para un direccionamiento de canal único.

Hay dos tipos de conexión:

- Circuitos virtuales permanentes (PVC) para conexiones persistentes destinadas a mantenerse durante largos períodos incluso si no se transfieren datos activamente.
- Circuitos virtuales conmutados (SVC) para conexiones temporales que duran solo una sesión.

Entonces, Frame Relay coloca los datos en una unidad de tamaño variable llamada frame y deja cualquier corrección de error necesaria (transmisión de datos) hasta los puntos finales, lo que acelera la transmisión general de datos. Para la mayoría de los servicios, la red proporciona un circuito virtual permanente (PVC), lo que significa que el cliente ve una conexión continua y dedicada sin tener que pagar una línea arrendada a tiempo completo, mientras que el proveedor de servicios determina la ruta a la que viaja cada trama su destino y puede cobrar en función del uso. Los circuitos virtuales conmutados (SVC), por el contrario, son conexiones temporales que se destruyen después de que se completa una transferencia de datos específica.

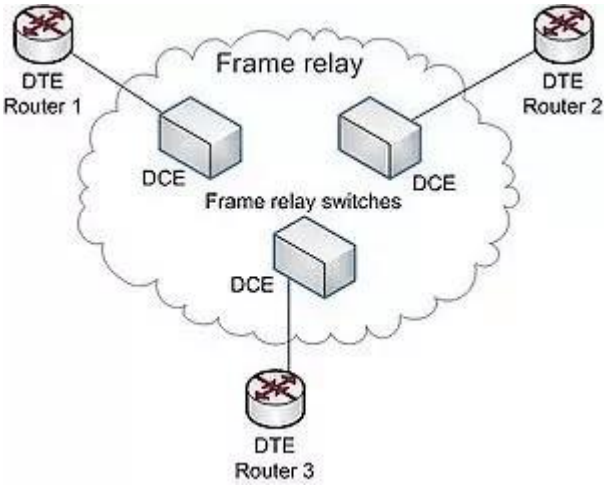
Frame Relay logra un mejor rendimiento que X.25 a un costo menor al no realizar la corrección de errores. La corrección de errores se descarga a otros componentes de la red para reducir la latencia de la red. También admite tamaños de paquetes de longitud variable para un uso más eficiente del ancho de banda de la red.



Rendimiento de Frame Relay

Frame Relay admite las velocidades de datos de las líneas T1 y T3 estándar (1.544 Mbps y 45 Mbps , respectivamente) con conexiones individuales de hasta 56 Kbps. También admite conexiones de fibra de hasta 2,4 Gbps.

Cada conexión se puede configurar con una Tasa de información comprometida (Committed Information Rate, CIR) que el protocolo mantiene de forma predeterminada. CIR se refiere a una velocidad de datos mínima que la conexión debería recibir en condiciones estables (y se puede superar cuando el enlace físico subyacente tiene suficiente capacidad libre para soportarlo). Frame Relay no restringe el rendimiento máximo al del CIR, sino que también permite el tráfico de ráfaga, durante el cual la conexión no puede exceder su CIR temporalmente (generalmente durante hasta dos segundos).



Rendimiento de Frame Relay

Actualmente, Frame Relay se usa más como una tecnología de capa de enlace de datos para transportar datagramas IP (encapsulado en un framework Frame Relay y enrutado a través de la red VC) de un router IP a otro. También es más seguro, ya que en lugar de enviar los datos a través de Internet pública, se envía a través de una red de VC privada.

Problemas con Frame Relay

Frame Relay proporciona una forma rentable para que las compañías de telecomunicaciones transmitan datos a largas distancias. Esta tecnología disminuyó en popularidad a medida que las empresas migraron sus implementaciones a otras soluciones basadas en el protocolo de Internet (IP).

Muchos vieron el modo de transferencia asincrónica (ATM) y el frame relay como competidores directos. La tecnología ATM difiere sustancialmente de la retransmisión de tramas. ATM utiliza paquetes de longitud fija en lugar de paquetes de longitud variable y requiere un hardware más costoso para operar.

Frame Relay enfrentó una fuerte competencia de MPLS (Conmutación de etiquetas multiprotocolo). Las técnicas MPLS ahora se usan ampliamente en los routers de Internet para habilitar soluciones de red privada virtual (VPN) que hubieran requerido previamente frame relay o soluciones similares.

ATM

HISTORIA.

ATM surge en 1986 como idea de un grupo de ingenieros de compañías telefónicas. Inicialmente pretende resolver dos problemas:

- mayor ancho de banda
- rápida conmutación

Se hizo popular en 1988 cuando se decidió que esta tecnología de conmutación sería la usada por las futuras redes ISDN en banda ancha.

INTRODUCCIÓN.

El modo de transferencia asíncrona ATM es una red de conmutación de paquetes basada en circuitos virtuales que envía paquetes (celdas ATM) de longitud fija a través de LAN o WAN, en lugar de paquetes de longitud variable utilizados en otras tecnologías.

Con la finalidad de aprovechar al máximo la capacidad de los sistemas de transmisión, la información es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes de longitud constante.

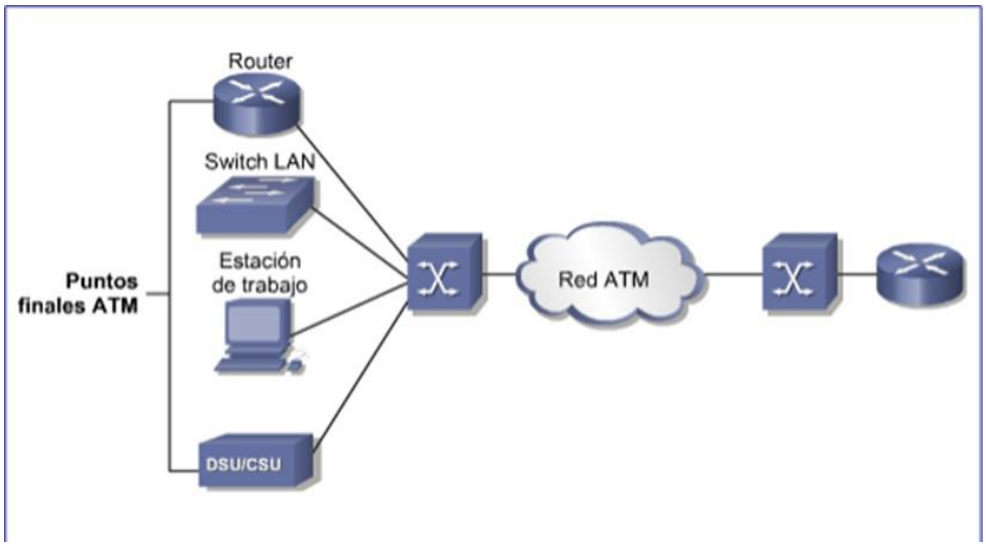
Una red ATM se encuentra conformada por uno o más switches ATM y por los terminadores ATM.

La tarea de un switch ATM se basa en aceptar las celdas entrantes desde un terminador ATM o switch ATM, luego lee y actualiza la información del encabezado de la celda y conmuta la celda hacia la interfaz de salida adecuada.

Un terminador ATM es aquel que contiene una interfaz ATM, ejemplos de estos pueden ser:

- Routers
- terminales de datos
- DSU/CSUs

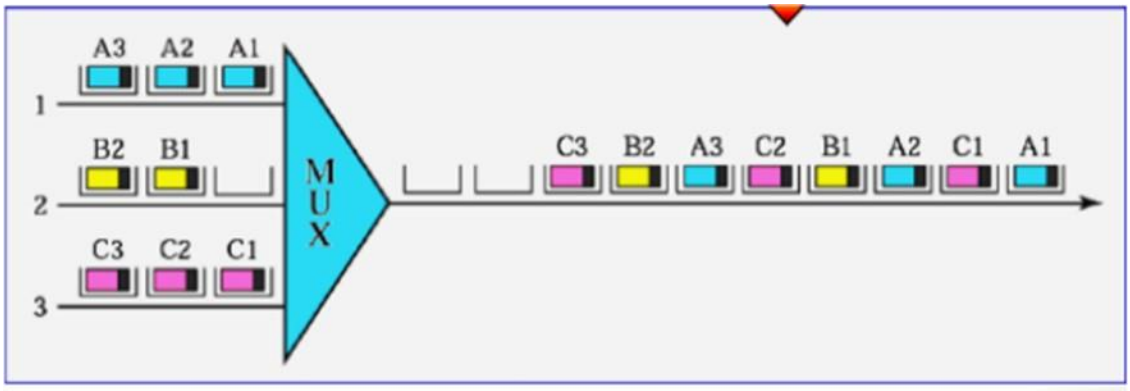
- Switches LAN.



MULTIPLEXACIÓN ASÍNCRONA.

ATM la utiliza para multiplexar las celdas que vienen de diferentes canales.

Por eso se denomina modo de transferencia asíncrono.



ESTRUCTURA BÁSICA DE LA CELDA

Una celda ATM consta de una cabecera de 5 bytes y una carga útil de 48 bytes.

La cabecera ATM proporciona información sobre el tipo de enrutamiento, y el destino de una celda.

La carga útil de una celda ATM transporta ya sea información de usuario o información de gestión de la capa.

Al igual que en otras tecnologías basadas en conmutación de paquetes, existen celdas de propósito especial que dan lugar a la aparición de los distintos tipos de celdas.

ATM define dos formatos de celda diferentes: Interfaz usuario-red (UNI) y red de red. (NNI). La mayoría de los enlaces ATM utilizan el formato de celda UNI.

Esquema de una celda ATM UNI .

Esquema de una celda ATM NNI

El encabezado de la celda ATM incluye los siguientes campos:

- Virtual Path Identifier (VPI)
- Virtual Channel Identifier (VCI)
- Payload Type Identifier (PTI)
- Header Error Control (HEC)
- Cell Loss Priority (CLP)

ENCABEZADO DE LA CELDA

- GFC (Generic Flow Control): provee funciones locales, como control de flujo entre un equipo terminador ATM y el switch ATM. Este campo no se utiliza actualmente.
- VPI (Virtual Path Identifier) y VCI (Virtual Chanel Identifier): juntos, identifican el próximo paso de una celda mientras ésta viaja a través de varios switches ATM hasta su destino final.
- PT (Payload Type): el primer bit del PT indica si la celda contiene datos de usuario o datos de control.
- Si la celda contiene datos de usuario (seteado a 0) entonces el segundo bit indica si existe congestión (seteado a 1) sobre el enlace o no (seteado a 1) y el tercero indica si ésta es la última de una serie de celdas que representan una trama.
- Si la celda contiene datos de control, entonces el segundo y tercer bit indican mantenimiento o administración del flujo de información.
- CLP (Cell Loss Priority): indica si la celda debe ser descartada si existe un caso extremo de congestión mientras ésta viaja a través de la red.
- HFC (Header Error Control): calcula una suma de comprobación sólo de los primeros 4bytes del encabezado.

RUTAS Y CANALES VIRTUALES:

Las redes ATM son redes orientadas a la conexión, por lo tanto, las conexiones virtuales ATM son de dos tipos:

Circuitos Virtuales Permanentes (PVC): U PVC permite la conectividad directa entre sitios. Es similar a una línea dedicada.

Ventaja: No requiere call setup entre los switches.

Desventaja: Conectividad estática y configuración manual.

Circuitos Virtuales Conmutados (SVC): Un SVC es creado y liberado dinámicamente y se usa solamente mientras exista información que transmitir. Es similar a una llamada telefónica. El control de llamadas dinámicas requiere de un protocolo entre el endpoint y el switch.

Ventaja: Flexibilidad de conexión y el call setup puede ser colgado automáticamente por los equipos.

Desventaja: Tiempo para llevar a cabo el call setup.

Una ruta virtual es un conjunto de canales virtuales, donde cada uno de ellos es conmutado en forma transparente a través de la red ATM y agrupados a través del mismo valor de VPI. Cada encabezado de celda contiene los campos VPI y VCI, estos asocian a cada celda en forma explícita con un determinado canal virtual sobre un enlace físico. Los campos VPI y VCI no son direcciones, como las direcciones MAC usadas en la conmutación de tramas de una LAN. Los campos VPI y VCI son asignados en forma explícita en cada segmento de la conexión, de esta forma, sólo tienen un significado local a través de un enlace determinado. Los campos VPI y VCI son mapeados en cada punto de conmutación. Las conexiones punto a punto conectan dos sistemas ATM y esta conexión puede ser unidireccional o bidireccional. Una conexión punto a multipunto agrupa un mismo origen (nodo raíz) hacia múltiples extremos remotos. Este tipo de conexiones pueden ser unidireccionales solamente.

NIVELES DE ATM

La funcionalidad de ATM se corresponde con el nivel físico y parte del nivel de enlace del modelo OSI.

El modelo ATM está compuesto por 3 niveles:

- AAL
- ATM
- Físico.

Los terminales ATM utilizan los 3 niveles y los conmutadores los 2 inferiores.

Aplicaciones: Son los niveles que residen sobre AAL. Aceptan los datos de usuario, los clasifican en paquetes, y los pasan a la AAL.

AAL: Nivel de adaptación ATM. Responsable de convertir los datos de aplicaciones a celdas ATM de 48 bytes. Detecta celdas erróneas perdidas. Controla el flujo y la temporización.

Nivel ATM: Responsable del transporte de celdas a través de la red Toma los datos que van a ser enviados y añade la información de cabecera de 5 bytes que asegura el envía de la celda por la conexión correcta.

Nivel físico: Responsable de convertir las celdas al formato óptico o eléctrico apropiado. Define las características ópticas o eléctricas y las interfaces de red. Los servicios se ofrecen en los extremos AAL sólo opera del lado del usuario.

APLICACIONES TÍPICAS

- Intercambio de información en tiempo real, dentro del ámbito empresarial.
- Interconexión de Redes de Área Local (LAN) que requieran un gran ancho de banda.
- Acceso a Internet de alta velocidad.
- Videoconferencia.
- Voz en entorno corporativo con compresión y supresión de silencios.
- Distribución de Audio/Vídeo.

VENTAJAS

¿Qué ventajas ofrece el servicio ATM respecto a servicios basados en X.25?

El servicio ATM no requiere complicados procedimientos de control y retransmisiones, lo que lleva consigo una alta proporción de información útil respecto a la información de control del Servicio (en las celdas ATM no existen cabeceras de control de nivel 3 como ocurre con la tecnología X.25).

Concretamente, ATM desplaza hacia los equipos terminales del cliente funcionalidad que en X.25 corresponde a la red (corrección de errores, control de flujo, etc.). Como consecuencia de la disminución de proceso en red, el servicio ATM se adecua mejor a altas velocidades de transmisión, minimiza el retardo en red y presenta un elevado rendimiento (alto porcentaje de información útil transmitida, cabeceras mínimas).

	X.25	ATM
Velocidad	2400 bit/s a 2 Mbit/s	34 Mbit/s
Retardo	Alto	Bajo
Caudal (throughput)	Medio	Alto

Tipo de tráfico	Datos	Datos/Voz/Video

X.25 está especialmente indicado para tráfico transaccional de bajo /medio caudal y, en particular, para comunicaciones centralizadas en las que muchos puntos se comunican con una instalación central. Ofrece gran cantidad de facilidades opcionales.

ATM está diseñado fundamentalmente para aplicaciones de entorno de Red de Área Local, es decir, transporte transparente de datos a alta velocidad, bajo retardo y alto caudal, transporte conjunto de diferentes tipos de tráfico y múltiples protocolos; también permite el transporte de voz y video.

¿Qué ventajas ofrece el servicio ATM respecto al servicio Frame Relay?

ATM es similar en concepto a Frame Relay. Ambos tienen la ventaja de proporcionar mayor velocidad de transmisión que X.25. En ATM la información está organizada en paquetes de tamaño fijo llamados celdas. Al igual que en Frame Relay , no hay información para el control de errores ni de flujo en las celdas, lo que permite alcanzar altas velocidades.

En ATM, el uso de celdas pequeñas de tamaño fijo tiene varias ventajas. En primer lugar, el uso de celdas pequeñas puede reducir el retardo en cola para una celda de alta prioridad cuando otra celda está siendo transmitida. En segundo lugar, al ser las celdas de tamaño fijo, la conmutación puede ser realizada más eficientemente. Este es un factor importante para obtener tasas de bits tan altas.

Preguntas:

¿Que capas del modelo OSI utiliza X25?

Capa Física: especifica la interfaz eléctrica, mecánica, procedimental y funcional entre DTE y DCE. Hace referencia a los estándares X21 (digital) y X21bis (analogico). Los circuitos se definen en X24.

Capa de Enlace de Datos: proporciona a la capa de Paquete un recurso de transporte confiable. No conoce de Circuitos Virtuales y utiliza los protocolos LAP y LAPB.

Capa de Red: se ofrecen servicios mediante Primitivas (se intercambian parametros). Maneja QoS (calidad del servicio) que tiene los valores mínimos y los valores deseables con respecto al retardo de transito, la probabilidad de error, la prioridad, el costo y la ruta.

¿Cual es la maxima cantidad de datos a transferir en X25?

La máxima cantidad de datos para transferir es de 128 octetos para dar rapidez y en algunos casos puede producir fragmentación.

Enumere 3 ventajas de X25

Segura.
Gran capacidad de transmisión.
Se pueden realizar varias conexiones lógicas sobre una física.

¿Cuáles son los dos circuitos virtuales de X25?

PVC (Circuitos virtuales permanentes): es el equivalente a una línea delicada, que está definido de manera estática y siempre está disponible, mientras que la red lo esté. Equivale a líneas privadas.

SVC (Circuitos virtuales conmutados): es el equivalente a una llamada. La red establece una conexión en un circuito virtual, transfiere paquetes y libera la conexión. Equivale a las llamadas

Enumere 3 ventajas de PAD.

Buffering: almacena los datos hasta que el dispositivo está lista para transmitir.
Ensambla paquetes: forma paquetes con los datos para enviarlos hacia el DCE.
Desensambla paquetes: los paquetes de entrada los desensambla antes de enviarlos al DTE.

¿Qué tipos de circuitos presentan las redes ATM?

Circuitos Virtuales Permanentes (PVC): PVC permite la conectividad directa entre sitios. Es similar a una línea dedicada.

Circuitos Virtuales Conmutados (SVC): Un SVC es creado y liberado dinámicamente y se usa solamente mientras exista información que transmitir. Es similar a una llamada telefónica. El control de llamadas dinámicas requiere de un protocolo entre el endpoint y el switch.

¿Cómo es la estructura de una celda ATM?

Una celda ATM consta de una cabecera de 5 bytes y una carga útil de 48 bytes. La cabecera ATM proporciona información sobre el tipo de enrutamiento, y el destino de una celda. La carga útil de una celda ATM transporta ya sea información de usuario o información de gestiónde la capa.

Mencione tres aplicaciones de ATM.

- Intercambio de información en tiempo real, dentro del ámbito empresarial.
- Interconexión de Redes de Área Local (LAN) que requieran un gran ancho de banda.
- Acceso a Internet de alta velocidad.

¿Qué ventajas presenta ATM sobre X.25?

El servicio ATM no requiere complicados procedimientos de control y retransmisiones, lo que lleva consigo una alta proporción de información útil respecto a la información de control del Servicio (en las celdas ATM no existen cabeceras de control de nivel 3 como ocurre con la tecnología X.25).

¿Cómo está formada una red ATM?

Una red ATM se encuentra conformada por uno o más switches ATM y por los terminadores ATM.

La tarea de un switch ATM se basa en aceptar las celdas entrantes desde un terminador ATM oswitch ATM, luego lee y actualiza la información del encabezado de la celda y conmuta la celdahacia la interfaz de salida adecuada**.**

¿Para qué se utiliza frame relay?

Es método de comunicación orientado a paquetes para la conexión de sistemas informáticos

¿Cuál es el rango de ancho de banda de frame relay?

Ofrece un ancho de banda comprendido en el rango de 56 Kbps y 1.544 Mbps.

¿Cuál es el tamaño máximo de paquete?

El tamaño máximo de trama es de 1 a 8 KB.

¿En qué capa se encuentra el modelo OSI?

Es un protocolo de capa física y capa de enlace de datos.

¿Qué indica el principio y final de la trama en frame relay?

El señalador indica el principio y el final de la trama Frame Relay.

VPN y FDDI

Materia: Redes Administrativas
Comisión: 5°A
Alumnos: Peralta Flavio, Perchet Katia, Sasso Patricio
Turno: Noche

Índice

FDDI 2

¿Qué es FDDI? 2

Historia de FDDI 2

Generalidades de FDDI 2

Composición de FDDI 2

Trama de Datos de FDDI 4

Tipos de Tráfico de FDDI 5

Especificaciones de FDDI 6

Método de Acceso de FDDI 6

Conclusión de FDDI 7

VPN 7

¿Qué es y cómo funciona una VPN? 7

Historia de la VPN 8

Ventajas de VPN 9

Desventajas de las VPN 10

Tipos de VPN 10

Protocolos de VPN 11

Arquitectura de las VPN 11

Ejemplos de Aplicación 12

Noticias 13

Conclusiones de VPN 13

Bibliografía 17

FDDI

¿Qué es FDDI?

Fiber Distributed Data Interfaces es un conjunto de estándares ANSI e ISO para la transmisión de datos en líneas de fibra óptica en redes de área local (LAN) que se pueden extender hasta un radio de unos 200 km.

Historia de FDDI

Comenzó a ser desarrollado a mediados de los años ochenta, en 1983, por la comisión normalizadora ANSI X3T9.5 para generar una alternativa a las tecnologías Ethernet y Token Ring que habían llegado a sus límites posibles. Cada una de sus especificaciones fue diseñada y mejorada hasta culminar con SMT en 1994.

En la actualidad, debido a sus superiores velocidad y coste, se prefiere utilizar fast Ethernet y Gigabit Ethernet, en lugar de FDDI.

Generalidades de FDDI

Una red de Interfaz de Datos Distribuidos por Fibra (FDDI) proporciona conexiones de alta velocidad para varios tipos de redes. Fue diseñado para su uso en equipos que requieren velocidades de más de 10 Mbps disponibles de Ethernet o los 4 Mbps disponibles de Token Ring.

Se encuentra formada por dos flujos de datos similares que fluyen en direcciones opuestas por dos anillos: existe uno primario y otro secundario. Si hay un problema con el anillo primario, como el fallo del anillo o una rotura del cable, el anillo se re-configura a sí mismo transfiriendo datos al secundario, que continúa transmitiendo.

Composición de FDDI

Una red FDDI está formada por dos flujos de datos similares que fluyen en direcciones opuestas por dos anillos.

FDDI puede ser implementada en dos formas básicas: como un **anillo dual** y como un **anillo basado en concentradores**.

En el escenario del anillo dual, las estaciones son conectadas directamente unas con otras. El diseño del anillo dual FDDI proporciona seguridad en el caso de que los nodos caigan. Si cualquier nodo falla, el anillo se re-configura alrededor del nodo que ha fallado. Sin embargo, una limitación del diseño del anillo dual es que dos nodos fallen, el anillo se ha roto en dos lugares, creando efectivamente dos anillos separados. Los nodos en un anillo son después aislados de otros nodos del anillo.

Características	Descripción
Método de acceso	Paso de testigo
Velocidad de transferencia	Fibra óptica de 155 Mbps a 622 Mbps

Topología de anillo doble paralelo:

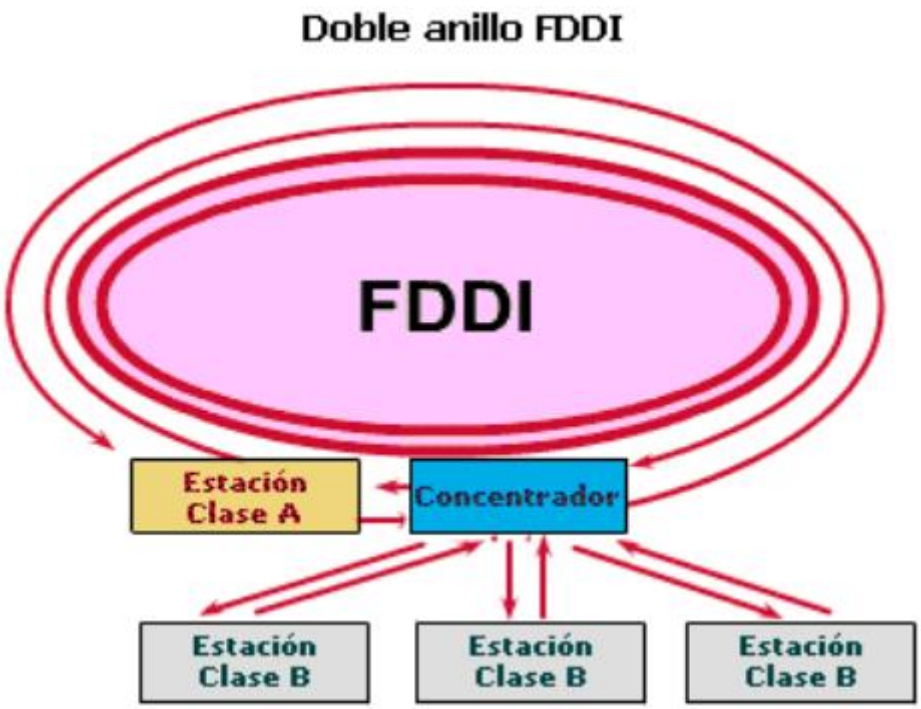
▪ Rotación de los datos en sentidos inversos.

▪ Al anillo primario se le denomina "A", y "B" al secundario.

▪ El anillo A es usado normalmente por los datos que viajan a través de la red.

▪ El anillo secundario es utilizado como backup, en caso de algún fallo en el anillo A, de una forma totalmente automática, y sin intervención por parte del usuario.

Las estaciones conectadas a la red FDDI pueden ser SAS (SingleAttached Station), DAS (Dual-Attached Station), SAC (Single-Attached Concentrator) o DAC (Dual-Attached Concentrator). Las estaciones FDDI de clase A (DAS o DAC), usan ambos anillos, ya que tienen la capacidad de re-configurarse en caso de interrupción del servicio en el primer anillo. Por el contrario, las estaciones de clase B (SAS y SAC), sólo pueden enlazarse al anillo primario, como solución de conexión de bajo coste, en caso de equipos en los que no es crítica la interrupción del servicio. Por lo general se emplea un DAC para interconectar múltiples estaciones SAS.



Otro camino relativo a este problema es usar **concentradores** para construir redes . Los concentradores son dispositivos con múltiples puertos donde los nodos FDDI son conectados. La función de los concentradores FDDI es similar a los hubs de Ethernet o las unidades de múltiple acceso (MAU's) de Token Ring. Los nodos son conectados al concentrador, el cual aísla los fallos cuando ocurre en estas estaciones finales. Con un concentrador, los nodos pueden ser activados o desactivados. Los concentradores hacen a las redes FDDI más fiables y también proporcionan funciones de manejo SNMP. Por esta razón, muchas de las redes FDDI actuales están construidas con concentradores.

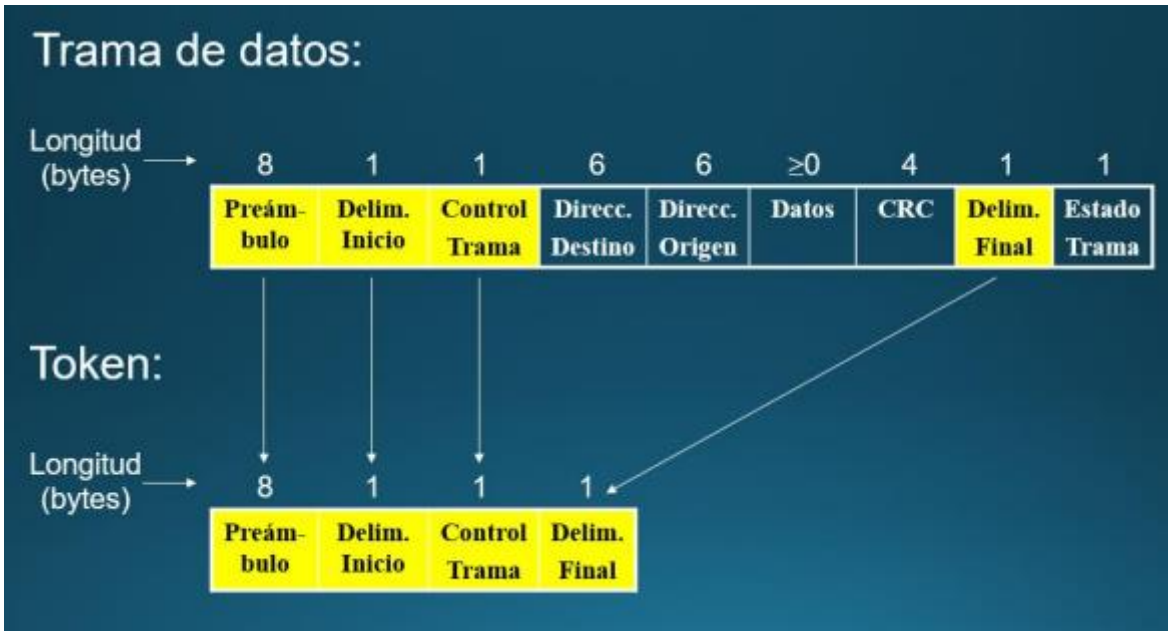
Trama de Datos de FDDI

Formato de la trama FDDI

Las tramas en la tecnología FDDI poseen una estructura particular. Cada trama se compone de los siguientes campos:

- **Preámbulo:** prepara cada estación para recibir la trama entrante.
- **Delimitador de inicio:** indica el comienzo de una trama, y está formado por patrones de señalización que lo distinguen del resto de la trama.
- **Control de trama:** indica el tamaño de los campos de dirección, si la trama contiene datos asíncronos o sincrónico y otra información de control.
- **Dirección destino:** contiene una dirección unicast (singular), multicast (grupal) o broadcast (cada estación); las direcciones destino tienen 6 bytes (por ejemplo, Ethernet y Token Ring).
- **Dirección origen:** identifica la estación individual que envió la trama. Las direcciones origen tienen 6 bytes (como Ethernet y Token Ring).
- **Datos:** información de control, o información destinada a un protocolo de capa superior.
- **Secuencia de verificación de trama (FCS):** la estación origen la completa con una verificación por redundancia cíclica (CRC) calculada, cuyo valor depende del contenido de la trama (como en el caso de Token Ring y Ethernet). La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado durante el tránsito. La trama se descarta si está dañada.
- **Delimitador de fin:** contiene símbolos que no son datos que indican el fin de la trama.

- **Estado de la trama:** permite que la estación origen determine si se ha producido un error y si la estación receptora reconoció y copió la trama.



Tipos de Tráfico de FDDI

¿Cómo funciona?

El método de acceso de FDDI es similar al método de acceso de Token Ring, y "Token" se usa en la comunicación de red. Se diferencia del token ring estándar en que FDDI utiliza un método de acceso de token temporizado.

Los tokens FDDI se mueven de un nodo a otro a lo largo de un bucle de red. Si un nodo no necesita transmitir datos, FDDI obtiene el token y lo envía al siguiente nodo.

Si el nodo que procesa el token necesita transmitir, puede enviar tantas tramas como necesite el usuario durante un tiempo específico llamado "Tiempo de ciclo de token de destino" (Target Token Rotation Time, TTRT).

La FDDI acepta la asignación en tiempo real del ancho de banda de la red, lo que la hace ideal para varios tipos de aplicación. La FDDI proporciona esta ayuda mediante la definición de dos tipos de tráfico: sincrónico y asíncrono. El tráfico sincrónico puede consumir una porción del ancho de banda total de 100 Mbps de una red FDDI, mientras que el tráfico asíncrono puede consumir el resto.

Existen dos tipos de tráfico:

▪ **Síncrono:** capacidad de transmisión continua

El ancho de banda sincrónico se asigna a las estaciones que requieren una capacidad de transmisión continua, en tiempo real. Esto resulta útil para transmitir información de voz y vídeo. El ancho de banda restante se utiliza para las transmisiones asíncronas.

▪ **Asíncrono.** Permite el uso de prioridades.

El ancho de banda asíncrono se asigna utilizando un esquema de prioridad de ocho niveles. A cada estación se asigna un nivel de prioridad asíncrono.

FDDI también permite diálogos extendidos, en los cuales las estaciones pueden usar temporalmente todo el ancho de banda asíncrono.

El mecanismo de prioridad de la FDDI puede bloquear las estaciones que no pueden usar el ancho de banda sincrónico y que tienen una prioridad asíncrona demasiado baja.

Especificaciones de FDDI

FDDI tiene cuatro componentes claves, el control de acceso al medio (MAC), la capa física (PHY), la capa dependiente del medio físico (PMD), y la capa de manejo de estación (SMT).

Como bien sabemos, FDDI es un protocolo de la capa de enlace, esto significa que los protocolos de las capas más altas operan independientemente del protocolo FDDI. Las aplicaciones van usando los protocolos desde las capas más altas hasta la capa de control de enlace lógico, en el mismo sentido que lo pueden hacer en Ethernet o Token Ring. Pero debido a que FDDI usa un protocolo de capa física distinto al de Ethernet o Token Ring, el tráfico debe ser puenteado o enrutado fuera del anillo FDDI. Además FDDI también permite paquetes de mayor longitud que las redes de baja velocidad; por esta razón, las conexiones entre una FDDI y LAN Ethernet o Token Ring requieren de fragmentación o reensamblado de tramas.

- La capa **MAC (control de acceso al medio)** define el direccionamiento, planificación, y enrutado de datos. También se comunica con los protocolos de las capas más altas, tales como TCP/IP, SNA, IPX, DECnet, DEC LAT, y Appletalk. Esta capa acepta mensajes de hasta 9000 símbolos que provengan de los protocolos de las capas superiores, agregándolos a la cabecera MAC, y luego pasándolos en paquetes de hasta 4500 bytes a la capa física. Algunas de sus tareas incluye el manejo del formato de trama, tratamiento del token, direccionamiento, aplicación del algoritmo para calcular una verificación por redundancia cíclica y mecanismos de recuperación de errores.
- La capa física **(PHY)** maneja la codificación y decodificación de paquetes de datos en flujos de símbolos. También maneja la sincronización del reloj en el anillo FDDI y el manejo del entramado.
- La capa **PMD (dependiente del medio físico)** maneja la transmisión analógica en banda base entre los nodos del medio físico. El estándar PMD incluye TP-PMD para par trenzado de cobre y Fiber-PMD para cable de fibra óptica. Sus tareas incluyen la gestión de enlaces de fibra óptica, niveles de energía, tasas de error en bits, componentes ópticos y conectores.
- La capa de **SMT (manejo de estación)** se encarga del manejo del anillo FDDI. Las funciones proporcionadas por SMT incluyen la identificación de vecinos, detección de fallos y reconfiguración, inserción y eliminación de nodos en el anillo, y la monitorización estadística del tráfico.

Método de Acceso de FDDI

El método de acceso utilizado en una red FDDI es el paso de testigo. Un equipo en una red FDDI tendrá un testigo, mientras lo tenga, transmitirá tantos paquetes como pueda producir en un tiempo predeterminado, tan pronto como un equipo haya finalizado la transmisión o después de un tiempo de transmisión predeterminado, el equipo libera el testigo. Una vez liberado el testigo, varios paquetes pueden circular por el anillo al mismo tiempo.

Este método de paso de testigo es más eficiente que el de una red Token Ring, que permite únicamente la circulación de una trama a la vez. Y proporciona un mayor rendimiento de datos a la misma velocidad de transmisión.

La velocidad de transferencia en una red FDDI se encuentra entre 155 y 622 Mbps; mientras que la velocidad de transferencia en una red Token Ring se encuentra entre 4 y 16 Mbps.

Conclusión de FDDI

Para concluir podemos decir que las redes FDDI son la evolución las redes Token Ring, aunque en realidad es la aplicación de 2 Token Ring simultáneas, las cuales se ven potenciadas por múltiples protocolos y un aumento de complejidad, esto ayuda de manera muy notoria a mejorar todas sus características, coronando a las redes FDDI como las más utilizadas para el backbone de las redes WAN pudiendo lograr una distancia de expansión de hasta 200 km.

VPN

¿Qué es y cómo funciona una VPN?

VPN significa "Virtual Private Network" (Red privada virtual) y describe la oportunidad de establecer una conexión protegida al utilizar redes públicas. Básicamente, al conectar cualquier dispositivo a una VPN, el dispositivo actúa como si estuviera en la misma red que la VPN. De este modo, todo el tráfico (o una determinada parte del tráfico) se envía cifrado y seguro por el túnel de comunicación VPN, permitiendo que se pueda disfrazar la identidad en línea. Esto le dificulta a terceros el seguimiento de sus actividades en línea y el robo de datos. El cifrado se hace en tiempo real.

Dicho en palabras sencillas : Una red privada virtual conecta un ordenador u otro dispositivo a otro ordenador (que actúa como servidor) ubicado en cualquier lugar de Internet para permitir al usuario navegar por Internet a través de su conexión a Internet.

¿Cómo funciona?

Una vez nos hayamos descargado e ingresado a nuestra VPN sucederá lo siguiente con tus datos:

1. El software VPN en tu ordenador cifra el tráfico de datos y lo envía (a través de tu proveedor de servicios de Internet) al servidor VPN a través de una conexión segura.
2. Los datos cifrados de tu ordenador son descifrados por el servidor VPN.
3. El servidor VPN enviará tus datos a Internet y recibirá una respuesta, es decir, para ti, el usuario.
4. Luego, el tráfico se te envía a ti después de que el servidor VPN lo cifre de nuevo.
5. El software VPN en tu dispositivo descifrará los datos y así podrás entenderlos y usarlos.

La aplicación VPN se ejecutará en segundo plano en el dispositivo, por lo que se podrá acceder a Internet como ocurre habitualmente y no se notará ninguna diferencia, salvo que será posible saltarse restricciones en línea.

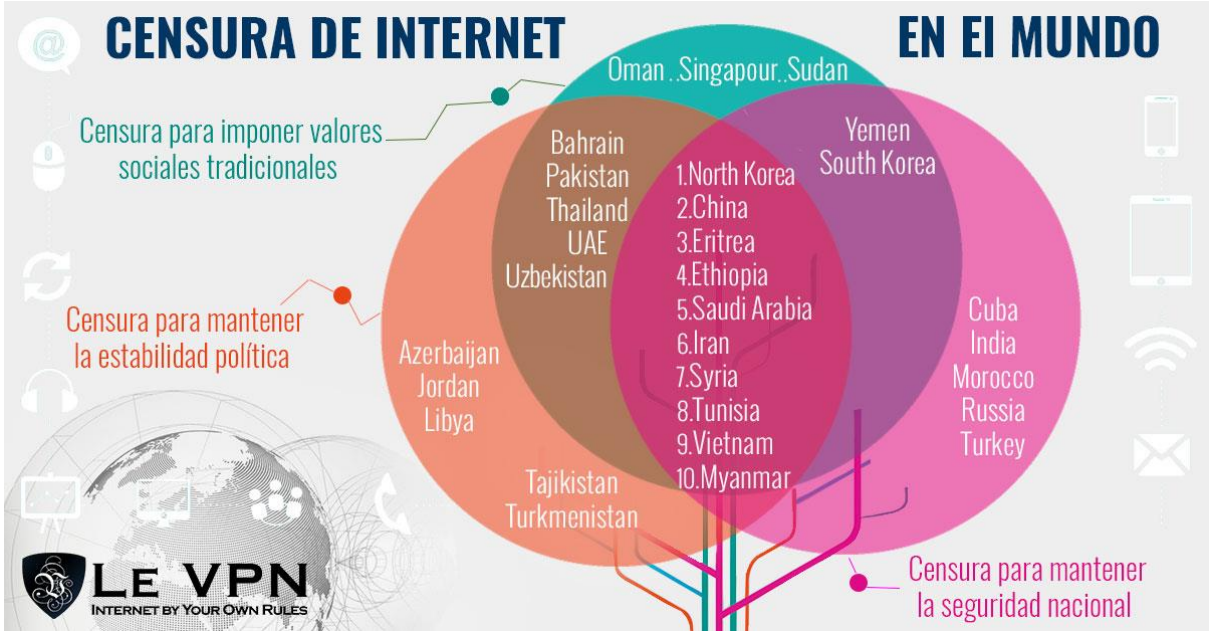
Historia de la VPN

La idea de cifrar y proteger la información que se transmite por la web no es nueva, sino que existe desde los inicios de la internet.

- Los ‘60 : Los orígenes de la VPN se remontan a la antigüedad de la Internet misma, aparecida en la década de 1960 como Arpanet, el primer sistema de redes de la historia, desarrollada por la inteligencia militar de Estados Unidos. Cumplio con el propósito principal de una VPN, conectar a otra red, aunque en sentidos de seguridad aún no se había desarrollado.
- Los ’80: Más adelante, sobre los ochenta, el conjunto de protocolos TCP/IP estableció un estándar en ese tipo de comunicación, la cual sería adoptada por la industria comercial al poco tiempo. Este intercambio de información también suponía riesgos, pues muchos enemigos políticos o simplemente hackers empezaron a causar problemas a quienes intentaban compartir datos por esta vía.
- Los ‘90: Es así que en 1993, John Ioannidis y un grupo de compañeros en la Universidad de Columbia y AT&T Bell Labs iniciaron el camino para la creación de un protocolo de encriptación de IP de Software, conocido como Swipe. Esta es el primer modelo de VPN con protocolos de seguridad como se conocen hoy en día. Esta creación fue mejorada al año siguiente por Xu Wei, que redobló la seguridad, mejorando el protocolo actual, preparándolo para la autenticación y cifrado de paquetes de información que se compartan en línea, así nació el protocolo IPSec. En 1996, un empleado de Microsoft llamado Gurdeep Singh-Pall creó un Peer-to-Peer Tunneling Protocol (PPTP). Durante este tiempo, el crecimiento de internet era cada vez mayor por lo que surgía la necesidad de sistemas de seguridad más sofisticados, si bien los antivirus eran eficaces para impedir malware y spywares, las personas y principalmente las empresas,ya que eran éstas últimas quienes quedaban más vulnerables ante ataques, comenzaban a exigir cifrado de software para ocultar su identidad en la búsqueda de internet.
- Los 2000 : Es así que las primeras VPN comenzaron a principios de los 2000, pero eran utilizadas casi de manera exclusiva por las empresas. Una vez se asentó su uso para las grandes empresas, comenzó a comercializarse a mayor escala para los usuarios, esto sucedió a partir del 2010 y al pasar del tiempo se vuelven más famosas entre los

usuarios principalmente por el hecho de superar las censuras regionales como por ejemplo, los servicios de transmisión de videos como Netflix o YouTube dan acceso a ciertos videos en ciertos países solamente.

Según GlobalWebIndex, el número de usuarios de VPN en todo el mundo se cuadruplicó entre 2016 y 2019. En China, Tailandia, Indonesia y otros países en los que el gobierno censura o restringe el uso de internet, uno de cada cinco usuarios de internet usa una VPN.



Ventajas de VPN

Una conexión VPN disfraza sus datos en línea y los protege del acceso externo. Cualquiera que tenga acceso a la red y quiera hacerlo puede ver los datos no cifrados. Con una VPN, los hackers y los cibercriminales no pueden descifrar estos datos.

- Cifrado seguro: Para leer los datos, necesita una clave de cifrado. Sin ella, le llevaría millones de años a una computadora descifrar el código en caso de un ataque de fuerza bruta. Con la ayuda de una VPN, sus actividades en línea se ocultan incluso en redes públicas. Es por esto que ofrece más seguridad ya que hará que sea mucho más difícil para los hackers u otros interceptar y ver tu información personal.
- Disfrazar su paradero: los servidores de VPN principalmente actúan como sus servidores proxy en internet. Debido a que los datos de ubicación demográficos provienen de un servidor en otro país, su ubicación real no se puede determinar. A esto se suma que, en la mayoría de los casos, los proveedores de estos servicios no guardan registros sobre sus actividades. Por otra parte, algunos proveedores registran su comportamiento, pero no transmiten esa información a terceros. Esto significa que cualquier registro potencial de su comportamiento de usuario permanece oculto de manera permanente. Ofrece más privacidad, ya que tomará los datos de la VPN ocultando la dirección IP real.
- Acceso a contenido regional: el contenido web regional no siempre es accesible desde cualquier parte. Los servicios y los sitios web a menudo contienen contenido que solo puede accederse desde ciertas partes del mundo. Las conexiones estándar utilizan servidores locales en el país para determinar su ubicación. Esto significa que no puede acceder al contenido en casa mientras viaja, y no puede acceder a contenido internacional desde casa. Con la suplantación de ubicación de VPN, se puede cambiar a un servidor a otro país y “cambiar” su ubicación de manera eficaz. Evita censura regional, permitiendo navegar con más libertad.

- Transferencia segura de datos: si trabaja de forma remota, puede necesitar acceder a archivos importantes en la red de su empresa. Por razones de seguridad, este tipo de información requiere una conexión segura. Para obtener acceso a la red, a menudo se requiere una conexión VPN. Los servicios de VPN establecen conexiones con servidores privados y utilizan métodos de cifrado para reducir el riesgo de filtración de datos. Ofrece más seguridad.

Desventajas de las VPN

Esta herramienta puede tener desventajas y es importante conocerlas:

- La velocidad de navegación puede ser más lenta, por lo que las velocidades de descargas son inferiores, lo que puede deberse a la distancia del servidor VPN a donde se desea conectar.
- Hay cierto riesgo que se corre al utilizar VPN gratuitas, desde el punto de vista de seguridad informática.
- Si el dispositivo donde se utiliza la VPN se encuentra infectado con algún virus de rastreo o robo de información, la VPN no protegerá.
- El uso de VPN puede ser ilegal en algunos países.
- Permite ocultar el historial de navegación, lo que podría ser utilizado con motivos maliciosos al mantener anonimato.

Tipos de VPN

Los servicios de redes privadas virtuales se dividen en cuatro tipos:

- **VPN Personales**: se utilizan para crear conexiones seguras y privadas en el internet abierto y para esquivar firewalls y las restricciones geográficas de internet
- **VPN de Acceso Remoto**: utilizada por empleados para que puedan acceder a la red privada de la empresa cuando viajan o trabajan en remoto
- **VPN móviles**: se utiliza cuando el usuario no dispone de una conexión a internet consistente o estable
- **VPN de sitio a sitio**: utilizado por las empresas que cuentan con varias sedes, o aquellas empresas que intentan conectarse a una misma red privada.

	VPN de Acceso Remoto	VPN Personal	VPN Móvil	VPN de Sitio a Sitio
¿Quién se conecta y adónde?	El usuario se conecta a una red privada.	El usuario se conecta a internet a través de un servidor de terceros.	El usuario se conecta a una red privada.	La red se conecta a otra red.
¿Qué software se necesita?	Los usuarios tienen que instalar un software en su dispositivo o configurar el	Los usuarios instalan el software de un servicio de VPN en el dispositivo.	Los usuarios tienen que instalar un software en su dispositivo o configurar el	Los usuarios no necesitan un software adicional.

	sistema operativo.		sistema operativo.	
Uso recomendado	Conectarte a la red de tu empresa (o a cualquier otra red privada) desde casa o desde otra ubicación remota.	Proteger tu privacidad y evitar las restricciones geográficas en línea.	Conseguir una conexión estable a una red privada utilizando una conexión a internet inestable.	Unir dos o más redes para crear una red única combinada.

Protocolos de VPN

- **OpenVPN**: es una tecnología de código abierto que utiliza la biblioteca de OpenSSL y los protocolos TLS, junto con otras tecnologías, para proporcionar una solución VPN sólida y confiable. Es el protocolo estándar de la industria. Su punto fuerte es que puede ser altamente configurable y que se encuentre en la mayoría de las plataformas a través de software de terceros.
- **IPSec/L2TP** (Seguridad del Protocolo de Internet/ Layer 2 Tunneling Protocol): Internet Protocol Security o IPSec asegura la comunicación del Protocolo de internet mediante la autenticación de la sesión y encripta cada paquete de datos durante la conexión. IPSec funciona en dos modos:
    - modo de transporte: encripta el mensaje en el paquete de datos
    - modo de túnel: encripta todo el paquete de datos
- **SSTP** (Secure Socket Tunneling Protocol): incluye la capacidad de usar el puerto TCP 443 para evadir la censura. La estrecha integración con Windows puede hacer que sea más fácil de usar y más estable que OpenVPN en esa plataforma.
- **PPTP** (Protocolo de túnel punto a punto): Crea un túnel y encapsula el paquete de datos. Utiliza un protocolo punto a punto (PPP) para cifrar los datos entre la conexión. PPTP es uno de los protocolos VPN más utilizados y ha estado en uso desde la época de Windows 95.
- **IKEv2** (Intercambio de Claves por Red versión 2): El protocolo de intercambio de claves de Internet versión 2 (IKEv2) establece y mantiene dinámicamente un estado compartido entre los puntos finales de un datagrama IP. IKEv2 realiza la autenticación mutua entre dos partes y establece la Asociación de Seguridad IKEv2 (SA).

Arquitectura de las VPN

Dentro de las posibles arquitecturas que encontramos dentro de las VPN se pueden mencionar las siguientes:

- Proporcionada por un servidor de Internet: El proveedor de Internet puede instalar en su oficina un dispositivo que se encargará de la creación del túnel para la organización.
- Basadas en firewalls: De la misma forma en que las VPN trabaja en los niveles más bajos del modelo OSI, el firewall actuará de la misma forma.
- Basadas en Caja Negra: Básicamente es un dispositivo con software de encriptación. No provee seguridad en la organización pero si en los datos. Para suplir esta falencia se pueden utilizar un firewall en serie o paralelo al dispositivo de VPN.
- Basadas en Routers: Puede ser en este caso que el software de encriptación se añada al router ya existente o bien que se utilice una salida exclusiva de otro proveedor.
- Basadas en acceso remoto: El cliente tiene software por el cual se conecta al servidor de VPN de la corporación a través de un túnel encriptado.
- Basadas en Software: Por lo general se utiliza de un cliente a un servidor de VPN que está instalado en alguna estación de trabajo. Es necesario tener procesos de administración de claves y un emisor de certificados.

Ejemplos de Aplicación

- Teletrabajo
    - Las VPN sirven para proteger la información que se intercambia entre terminales y servidores, a través de un túnel de comunicación segura entre el ordenador que se está usando (cliente) y el terminal o servidor de la empresa. El nivel de protección se consigue gracias a distintas técnicas de cifrado que tratan de garantizar la integridad y confidencialidad de los datos. Al establecer la conexión, se está permitiendo a un equipo ajeno a la empresa tener conexión directa con la red empresarial.

- Intercambio de archivos por P2P
    - Un servidor VPN P2P se encarga de enrutar su actividad a través de un túnel de cifrado antes de que llegue a Internet, de modo que nadie puede ver lo que está haciendo, incluso cuando está descargando un archivo grande de varias fuentes que lo alojan.
    - El bloqueo de las redes P2P ayuda a las empresas y a los servicios de streaming a controlar qué contenidos son visibles en línea; también pueden utilizar prácticas como el geobloqueo. Proteger las redes P2P con VPN dedicadas a P2P es fundamental para que Internet siga siendo un espacio abierto y seguro para que la gente comparta ideas y contenidos.

    - **¿Cuáles son las ventajas de una VPN P2P?**

      El P2P es seguro con una VPN porque las ventajas de la codificación mitigan los riesgos y las restricciones asociadas al P2P.

      El uso de «torrent» puede exponer su red a archivos de fuentes anónimas. Asimismo, un ISP puede detectar fácilmente la actividad P2P y restringir el ancho de banda. Por eso una VPN P2P es esencial para mantener la privacidad y la seguridad.

      La tunelización de la VPN no solo oculta la actividad P2P a su proveedor de servicios de Internet (y reduce así las posibilidades de estrangulamiento del ancho de banda), sino que también cifra cada parte del archivo grande que se envíe y reciba para aumentar la seguridad.

- Censura
    - Algunas plataformas a las que nos conectábamos discriminaba por IPs, ahora son los proveedores de conexión de un determinado país (en el que nos encontramos en el momento de acceder a la web en cuestión) quienes bloquean masivamente cualquier intento de acceder a la misma.
    - En cualquier caso, la solución es usar un punto de conexión situado en otro país, nuestra IP quedará enmascarada, y podremos conectarnos sin problemas a la web bloqueada.

Noticias

- Neutralidad de Red
    - La no discriminación de los paquetes de datos en la red llegó a su fin, a pesar de ser uno de sus principios fundamentales. El crecimiento del streaming hace que la gestión del tráfico sea ineludible y hasta deseable, aunque en ocasiones las necesidades técnicas se chocan contra los derechos de los usuarios. Hoy vivimos en un esquema autorregulado, que funciona a favor del consumidor, aunque con discusiones pendientes.
- Irán
    - Las autoridades iraníes están a punto de "criminalizar" la venta de redes privadas rápidas, o VPN, utilizadas para eludir las restricciones impuestas a internet, dijo el miércoles el ministro de Telecomunicaciones de Irán, país sacudido por las protestas provocadas por la muerte de la joven Mahsa Amini.

Conclusiones de VPN

Una VPN es tan segura y útil como su proveedor. Si no confías en tu VPN, no la uses, ya que en lugar de un ISP sería la VPN misma que monitoree absolutamente todo lo que haces en Internet.

Cosas a tener en cuenta

- El precio**:** Aunque hay servicios VPN gratuitos para enmascarar nuestra IP y navegar “anónimamente”, estos son lentos y no deberíamos confiar mucho en ellos.
- **La velocidad:** Si el servidor VPN está muy lejos, experimentarás mucha latencia a la hora de navegar por la red. Además de latencia, es normal que la velocidad de descarga y subida máxima estén limitadas.
- Su **seguridad** no es confiable, especialmente si estamos hablando de conexiones VPN basadas en el protocolo PPTP.
- No siempre pueden **falsear tu ubicación.** Especialmente en el móvil, cada vez hay más tecnologías por las cuales se puede triangular y aproximar tu ubicación más allá de tu dirección IP.
- **No te proporcionan privacidad**. Usar una VPN no supone que la navegación sea anónima. La combinación ganadora para un mayor anonimato, podríamos usar una conexión VPN y Tor.

Problemas de seguridad

Es indispensable en una VPN generar una transmisión de datos que sea segura, en el caso del protocolo TCP/IP en particular se creó para que se tenga un alto grado de confiabilidad en la transmisión de los datos pero no a nivel seguridad, los paquetes en Internet viajan sin

encriptación alguna con lo cual no hay una privacidad (Sniffing) ni control de suplantación (Spoofing) de los datos que se transmiten por la misma.

Los problemas de seguridad que encontramos son los siguientes:

Escuchas clandestinas de datos (Sniffing).

Normalmente los dispositivos de una red solo toman los paquetes que le corresponden, el sniffing es una técnica por la cual una máquina de una red toma todos los paquetes que circulan por ella más allá de que estén destinados o no para ella, accediendo de esa forma a toda la información que circule por la red.

Suplantación de datos (Spoofing).

En esta técnica una terminal emula a otra. El usuario fuerza a la computadora a tomar los certificados de otra. De esta forma está capacitada para enviar mensajes a un dispositivo teniendo la posibilidad de acceder a una red a la cual no pertenezca y enviando mensajes que para las demás estaciones de trabajo parecen legítimos.

Captura de direcciones.

Los paquetes que se transmiten contienen información en los encabezados y en el cuerpo que pueden ser direcciones de servidores, DNS, proxys, estaciones de trabajo y de todos los dispositivos de red.

Hijacking.

La comunicación en VPN se realiza por una sesión. El hijacking consiste en tomar el control de la sesión y de esa forma ingresar en la VPN.

Para solucionar estos problemas de seguridad mencionados anteriormente podemos emplear técnicas de encriptación, autenticación y validación. Algunas de ellas pueden ser las siguientes:

Autenticación de usuario: Se deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados solamente. También es conveniente llevar registros de quienes entran en la VPN y los horarios en que lo hacen.

Administración de dirección: Se deberá asignar una dirección al cliente en la red privada, y asegurarse de que las direcciones privadas se mantengan así.

Encriptación de datos: Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red para lo cual se usan técnicas de encriptación detalladas en este mismo trabajo. Entre las tareas en la encriptación de datos esta la de generar y renovar las llaves de encriptación para el cliente y para el servidor.

Soporte de protocolo múltiple: La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen Protocolo de Internet. Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto (PPTP) o un Protocolo de túnel de nivel 2 (L2TP) cumple con todos estos requerimientos básicos, y aprovecha la amplia disponibilidad de Internet a nivel mundial.

Preguntas

1. **¿En qué año comenzó a ser desarrollado FDDI?**

   Comenzó a ser desarrollado en 1983 y terminó de ser culminado en 1994

2. **¿Es usado en la actualidad FDDI?**

   En la actualidad se prefiere utilizar Fast Ethernet y Gigabit Ethernet

3. **¿Cuántos anillos conforman la estructura de FDDI? ¿En qué dirección transportan la información?**

   Se encuentra conformado por dos anillos, cuyos flujos de datos similares que fluyen en direcciones opuestas, existe uno primario y otro secundario.

4. **¿Qué ocurre cuando el anillo primario falla?**

   Si hay un problema con el anillo primario, como el fallo del anillo o una rotura del cable, el anillo se re-configura a sí mismo transfiriendo datos al secundario, que continúa transmitiendo

5. **En la Trama de Datos de FDDI como se llama el campo que identifica la estación individual que envió la trama?**

   Dirección Origen

6. **¿Qué tipos de Tráfico existen en FDDI?**

   Síncrono y Asíncrono

7. **En la Trama de Datos de FDDI, ¿qué hace el Control de trama?**

   Indica el tamaño de los campos de dirección, si la trama contiene datos asíncronos o sincrónicos y otra información de control.

8. **Nombre y defina brevemente las especificaciones de FDDI.**

   - MAC (control de acceso al medio): Define el direccionamiento, planificación, y enrutado de datos.
   - PHY (Capa física): maneja la codificación y decodificación de paquetes de datos en flujos de símbolos.
   - PMD (dependiente del medio físico): maneja la transmisión analógica en banda base entre los nodos del medio físico
   - SMT (manejo de estación): se encarga del manejo del anillo FDDI

9. **¿Cómo funcionan las VPN?**

   Una red privada virtual conecta un ordenador u otro dispositivo a otro ordenador (que actúa como servidor) ubicado en cualquier lugar de Internet para permitir al usuario navegar por Internet a través de su conexión a Internet.

10. **¿Las VPN corren en primer o segundo plano? ¿ Interfiere con el uso normal del dispositivo?**

    La aplicación VPN se ejecutará en segundo plano en el dispositivo, por lo que se podrá acceder a Internet como ocurre habitualmente y no se notará ninguna diferencia, salvo que será posible saltarse restricciones en línea

11. **¿Cuáles tipos de VPN existen?**

    Acceso remoto, Acceso sitio a sitio, Acceso Móvil, Acceso Personal

12. **¿Cuáles son los principales protocolos de VPN?**

    OpenVPN, IPSec/L2TP, SSTP, PPTP, IKEv2

13. **¿Cuál es su ventaja principal?**

    Permite ocultar nuestra identidad, trayendo como consecuencia más seguridad y privacidad.

14. **¿Cuál es su principal desventaja?**

    Se corre un riesgo en seguridad al utilizar VPN gratuitas

15. **Nombre 3 usos comunes de las VPN**

    Teletrabajo, Intercambio de archivos por P2P, evitar censura.

VOIP +h323 + sip

Índice **¡Error! Marcador no definido.**

Consigna 17

Desarrollo de la actividad 17

VOIP 17

VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS. 18

VoIP Retardo. 18

CAUSAS DEL DELAY. 18

Jitter. 19

JITTER: BUFFER ADAPTATIVO. 19

Pérdida de Paquetes. 20

CODIFICACIÓN DE LA VOZ: OTROS ASPECTOS. 20

LATENCIA. 20

PARÁMETROS DE LA VOZ. 21

Calidad de la Voz VSQ. 21

PROTOCOLOS VOIP. 22

TRANSPORTE DE INFORMACIÓN EN TELEFONÍA IP. 23

REAL TIME TRANSPORT PROTOCOL 24

PROTOCOLO RTCP (REAL TIME CONTROL PROTOCOL). 26

SEÑALIZACIÓN Y CONTROL DE LLAMADA H.323 y SIP 27

PROTOCOLO DE SEÑALIZACIÓN H.323 28

EL ESTABLECIMIENTO DE LLAMADAS EN H.323. 31

PROTOCOLO DE SEÑALIZACIÓN SIP 32

SERVIDORES DE REDIRECCIÓN. 33

SERVIDORES PROXY. 34

SERVIDORES DE REGISTRO. 34

Bibliografía consultada **¡Error! Marcador no definido.**

Consigna

Desarrollo de la actividad

VOIP

IP ha tenido su origen en transmisión de datos y no estaba adaptada a la transmisión de voz e imágenes. La tecnología de transmisión de paquetes, en la que está basada IP, ofrece tamaño

de celdas variable, que en comparación con tecnologías de tamaño de celda fija como ATM, introduce ineficiencias y necesidad de proceso extra. IP es un protocolo que en principio ofrece un tipo de calidad de servicio (QoS) basado en proporcionar el mejor rendimiento posible en el enlace disponible. (Best Effort)

VoIP es una tecnología que permite enviar y recibir llamadas o videollamadas por internet. Recopila la voz humana para codificarla en datos digitales y mandarla a otro dispositivo que los traduce de nuevo en voz, en tiempo real. Su nombre proviene del inglés voice over IP y significa «voz sobre protocolo de internet».

La configuración de las llamadas VoIP permite que estas se realicen con teléfonos o celulares y también por medio de computadoras, laptops o adaptadores telefónicos. Se puede realizar entre dos o más dispositivos conectados a la red. Entre las aplicaciones más populares que utilizan esta tecnología están WhatsApp, Messenger de Facebook, Telegram, Skype y Zoom, entre otras.

Existen además proveedores de VoIP privados que ofrecen más funciones y ventajas que las de uso común, como una red más segura que protege el servicio de software maliciosos, robos de base de datos, intentos de hackeo de las cuentas y fraudes.

VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS.

■ Retardos de los paquetes: una red IP no asegura el retardo de un paquete. Solamente a través del control y gestión global extremo a extremo, y la disponibilidad de suficiente ancho de banda, así como la tecnología de switching-routing necesaria, es posible asegurar unos niveles de retardo máximos.

■ Jitter: es muy dependiente del retardo de los paquetes, y consiste en el tiempo de variación en la llegada de paquetes. Este parámetro tiene los mismos problemas y dificultades que el retardo, por lo que las soluciones van en la misma línea.

■ Pérdida de paquetes: al estar basados sobre UDP, (una transmisión no fiable) las pérdidas de paquetes pueden llegar a ser importantes si existe congestión o problemas en la transmisión.

VoIP Retardo.

El retardo produce dos problemas:

■ La presencia de Eco

■ Talking Overlap

El eco es causado por la reflexión de la señal de voz del que habla y que vuelve a su oído. Es producida por las desadaptaciones en el terminal receptor del equipo lejano. Se convierte en un problema importante cuando el retardo de ida y vuelta es mayor a 50 mseg. Como el eco es percibido como problema significativo desde el punto de vista de la calidad, se debe corregir con la utilización de canceladores de eco. La presencia de Eco - Talking Overlap (Solapamiento de hablantes) Se produce cuando los dos interlocutores hablan simultáneamente, particularmente cuando uno está hablando y el otro se superpone. Se convierte en un problema importante cuando el retardo extremo a extremo es mayor a 150 mseg.

Por esto, el retardo “end to end”, es el mayor condicionante para el diseño de una red de VoIP, para asegurar un nivel de calidad acorde a los requerimientos de los clientes.

CAUSAS DEL DELAY.

■ Demora de trama (demora de algoritmo o de acumulación)

■ Demora de procesamiento (depende del hardware)

■ Demora de red.

Es causada por el modo de operación de los codificadores de voz. Estos requieren una o más tramas completas de muestra por lo que es necesario un “buffering”. Esto implica cierta demora inevitable, y que es inherente al proceso de codificación. El codificador acorde a la norma G.729 CS-ASELP que comprime la voz a 8 Kbits/seg introduce un retardo de 10 mseg. Es el tiempo que toma el codificador en “analizar” la voz, esto es, la toma de las muestras de voz, más el tiempo que consume el decodificador en reconstruirla y es dependiente del hardware. Esta demora es causada por el medio físico de la red, de la capacidad de los links de la misma y los protocolos usados en la transmisión de la VoIP y además por los buffers utilizados para remover el jitter en el extremo receptor. Es una parte significativa en la suma de la demora total extremo a extremo.

Jitter.

Es la variación del tiempo de arribo de los frames del codec. Se producen por los distintos caminos que puede tomar el paquete al cruzar la red y afecta la calidad. Si la muestra entra en el buffer introduce retardo y si no entra en el buffer afecta por el descarte de paquetes. Para contrarrestarlo se utilizan Buffers Anti-jitter Adaptativos: el Gateway sensa el Jitter de la red (RTP) y ajusta el tamaño del “de-jitter buffer” para compensar las diferencias de tiempo de arribo de paquetes. Esto afecta la latencia pues introduce retardos en la red.

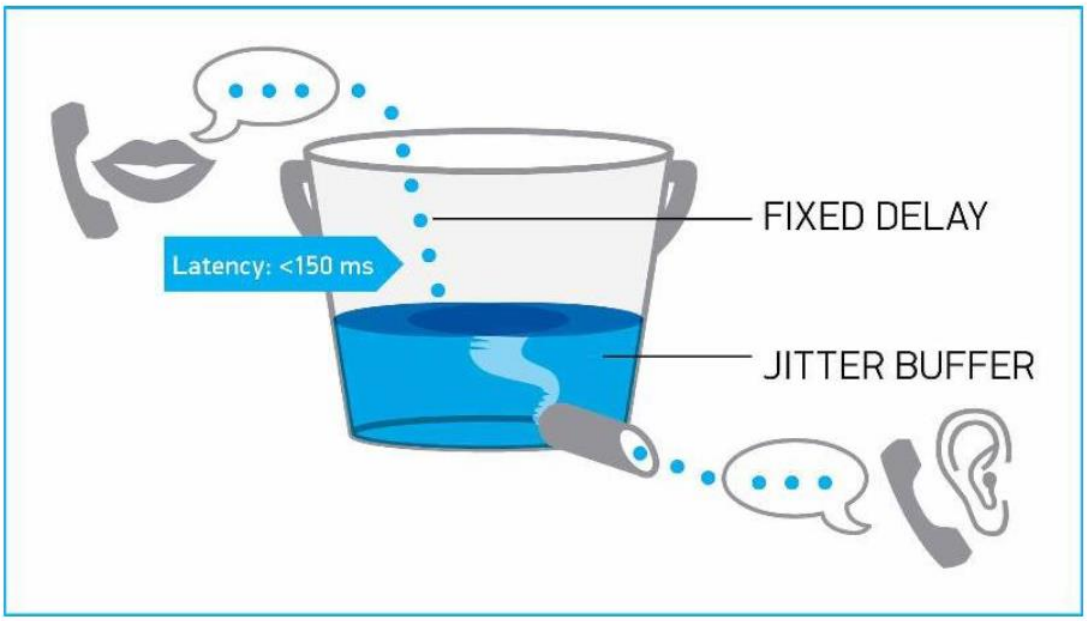
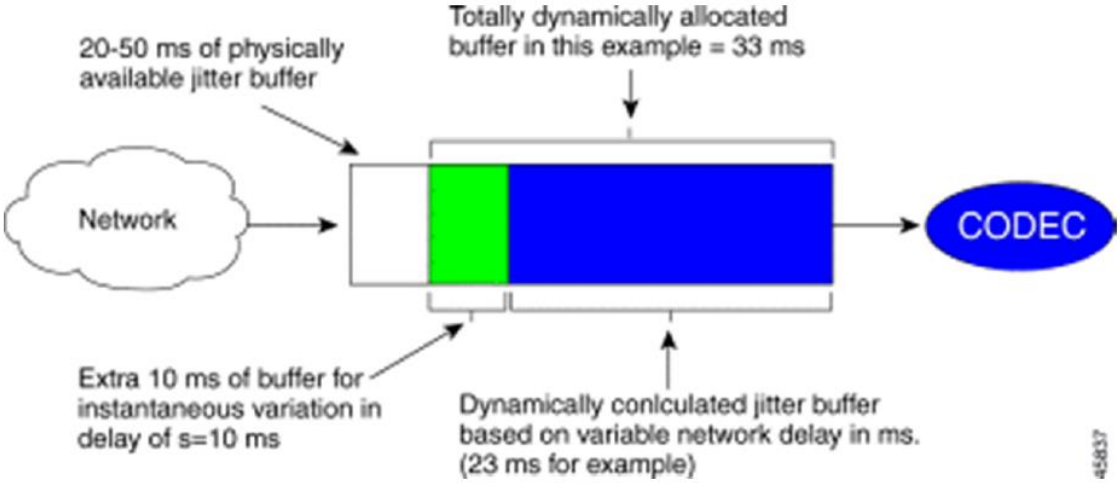


Ilustración 3 Buffer anti jitter

JITTER: BUFFER ADAPTATIVO.

El buffer adaptativo es calculado dinámicamente tomando como variable el delay de la red en milisegundos.



Pérdida de Paquetes.

Al estar basado VOIP sobre UDP, (una transmisión no fiable) las pérdidas de paquetes pueden llegar a ser importantes si existe congestión o problemas en la transmisión. La pérdida de paquetes introduce tasa de error en las comunicaciones.

Se minimiza:

■ Sobredimensionando las redes de modo que no se tengan que descartar paquetes en forma preventiva en los routers (WRED)

■ Marcando los paquetes de VoIP como prioritarios (Diffserv)

El oído humano tolera no más de 1% al 3% de paquetes perdidos

CODIFICACIÓN DE LA VOZ: OTROS ASPECTOS.

Se debe tener en cuenta los “silencios” de la conversación, para una mejor explotación del ancho de banda. Para ello se emplean “algoritmos de compresión del silencio” en la codificación de voz.

Por ello se requiere la utilización de:

■ Algoritmos de detección de la actividad de voz (VAD)

■ Algoritmos de generación de ruido de confort (CNG)

La señal de voz codificada resultante se transmite con una velocidad no uniforme en función del nivel de actividad que presente la fuente generadora.

El mecanismo de compresión del silencio es crítico en las prestaciones de la codificación de voz. Una implementación inadecuada conlleva a un deterioro significativo de la inteligibilidad de la voz.

LATENCIA.

Es el retardo one-way entre ambos extremos No debe superar los 150ms para no afectar la interactividad.

Factor a considerar	Valor aproximado
Retardo en el armado del frame a codificar	2*10ms (G.729) – [Por ej G.711, 1,5ms]
Tiempo de procesamiento para la codificación de la señal (look-ahead)	5ms (G.729)
Cantidad de muestras de código por paquete IP	+10ms (2 muestras en G.729) => (m-1) *t.frame
Si se emplea VAD	+5ms
Tiempo de armado del paquete IP	Depende intefaz de salida (Eth despreciable)
Delay introducido por la transmisión del paquete IP	40ms (aprox. BBIP)
Delay introducido por el buffer anti-jitter	20ms (aprox., se adapta dinámicamente puede llegar a 50ms)
Tiempo de procesamiento de decodificación	1ms
Tiempo total (para nuestro ejemplo)	101ms (aprox.)

PARÁMETROS DE LA VOZ.

Calidad de la Voz VSQ.

La calidad de la voz (Voice Speach Quality) es evaluada por medio de dos parámetros:

■ Claridad: que refleja el grado de palabras y frases entendidas

■ Fidelidad: califica el grado de reconocimiento de la personal que habla.

La VSQ se puede medir en mediciones subjetivas o mediciones objetivas.

Las medidas objetivas de la ejecución de servicios, como la pérdida de información y el retardo contribuyen a la QoE (calidad de experiencia). Para realizar estas mediciones habitualmente se utilizan sistemas electrónicos, los cuales están basados en algoritmos y fórmulas matemáticas que miden la QoE en sistemas de IPTV, algunas de las técnicas que estos equipos electrónicos implementan son:

■ Técnicas basadas en modelos de percepción humana de vídeo.

■ Técnicas basadas en parámetros que indican el grado de deterioro de la red.

■ Técnicas basadas en el tiempo del deterioro de la señal de vídeo.

■ Técnicas basadas en los parámetros de las señales de vídeo.

Denominación	Descripción
PSQM	Perceptual Speach Quality Measure
PESQ	Perceptual Evaluation of Speach Quality
PSESQ_LQ	PSQM Listening Quality

En las mediciones subjetivas se aplica la Recomendación P.830 del ITU en la que se aplica el método Mean Option Score (MOS). Estas medidas se realizan en entornos donde participan grupos de personas, las cuales realizan un conjunto de pasos como los que se listan a continuación:

■ Elegir las secuencias de vídeo a evaluar.

■ Evaluación y calificación numérica por parte de los observadores.

■ Depuración de los observadores por fallos en el proceso.

■ Cálculo de la calidad subjetiva media, mediante el análisis estadístico de los resultados encontrados por los observadores, este valor es conocido como MOS (Mean Opinion Scale).

Score	Nivel VSQ	Descripción
5	Excelente	Muy claro, pequeño retardo y comunicación tranquila
4	Bueno	Claro, bajo retardo y comunicación tranquila con poco ruido
3	Razonable	No muy claro, nivel medio de retardo y comunicación posible
2	Pobre	No claro, alto retardo y comunicación dificultosa
1	Malo	No comprensible, muy alto retardo y comunicación bloqueada

PROTOCOLOS VOIP.

Las tecnologías "IP" hacen referencia a un conjunto de protocolos que conforman la red IP.

Los protocolos de transporte más usados son:

■ TCP: capaz de proporcionar conexiones garantizadas para paquetes de datos sobre IP

■ UDP: que proporciona un servicio de entrega no garantizado

Ninguno de estos protocolos por sí mismos pueden proporcionar el soporte de aplicaciones en tiempo real como la voz.

Existen una serie de protocolos que proporcionan servicios en tiempo real sobre IP

■ RTP (Real Time Transport Protocol)

■ RTCP (Real Time Control Protocol)

■ RSVP (Resource Reservation Protocol)

■ RTSP (Real Time Streaming Protocol)

Existen a su vez protocolos de señalización, que permiten el inicio, mantenimiento y fin de cada comunicación:

■ Modelo H.323 (solución UIT)

■ Modelo SIP (solución IETF)

■ Modelo MEGACO (H.248)

TRANSPORTE DE INFORMACIÓN EN TELEFONÍA IP.

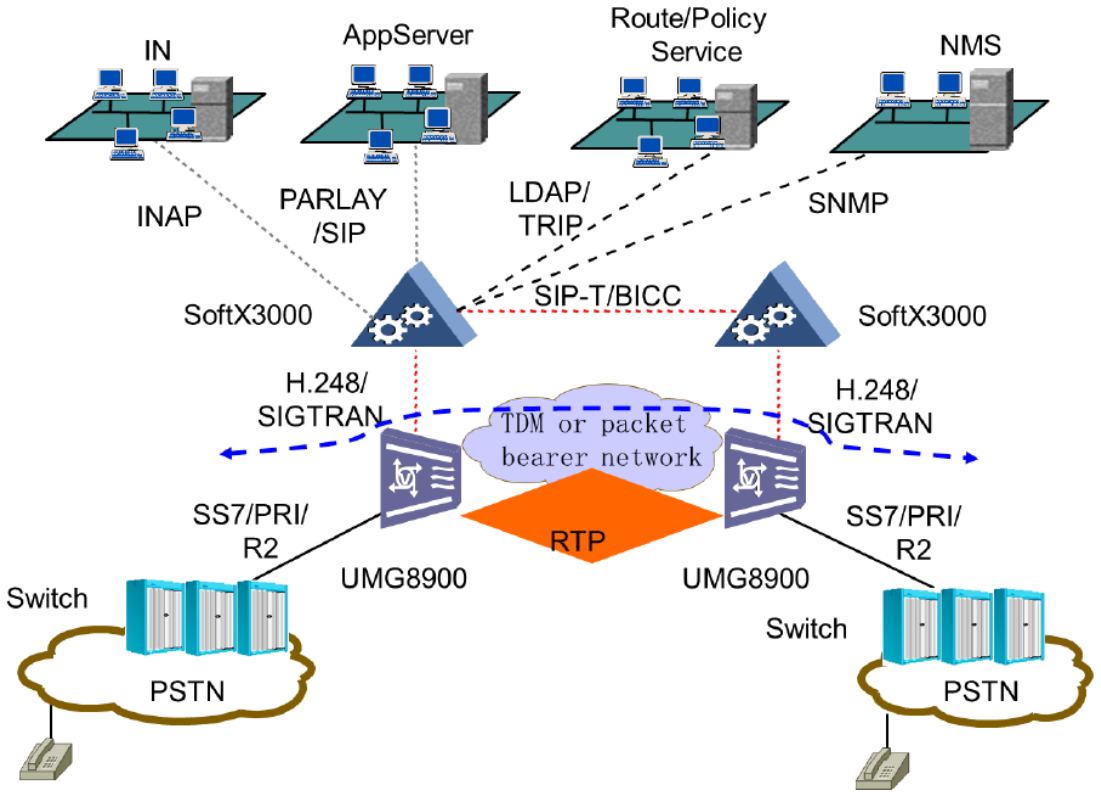
Se requiere un protocolo, o conjunto de ellos, que se ocupe de esta tarea y garantice la entrega de los paquetes de "medios" en tiempo real, o casi en tiempo real, siempre y cuando el deterioro de la calidad no sobrepase lo humanamente admisible, según el caso.

En relación con esto hay que señalar que la red IP no solo "mueve" a través de ella paquetes de información de usuario propiamente dicha, sino también "mueve" paquetes de control, es decir paquetes de señalización.

El término señalización en Telefonía IP tiene una connotación algo más amplia que el concepto correspondiente en las redes clásicas de Telecomunicaciones modo circuito.

Se trata ahora no sólo de la señalización necesaria para el control de la llamada en el sentido clásico (establecimiento, mantenimiento-modificación y terminación de la "conexión"), sino también señalización para garantizar QoS.

En correspondencia con esto, hay que hacer la distinción entre "transporte de medios", en alusión a la información de usuario (voz, imágenes, etc.), y "transporte de información de control", es decir, señalización.



El transporte de los medios (voz, vídeo, datos, etc.) por la red IP no sólo se traduce en mover por la misma secuencia de bits empaquetados, sino que también se requiere adicionarles a éstos cierta información de control, por ejemplo:

■ Tipo de información transportada

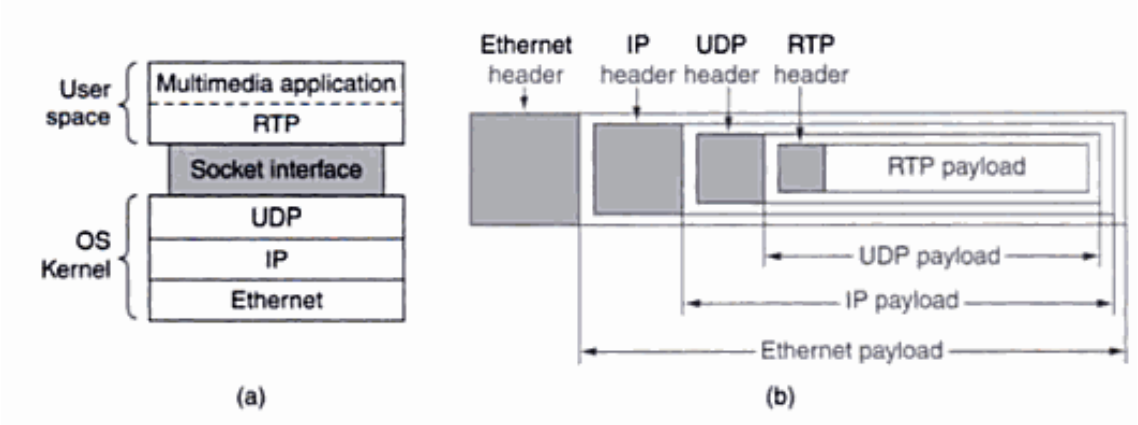
■ Números de secuencia

■ Marcas de tiempo, etc.

Esto supone una manera de "formatear" los paquetes IP y hacerlos aptos para el transporte de información con requerimientos de tiempo real.

REAL TIME TRANSPORT PROTOCOL

RTP – significa "Real Time Transport Protocol" (Protocolo de transporte en tiempo real), y define un formato de paquete estándar para el envío de audio y video sobre Internet. Es definido en el RFC1889. Fue desarrollado por el grupo de trabajo de transporte de audio y video y fue publicado por primera vez en 1996. RTP se utiliza en los sistemas de comunicación y entretenimiento que involucran medios de transmisión, tales como la telefonía, aplicaciones de videoconferencias, servicios de televisión y web basado en funcionalidades push-to-talk.



Posición de RTP en el stack de protocolos

El transporte de medios exige cumplir una serie de requisitos:

■ Caracterización de la carga útil, su identificación, cómo ha sido codificada, su formato, cuántas tramas por paquete, etc.

■ Información de tiempo que posibilite su reconstrucción temporal en el receptor o los receptores, y la sincronización de diferentes flujos de medios en el tiempo.

■ Secuenciamiento de los paquetes que constituyen los streams de medios, para posibilitar su reproducción en orden correcto y la detección de paquetes perdidos

Todo esto posibilita la gestión adecuada de los streams de medios en el receptor.

Concebido para compensar el jitter y la pérdida de secuencia de los paquetes que introducen las redes IP. Puede ser empleado para el transporte de streams de datos sensibles al tiempo, p.e. voz y vídeo.

RTP se utiliza junto con el protocolo de control de RTP (RTCP). Mientras que RTP transporta los flujos de medios (por ejemplo, audio y vídeo), RTCP se usa para supervisar las estadísticas de transmisión y calidad de servicio (QoS) y ayuda a la sincronización de múltiples flujos. RTP es originado y recibido en número de puerto par y la comunicación asociadas a RTCP utilizan el próximo número de puerto impar superior. RTP es uno de los fundamentos de VoIP y se utiliza conjuntamente con SIP el cual ayuda a establecer las conexiones a través de la red.

Los protocolos RTP y RTCP no ejercen ningún tipo de influencia en las condiciones de la red IP, no controlan la calidad de servicio, sólo posibilitan que los receptores puedan “resolver” apropiadamente las “perturbaciones” (jitter, pérdida de secuencia) a que son sometidos los paquetes IP con contenidos de tiempo real al atravesar la red.

Los paquetes RTP transportan streams de datos sensibles a:

■ A las demoras de la red

■ A sus fluctuaciones

■ A las pérdidas de paquetes,

■ A las pérdidas de información adicional que posibilite su recuperación y entrega adecuada.

Con respecto a las pérdidas de información adicional:

■ La identificación de la fuente

■ Tipo de carga útil que transporta el paquete

■ La secuenciación de paquetes

■ La información de temporización

El protocolo RTP provee monitorización, diagnóstica y realimenta al emisor de la calidad de la transmisión; soporta también la integración de tráfico transmitiendo múltiples fuentes en un simple flujo.

RTP Provee:

■ Sincronismo

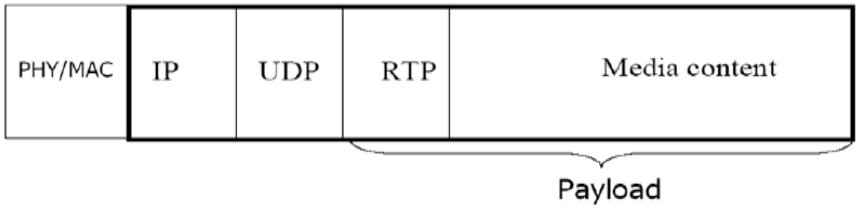
■ Secuenciamiento y Detección de pérdida de paquetes

■ Segmentación y rearmado

Cada flujo RTP es unidireccional y tiene asociado un flujo RTCP en el port UDP n+1.

El lado origen envía: información sobre los datos enviados, sincronización y timestamp

El lado receptor envía: información sobre los datos recibidos, pérdida de paquetes, jitter y delay.



RTP posibilita el transporte de datos isócronos a través de redes de paquetes

Ha sido optimizado para transferencias con requisitos de tiempo real, tanto unicast como multicast, soportando servicios extremos a extremo.

Pero no garantiza:

■ Reserva de recursos ni da garantía de calidad de servicio

■ Provisión de mecanismos para garantizar la entrega en tiempo

■ Asume que la red es segura y entrega los paquetes en secuencia.

Su papel fundamental es actuar como una interfaz entre aplicaciones de tiempo real y los protocolos de la capa de transporte, sin establecer qué protocolo debe ésta usar, aunque típicamente se soporta sobre UDP.

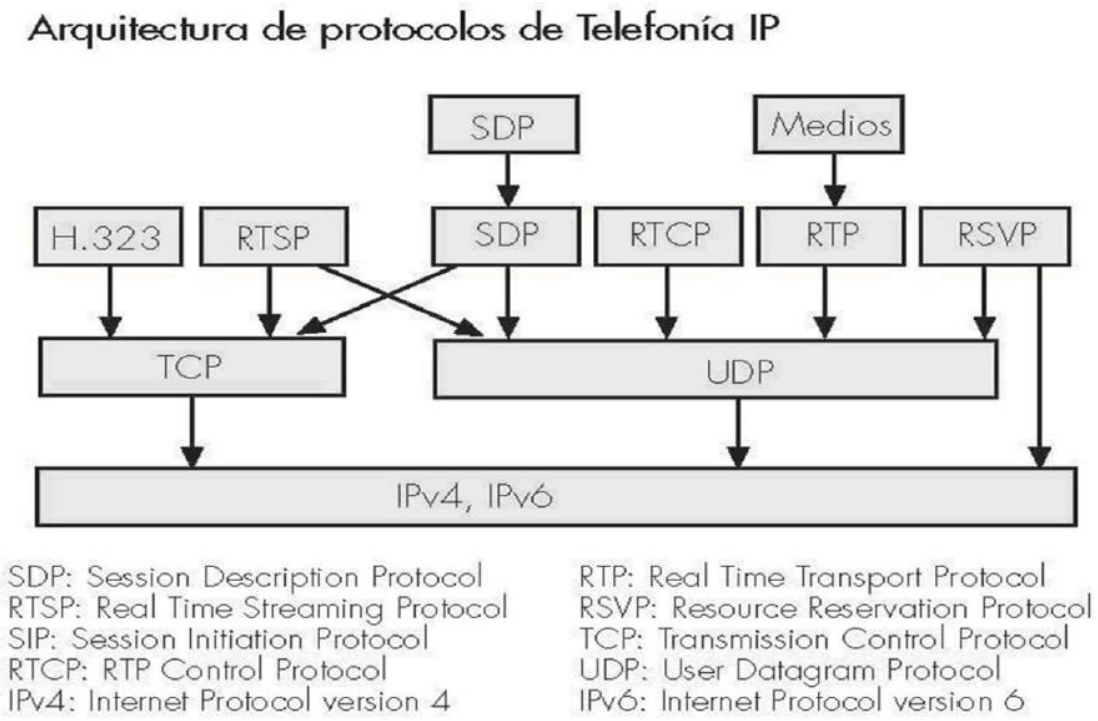
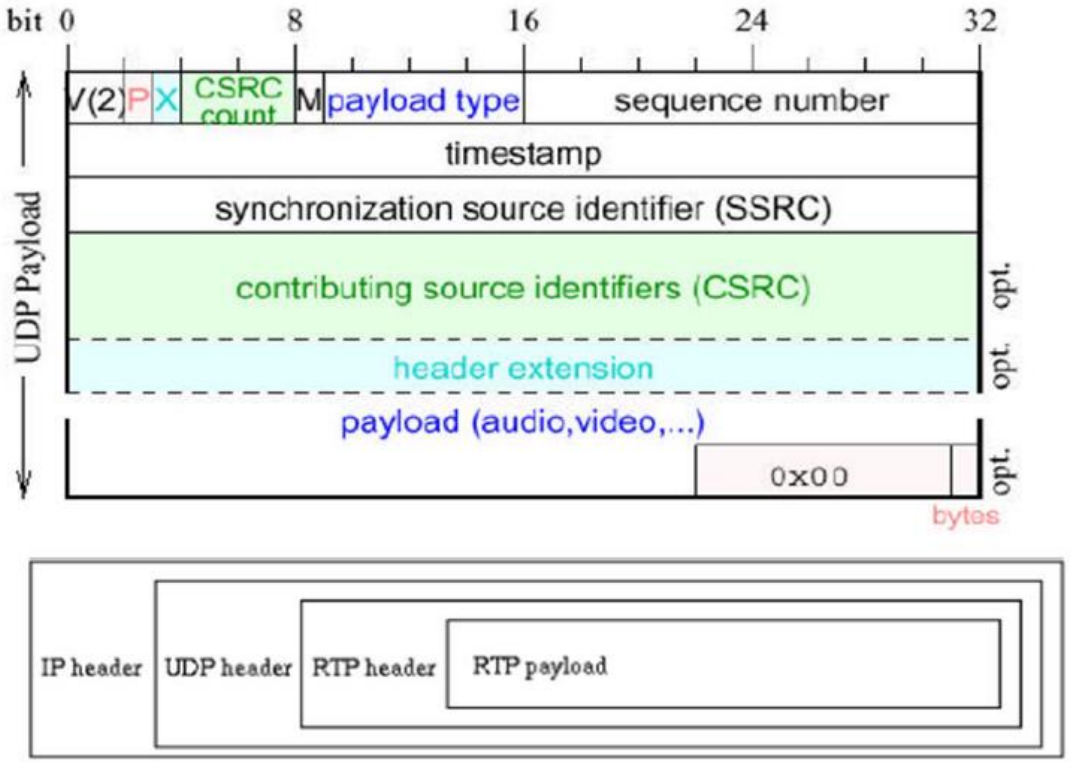


Ilustración 5 Arquitectura del protocolo RTP

A continuación, se muestra la trama RTP:



PROTOCOLO RTCP (REAL TIME CONTROL PROTOCOL).

RTCP es un protocolo de control que “acompaña” al protocolo RTP para la transferencia entre fuentes y destinos de streams multimedia. Proporciona información de la calidad de la transmisión en la red, posibilitando adaptar las fuentes al estado de la red.

RTCP se basa en la transmisión periódica de paquetes de control a todos los participantes en la sesión, empleando el mismo mecanismo de distribución que los paquetes de datos, por lo que debe proveer la multiplexación de paquetes de datos y paquetes de control RTCP, p.e., mediante el empleo de puertos diferentes del protocolo UDP.

RTCP es imprescindible en sesiones multicast, como realimentación de cómo reciben los streams de datos los destinatarios, posibilitando así homogeneizar la calidad. En comunicaciones unicast no es necesario, pero si es útil su uso.

Sus funciones son las de suministrar información respecto a la calidad de la distribución de los datos, "realimentación" que posibilita a la fuente de los datos:

■ aplicar control de flujo

■ aplicar control de congestión

■ aplicar codificación adaptativa

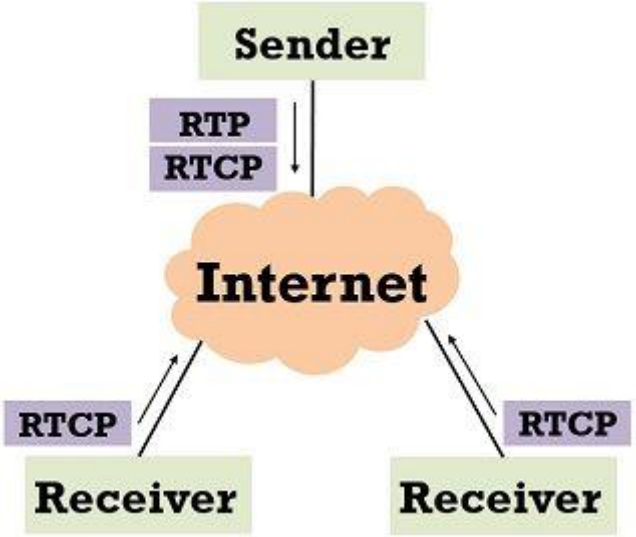
■ diagnosticar fallos en la distribución multicast

■ posibilita obtener información útil para diagnóstico y gestión de la red.

También controla la velocidad de emisión de paquetes RTP, para que éste sea escalable en cuanto al número de participantes.

RTCP debe ser utilizado por todos los participantes de una sesión RTP, enviando cada uno de ellos paquetes RTCP periódicamente.

Se debe dejar una pequeña parte (5 %) del ancho de banda asignado a RTP para RTCP, y se reparte entre todos los participantes.



SEÑALIZACIÓN Y CONTROL DE LLAMADA H.323 y SIP

Por las propias características de las redes IP, que no asignan recursos en exclusividad para cada comunicación, sino que existe una compartición máxima de los mismos, se hace necesario que los sistemas de VoIP requieran señalizar, con los protocolos adecuados, todo el control de la comunicación, por ejemplo:

■ Negociar el tipo de codificador a utilizar

■ Negociar los parámetros de empaquetado de la voz (y vídeo)

■ Negociar la calidad de servicio con la red (demoras, pérdida de paquetes)

■ Intercambiar N° de Puertos por los que se llevará a cabo la comunicación.

La señalización de VoIP y demás medios sobre IP debe garantizar los servicios clásicos que brindan las redes telefónicas, sumar la potencialidad que presentan las redes IP para la integración de servicios de voz, datos y vídeo.

También debe dar solución a la problemática particular de manejar tráfico con requerimientos de tiempo real sin que la QoS se deteriore más allá de lo admisible.

El flujo de la información de usuario y el flujo de señalización siguen trayectorias diferentes en su paso por las redes IP

En la señalización intervienen elementos funcionales que no intervienen en el manejo de los paquetes de la información del usuario.

La voz (información de usuario) y la señalización no presentan los mismos requerimientos de transporte por la red, la voz tiene que ser tratada con demora y jitter mínimos, pues pierde "valor" con el tiempo, dados sus requerimientos de tiempo real. La señalización carece de requerimientos de tiempo real.

Los "momentos" de la señalización no tienen coincidencia total con los "momentos" de la conversación, en lo fundamental la señalización precede y sucede a la conversación.

Según el caso también puede coincidir en el tiempo con ésta, es decir, que durante el trasiego por la red de paquetes de voz también se transfieran paquetes de señalización de una comunicación ya establecida.

El tráfico de información de usuario (voz, etc.) es tratado por la red IP de manera diferente a como lo hace con el tráfico de señalización.

Los protocolos de señalización son los que se usan para garantizar el establecimiento, mantenimiento, modificación y terminación de llamadas de voz sobre las redes IP: señalización de control de llamadas.

También intervienen en la QoS, seguridad y control de medios.

Se han desarrollado diferentes soluciones para la problemática de la señalización de control de llamada en sistemas de VoIP:

- Modelo H.323 (solución UIT)
- Modelo SIP (solución IETF)
- Modelo MEGACO (H.248)

Son tres soluciones diferentes a la misma problemática, la señalización de control de llamada para el servicio de VoIP, cada una con una arquitectura funcional y protocolos que las caracterizan.

PROTOCOLO DE SEÑALIZACIÓN H.323

H.323 es el protocolo internacional para conferencia sobre redes de paquetes que ha sido aprobado por la UIT en 1996. Esto garantiza la Interoperabilidad de aplicaciones con diferente hardware y software sobre IP y con Interoperabilidad de aplicaciones con diferente hardware y software sobre IP y con ISDN y PSTN.

H.323 se define como el estándar que permite que el tráfico multimedia en tiempo real sea intercambiado sobre una red de paquetes, por ejemplo, la red IP. También define una serie de entidades en una red cada una de ellas con una serie de funcionalidades.

H.323 incluye las siguientes recomendaciones:

■ H.225.0: paquetización, sincronización, señalización (Contiene el protocolo RAS)

■ H.245 : control de canal

■ H.261 y H.263: codificación de vídeo

■ G.711, G.722, G.723.1, G.728, G.729: codificación de audio

■ T.120: conferencias de datos en tiempo real, punto a punto y multipunto.

COMPONENTES H.323. H.323 define los siguientes componentes: Terminal, Gateway, Gatekeeper, Unidad de Control Multipunto, etc.

Gateways: son los sistemas encargados de permitir que los equipos H.323 puedan operar con otras redes.

Las pasarelas (Gateways) sirven de "puente" entre redes H.323 y otras redes, por ejemplo, con las redes de conmutación de circuitos de telefonía.

Desarrollan la "traducción" de la señalización, y la formación del control e información de usuario, según requerimientos de las redes que interconecta, posibilitando así la interoperabilidad entre redes, terminales y servicios, haciendo viable la integración de servicios aún con plataformas dispares (p.e., PSTN y redes IP).

Los Gateways cursan información de usuario, soportada ésta en RTP/UDP/IP.

Los Gateways, "vistos" desde cada una de las redes que interconecta, se comportan como un elemento más de las mismas, es decir, vista desde la red telefónica se comporta como una central de conmutación más de ésta, y vista desde una red IP como un nodo más de ésta.

Los Gateways son elementos funcionales opcional en entornos H.323, sólo son necesarios cuando se requiere interconexión entre entornos H.323 y entornos no H.323.

Así tenemos:

■ Gateways H.320, para redes N-ISDN

■ Gateways H.321, para redes B-ISDN

■ Gateways H.322, para redes LAN con calidad de servicio

■ Gateways H.324, para redes GSTN e inalámbricas

Y realizan funciones como la Traducción de formatos de transmisión, traducción de procedimientos de comunicación, transcodificación de audio y video y el establecimiento y liberación de llamadas.

Gatekeepers: Dentro de su zona LAN actúa de monitor de la red, proporcionando los servicios de resolución de direcciones (por ejemplo, asignación de la dirección IP a su alias, ya sea número telefónico o nombre) y de conceder permisos de llamadas.

Son entidades de control y señalización y constituyen los elementos funcionales más complejos en el marco H.323.

Proveen aquellos servicios que no pueden ser descentralizados e implementados en los "endpoints" (terminales, pasarelas, MCU´s).

Las funciones que lleva a cabo un gatekeeper se clasifican en funciones básicas y opcionales.

Entre las funciones básicas encontramos:

■ Traducción de direcciones.

■ Control de admisión.

■ Control del ancho de banda.

■ Gestión de Zona H.323.

Traducción de direcciones: Entre direcciones de transporte y alias de direcciones

Control de admisión: controla el acceso sobre la base de diferentes criterios, p.e., autorización, ancho de banda, etc. Puede no existir, esto es, se admiten todas las solicitudes de acceso

Control del ancho de banda: puede basarse en la gestión del ancho de banda. Puede no estar presente, admitiéndose todas las solicitudes de ancho de banda

Gestión de Zona H.323: se refiere a las funciones anteriores para los terminales, Gateways y MCU´s registrados en su zona de control.

Como funciones opcionales tendremos:

Señalización de control de llamada: en conferencias punto a punto el GK puede procesar mensajes Q.931

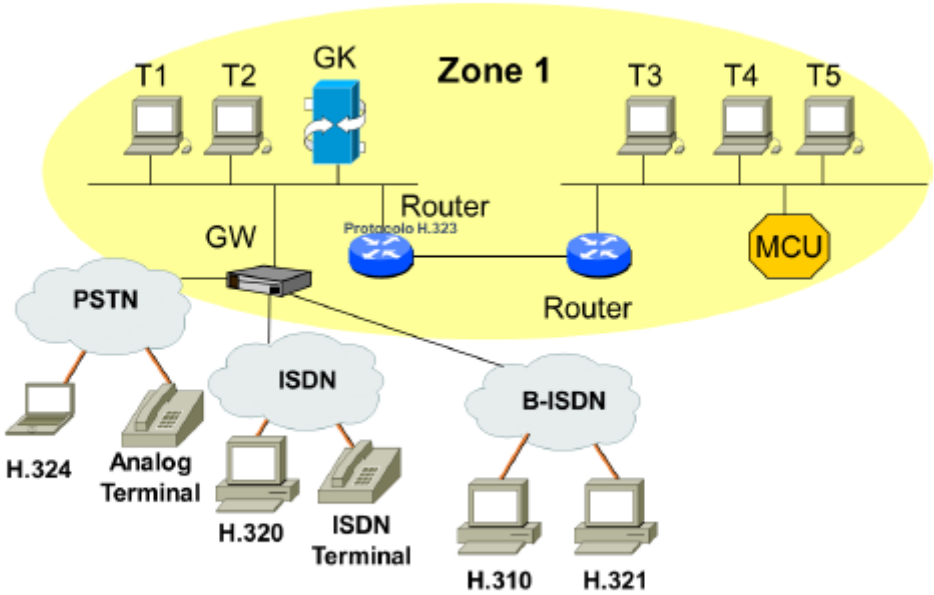
Autorización de llamadas: sobre la base de la especificación Q.931 el GK puede rechazar llamadas, p.e., acceso restringido a y desde determinados terminales o Gateways, restringir el acceso durante ciertos periodos de tiempo, etc.

Gestión de ancho de banda: el GK puede rechazar llamadas si el ancho de banda que éstas solicitan no está disponible, bien en nuevas llamadas o en llamadas en curso que soliciten ancho de banda adicional.

Gestión de llamadas: el GK puede, mediante una tabla propia, disponer del estado de las llamadas H.323, pudiendo saber el estado de un terminal dado y el “gasto” de ancho de banda asociado a las llamadas en curso, y proceder en consecuencia respecto a las nuevas solicitudes.

Terminales: son los dispositivos que se pueden conectar directamente a IP y soportan H.323

MCUs: (Multipoint Control Unit): es el sistema encargado del control de las conferencias múltiples, proporciona todos los servicios para establecer comunicaciones multipunto.



• La recomendación H.323 (ITU-T) cubre los requerimientos técnicos para brindar servicios de comunicación (audio y video) sobre ambientes LAN

EL ESTABLECIMIENTO DE LLAMADAS EN H.323.

El establecimiento de la llamada se lleva a cabo en tres fases.

■ Fase RAS: intercambio de mensajes entre gatekeeper y endpoint, para traducción de direcciones, autorización (o rechazo) de llamadas y gestión de ancho de banda.

■ Fase Q.931: intercambio de mensajes entre endpoints para el establecimiento de conexiones lógicas

■ Fase H.245: intercambio de mensajes entre endpoints para "acordar" el intercambio de información de usuario.

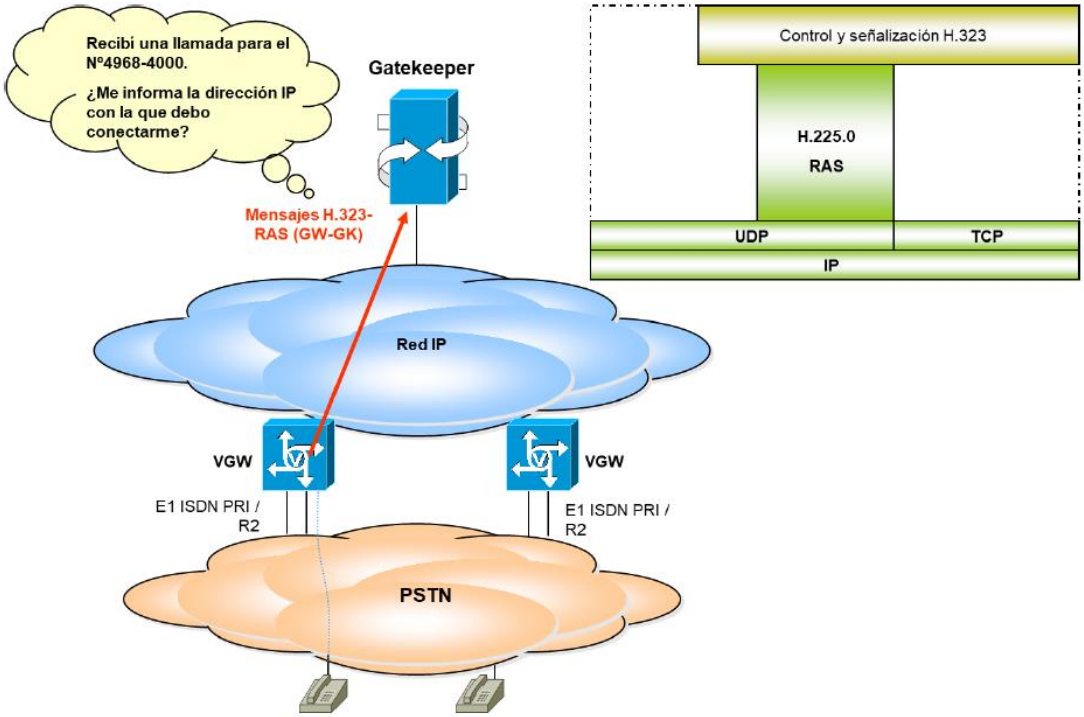
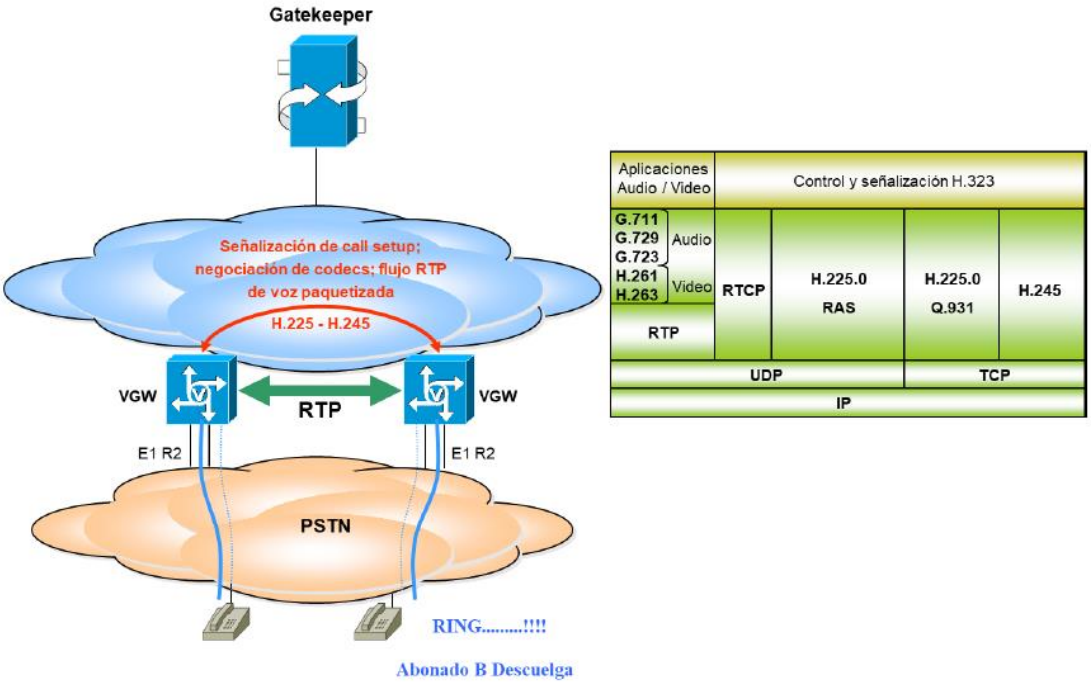


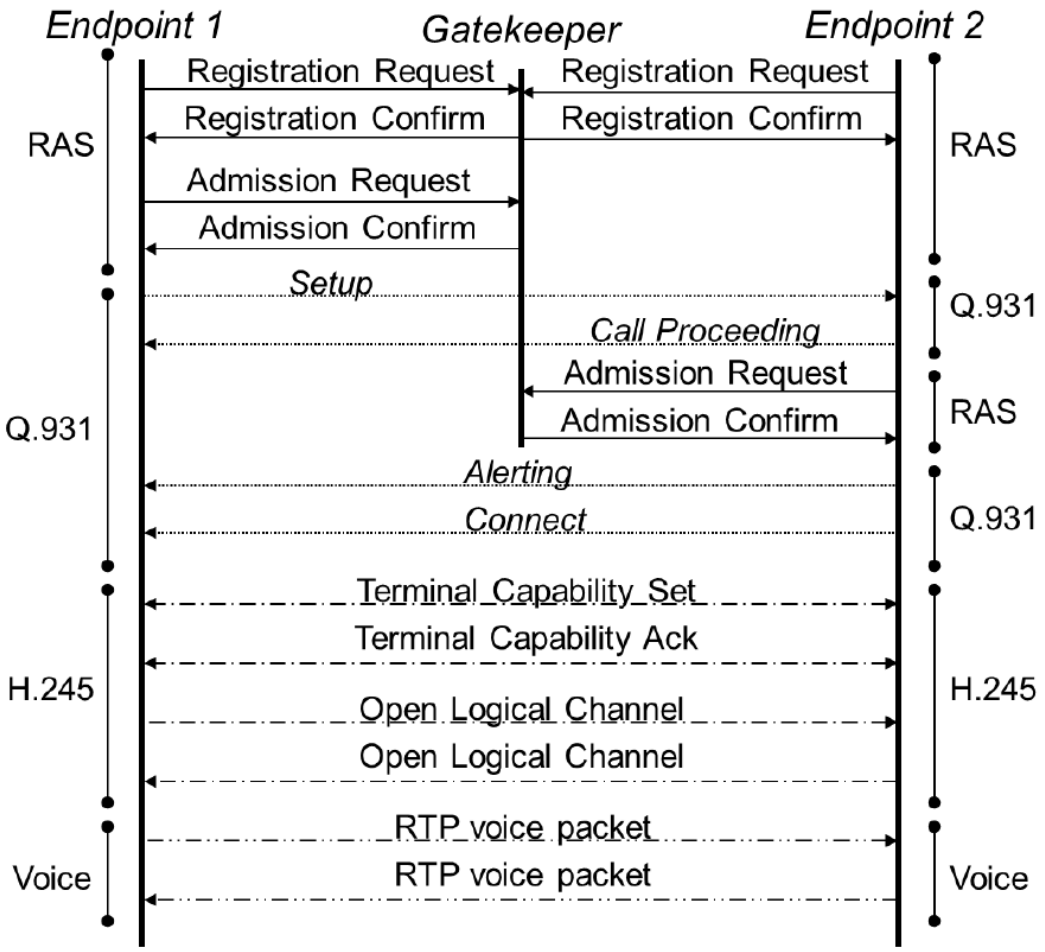
Ilustración 6 pedido de una llamada hacia la red PSTN

A continuación, el gatekeeper verifica las listas de numeración y la tabla de enrutamiento IP y le indica a que IP debe conectarse para establecer la llamada.

El destino solicita permiso al gatekeeper para establecer la llamada y al autorizar se produce el enlace con la red PSTN.



En la siguiente ilustración pueden verse los mensajes entre los componentes de H.323.



PROTOCOLO DE SEÑALIZACIÓN SIP

(Session Initiation Protocol) es un protocolo de control del nivel de aplicación que maneja la señalización y el control de llamadas.

Controla el establecimiento, modificación y terminación de sesiones o llamadas multimedia, directa o indirectamente.

SIP se cataloga como un protocolo de señalización y forma parte de las especificaciones del IETF para comunicaciones multimedia, juntamente con otros protocolos como RSVP, RTP, RTSP, SAP, SDP, pero su funcionalidad no depende de ninguno de éstos.

Soporta comunicaciones entre usuarios pertenecientes a redes IP, como también con usuarios de las redes telefónicas por intermedio de pasarelas (gateways).

Debemos notar que es neutral en relación con los protocolos de las capas inferiores, por lo que puede soportarse sobre TCP o UDP, igualmente sobre IP, IPX, ATM AAL5, F-R o X.25.

Provee por sí mismo sus propios mecanismos de seguridad.

Por otra parte, SIP es un protocolo basado en texto, emplea el juego de caracteres ISO 10646 con codificación UTF-8 (RFC 2279), lo que posibilita una fácil implementación y depuración, lo hace flexible y extensible.

El sobre encabezamiento que implica usar un protocolo basado en texto no tiene aquí mayores trascendencias, pues SIP es un protocolo de señalización, no es un protocolo para transmisión de datos de usuario donde sí tendría consecuencias su orientación a texto.

Los elementos funcionales de SIP son:

■ Agentes de Usuario (User Agent, UA),

■ Servidores de Red.

■ Agentes de Usuario Clientes (User Agent Client, UAC)

■ Agentes de Usuario Servidores (User Agent Server, UAS).

Los UAC originan las solicitudes SIP (asociados al extremo que origina la llamada).

Los UAS responden a estas solicitudes, es decir, originan respuestas SIP (asociados al extremo que recibe la llamada).

Los UAC y UAS por sí solos son capaces, sin los servidores de red, de soportar una comunicación básica (modelo de llamada básico, directamente entre endpoints).

La potencialidad del Modelo SIP se aprovecha con el empleo de los Servidores de Red (modelo de llamada con servidores proxy y modelo de llamada con servidores de redirección).

Los UA deben implementar el transporte tanto sobre TCP como sobre UDP.

Los Servidores de Red se pueden clasificar de la siguiente manera:

■ Servidores de Redirección

■ Servidores Proxy

■ Servidores de Registro

SERVIDORES DE REDIRECCIÓN.

■ Redireccionan las solicitudes de llamadas (mensajes INVITE), que son solicitudes SIP

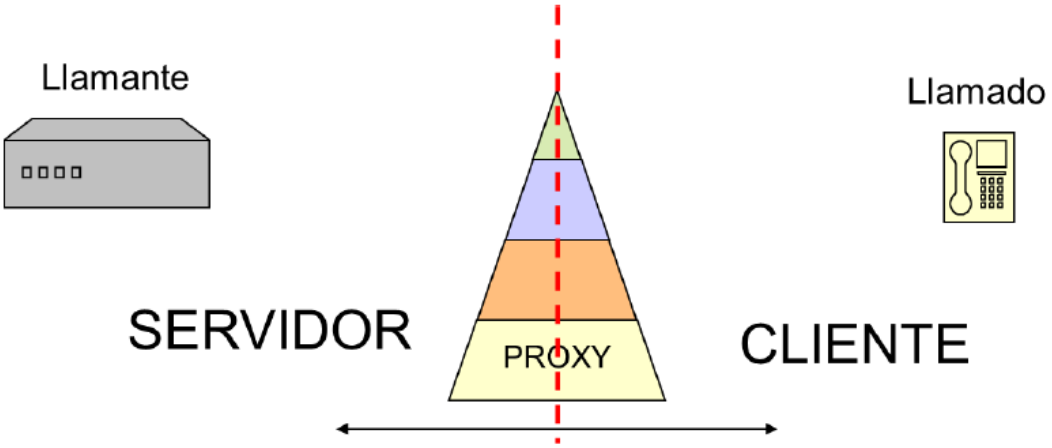
■ Retorna la dirección (o direcciones) de la parte llamada, (SIP-URL), o cómo contactar con ella (respuesta 3xx).

■ Rechazan la llamada error de cliente, enviando una (respuesta 4xx)

■ Rechazan la llamada error de servidor, enviando una (respuesta 5xx)

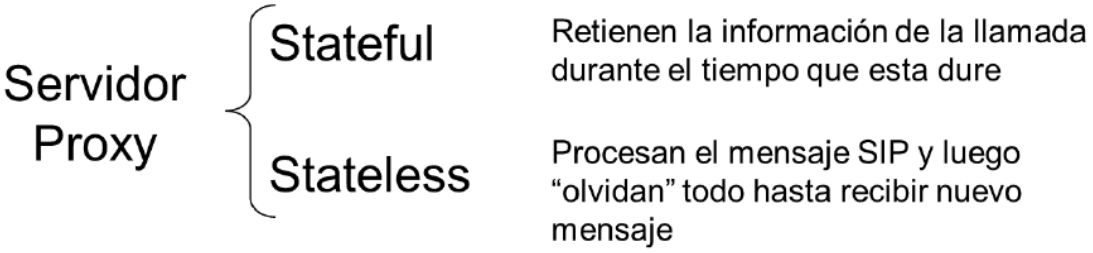
SERVIDORES PROXY.

Corren un programa “intermediario” que actúa como servidor y como cliente. Respecto al llamante se comporta como servidor y, al llamado como cliente.



Un servidor proxy puede enviar solicitudes hasta el destino final sin efectuar cambio alguno en ellas.

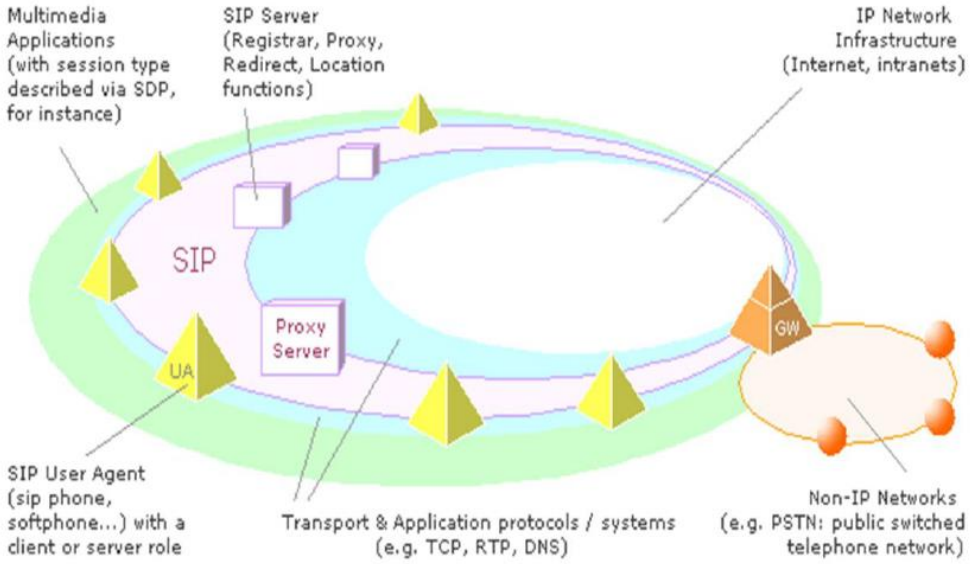
Puede cambiar alguno de sus parámetros si se requiere y desarrollan el ruteo de las solicitudes y respuestas SIP.



SERVIDORES DE REGISTRO.

Registran las direcciones SIP (SIP-URL) y las direcciones IP asociadas. Garantizan el “mapping” entre direcciones SIP y direcciones IP. Son servidores que sólo aceptan solicitudes REGISTER, posibilitando el registro correspondiente a la localización actual de los usuarios. Se les denomina servidores de localización, pues son utilizados por los servidores proxy y de redirección para obtener información respecto a la localización o localizaciones posibles de la parte llamada. Deben implementar el transporte sobre TCP y UDP.

EL MODELO SIP.



El protocolo SIP intercambia mensajes SIP (solicitudes y respuestas) a través de transacciones entre los entes funcionales (Agentes de Usuario y Servidores de Red).

Estos mensajes emplean el formato de mensaje definido en la RFC 822.

Los métodos SIP, esto es, mensajes de solicitud, son:

- INVITE
- ACK
- OPTIONS
- BYE
- CANCEL
- REGISTER

INVITE: invita a un usuario o servicio a participar en una sesión. El cuerpo del mensaje contiene una descripción de la sesión.

ACK: confirma que el cliente llamador ha recibido una respuesta final desde un servidor a una solicitud, p.e. a la solicitud INVITE, reconociendo la respuesta como adecuada.

OPTIONS: posibilita descubrir las capacidades del receptor.

BYE: finaliza una llamada o una solicitud de llamada. Puede ser enviado por el agente llamante o por el agente llamado.

CANCEL: cancela una solicitud pendiente, pero no afecta una solicitud completada. Este método finaliza una solicitud de llamada incompleta.

REGISTER: se utiliza este método como un servicio de localización que registra la localización actual de un usuario. También es necesario cuando hay varios servidores SIP en un mismo host, en cuyo caso solo uno de los servidores puede usar el número de puerto por defecto. Un servidor SIP que es capaz de aceptar mensajes REGISTER se denomina as register.

Las posibles respuestas a estas solicitudes son códigos de tres enteros, e indican el resultado de comprender y satisfacer una solicitud.

■ 1xx: Informativo. Solicitud recibida, que continúa para procesar la solicitud. Por ejemplo, 180 RINGING,

■ 2xx: Sucesos. La acción fue recibida de forma adecuada, comprendida y aceptada. Ej: 200 OK,

Redes administrativas – Unidad 7 Redes de próxima generación pág. 34

■ 3xx: Redireccionado. Más acciones deben ser consideradas para completar la solicitud. Ej: 302 MOVED TEMPORARILY,

■ 4xx: Error de cliente. La solicitud contiene mal la sintaxis o no puede ser resuelta en este servidor. Ej: 404 NOT FOUND,

■ 5xx: Error de servidor. El servidor ha errado en la resolución de una solicitud aparentemente válida. Ej: 501 NOT IMPLEMENTED,

■ 6xx: Fallo global. La solicitud no puede ser resuelta en servidor alguno. Ej: 600 BUSY EVERYWHERE.

MODELO BÁSICO DE LLAMADA SIP: (MODO DIRECTO)

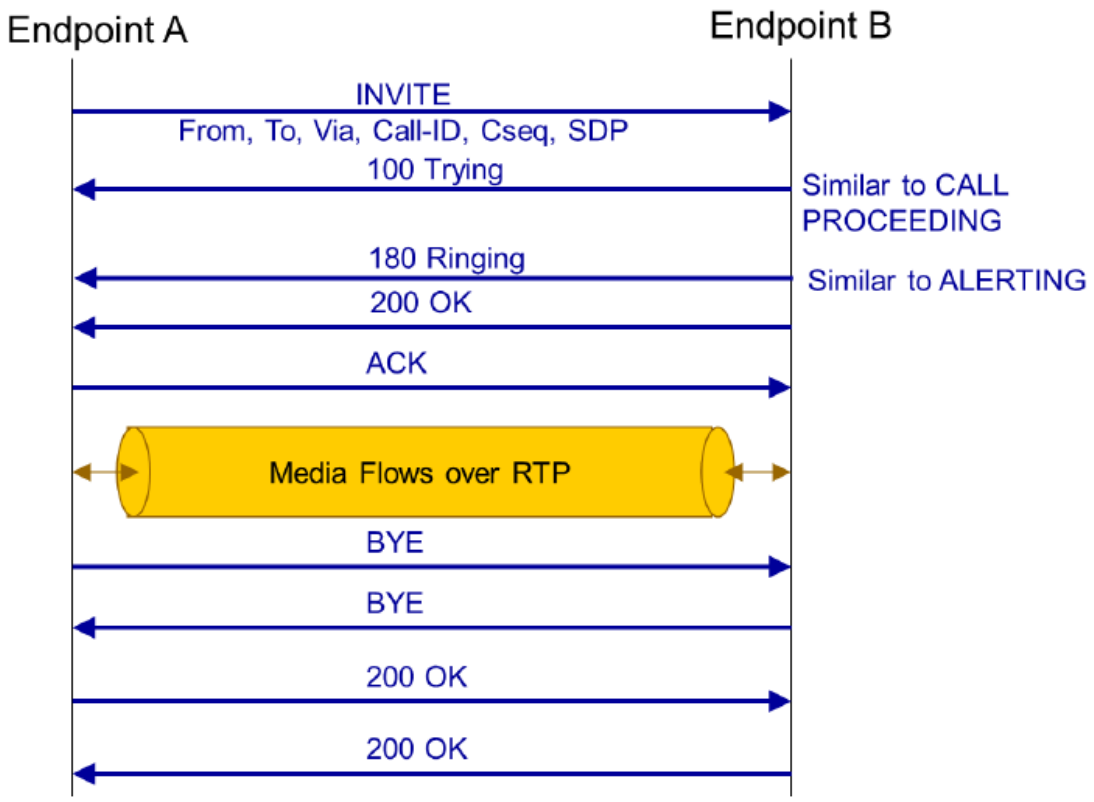
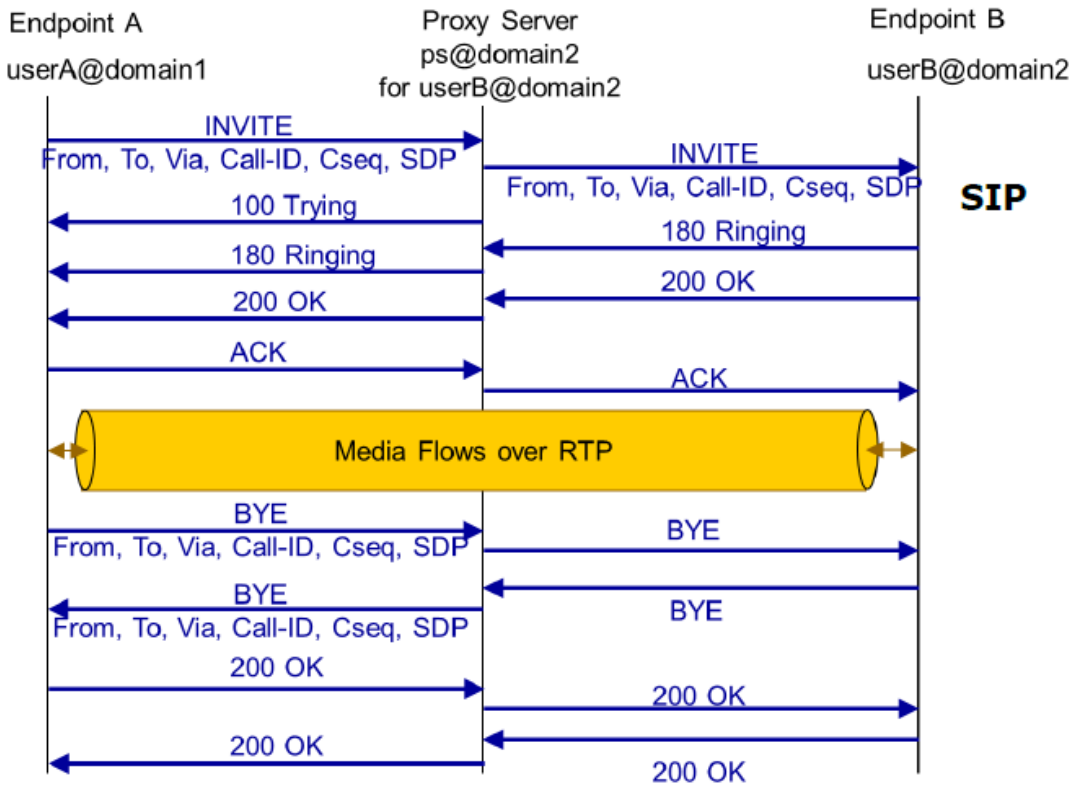
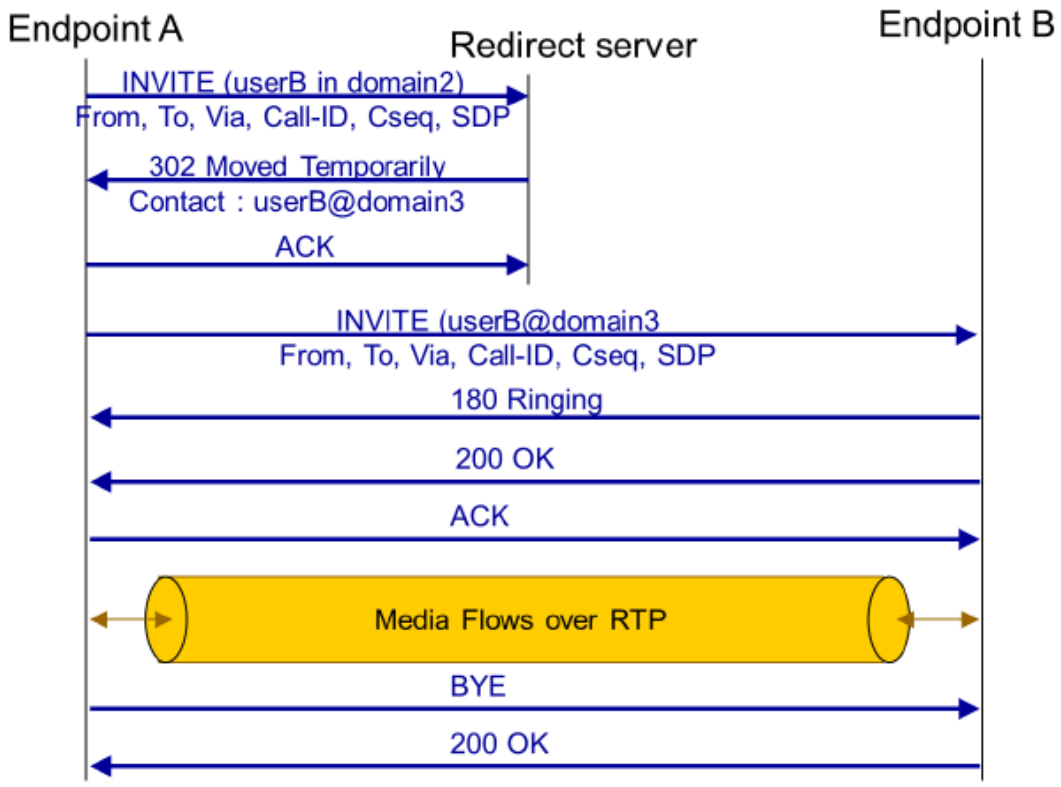


Ilustración 7 Modelo básico de la llamada SIP

SIP PROXY CALL MODEL.



REDIRECT CALL MODEL.



Redes por software (SDN) y Metro Ethernet

Contenido

Redes por software 40
¿Que son las redes por software? 40
¿Como funcionan las SDN? 40
Openflow 41
Metro Ethernet: 45
Estándares 48
Estándares de Ethernet Sobre Fibra Óptica 49
Trama Ethernet 49
802.Q/P Encabezado de Encapsulación. 50
Prioridad del usuario 51
IEEE 802.1P 51
CFI 51
VID- VLAN ID 51
Ethernet SLA 51
Bandwith profile. 51
Clases de Servicio. 51
Servicios 52
Tecnologías 53
Evolución de Ethernet 53
Parámetros de tráfico 55
PARÁMETROS DE PERFORMANCE 58
Frame delay (Retardo de trama) 58
Frame Jitter 58
Frame loss (Pérdida de trama) 58
Categorías de los servicios 58
Atributos: 59
SERVICIO DE 59
MULTIPLEXACIÓN 59
BUNDLING 60
SECURITY FILTERS 60
Servicios Ofrecidos 60
1 Acceso a Internet dedicado 60
2 Intranet extranet L2 VPN 61
3 Extencion de Lan 61
Preguntas 62

Redes por software 62
METRO..... 63

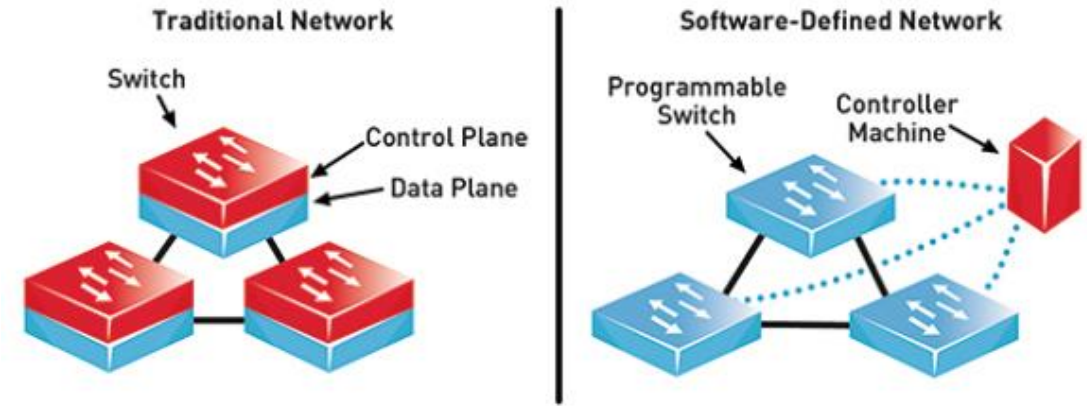
Redes por software

¿Que son las redes por software?

Las redes definidas por software (SDN**)** representan un enfoque en el que las redes utilizan controladores basados en software o interfaces de programación de aplicaciones (API) para dirigir el tráfico en la red y comunicarse con la infraestructura de hardware subyacente.

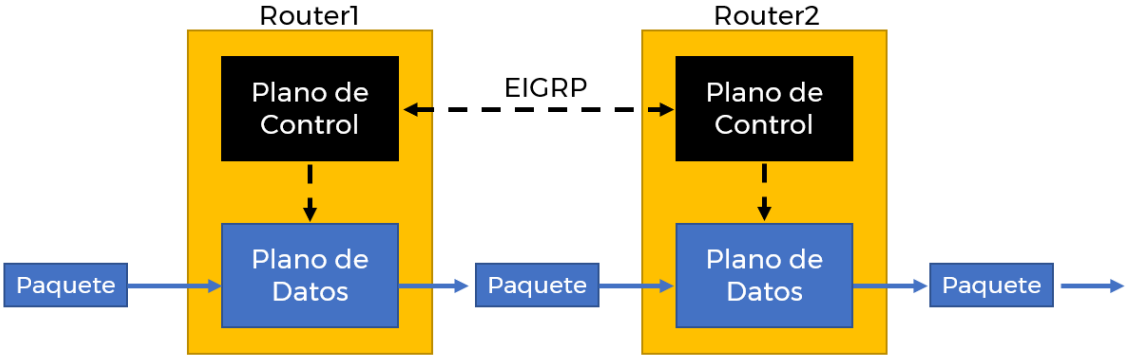
Este enfoque es distinto al de las redes tradicionales, que utilizan dispositivos de hardware dedicados (enrutadores y conmutadores) para controlar el tráfico de la red. Una SDN puede crear y controlar una red virtual o controlar una red de hardware tradicional mediante el software.

¿Como funcionan las SDN?



Normalmente un switch se divide en 2 planos, el plano de control y el plano de datos (controla plane y data plane). El plano de datos es el encargado de tomar las tramas entrantes al switch, revisar la tabla de ruteo para comprobar el destino de la trama y direccionarla por el puerto de salida correspondiente a su destino. Para realizar esta tarea utiliza unos circuitos lógicos denominados ASICS. También existen switches que realizan esta tarea por medio de CPU, pero son menos performantes.

Por otro lado, el plano de control se refiere a cualquier acción que controla el plano de datos. La mayoría de estas acciones tienen que ver con crear las tablas utilizadas por el plano de datos, tablas como la Tabla de enrutamiento IP, un protocolo de resolución de direcciones IP (ARP), una tabla de direcciones MAC, etc.



Enhanced Interior Gateway Routing Protocol (EIGRP), el protocolo del plano de control se ejecuta en cada enrutador (es decir, se distribuye entre todos los enrutadores). EIGRP en cada enrutador se agrega, elimina y cambia la tabla de enrutamiento IP de cada enrutador. Una vez poblada con rutas útiles, la tabla de enrutamiento IP del plano de datos en cada enrutador puede reenviar paquetes entrantes, como se muestra de

izquierda a derecha en la parte inferior de la figura. La siguiente lista incluye muchos de los protocolos de plano de control más comunes:

- OSPF
- Enhanced Interior Gateway Routing Protocol [EIGRP]
- Routing Information Protocol [RIP]
- Border Gateway Protocol [BGP]
- IPv4 ARP
- IPv6 Neighbor Discovery Protocol (NDP)
- Switch MAC learning
- STP

Además, algunos switches incluyen un tercer plano llamado plano de gestión. A partir de este los administradores pueden realizar todo tipo de tareas administrativas sobre los equipos. Estas pueden realizarse de manera remota o directamente conectado al equipo. Las tareas de gestión involucran todas las configuraciones del equipo que luego va a tomar el plano de control para realizar su actividad de control sobre el plano de datos. Cabe aclarar que las tareas de configuración de switches son muy extensas y se deben realizar switch por switch.

Las redes SDN plantean una separación de los planos dentro del switch. En esta separación el switch solamente contiene el plano de datos y una interfaz de configuración, y por fuera, en un servidor centralizado, se configura el plano de control. Este plano de control se conecta con los distintos switches de la red para realizar las configuraciones necesarias de manera automática. Por lo tanto, el administrador cuanta con una única interfaz de control, a través de la cual realiza todas las configuraciones de red necesarias de forma centralizada y sin conocer la ubicación y la cantidad de switches de la red. Luego el software de la capa de control se encarga de distribuir todas las configuraciones según la necesidad del administrador.

Openflow

Openflow es la primera interfaz de comunicaciones estándar definido entre el control y reenvío de las capas de una arquitectura SDN. Openflow permite acceso directo y la manipulación al plano de reenvío de dispositivos de red tales como switches y routers, tanto físicos como virtuales. Es la ausencia de una interfaz abierta para el plano de reenvío que ha llevado a la caracterización de dispositivos de red hoy en día como monolítico, cerrado y mainframe. Ningún otro protocolo: estándar hace lo que Openflow hace, y un protocolo como Openflow es necesario para mover el control de la red fuera de los switches de red hacia el software de control de lógica centralizado.

El protocolo Openflow se implementa en ambos lados de la interfaz entre dispositivos de infraestructura de red y el software de control SDN. Openflow utiliza el concepto de flujos para identificar el tráfico de red basado en reglas predefinidas de coincidencia que puede ser estática o dinámicamente programadas por el software de control SDN. Además, permite definir cómo el tráfico puede fluir a través de dispositivos de red sobre la base de parámetros tales como los patrones de uso, aplicaciones y recursos de la nube. Desde que Openflow le permite a la red ser programada sobre una base por flujo, una arquitectura SDN basada en Openflow proporciona un control extremadamente granular, permitiendo a la red responder a cambios en tiempo real a nivel de la aplicación y usuario.

El protocolo Openflow es un factor clave para las Redes Definidas por Software o SDN, y en la actualidad es el único protocolo SDN estandarizado que permite la manipulación del plano de reenvío de los dispositivos de red.

Openflow basado en SDNS se puede implementar en las redes existentes, tanto físicas como virtuales. Los dispositivos de red deben soportar envíos basados en Openflow.

Un switch Openflow consiste en una o más tablas de flujo y una tabla de grupo, los cuales realizan búsquedas de paquetes y reenvíos, y un canal Openflow hacia un controlador externo llamado controller. Este controlador se apropia del switch vía protocolo-Openflow. Usando este protocolo, el controlador puede adicionar, actualizar y borrar flujos de entrada.

Cada tabla de flujo en el switch contiene un conjunto de flujos de entrada, cada flujo de entrada consta de campos de enlace o de comparación, contadores y un conjunto de instrucciones para aplicar a los paquetes enlazados o comparados. La comparación comienza en la primera tabla de flujo y puede continuar a tablas de flujo adicionales. Los flujos de entrada comparan paquetes en orden de prioridad, con la primera entrada comparada en cada tabla que se utilice. Si una entrada comparada coincide, las instrucciones asociadas con la entrada de flujo especificada son ejecutadas. Si no hay coincidencia en una tabla de flujo, la salida depende de la configuración del switch: el paquete puede ser enviado al controlador a través del canal Openflow, puede ser eliminado o puede continuar a la siguiente tabla de flujo.

Las instrucciones asociadas con cada flujo de entrada describen el reenvío del paquete, la modificación del paquete, el procesamiento de la tabla de grupo y el procesamiento pipeline.

Las instrucciones del procesamiento pipeline permiten que los paquetes sean enviados a tablas siguientes para el procesamiento adicional y permiten que la información, en forma de metadata, para que se comunique con entre tablas. El procesamiento de tablas pipeline se detiene cuando el conjunto de instrucciones asociadas con una comparación de flujo de entrada no especifica una tabla próxima en este punto, el paquete usualmente se modifica y se reenvía.

Los flujos de entrada pueden enviarse a un puerto. Usualmente un puerto físico, pero también puede ser un puerto virtual definidos por el switch a un puerto virtual reservado pueden especificar acciones genéricas de reenvío, así como las que se envían al controlador

Los flujos de entrada pueden apuntar a un grupo, lo cual, especifica procesamiento adicional. Los grupos representan conjuntos de acciones para las inundaciones o flooding, así como más complejos reenvíos como: multipath, redireccionamiento rápido y agregación de enlaces. Los grupos también permiten enviar múltiples flujos a un solo identificador, como por ejemplo el reenvío IP para un siguiente salto común. Esta abstracción permite acciones de salida comunes a través de los flujos para ser cambiados de manera eficiente.

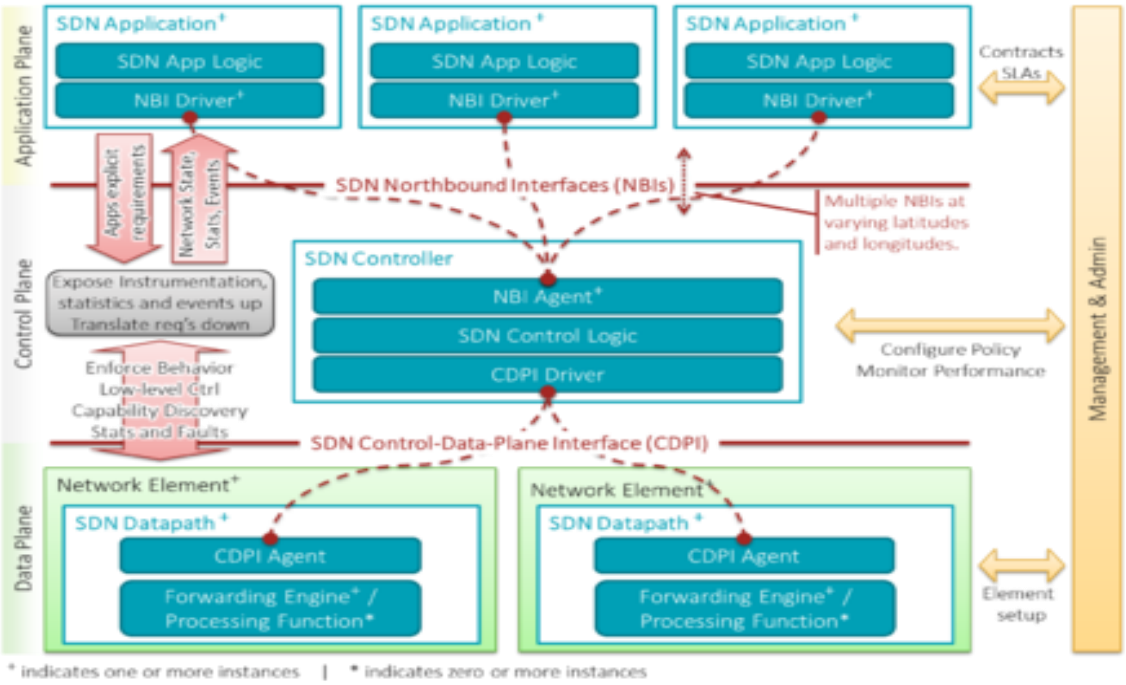
Arquitectura

Aunque la ONF está continuamente modificando la terminología, los términos más comunes para los componentes de esta arquitectura son los siguientes:

- **Aplicación SDN (*SDN App*):** las aplicaciones SDN son programas que directamente comunican las necesidades y los comportamientos deseados de su red al controlador SDN a través de los NBI. Están formadas por una lógica de aplicación y uno o más NBI.
- **Controlador SDN (*SDN Controller*):** entidad lógica de control encargada de traducir las peticiones de la aplicación SDN a las rutas de datos más abajo, dando a la capa de aplicación una visión abstracta de la red mediante estadísticas y posibles eventos. Un controlador SDN consiste en uno o más NBIs, la lógica de control SDN y el CDPI *driver*.
- **Ruta de datos SDN (*SDN Datapath*):** componente lógico que expone visibilidad y control sobre sus capacidades de reenvío y procesamiento. La

representación lógica, por lo tanto, puede abarcar todos o un subconjunto de los recursos físicos. Está formado por un agente CDPI, un conjunto de motores de reenvío y de funciones de procesamiento, que incluyen simples reenvíos entre interfaces externas de esta y procesamiento interno del tráfico. Las rutas de datos pueden contenerse en un único elemento de red (físico).

- **Interfaz SDN del plano de control al plano de datos (*SDN Control to Data-Plane Interface*, CDPI):** interfaz entre el controlador y la ruta de datos, que provee programabilidad a la hora del reenvío, anuncio de capacidades, reporte estadístico y notificación de eventos.
- **Interfaces *hacia el norte* SDN (NBI):** son interfaces entre las aplicaciones SDN y los controladores que proveen vistas abstractas del comportamiento de la red y sus requerimientos.
- ***Conductores* y *agentes* de interfaz (*Interface Drivers & Agents*):** cada interfaz es implementada por un par de este tipo, que representa el fondo (relacionado con la infraestructura) y la cima (relacionada con la aplicación).
- **Gestión y administración (*Management & Admin*):** el plano de gestión cubre tareas estáticas, manejadas mejor fuera de los planos de aplicación, control y datos, como la asignación de recursos a los clientes, la configuración de equipos físicos y la concordancia entre alcanzabilidad y credenciales entre entidades físicas y lógicas.



La arquitectura típica de SDN se divide en tres partes:

- Las aplicaciones, que comunican las solicitudes de recursos o información sobre la red en su conjunto.
- Los controladores, que utilizan la información de las aplicaciones para decidir cómo enrutar un paquete de datos.
- Los dispositivos de red, que reciben información del controlador sobre dónde mover los datos.

Ventajas de las redes definidas por software

Las SDN ofrecen toda una serie de ventajas sobre las redes tradicionales, entre ellas:

- **Mayor control con una velocidad y flexibilidad superiores**: en lugar de programar manualmente varios dispositivos de hardware específicos de un proveedor, los desarrolladores pueden controlar el tráfico que fluye en una red con solo programar un controlador basado en software de estándar abierto. Los administradores de red también tienen más flexibilidad para elegir el equipo de las redes, puesto que pueden optar por un protocolo de código abierto para comunicarse con cualquier cantidad de dispositivos de hardware a través de un controlador central.
- **Infraestructura de red personalizable**: al utilizar una red definida por software, los administradores pueden configurar los servicios de red y asignar recursos virtuales para cambiar la infraestructura de la red en tiempo real desde una ubicación centralizada. Esto permite que los administradores de red optimicen el flujo de datos en la red, dando prioridad a las aplicaciones que requieren una mayor disponibilidad.
- **Seguridad sólida:** una red definida por software aumenta la visibilidad de toda la red, lo que proporciona una visión integral de las amenazas a la seguridad. Dada la proliferación de dispositivos inteligentes que se conectan a Internet, una SDN ofrece ventajas patentes en comparación con las redes tradicionales. Los desarrolladores pueden crear zonas independientes para los dispositivos que exijan distintos niveles de seguridad o poner en cuarentena al momento cualquier dispositivo con alguna vulnerabilidad para que no pueda infectar el resto de la red.

En qué se diferencian las SDN de las redes tradicionales?

La diferencia clave entre las SDN y las redes tradicionales es la infraestructura: las SDN están basadas en software, mientras que las redes tradicionales están basadas en hardware. Ya que el plano de control está basado en software, las SDN son mucho más flexibles que las redes tradicionales. Permiten que los administradores controlen la red, cambien los ajustes de configuración, aprovisionen recursos y aumenten la capacidad de la red, todo ello desde una interfaz de usuario centralizada y sin necesidad de añadir más hardware.

También hay diferencias relativas a la seguridad entre las SDN y las redes tradicionales. Gracias a una mayor visibilidad y a la capacidad de definir rutas seguras, las SDN ofrecen una seguridad mejor en muchos aspectos. Sin embargo, puesto que las redes definidas por software hacen uso de un controlador centralizado, protegerlo es crucial para mantener una red segura, puesto que este punto único de fallo representa una posible vulnerabilidad de las SDN.

Aplicaciones y servicios que pueden sacar provecho de las redes definidas por software (SDN)

Muchos de los servicios y aplicaciones actuales, en especial cuando involucran a la nube, no podrían funcionar sin las SDN. Las SDN permiten que los datos se desplacen

fácilmente entre ubicaciones distribuidas, lo que es fundamental para las aplicaciones en la nube.

Además, las SDN permiten desplazar cargas de trabajo rápidamente dentro de una red. Por ejemplo, dividir una red virtual en secciones, mediante una técnica denominada virtualización de funciones de red (NFV), permite a los proveedores de telecomunicaciones trasladar los servicios del cliente a servidores más económicos o incluso a los propios servidores del cliente. Los proveedores de servicios pueden utilizar una infraestructura de red virtual para trasladar las cargas de trabajo desde las infraestructuras de nube privada hasta las de la pública, según sea necesario, y poner a disposición de los clientes nuevos servicios de forma instantánea. Las SDN también facilitan que cualquier red se flexibilice y crezca a medida que los administradores de red añadan o eliminen máquinas virtuales, ya estén en el entorno local o en la nube.

Por último, gracias a la velocidad y la flexibilidad que ofrecen las SDN, es posible dar soporte a tendencias y tecnologías emergentes, como la informática perimetral y el Internet de las cosas, que requieren una transferencia de datos rápida y sencilla entre sitios remotos.

Metro Ethernet:

Una Red Metro Ethernet, es una arquitectura tecnológica destinada a suministrar servicios de conectividad de datos en una Red de área metropolitana (MAN) de capa 2 en el modelo OSI, a través de interfaces (UNIs) Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios, aplicaciones, y cuentan con mecanismos donde se incluye soporte a tráfico "RTP" (tiempo real), para aplicaciones como Telefonía IP y Video IP, aun cuando este tipo de tráfico es especialmente sensible al retardo y al jitter (Fluctuación).

Las redes Metro Ethernet pueden utilizar líneas de cobre (MAN BUCLE), lo que garantiza la posibilidad de despliegue en cualquier punto del casco urbano, soportando el 100% de los servicios demandados por los proyectos de Smart City.

Las redes Metro Ethernet suelen utilizar principalmente medios de transmisión guiados, como son el cobre (MAN BUCLE) y la fibra óptica, existiendo también soluciones de radio licenciada, los caudales proporcionados son de 10 Mbit/s, 20 Mbit/s, 34 Mbit/s, 100 Mbit/s, 1 Gbit/s y 10 Gbit/s.

La tecnología de agregación de múltiples pares de cobre, (MAN BUCLE), permite la entrega de entre 10 Mbit/s, 20 Mbit/s, 34 Mbit/s y 100 Mbit/s, mediante la transmisión simultánea de múltiples líneas de cobre, además esta técnica cuenta con muy alta disponibilidad ya que es casi imposible la rotura de todas las líneas de cobre y en caso de rotura parcial el enlace sigue transmitiendo y reduce el ancho de banda de forma proporcional.

La fibra óptica y el cobre, se complementan de forma ideal en el ámbito metropolitano, ofreciendo cobertura total a cualquier servicio a desplegar.

Los beneficios que Metro Ethernet ofrece son:

El modelo básico de los servicios Metro Ethernet, está compuesto por una Red switcheada MEN (Metro Ethernet Network), ofrecida por el proveedor de servicios; los usuarios acceden a la red mediante CEs (Customer Equipment), CE puede ser un router; Bridge IEEE 802.1Q (switch) que se conectan a través de UNIs (User Network Interface) a velocidades de 10 Mbit/s, 20 Mbit/s, 34 Mbit/s, 100 Mbit/s, 1 Gbit/s y 10 Gbit/s.

Los organismos de estandarización (IEEE, IETF, ITU) y los acuerdos entre fabricantes, están jugando un papel determinante en su evolución. Incluso se ha creado el MEF (Metro Ethernet Forum), organismo dedicado únicamente a definir Ethernet como servicio metropolitano.

Para Metro Ethernet se tienen en cuenta los siguientes parámetros:

Un EVC es la asociación entre una o más interfaces UNIs. Es un tubo virtual que proporciona al usuario servicios extremo a extremo atravesando múltiples redes MEN (Metro Ethernet Network). Un EVC tiene dos funciones:

Un EVC puede ser usado para construir VPN (Virtual Private Network) de nivel 2.

El MEF (Metro Ethernet Forum) ha definido dos tipos de EVC:

El servicio E-Line proporciona un EVC punto a punto entre dos interfaces UNI. Se utiliza para proporcionar una conexión Ethernet punto a punto entre dos sitios.

Dentro del tipo de servicio E-Line se incluye una amplia gama de servicios. El más sencillo consiste en un ancho de banda simétrico para transmisión de datos en ambas direcciones, no fiable, entre dos interfaces UNI a 10 Mbit/s. Un servicio más sofisticado considerado dentro del tipo de servicio E-Line sería, por ejemplo, una línea E-Line, que ofrezca una CIR concreta junto con una CBS, y una EIR junto con una EBS, y un retardo, variación del retardo y máximos asegurados entre dos interfaces UNI.

El tipo de servicio E-LAN proporciona conectividad multipunto a multipunto. Conecta dos o más interfaces UNI. Los datos enviados desde un UNI llegarán a 1 o más UNI de destino. Cada uno de ellos está conectado a un EVC multipunto. A medida que va creciendo la red y se van añadiendo más interfaces UNI, éstos se conectarán al mismo EVC multipunto, simplificando enormemente la configuración de la misma. Desde el punto de vista del usuario, la E-LAN se comporta como una LAN.

Los atributos se definen como las capacidad de los diferentes tipos de servicio. Algunos atributos aplican a los puntos de acceso UNI (User Network Interface), mientras que otros a los canales virtuales (EVC).

Servicios de Metro Ethernet

Para una empresa con múltiples ubicaciones y entre las áreas metropolitana, se puede conseguir un punto a punto o de cualquier a cualquier conexión, o una mezcla de ambos mediante una red Metro Ethernet la cual proporciona conexiones de 10Mbps a 1Gbps, 24x7 vigilancia y atención al cliente, acuerdos de nivel de servicio, más un apoyo para 10BaseT, 100BaseTX y 1000LX están disponibles en todos los servicios de Metro Ethernet

Metro Ethernet Reduce los cuellos de botella de rendimiento WAN con anchos de banda de hasta 10Mbps a 1Gbps (Gigabit Ethernet), dándole la libertad de las limitaciones de rendimiento de la WAN de transporte, se reducen ciertos costos mediante la reducción de la necesidad de transporte de personal técnico encargado también aplicar una solución que puede escalar para apoyar una organización a medida que crece

La Simplificación de la interconexión de sus ubicaciones dentro y entre las áreas metropolitanas garantizar el rendimiento óptimo de la velocidad de LAN en el envío de datos un enlace puede soporta Full Duplex o Half Duplex o auto negociación. La red Metro Ethernet ofrece una sencilla migración a un mayor rendimiento y valor. Que aprovecha su actual infraestructura de la red local de TI y los recursos de personal, la eliminación de los costes intensivos cliente premisa compras de equipo y capacitación del personal de TI

Beneficios de Metro Ethernet

Las redes metro Ethernet ofrecen un ancho de banda alto Ethernet a bajo costo porque ofrece un ancho de banda dedicado superior y el servicio para la red privada a un costo reducido. Además, hace de Ethernet de red privada de

conectividad sencilla. Velocidades de LAN nativo a través de su red de servicios múltiples y simplificados de configuración y creación de redes Ethernet

Metro Ethernet proporciona la perfecta capacidad de mezclar velocidades por zonas y la aplicación de apoyo a datos de alta velocidad, Voz sobre IP y aplicaciones de vídeo. Metro Ethernet está disponible en el punto a punto y soluciones de conmutación de 10 megabits por segundo a 1 gigabit por segundo, lo cual permite:

- Velocidades flexible por ubicación y aplicación
- Totalmente compatible con el estándar 802.3z
- Conmutada y punto a punto soluciones
- Full Duplex velocidades 512K - 10.000 Mbps

Metro Ethernet permite actualizar a una red rápida, sin los costos de nuevos equipos o la formación en una tecnología de redes diferentes. Porque la mayoría de las empresas utiliza actualmente de Ethernet en su entorno de red, las interconexiones de red Metro Ethernet no requieren grandes cambios. Metro Ethernet utiliza extensiones familiares de la tecnología LAN de Ethernet y se integra perfectamente con las actuales redes Ethernet y Fast Ethernet. Metro Ethernet de red de gestión y herramientas de solución de problemas son un complemento natural a las actuales capacidades de Ethernet de apoyo, por lo que Metro Ethernet incrementales sólo requiere formación, no mayor de adopción de nuevos conceptos. Metro Ethernet utiliza los mismos protocolos y estándares como Ethernet de 10 Mbps y 100 Mbps Fast Ethernet y cumple con el formato IEEE 802.3z marco, dúplex completo y flujo de operación de los métodos de control

Metro Ethernet en comparación con Frame Relay y ATM

En comparación familiar con las aplicaciones Ethernet, Frame Relay y ATM, la demanda de formación y experiencia que aumentar el costo de la aplicación y operación. También requieren de equipo adicional que se suma a los costos iniciales y de mantenimiento. Metro Ethernet ofrece ahora servicio de ancho de banda de hasta 10.000 Mbps, ancho de banda comprometido características, prioridades, o incluso una transmisión full duplex conexión. Con el Servicio de Metro Ethernet, puede obtener rentables, de alta capacidad entre las conexiones de LAN múltiples sitios en un área metropolitana. El resultado: menores costes de formación, reducir los costes operativos y la simplificación de cambio y el crecimiento en sus operaciones de red - todo con la fiabilidad y la calidad del servicio.

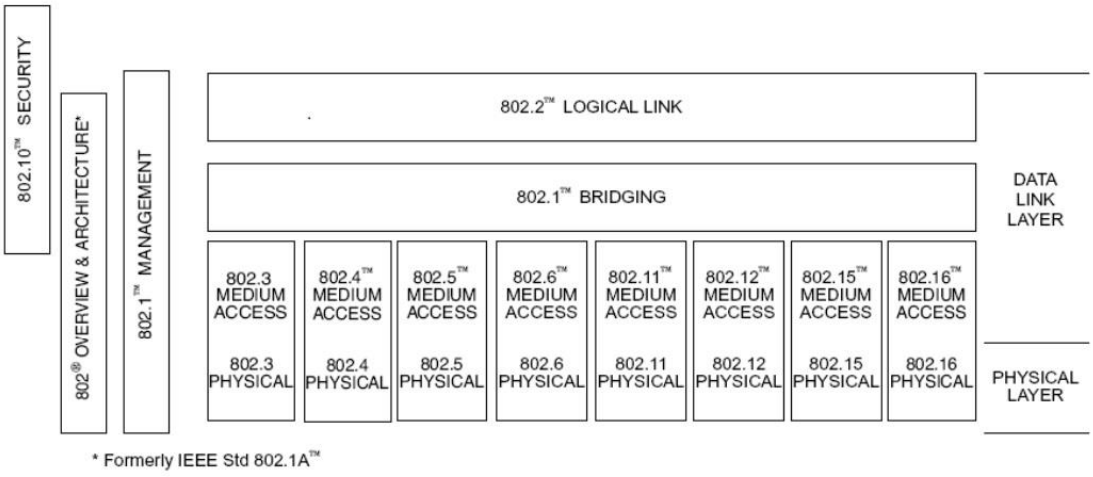
Metro Ethernet es:

Rentable

- Menos costoso que la multiplexación por división de tiempo (TDM) de servicios
- Reduce los costos de TI mediante la eliminación de las conversiones de la señal
- Reduce los costes de equipamiento con interfaces Ethernet Flexible
- Escalable a crecer como crecen las necesidades de su ancho de banda
- Aumentar el ancho de banda en unos cuatro días hábiles a partir de orden de servicio y la aceptación Rápido
- Velocidades de 512K a 10Gbps Fiable
- 99,9% la disponibilidad del servicio, que puede ser aumentado a 99,999% mediante la adición de QoS
- 24 / 7 vigilancia preventiva

Estándares

- Ethernet.



Se basa en los estándares 802.3 de IEEE

802.3a 1985 Original 802.3: 10BASE-5 10BASE-2 10BROAD-36

802.3c 1986 Especificaciones de repetidores

802.3d 1987 FOIRL (enlace de fibra)

802.3i 1990 10Base-T Ethernet sobre par trenzado de cobre

802.3j 1993 10Base-F Ethernet sobre fibra

802.3u 1995 100Mbps Ethernet

802.3x e 802.3y 1997 operación full duplex

802.3z 1998 1000Base-X (Gigabit Ethernet)

802.3ab 1999 1000Base-T (GE sobre par trenzado)

802.3ac 1998 Extensiones de trama (hasta 1522 bytes) para VLANs

802.3ad 2000 link aggregation

802.3ae 2002 10 GE

802.3af 2003 PoE (Power over Ethernet). Hasta 15W

802.3ah 2004 Ethernet in First Mile

802.3an 10 Gbase-T (en draft)

Bridging en 802.1D

802.1w Cambios y mejoras en el spanning tree

802.1s Múltiples spanning trees

Estándares de Ethernet Sobre Fibra Óptica

ITU-T G.7041 Generic Framing Procedure (GFP)

ITU-T X.86 Link Access Protocol (LAPS)

ITU-T H.707 Virtual Concatenation (VCAT)

ITU-T G.7042 Link Capacity Adjustment Scheme (LCAS)

Otros:

IEEE 802.1X Port Based Network Access Control

IEEE 802.1D Ethernet switching

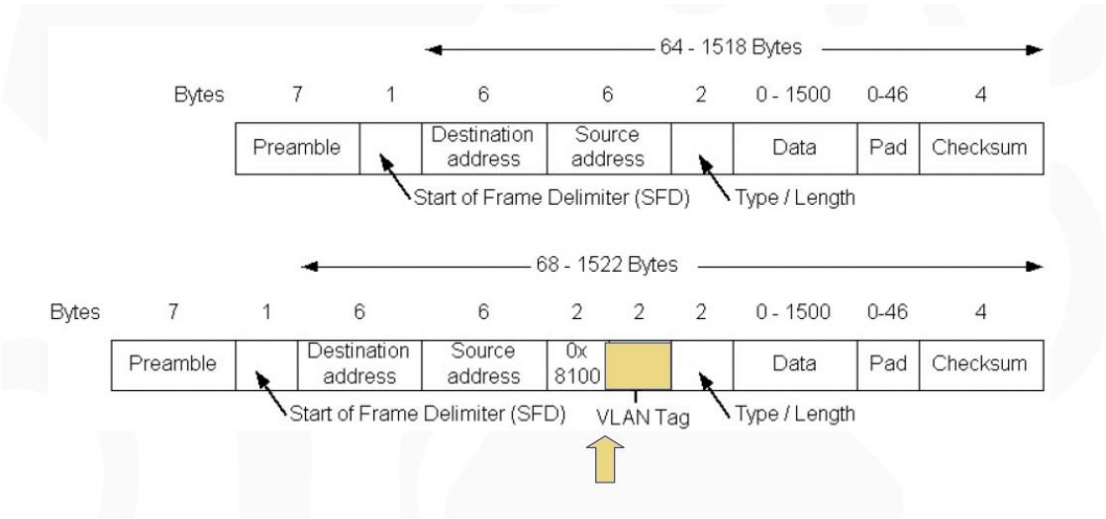
IEEE 802.1Q Virtual LAN (VLAN)

IEEE 802.1P Priorización de tráfico a nivel 2

IETF: MPLS Multi-Protocol Label Switching

IEEE 802.17 Resilient Packet Ring (RPR)

Trama Ethernet



Trama ethernet El tamaño de trama varía desde 64 a 1518 Bytes,

Longitud/Tipo- 2 bytes. Este campo indica el número de bytes de datos del cliente MAC que están contenidos en el campo de datos de la trama o el ID del tipo de trama si la trama se ensambla utilizando un formato opcional.

Datos- Es una secuencia de nbytes (48=< n =<1500) de cualquier valor. El marco total mínimo es de 64 bytes.

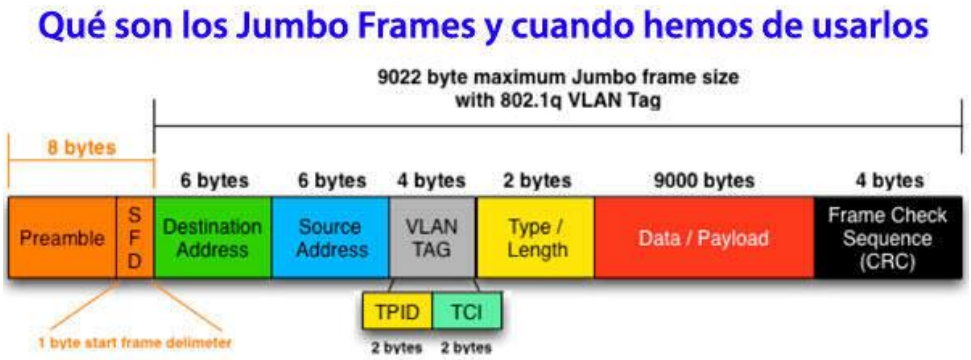
Secuencia de verificación de trama (FCS) - 4 bytes. Esta secuencia contiene un valor de verificación de redundancia cíclica (CRC) de 32 bits, que crea el MAC de envío y vuelve a calcular el MAC de recepción para verificar si hay tramas dañadas.

El tamaño de trama varía desde 64 a 1518 Bytes, y de 68 a 1522

esto ocurre cuando se usa el identificadir (tag) de VLAN

o se usa jumboframes.

Los Jumbo Frame son una función soportada por las tarjetas de red y los switches, se diseñó específicamente para las redes Gigabit que requerían de paquetes de información superiores en tamaño.



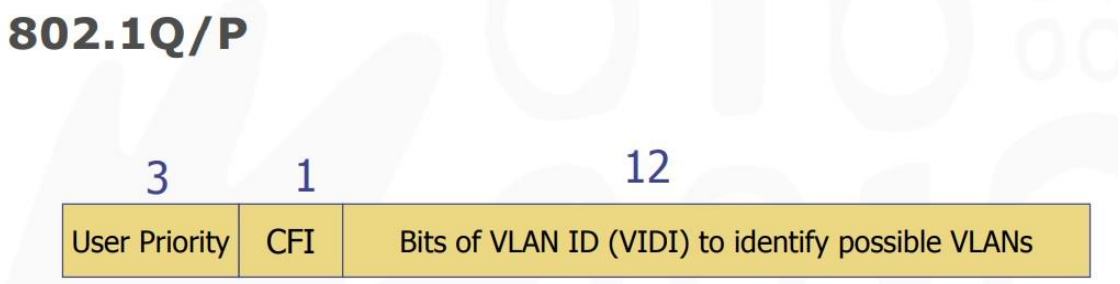
Los switches son dispositivos de Capa 2. Sólo utilizan la información del encabezado de la trama de Ethernet para enviar paquetes.

El encabezado de la trama no contiene la información que indique a qué VLAN pertenece la trama.

Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen.

Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q.

802.Q/P Encabezado de Encapsulación.



Prioridad del usuario**:** define la prioridad del usuario, otorgando ocho (2^3) niveles de prioridad.

IEEE 802.1P define la operación para estos 3 bits de prioridad de usuario.

CFI**:** el indicador de formato canónico siempre se establece en cero para los conmutadores Ethernet. CFI se utiliza por motivos de compatibilidad entre la red de tipo Ethernet y la red de tipo Token Ring. Si una trama recibida en un puerto Ethernet tiene un CFI establecido en 1, entonces esa trama no debe reenviarse como lo está a un puerto sin etiquetar.

VID- VLAN ID es la identificación de la VLAN, que es utilizada básicamente por el estándar 802.1Q. Tiene 12 bits y permite la identificación de 4096 (2^12) VLAN. De los 4096 VID posibles, se utiliza un VID de 0 para identificar las tramas prioritarias y se reserva el valor 4095 (FFF), por lo que las configuraciones de VLAN máximas posibles son 4094.

Ethernet SLA.

Dos basicas: Bandwidth profile y clases de servicio.

Bandwith profile. Especificación similar a FR.

CIR. Siempre disponible AB minimo. PIR.Máximo bit rate a la cual el cliente puede mandar trafico.

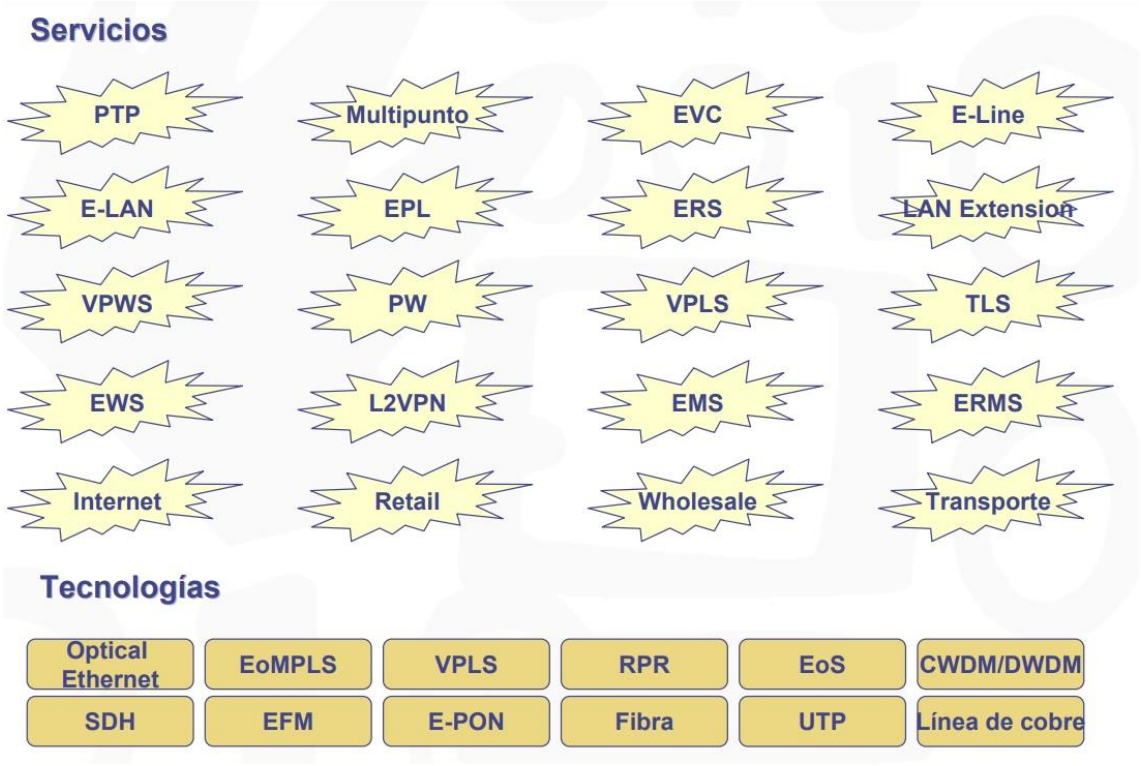
Para cualquier aplicación el trafico es tratado igual. No sirve para servicios customizados.

Clases de Servicio.

Diferentes aplicaciones tienen diferentes requerimientos de transporte.

Contrato similar al CIR. Pero enfocado a servicios mas que al ancho de banda.

Ejemplos : trafico de voz, trafico optimizado a la latencia, optimizado al throughput.(Rendimiento)



Servicios

Conectividad Internet

Transparent LAN service (punto a punto LAN to LAN)

L2VPN (punto a punto o multipunto a multipunto LAN to LAN)

LAN a Frame Relay/ATM VPN

Metro transport (backhaul)

VoIP

EVC Ethernet Virtual Connection es una asociación entre dos o más UNIs. Es creada por el proveedor del servicio para un cliente.

Una trama enviada en un EVC puede ser enviada a uno o más UNIs. Nunca será enviada de vuelta al UNI de entrada. tampoco será enviada a un UNI que no pertenezca al EVC.

Las EVC´s pueden ser:

Punto a punto (E-Line)

Servicio Ethernet LAN (E-LAN).

Este servicio provee conexión multipunto. Cada sitio (UNI) es conectado a el EVC multipunto y se pueden establecer diversos rate para cada UNI (ej: UNI 1 y 3 10Mbps - UNI 2 y 4: 100Mbps).

Una ELAN puede operar con ancho de banda dedicado o con un ancho de banda compartido , Multipunto a multipunto (E-LAN).

EPL, Ethernet Private Line, es un servicio EVC punto a punto con un ancho de banda dedicado. El cliente siempre dispone del CIR.

Normalmente opera en canales SDH (en NGN) o en redes MPLS.

Es como una línea en TDM, pero con una interfaz ethernet

EVPL: Ethernet Virtual Private Line.

En este caso el cliente dispne de un CIR.

Es similar a Frame Relay. Se suele implementar con canales TDM compartidos o con redes de conmutación de paquetes usando Switchs y/o routers.

EPLan: Ethernet Private LAN

Suministra una conectividad multipunto entre dos o más UNI´s, con un ancho de banda dedicado.

EVPLan: Ethernet Virtual Private LAN

Otros nombres:

VPLS: Virtual Private Lan Service

TLS: Transparent Lan Service

VPSN: Virtual Private Switched Network

Está limitado a 4096 VLAN.

Es el servicio más rentable desde el punto de vista del proveedor.

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

Tecnologías

Ethernet sobre “wavelengths” (longitudes de onda) (EoW)

Ethernet sobre SONET/SDH (EoS)

Optical Ethernet (native Ethernet nativo sobre fibra óptica)

Ethernet en “first mile” (EFM) sobre cobre ó fibra: IEEE

802.3ah

Ethernet over SONET/SDH (EOS)

Resilient Packet Ring (RPR)

Ethernet Transport

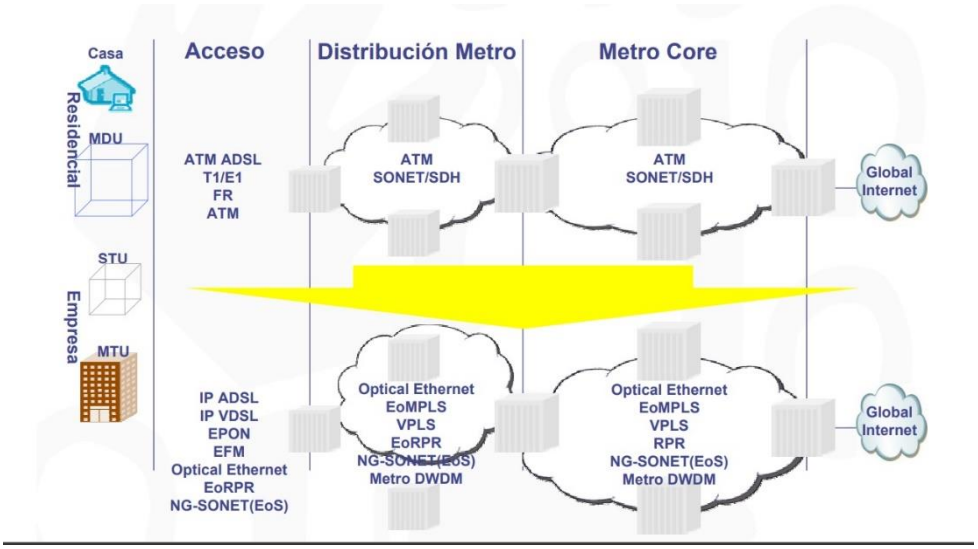
Ethernet sobre MPLS

Evolución de Ethernet

Servicio Ethernet

Algunos se están ofreciendo desde hace años. La diferencia está

en que ahora se ofrecen usando conectividad Ethernet.



	Service Type	Port-based Service	VLAN-aware Service
EVC Services	E-Line P2P EVC	Ethernet Private Line (EPL)	Ethernet Virtual Private Line (EVPL)
	E-LAN MP2MP EVC	Ethernet Private LAN (EP-LAN)	Ethernet Virtual Private LAN (EVP-LAN)
	E-Tree RMP EVC	Ethernet Private Tree (EP-Tree)	Ethernet Virtual Private Tree (EVP-Tree)
OVC Services	E-Access	Access EPL	Access EVPL
		Access E-Line P2P OVC with 1 UNI and 1 ENNI	
		Access E-LAN MP2MP OVC with UNI(s) and 1 ENNI	
	E-Transit	Transit E-Line P2P OVC with 2 ENNIs	
		Transit E-LAN MP2MP OVC with ENNIs	

EVC: Ethernet Virtual Connection
OVC: Operator Virtual Connection
MP2MP: Mulitpoint-to-Multipoint
RMP: Rooted MultiPoint
EPL: Ethernet Private Line
EVPL: Ethernet Virtual Private Line

Aparte de la IEEE , existe la MEF METRO ETHERNET FORUM sus objetivos son Las principales competencias del MEF son definir:

■ Servicios Ethernet para las redes de transporte metropolitanas Dichos servicio deberán ser suministrados sobre redes Metro de Ethernet nativo y podrán estar soportadas por otras tecnologías de transporte

■ Tecnologías de transporte de ethernet para áreas metro “carrier-class”, especificando arquitecturas, protocolos y gestión

■ Con menor prioridad el MEF también se encarga de definir:

El trabajo que deben hacer otras organizaciones sobre otras

tecnologías de transporte (actividad de enlace y coordinación)

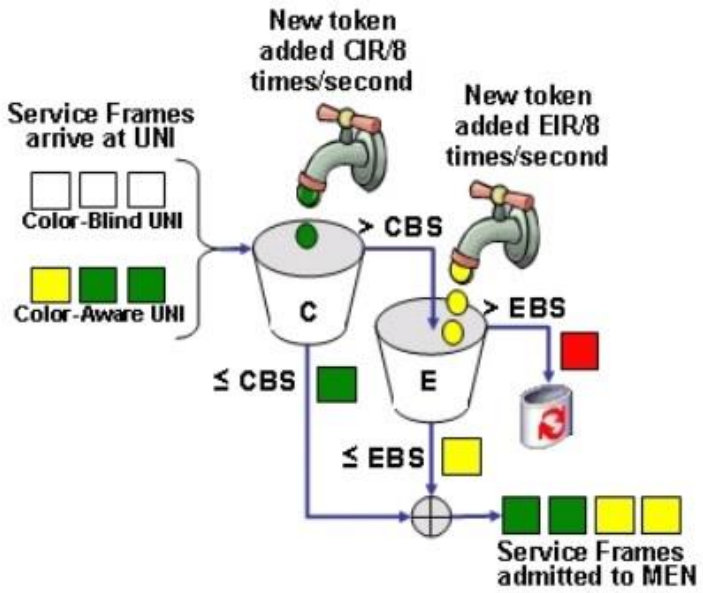
Paralelamente al trabajo del IEEE, el MEF viene desarrollando la definición de los servicios Carrier Ethernet desde 2001. Las primeras definiciones (recuerde E-Line, E-LAN, E-Tree) ahora forman parte de los catálogos de servicios de la mayoría de los proveedores de servicios. Un poco más tarde se introdujeron los servicios mayoristas E-Access y E-Transit para permitir a los proveedores de servicios enlazar servicios de extremo a extremo usando redes de múltiples operadores. Con una mirada hacia el futuro, el MEF introdujo su marco de Orquestación de Servicios de Ciclo de Vida para facilitar una variedad de servicios de conectividad además de Ethernet propiamente dicho (como IP, óptica, L4+) y servicios de valor agregado (como seguridad) además de aquellos. Nuevamente, las innovaciones no van a detenerse en un futuro cercano.

Parámetros de tráfico

Se define un Bandwith Profile (B.P), que está compuesto por 4

parámetros que definen el bandwidth o throughput del servicio

- **CIR** (Committed Information Rate)
- **CBS** (Committed Burst Size)
- **EIR** (Excess Information Rate)
- **EBS (Excess Burst Size)**
- **PIR** (Peak Information Rate)
- **MBS** (Maximum Burst Size)



■ CIR (tasa de información comprometida)

■ CBS (Tamaño de ráfaga comprometido)

EIR Tasa de Exceso de Información)

EBS Exceso de tamaño de ráfaga)

Existe un Service Frame Color, el color de la trama determina qué

tipo de Bandwith Profile tiene que ver con el **Encabezado de Encapsulación**

Un servicio puede tener 2 o más colores.

CIR (Committed Information Rate) Es el rate promedio el cual las

tramas pueden ser transmitidas por la red de acuerdo a una

performance establecida (ej: SLA)

CBS (Committed Burst Size)

Además de esto, también existe el caso de que su proveedor puede ser flexible. Por ejemplo, su proveedor es flexible para 1 Mb de su ancho de banda y si no excede el valor de 11 Mb, entonces su tráfico no será descartado ni moldeado. Este es su CBS (Tamaño de ráfaga comprometido). CBS es el tamaño del tráfico de clientes que se permite en ráfagas.

EIR (Excess Information Rate) Es el rate promedio el cual las

tramas pueden ser transmitidas por la red sin una performance

establecida , es el tráfico máximo permitido en un horario no ocupado sin ninguna garantía.

EBS (Excess Burst Size) EBS es la flexibilidad de su proveedor para EIR como CBS para CIR.

PIR (Peak Information Rate) es el punto de ancho de banda superior del tráfico permitido en horas no ocupadas sin ninguna garantía.

Al ingreso del Perfil de ancho de banda por atributo de servicio de identificador de CoS

se aplica a todos los marcos de servicio dentro de un EVC identificado a través de

los valores de bit de prioridad de usuario IEEE 802.1p del cliente en el

Campo IEEE 802.1Q

. En terminología MEF, el campo 802.1p

se refiere a Customer Edge VLAN , (VLAN de borde de cliente) , CoS o CEVLAN CoS.

En resumen, los atributos del servicio de perfiles de ancho de banda son como sigue.

Cada perfil de ancho de banda consta de parámetros de tráfico <CIR, CBS, EIR, EBS, CM>.

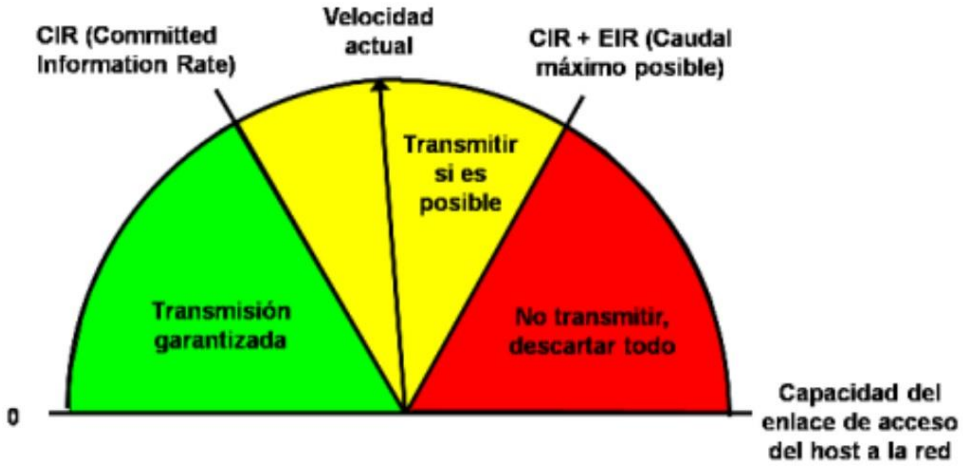
• Perfil de ancho de banda de ingreso por UNI de ingreso

• Perfil de ancho de banda de entrada por EVC

• Perfil de ancho de banda de entrada por CoS(classe of service)

Conformance	Color	Service Frame Delivery
CIR Conformant		Service Frames green and delivered per the performance objectives specified in the SLA/SLS.
EIR Conformant		Service Frames are yellow and may be delivered but with no performance assurances.
None		Service Frames are red and dropped.

Service Frame Color Summary



PARÁMETROS DE PERFORMANCE

Frame delay (Retardo de trama)

Son retardos presentados en la transmisión, es un parámetro crítico y tiene un alto impacto en la QoS de las aplicaciones en tiempo real.

Frame Jitter

Es la variación de los retardos (delay), es un parámetro crítico en las aplicaciones de tiempo real, (Telefonía IP / video)

Frame loss (Pérdida de trama)

Es el porcentaje de tramas que no son transmitidas correctamente en un intervalo de tiempo, está definido como:

Cada clase de servicio puede ofrecer diferentes niveles de desempeño, es utilizado por el proveedor de servicio para brindar distintas características de sus servicios

% tramas no trasmitidas = (1 X Numero de tramas entregadas a destino % total de tramas enviadas)

X100

Categorías de los servicios

Las categorías de servicios se agrupan en:

- Ethernet Physical Interface (UNI)
- Traffic Parameters (EVC)
- Performance Parameters (EVC)
- Class of Service (EVC)
- Service Frame Delivery (EVC)
- VLAN Tag Support (UNI)
- Service Multiplexing (UNI)
- Bundling UNI)
- Security Filters (UNI)

Atributos:

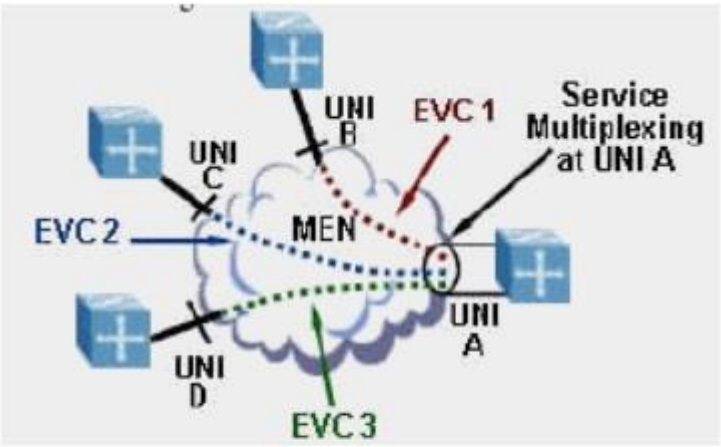
Atributos de UNI:

- identificador, tipo de medio, velocidad, duplex, etc)
- Atributo de soporte de VLAN tag
- Atributo de multiplexación de servicio
- Bundling attribute
- Security filters attribute

Atributos de EVC:

- Parámetros de tráfico (CIR, PIR, in, out, etc)
- Parámetros de prestaciones (delay, jitter, etc)
- Parámetros de Clase de Servicio (VLAN-ID, valor de .1p, etc)
- Atributo de Service frame delivery
- Unicast frame delivery
- Multicast frame delivery

SERVICIO DE MULTIPLEXACIÓN



Multiplexación

Se utiliza para que una UNI soporte varios EVC

Reduce el costo de equipamiento

Ahorra espacio, energía y cableado

Simplifica las activaciones de nuevos

Este servicio es usado para soportar varios canales virtuales (EVC) de diferentes velocidades simultáneamente en un solo enlace de conexión (UNI) [figura 7]. Usando multiplexación se elimina la necesidad de tener diferentes interfaces físicas para tener enlaces a diferentes velocidades.

BUNDLING

Este servicio permite que dos o mas CD VLAN Ids puedan ser mapeadas a un mismo EVC en la UNI

SECURITY FILTERS

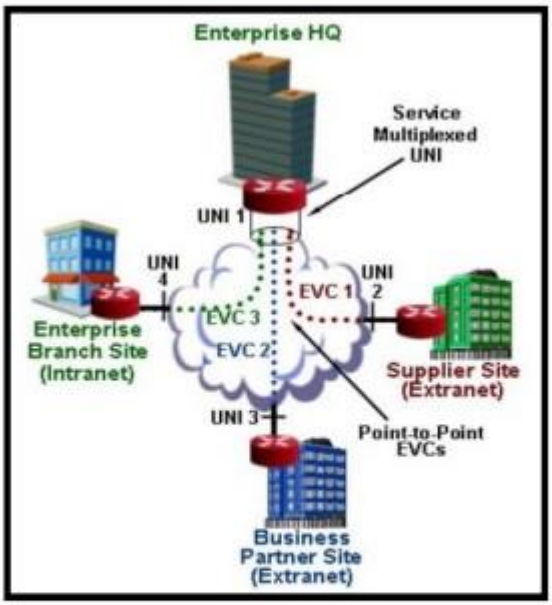
Se pueden establecer Access Control List, para adicionar seguridad o administrar el tráfico.(por ej: lista de direcciones MAC a las cuales se les puede garantizar el acceso.

Servicios Ofrecidos

1 Acceso a Internet dedicado

El cliente tiene servicios E-Line separados (UNI 1 y 2), no es necesario el uso del tag VLAN ID y se utiliza el servicio de multiplexing (UNI 3).

2 Intranet extranet L2 VPN

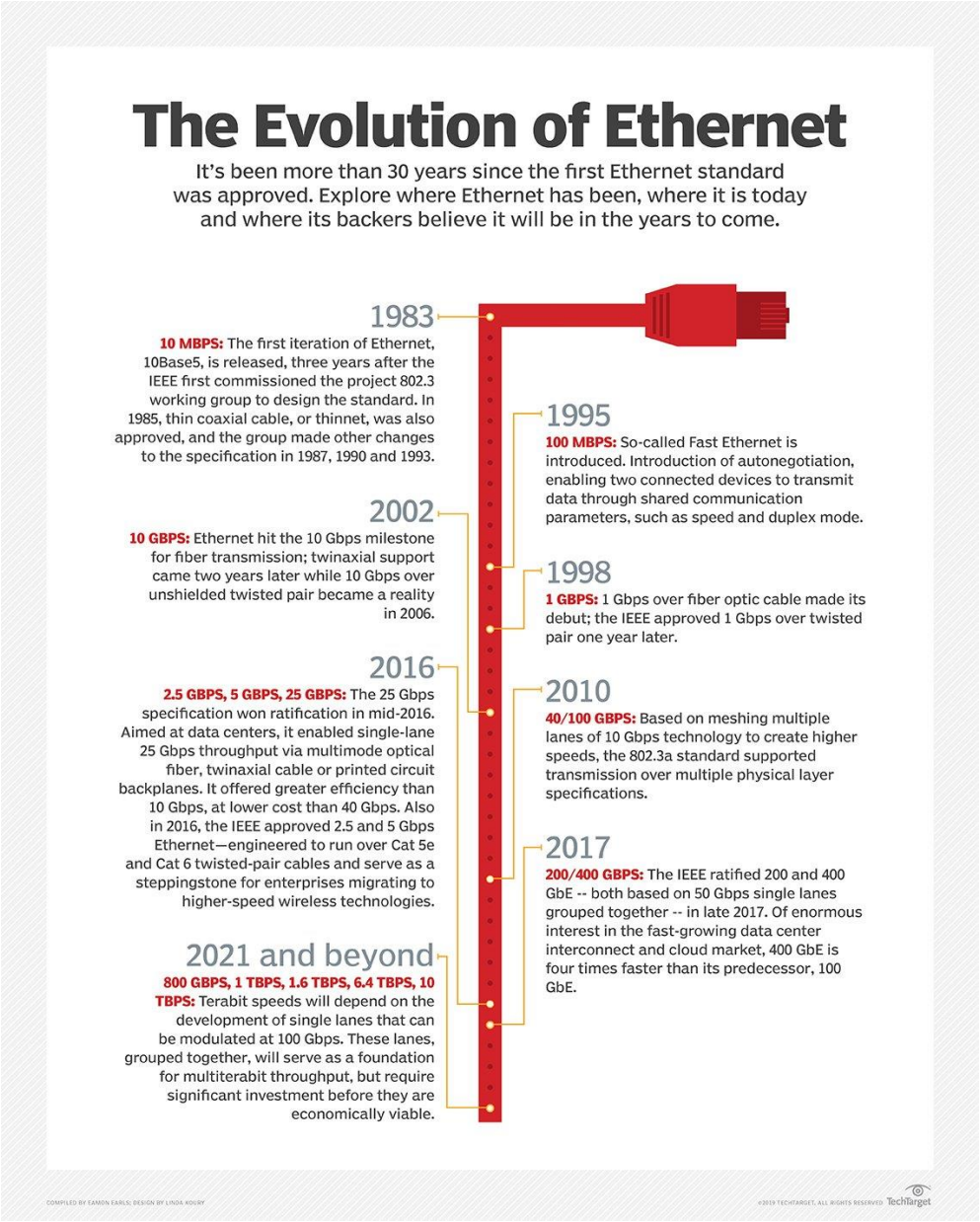


	CE-VLAN ID	EVC
CE-VLAN ID / EVC Map	10, 11, 12	1
	20, 21, 22	2
	30, 31, 32	3

En este caso se utilizan 3 EVC PtP. Utiliza VLAN soportando (CE VLAN Ids). Hay un mapeo de CE VLAN Ids con los EVC.
También utiliza multiplexing.
Si el cliente utilizará CoS se debe usar CoS preservation

3 Extencion de Lan

Lo más conveniente es usar un servicio E-LAN. Utiliza VLAN soportando (CE VLANIds).
Todas las CE VLAN están mapeadas al mismo EVC y no utiliza multiplexing.
Si el cliente utilizará CoS se debe usar CoS preservation



Preguntas

Redes por software

1. Cuáles son las partes en las que se divide una típica arquitectura de SDN.?
    a. Aplicaciones.
    b. Controladores.
    c. Dispositivos de red.
2. Nombrar alguna ventaja de las redes definidas por software
    a. Mayor control de una velocidad y flexibilidad superior.
    b. Infraestructura de la red personalizable
    c. Seguridad solida
3. ¿En qué se diferencian las SDN de las redes tradicionales?
    La diferencia clave entre las SDN y las redes tradicionales es la infraestructura: las SDN están basadas en software, mientras que las redes tradicionales están basadas en hardware. Ya que el plano de control está basado en software, las SDN son mucho más flexibles que las redes tradicionales. Permiten que los administradores controlen la red, cambien los ajustes de configuración, aprovisionen recursos y aumenten la

capacidad de la red, todo ello desde una interfaz de usuario centralizada y sin necesidad de añadir más hardware.

4. ¿Cuáles son los modelos de SDN?
    a. Abierta
    b. Por API
    c. Por superposición de SDN.
    d. SDN hibrida.

METRO

1. Nombren dos servicios que se proveen en metro eternet.
   EPL, Ethernet Private Line, es un servicio EVC punto a punto con un ancho de banda dedicado. El cliente siempre dispone del CIR. Normalmente opera en canales SDH (en NGN) o en redes MPLS. Es como una línea en TDM, pero con una interfaz ethernet Multipunto a multipunto (E-LAN). Una E-Line puede operar con ancho de banda dedicado ó con un ancho de banda compartido.

2. Nombren 2 tecnologías de capa fisica que soporta.
   Ethernet sobre SONET/SDH (EoS)
   Optical Ethernet (native Ethernet nativo sobre fibra óptica)

3. ¿Qué es la UNI?
   UNI: User Network Interface

4. ¿Qué es la EIR?
   (Excess Information Rate) Es el rate promedio el cual las tramas pueden ser transmitidas por la red sin una performance establecida, es el tráfico máximo permitido en un horario no ocupado sin ninguna garantía.

5. ¿Cuál es el estandar de la ieee que rige ethernet?
   Se basa en los estándares 802.3 de IEEE

6. ¿qué es la MEF?
   METRO ETHERNET FORUM y las principales competencias del MEF son definir:
   - Servicios Ethernet para las redes de transporte metropolitanas. Dichos servicios deberán ser suministrados sobre redes Metro de Ethernet nativo y podrán estar soportadas por otras tecnologías de transporte
   - Tecnologías de transporte de ethernet para áreas metro “carrier-class”, especificando arquitecturas, protocolos y gestión

Índice

Contenido

ADSL 66

Características: 66

Modulación en ADSL 67

Ventajas ADSL 67

CATV 69

¿Qué es CATV? 69

Redes modernas 69

Cable Modem 70

FTTX 71

FTTH - Fiber-to-the-home 71

FTTO - Fiber-to-the-office 73

FTTB - Fiber-to-the-basement 71

FTTP - Fiber-to-the-premises 73

FTTN - Fiber-to-the-node 73

FTTA - Fiber-to-the-antenna 73

Tecnología FTTx 72

Diseño y planificación de redes 72

¿FTTH (fibra óptica hasta la casa) O HFC (híbrido de fibra coaxial)? 73

Ventajas de FTTH 73

Ventajas de HFC 73

Instalación 73

Transmisión de datos 73

Velocidad 73

Ancho de banda 73

Precio 73

MPLS 74

¿Qué es? 74

¿Cómo funciona una red MPLS? 74

Partes importantes en MPLS 75

La etiqueta: 75

Bits experimentales 75

Parte inferior de la pila: 75

Tiempo de vida 75

Beneficios de una red MPLS 75

- **Mayor rendimiento en la interconexión de sedes** 75
- **Optimiza el presupuesto** 75
- **Es adaptable a cualquier empresa** 76
- **Mejor experiencia de usuario** 76

Conclusión 76

Preguntas 76

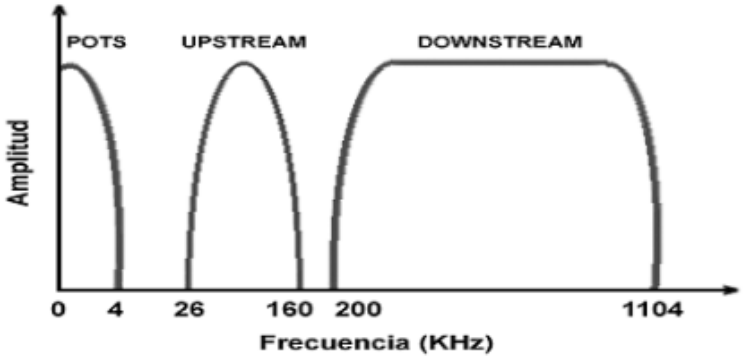
Referencias **¡Error! Marcador no definido.**

ADSL

Es el servicio de acceso a Internet por banda ancha que brindan mayormente las empresas telefónicas.

Se caracteriza por utilizar para el tráfico de datos el mismo cable telefónico que para las transmisiones de voz, pero en bandas de frecuencia diferentes logrando de esta forma la simultaneidad de ambos tipos de comunicación.

Aprovechando que la telefonía básica utiliza únicamente bajas frecuencias (hasta 16 KHz), ADSL utiliza la porción del espectro que va desde 25 KHz, hasta 1,1 MHz.



Dentro de la arquitectura ADSL se encuentran 3 elementos principales que hacen posible esta tecnología: un Módem ADSL, un Filtro y el DSLAM (Digital Subscriber Line Access Multiplexer).

El servicio de voz y datos viajan dentro del par de cobre en frecuencias independientes (lo cual hace posible utilizar simultáneamente ambos), el filtro tiene la función de separar las frecuencias de la línea para entregar la voz al aparato telefónico y los datos al modem ADSL.

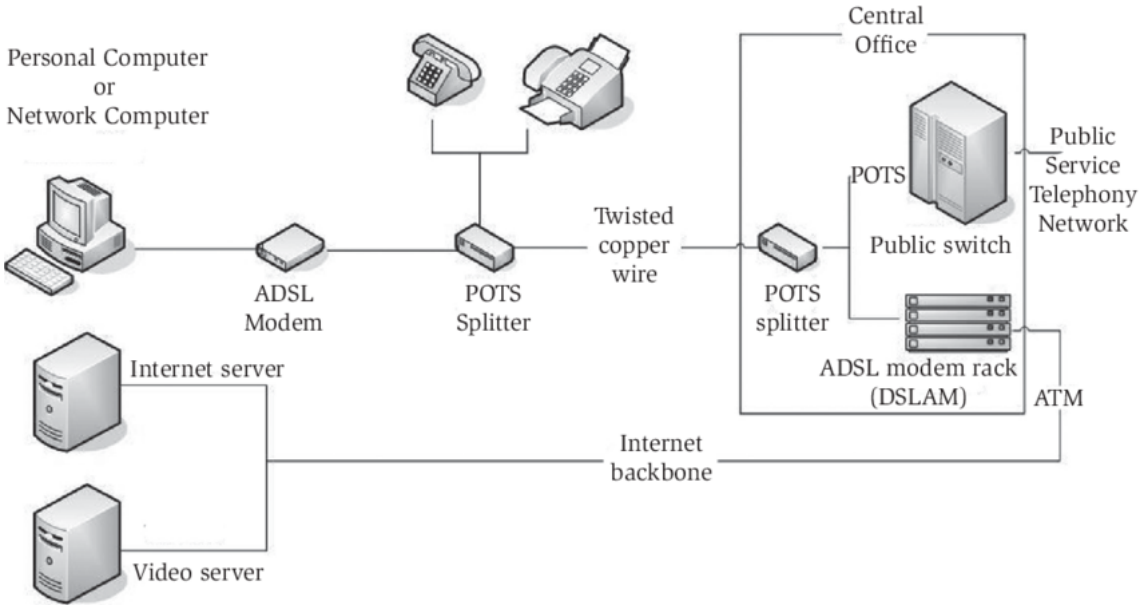
El módem (modulador / demodulador) ADSL toma los datos y los entrega a la computadora o red LAN del cliente.Dentro de la central Telmex un equipo denominado DSLAM separa las frecuencias entregando el servicio de voz a la red telefónica tradicional y los datos a la velocidad contratada a la red de datos o Internet directamente. Al ser la tecnología ADSL una tecnología sobre líneas de cobre, no aplica para casos de clientes servidos con accesos de fibra óptica.

Un sistema ADSL está compuesto por los siguientes dispositivos:

- Un ATU-C: ADSL transceiver unit-central office (Transceptor ADSL central) que es la terminal situada en la central.
- Un ATU-R: ADSL transceiver unit-remote (Transceptor ADSL remoto, módem ADSL, CPE), que es el modem situado en la casa del usuario.
- Un Splitter (Divisor). Es el filtro que separa las señales de ADSL y POTS
- Un DSLAM: Digital subscriber line access multiplexer (Multiplexor de acceso), que es el elemento de red que concentra el tráfico de los usuarios finales y estará conectado de alguna forma a la red de datos (backbone) del proveedor.

Características:

- Hace uso del par trenzado de cobre instalado para brindar servicio de telefonía básica.
- Tecnología no conmutada (siempre conectado)
- Velocidades diferentes de bajada y subida.
- Mercado: Hogares y Negocios.



El sucesor de ADSL es ADSL2/2+ y la diferencia más notable es la velocidad y la tecnología. Mientras que ADSL puede llegar a niveles de descargas de 8 Mbps (megabytes por segundo), ADSL 2/2+ llega hasta 24 Mbps. Sin embargo, ambas tienen el mismo límite máximo de envío: 1 Mbps.

El equipo que desarrolló la ADSL2/2+ decidió aumentar solamente la tasa de descarga (sin alterar la tasa de subida). Esto fue de acuerdo con el perfil de tráfico típico de los usuarios de ADSL, 1 Mbps sería suficiente para sus necesidades.

Modulación en ADSL

En un principio se desarrollaron dos técnicas de modulación diferentes para ADSL: la modulación CAP (Carrierless Amplitude Phase) y la modulación DMT (Modulation Discrete Multi-Tone). Ambas basadas en el sistema de modulación en cuadratura o QAM8 aunque cada una lo adopta de forma distinta.

Finalmente los organismos de estandarización (ANSI y ETSI) optaron por la solución DMT, con mayor rendimiento.

La solución DMT emplea varias portadoras, como si de diversos módems de banda vocal se tratara. Cada una de las portadoras, denominadas subportadoras, se modulan en cuadratura (de aquí el uso de QAM) por parte del flujo de datos a transmitir. Las subportadoras están separadas entre sí 4,3125 KHz y el ancho de banda que ocupa cada una de ellas es de 4 KHz. El número de subportadoras en el módem del usuario es de un máximo de 32, pudiendo llegar a 256 en el lado de la central.

Ventajas ADSL

- Conexión permanente a Internet con TARIFA PLANA.
- Velocidad hasta 2 Mbps.
- Utilización simultánea del servicio ADSL y del servicio telefónico básico.
- Tarificación independiente de ambos servicios (ADSL y telefónico básico).
- Acceso a todos los contenidos y servicios que ofrece Internet:
    - Servicios y contenidos de transmisión de datos.
    - Acceso a servicios de información (acceso a Internet, email, comercio electrónico, etc.).
- Acceso a servicios y contenidos de banda ancha:
    - Audio y vídeo difusión (radio o TV).

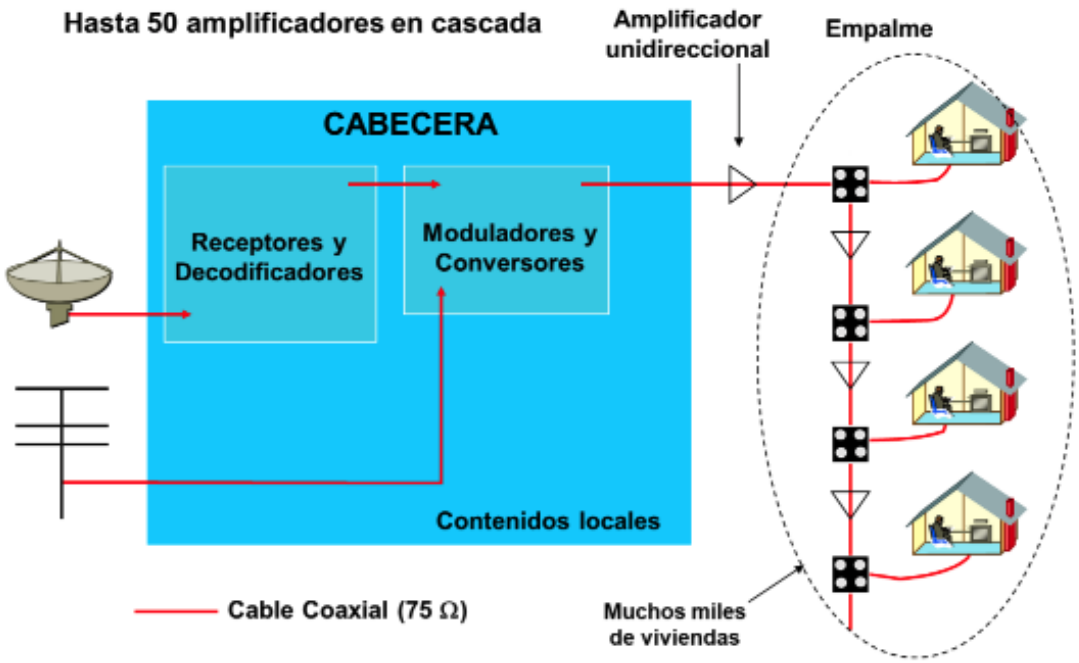
    - Audio y vídeo bajo demanda.
    - Audio y vídeo conferencia.
    - Acceso a bases de datos documentales.
    - Aplicaciones interactivas en red (juegos, software en red, etc.).
    - Teleformación.
- Servicios y contenidos se beneficiarán de una conexión permanente:
    - Acceso remoto y teletrabajo.
    - Trabajo en grupo.
    - Interconexión de redes de área local.

CATV

¿Qué es CATV?

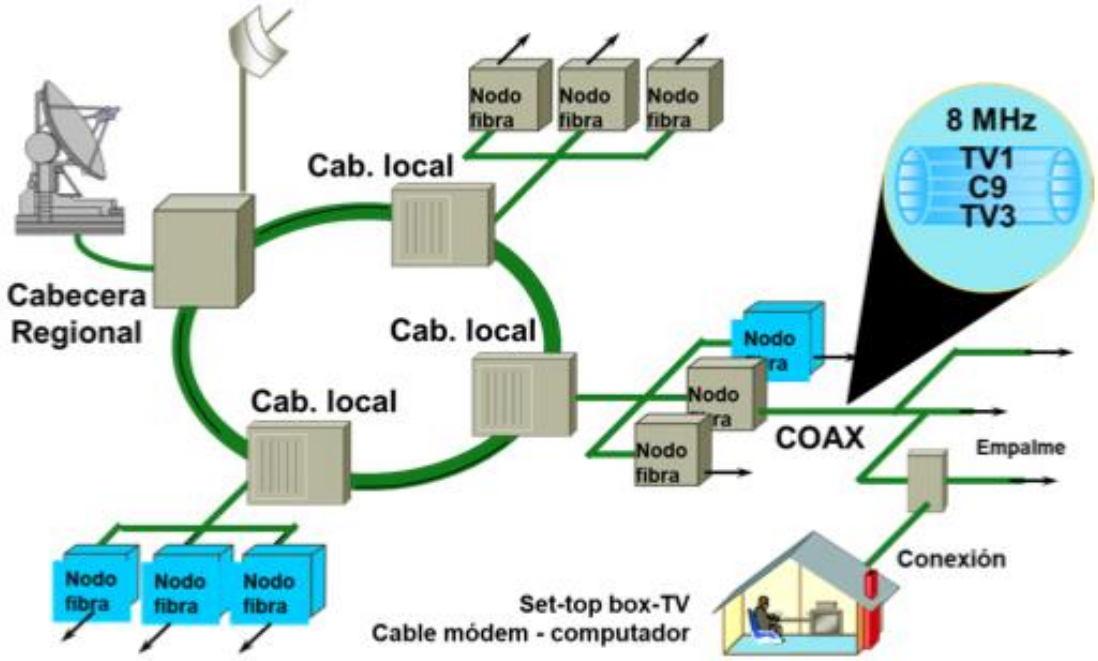
La televisión por cable o CATV (Community Antenna Television) es un sistema de televisión que se transmite a través de señales de radiofrecuencia que se reproducen en televisiones por medio de redes de fibra óptica y cables coaxiales. Además de CATV, dicho cable también puede proporcionar servicios de telefonía e internet. Este sistema aprovecha las redes de televisión por cable de fibra óptica o cable coaxial, para convertirlas en una línea digital o analógica. Los cables de televisión se distribuyen en las ciudades junto con los cables de electricidad y teléfonos a diferencia de la radiodifusión televisiva tradicional, por ondas de radio, en la que se requiere una antena de televisión para captar la señal emitida por la televisora. La televisión por cable surge por la necesidad de llevar señales de televisión y radiodifusión sonora,hasta hogares con mala recepción satelital que se encuentran en las urbes y no pueden colocar una antena. Esta tecnología ayuda a comunicar las ciudades de forma ordenada y estética.

Aparecieron en EE.UU a finales de los años 40 para resolver las malas condiciones de recepción de la señal de televisión. La solución consistía en instalar una antena en un sitio elevado con buenas condiciones de recepción, y desde allí distribuir la señal mediante cable coaxial a los usuarios.



Redes modernas

A finales de los años 80 empezaron a aparecer redes CATV con la arquitectura denominada HFC (Hybrid Fiber Coax). Tiene dos niveles jerárquicos, compuesto por fibra óptica y cable coaxial. El primer nivel está formado por un tendido de fibra óptica con topología de estrella que distribuye la señal desde el centro emisor hasta cada zona de la ciudad. Y un segundo nivel formado por un nodo que se encarga de convertir la señal óptica en eléctrica para su distribución final en cable coaxial.



Cable Modem

Una conexión del tipo "cable módem" es un híbrido entre una conexión por módem tradicional y una conexión LAN.

FUNCIONES DEL CABLEMODEM:

- Captar/generar señal de Radiofrecuencia
- Modular/demodular los datos
- Generar/verificar la información de control de errores (FEC)
- Encriptar/desencriptar la información
- Respetar protocolo MAC en Upstream
- Gestión y control del tráfico

FTTX

La fibra hasta “x” (Fiber to the “x”, FTTx) es un término genérico que se emplea para describir una amplia variedad de opciones de arquitectura de redes de banda ancha que emplean fibra óptica para algunos o todos los últimos tramos de conectividad. La tecnología FTTx, donde la “x” representa el punto de terminación de la fibra, engloba diferentes implementaciones de fibra óptica como:

FTTH - Fiber-to-the-home

La fibra hasta el hogar (FTTH) crea una conexión directa de fibra óptica a la caja de conexiones del residente, con lo que se ofrece el ancho de banda más alto posible a los suscriptores individuales de la vivienda. Dado que esta opción también puede suponer un elevado coste de instalación, se da con más frecuencia en zonas de construcciones nuevas. Una posible desventaja de la FTTH es la ubicación de la línea eléctrica. La energía eléctrica no se puede suministrar por los cables de fibra óptica, por lo que estas implementaciones pueden requerir la instalación de líneas eléctricas completamente independientes. A pesar de estas dificultades, la FTTH se ha convertido en una de las aplicaciones más frecuentes en todo el mundo.

FTTO - Fiber-to-the-office

La fibra óptica llega hasta el interior de la misma oficina del abonado. Es básicamente igual a FTTH pero con configuraciones específicas para empresas.

FTTB - Fiber-to-the-basement

La fibra hasta la acometida del edificio (FTTB) es similar a la FTTH, excepto por el hecho de que la terminación de la fibra se realiza en un lugar que no es un domicilio privado. La “B” también puede referirse a una empresa (“business”) o a un sótano (“basement”). La terminación en un sótano se suele encontrar en una vivienda multifamiliar en la que la fibra óptica se incorporaría a una determinada sala de control eléctrico.

FTTP - Fiber-to-the-premises

La fibra hasta las instalaciones (FTTP) es una designación general que incluye la FTTH y la FTTB. Lo que tienen en común todas las configuraciones de FTTP es que la fibra óptica se extiende más allá de los límites de la propiedad, tanto si se trata de un domicilio, un edificio de apartamentos, un pequeño comercio o un colegio.

FTTN - Fiber-to-the-node

La fibra hasta el nodo (FTTN) incorpora enlaces de fibra óptica que terminan en el nodo central próximo a los negocios o los domicilios de los usuarios finales. Desde la ubicación del nodo, la conexión se finaliza por medio de la infraestructura de cable de cobre o coaxial existente. Una configuración de FTTN típica puede prestar servicio a cientos de clientes desde un solo nodo. El nodo se encuentra normalmente a 1,6 km o menos de todas las ubicaciones de los clientes, ya que un segmento coaxial de mayor longitud tiene más probabilidades de afectar a la velocidad de forma significativa.

FTTC - Fiber-to-the-cabinet

La fibra hasta la acera (FTTC) es un concepto engañoso en cierto modo, ya que el término “curb” (bordillo o acera en inglés) se emplea realmente para designar una caja o un poste en los que se instalan los componentes físicos de la red. La fibra hasta la acera es similar a la FTTN, pero son menos los clientes a los que se presta servicio desde cada ubicación y los

tendidos de cable coaxial tienen normalmente una longitud mucho menor. Esta configuración resulta útil porque se acerca a proporcionar un enlace de fibra óptica directo y no requiere una conexión de fibra óptica dentro de los límites de la propiedad.

FTTA - Fiber-to-the-antenna

La fibra hasta la antena (FTTA) es una arquitectura de red que emplea fibra óptica para distribuir las señales de una unidad de banda base (BBU) a un cabezal de radio remoto (RRH) cerca de la parte superior de la torre. La FTTA es un elemento esencial de la tecnología 5G, dado que la tecnología MIMO masiva conlleva más antenas y más cableado. El menor peso y resistencia al viento hacen que sea la sustituta lógica del cableado coaxial en esta aplicación. La FTTA permite también una ubicación más flexible de la BBU, ya que el enlace de fibra óptica al RRH puede abarcar largas distancias.

Tecnología FTTx

Las redes FTTx ofrecen la ventaja doble de velocidades de transmisión más altas y consumo de energía menor. Al trasladar la fibra óptica más cerca del usuario, se pueden aprovechar al máximo las técnicas más recientes de construcción, conexión y transmisión, y se disminuye la probabilidad de que se produzcan cuellos de botella en las redes coaxiales convencionales. Para que esto sea factible, han de aplicarse una planificación y una ejecución bien fundamentadas en todas las fases del ciclo de vida.

Diseño y planificación de redes

El primer paso para la implementación de esta tecnología es un diseño y una planificación bien coordinados. Antes de establecer el diseño detallado de la red FTTx, las primeras consideraciones en cuanto a la planificación incluyen la cantidad y la ubicación de los usuarios, la distribución de la fibra óptica y los puntos de acceso, así como los elementos arquitectónicos, como las tecnologías de red óptica pasiva (PON) que se incorporarán en el diseño. Entre los elementos de diseño detallado de nivel “microscópico”, se incluyen las ubicaciones de los empalmes, los patrones precisos de distribución y los cálculos de la pérdida general. Evitar los servicios existentes y establecer ubicaciones de equipos son algunas de las otras consideraciones que se incluyen en un diseño completo de una red FTTx.

¿FTTH (fibra óptica hasta la casa) O HFC (híbrido de fibra coaxial)?

Ventajas de FTTH

- La señal es más resistente a interferencias.
- Mayor cantidad de servicios disponibles.
- Ofrece alta velocidad para las conexiones de los diferentes servicios.

Ventajas de HFC

- Es más económico instalar este tipo de redes.
- Se puede aprovechar la conexión coaxial preexistente.
- El ancho de banda del cable coaxial es muy bueno.

Instalación

Si analizamos de cerca la instalación de estos dos tipos de conexiones, notaremos un par de detalles muy importantes: el precio y la complejidad. Es posible que, en la mayoría de los casos, sea más económico instalar una red HFC. Esto se debe a que, se aprovecha la conexión coaxial preexistente para el servicio de televisión.

Además, los puentes y separadores de señal para la red coaxial suelen ser más económicos. Por otra parte, la complejidad o sencillez de la instalación se inclina a favor de las redes FTTH, sin duda, estas son más sencillas de instalar. Además, existe una compatibilidad en la red de principio a fin, lo que resulta muy propicio.

Transmisión de datos

Uno de los aspectos que más nos interesa es la transmisión de datos hasta nuestro ordenador. La estabilidad de la conexión es muy importante, ya que de ello depende la calidad del servicio. La fibra directa a casa posee una característica que destaca sobre la HFC. Esta es que la velocidad de subida y bajada son más parecidas entre sí. Por el contrario, en la conexión HFC, en el momento en que la velocidad de bajada es mayor, la velocidad de subida disminuye notoriamente. De la misma forma, cuando hay excelente velocidad de subida, la de bajada es precaria.

Velocidad

La velocidad de transmisión de datos también puede variar mucho entre un tipo de infraestructura y otra. En condiciones óptimas la red FTTH es más veloz que la HFC. Pero, en algunos casos puede haber inestabilidad en su funcionamiento. Si la red híbrida se instala con precisión, esta ofrece una conexión más estable. Esto a diferencia de la FTTH, que con un mínimo descuido en su instalación está más vulnerable a interferencia o fallos.

Ancho de banda

En las redes híbridas, existe una particularidad en cuanto al ancho de banda. Por ejemplo, si se trata de un edificio o vecindario con pocos usuarios de Internet conectados en un mismo nodo, no hay mayores inconvenientes.

Una red híbrida coaxial podrá suministrar un ancho de banda estable y suficiente para que todos naveguen con comodidad. Sin embargo, a medida que aumentan los usuarios conectados, el ancho de banda que la fibra óptica proporciona no es tan amplio.

Por el contrario, cuando instalas una fibra directa en casa, el ancho de banda jamás varía. Ya que, los datos viajan desde un terminal de red óptica hasta tu vivienda, sin tener que compartir el ancho de banda con ningún usuario.

Precio

Muchas personas se preocupan por el costo que genera toda modalidad de red. En el caso de FTTH, los gastos de infraestructura quedan cubiertos por la compañía. Pero, en la mayoría de los casos la red híbrida será de más fácil instalación, y por tanto más barata. Esto considerando que la infraestructura de la red coaxial está previamente colocada en muchos conjuntos residenciales.

MPLS

¿Qué es?

La conmutación de etiquetas de protocolo múltiple (MPLS) establece rutas predeterminadas y eficientes. Con MPLS, la primera vez que un paquete ingresa a la red, es asignado a una clase de equivalencia de reenvío específica (FEC). Esta agrega una secuencia de bit corto. Es la etiqueta, el paquete. Cada enrutador de red tiene una tabla que indica cómo manejar los paquetes de un tipo de FEC específico. Por eso, una vez que el paquete ingresa en la red, los enrutadores no necesitan hacer un análisis de encabezado. Después, los enrutadores posteriores usan la etiqueta como un índice en una tabla que les proporciona un nuevo FEC para ese paquete.

Por eso la red MPLS tiene capacidad para manejar paquetes con características particulares. Por ejemplo, los provenientes de puertos particulares o los que transportan tráfico de tipos de aplicaciones particulares de forma consistente. Los paquetes que transportan tráfico en tiempo real, como voz o video, pueden asignarse fácilmente a rutas de baja latencia en toda la red. Esto es difícil con el enrutamiento convencional. Las etiquetas proporcionan una forma de adjuntar información adicional a cada paquete.

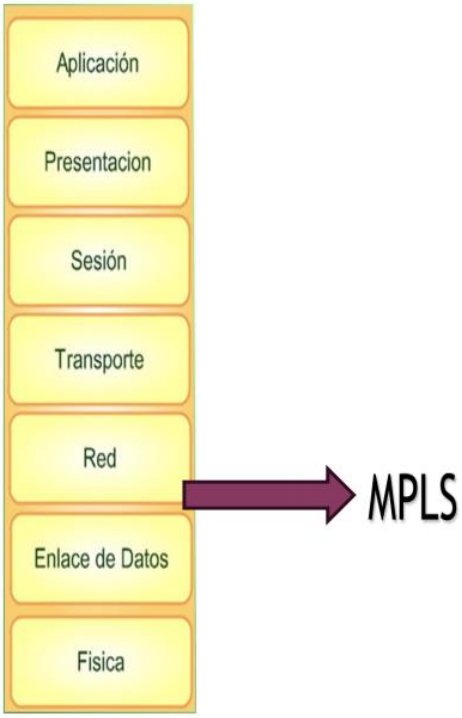
¿Cómo funciona una red MPLS?

Sabemos que este es un tema muy técnico y difícil de enter, por lo tanto vamos a explicarlo de manera más simple sobre cómo funciona la arquitectura MPLS

La interconexión de las redes MPLS se realiza incorporando en cada uno de los paquetes de datos que está siendo enviado a través de la red (voz, texto, video, imagen) un encabezado que contiene una o varias etiquetas agrupadas para establecer los circuitos virtuales según el propósito que llevan a cabo en los enrutadores para alcanzar su destino.

MPLS tiene la capacidad de aplicar QoS, acrónimo de Quality of Service (calidad de servicio), que establece varios mecanismos para asegurar la fluidez en el tráfico de la red. Para ello, prioriza el tráfico en función del tipo de datos.

Este protocolo opera entre la capa de enlace de datos (capa 2) y la capa de red (capa 3) del modelo OSI, gracias a esto puede juntar las características de las dos capas haciendo uso de la velocidad del forwarding y del control del routing



Partes importantes en MPLS

La etiqueta:

Contiene toda la información de los enrutadores MPLS para determinar hacia dónde se debe reenviar los datos para lograr una buena velocidad de transmisión

Bits experimentales

Se usan para mejorar la calidad de servicio, gracias a estos bits se le puede dar prioridad a paquetes de información sobre otros, dependiendo de las actividades que realicen los usuarios de la red.

Parte inferior de la pila:

Es el mensaje que indica a los enrutadores que no hay más paquetes que compartir y que los paquetes anteriores fueron enviados de forma exitosa.

Tiempo de vida

Es la cantidad de veces que un paquete puede ser enviado antes de ser descartado.

Beneficios de una red MPLS

- Mayor rendimiento en la interconexión de sedes

La arquitectura MPLS es recomendada para empresas o instituciones que tengan más de una sede en distintas ubicaciones, ya que permite una comunicación más fluida y con baja latencia y más segura en comparación con las redes tradicionales.

- Optimiza el presupuesto

Una red MPLS proporciona un menor coste de equipos, disminuye los problemas de seguridad, menor gasto de mantenimiento y más fluidez en la transmisión de datos. Se puede decir entonces que reduce costos en infraestructura y mantenimiento.

- Es adaptable a cualquier empresa

No importa el tamaño de la empresa, las redes MPLS pueden diseñarse a la medida de las necesidades.

- Mejor experiencia de usuario

Al tener una red fluida, tanto colaboradores como clientes pueden verse beneficiados de contar con una conectividad de primer nivel.

Conclusión

Como puedes ver, es una técnica eficiente para la comunicación internacional que sirve también para mantener ciertos nivel de seguridad de la información con oficinas remotas y franquicias. Sin embargo su costo es elevado y hay soluciones más prácticas disponibles para la conexión a nivel internacional. Una de las mejores alternativas para conectar con las entidades a nivel internacional es implementar las soluciones cloud que permiten almacenar información y comunicarse con los compañeros de trabajo. Adicionalmente una conexión a Internet rápida de nivel empresarial permite desplegar las soluciones cloud sin problemas y mantener un flujo de trabajo fluido a la altura de las exigencias del mercado.

Preguntas

1. ¿En la tecnología ADSL tenemos la misma velocidad de subida que de bajada?
    a. Si
    b. No
2. ¿Qué diferencia hay entre ADSL y ADSL2 +?
    a. Velocidad de subida
    b. Velocidad de bajada
    c. Velocidad de subida y de bajada
3. ¿ Un splitter ADSL se utiliza para separar el tráfico de bajada con el de subida ?
    a. Verdadero
    b. Falso, el splitter ADSL se utiliza para separar la frecuencia telefónica de la de internet.
4. ¿De qué otra modulación surge la modulación CAP utilizada en ADSL?
    a. QAM
    b. DTM
    c. WDM
5. ¿Para qué sirve CATV?
    a. Antena de televisión
    b. Antena de televisión + internet + teléfono
    c. Antena de amplificación de señal de internet
    d. Antena de electricidad
6. ¿Qué problema soluciona la antena CATV?
    a. Recepción de señal de TV
    b. Disminución de señal de internet
    c. Cableado extenso
7. ¿Cómo se conforma una red CATV HFC?
    a. Cable coaxial
    b. Fibra óptica

   c. Combinación de Fibra óptica, cable coaxial, modem
   d. Solo un modem
8. Mientras más amplificadores tenemos para las redes CATV ¿Qué sucede?
   a. Mejor la señal
   b. Degradan la señal
9. ¿Qué significa la sigla FTTB?
   a. Fiber to basement
   b. Fiber to buss
   c. Fiber to business
10. ¿El protocolo MPLS opera entre la capa 1 y capa 2 del modelo OSI?
   a. Verdadero
   b. Falso opera entre la capa 2 y 3
11. ¿Qué significan las siglas MPLS?
   a. Multi Protocol Language Switching
   b. Multi Protocol Label Switching
12. Ventajas de FTTH
   a. La señal es más resistente a interferencias.
   b. Mayor cantidad de servicios disponibles.
   c. Es más económico instalar este tipo de redes.
   d. Ofrece baja velocidad para las conexiones de los diferentes servicios.
13. La fibra ….. crea una conexión directa de fibra óptica a la caja de conexiones del residente.
   a. FTTO
   b. FTTH
   c. FTTP
   d. FTTN
14. ¿Cuál red ofrece la ventaja de doble velocidad de transmisión y consumo de energía menor?
   a. FTTx
   b. HFC

Índice

WIFI 79

Tipos de Wifi 80

Estándares que certifica la Alianza Wi-Fi 80

Dispositivos 81

Tipos de seguridad en conexiones WiFi 81

Ventajas e inconvenientes redes WiFi 82

WIMAX 83

Características 84

Tipos de WiMax 85

Dispositivos y funcionamiento WiMax 85

Estándares WIMAX 86

Ventajas tecnología Wimax 87

Desventajas tecnología Wimax 87

Diferencias entre WiFi y WiMax 87

GSM 88

Objetivos 88

Tipos de Servicios 89

Radios de frecuencia 89

Codificación de la voz 89

Celdas GSM 89

Arquitectura 90

Roaming 90

GPRS 91

¿Por qué el GPRS trajo tantos cambios? 91

Importantes mejoras 92

Características de GPRS 92

Diferencias entre GSM y GPRS 93

Ventajas 93

Desventajas 93

UMTS 95

Cómo funciona la red 3G 95

Ventajas y desventajas de la red 3G 96
4G LTE 97
Ventajas y desventajas de la tecnología móvil 4G 98
Ventajas 98
Desventajas 98
4G EN ARGENTINA 98
Bibliografía 101
Preguntas y Respuestas 102

WIFI

WiFi significa **Wireless Fidelity**.Wifi no es un acrónimo, sino un nombre comercial creado por una compañía de marketing con el objetivo de definir un sello de interoperabilidad para las actividades de marketing. Es una tecnología de red inalámbrica a través de la cual los dispositivos, como computadoras, dispositivos móviles y otros equipos como impresoras, consolas de videojuego y/o televisores, pueden interactuar con Internet, permitiendo intercambio de información entre sí y establecer, de esta manera, una red. La conectividad a Internet se logra a través de un router inalámbrico que permite que los dispositivos que admiten wifi interactúen con Internet.

El estándar IEEE 802.11 define los protocolos que permiten la comunicación con los dispositivos inalámbricos actuales que admiten wifi, incluidos routers y puntos de acceso inalámbrico. Los puntos de acceso inalámbrico son compatibles con diferentes estándares IEEE. Cada estándar es una modificación que recibe aprobación después de cierto tiempo. Los estándares funcionan con diversas frecuencias, proporcionan distintos anchos de banda y admiten distintas cantidades de canales.

El Wifi surgió como respuesta a la necesidad de estandarización y compatibilidad en los modelos de conexión inalámbrica de los diversos dispositivos digitales, superando además otras formas no compatibles de conexión como son el Bluetooth, GPRS, UMTS, etc. A diferencia de estos, el Wifi emplea las ondas de radio como vehículo de transmisión de la información. El concepto de funcionamiento de este tipo de redes es bastante sencillo. El router recibe Internet a través de un cable Ethernet, y convierte los datos en ondas de radio que envía al dispositivo receptor, dotado de un chip WiFi, que recibe esas ondas y las decodifica para convertirlas en unos y ceros, datos que entienden los ordenadores y los móviles. Este chip WiFi también tiene capacidad para convertir datos en ondas de radio, y enviárselas al router. Así es como subimos datos a Internet.

Las ondas de radio que usa el WiFI son las mismas que utilizan los móviles, los canales de televisión, incluso el microondas, pero a una frecuencia (velocidad) mucho mayor. De hecho la frecuencia WiFi más usada, 2.4 GHz, es la misma que usa el microondas, por eso a veces se producen interferencias. La frecuencia se mide en Hercios o Hertz, que mide la rapidez a la que se transmiten las ondas. Un hercio indica un ciclo por segundo, mientras que un KHz son 1.000 hercios. El WiFi transmite en las bandas de 2.4 y 5 GHz, y puesto que 1 GHz son 1.000 millones de hercios, un router de 5 GHz es capaz de transmitir 5.000 millones de datos por segundo. A mayor frecuencia, se pueden transmitir más datos por segundo, pero el alcance es menor. Todos los routers transmiten en la misma frecuencia, y también los móviles y ordenadores que reciben su señal. Para evitar interferencias, los routers pueden variar ligeramente la frecuencia para crear diferentes canales. Así, la banda de los 2.4 GHz tiene 12 canales y la de 5 GHz

alrededor de 30. Los routers modernos son capaces de ver en qué canal transmiten routers cercanos, y elegir uno que esté poco ocupado. Como los móviles y ordenadores ajustan el canal automáticamente, el usuario no tiene que preocuparse.

Esta tecnología está diseñada para conectar dispositivos a distancias relativamente cortas (100 metros como máximo), en especial en entornos que ofrezcan mucha interferencia o ruido a la señal, como la producida por la saturación del espectro radioeléctrico debido a la multiplicidad de emisiones. Además, es una conexión más lenta que la cableada, pero significativamente más cómoda y versátil.

Tipos de Wifi

Se conocen diversos tipos de Wifi o diversas frecuencias de Wifi, de acuerdo a los estándares que emplean para su identificación y que pueden distinguirse en dos categorías:

- Banda de 2,4 GHz. Aquí se encuentran los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n, cuyo manejo es internacional y permite velocidades de 11 Mbit/s, 54 Mbit/s y 300 Mbit/s respectivamente. Sin embargo, es el tipo que mayor interferencia cuenta, dado que la banda de 2,4 GHz es también empleada por Bluetooth y otros sistemas inalámbricos.
- Banda de 5GHz. El nuevo tipo de Wifi, conocido como WIFI 5, aplica el estándar IEEE 802.11ac y se maneja en un canal completamente nuevo y libre de interferencias, por lo que, a pesar de ser una tecnología reciente y de tener la desventaja de un 10% menos de distancia de alcance, se le considera sumamente conveniente dada su estabilidad y velocidad.

Estándares que certifica la Alianza Wi-Fi

Los diferentes tipos de WiFi se clasifican según los estándares 802.11 y, en función del utilizado, varía la velocidad de la señal.

- IEEE 802.11. Creado en 1997, en el presente ya no se usa. Éste permitía una velocidad máxima de conexión de dos megabits por segundo, unos valores muy lentos para la mayor parte de las aplicaciones.
- IEEE 802.11a. Surgió en 1999 con una velocidad máxima de 54 megabits por segundo. Esta versión fue la primera en funcionar a 5 GHz, una frecuencia que bloquea fácilmente los objetos y que hace que este estándar tenga un alcance limitado.
- IEEE 802.11b, IEEE 802.11g, IEEE 802.11n. Cuentan con velocidades máximas de 11, 54 y 300 megabits por segundo y disponen de una frecuencia de 2,4 GHz, una banda casi universal que los convierte en los más empleados internacionalmente.
- IEEE 802.11ac. Nacido en 2014 y conocido como WiFi 5, funciona a una velocidad máxima de 1.300 megabits por segundo y opera en la banda de 5GHz.
- IEEE 802.11ax, También conocido como WiFi 6 y diseñado para operar en los espectros de 2.4 y 5 GHz. Además de utilizar MIMO y MU-MIMO, este nuevo estándar introduce OFDMA para mejorar la eficiencia espectral global y ofrecer un mayor rendimiento. Es compatible con los protocolos anteriores y ofrece una velocidad máxima teórica de 10 Gbps.

Dispositivos

Existen varios dispositivos wifi, los cuales se pueden dividir en dos grupos: dispositivos de distribución o de red, entre los que destacan los enrutadores, puntos de acceso y repetidores; y dispositivos terminales, que en general son las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB.

Dispositivos de distribución o de red:

- Los puntos de acceso son dispositivos que generan un set de servicio que podría definirse como una red wifi a la que se pueden conectar otros dispositivos. Los puntos de acceso permiten conectar dispositivos de forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal.
- Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica. Se conectan a una red existente que tiene señal más débil y crean una señal más fuerte a la que se pueden conectar los equipos dentro de su alcance. Algunos de ellos funcionan también como punto de acceso.
- Los enrutadores (router) inalámbricos son dispositivos compuestos especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen un enrutador (encargado de interconectar redes; por ejemplo, la red del hogar con Internet), un punto de acceso (explicado más arriba) y generalmente un conmutador que permite conectar algunos equipos vía cable (Ethernet y USB). Su tarea es tomar la conexión a Internet y brindar a través de ella acceso a todos los equipos que se conecten, sea por cable o en forma inalámbrica.

Los dispositivos terminales abarcan tres tipos mayoritarios: tarjetas PCI, tarjetas PCMCIA y tarjetas USB:

- El wifi puede ser desactivado por un terminal del dispositivo.
- Las tarjetas PCI para wifi se agregan (o vienen de fábrica) a los ordenadores de sobremesa. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.
- Las tarjetas PCMCIA son un modelo que se utilizó mucho en los primeros ordenadores portátiles, ya en desuso, debido a la integración de tarjeta inalámbricas internas en estos ordenadores. La mayor parte de estas tarjetas solo son capaces de llegar hasta la tecnología B de wifi, no permitiendo por tanto disfrutar de una velocidad de transmisión demasiado elevada.
- Las tarjetas USB para wifi son el tipo de tarjeta más común que existe en las tiendas y el más sencillo de conectar a un ordenador personal, ya sea de sobremesa o portátil, disponiendo de todas las ventajas de la tecnología USB. Hoy en día pueden encontrarse incluso tarjetas USB con el estándar 802.11ac (Wireless-AC), que es el penúltimo estándar liberado para redes inalámbricas.
- También existen impresoras, cámaras Web y otros periféricos que funcionan con la tecnología wifi, permitiendo un ahorro de mucho cableado en las instalaciones de redes y especialmente gran movilidad de equipo.

Tipos de seguridad en conexiones WiFi

La WiFi Alliance es quien regula los estándares de WIFI. La seguridad del WiFi es variable, principalmente en función del cifrado que se aplique a las comunicaciones entre el router y los adaptadores inalámbricos. Existen varias opciones, y se pueden dividir entre seguras y no seguras por sus características técnicas:

- WEP (Wired Equivalent Privacy): Este tipo de cifrado nos remonta hasta el año 1999. En esa época era el más utilizado en el mundo, pero como es lógico, su uso ha ido disminuyendo con el paso de los años. En su llegada se descubrieron muchos fallos y agujeros de seguridad, lo que hizo que tuviera que ir mejorando con el paso del tiempo. Aunque los principales fallos y agujeros fueron solucionados, lo cierto es que se trata de un cifrado poco fiable y fácil de explotar.
- WPA (WiFi Protected Access): WPA fue la respuesta a los principales fallos y vulnerabilidades de WEP. Las claves usadas por WPA son de 256 bits, a diferencia de los 128 bits usados por WEP, aunque no es la única mejora ya que incorpora la comprobación de contenidos e integridad de mensajes para evitar que puedan ser interceptados y el uso del protocolo de clave temporal TKIP, lo cual ayuda a que un router pueda ser atacado fácilmente como ocurría con WEP.
- WPA2: La principal diferencia con WPA es el uso del AES, que realiza un cifrado por bloques para permitir claves más largas y seguras y la implementación del CCMP que se trata de un protocolo mejorado de encriptación que sustituye a TKIP.
- WPA3: Incorpora el cifrado de 192 bits en vez de 129 bits, lo que hace que el cifrado sea más seguro y difícil de romper. Esto hace que sea más seguro incluso con contraseñas menos fuertes, por lo tanto, una misma clave es más vulnerable a ataques de fuerza bruta en WPA2 que en WPA3. Cuenta también con un nuevo modo de configurar y conectar a la red dispositivos sin la necesidad de que tengan pantalla ni botones físicos, etc.

Ventajas e inconvenientes redes WiFi

La conectividad inalámbrica está cada vez más extendida y sin duda ha hecho que nuestra vida haya cambiado completamente. Vivimos en una era tecnológica en la que vivimos conectados y eso es, en gran parte, por la gran cantidad de conexiones WiFi a las que podemos tener acceso allá donde vayamos. Sin embargo, aunque este tipo de conexiones ofrecen ciertas ventajas, también podemos encontrar con ciertos inconvenientes.

Entre las principales ventajas que nos ofrece el WIFI, caben destacar:

- Conectividad inalámbrica: Sin duda una de las principales ventajas que nos ofrece el WiFi es que se trata de un tipo de conectividad inalámbrica. Por lo tanto, no es necesaria la conexión física por cables, por lo que evitamos tener que llenar nuestra casa u oficina de cables por todos lados.
- Comodidad: El hecho de que sea una conectividad inalámbrica no ofrece también una gran comodidad y libertad. Es decir, podremos ir de un lado para otro con nuestro ordenador, tablet o móvil y seguir conectado sin que esto suponga ningún problema. El alcance suele ser más que suficiente en la mayoría de hogares, aunque existen

numerosas opciones para ampliar el alcance de una WiFi en el caso de que sea necesario.

- Coste: El no tener que hacer uso de cableado y dispositivos como hubs o similares, hace que una red WiFi tenga un coste mucho menor que las redes cableadas.
- Compatibilidad: La WiFi Alliance asegura la compatibilidad total entre dispositivos, por lo tanto, permite que podamos utilizar la tecnología WiFi con una compatibilidad total en cualquier parte del mundo.

Ahora bien, también ofrecen ciertas desventajas o inconvenientes con respecto a las redes cableadas:

- Velocidad: En el caso de usar una conexión WiFi, existen numerosos factores que pueden afectar a la velocidad de nuestra conexión en el dispositivo utilizado para la conexión, algo que con el cable es mucho menos probable salvo que utilicemos longitudes exageradas o cables de muy baja calidad.
- Latencia: Es otro de los principales problemas con los que nos podemos encontrar en este tipo de conexiones inalámbricas. Las conexiones WiFi son más propensas a sufrir ciertos lags, sobre todo cuando queremos reproducir contenido multimedia en alta resolución en streaming o jugar online. Además, hay ciertos agentes externos que pueden afectar de esta forma negativa a nuestra conexión.
- Interferencias: Las redes WiFi pueden verse afectadas por determinadas interferencias, lo cual supondrá un menor rendimiento de las mismas. Ciertos aparatos electrónicos y electrodomésticos pueden generar ondas que interfieren con las de este tipo de redes inalámbricas, pero, además, hay ciertos elementos como muros o puertas que también pueden hacer que la señal llegue a ciertos rincones de la casa.
- Microcortes: Todo este tipo de aspectos que pueden influenciar negativamente en una red WiFi pueden provocar ciertos cortes en nuestra conexión. En determinadas ocasiones puede que no afecten a aquello que estamos realizando, pero en determinados casos puede ser un gran problema.

WIMAX

Las siglas de WiMAX significan Worldwide Interoperability for Microwave Access, lo que en español se podría traducir como Interoperabilidad Mundial para Acceso por Microondas. Se trata de un método de transmisión de datos a través de ondas de radio, y que utiliza las frecuencias de 2,5 a 5,8 GHz, mediante conexión inalámbrica basada en los estándares de comunicación IEEE 802.16, y que permite llevarte Internet con un alcance que puede llegar a los 70 kilómetros.

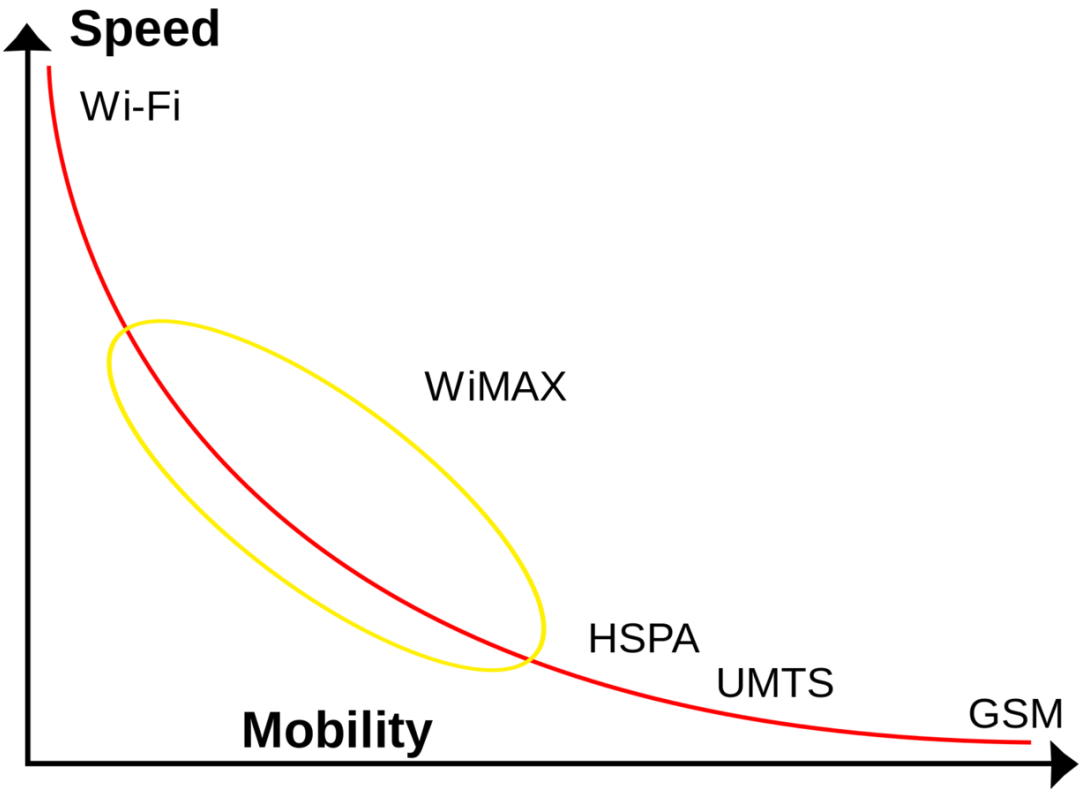
El funcionamiento de WiMAX es sencillo, ya que simplemente es el repetidor de la empresa a la que lo contrates emitiendo las señales de microondas que te llegan a la antena que tengas en tu casa. Por lo tanto, lo primero que necesitas es contactar con una empresa que ofrezca estos servicios y que tenga un repetidor cerca de tu casa para poder enviarte la señal.

Luego, tienes que poner una pequeña antena en la fachada de tu casa. Esta antena tendrá que apuntar directamente al repetidor de la empresa que te va a dar el servicio, o sino a un punto de conexión intermedio que se utilice para salvar obstáculos que se interpongan entre tu antena y su repetidor. La instalación la hará la propia compañía.

Entonces, desde la antena bajará un cable que llegará a tu casa, y que se conectará directamente a tu ordenador o a un router con el que poder gestionar la conexión como si se tratase de una red de fibra o cable convencional, pudiendo crear tu propia WiFi doméstica.

Las conexiones de WiMAX pueden alcanzar velocidades de hasta 1Gbps en puntos fijos, por ejemplo una casa, y de 365Mbps en puntos móviles. Aun así, siempre dependerá de lo que te ofrezca la empresa a la que le contratas el servicio, y con el 4G tan extendido y la llegada inminente del 5G puede que la alternativa móvil no sea tan atractiva.

Por lo general, cuando contratas una conexión WiMAX obtendrás velocidades asimétricas, lo que quiere decir que la velocidad de descarga será muy superior a la de subida. Además, la estabilidad podría verse afectada más fácilmente en momentos de congestión. Pese a eso, siguen siendo en general más rápidos que el ADSL rural a un precio mensual muy similar



Características

- Posee un gran ancho de banda Una sola estación de base puede admitir de manera simultánea más de 60 enlaces con conectividad tipo T1/E1 o cientos de conexiones tipo DSL.
- Es independiente de protocolo, puede transportar IP, Ethernet, ATM y otros. Eso hace que sea compatible con otros estándares como Wi-Fi, Ethernet, o Token Ring.
- Puede transmitir otros servicios agregados como VoIP, datos o vídeos.
- Soporta las llamadas antenas inteligentes (smart antenas), propias de las redes de telefonía de tercera generación (3G), lo cual mejora la eficiencia espectral.
- Estas antenas emiten un haz muy estrecho que se puede ir moviendo, electrónicamente, para enfocar siempre al receptor, con lo que se evitan las interferencias entre canales adyacentes y se consume menos potencia al ser un haz más concentrado.
- Velocidad: En circunstancias ideales y sin obstáculos que interfieran en los enlaces establecidos, la conexión puede alcanzar una distancia cercana a los 50 kilómetros y la velocidad de transferencia de los datos puede llegar a los 70 Mbps.

- Seguridad: incluye medidas para la autenticación de usuarios y la encriptación de los datos mediante los algoritmos Triple DES (128 bits) y RSA (1.024 bits).
- Como principales inconvenientes cabe mencionar la limitación de potencia para prever interferencias con otros sistemas, y el alto consumo de batería que se requiere.
- Sin embargo, los más recientes avances en los procesadores digitales de señal hacen que señales muy débiles puedan ser interpretadas sin errores, un hecho del que se aprovecha WiMAX.

Tipos de WiMax

Existen dos tipos principales de esta tecnología:

- WiMAX fija (802.16d-2004): tecnología de punto a varios puntos, en tanto que la móvil es una tecnología de varios puntos a varios puntos, que se asemeja a la de una infraestructura celular.
- WiMAX móvil (802.16e-2005), se basa en la tecnología OFDMA (acceso múltiple por división de frecuencia ortogonal) que ofrece ventajas inherentes en términos de latencia, eficiencia en el uso del espectro de frecuencia de radio y soporte avanzado de antenas, lo que en definitiva se traduce en un desempeño superior al de las actuales tecnologías de redes inalámbricas de área amplia.

Dispositivos y funcionamiento WiMax

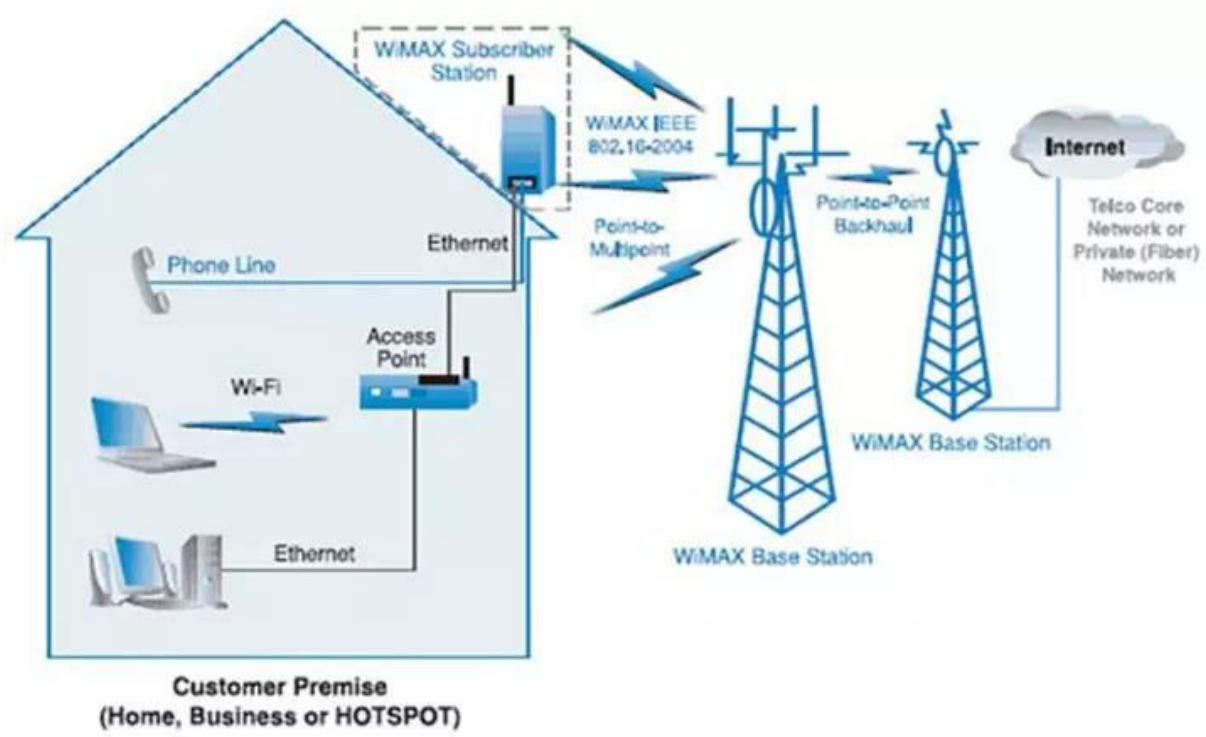
Esta tecnología necesita de una serie de elementos para su correcto funcionamiento:

- *Estación base o Repetidor*
- *Puntos de conexión intermedios (opcional)*
- *Antena*
- *Cableado hasta nuestro router o dispositivo*

En este sentido, el repetidor hace las veces de antena para dar cobertura de telefonía móvil. Suelen situarse en lugares a gran altitud para evitar objetos que se puedan interponer con el objetivo donde se quiere hacer llegar las ondas para permitir la conexión a Internet. Por lo tanto, es el encargado de emitir las señales de microondas.

Si fuese necesario para sortear algún elemento que pueda impedir el alcance máximo de las ondas emitidas desde el repetidor, entonces es posible que se necesiten instalar puntos de conexión intermedios para facilitar que lleguen las microondas hasta el objetivo.

En la fachada de nuestra casa tendremos que instalar una pequeña antena que estará orientada hacia el repetidor o punto de conexión intermedio de la empresa que nos va a dar el servicio. La instalación de la antena la realizará la propia compañía, así como el cableado necesario hasta llegar al router o directamente a nuestro ordenador. Una vez realizada toda la instalación, es importante saber que podremos crear nuestra propia WiFi en casa para conectarnos desde otros dispositivos.



Estándares WIMAX

Estándar	Descripción
802.16	Utiliza espectro licenciado en el rango de 10 a 66 GHz, necesita línea de visión directa, con una capacidad de hasta 134 Mbit/s en celdas de 3 a 7,5 km (2 a 5 millas). Soporta calidad de servicio. Publicado en 2002.
802.16a	Ampliación del estándar 802.16 hacia bandas de 2 a 11 GHz, con sistemas NLOS y LOS, y protocolo PTP y PTMP. Publicado en abril de 2003.
802.16c	Ampliación del estándar 802.16 para definir las características y especificaciones en la banda de 10-66 GHz. Publicado en enero de 2003.
802.16d	Revisión del 802.16 y 802.16a para añadir los perfiles aprobados por el WiMAX Forum. Aprobado como 802.16-2004 en junio de 2004 (la última versión del estándar).
802.16e	Extensión del 802.16 que incluye la conexión de banda ancha nómada para elementos portátiles del estilo de los notebooks. Publicado en diciembre de 2005.
802.16m	Extensión del 802.16 que entrega datos a velocidad de 1 Gbit/s en reposo y 100 Mbit/s en movimiento.

802.16m-2011	Conocido como Mobile WiMAX Release 2, interfaz de aire avanzada, con tasas de 100 Mbit/s móvil y 1 Gbit/s de datos fija, con OFDMA

Ventajas tecnología Wimax

- Numerosos servicios: es posible la utilización de otros servicios añadidos como datos, vídeos, VoiP, etc.
- Alta seguridad: este tipo de internet incluye medidas de seguridad tanto a nivel de usuarios como en la encriptación.
- Gran ancho de banda: la tecnología WIMAX proporciona un gran ancho de línea llegando a admitir más de 60 conexiones.
- Internet rural: esta tecnología es la más utilizada en aquellos lugares en los que resulta muy caro hacer llegar el ADSL o la fibra óptica.

Desventajas tecnología Wimax

- Instalación: el uso de la tecnología WIMAX requiere la instalación de una pequeña antena exterior adecuadamente instalada por el operador correspondiente.
- Cobertura: sólo es posible utilizar esta tecnología en aquellos lugares en los que un operador proporcione cobertura y tenga las antenas necesarias instaladas.
- Interferencias: la conexión a la red mediante WIMAX puede verse afectada por diversos agentes como ondas, interferencias.

Diferencias entre WiFi y WiMax

Tras el éxito que vieron las operadoras de internet con wifi, rápidamente los fabricantes empezaron a pensar en una tecnología bastante más avanzada y ahí surgió la certificación WiMax en el año 2001.

Como ves la gran diferencia con wifi es su enorme distancia de cobertura y que es mucho más rápida.

Pero no solo eso, con WiMax tendremos cobertura incluso en movimiento, viajando a velocidades de hasta 250Km/h tendremos cobertura.

Además Wi-Fi está diseñado para entornos de interior, mientras que WiMax lo está para entornos exteriores, pudiendo dar acceso a más de 1000 usuarios de forma simultánea.

CARACTERÍSTICAS	WIFI	WIMAX
PROTOCOLO	802.11	808.16
VELOCIDAD	11-54 Mbit/s	124 Mbit/s
COBERTURA	300m	40-70 km
LICENCIA	No	Si/No
VENTAJAS	Velocidad/precio	Velocidad/alcance
DESVENTAJAS	Bajo alcance	Cobertura limitada
USUARIOS	Cientos	Miles
MOVILIDAD	Limitado a puntos de conexión	Cualquier momento/Cualquier lugar

GSM

GSM es la abreviatura de **Global System for Mobile Communications.**

Es el sistema de comunicación más seguro puesto que toda la información que transmitimos viaja de manera encriptada por el aire, donde en cada llamada genera nuevos códigos para evitar ser interceptada y/o reconstruida.

Posee un ancho de banda de 200 Khz.

El GSM es la tecnología líder a nivel mundial, con más de 380 millones de usuarios en más de 150 países.

Objetivos

- Uso más eficiente del espectro que la telefonía analógica, utilizando técnicas de multiplexación en tiempo y frecuencia.
- Incluir roaming internacional
- Terminales y sistema de bajo coste
- Buena calidad de voz (comparable a la telefonía fija)
- Ampliación de servicios
- Baja potencia de transmisión: reutilización de canales, al no saturar canales de células vecinas

Tipos de Servicios

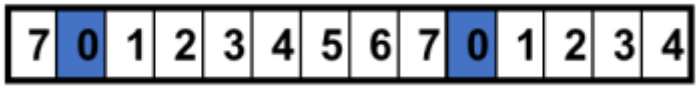
- Teleservicios (voz, SMS, fax, etc.)
- Servicios portadores (datos)
- Servicios complementarios (llamadas en espera, multiconferencias, etc.)

Radios de frecuencia

El GSM utiliza dos bandas de frecuencia, cada una son de 25 Mhz de ancho:

- 890-915 Mhz, desde la estación móvil a la estación base (ascendente)
- 935-960 Mhz, desde la estación base a la estación móvil (descendente)

Cada banda se divide en 125 canales de 200 KHz de ancho cada uno. El primer canal está reservado, por lo que hay disponibles 124. Cada canal se divide por TDMA (Acceso Múltiple por División de Tiempo) en ocho ranuras que dan servicio a otros tantos usuarios:



La ranura asignada a una comunicación se cambia (en tiempo y frecuencia) a razón de 217 cambios/seg; esto se denomina frequency hopping y se hace para evitar interferencias. Cada ranura transporta 22,8 Kb/s de información digital 'en bruto' y por ella se puede enviar voz (13,2 Kb/s) o datos (9,6 Kb/s).

La combinación de una ranura de subida y una de bajada permite una comunicación full dúplex.

El número máximo de comunicaciones simultáneas es teóricamente de 124*8=992. Sin embargo, muchos canales no se pueden usar para evitar conflicto con las celdas vecinas.

Codificación de la voz

Una conversación telefónica normal ocupa en formato digital 64 Kb/s (8.000 muestras de un byte por segundo).

En GSM la voz se comprime según un algoritmo llamado RPE-LPC (Regular Pulse Excited – Linear Predictive Coder) que da una calidad casi equivalente usando sólo 13,2 Kb/s

Además, en GSM sólo se transmite cuando la persona habla (transmisión discontinua o supresión de silencios).

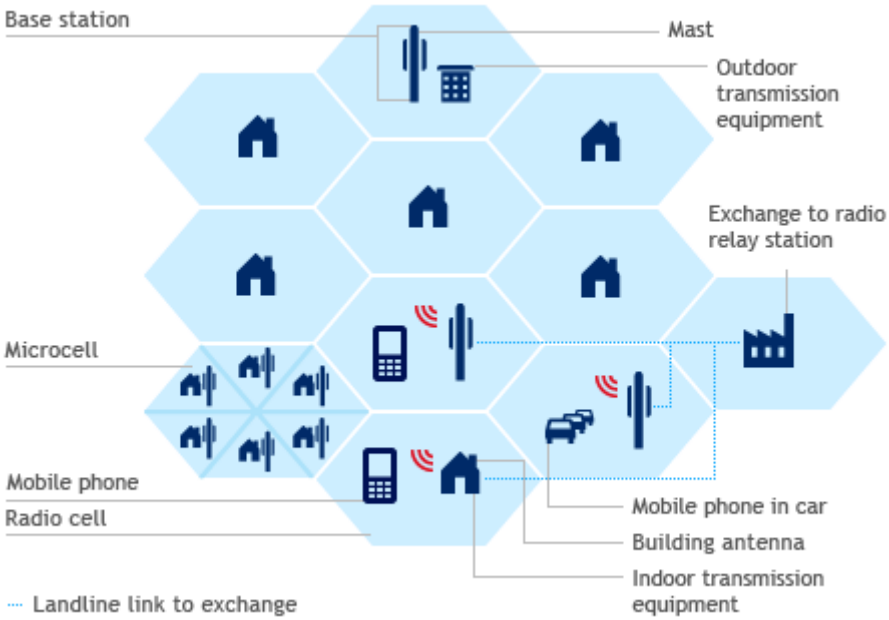
Esto supone un ahorro del 60% en el canal y reduce el gasto de batería del emisor

Para evitar que el receptor crea que la conexión se ha cortado la transmisión discontinua se acompaña de ruido de confort.

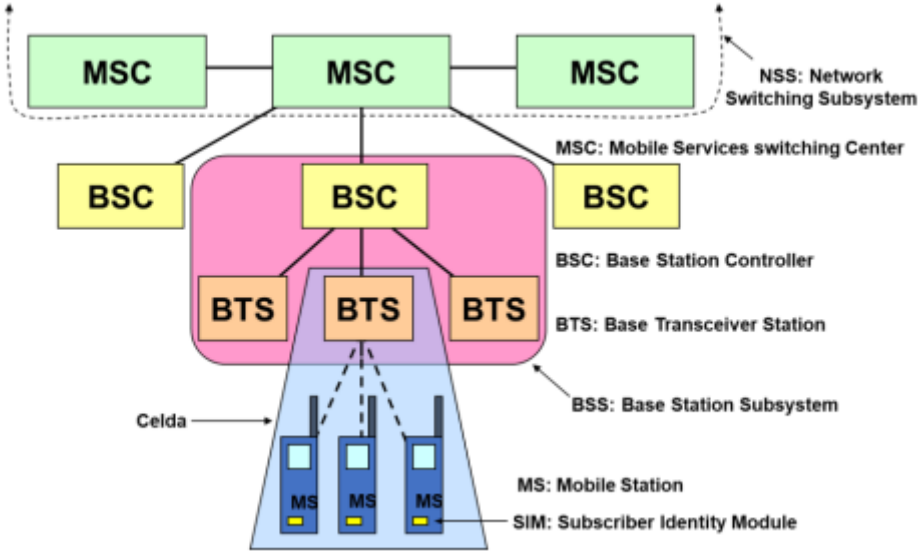
Celdas GSM

El área atendida por una estación base (BTS) se denomina celda. Todos los usuarios de una misma celda comparten los canales disponibles. Cuantos más usuarios hay dentro de una celda más riesgo hay de que se produzca saturación. En zonas con elevada densidad de usuarios (ej. ciudades) se tiende a crear celdas pequeñas. En zonas rurales, con densidad pequeña, se prefiere crear celdas grandes. Las celdas vecinas se agrupan en clusters. Dentro de un cluster

cada canal solo se utiliza una vez, para evitar interferencias. Cada cluster está formado por 4, 7, 12 o 21 celdas, según la topología del terreno y las circunstancias concretas de la zona.



Arquitectura

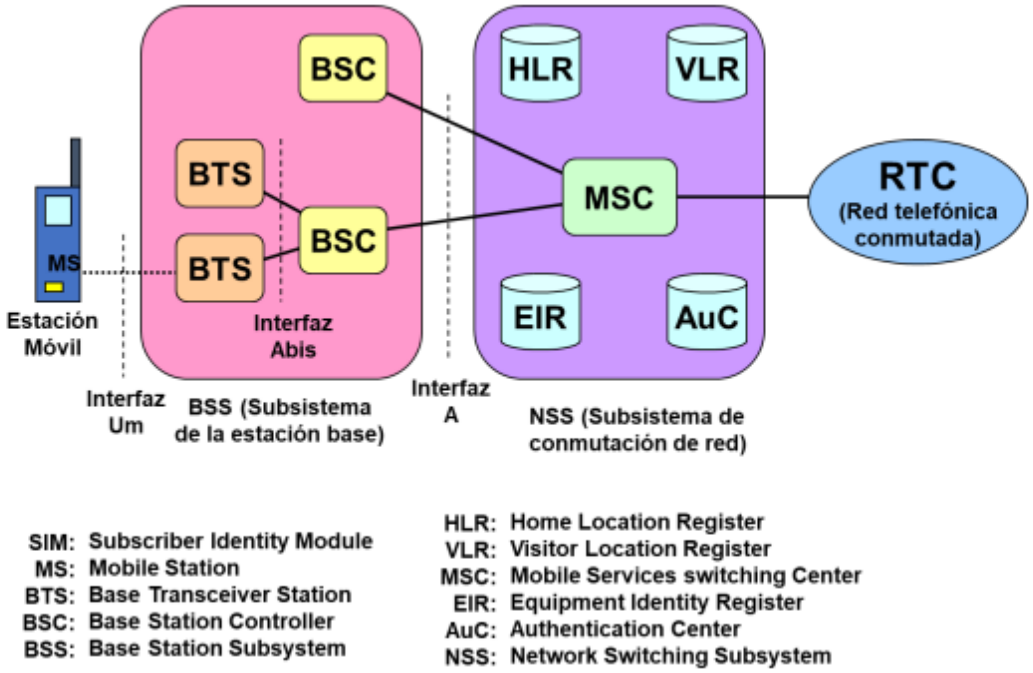


Roaming

Se produce cuando tratamos de identificarnos y el terminal no es capaz de encontrar la red. Permite que un usuario haga uso de una red foránea (si el operador tiene acuerdo y el roaming está habilitado)

La red foránea obtiene el HLR (Home Location Register) del usuario y lo incorpora en su VLR (Visitor Location Register.

El usuario visitante corre a cargo con el costo extra cuando recibe una llamada



GPRS

El GPRS es un sistema de comunicación móvil que se creó en la década de los 80. Por entonces ya existía el GSM (Sistema Global para comunicaciones móviles) pero el GPRS llegó con fuerza y se convirtió en una extensión de este segundo, ofreciendo muchas más ventajas y actualizaciones de múltiples servicios, así como incorporando aplicaciones nuevas. Si el GSM era un sistema que se basaba en dar cobertura a las comunicaciones móviles por satélite sin tener que utilizar cables para ello, el GPRS funcionaba de igual modo, pero con la diferencia de que el sistema se orientaba a través de enlaces de radio. De la misma manera, cuando el sistema GSM transmitía la información por audio, el otro realizaba su papel a través de los datos. Fue popularmente bautizado como la generación 2.5 en relación a este tipo de comunicaciones.

¿Por qué el GPRS trajo tantos cambios?

Aunque el sistema GSM estaba muy asentado, lo cierto es que con la llegada del GPRS quedó algo obsoleto, puesto que este trajo consigo varios cambios y aportaciones innovadoras a las comunicaciones móviles. Una de las principales novedades que introdujo este sistema fue la utilización del protocolo WAP establecido para las aplicaciones inalámbricas. Con él los dispositivos móviles podían tener un gran número de aplicaciones dentro de la red, pudiendo disfrutar de Internet a través de nuestros terminales móviles. Y no solo eso, también accedíamos por ejemplo al correo electrónico y a otros muchos programas más que hasta entonces solo teníamos en el ordenador.

Se mejoraron los servicios de mensajería instantánea y se incluyeron otros nuevos como es el caso de los mensajes cortos, conocidos como SMS o los de tipo multimedia, MMS. Otro de los cambios que se introdujeron en la telefonía móvil gracias a la aparición del sistema GPRS fue el uso del protocolo IP. Hasta entonces este solo se encontraba en la red tradicional de los ordenadores, pero con la extensión del GSM cada dispositivo móvil gozaba ya de una

identificación propia de IP, lo que permitía que estuviera integrado dentro de Internet. Una de las nuevas aplicaciones de este sistema que causó gran expectación fue la posibilidad de utilizar el propio dispositivo como un módem USB.

Importantes mejoras

La cuestión fue que aunque el GPRS tenía como base el sistema GSM, el primero resultaba ser menos costoso, ofrecía muchos más servicios al usuario y además tenía un mayor porcentaje de rendimiento. La segunda generación evolucionó rápidamente con este sistema a la 2.5. Finalmente, hay que destacar que una de las novedades más ventajosas que incluyó el GPRS fue el cambio de método de pago con respecto a las transferencias de datos. Antes era un proceso que se facturaba a través del tiempo de conexión, lo que limitaba bastante a los usuarios además de engordar la factura. Después el pago se asentó por megabytes consumidos, así todo aquel que tuviera un teléfono móvil podía tener la posibilidad de estar conectado a la red durante más tiempo, además de tener la posibilidad de interactuar con varias aplicaciones a la vez.

El GPRS fue un sistema de comunicación móvil revolucionario en el momento que salió al mercado y a pesar de que lleva muchos años ya en funcionamiento en la actualidad se sigue usando bastante en un gran número de dispositivos y aplicaciones. Si bien es cierto, eso sí, con los nuevos avances tecnológicos este sector sigue renovándose y es por ello que hoy en día otros sistemas como el 3G o el 4G se están asentando. Pero aún no han sido capaces de hacer que nos olvidemos de la importancia del sistema GPRS.

Características

Características de GPRS

El sistema de telecomunicaciones GPRS cuenta con las siguientes características:

- Dado que la facturación se realiza en función del consumo de datos y no del tiempo de conexión, un usuario puede mantenerse conectado de forma permanente.
- Cuenta con todos los beneficios del sistema GSM, es decir, servicio de mensajes cortos (SMS), servicio de mensajería multimedia (MMS) y otros.
- Permite descargar archivos de manera mucho más rápida que por medio de tecnologías predecesoras.
- Al estar basado en la tecnología GSM, permite una comunicación permanente y estable durante la realización de llamadas de voz.
- Permite realizar llamadas de voz sin cortar la transmisión de datos en el equipo, ya que el GPRS trabaja de manera simultánea al sistema GSM (solo en equipos clase A).

Diferencias entre GSM y GPRS

Las tecnologías GSM y GPRS funcionan de manera similar. En los siguientes párrafos se señalan cuáles son las diferencias entre GPRS y GSM:

El sistema de telecomunicaciones GSM significó el inicio de la era 2G, mientras que el GPRS surgió como una versión posterior y mejorada del GSM.

La velocidad de transferencia de datos tiene una tasa de hasta 114 Kbps, mientras que GSM es capaz de ofrecer aproximadamente 9,6 Kbps.

La tarificación en los equipos conectados a una red GSM se estipula en función del tiempo de conexión. Por otro lado, en una conexión GPRS el cobro por servicios se basa en la cantidad de datos utilizados.

Ventajas

El surgimiento del sistema GPRS mejoró aún más lo ofrecido por la tecnología GSM en la década de los años 90. A continuación, se destacan algunas de las más importantes ventajas del sistema GPRS:

Puede brindar una velocidad de conexión 5 veces mayor que su predecesora GSM.

Ofrece un amplio número de servicios que van más allá de las llamadas de voz.

No existe tarificación por tiempo de conexión, siendo esta realizada a partir del volumen de datos utilizado.

Al utilizar un modo asimétrico de transmisión, la velocidad de transferencia se optimiza según el uso que se le dé a la red.

Desventajas

Aunque implicó una mejora en la telefonía de muchos años atrás, hoy en día es posible señalar algunas importantes desventajas del sistema GPRS, las cuales son:

A pesar de ofrecer una velocidad de conexión mayor al GSM, su tasa de transferencia de datos es obsoleta actualmente, en comparación a las generaciones de telefonía actuales.

La posibilidad de utilizar el sistema GSM y GPRS de manera simultánea solo es posible en equipos Clase A, por lo que muchos teléfonos móviles de la época no contaban con esta posibilidad.

Al descargar archivos, se generan colas de espera para unir cada parte del archivo, algo causado por la conmutación de circuitos y que genera retardo.

Debido a que los paquetes de archivo son enviados y descargados de forma segmentada, existe el riesgo de que alguno de ellos se dañe y el archivo completo sea inservible.

Las estaciones base se congestionan con facilidad.

La velocidad de transferencia de datos dependerá de la cercanía que exista entre el terminal (teléfono móvil) y la estación base (antena de telefonía).

Estas son las ventajas y desventajas más relevantes a tener en consideración respecto a la tecnología GPRS.

UMTS

Es un sistema de tecnología universal de comunicaciones móviles, conocido por sus siglas en ingles UMTS, y sustituyo la red GSM debido a los avances. Sus características permiten que muchos consumidores obtengan el acceso a la red, pues dos estructuras de redes se combinan, mientras una transmite la otra gestiona.

Este sistema le brinda a sus usuarios varios servicios avanzados, incluso el servicio de red aparecen en la pantalla de tu móvil con otros símbolos. Este sistema de red, le ha brindado a la sociedad la oportunidad de avanzar en el desarrollo de las comunicaciones, aunque te encuentres a distancias.

De igual modo, esta red es utilizada en su mayoría por móviles pertenecientes a la tercera generación. Según expertos esta es la red sucesora de la GRPS, sin embargo al momento de su creación esta fue diseñada exclusivamente para el uso de dispositivos móviles pero ha ido en constante evolución y en la actualidad permite su acceso incluso desde otros dispositivos. Y por si fuera poco es conocida por sus características principales como lo son: las capacidades multimedia que esta red abarca, su velocidad cuando de internet se trata, y la transmisión de voz de calidad.

Este sistema además resulta ser muy completo ya que utiliza todos los servicios existentes en la tecnología, es decir que con ella puedes utilizar cualquier tipo de terminal. si, así como lo lees cualquiera. Su sistema es bastante global ya que permite su acceso en redes terrestres y satelitales. Sus servicios son bastante simétricos y asimétricos, por lo que proporciona gran flexibilidad a la hora de ofrecer sus servicios.

Cómo funciona la red 3G

Este sistema digital nos sirve para mantener esa comunicación diariamente sin límites, como los que teníamos muchísimos años atrás con otros sistemas. A continuación la funciones que nos brinda UMTS con una estructura que permite la comunicación de voz y al mismo tiempo multimedia:

- Práctico usó de sus servicios, lo que hace que se adapte al masivo consumo del mismo.
- Bajo costo o tarifa de los paquetes.
- Facilidad de conexión: Por medio de varias interfaces y cumpliendo los procedimientos de transporte de datos se logra mantener una calidad de conexión simultánea.
- Soporte de hasta 2 Mbps.
- Conectarse a internet.
- Combinación de transmisión de datos GSM y alta velocidad por circuitos.
- Servicio de datos multimedia.
- Facilidad de pago virtual.

Podemos decir que el sistema de red UMTS dio sobre otros una eficiencia innovadora, ampliando exponencialmente sus servicios con una capacidad y cobertura excelente.

Un punto muy importante a resaltar es que esta red funciona totalmente diferente a la red 2G. Y es que en la red 3G los datos son enviados en paquetes de datos bastantes diminutos que en su camino se van estructurando nuevamente para ser entregado de manera correcta al

receptor. Esto permite que en esta red sea enviada una mayor cantidad de datos y sean entregados con mayor rapidez y eficiencia. Y no solo eso, sino que la red 3G te permite estar conectado con más de una red base a la vez.

Esta red además consume una potencia muy baja y su consumo de energía es casi similar a la red 2G. Esta además es capaz de bajar de manera automática su potencia para ofrecer a su usuario una mejor calidad de servicio. La razón para que esto suceda es porque esta red aprovecha el espectro de frecuencia con más eficacia debido a que utiliza un ancho de banda mucho más alto.

Ventajas y desventajas de la red 3G

En esta sección verá que hace superior a UMTS o red 3G, en comparación con los sistemas anteriores, visualizará las grandes ventajas tecnológicas que trajo.

- Es dinámico: Un servicio por capas que permite un despliegue rápido y centralizado.
- Mayor velocidad que la de 2G.
- Buena transmisión de voz.
- Calidad y confianza.
- Paquetes de descargas, conocidos como datos móviles que puedes activar y desactivar para el ahorro de consumo.
- Autentificación de red segura.
- Banda ancha.
- Usar la mejor calidad de imágenes disponibles en 3G.
- Acceder con excelente cobertura a cualquier sitio de internet.
- Puedes acceder a tu bandeja de correos electrónicos desde tu móvil
- Al tomar una buena foto ya no solo la guardas en tu móvil, sino que también la puedes compartir.
- Descargar videos, así como de enviar los que hacen con tu móvil, a través de internet.
- Al presentar algún inconveniente cuenta con soporte técnico a distancia.

Aunque esta red sigue siendo útil, la tecnología avanza rápidamente trayendo con ella varias desventajas para la red UMTS, acá algunas de ellas.

- El costo de la estructura junto con su mantenimiento genera alto costo.
- Es limitada en cuando al desarrollo de otro sistema de red mejorado, como el 4G que es diferente al 3G.
- A poca cobertura menos probabilidad de mover datos.
- No disponible en todos los lugares, ya que hay zonas no hay antenas repetidoras de señal.
- Los dispositivos que por general usan este sistema de red son un poco costoso.
- No tener precisión del consumo de datos.
- No todos los modelos de dispositivos que usen este sistema funcionan igual con los diferentes paquetes.
- A medida que ha avanzado la tecnología, no resulta compatible con los nuevos dispositivos que se encuentran en el mercado.

Hay dispositivos móviles que posee red de comunicación tales como 4G o 5G y que ha dejado un poco atrás este sistema UMTS. Sin embargo, su aporte a la sociedad fue enorme, gracias a ella logramos conectarnos a internet desde nuestros móviles.

4G LTE

En telecomunicaciones, **4G** es la sigla utilizada para referirse a la cuarta generación de tecnologías de telefonía móvil. Es la sucesora de las tecnologías 2G y 3G, y precede a la próxima generación, la 5G.

Al igual que en otras generaciones, la Unión Internacional de Telecomunicaciones (UIT) creó un comité para definir las especificaciones. Este comité es el IMT-Advanced y en él se definen los requisitos necesarios para que un estándar sea considerado de la generación 4G. Entre los requisitos técnicos que se incluyen hay uno muy claro: las velocidades máximas de transmisión de datos deben estar entre 100 Mbit/s (12,5 MB/s) para una movilidad alta y 1 Gbit/s (125 MB/s) para movilidad baja. De aquí se empezó a estudiar qué tecnología eran las candidatas para llevar la «etiqueta 4G». Hay que resaltar que los grupos de trabajo de la UIT no son puramente teóricos, sino que la industria forma parte de ellos y estudian tecnologías reales existentes en el momento. Por esto, el estándar LTE (*long term evolution:* 'evolución a largo plazo') de la norma 3GPP no es 4G porque no cumple los requisitos definidos por la IMT-Advanced en características de velocidades pico de transmisión y eficiencia espectral. Aun así la UIT declaró en 2010 que los candidatos a 4G, como era aquel, podían publicitarse como 4G.

La 4G está basada completamente en el protocolo IP, siendo un sistema y una red, que se alcanza gracias a la convergencia entre las redes cableadas e inalámbricas. Esta tecnología podrá ser usada por módems inalámbricos, móviles inteligentes y otros dispositivos móviles. La principal diferencia con las generaciones predecesoras será la capacidad para proveer velocidades de acceso mayores de 100 Mbit/s en movimiento y 1 Gbit/s en reposo, manteniendo una calidad de servicio (QoS) de punta a punta de alta seguridad que permitirá ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo coste posible.

El WWRF (*Wireless World Research Forum*) pretende que 4G sea una fusión de tecnologías y protocolos, no solo un único estándar, similar a 3G, que actualmente incluye tecnologías como lo son GSM y CDMA.[1]

La empresa NTT DoCoMo en Japón fue la primera en realizar experimentos con las tecnologías de cuarta generación, alcanzando 100 Mbit/s (12,5 MB/s) en un vehículo a 200 km/h. La firma lanzó los primeros servicios 4G basados en tecnología LTE en diciembre de 2010 en Tokio, Nagoya y Osaka.

Algunas de las características más relevantes de LTE son:

- Velocidad de transmisión: en el enlace ascendente se pueden obtener hasta 100 Mbps y 50 Mbps en el enlace descendente para un ancho de banda de 20Mhz [4].
- Cobertura: el área de las celdas puede ir de 5Km hasta 100 Km con una degradación después de los 30 Km.
- Movilidad: soporta movilidad de hasta 500 Km/h pero presenta mejores características para velocidades menores, de 0Km/h a 15Km/h [4].
- Latencia: menor a 5 ms, lo cual proporciona una ventaja directa en el servicio para los entornos de aplicaciones tridimensionales y de gran interacción, como software de jugadores múltiples y comunicaciones multimedia [4].
- Capacidad del plano de control: mayor a 200 usuarios por celda para un ancho de banda de 5MHz [4].
- Eficiencia espectral: de 3 a 4 veces la de HSDPA en el enlace descendente y de 2 a 3 veces en el enlace ascendente [4].

Ventajas y desventajas de la tecnología móvil 4G

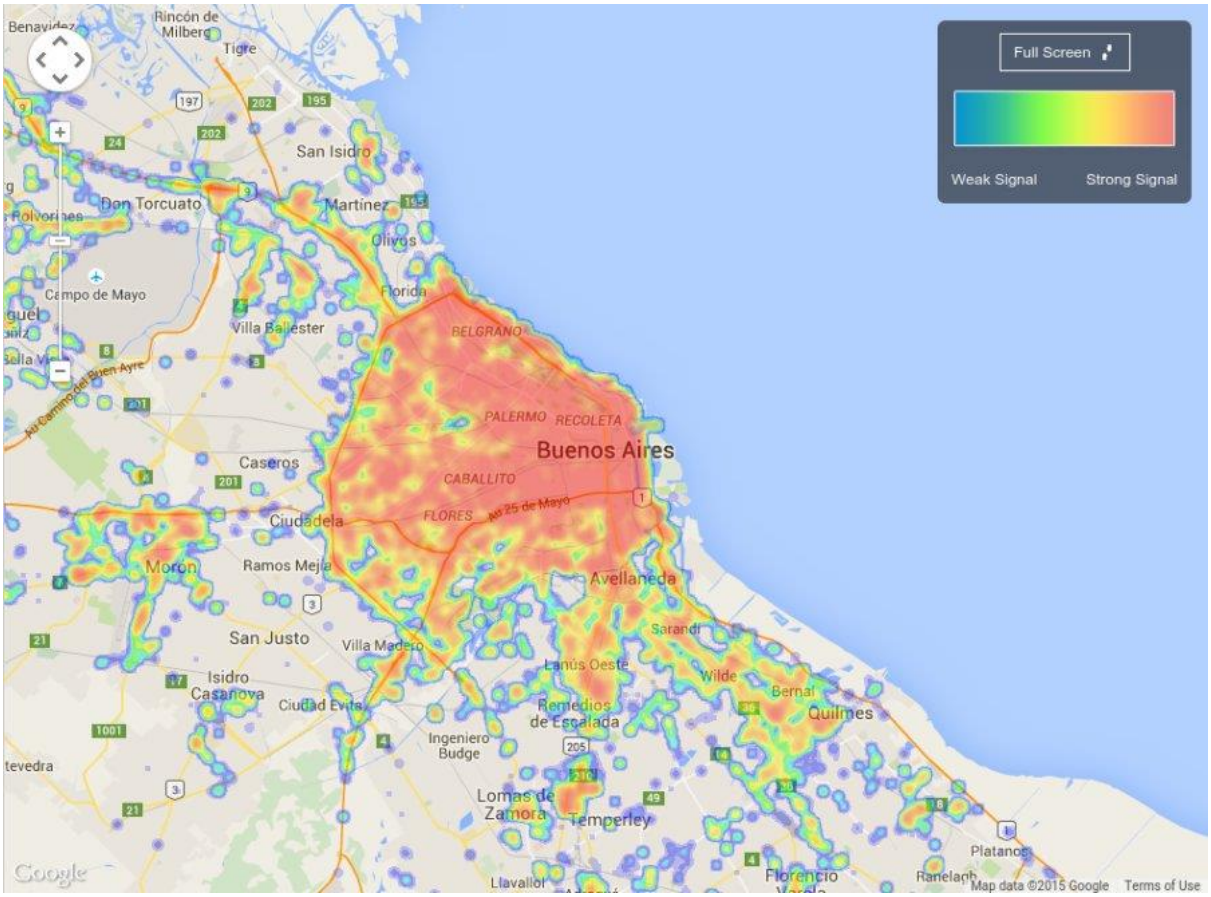
Ventajas

- El 4G es una versión más moderna del 3G con dos mejoras fundamentales: la velocidad y la cobertura.
- Los contenidos que manejamos hoy son fundamentalmente multimedia, es decir, más pesados y que requieren mayor tiempo de carga-descarga. El 4G aumenta la velocidad y reduce estos tiempos.
- El 4G se diseñó para mejorar la velocidad de descarga, alcanzando velocidades máximas de hasta 300 Mbps.
- La tecnología móvil 4G permite una visualización de contenido por streaming con muchos menos cortes que la tecnología de tercera generación.
- Existe una amplia red de cobertura 4G.
- Los dispositivos 4G también son capaces de conectarse a redes 3G para garantizar la cobertura en las zonas más rurales. No ocurre al revés: los dispositivos 3G no podrán conectarse a una red 4G.

Desventajas

- Los dispositivos 4G tienen mayor consumo de batería que los 3G.
- Es más cara que la tecnología 3G.
- Se debe contar un dispositivo compatible con la tecnología 4G. Por lo que, aun teniendo cobertura 4G, será imposible acceder a ella.
- En algunas zonas rurales con cobertura limitada se podrá conectar a la red 3G, pero bajará la velocidad.
- Se irá quedando obsoleta con la llegada de la tecnología de quinta generación (5G).[31]

4G EN ARGENTINA



SATURACIÓN DE SEÑAL

La saturación de las redes suele producirse por una causa muy simple y común: un **aumento de actividad o de usuarios** en las redes móviles o fijas durante un periodo de tiempo, debido a un tráfico inusual de actividad, en el cual las redes no pueden asimilar todo el tráfico, y por tanto **no permiten que más usuarios puedan tramitar sus peticiones de conexión de voz o datos**.

En el caso de las **comunicaciones móviles**, indicar que el espectro del que dispone una operadora es limitado (recurso natural que se distribuye en diferentes **bandas de frecuencia**) y por tanto, tiene un número máximo de usuarios que pueden conectarse y tramitar sus peticiones simultáneamente. El mejor símil es pensar en una autopista donde no hay apenas tráfico y otra en la que, en ciertos horarios, el tráfico es más denso y provoca que no podamos siquiera acceder a la misma o tengamos que movernos a velocidades reducidas.

En el entorno de las conexiones inalámbricas, es decir, las **conexiones vía teléfono móvil** o **WiFi**, las saturaciones normalmente son debidas a la coincidencia simultánea de numerosas petición de conexión (sea datos o voz) por parte de un número de usuarios que supera la capacidad del canal y por tanto satura la red, por ejemplo, durante un evento deportivo, un concierto o una manifestación.

Bibliografía

https://www.telecomsharing.com/es/biblioteca/lte-4g/item/31-que-es-4g-y-cuales-son-las-caracteristicas-tecnicas-mas-importantes

https://es.wikipedia.org/wiki/Telefon%C3%ADa_m%C3%B3vil_4G

https://dplnews.com/argentina-personal-es-el-operador-mas-veloz-y-claro-tiene-mejor-experiencia-de-juego-opensignal/

https://www.adslzone.net/reportajes/tecnologia/que-es-wifi-como-funciona/#370530-los-dos-componentes-del-wifi

https://www.netspotapp.com/es/blog/all-about-wifi/what-is-wifi.html

https://concepto.de/wifi/

https://www.ceac.es/blog/como-funcionan-las-redes-wifi#:~:text=La%20tecnolog%C3%ADa%20Wifi%20se%20basa,del%20rango%20de%20frecuencias%20usado.

https://www.xataka.com/basics/wimax-que-como-funciona

https://www.embou.com/blog/que-es-el-wimax

https://www.adslzone.net/reportajes/wifi/que-es-wimax/

https://www.universidadviu.com/es/actualidad/nuestros-expertos/sistemas-gprs-concepto-general-y-usos-principales

PPT:

https://alumnosuaiedu-my.sharepoint.com/:p:/g/personal/javierramon_avila_alumnos_uai_edu_ar/ETeEpYKA4RFLqoNo1wQLj5kB3jpalwmNcyGrrwoZGOse0A?rtime=ZFilM5fB2kg

Preguntas y Respuestas

1. Defina WIFI y cómo funciona brevemente.
2. Mencione las principales ventajas y desventajas de Wifi
3. Defina WiMax y como funciona brevemente.
4. WIMAX, Qué dispositivos se necesitan y para qué sirven?.
5. Diferencias entre Wifi y WiMax
6. ¿Qué es un sistema GSM?
7. Mencione 4 objetivos del sistema GSM
8. En las celdas GSM, todas las celdas son del mismo tamaño en cada zona geográfica. Verdadero o Falso? y Porque?
9. ¿Cuáles son las características de GPRS?
10. Nombre alguna de las ventajas y desventajas de Umts(3G)
11. ¿Cuáles son algunas de las características que debe tener la red móvil para ser considerada 4g?
12. Nombre tres ventajas de la red 4g
13. Nombre tres desventajas de la red 4g
14. Cual es el espectro radioeléctrico para el 4G en Argentina
15. ¿Porque un móvil celular se queda sin señal?

1. El Wifi es la sigla para Wireless Fidelity, es una tecnología inalámbrica que permite a los dispositivos acceder a internet sin necesidad de cables. Dependiendo del router y la conexión, tiene un alcance de alrededor de 100 metros. La conexión es posible mediante infrarrojos y ondas de radiofrecuencia, gracias a las cuales se puede transmitir información. Para poder acceder a la red Wifi necesitamos su nombre de identificación y la contraseña a través de la cual poder conectar los dispositivos a internet.

El concepto de funcionamiento de este tipo de redes es bastante sencillo. El router recibe Internet a través de un cable Ethernet, y convierte los datos en ondas de radio que envía al dispositivo receptor, dotado de un chip WiFi, que recibe esas ondas y las decodifica para convertirlas en unos y ceros, datos que entienden los ordenadores y los móviles. Este chip WiFi también tiene capacidad para convertir datos en ondas de radio, y enviárselas al router. Así es como subimos datos a Internet.

2. Ventajas Wifi:

- Conectividad inalámbrica: no es necesaria la conexión física por cables
- Comodidad: El hecho de que sea una conectividad inalámbrica no ofrece también una gran comodidad y libertad. El alcance suele ser más que suficiente en la mayoría de hogares, aunque existen numerosas opciones para ampliar el alcance de una WiFi en el caso de que sea necesario.
- Coste: El no tener que hacer uso de cableado y dispositivos como hubs o similares, hace que una red WiFi tenga un coste mucho menor que las redes cableadas.
- Compatibilidad: La WiFi Alliance asegura la compatibilidad total entre dispositivos, por lo tanto, permite una compatibilidad total en cualquier parte del mundo.

Desventajas:

- Velocidad: existen numerosos factores que pueden afectar a la velocidad de nuestra conexión en el dispositivo utilizado para la conexión, como interferencias, grandes distancias y obstáculos.
- Latencia: son más propensas a sufrir ciertos lags, sobre todo cuando queremos reproducir contenido multimedia en alta resolución en streaming.
- Interferencias: ciertos aparatos electrónicos y electrodomésticos pueden generar ondas que interfieren con las de este tipo de redes inalámbricas, pero, además, hay ciertos elementos como muros o puertas que también pueden hacer que la señal llegue a ciertos rincones de la casa.
- Microcortes: pequeños cortes en la señal wifi que pueden influenciar negativamente en nuestra conexión.

3. WiMAX significa Worldwide Interoperability for Microwave Access, lo que en español se podría traducir como Interoperabilidad Mundial para Acceso por Microondas. Se trata de un método de transmisión de datos a través de ondas de radio, y que utiliza las frecuencias de 2,5 a 5,8 GHz, mediante conexión inalámbrica basada en los estándares de comunicación IEEE 802.16, y que permite llevarte Internet con un alcance que puede llegar a los 70 kilómetros.

El funcionamiento de WiMAX es sencillo, ya que simplemente es el repetidor de la empresa a la que lo contrates emitiendo las señales de microondas que te llegan a la antena que tengas en tu casa. Por lo tanto, lo primero que necesitas es contactar con una empresa que ofrezca estos servicios y que tenga un repetidor cerca de tu casa para poder enviarte la señal. Luego, tienes que poner una pequeña antena en la fachada de tu casa. Esta antena tendrá que apuntar directamente al repetidor de la empresa que te va a dar el servicio, o sino a un punto de conexión intermedio que se utilice para salvar obstáculos que se interpongan entre tu antena y su repetidor. Entonces, desde la antena bajará un cable que llegará a tu casa, y que se conectará directamente a tu ordenador o a un router con el que poder gestionar la conexión como si se tratase de una red de fibra o cable convencional, pudiendo crear tu propia WiFi doméstica.

4. Participan los siguientes dispositivos:

- Estación base o Repetidor: es el encargado de emitir las señales de microondas para permitir la conexión a Internet.
- Puntos de conexión intermedios: facilita que lleguen las microondas hasta el objetivo si existe algún elemento que pueda impedir el alcance máximo de las ondas emitidas hasta el objetivo.
- Antena: se instala para recibir la señal de repetidor en el destino.
- Cableado hasta nuestro router o dispositivo: instalación del cableado necesario para que los dispositivos tengan acceso a la red o conexión a un router para este luego crear una red Wifi interna.

5.

Características	WIFI	WIMAX
Protocolo	802.11	808.16
Velocidad	11-54 Mbit/s	124 Mbit/s
Cobertura	300m	40-70 km
Licencia	No	Si/No
Ventajas	Velocidad/precio	Velocidad/alcance
Desventajas	Bajo alcance	Cobertura limitada
Usuarios	Cientos	Miles
Movilidad	Limitado a puntos de conexión	Cualquier momento/Cualquier lugar

6. Se llama Global System for Mobile Communications**,** es un sistema de comunicación más seguro ya que toda la información que transmitimos viaja de manera encriptada por el aire, donde en cada llamada genera nuevos códigos para evitar ser interceptada y/o reconstruida.

7. Objetivos:

- Incluir roaming internacional
- Terminales y sistema de bajo coste
- Buena calidad de voz (comparable a la telefonía fija)
- Ampliación de servicios

8. Falso, porque depende de la cantidad de usuarios, cuando hay más usuarios, más riesgo hay de que se produzca saturación. En zonas con elevada densidad de usuarios (ej. ciudades) se tiende a crear celdas pequeñas, mientras que en zonas rurales, con densidad pequeña, se prefiere crear celdas grandes.

9.

- Cuenta con todos los beneficios del sistema GSM, es decir, servicio de mensajes cortos (SMS), servicio de mensajería multimedia (MMS) y otros.
- Permite descargar archivos de manera mucho más rápida que por medio de tecnologías predecesoras.
- Al estar basado en la tecnología GSM, permite una comunicación permanente y estable durante la realización de llamadas de voz.
- Permite realizar llamadas de voz sin cortar la transmisión de datos en el equipo, ya que el GPRS trabaja de manera simultánea al sistema GSM (solo en equipos clase A).

10. Ventajas :

- Es dinámico: Un servicio por capas que permite un despliegue rápido y centralizado.

- Mayor velocidad que la de 2G.
- Buena transmisión de voz.
- Calidad y confianza.

Desventajas:

- El costo de la estructura junto con su mantenimiento genera alto costo.
- Es limitada en cuando al desarrollo de otro sistema de red mejorado, como el 4G que es diferente al 3G.
- A poca cobertura menos probabilidad de mover datos.
- No disponible en todos los lugares, ya que hay zonas no hay antenas repetidoras de señal.
- Los dispositivos que por general usan este sistema de red son un poco costoso.
- No tener precisión del consumo de datos.

11. Algunas característica de la red movil que debe cumplir para que sea considerada 4G son:

- Velocidad de transmisión: en el enlace ascendente se pueden obtener hasta 100 Mbps y 50 Mbps en el enlace descendente para un ancho de banda de 20Mhz [4].
- Cobertura: el área de las celdas puede ir de 5Km hasta 100 Km con una degradación después de los 30 Km.
- Movilidad: soporta movilidad de hasta 500 Km/h pero presenta mejores características para velocidades menores, de 0Km/h a 15Km/h [4].

12. Algunas de las ventajas de la red 4G son:

- El 4G es una versión más moderna del 3G con dos mejoras fundamentales: la velocidad y la cobertura.
- Los contenidos que manejamos hoy son fundamentalmente multimedia, es decir, más pesados y que requieren mayor tiempo de carga-descarga. El 4G aumenta la velocidad y reduce estos tiempos.
- El 4G se diseñó para mejorar la velocidad de descarga, alcanzando velocidades máximas de hasta 300 Mbps.

13. Algunas de las desventajas del 4G son:

- Precio de los equipos compatible con esta tecnología
- Consumo de Batería
- Precio de consumir el servicio 4G
- Las áreas de cobertura 4G se reserva para las grandes urbes, dejando a la zonas rurales aun con tecnología 3G

14. El espectro de frecuencia para el 4G en argentina oscila entre 1700 MHZ y 2100 MHZ.

15. Un celular puede quedarse sin señal, por algunos de los siguientes motivos:

- Problema en el equipo celular o el módulo GSM
- Saturación de las antenas de telefonía de la zona, caída en los servicios de las prestadoras telefónicas,
- El equipo se quedó sin saldo, por lo cual la prestadora bloquea el envio a ese equipo.

REDES ADMINISTRATIVAS

UNIDAD 6: REDES INALAMBRICAS DE AREA AMPLIA

CLASE 12 WWAN WLAN WPAN

Claudio Milio 2020

Bienvenidos a la clase 12 donde veremos las diferentes tecnologías inalámbricas de redes WAN.

COMPARACION DE LAS DISTINTAS REDES

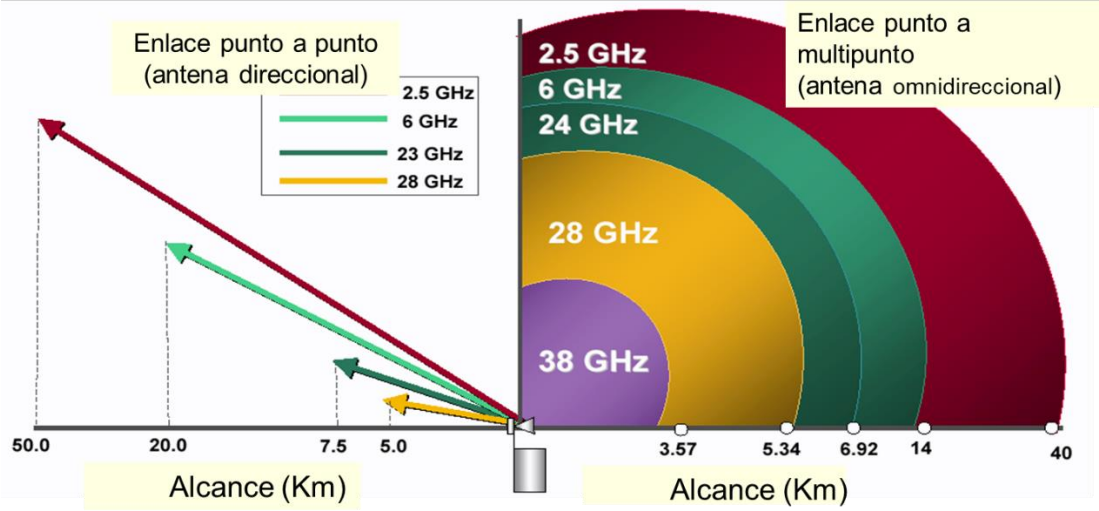
En la figura siguiente se muestra las características de cada tecnología inalámbrica.

Tipo de red	WWAN (Wireless WAN)	WLAN (Wireless LAN)	WPAN (Wireless Personal Area Network)
Estándar	GSM/GPRS/UMTS	IEEE 802.11	IEEE 802.15 (Bluetooth)
Velocidad	9,6/170/2000 Kb/s	1-2-11-54 Mb/s(*)	721 Kb/s
Frecuencia	0,9/1,8/2,1 GHz	2,4 y 5 GHz Infrarrojos	2,4 GHz
Rango	35 Km	70 - 150 m	10 m
Técnica radio	Varias	FHSS, DSSS, OFDM	FHSS
Itinerancia (roaming)	Sí	Sí	No
Equivalente a:	Conexión telef. (módem)	LAN	Cables de conexión

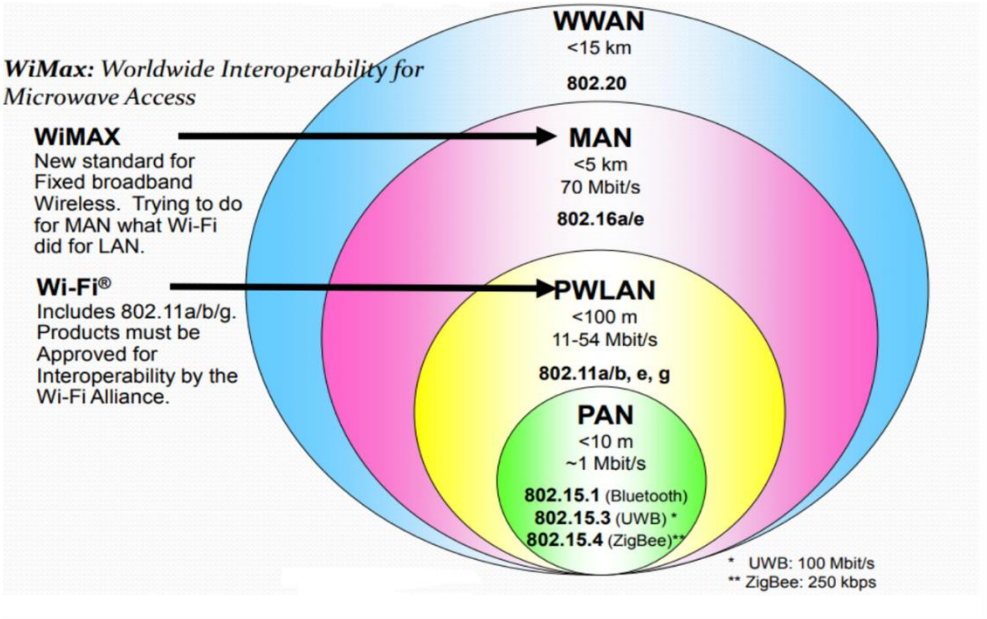
(*) Las velocidades bajas (1-2 Mb/s) corresponden a la norma 802.11 antigua

En función de la frecuencia varía el alcance de las ondas de radio.

- El alcance de las señales de radio disminuye a medida que aumenta la frecuencia.
- Otro factor que influye en el alcance es el uso de antenas direccionales, que permite concentrar el haz de emisión electromagnética en una dirección concreta.



En este gráfico, se muestra la variación de la frecuencia según la tecnología.



¿Qué es Wireless Local Loop?

El bucle local inalámbrico (Wireless local loop (WLL), radio in the loop (RITL), fixed-radio access (FRA) o fixed-wireless access (FWA) en inglés), es el uso de un enlace de comunicaciones inalámbricas como la conexión de "última milla" para ofrecer servicios de telefonía (POTS) e Internet de banda ancha a los usuarios.

Se trata principalmente del uso de frecuencias licenciadas, descartándose las llamadas "bandas libres" debido a la carencia de garantías, por tratarse de frecuencias de uso compartido, con el correspondiente riesgo de saturación y no disponibilidad de la red.

Se utiliza una red de Estaciones Base que concentran el tráfico que le envían mediante radioenlaces los diferentes terminales instalados en los abonados. Estas estaciones llevan ese tráfico hasta la central de conmutación a través de las Redes de Transporte ya sea por fibra óptica o radioenlace.

- Se instala una estación transmisora y antenas receptoras en los sitios de abonado.
- Requiere línea de vista para la transmisión.
- Transmisión sujeta a licencias de uso del espectro.
- Permiten la transmisión y recepción de señales de datos.

WIRELESS WAN

La red inalámbrica WAN, enlazan dispositivos sobre grandes distancias de tierra.

Las compañías de teléfonos celulares utilizan estas redes para permitir el acceso a Internet a sus clientes, a menudo bajo el término "banda ancha móvil".

La red inalámbrica WAN tiende a ofrecer una transferencia de datos más lenta que la red WLAN.

Los servicios WWAN suelen incluirse en los teléfonos inteligentes y otros dispositivos de mano, que son comercializados por proveedores de servicios celulares.

A diferencia de las tarjetas Wi-Fi, que se pueden utilizar en casi cualquier punto de acceso, los dispositivos WWAN deben ser provistos por el proveedor del servicio específicamente para el acceso a la red.

Su proveedor de servicios se encargará de la facturación para la itinerancia de acceso que implica otras redes de proveedores.

Las redes inalámbricas de área extensa (WWAN) tienen el alcance más amplio de todas las redes inalámbricas.

Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa.

Las principales tecnologías son:

- GSM (Global System for Mobile Communication)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System)
- LTE (Long Evolution Term).

ESTANDAR GSM

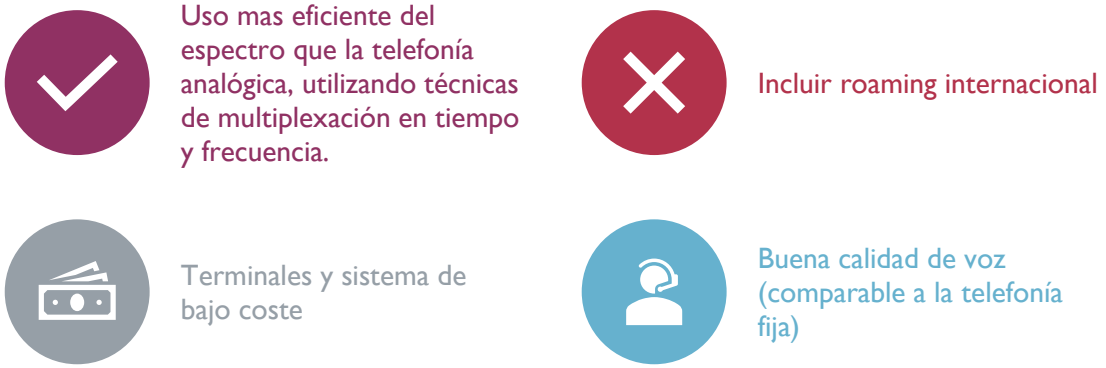
GSM es la abreviatura de Global System for Mobile Communications

La tecnología GSM es el sistema de comunicación más seguro puesto que toda la información que usted transmite viaja encriptada por el aire, con nuevos códigos en cada llamada, y no se han dado nunca casos de ser interceptada y/o reconstruida.

Posee un ancho de banda de 200 KHZ.

El GSM es la tecnología líder a nivel mundial, con más de 380 millones de usuarios en más de 150 países.

Son objetivos de GSM:



Ampliación de servicios

Baja potencia de transmisión: reutilización de canales, al no saturar canales de células vecinas

Ofrece diversos tipos de servicios como:

- Teleservicios: voz, SMS (Short Message Service) de 160 bytes, fax, etc...
- Servicios portadores (datos)
- Servicios complementarios (llamadas en espera, multiconferencias, identificación de llamadas, etc.)

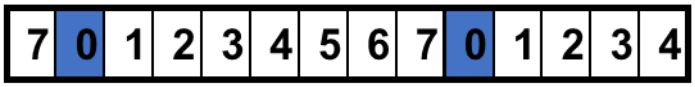
En cuanto a la radio frecuencia, GSM utiliza dos bandas de frecuencia cada una de 25 Mhz de ancho:

- 890-915 Mhz, desde la estación móvil a la estación base (ascendente)
- 935-960 Mhz, desde la estación base a la estación móvil (descendente)

Cada banda se divide en 125 canales de 200 KHz de ancho cada uno.

El primer canal está reservado, por lo que hay disponibles 124.

Cada canal se divide por TDMA (Acceso Multiple por Division de Tiempo) en ocho ranuras que dan servicio a otros tantos usuarios:



La ranura asignada a una comunicación se cambia (en tiempo y frecuencia) a razón de 217 cambios/seg; esto se denomina frequency hopping y se hace para evitar interferencias.

Cada ranura transporta 22,8 Kb/s de información digital 'en bruto' y por ella se puede enviar voz (13,2 Kb/s) o datos (9,6 Kb/s).

La combinación de una ranura de subida y una de bajada permite una comunicación full dúplex.

El número máximo de comunicaciones simultáneas es teóricamente de 124*8=992. Sin embargo, muchos canales no se pueden usar para evitar conflicto con las celdas vecinas.

CODIFICACION DE LA VOZ

Una conversación telefónica normal ocupa en formato digital 64 Kb/s (8.000 muestras de un byte por segundo)

En GSM la voz se comprime según un algoritmo llamado RPE-LPC (Regular Pulse Excited – Linear Predictive Coder) que da una calidad casi equivalente usando sólo 13,2 Kb/s

Además, en GSM solo se transmite cuando la persona habla (transmisión discontinua o supresión de silencios).

Esto supone un ahorro del 60% en el canal y reduce el gasto de batería del emisor.

Para evitar que el receptor crea que la conexión se ha cortado la transmisión discontinua se acompaña de ruido de confort.

CELDAS GSM

El área atendida por una estación base (BTS) se denomina celda.

Todos los usuarios de una misma celda comparten los canales disponibles.

Cuantos más usuarios hay dentro de una celda más riesgo hay de que se produzca saturación.

En zonas con elevada densidad de usuarios (ej. ciudades) se tiende a crear celdas pequeñas.

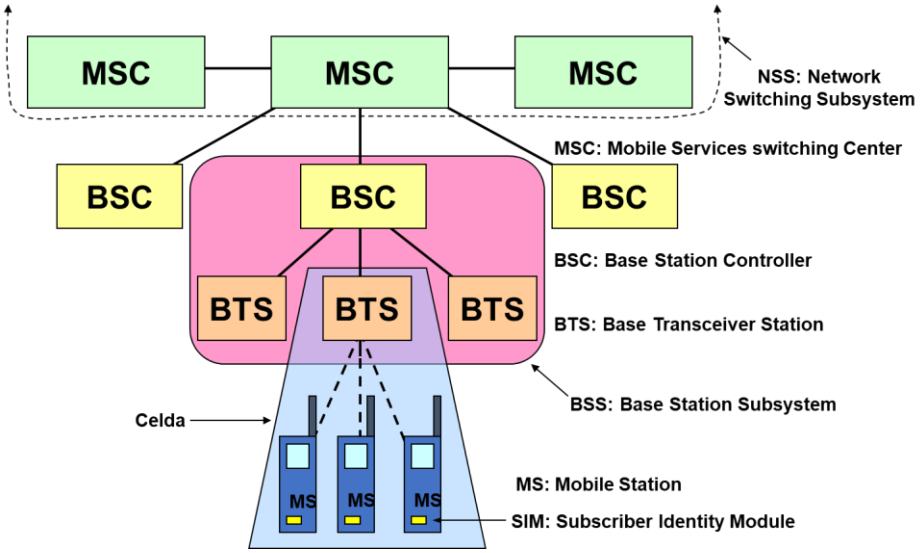
En zonas rurales, con densidad pequeña, se prefiere crear celdas grandes.

Las celdas vecinas se agrupan en clusters.

Dentro de un cluster cada canal solo se utiliza una vez, para evitar interferencias.

Cada cluster está formado por 4, 7, 12 o 21 celdas, según la topología del terreno y las circunstancias concretas de la zona.

ARQUITECTURA DE UNA RED GSM



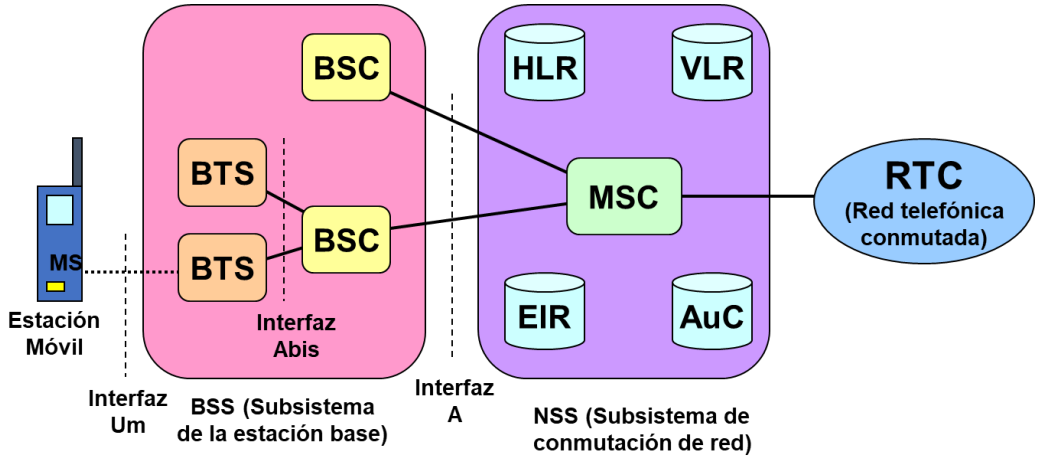
ROAMING

Se produce cuando tratamos de identificarnos y el terminal no es capaz de encontrar la red.

Permite que un usuario haga uso de una red foránea (si el operador tiene acuerdo y el roaming está habilitado)

La red foránea obtiene el HLR (Home Location Register) del usuario y lo incorpora en su VLR (Visitor Location Register.

El usuario visitante corre a cargo con el costo extra cuando recibe una llamada.



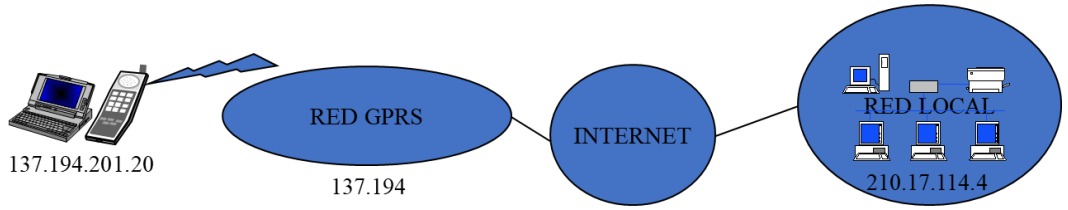
SIM: Subscriber Identity Module
MS: Mobile Station
BTS: Base Transceiver Station
BSC: Base Station Controller
BSS: Base Station Subsystem

HLR: Home Location Register
VLR: Visitor Location Register
MSC: Mobile Services switching Center
EIR: Equipment Identity Register
AuC: Authentication Center
NSS: Network Switching Subsystem

GPRS

GPRS retoma la arquitectura BSS (Base Station Subsystem) de GSM, pero tiene una arquitectura fija diferente de NSS (Network Switching Subsystem).

Utiliza los conceptos de IP móvil y de CDPD (Cellular Digital Packet Data) de USA



Usa multiplexado estadístico en BSS para transmitir los paquetes sobre la radio.

Puede utilizar más de una ranura de tiempo por trama TDMA, lo que permitiría velocidades de hasta 171,2 kbps (máximo teórico inalcanzable)

En la práctica, se usan como máximo 4 ranuras a 12 kbps c/u o sea 48 kbps.

SERVICIOS QUE OFRECE.

Las velocidades previstas permiten:

- Consulta de la Web (HTTP)
- Transferencia de archivos (FTP)
- Transmisión de video comprimido
- Servicios Punto a Punto y Punto a Multipunto (para una segunda fase)
- Los servicios PTP pueden ser orientado a conexión (X.25) o sin conexión (IP)
- También tiene un servicio de mensajes cortos

En cuanto a la calidad de servicio, brinda:

- Prioridad
- Confiabilidad
- Retardo
- Velocidad

ARQUITECTURA GPRS

Los 2 elementos fundamentales de la arquitectura GPRS son SGSN y GGSN:

- SGSN (Serving GPRS Support Node)

  Es el elemento que gestiona todas las funciones de movilidad, autenticación y registro en la red de las estaciones móviles.

  Está conectado al BSC y es el punto de acceso a la red GPRS cuando un terminal solicita este servicio.

  Cuando una estación quiere enviar/recibir datos hacia o desde redes externas, el SGSN intercambia los datos con el pertinente GGSN. Encapsula los paquetes.

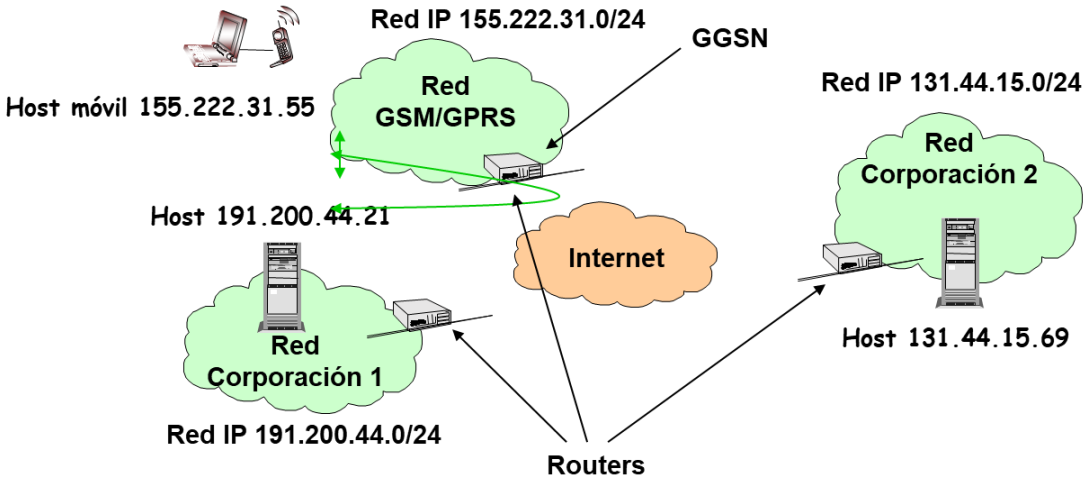
- GGSN (Gateway GPRS Support Node)

  Se conecta a redes externas como Internet o X.25.

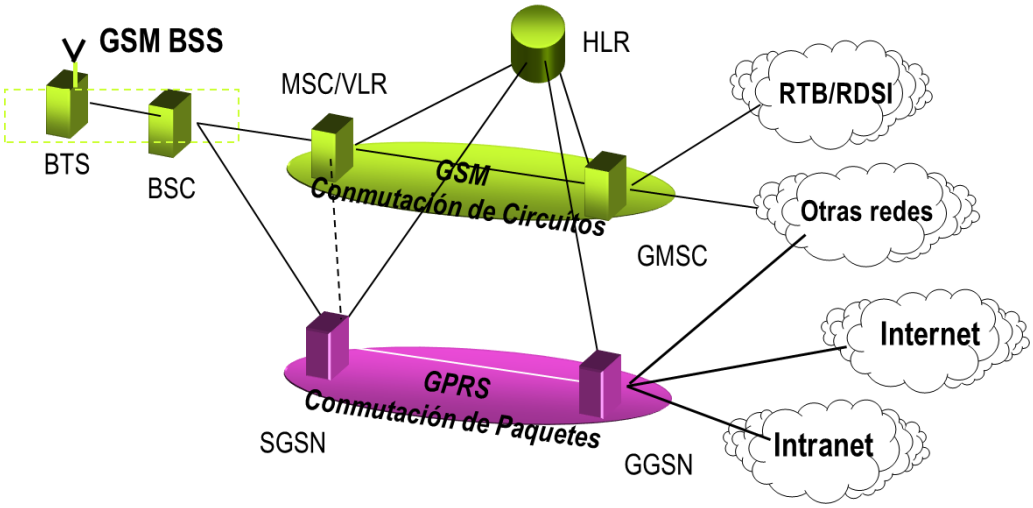
  Es un dispositivo de encaminamiento hacia una subred ya que hace que la infraestructura de la red GPRS sea transparente vista desde fuera.

  Cuando recibe datos dirigidos hacia un usuario específico, comprueba si la dirección está activa, y en caso afirmativo, envía los datos al SGSN.

Encamina hacia la red correspondiente los datos que origina el móvil.



El GGSN se comporta como un router, de forma que "camufla" las características especiales de la red GPRS desde el punto de vista de la red externa



La red GPRS es una red de Conmutación de Paquetes que se superpone y convive con la estructura de Conmutación de Circuitos propia de GSM.

TRAFICO DE DATOS EN GPRS.

GPRS utiliza las mismas ranuras TDM que GSM, con cuatro posibles esquemas de codificación:

- Se pueden usar varias ranuras de un mismo canal en una misma comunicación.

- La velocidad máxima teórica es de 21,4 * 8 = 171,2 Kb/s
- El número de ranuras y la codificación empleadas son negociados entre la red y el usuario
- Se distingue entre la información real y la útil transmitida

GESTION DE LAMOVILIDAD.

Los datos se transmiten a un móvil, sólo cuando está activo.

En el estado activo, el SGSN conoce la celda donde está localizado el móvil.

En standby, se conoce la ubicación a nivel de Area de Enrutamiento (similar a Area de Localización en GSM)

Para enviar paquetes a un móvil en standby, primero hay que hacer paging, para localizarlo, y pasar al estado activo para recibir los datos

Para enviar paquetes a un móvil activo, se le avisa que hay paquetes y luego se le transmiten

La razón del estado standby es para reducir la carga sobre la red para conocer la celda donde está

En el estado inactivo el móvil no tiene dirección asignada

DIRECCIONAMIENTO DE GPRS.

El direccionamiento se realiza por medio de direcciones IP

Según la naturaleza de estas direcciones tendremos:

- Direcciones IP Privadas: accesibles sólo dentro de un entorno determinado dentro de la red
- Direcciones IP Públicas: accesibles desde cualquier punto de Internet.

Según la asignación de estas direcciones tendremos:

- Direcciones IP Estáticas: estas direcciones irán asociadas de forma estática vía el HLR
- Direcciones IP Dinámicas: estas direcciones se obtienen de unos pools de direcciones gestionados bien por el Operador de la red bien por una Entidad Externa (como un servidor DHCP).

CLASES DE TERMINALES MOVILES QUE ACEPTAN GPRS

Clase A: Soportan GPRS y GSM simultáneamente. Se pueden efectuar o recibir llamadas mientras se está en internet.

Clase B: Soportan GPRS y GSM pero permiten el tráfico simultáneo.

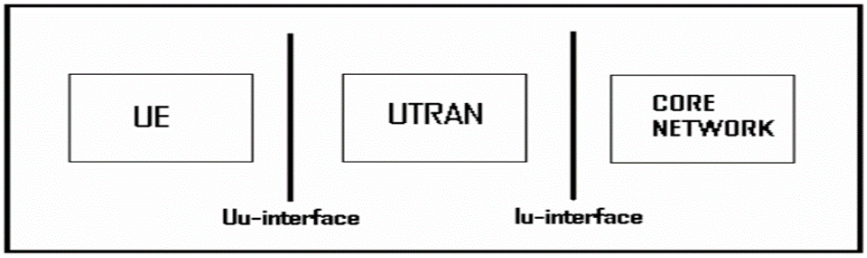
Clase C: El usuario debe seleccionar a que tipo de servicio se conectará. El servicio que no está activado no es operativo, salvo SMS (Short Messages Service) que es optativo.

UMTS

UMTS (Universal Mobile Telecommunication System) presenta una arquitectura en la cual se describen tres elementos principalmente, el UE o equipo de usuario, UTRAN (UMTS Terrestrial Radio Access Network) y la red central

La interfaz Uu se encuentra entre el UE y la red UTRAN, y entre esta y la red central o Core Network se encuentra la interfaz Iu. Cabe destacar que la interfaz entre el UE y la red UTRAN es la tecnología WCDM

La conexión entre el equipo de usuario y la red de acceso de radio para UMTS es mediante la tecnología WCDMA.



Si consideramos una arquitectura más detallada de la red de UMTS, podemos encontrar diferentes elementos como lo son el BSS, BTS, RNS, Nodo B, RNC, MSC, VLR, HLR entre otros, y diferentes interfaces como lo son: la interfaz Iu, Uu, Iub y Iur entre otras, las cuales interconectan dichos elementos.

UMTS adoptó para el acceso de radio la tecnología CDMA de banda ancha, conocido como WCDMA.

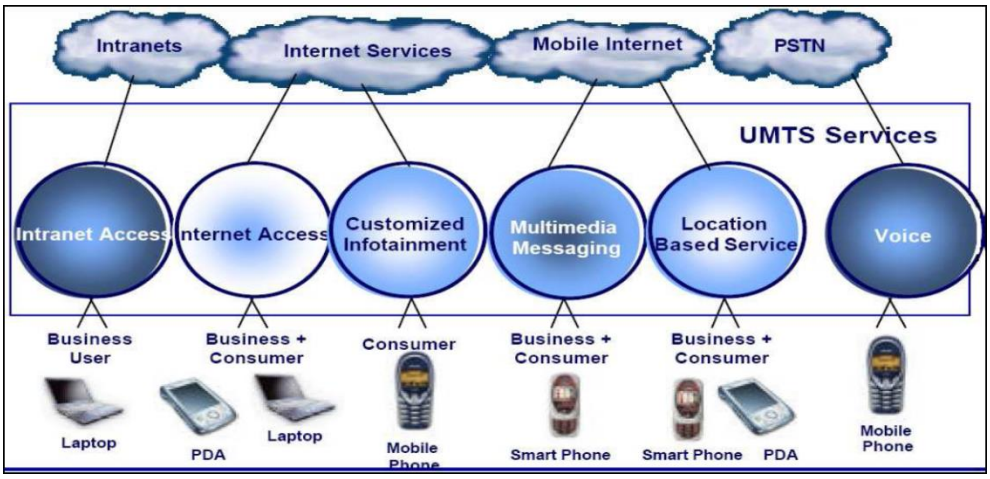


Ilustración 1 Servicios de UMTS

La concepción del sistema UMTS viene condicionada por los requisitos de los servicios que ofrece esta generación de redes móviles

- Tasas de transmisión de 2048 Kbps para interiores o ambientes de poco movimiento.
- Tasas de transmisión de 384Kbps en ambientes urbanos y a velocidades máximas de 130 Km/h
- Movilidad global
- Mayor eficiencia espectral
- El usuario podrá distinguir que red lo está sirviendo

ARQUITECTURA UMTS.

Conserva la estructura de la red GSM/GPRS

A diferencia de GPRS, aparece una interfaz de radio, la UTRAN, en ella, las BTSs serán sustituidas por nodos B y las BSCs por los RNC (Radio Network Controller), aparece la interfaz Iu.

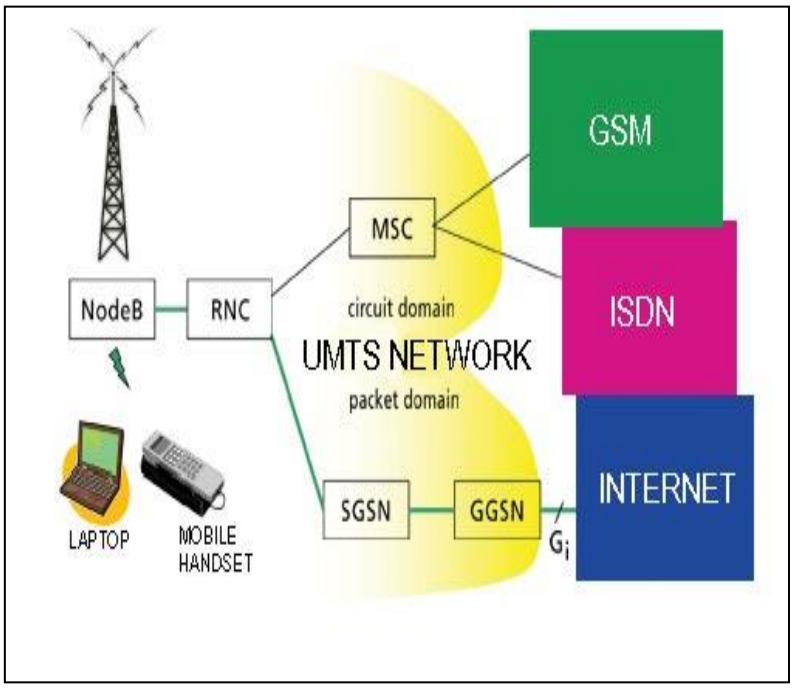
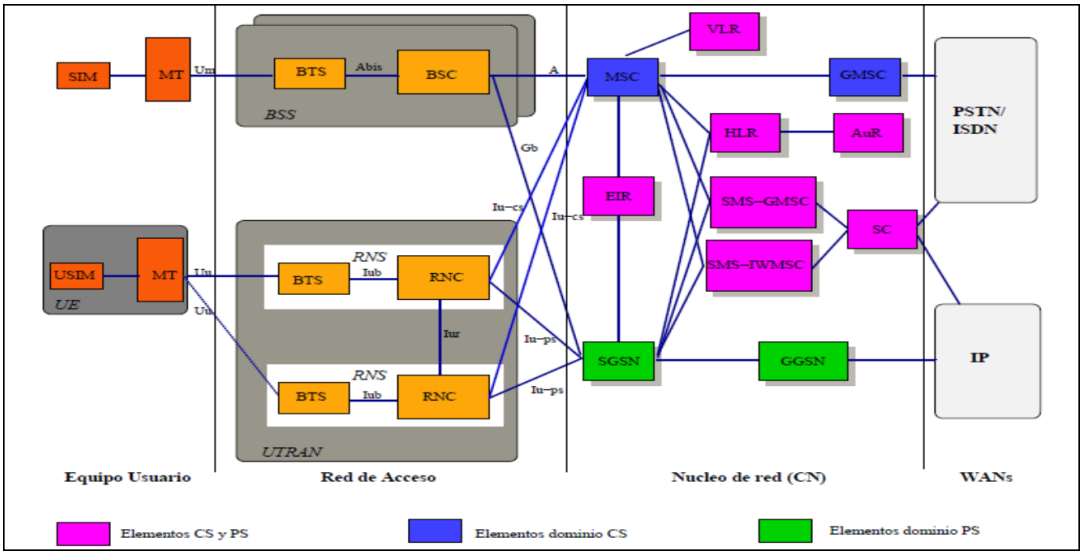


Ilustración 2 UMTS

NUCLEO DE RED.

UMTS establecida por la 3GPP R99, establece un sistema de Radio Acceso de Banda Ancha y un Núcleo de Red evolucionado de GSM que contiene el dominio de conmutación de circuitos (Domain CS) y dominio de conmutación de paquetes (Domain PS).



UE. EQUIPOS DE USUARIO.

El equipo de usuario o UE, también llamado móvil, es el equipo que el usuario trae consigo para lograr la comunicación con una estación base en el momento que lo desee y en el lugar en donde exista cobertura.

Este puede variar en su tamaño y forma, sin embargo debe estar preparado para soportar el estándar y los protocolos para los que fue diseñado.

Por ejemplo, si un móvil trabaja bajo el sistema UMTS, debe ser capaz de acceder a la red UTRAN mediante la tecnología de WCDMA para lograr la comunicación con otro móvil, con la PSTN, o un sistema diferente como GSM de 2.5G, tanto para voz como para datos.

UTRAN. RED DE ACCESO DE RADIO.

UTRAN es el nombre de la nueva red de acceso de radio diseñada para el sistema UMTS.

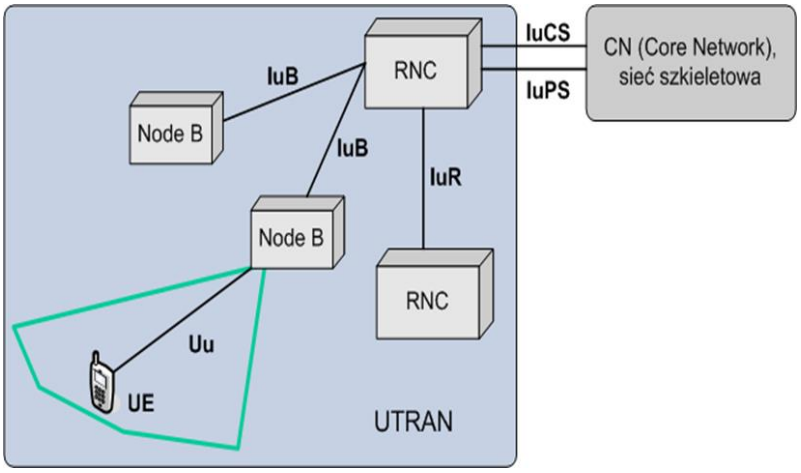
Tiene dos interfaces que lo conectan con la red central y con el equipo de usuario, la interfaz Iu y la interfaz Uu respectivamente.

La red UTRAN consiste de varios elementos, entre los que se encuentran los RNC (Radio Network Controller) y los Nodo B (en UTRAN las estaciones base tienen el nombre de Nodo B).

Ambos elementos juntos forman el RNS (Radio Network Subsystem)

Contiene uno o más subsistemas RNS (Radio Network Subsystem) y está formado por un controlador RNC (Radio Network Controller) y un conjunto de estaciones base (Nodos B).

Se especifican dos tipos de interfaces: la interfaz Iub entre cada Nodo B y el RNC que lo controla y la interfaz Lur entre RNCs.



RNC. RADIO NETWORK CONTROLER.

El RNC controla a uno o varios Nodos B y se conecta con el MSC mediante la interfaz luCS o con un SGSN mediante la interfaz luPs.

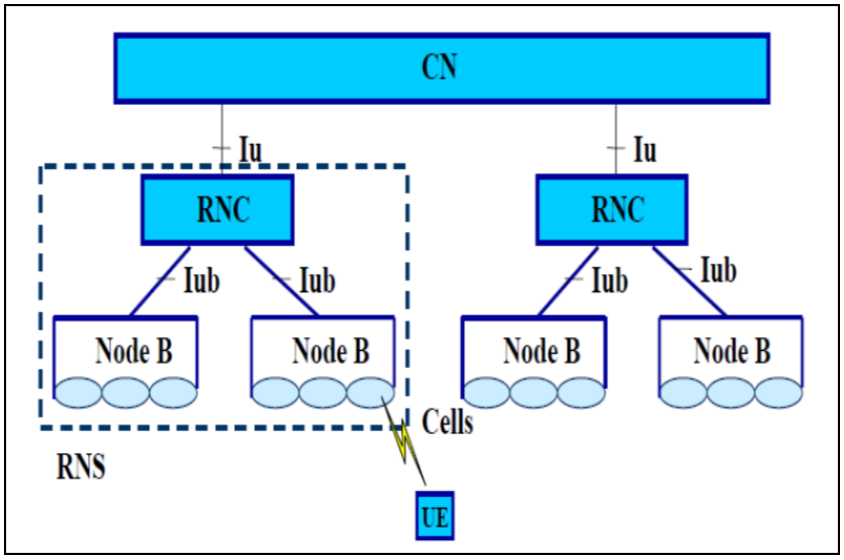
La interfaz entre dos RNC's es lógica y es la interfaz lur por lo tanto una conexión directa entre ellos no es necesario que exista.

Si comparamos al RNC con la red de GSM, éste es comparable con el BTS (Base Station Controller).

Desde el RNC se controlan los recursos lógicos hacia el nodo B y provee el control descentralizado de los Nodos B en su área de cobertura.

También se encarga del manejo de los recursos de radio:

- El control de admisión
- Asignación de canal
- Control de Handover
- Señalización de Broadcast
- Control de potencia



El NODO B.

Es la unidad de transmisión/recepción que permite la comunicación entre las radio celdas

Se conecta con el equipo del usuario (UE) a través de la interfaz de radio Uu utilizando WCDMA.

Soporta los modos FDD y TDD simultáneamente

La principal función del nodo B es la conversión de unidades de radio en la interfaz de radio Uu

El nodo B es el equivalente en UMTS del BTS de GSM (Base Tranceiver Station). El Nodo B puede dar servicio a una o más células, sin embargo, las especificaciones hablan de una sola célula por Nodo B.

INTERFAZ Lu.

Esta interfaz conecta a la red central con la red de acceso de radio de UMTS (UTRAN).

Cabe mencionar que UTRAN es un concepto genérico y puede tener muchas implementaciones físicas.

La primera a ser implementada es la UTRAN, la cual utiliza a la tecnología de WCDMA como interfaz aérea.

Es la interfaz central y la más importante para el concepto de 3GPP.

La interfaz lu puede tener dos diferentes instancias físicas para conectar a dos diferentes elementos de la red central, todo dependiendo si se trata de una red basada en conmutación de circuitos o basada en conmutación de paquetes.

En el primer caso, es la interfaz lu-CS la que sirve de enlace entre UTRAN y el MSC y es la interfaz lu-PS la encargada de conectar a la red de acceso de radio con el SGSN de la red central.

MOBILE SWITCHING CENTER (MSC)

Es el mismo MSC tanto para GSM como para UMTS

La BSS de GSM y el RNS de UTRAN se pueden conectar con el mismo MSC.

Constituye la interfaz entre el sistema de radio y la red fija.

Cobertura de radio de un área geográfica

HOME LOCATION REGISTER (HLR)

Contiene los datos permanentes del registro de suscriptor.

Hay dos tipos de información en HLR, el registro de entrada permanente y temporal.

Los datos permanentes incluyen:

- Identidad internacional de suscriptor
- Posibles restricciones de roaming
- Clave de autentificación
- Parámetros de servicios suplementarios

Los datos temporales incluyen:

- Identidad local de la estación móvil
- Numero de MSC
- Numero de VLR

VISITOR LOCATION REGISTER (VLR)

Contiene información acerca del Roaming en esta área del MSC

El VLR contiene mucha de la misma información que el HLR

El VLR contiene toda la información necesaria para manejar las llamadas realizadas o recibidas por el móvil registrado en la base de datos

EQUIPMENT IDENTITY REGISTER (EIR)

Es una base de datos en la que existe información sobre el estado de los teléfonos móviles con los siguientes datos:

- **Lista blanca**: Los IMEIs de equipos que están en buen orden
- **Lista Negra**: Los IMEIs de equipos reportados o perdidos

- **Lista Gris**: Los IMEIs de equipos que contienen problemas

AUTHENTICATION CENTER (AUC)

Almacena la clave de autentificación del suscriptor. Este se asocia con un HLR y almacena su correpondiente IMSI (International Mobile Suscriber Identity).

SERVING GPRS SUPPORT NODE (SGSN)

Es un elemento central en la conmutación de paquetes y se conecta con UTRAN mediante la interfaz Iu-PS.

GATEWAY MSC (GMSC)

Es un MSC que está localizado entre la PSTN y los otros MSCs en la Red y rutea llamadas entrantes al apropiado MSC.

LTE

LTE"Long-Term Evolution" es una evolución a largo plazo del sistema UMTS para permitir mayores tasas binarias y menor latencia (retardo).

El termino LTE se planteó inicialmente en 3GPP para denominar una línea de trabajo interna cuyo objeto de estudio era la evolución de la red de acceso de UMTS, denominada como UTRAN (Universal Terrestrial Radio Access Network).

Formalmente, la nueva red de acceso recibe el nombre de E-UTRAN (Evolved Universal Terrestrial Radio Access Network) aunque muchas veces se utiliza también el término LTE en las especificaciones como sinónimo de E-UTRAN.

Asimismo, en lo concerniente a la red troncal, 3GPP utilizó el término SAE (System Architecture Evolution)

Formalmente, dicha red troncal se denomina EPC (Evolved Packet Core) y de la misma forma que pasa con la red de acceso, es común encontrar el término de SAE como sinónimo de EPC.

La combinación de la red de acceso E-UTRAN y la red troncal EPC es lo que constituye la nueva red UMTS evolucionada y recibe el nombre formal de EPS (Envolved Packet System).

La primera especificación del sistema EPS ha sido incluida en las especificaciones del 3GPP).

El nombre "LTE" se refiere a la interfaz radio.

El núcleo de red se conoce como "System Architecture Evolution"(SAE).

ARQUITECTURA GENERAL DE LOS SISTEMAS 3GPP

Las arquitecturas de red contempladas en la familia de sistemas especificados por 3GPP se adaptan a la arquitectura genérica de los sistemas celulares.

Tal como se muestra en la figura, los sistemas 3GPP abarcan la especificación del equipo de usuario y de una infraestructura de red que se divide de forma lógica en una infraestructura de red troncal (Core Network, CN) y una de red de acceso (Access Network, AN).

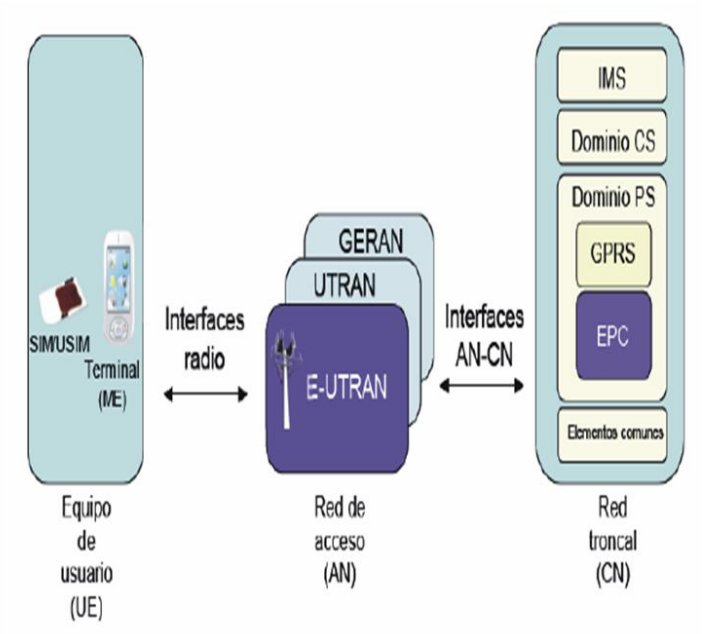


Ilustración 3 Arquitectura de alto nivel de los sistemas 3GPP (GSM, UMTS y LTE)

El equipo de usuario en 3GPP se compone de dos elementos básicos: el propio dispositivo móvil o terminal (denominado como Mobile Equipment, ME, en las especificaciones) y una tarjeta UICC (Universal Integrated Circuit Card).

La tarjeta UICC, también denominada SIM (Subscriber Identity Module) en sistemas GSM y USIM (Universal SIM) en UMTS y LTE, es la encargada de almacenar la información y sustentar los procedimientos que tienen que ver con la suscripción del usuario a los servicios proporcionados por la red.

Mediante esta separación entre terminal y tarjeta se permite que un usuario, identificado a través de la SIM/USIM, pueda utilizar diferentes terminales para acceder a la red.

Respecto a la red de acceso, 3GPP ha especificado tres tipos de redes de acceso diferentes: GERAN (GSM/EDGE Radio Access Network), UTRAN (UMTS Terrestrial Radio Access Network) y E-UTRAN Evolved UTRAN).

Las redes de acceso GERAN y UTRAN forman parte del sistema 3G UMTS mientras que E-UTRAN es la nueva red de acceso del sistema LTE.

Cada red de acceso define su propia interfaz radio para la comunicación con los equipos de usuario: GERAN, también denominada de forma habitual simplemente como GSM, utiliza un acceso basado en TDMA (Time Division Multiple Access), la tecnología utilizada en UTRAN es WCDMA (Wideband Code Division Multiple Access) y, E-UTRAN ha apostado por la tecnología OFDMA (Orthogonal Frecuency-Division Multiple Access).

Asimismo, la interconexión de las redes de acceso a la red troncal se realiza mediante interfaces AN-CN específicas a cada una de ellas.

OFDMA

El sistema de acceso múltiple por división ortogonal de frecuencias aplica los mismos principios que OFDM para conseguir que diversos usuarios hagan uso simultáneo de una banda de frecuencias manteniendo plena ortogonalidad entre sus respectivas señales.

Para ello, cada usuario utiliza un conjunto diferente de subportadoras, que pueden ser contiguas o no.

Para obtener todas las ventajas de OFDMA es vital que sea la estación base quien gestione los recursos radio, en lugar del Radio Network Controller (RNC), como ocurre en Universal Mobile Telecommunications System (UMTS).

Por este motivo, en LTE todos los protocolos radio del plano de usuario acaban en el evolved Node B (eNodeB).

ESPECIFICACIONES LTE

LTE es una tecnología definida como un nuevo concepto de arquitectura evolutiva hacia la 4G, como la actualización de la precedente tecnología UMTS.

LTE no es un estándar definido, se entiende como una nueva tecnología capaz de integrar lo mejor de GSM, GPRS, UMTS y HSPA (High-Speed Packet Access),

Presenta dentro de sus principales premisas proveer una alta tasa de tráfico y baja latencia.

La interfaz y la arquitectura de radio del sistema LTE completamente nueva, propone la prestación de servicios mediante la técnica de conmutación de paquetes IP, soportando además la movilidad de estos.

El sistema presenta flexibilidad ante el uso del espectro, dado sus dos posibles sistemas de transmisión de doble cara, FDD y TDD, posee tecnologías de acceso de radio OFDMA para el DL (Downlink) y SC-FDMA (Single Carrier Frequency Division Multiple Access) para el UL (Up link) y una tecnología de aprovechamiento de la diversidad espacial MIMO (Multiple Input Multiple Output)

LTE trabaja en un rango de bandas de frecuencias que comprenden entre los 800 MHz y 3.5 GHz.

Posee también diferentes anchos de bandas, regulados en los 1.4, 3, 5, 10, 15 y 20 MHz.

El radio de la célula LTE alcanza los 5 Km y puede contener más de 200 usuarios para 5 MHz de ancho de banda y más de 400 para 20 MHz de ancho de banda.

Los componentes fundamentales del sistema LTE son, por un lado, la nueva red de acceso E-UTRAN y el nuevo dominio de paquetes EPC de la red troncal y por otro, la evolución del subsistema IMS concebido inicialmente en el contexto de los sistemas UMTS.

La red de acceso E-UTRAN y la red troncal EPC proporcionan de forma conjunta servicios de transferencia de paquetes IP entre los equipos de usuario y redes de paquetes externas tales como plataformas IMS u otras redes de telecomunicaciones como Internet

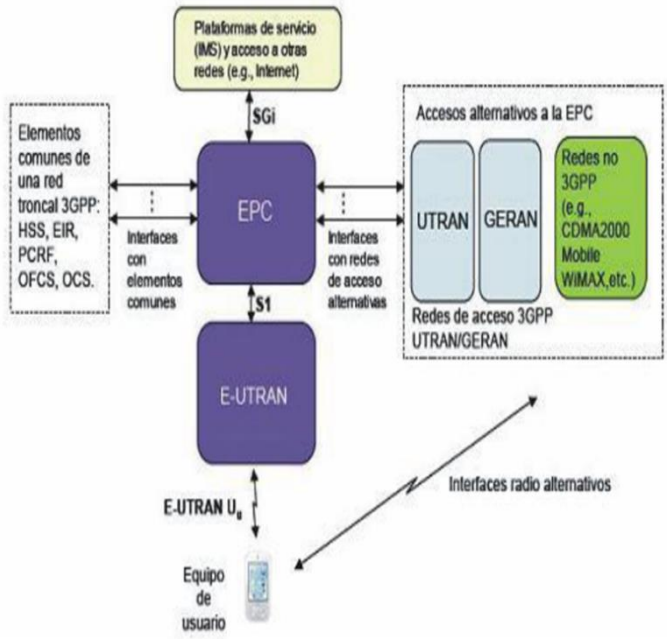
El servicio de transferencia de paquetes IP ofrecido por la red LTE entre el equipo de usuario y una red externa se denomina servicio portador EPS (EPS Bearer Service).

Asimismo, la parte del servicio de transferencia de paquetes que proporciona la red de acceso E-UTRAN se denomina E- RAB (E-UTRAN Radio Access Bearer).

La interfaz entre E-UTRAN y EPC se denomina S1 y proporciona a la EPC los mecanismos necesarios para gestionar el acceso de los terminales móviles a través de E-UTRAN.

La interfaz radio entre los equipos de usuario y E-UTRAN se denomina E-UTRAN U.

Por otro lado, las plataformas de servicios como IMS y la conexión a redes de paquetes externas IP se llevan a cabo mediante la interfaz SGi de la EPC.



La interfaz SGi es análoga a la interfaz Gi definida en las redes GPRS/UMTS y constituye el punto de entrada/salida al servicio de conectividad IP proporcionado por la red LTE

Los mecanismos de control de los servicios de transporte ofrecidos por EPC se sustentan en información proporcionada por otros elementos de la red troncal que no son exclusivos del sistema LTE sino que pueden dar soporte también a otros dominios de los sistemas 3GPP

Otra característica fundamental del sistema LTE es que contempla también el acceso a sus servicios a través de UTRAN y GERAN así como mediante la utilización de otras redes de acceso que no pertenecen a la familia 3GPP (CDMA2000, Mobile WiMAX, redes 802.11, etc.).

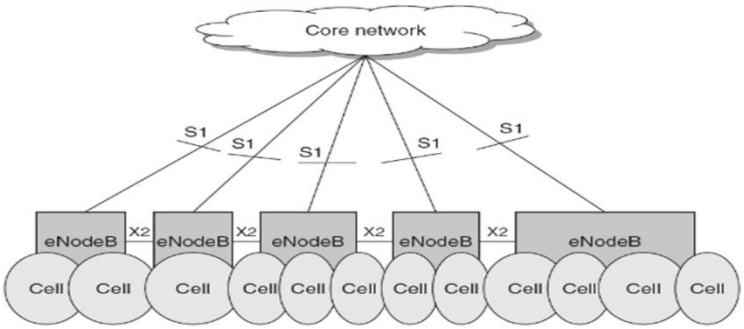
Finalmente, aunque no está reflejado en la figura anterior, es importante destacar que la interconexión de los diferentes equipos físicos donde se ubicarían las funciones tanto de la red troncal EPC como de la red de acceso E-UTRAN, se realiza mediante tecnologías de red basadas en IP.

De esta forma, la red física que se utiliza para interconectar los diferentes equipos de una red LTE, y que se denomina comúnmente como red de transporte, es una red IP convencional.

Por tanto, la infraestructura de una red LTE, además de los equipos propios que implementan las funciones del estándar 3GPP, también integra otros elementos de red propios de las redes IP tales como routers, servidores DHCP (Dynamic Host Configuration Protocol) para la configuración automática de las direcciones IP de los equipos de la red LTE y servidores DNS (Domain Name Server) para asociar los nombres de los equipos con sus direcciones IP.

RED DE ACCESO EVLUCIONADA. E-UTRAN

La red de acceso radio LTE está formada por un solo tipo de nodos: la estación base o "e-Nodo B" (e-Node B).



Como se muestra en la figura, una red de acceso E-UTRAN está formada por eNBs que los proporcionan la conectividad entre los equipos de usuario y la red troncal EPC.

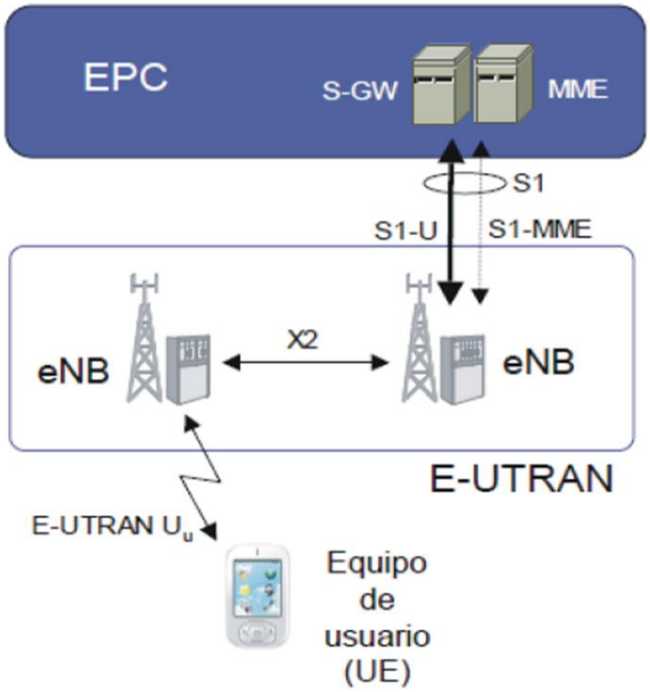
Un eNB se comunica con el resto de elementos del sistema mediante tres interfaces: E-UTRAN Uu , S1 y X2.

La interfaz E-UTRAN Uu, también denominada LTE Uu o simplemente interfaz radio LTE, permite la transferencia de información por el canal radio entre el eNB y los equipos de usuario.

Todas las funciones y protocolos necesarios para realizar el envío de datos y controlar la operación de la interfaz E-UTRAN Uu se implementan en el eNB.

El eNB se conecta a la red troncal EPC a través de la interfaz S1.

Dicha interfaz está desdoblada en realidad en dos interfaces diferentes: S1-MME para sustentar el plano de control y S1-U como soporte del plano de usuario.



Así, el plano de usuario de una interfaz se refiere a la torre de protocolos empleada para el envío de tráfico de usuario a través de dicha interfaz (paquetes IP del usuario que se envían entre E-UTRAN y EPC a través de S1-U).

Por otro lado, el plano de control se refiere a la torre de protocolos necesaria para sustentar las funciones y procedimientos necesarios para gestionar la operación de dicha interfaz o de la entidad correspondiente.

Esta separación entre plano de control y plano de usuario en la interfaz S1 permite realizar la conexión del eNB con dos nodos diferentes de la red troncal. Así, mediante la interfaz S1-MME, el eNB se comunica con una entidad de red de la EPC encargada únicamente de sustentar las funciones relacionadas con el plano de control (dicha entidad de red de la red troncal EPC se denomina MME (Mobility Management Entity).

Por otra parte, mediante la interfaz S1-U, el eNB se comunica con otra entidad de red encargada de procesar el plano de usuario (dicha entidad de red de la EPC se denomina S-GW (Serving Gateway)).

EVOLVED NODEB (ENB)

El eNB integra todas las funciones de la red de acceso. Por ello, en el eNB terminan todos los protocolos específicos de la interfaz radio.

Mediante dichos protocolos, el eNB realiza la transmisión de los paquetes IP hacia y desde los equipos de usuario junto con los mensajes de señalización necesarios para controlar la operación de la interfaz radio.

El servicio de transferencia de paquetes IP entre un eNB y un equipo de usuario se denomina formalmente como servicio portador radio RB (Radio Bearer).

El eNB mantiene un contexto de cada uno de los equipos de usuario que tiene (información sobre el estado del equipo de usuario, servicios portadores activos, información de seguridad, capacidades del terminal, etc.).

Sin duda, la funcionalidad clave de un eNB consiste en la gestión de los recursos radio.

Así, el eNB alberga funciones de control de admisión de los servicios portadores radio, control de movilidad (Por ejemplo, decisión de realizar un handover), asignación dinámica de los recursos radio tanto en el enlace ascendente como descendente (denominadas funciones de scheduling), control de interferencias entre estaciones base, control

de la realización y del envío de medidas desde los equipos de usuario que puedan ser útiles en la gestión de recursos, etcétera.

Otra función importante introducida en la funcionalidad de un eNB es la selección dinámica de la entidad MME de la red troncal EPC cuando un terminal se registra en la red LTE.

Esta función otorga un grado de flexibilidad muy importante en la operatividad de la red

Al igual que la posibilidad de interactuar con múltiples MMEs, un eNB puede enviar y recibir paquetes IP de los usuarios a los que sirve a través de diferentes pasarelas S-GW de la red troncal EPC.

Ello conlleva que el eNB albergue funciones de encaminamiento del tráfico de los usuarios hacia la pasarela de red S-GW correspondiente.

La elección de S-GW en este caso compete a la entidad MME y no al eNB

Un eNB puede gestionar una o varias celdas.

SISTEMAS WIMAX

WiMAX (Worldwide Interoperability for Microwave Access) es un estándar de comunicación radio de última generación, promovido por el IEEE y especialmente diseñado para proveer accesos vía radio de alta capacidad a distancias inferiores a 50 kilómetros y con tasas de transmisión de hasta 70 Mbps.

Las soluciones WiMAX se pueden aplicar en multitud de escenarios (enlaces punto a punto, redes metropolitanas, cobertura de hot-spots Wi-Fi, redes empresariales, backbones, etc.) con altas garantías de disponibilidad y estabilidad.

¿Cuál es su propósito?

Permite el rápido despliegue mundial de productos BWA (acceso inalámbrico de banda ancha) Multi-Proveedores innovadores, Rentables e Ínter operables.

Reemplazar o competir directamente con el Internet por cable y el ADSL.

Facilita la competencia en el acceso a Banda Ancha proveyendo alternativas para BWA Wireline.

Impulsa la asignación del espectro radioeléctrico y acelera la comercialización de los sistemas de BWA.

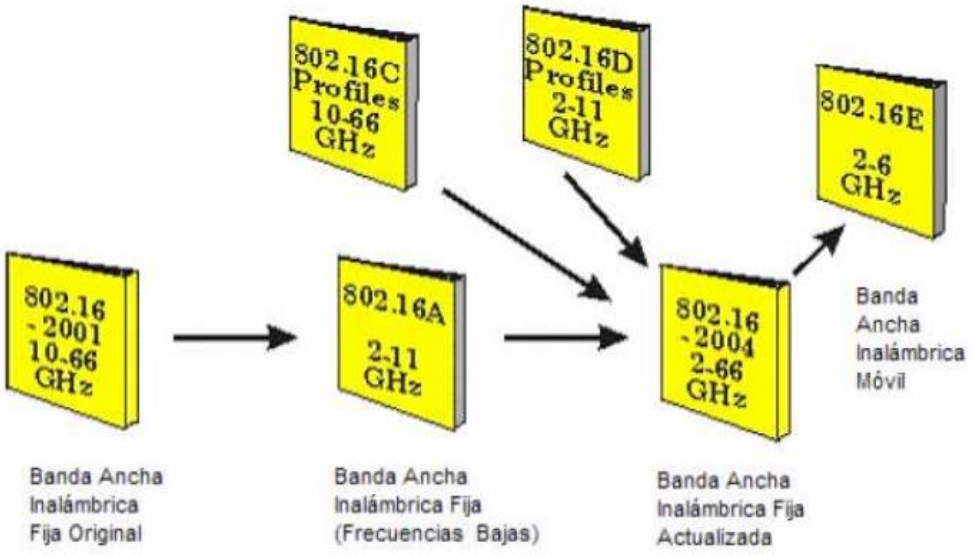
ESTANDARES.

Integra la familia de estándares IEEE 802.16 y el estándar HyperMAN del organismo de estandarización europeo ETSI.

El estándar inicial 802.16 se encontraba en la banda de frecuencias de 10-66 GHz y requería torres LOS.

La nueva versión 802.16a, ratificada en marzo de 2003, utiliza una banda del espectro más estrecha y baja, de 2-11 GHz, facilitando su regulación.

Además, como ventaja añadida, no requiere de torres donde exista enlaces del tipo LOS sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras/receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicio a edificios completos.



EVOLUCION.

Estándar	Descripción
802.16	Utiliza espectro licenciado en el rango de 10 a 66 GHz, necesita línea de visión directa, con una capacidad de hasta 134 Mbps en celdas de 2 a 5 millas. Soporta calidad de servicio. Publicado en 2002.
802.16a	Ampliación del estándar 802.16 hacia bandas de 2 a 11 GHz, con sistemas NLOS y LOS, y protocolo PTP y PTMP. Publicado en abril de 2003
802.16c	Ampliación del estándar 802.16 para definir las características y especificaciones en la banda d 10-66 GHz. Publicado en enero de 2003
802.16d	Revisión del 802.16 y 802.16a para añadir los perfiles aprobados por el WiMAX Forum. Aprobado como 802.16-2004 en junio de 2004 (La última versión del estándar)
802.16e	Extensión del 802.16 que incluye la conexión de banda ancha nómada para elementos portables del estilo a notebooks. Publicado en diciembre de 2005

PRINCIPALES CARACTERÍSTICAS DE WIMAX.

- Posee un gran ancho de banda

  Una sola estación de base puede admitir de manera simultánea más de 60 enlaces con conectividad tipo T1/E1 o cientos de conexiones tipo DSL.

- Es independiente de protocolo.
- Es decir, puede transportar IP, Ethernet, ATM y otros. Eso hace que sea compatible con otros estándares como Wi-Fi, Ethernet, o Token Ring.
- Puede transmitir otros servicios agregados como VoIP, datos o vídeos.
- Soporta las llamadas antenas inteligentes (smart antenas), propias de las redes de telefonía de tercera generación (3G), lo cual mejora la eficiencia espectral.
- Estas antenas emiten un haz muy estrecho que se puede ir moviendo, electrónicamente, para enfocar siempre al receptor, con lo que se evitan las interferencias entre canales adyacentes y se consume menos potencia al ser un haz más concentrado.

- Velocidad: En circunstancias ideales y sin obstáculos que interfieran en los enlaces establecidos, la conexión puede alcanzar una distancia cercana a los 50 kilómetros y la

velocidad de transferencia de los datos puede llegar a los 70 Mbps.

- Seguridad: incluye medidas para la autenticación de usuarios y la encriptación de los datos mediante los algoritmos Triple DES (128 bits) y RSA (1.024 bits).
- Como principales inconvenientes cabe mencionar la limitación de potencia para prever interferencias con otros sistemas, y el alto consumo de batería que se requiere.
- Sin embargo, los más recientes avances en los procesadores digitales de señal hacen que señales muy débiles puedan ser interpretadas sin errores, un hecho del que se aprovecha WiMAX.

¿COMO FUNCIONA?

servicios

- Acceso a Internet de Alta Velocidad.
- Voz (VoIP).
- Transmisión de Datos (VPN IP, Linea Dedicada).
- Conectividad a Internet para redes Wifi / GSM / GPRS / UMTS

prestaciones

- Soporta diferentes niveles de servicio para usuarios particulares y empresas.
- Posibilidad de aumentar el ancho de banda o las prestaciones en función del aumento de las necesidades de los usuarios.
- Precio de servicios similares a ADSL/cable pero con prestaciones superiores:
  - simetrica o asimetrica,
  - mayor ancho de banda,
  - calidades de servicio con velocidades garantizadas,
  - control remoto para la resolución de incidencias.

prestaciones

- Gran ancho de banda: hasta 70 Mbps por usuario y hasta 420 Mbps por estación base.
- Rápido despliegue (hasta 50 km de cobertura).
- Fácil instalación (se puede ejecutar en plazo de 2 horas).
- La prestación de servicios WiMAX en frecuencias de uso exclusivo permite garantizar calidades de servicio (carrier class).
- Alta eficiencia en el uso del espectro y estabilidad.
- Permite la transmisión simultánea de voz, datos y video.

WiMax funcionaría similar a WiFi pero a velocidades más altas, mayores distancias y para un mayor número de usuarios.

WiMax podría solventar la carencia de acceso de banda ancha a las áreas suburbanas y rurales que las compañías del teléfono y cable todavía no ofrecen.

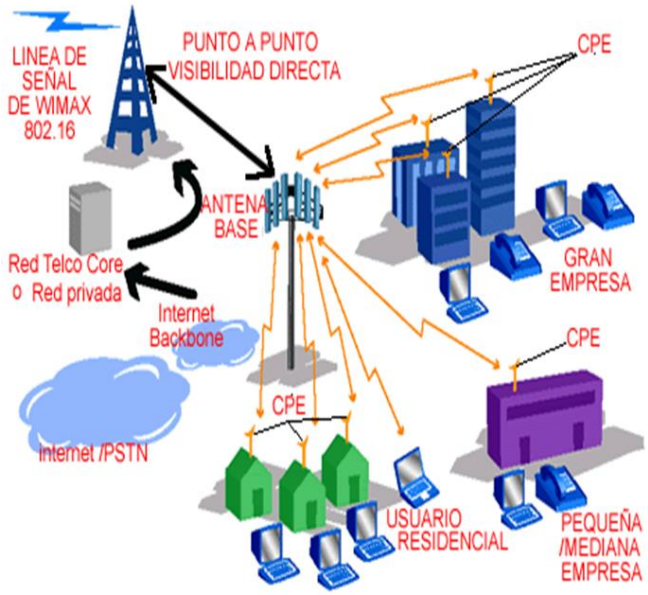
Por un lado están las torres WiMax, que dan cobertura de hasta 8.000 kilómetros cuadrados según el tipo de señal transmitida.

Por otro están los receptores, es decir, las tarjetas que conectamos a nuestro PC, portátil, PDA y demás para tener acceso.

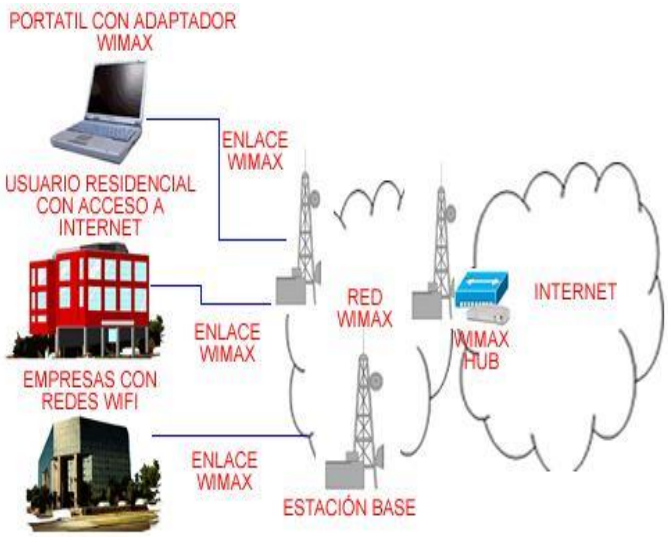
Al principio WiMAX ofrecerá limitados anchos de banda y sin movilidad en exteriores, con un punto de visibilidad directa.

Se necesitará la instalación del equipo en cada domicilio para poder utilizarlo.

Se empezará contando tan solo con las mismas prestaciones que un acceso básico a internet.



La segunda generación de WiMAX será para interiores, con módems auto instalables similares a los de xDSL. A partir de ese momento WiMAX ofrecerá movilidad a los usuarios para que puedan desplazarse sin perder la conexión



RADIO PLANNING 802.16E.

Capa física de WiMAX.

Como ya se mencionó anteriormente, la capa física de WiMAX está basada en OFDM este es un esquema de transmisión, que permite la transferencia de datos, video y multimedia a alta velocidad y es utilizada en varios sistemas de banda ancha como lo son DSL, Wi-Fi, etc.

Es un esquema eficiente para la transmisión de tasas de datos muy altas en un ambiente NLOS o un radio de múltiples trayectorias.

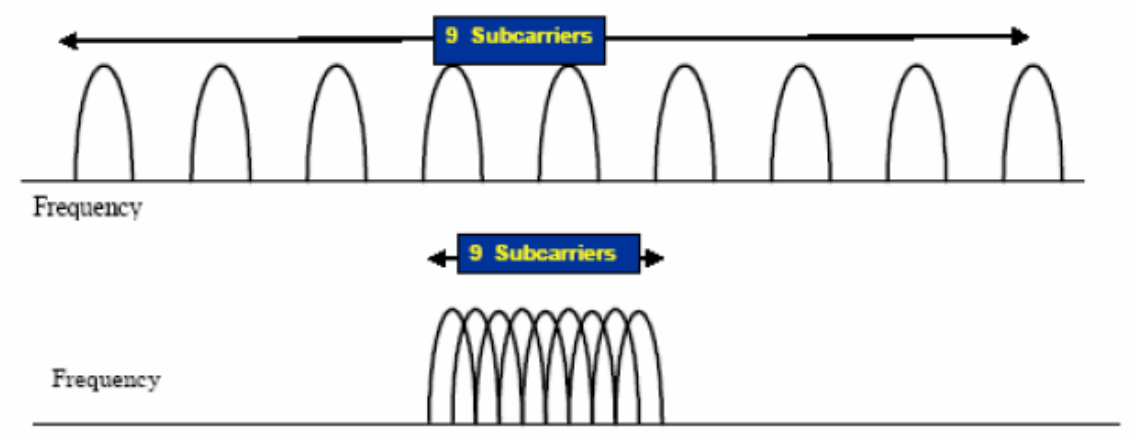
BASES DE OFDM.

OFDM es parte de lo que se conoce como muílticarrier modulation, que está basada en la idea de dividir una secuencia de una alta tasa de transmisión de bits en varias secuencias paralelas de baja transmisión de bits y modular cada secuencia en diferentes portadoras.

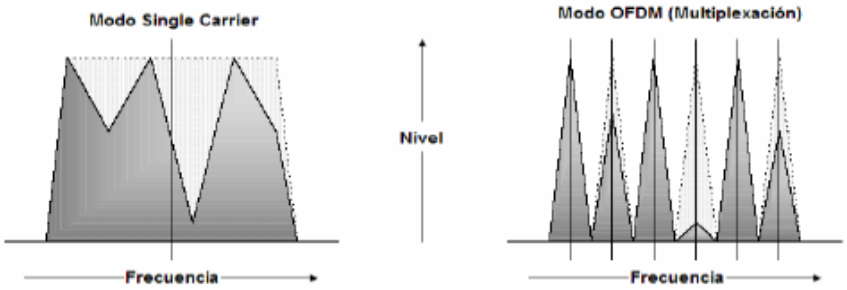
Este esquema permite reducir o eliminar la interferencia entre símbolos (ISI) al hacer el tiempo de símbolo lo suficientemente grande para que los retrasos inducidos en el canal sean una fracción insignificante de la duración del símbolo.

Técnica de transmisión multiportadora OFDM (Orthogonal Frecuency Division Multiplexing).

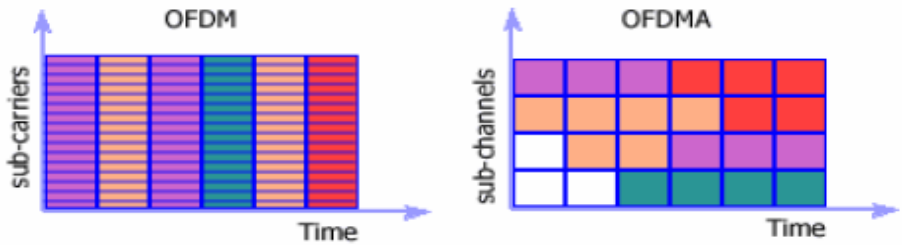
Divide el ancho de banda disponible en diferentes subportadoras de banda estrecha (FDM).



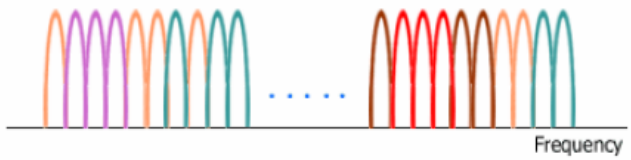
- POR QUE ES IMPORTANTE ESTE DESARROLLO?
  - Solucion



- **OFDMA Acceso de múltiples usuarios (FDMA optimizado)**



Subcanalización



Mejora SOFDMA

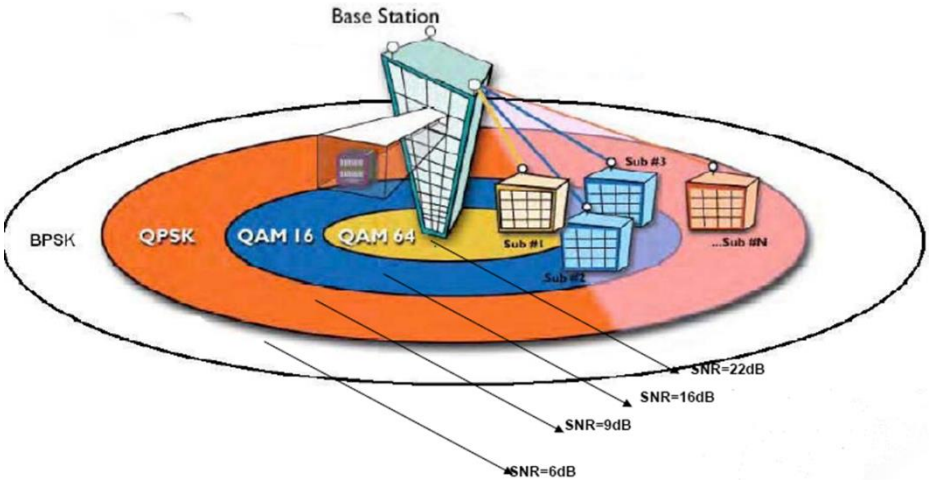
Subportadoras con el mismo color representan un subcanal

COMPATIBILIDAD ENTRE 802.16-2004 Y 802.16E.

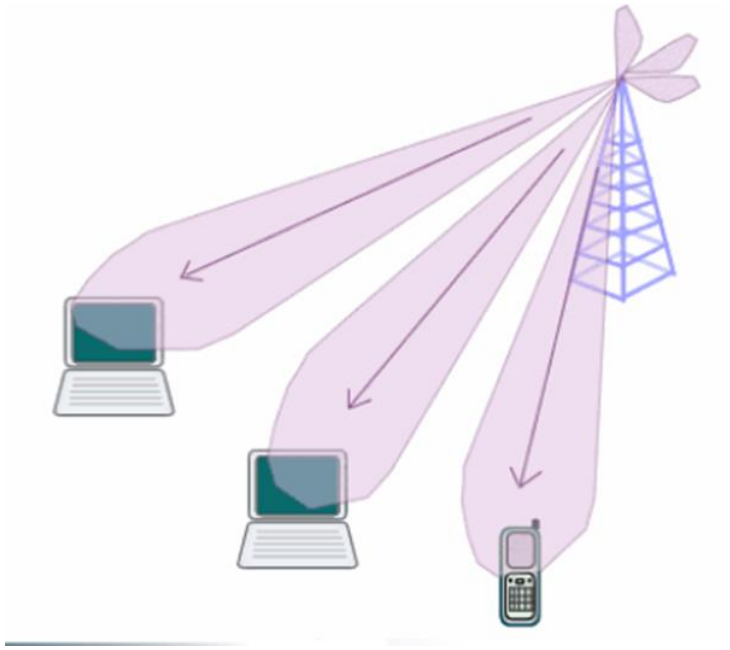
Estas versiones no son compatibles, básicamente, por la tecnología de acceso. En 802.16e el acceso se hace al mismo tiempo en conjuntos de subportadoras diferentes, mientras que en 802.16-2004 el acceso se hace en diferentes tiempos a todas las subportadoras.

LINK ADAPTATION: MODULACIÓN Y CODIFICACIÓN ADAPTATIVA.

Adecúa parámetros del protocolo a las condiciones en el enlace.



La técnica consiste en ajustar el ángulo y ancho del lóbulo de la antena dependiendo donde este el tráfico.



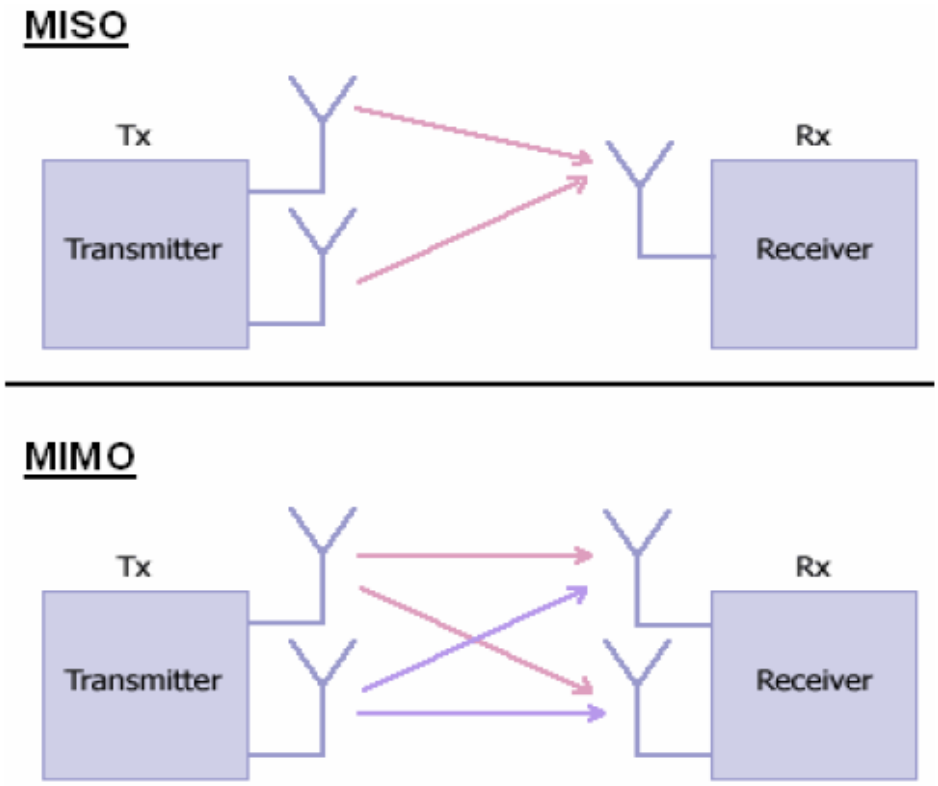
MISO – MIMO.

Utilizar no una sino varias antenas en el lado Tx ó Rx para aplicar la técnica de diversidad de ruta, mejorando las características del enlace de radio.

La tecnología de MIMO ha atraído la atención en comunicaciones sin hilos, porque ofrece aumentos significativos en rendimiento de procesamiento de datos y gama del acoplamiento sin anchura de banda adicional o transmite energía.

Alcanza esto por una eficacia espectral más alta (más pedacitos por segundo por hertzios de la anchura de banda) y confiabilidad o diversidad (el descolorarse reducido) del acoplamiento.

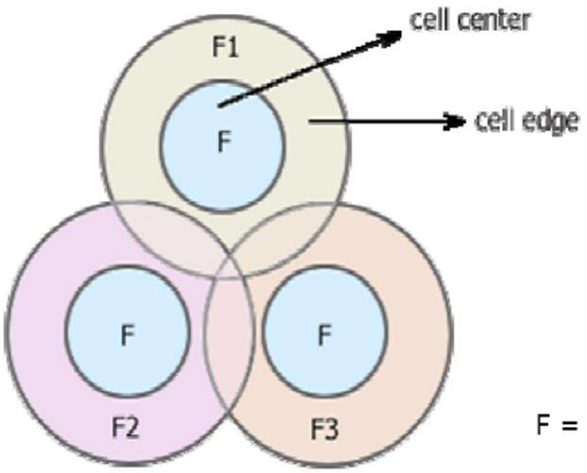
Debido a estas características, MIMO es una parte importante de estándares sin hilos modernos de la comunicación como la evolución a largo plazo 802.11n (Wifi), 3GPP de IEEE, WiMAX y HSPA+.



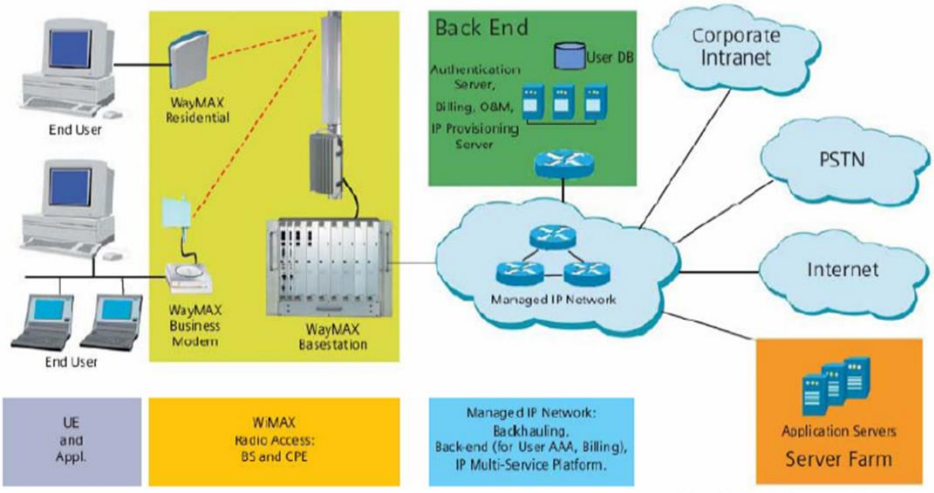
REUSO FRACCIONAL DE FRECUENCIAS.

Los usuarios que estén en el centro de la celda tienen disponibles todos los subcanales, pero los que estén en los bordes solo pueden operar una fracción de todos los subcanales disponibles.

- F = F1+F2+F3



ARQUITECTURA DE UNA RED 802.16e



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).

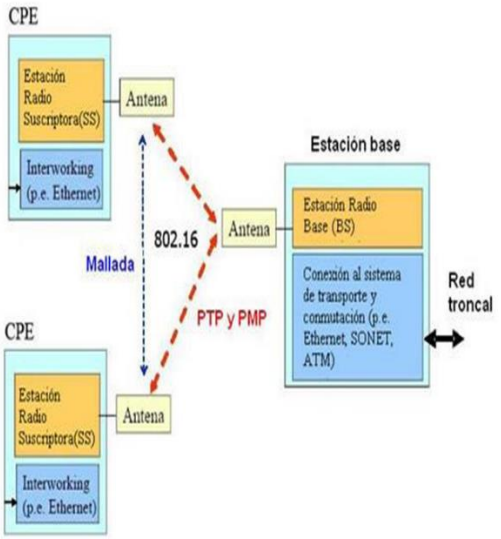
  Además de proporcionar conectividad con las SS también proporciona los mecanismos de control y gestión de los equipos SS. La estación base tiene los elementos necesarios para conectarse con el sistema de distribución.

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.



TIPOS DE TOPOLOGÍA DE RED PARA WIMAX.

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 puede 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 es 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.

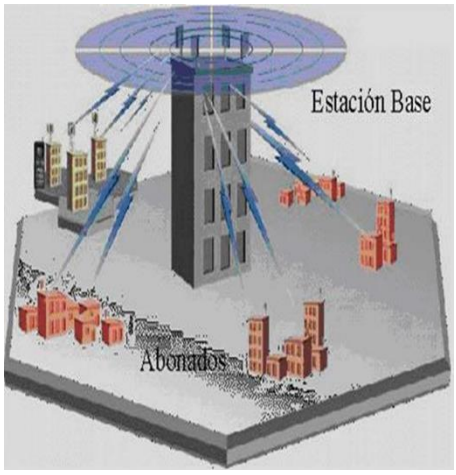
En síntesis, existe una Estación Base que controla la red, donde:

- 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.

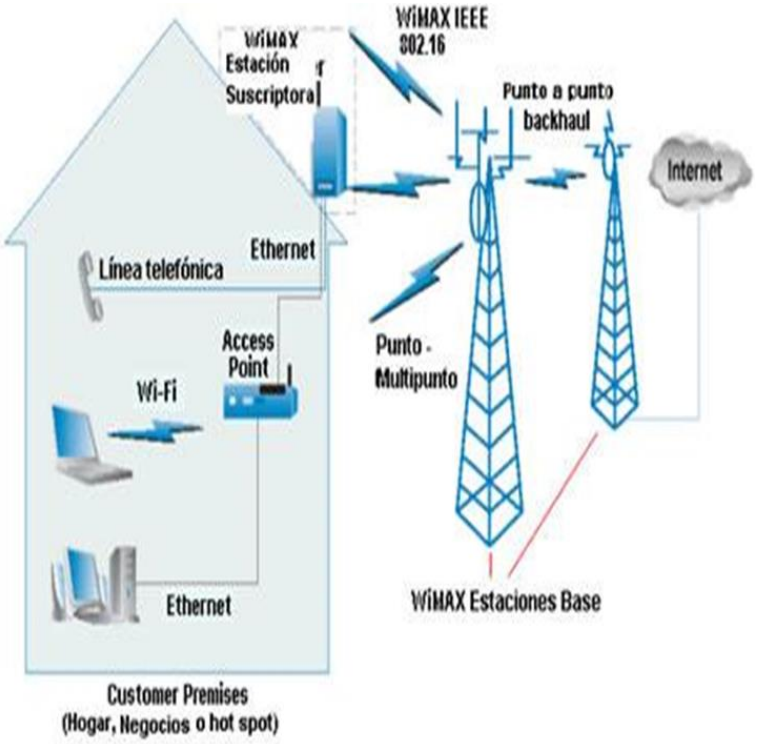
El flujo de servicio define los parámetros de QoS de los packet data units (PDU) que se intercambian durante la conexión.



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.



REDES ENMALLADAS (MESH).

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.

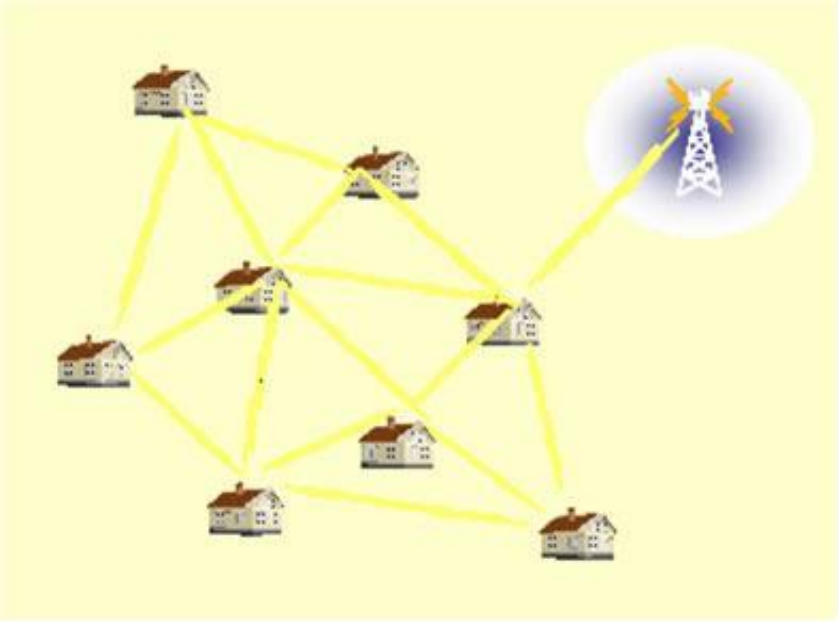
Para este tipo de redes, se pueden realizar las operaciones de dos maneras diferentes: distribuida ó centralizada: para la distribuida, todos los nodos deben coordinar con los demás la manera de transmitir para evitar colisiones con los datos y realizar el control de tráfico, y además deben enviar por 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 CONEXION POR WIMAX.

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 portatil 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)

GIGASET SE461 WIMAX

- Conexión de la mini-antena
- Conexión adaptadora de energía
- Conexión de Red
- RSI: Intensidad de la señal
- DATA: Transmisión de datos
- LINK: Cable de red conectado
- STATUS: Estado
- POWER: Indicador de Energía

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.

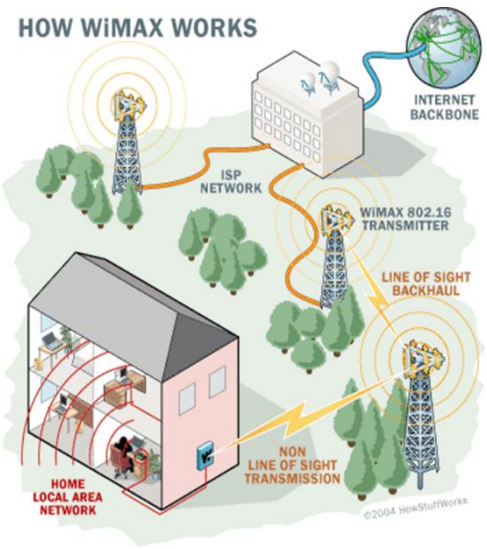
En el otro extremo de la conexión, esta el usuario final, que puede ser residencial o corporativo, se encuentra instalado el CPE (Customer Premises Equipament, Equipo Local de Cliente), que constituye el último eslabón de este tipo de redes y en donde acaba el flujo de transferencia de datos entre operador y el cliente final.

En una Torre o Estación Base, pueden coincidir distintos tipos de antenas, con las que atender distintas necesidades y oferta de servicio para abonados.

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 sean 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.

REUTILIZACIÓN DE FRECUENCIAS.

Existen además otras técnicas para optimizar la reutilización de frecuencias en redes WIMaX, las principales se describen a continuación:

- Minimización de múltiples caminos y cruce de polarización
- Maximización de la direccionalidad de las antenas de las celdas a través de la sectorización del sistema de distribución
- Maximización del aislamiento entre sectores adyacentes a través de la polarización

- Minimización de múltiples caminos y cruce de polarización:
    - utilizando antenas altamente direccionales y posicionándolas a grandes alturas.

- Maximización de la direccionalidad de las antenas de las celdas a través de la sectorización del sistema de distribución:
    - El equipo montado en la celda se configura con múltiples sectores, antenas, transmisores y receptores.
    - Una configuración típica es una celda con cuatro sectores, utilizando antenas de 90 grados de amplitud de rayo.
    - Cada una de estas antenas sectorizadas puede soportar el ancho de banda total del espectro reservado.

- Maximización del aislamiento entre sectores adyacentes a través de la polarización:
    - Para esto se utiliza la polarización horizontal (H) y vertical (V) que pueden ser empleadas a lo largo del sistema a través de un patrón alternado entre los sectores.

SECTORIZACION.

La sectorización consiste en dividir el patrón de transmisión de una estación base.

Para ello, en lugar de utilizar una radiación de 360 grados (omnidireccional) se usan antenas direccionales con cobertura fraccionaria, de modo que múltiples antenas completan el patrón de radiación de 360 grados.

La sectorización puede llevarse a cabo con una amplitud de 15 y hasta 90 grados por sector, con lo que la celda o estación base se divide en 4 y hasta 24 sectores.

USO DE POLARIZACIÓN CRUZADA.

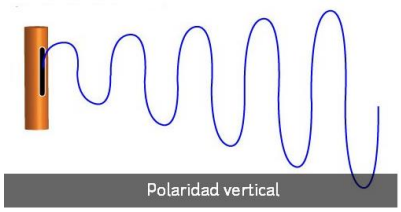
La polarización cruzada es otro de los métodos que pueden aplicar para lograr una reutilización efectiva de las frecuencias.

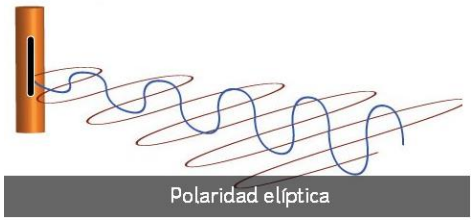
Este método se utiliza en una sectorización basada en polarizaciones ortogonales (horizontal y vertical) de las señales

Las señales radioeléctricas pueden polarizarse, es decir, responder a señales cuyo campo eléctrico se expande con un frente horizontal o bien con un frente vertical.

En sistemas de antenas ideales, una señal emitida con una determinada polarización no será captada por una antena receptora con la polarización cruzada, aunque trabajen en la misma frecuencia.

Bajo un esquema de este tipo, se podrían utilizar por ejemplo cuatro sectores de 90 grados cada uno, de forma tal que cada uno opere con una polarización diferente en forma alternada, es decir, cada uno de los sectores trabaja en la misma frecuencia, pero con polarizaciones alternadas.





En este esquema podríamos ver las celdas como cuadrados y el plan es tal que dos celdas vecinas presentan siempre polarizaciones cruzadas evitando así las interferencias entre una y otra.

Además, en un diseño más cuidadoso del sistema, existe otro factor a considerar para un buen funcionamiento de un sistema con sectores polarizados.

Este factor es la lluvia, que además de los efectos ya mencionados, también provoca la despolarización de las señales.

Por lo tanto, una solución de este tipo no es particularmente adecuada para zonas de grandes precipitaciones pluviales salvo que se acepte una menor disponibilidad de los enlaces o se recurran a otros métodos para mejorar los efectos de este fenómeno.

El esquema de polarización cruzada permite optimizar la reutilización de frecuencias.

Fin de la clase
UAI
Universidad Abierta
Interamericana

REDES ADMINISTRATIVAS

UNIDAD 7: REDES DE PROXIMA GENERACION

CLASE 13 VOIP H.323 SIP

Claudio Milio 2020

Bienvenidos a la clase 13 donde veremos las diferentes tecnologías sobre las redes NGN.

INTRODUCCION A LAS REDES NGN

Primero… ¿qué es convergencia?

Es la posibilidad de un usuario de poder acceder a una amplia variedad de servicios de comunicaciones:

- Con calidad consistente.
- Independiente de su ubicación geográfica y del equipo Terminal utilizado
- Sobre una sola red integrada de comunicaciones.

Las tendencias de las comunicaciones en el mundo son:

- Convergencia de voz, video y datos en una sola red conmutada en paquetes.
- Predominio del protocolo IP.
- Surgimiento de las Redes de Próxima Generación (NGN).
- Aumento de la velocidad en el Acceso: Servicios de banda ancha.
- Redes de Acceso Móviles de voz y datos.
- Red Óptica Total.

"Las redes de próxima generación (Next Generation Networks NGN) son redes convergentes multiservicios de voz y datos que funcionan en un mercado de múltiples proveedores.

Las NGN requieren una arquitectura que permita la integración perfecta de servicios de telecomunicaciones tanto nuevos como tradicionales entre redes de paquetes de alta velocidad, ínter operando con clientes que poseen capacidades heterogéneas."

Las NGN deberán poder trabajar con nuevos servicios adaptables, pero también es importante preservar los servicios existentes provenientes de las redes anteriores.

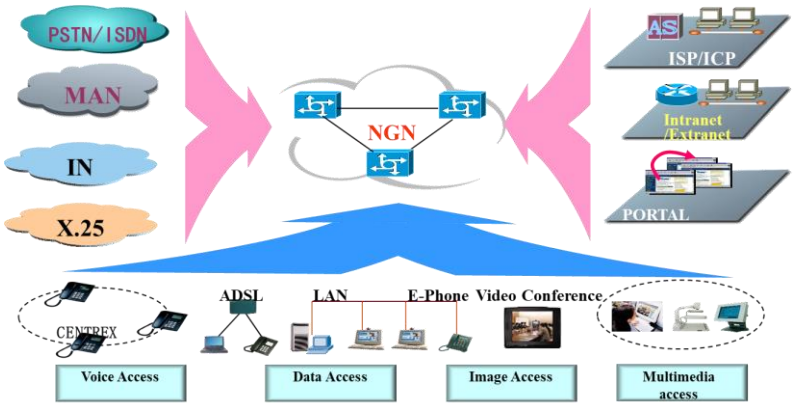


Ilustración 1 Arquitectura convergente de voz y datos

En NGN, las funciones de conmutación y control de la llamada están bien definidas en diferentes capas.

- Servicio y Aplicación
- Control de red
- Transporte (núcleo de conmutación IP con IP/ATM/SDH/WDM o IP/WDM)
- Acceso (Gateways de media para la interconexión con los abonados y con las redes tradicionales como la PSTN)

NGN es una red de conmutación de paquetes basada en el protocolo IP.

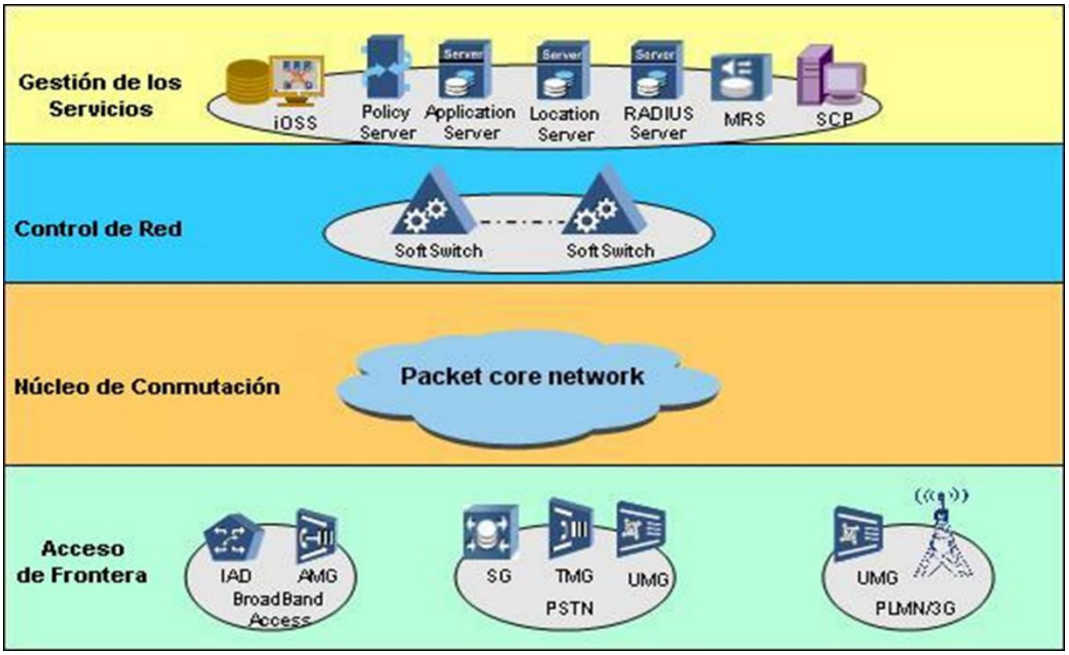
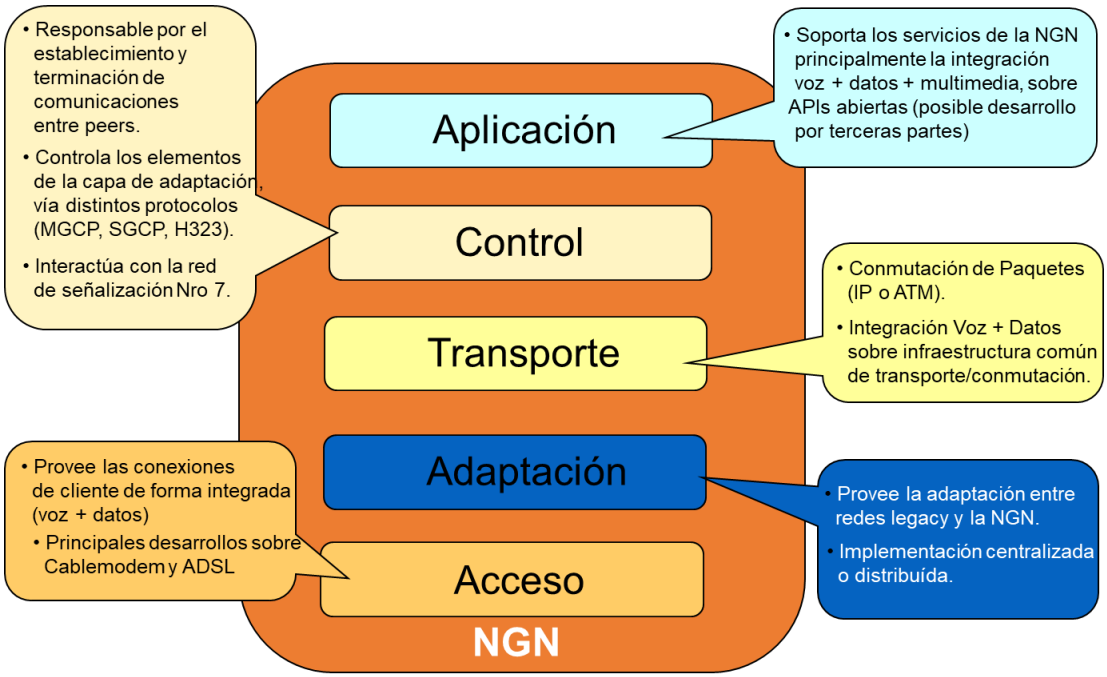


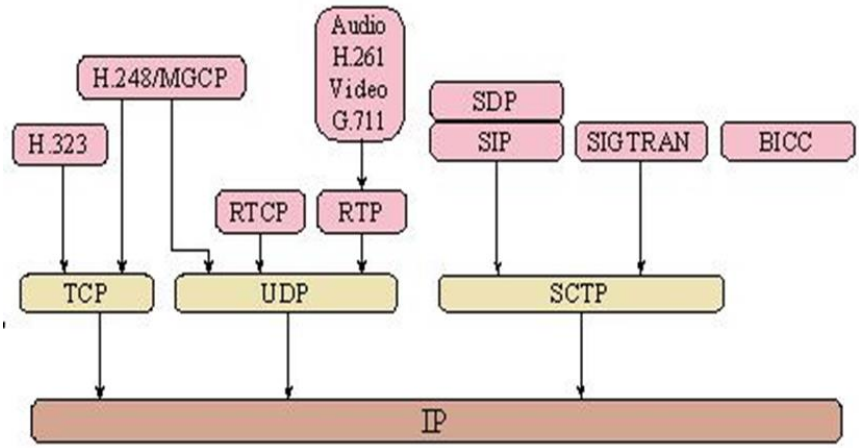
Ilustración 2 modelo en capas

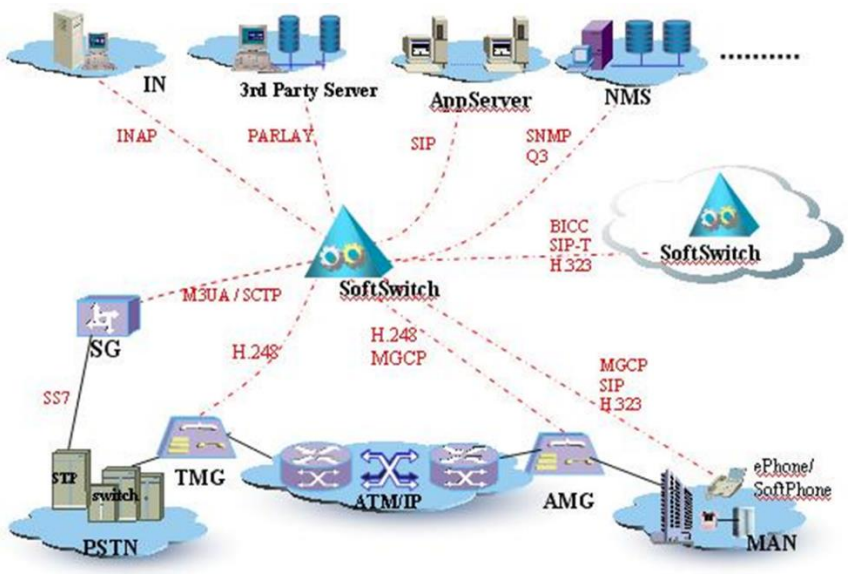


NGN se compone de Sosftswitch, Gateways, dispositivos de acceso como los llamados IAD (Integrated Access Device) , las PABX con GW IP, asi como un núcleo de conmutación y transporte compuesto por Routers IP.

Estas estructuras son menos costosas y más compactas que los conmutadores de la red de voz tradicional.

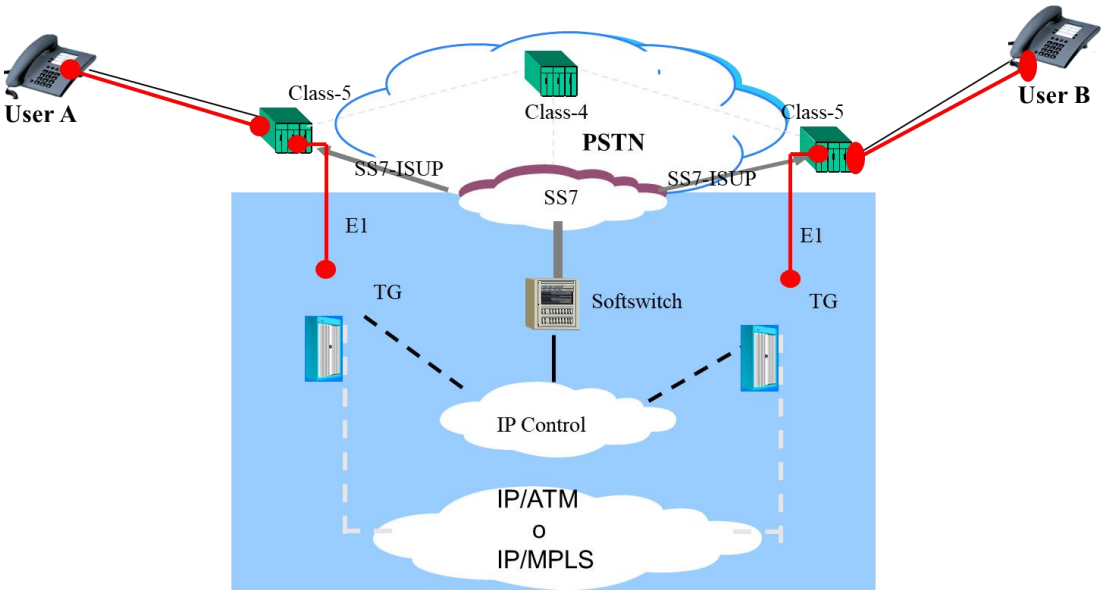
A continuación, mostramos la pila de protocolo NGN y la relación de protocolo por capa





Y alguna de las consecuencias de la aplicación es la sustitución parcial de la PSTN y la sustitución total de la red tradicional.

SOLUCIONES NGN PARA REDES TANDEM Y DE LARGA DISTANCIA.



Como se comentó anteriormente el objetivo es que el usuario de poder acceder a una amplia variedad de servicio de comunicaciones:

- Con calidad consistente.
- Independiente de su ubicación geográfica y del equipo Terminal utilizado
- Sobre una sola red integrada de comunicaciones.

CONVERGENCIA DE TERMINALES.

Equipos para múltiples aplicaciones y diferentes formas de acceso a la red.

CONVERGENCIA DE RED.

Pasaje de una red a otra sin percepción para el usuario y manteniendo la QoS

Ejemplos de os tipos de convergencia:

- Capa Tecnológica: NGN(IP), Redes Multiservicio (Triple Play y Cuádruple Play)
- Capa de Servicios: Servicios genéricos y Prestadores Multiservicio
- Capa Regulatoria: Convergencia Externa (Telecomunicaciones + Radiodifusión + Información)

Triple Play
- Telefonía Fija
- Internet y Datos IP
- IPTV

Cuádruple Play
- Telefonía Fija
- Telefonía Móvil
- Internet y Datos IP
- IPTV + TV Móvil

ARQUITECTURA DE UNA RED NGN.

Las redes NGN tienen una arquitectura funcional debido a que es de servicio general y no depende de la tecnología y se adapta a casos específicos.

Lo que se busca con la definición de la arquitectura es tener elementos independientes para armar cada una de las capas.

Los principios que debe tener en cuenta la arquitectura funcional de las NGN son:

- **Soporte para múltiples tecnologías de acceso:** La flexibilidd de configuración para el soporte de diferentes tecnologías, debe soportar la arquitectura funcional de las NGN.
- **Control distribuido:** Debido a éste, se tolera la transparencia para la computación distribuida, además se adecúan a la naturaleza de procesamientos distribuidos de redes de paquetes.
- **Control abierto:** Debe abrirse para sostener la creación de servicios y la adaptación de configuración lógica de servicios para terceros.
- **Configuración independiente de servicios:** Para generar un entorno competitivo para el desarrollo de las NGN, el cual permite apresurar la prestación de servicios diversificados de NGN, se debe aislar la red de trasporte de la configuración de servicio.
- **Soporte de servicios para redes convergente:** Es importante para los servicios de multimedia, utilizando al máximo las ventajas de la arquitectura funcional fija-móvil, para alcanzar la convergencia de las NGN.
- **Mejoramiento de la seguridad y protección:** Se debe proteger la infraestructura de toda la red manejando dispositivos de seguridad y utilizando las capas de la arquitectura que sean necesarias. Esto es lo que se conoce como el principio básico de la arquitectura abierta.

Las redes NGN poseen una arquitectura funcional, similar al modelo de refencia de interconexión de sistemas abiertos (OSI: Open System Interconnection), elaborado por la ISO (Organización de Estándares Internacionales (ISO por sus siglas en inglés)), el fin de este, es que los dispositivos que hacen parte de la transmisión de datos, los cuales establece la UIT (Unión Internacional de Telecomunicaciones) y así facilitar la interrelación entre los fabricantes de los equipos.

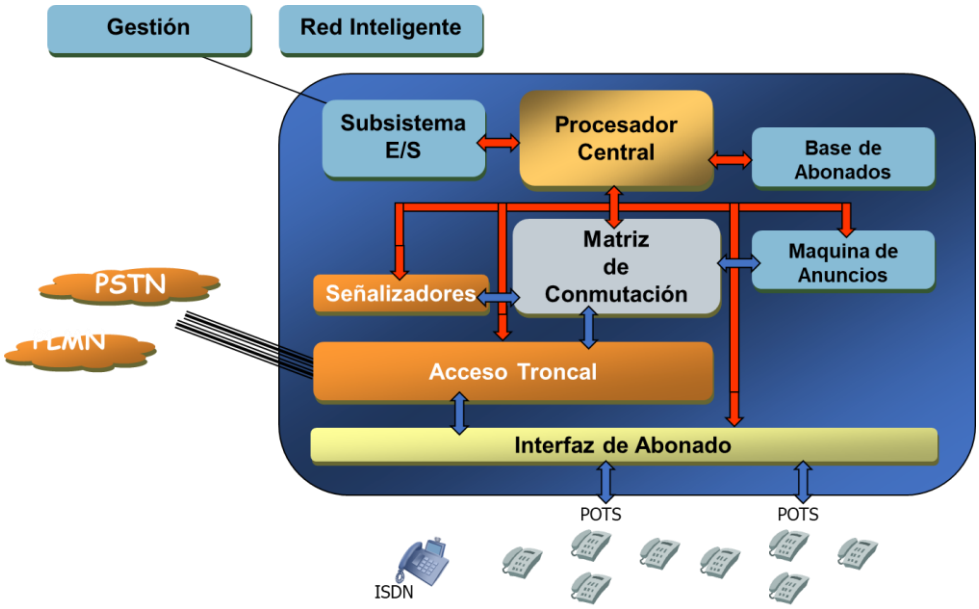
El modelo OSI es importante y está presente en todo sistema de telecomunicaciones al momento de realizar la transmisión de datos.

Aunque los sistemas NGN y OSI poseen una arquitectura basada en capas, existen diferencias como son:

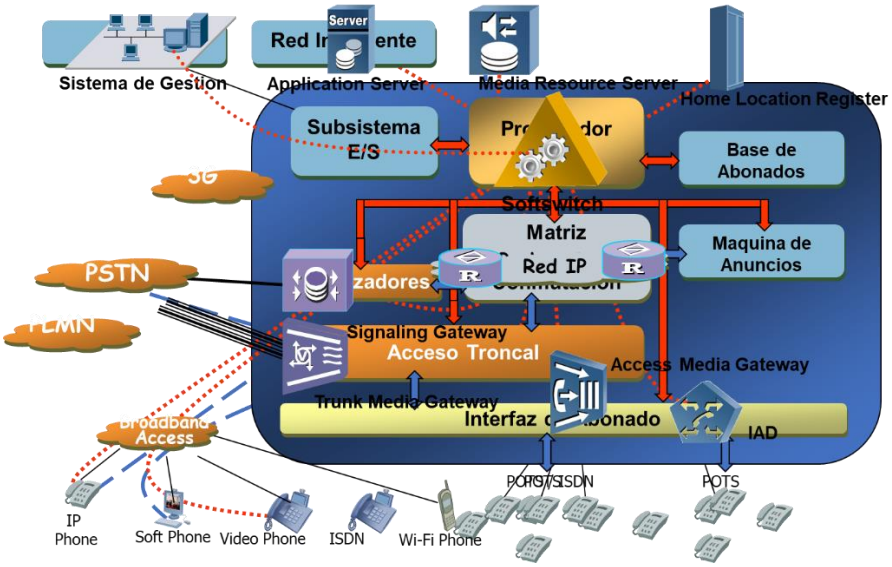
NGN	OSI
Topología de red basada en cinco (5) capas	Modelo de red basado en siete (7) capas
Capas: 1. Acceso 2. Adaptación 3. Transporte 4. Control 5. Servicios de Red o Aplicación	Capas: 1. Nivel Físico 2. Enlace de Datos 3. Red 4. Transporte 5. Sesión 6. Presentación 7. Aplicación
Las funciones y los servicios están distribuidos diferente.	Cada capa precisa características de servicio y funciones muy detallas
Trabaja con protocolo IP	Trabaja con diferentes protocolos, según el nivel

CONVERGENCIA DE TDM A NGN

Ac continuación se muestra el modelo TDM

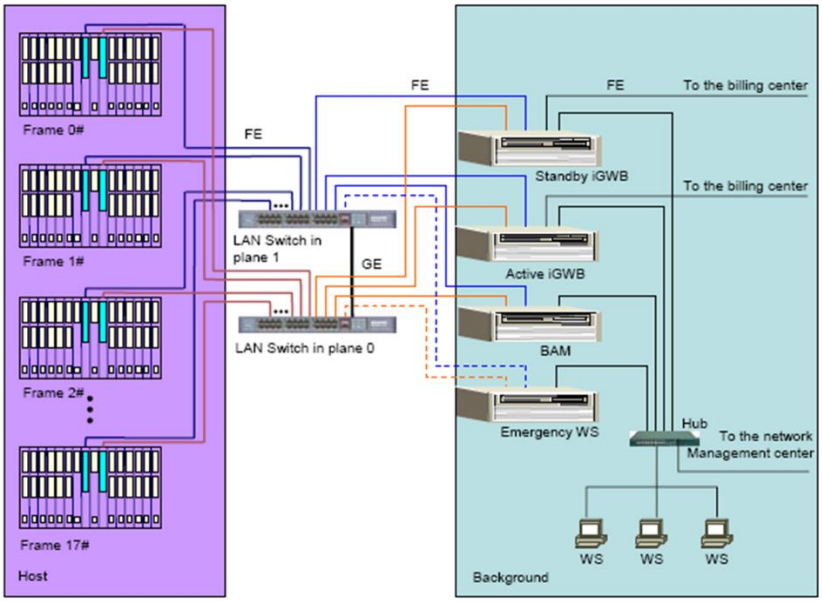


Y EL MODELO NGN y TDM



SOFTSWITCH.

El Softswitch es el principal dispositivo en la capa de control dentro de una arquitectura NGN, encargado de proporcionar el control de llamada, procesamiento de llamadas, y otros servicios, sobre una red de conmutación de paquetes.

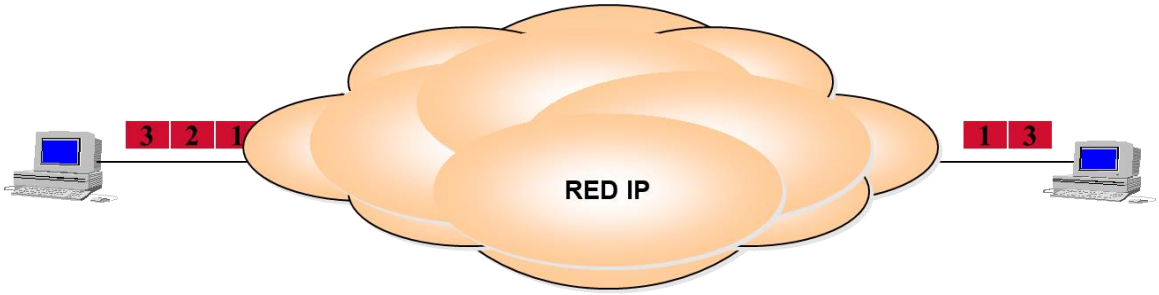


EL TRANSPORTE DE LA VOZ SOBRE REDES IP: LA RED IP.

Es una red de conmutación de paquetes, no orientada a la conexión, donde el camino de cada paquete se resuelve nodo a nodo en base a la dirección destino contenida en cada paquete.

Cada elemento de red "conoce" la topología de la red, por medio del intercambio automático de información entre los routers (protocolos de ruteo).

Cada router mantiene en forma dinámica una tabla que relaciona la interfaz de salida asociada a una red IP destino.



VOIP

IP ha tenido su origen en transmisión de datos y no estaba adaptada a la transmisión de voz e imágenes.

La tecnología de transmisión de paquetes, en la que está basada IP, ofrece tamaño de celdas variable, que en comparación con tecnologías de tamaño de celda fija como ATM, introduce ineficiencias y necesidad de proceso extra.

IP es un protocolo que en principio ofrece un tipo de calidad de servicio (QoS) basado en proporcionar el mejor rendimiento posible en el enlace disponible. (Best Effort)

VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS.

- **Retardos de los paquetes:** una red IP no asegura el retardo de un paquete. Solamente a través del control y gestión global extremo a extremo, y la disponibilidad de suficiente ancho de banda, así como la tecnología de switching-routing necesaria, es posible asegurar unos niveles de retardo máximos.
- **Jitter:** es muy dependiente del retardo de los paquetes, y consiste en el tiempo de variación en la llegada de paquetes. Este parámetro tiene los mismos problemas y dificultades que el retardo, por lo que las soluciones van en la misma línea.
- **Pérdida de paquetes:** al estar basados sobre UDP, (una transmisión no fiable) las pérdidas de paquetes pueden llegar a ser importantes si existe congestión o problemas en la transmisión.

VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS.

VoIP Retardo.

El retardo produce dos problemas:

- La presencia de Eco
- Talking Overlap

El eco es causado por la reflexión de la señal de voz del que habla y que vuelve a su oído. Es producida por las desadaptaciones en el terminal receptor del equipo lejano.

Se convierte en un problema importante cuando el retardo de ida y vuelta es mayor a 50 mseg.

Como el eco es percibido como problema significativo desde el punto de vista de la calidad, se debe corregir con la utilización de canceladores de eco.

La presencia de Eco - Talking Overlap (Solapamiento de hablantes)

Se produce cuando los dos interlocutores hablan simultáneamente, particularmente cuando uno está hablando y el otro se superpone.

Se convierte en un problema importante cuando el retardo extremo a extremo es mayor a 150 mseg.

Por esto, el retardo “end to end”, es el mayor condicionante para el diseño de una red de VoIP, para asegurar un nivel de calidad acorde a los requerimientos de los clientes

CAUSAS DEL DELAY.

- Demora de trama (demora de algoritmo o de acumulación)
- Demora de procesamiento (depende del hardware)
- Demora de red.

Es causada por el modo de operación de los codificadores de voz. Estos requieren, una o más tramas completas de muestra por lo que es necesario un "buffering". Esto implica cierta demora inevitable, y que es inherente al proceso de codificación.

Como se mostró en el cuadro anterior el codificador acorde a la norma G.729 CS-ASELP que comprime la voz a 8 Kbits/seg introduce un retardo de 10 mseg.

Es el tiempo que toma el codificador en "analizar" la voz, esto es, la toma de las muestras de voz, más el tiempo que consume el decodificador en reconstruirla y es dependiente del hardware.

Esta demora es causada por el medio físico de la red, de la capacidad de los links de la misma y los protocolos usados en la transmisión de la VoIP y además por los buffers utilizados para remover el jitter en el extremo receptor.

Es una parte significativa en la suma de la demora total extremo a extremo.

VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS.

Jitter.

Es la variación del tiempo de arribo de los frames del codec. Se produce los distintos caminos que puede tomar el paquete al cruzar la red y afecta la calidad.

Si la muestra entra en el buffer introduce retardo y si no entra en el buffer afecta por el descarte de paquetes

Para contrarrestarlo se utilizan **Buffers Anti-jitter Adaptativos**: el Gateway sensa el Jitter de la red (RTP) y ajusta el tamaño del "de-jitter buffer" para compensar las diferencias de tiempo de arribo de paquetes.

Esto afecta la latencia pues introduce retardo en la red.

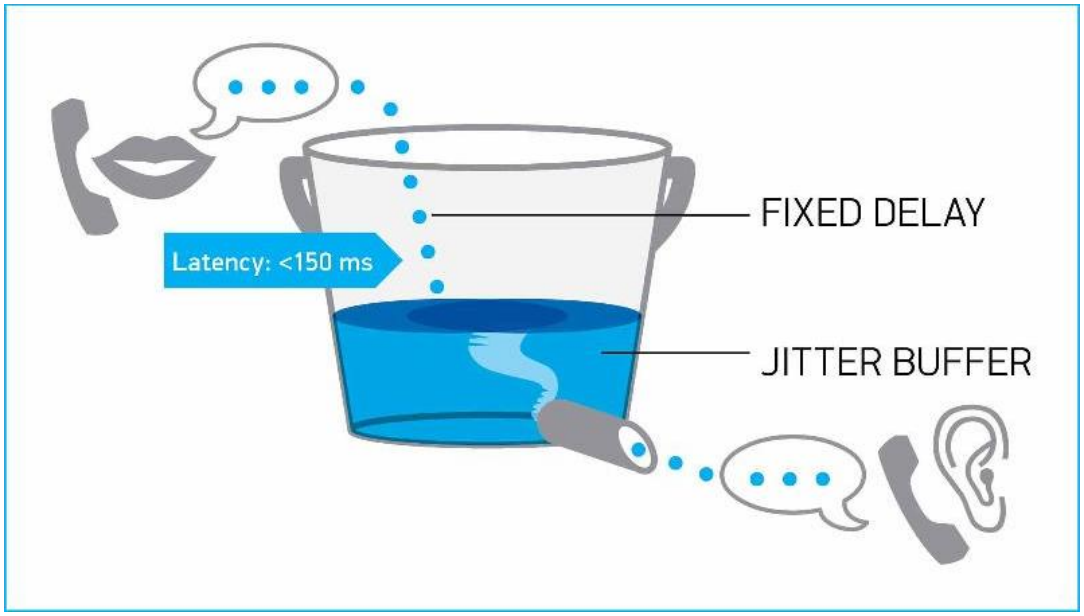
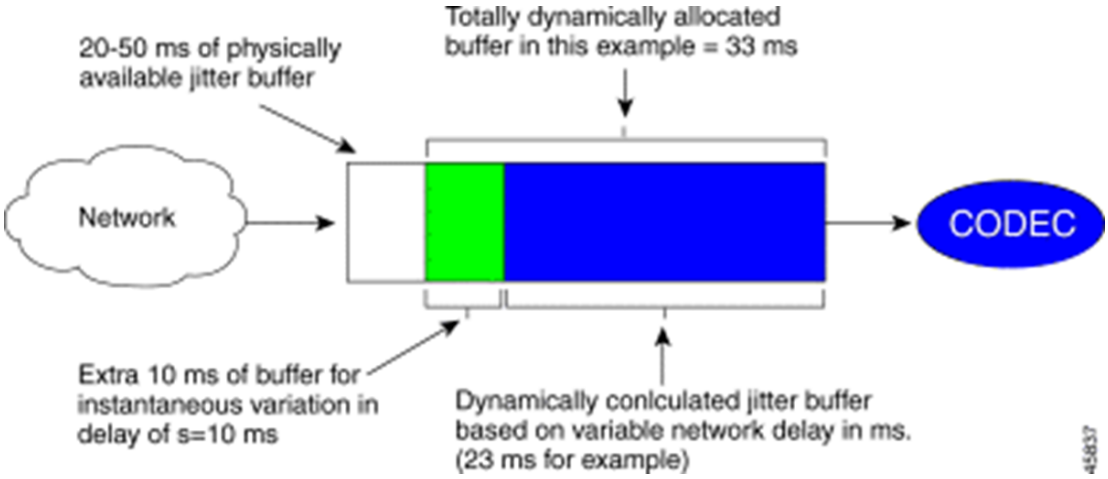


Ilustración 3 Buffer anti jitter

JITTER: BUFFER ADAPTATIVO.

El buffer adaptativo es calculado dinámicamente tomando como variable en delay de la red en milisegundos.



VOIP PARÁMETROS MÁS INFLUYENTES EN LA QOS.

Pérdida de Paquetes.

Al estar basados sobre UDP, (una transmisión no fiable) las pérdidas de paquetes pueden llegar a ser importantes si existe congestión o problemas en la transmisión.

La pérdida de paquetes introduce tasa de error en las comunicaciones

Se minimiza:

- Sobredimensionando las redes de modo que no se tengan que descartar paquetes en forma preventiva en los routers (WRED)
- Marcando los paquetes de VoIP como prioritarios (Diffserv)

El oído humano tolera no más de 1% al 3% de paquetes perdidos

CODIFICACIÓN DE LA VOZ: OTROS ASPECTOS.

Se debe tener en cuenta los "silencios" de la conversación, para una mejor explotación del ancho de banda. Para ello se emplean "algoritmos de compresión del silencio" en la codificación de voz.

Por ello se requiere la utilización de:

- Algoritmos de detección de la actividad de voz (VAD)
- Algoritmos de generación de ruido de confort (CNG)

La señal de voz codificada resultante se transmite con una velocidad no uniforme en función del nivel de actividad que presente la fuente generadora.

El mecanismo de compresión del silencio es crítico en las prestaciones de la codificación de voz.

Una implementación inadecuada conlleva a un deterioro significativo de la inteligibilidad de la voz.

LATENCIA.

Es el retardo one-way entre ambos extremos No debe superar los 150ms para no afectar la interactividad.

Factor a considerar	Valor aproximado
Retardo en el armado del frame a codificar	2*10ms (G.729) – [Por ej G.711, 1,5ms]
Tiempo de procesamiento para la codificación de la señal (look-ahead)	5ms (G.729)
Cantidad de muestras de código por paquete IP	+10ms (2 muestras en G.729) => (m-1) *t.frame
Si se emplea VAD	+5ms
Tiempo de armado del paquete IP	Depende intefaz de salida (Eth despreciable)
Delay introducido por la transmisión del paquete IP	40ms (aprox. BBIP)
Delay introducido por el buffer anti-jitter	20ms (aprox., se adapta dinámicamente puede llegar a 50ms)
Tiempo de procesamiento de decodificación	1ms
Tiempo total (para nuestro ejemplo)	101ms (aprox.)

PARÁMETROS DE LA VOZ.

Calidad de la Voz VSQ.

La calidad de la voz (Voice Speach Quality) es evaluada por medio de dos parámetros:

- Claridad: que refleja el grado de palabras y frases entendidas
- Fidelidad: califica el grado de reconocimiento de la personal que habla.

La VSQ se puede medir en mediciones subjetivas o mediciones objetivas.

Las medidas objetivas de la ejecución de servicios, como la pérdida de información y el retardo contribuyen a la QoE (calidad de experiencia).

Para realizar estas mediciones habitualmente se utilizan sistemas electrónicos, los cuales están basados en algoritmos y fórmulas matemáticas que miden la QoE en sistemas de IPTV, algunas de las técnicas que estos equipos electrónicos implementan son:

- Técnicas basadas en modelos de percepción humana de vídeo.
- Técnicas basadas en parámetros que indican el grado de deterioro de la red.
- Técnicas basadas en el tiempo del deterioro de la señal de vídeo.
- Técnicas basadas en los parámetros de las señales de vídeo.

Denominación	Descripción
PSQM	Perceptual Speach Quality Measure
PESQ	Perceptual Evaluation of Speach Quality
PSESQ_LQ	PSQM Listening Quality

En las mediciones subjetivas se aplica la Recomendación P.830 del ITU en la que se aplica el método Mean Option Score (MOS).

Estas medidas se realizan en entornos donde participan grupos de personas, las cuales realizan un conjunto de pasos como los que se listan a continuación:

- Elegir las secuencias de vídeo a evaluar.
- Evaluación y calificación numérica por parte de los observadores.
- Depuración de los observadores por fallos en el proceso.
- Cálculo de la calidad subjetiva media, mediante el análisis estadístico de los resultados encontrados por los observadores, este valor es conocido como MOS (Mean Opinion Scale).

Score	Nivel VSQ	Descripción
5	Excelente	Muy claro, pequeño retardo y comunicación tranquila
4	Bueno	Claro, bajo retardo y comunicación tranquila con poco ruido
3	Razonable	No muy claro, nivel medio de retardo y comunicación posible
2	Pobre	No claro, alto retardo y comunicación dificultosa
1	Malo	No comprensible, muy alto retardo y comunicación bloqueada

PROTOCOLOS VOIP.

Las tecnologías "IP" hacen referencia a un conjunto de protocolos que conforman la red IP.

Los protocolos de transporte más usados son:

- TCP: capaz de proporcionar conexiones garantizadas para paquetes de datos sobre IP
- UDP: que proporciona un servicio de entrega no garantizado

Ninguno de estos protocolos por sí mismos pueden proporcionar el soporte de aplicaciones en tiempo real como la voz.

Existen una serie de protocolos que proporcionan servicios en tiempo real sobre IP

- RTP (Real Time Transport Protocol)
- RTCP (Real Time Control Protocol)
- RSVP (Resource Reservation Protocol)
- RTSP (Real Time Streaming Protocol)

Existen a su vez protocolos de señalización, que permiten el inicio, mantenimiento y fin de cada comunicación:

- Modelo H.323 (solución UIT)
- Modelo SIP (solución IETF)
- Modelo MEGACO (H.248)

TRANSPORTE DE INFORMACIÓN EN TELEFONÍA IP.

Se requiere un protocolo, o conjunto de ellos, que se ocupe de esta tarea y garantice la entrega de los paquetes de "medios" en tiempo real, o casi en tiempo real, siempre y cuando el deterioro de la calidad no sobrepase lo humanamente admisible, según el caso.

En relación con esto hay que señalar que la red IP no solo "mueve" a través de ella paquetes de información de usuario propiamente dicha, sino también "mueve" paquetes de control, es decir paquetes de señalización.

El término señalización en Telefonía IP tiene una connotación algo más amplia que el concepto correspondiente en las redes clásicas de Telecomunicaciones modo circuito

Se trata ahora no sólo de la señalización necesaria para el control de la llamada en el sentido clásico (establecimiento, mantenimiento-modificación y terminación de la "conexión"), sino también señalización para garantizar QoS.

En correspondencia con esto, hay que hacer la distinción entre "transporte de medios", en alusión a la información de usuario (voz, imágenes, etc.), y "transporte de información de control", es decir, señalización.

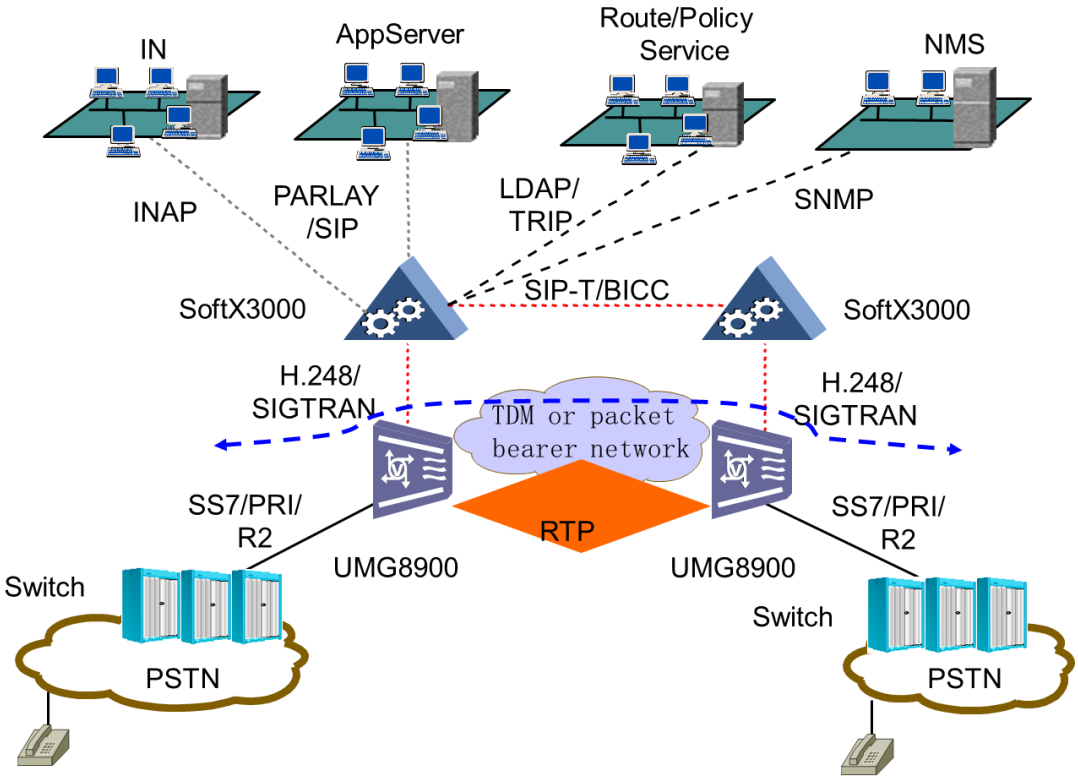


Ilustración 4 Flujo de señalización y de voz

TRANSPORTE DE INFORMACIÓN EN TELEFONÍA IP.

El transporte de los medios (voz, vídeo, datos, etc.) por la red IP no sólo se traduce en mover por la misma secuencia de bits empaquetados, sino que también se requiere adicionarles a éstos cierta información de control, por ejemplo:

- Tipo de información transportada
- Números de secuencia
- Marcas de tiempo, etc.

Esto supone una manera de "formatear" los paquetes IP y hacerlos aptos para el transporte de información con requerimientos de tiempo real.

REAL TIME TRANSPORT PROTOCOL

El transporte de medios exige cumplir una serie de requisitos:

- **Caracterización de la carga útil**, su identificación, cómo ha sido codificada, su formato, cuántas tramas por paquete, etc.
- **Información de tiempo** que posibilite su reconstrucción temporal en el receptor o los receptores, y la sincronización de diferentes flujos de medios en el tiempo.
- **Secuenciamiento** de los paquetes que constituyen los streams de medios, para posibilitar su reproducción en orden correcto y la detección de paquetes perdidos

Todo esto posibilita la gestión adecuada de los streams de medios en el receptor.

PROTOCOLO RTP (REAL TIME TRANSPORT PROTOCOL).

Concebido para compensar el jitter y la pérdida de secuencia de los paquetes que introducen las redes IP. Puede ser empleado para el transporte de streams de datos sensibles al tiempo, p.e. voz y vídeo.

Juntamente con el protocolo RTP se utiliza el RTCP (Rel time Control Protocol) con funciones de monitorización de la calidad de servicio y otras.

Los protocolos RTP y RTCP no ejercen ningún tipo de influencia en las condiciones de la red IP, no controlan la calidad de servicio, sólo posibilitan que los receptores puedan "resolver" apropiadamente las "perturbaciones" (jitter, pérdida de secuencia) a que son sometidos los paquetes IP con contenidos de tiempo real al atravesar la red.

Los paquetes RTP trasportan streams de datos sensibles a:

- A las demoras de la red
- A sus fluctuaciones
- A las pérdidas de paquetes,
- A las pérdidas de información adicional que posibilite su recuperación y entrega adecuada.

Con respecto a las pérdidas de información adicional:

- La identificación de la fuente
- Tipo de carga útil que transporta el paquete
- La secuenciación de paquetes
- La información de temporización

El protocolo RTP provee monitorización, diagnostica y realimenta al emisor de la calidad de la transmisión; soporta también la integración de tráfico transmitiendo múltiples fuentes en un simple flujo.

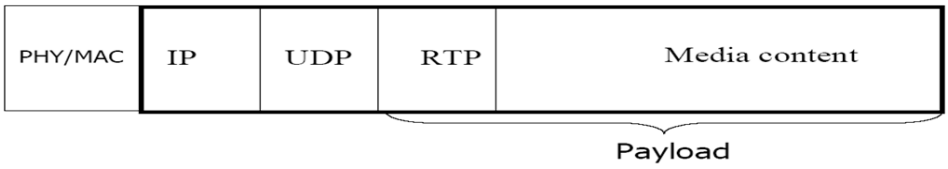
RTP Provee:

- Sincronismo
- Secuenciamiento y Detección de perdida de paquetes
- Segmentación y rearmado

Cada flujo RTP es unidireccional y tiene asociado un flujo RTCP en el port UDP n+1.

El lado origen envía: información sobre los datos enviados, sincronización y timestamp

El lado receptor envía: información sobre los datos recibidos, perdida de paquetes, jitter y delay.



RTP posibilita el transporte de datos isócronos a través de redes de paquetes
Ha sido optimizado para transferencias con requisitos de tiempo real, tanto unicast como multicast, soportando servicios extremos a extremo.

Pero no garantiza:

- Reserva de recursos ni da garantía de calidad de servicio
- Provisión de mecanismos para garantizar la entrega en tiempo
- Asume que la red es segura y entrega los paquetes en secuencia.

Su papel fundamental es actuar como una interface entre aplicaciones de tiempo real y los protocolos de la capa de transporte, sin establecer qué protocolo debe ésta usar, aunque típicamente se soporta sobre UDP.

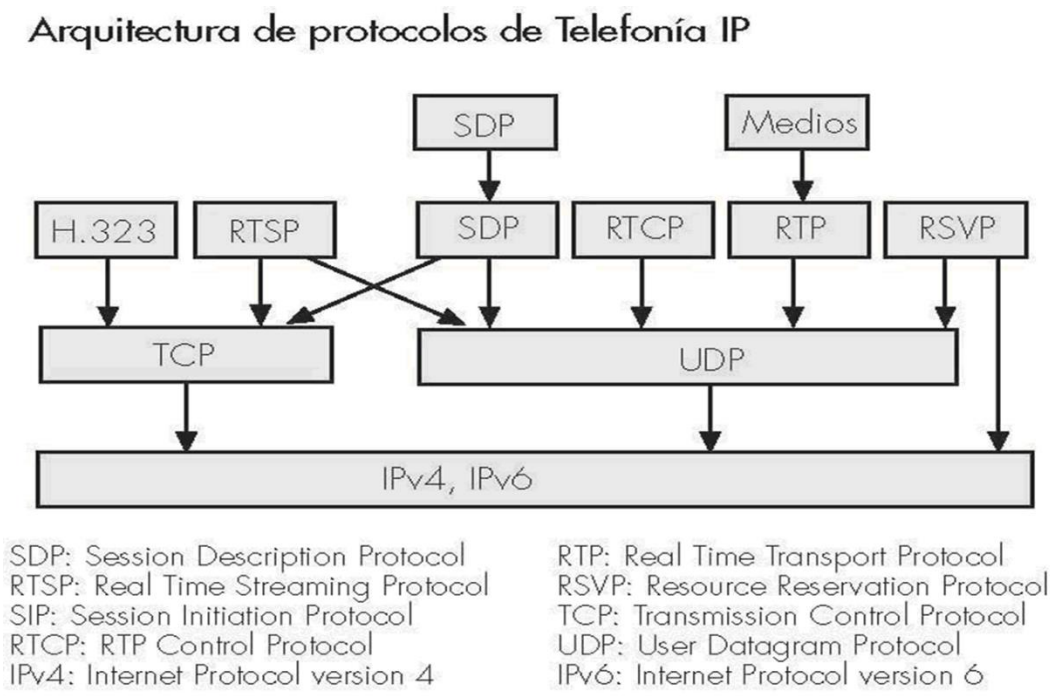
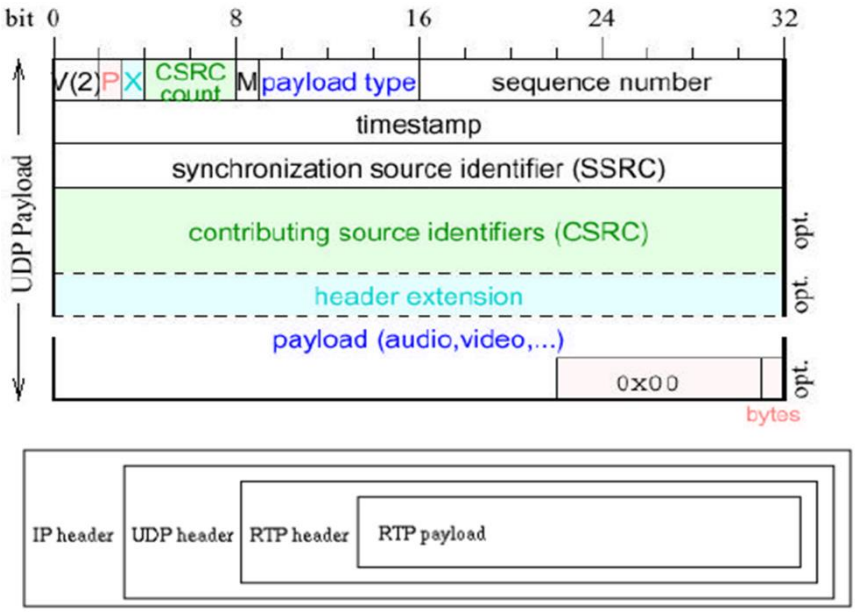


Ilustración 5 Arquitectura del protocolo RTP

A continuación, se muestra la trama RTP



PROTOCOLO RTCP (REAL TIME CONTROL PROTOCOL).

RTCP es un protocolo de control que "acompaña" al protocolo RTP para la transferencia entre fuentes y destinos de streams multimedia. Proporciona información de la calidad de la transmisión en la red, posibilitando adaptar las fuentes al estado de la red.
RTCP se basa en la transmisión periódica de paquetes de control a todos los participantes en la sesión, empleando el mismo mecanismo de distribución que los paquetes de datos, por lo que debe proveer la multiplexación de paquetes de datos y paquetes de control RTCP, p.e., mediante el empleo de puertos diferentes del protocolo UDP.
RTCP es imprescindible en sesiones multicast, como realimentación de cómo reciben los streams de datos los destinatarios, posibilitándose así homogeneizar la calidad. En comunicaciones unicast no es necesario, pero si es útil su uso.

Sus funciones son las de suministrar información respecto a la calidad de la distribución de los datos, "realimentación" que posibilita a la fuente de los datos:

- aplicar control de flujo
- aplicar control de congestión
- aplicar codificación adaptativa
- diagnosticar fallos en la distribución multicast
- posibilita obtener información útil para diagnóstico y gestión de la red.

También Controla la velocidad de emisión de paquetes RTP, para que éste sea escalable en cuanto al número de participantes.

RTCP debe ser utilizado por todos los participantes de una sesión RTP, enviando cada uno de ellos paquetes RTCP periódicamente.

Se debe dejar una pequeña parte (5 %) del ancho de banda asignado a RTP para RTCP, y se reparte entre todos los participantes.

SEÑALIZACION Y CONTROL DE LLAMADA H.323 y SIP

Por las propias características de las redes IP, que no asignan recursos en exclusividad para cada comunicación, sino que existe una compartición máxima de los mismos, se hace necesario que los sistemas de VoIP requieran señalizar, con los protocolos adecuados, todo el control de la comunicación, por ejemplo:

- Negociar el tipo de codificador a utilizar
- Negociar los parámetros de empaquetado de la voz (y vídeo)
- Negociar la calidad de servicio con la red (demoras, pérdida de paquetes)
- Intercambiar N° de Puertos por los que se llevará a cabo la comunicación.

La señalización de VoIP y demás medios sobre IP debe garantizar los servicios clásicos que brindan las redes telefónicas, sumar la potencialidad que presentan las redes IP para la integración de servicios de voz, datos y vídeo.

También debe dar solución a la problemática particular de manejar tráfico con requerimientos de tiempo real sin que la QoS se deteriore más allá de lo admisible.

El flujo de la información de usuario y el flujo de señalización siguen trayectorias diferentes en su paso por las redes IP

En la señalización intervienen elementos funcionales que no intervienen en el manejo de los paquetes de la información de usuario.

La voz (información de usuario) y la señalización no presentan los mismos requerimientos de transporte por la red, la voz tiene que ser tratada con demora y jitter mínimos, pues pierde "valor" con el tiempo, dados sus requerimientos de tiempo real

La señalización carece de requerimientos de tiempo real.

Los "momentos" de la señalización no tienen coincidencia total con los "momentos" de la conversación, en lo fundamental la señalización precede y sucede a la conversación
Según el caso también puede coincidir en el tiempo con ésta, es decir, que durante el trasiego por la red de paquetes de voz también se transfieran paquetes de señalización de una comunicación ya establecida.

El tráfico de información de usuario (voz, etc.) es tratado por la red IP de manera diferente a como lo hace con el tráfico de señalización.

Los protocolos de señalización son los que se usan para garantizar el establecimiento, mantenimiento, modificación y terminación de llamadas de voz sobre las redes IP: señalización de control de llamadas.

También intervienen en la QoS, seguridad y control de medios.

Se han desarrollado diferentes soluciones para la problemática de la señalización de control de llamada en sistemas de VoIP:

- **Modelo H.323 (solución UIT)**
- **Modelo SIP (solución IETF)**
- **Modelo MEGACO (H.248)**

Son tres soluciones diferentes a la misma problemática, la señalización de control de llamada para el servicio de VoIP, cada una con una arquitectura funcional y protocolos que las caracterizan.

PROTOCOLO DE SEÑALIZACION H.323

H.323 es el protocolo internacional para conferencia sobre redes de paquetes que ha sido aprobado por la UIT en 1996. Esto garantiza la Interoperabilidad de aplicaciones con diferente hardware y software sobre IP y con Interoperabilidad de aplicaciones con diferente hardware y software sobre IP y con ISDN y PSTN.

H.323 se define como el standard que permite que el tráfico multimedia en tiempo real sea intercambiado sobre una red de paquetes, por ejemplo, la red IP. También define una serie de entidades en una red cada una de ellas con una serie de funcionalidades.

H.323 incluye las siguientes recomendaciones:

- **H.225.0**: paquetización, sincronización, señalización (Contiene el protocolo RAS)
- **H.245** : control de canal
- **H.261 y H.263**: codificación de vídeo
- **G.711, G.722, G.723.1, G.728, G.729**: codificación de audio
- **T.120:** conferencias de datos en tiempo real, punto a punto y multipunto.

COMPONENTES H.323.

H.323 define los siguientes componentes: Terminal, Gateway, Gatekeeper, Unidad de Control Multipunto, etc.

Gateways: son los sistemas encargados de permitir que los equipos H.323 puedan operar con otras redes.

Las pasarelas (Gateways) sirven de "puente" entre redes H.323 y otras redes, por ejemplo con las redes de conmutación de circuitos de telefonía.

Desarrollan la "traducción" de la señalización, y la formación del control e información de usuario, según requerimientos de las redes que interconecta, posibilitando así la interoperabilidad entre redes, terminales y servicios, haciendo viable la integración de servicios aún con plataformas dispares (p.e., PSTN y redes IP).

Los Gateways cursan información de usuario, soportada ésta en RTP/UDP/IP.

Los Gateways, "vistos" desde cada una de las redes que interconecta, se comportan como un elemento más de las mismas, es decir, vista desde la red telefónica se comporta como una central de conmutación más de ésta, y vista desde una red IP como un nodo más de ésta.

Los Gateways son elementos funcionales opcional en entornos H.323, sólo son necesarias cuando se requiere interconexión entre entornos H.323 y entornos no H.323.

Así tenemos:

- Gateways H.320, para redes N-ISDN
- Gateways H.321, para redes B-ISDN
- Gateways H.322, para redes LAN con calidad de servicio
- Gateways H.324, para redes GSTN e inalámbricas

Y realizan funciones como la Traducción de formatos de transmisión, traducción de procedimientos de comunicación, transcodificación de audio y video y el establecimiento y liberación de llamadas.

Gatekeepers: Dentro de su zona LAN actúa de monitor de la red, proporcionando los servicios de resolución de direcciones (por ejemplo, asignación de la dirección IP a su alias, ya sea número telefónico o nombre) y de conceder permisos de llamadas.

Son entidades de control y señalización y constituyen los elementos funcionales más complejos en el marco H.323.

Proveen aquellos servicios que no pueden ser descentralizados e implementados en los "endpoints" (terminales, pasarelas, MCU´s).

Las funciones que lleva a cabo un gatekeeper se clasifican en funciones básicas y opcionales.

Entre las funciones básicas encontramos:

- Traducción de direcciones.
- Control de admisión.
- Control del ancho de banda.
- Gestión de Zona H.323.

Traducción de direcciones: Entre direcciones de transporte y alias de direcciones

Control de admisión: controla el acceso sobre la base de diferentes criterios, p.e., autorización, ancho de banda, etc. Puede no existir, esto es, se admiten todas las solicitudes de acceso

Control del ancho de banda: puede basarse en la gestión del ancho de banda. Puede no estar presente, admitiéndose todas las solicitudes de ancho de banda

Gestión de Zona H.323: se refiere a las funciones anteriores para los terminales, Gateways y MCU´s registrados en su zona de control.

Como funciones opcionales tendremos:

Señalización de control de llamada: en conferencias punto a punto el GK puede procesar mensajes Q.931

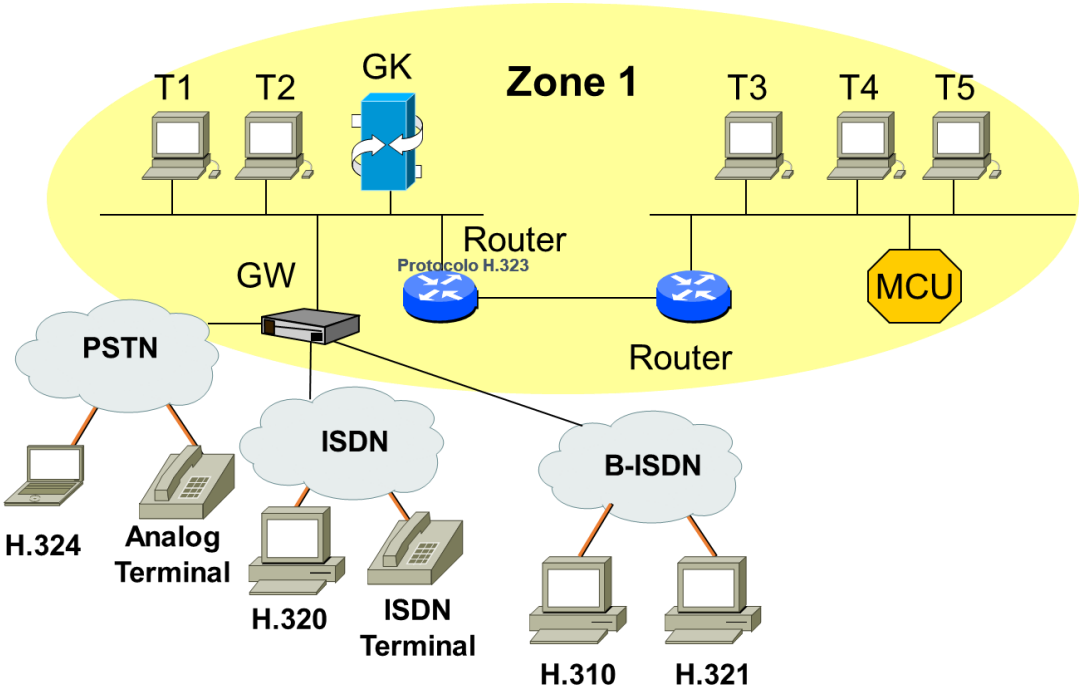
Autorización de llamadas: sobre la base de la especificación Q.931 el GK puede rechazar llamadas, p.e., acceso restringido a y desde determinados terminales o Gateways, restringir el acceso durante ciertos periodos de tiempo, etc.

Gestión de ancho de banda: el GK puede rechazar llamadas si el ancho de banda que éstas solicitan no está disponible, bien en nuevas llamadas o en llamadas en curso que soliciten ancho de banda adicional.

Gestión de llamadas: el GK puede, mediante una tabla propia, disponer del estado de las llamadas H.323, pudiendo saber el estado de un terminal dado y el "gasto" de ancho de banda asociado a las llamadas en curso, y proceder en consecuencia respecto a las nuevas solicitudes.

Terminales: son los dispositivos que se pueden conectar directamente a IP y soportan H.323

MCUs: (Multipoint Control Unit): es el sistema encargado del control de las conferencias múltiples, proporciona todos los servicios para establecer comunicaciones multipunto.



• La recomendación H.323 (ITU-T) cubre los requerimientos técnicos para brindar servicios de comunicación (audio y video) sobre ambientes LAN

EL ESTABLECIMIENTO DE LLAMADAS EN H.323.

El establecimiento de la llamada se lleva a cabo en tres fases.

- **Fase RAS:** intercambio de mensajes entre gatekeeper y endpoint, para traducción de direcciones, autorización (o rechazo) de llamadas y gestión de ancho de banda.
- **Fase Q.931:** intercambio de mensajes entre endpoints para el establecimiento de conexiones lógicas
- **Fase H.245:** intercambio de mensajes entre endpoints para "acordar" el intercambio de información de usuario.

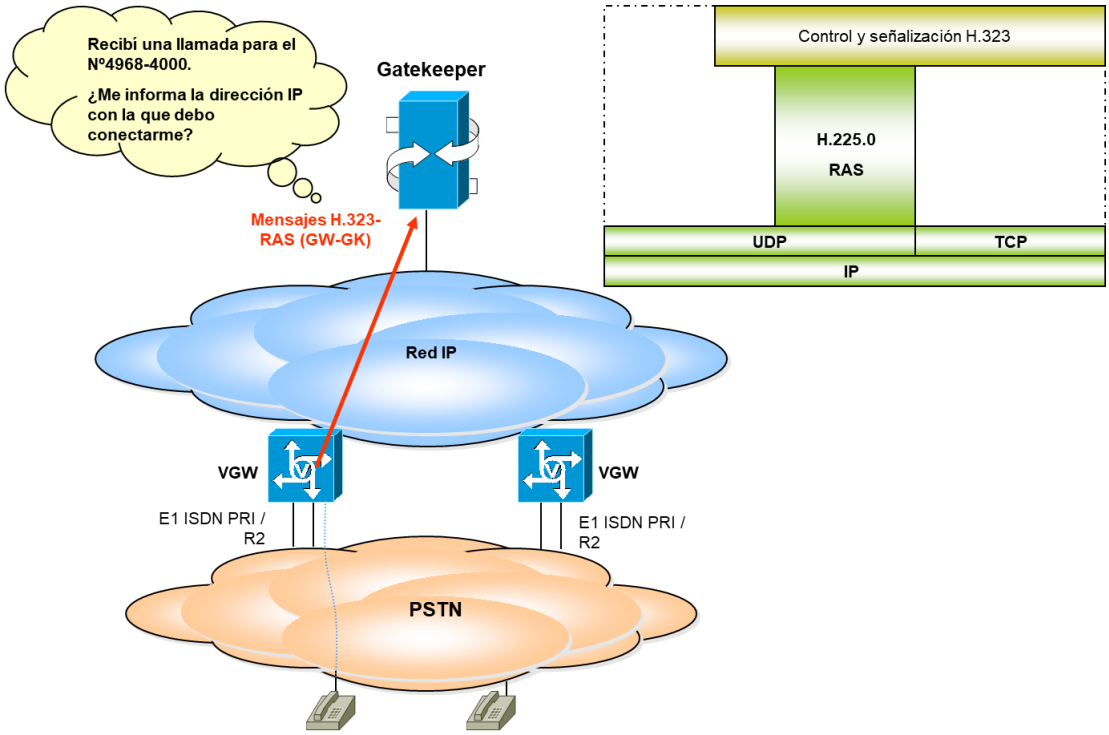
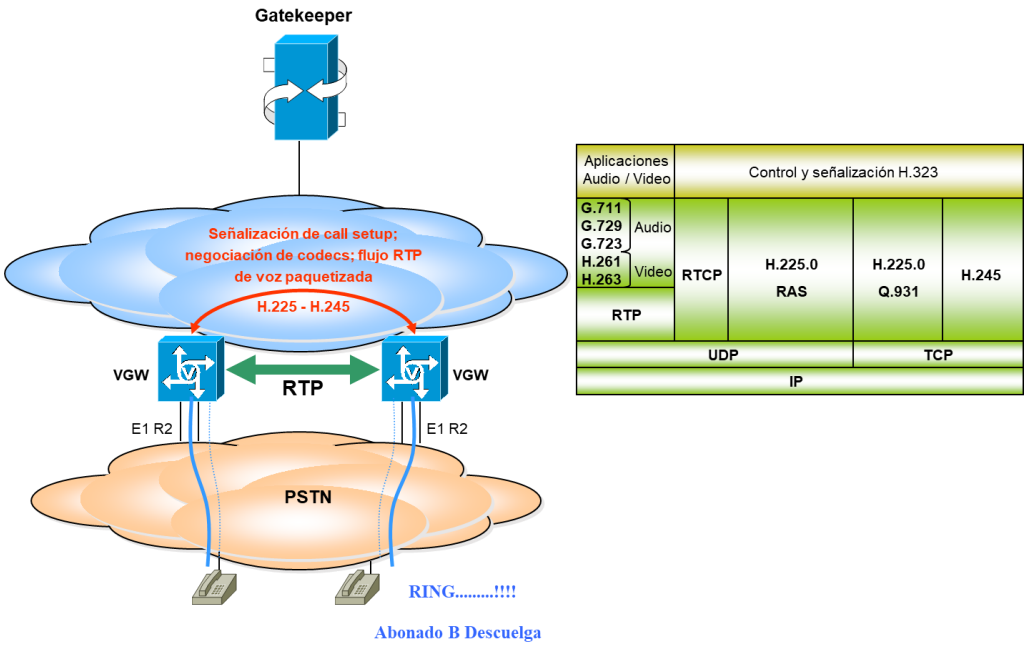


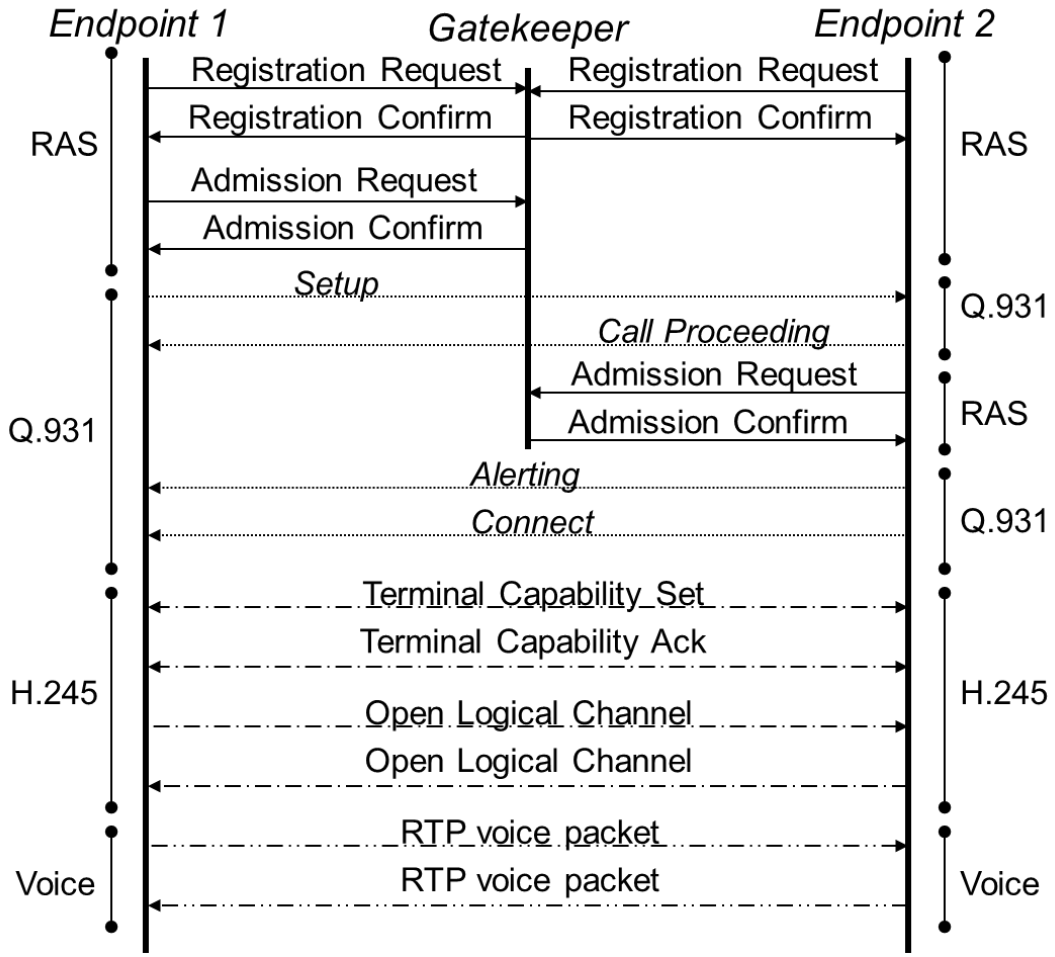
Ilustración 6 pedido de una llamada hacia la red PSTN

A continuación, el gatekeeper verifica las listas de numeración y la tabla de enrutamiento IP y le iindica a que IP debe conectarse para establecer la llamada.

El destino solicita permiso al gatekeeper para establecer la llamada y al autorizarla se produce el enlace con la red PSTN



En la próxima ilustración pueden verse los mensajes ente los componentes de H.323



PROTOCOLO DE SEÑALIZACION SIP

SIP (Session Initiation Protocol) es un protocolo de control del nivel de aplicación que maneja la señalización y el control de llamadas.

Controla el establecimiento, modificación y terminación de sesiones o llamadas multimedia, directa o indirectamente.

SIP se cataloga como un protocolo de señalización y forma parte de las especificaciones del IETF para comunicaciones multimedia, juntamente con otros protocolos como RSVP, RTP, RTSP, SAP, SDP, pero su funcionalidad no depende de ninguno de éstos.

Soporta comunicaciones entre usuarios pertenecientes a redes IP, como también con usuarios de las redes telefónicas por intermedio de pasarelas (gateways).

Debemos notar que es neutral en relación con los protocolos de las capas inferiores, por lo que puede soportarse sobre TCP o UDP , igualmente sobre IP, IPX, ATM AAL5, F-R o X.25.

Provee por sí mismo sus propios mecanismos de seguridad.

Por otra parte, SIP es un protocolo basado en texto, emplea el juego de caracteres ISO 10646 con codificación UTF-8 (RFC 2279), lo que posibilita una fácil implementación y depuración, lo hace flexible y extensible.

El sobre encabezamiento que implica usar un protocolo basado en texto no tiene aquí mayores trascendencias, pues SIP es un protocolo de señalización, no es un protocolo para transmisión de datos de usuario donde sí tendría consecuencias su orientación a texto.

Los elementos funcionales de SIP son:

- Agentes de Usuario (User Agent, UA),
- Servidores de Red.
- Agentes de Usuario Clientes (User Agent Client, UAC)
- Agentes de Usuario Servidores (User Agent Server, UAS).

Los UAC originan las solicitudes SIP (asociados al extremo que origina la llamada).

Los UAS responden a estas solicitudes, es decir, originan respuestas SIP (asociados al extremo que recibe la llamada).

Los UAC y UAS por sí solos son capaces, sin los servidores de red, de soportar una comunicación básica (modelo de llamada básico, directamente entre endpoints).

La potencialidad del Modelo SIP se aprovecha con el empleo de los Servidores de Red (modelo de llamada con servidores proxy y modelo de llamada con servidores de redirección).
Los UA deben implementar el transporte tanto sobre TCP como sobre UDP.
Los Servidores de Red se pueden clasificar de la siguiente manera:

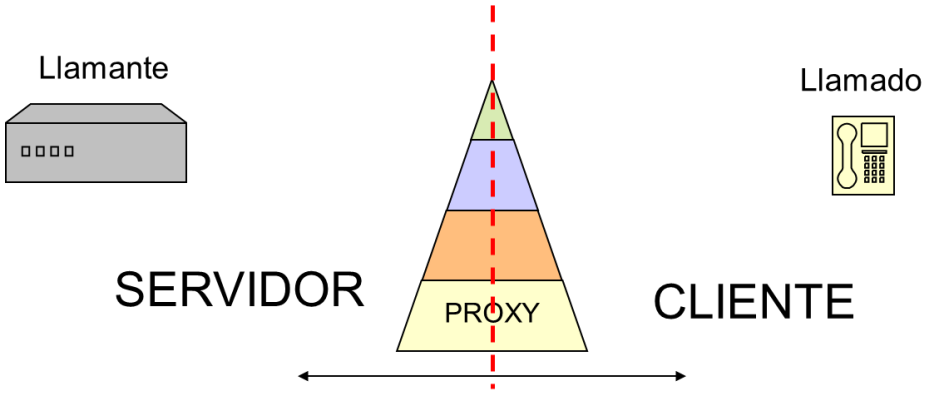
- Servidores de Redirección
- Servidores Proxy
- Servidores de Registro

SERIDORES DE REDIRECCION.

- Redireccionan las solicitudes de llamadas (mensajes INVITE), que son solicitudes SIP
- Retornan la dirección (o direcciones) de la parte llamada, (SIP-URL), o cómo contactar con ella (respuesta 3xx).
- Rechazan la llamada error de cliente, enviando una (respuesta 4xx)
- Rechazan la llamada error de servidor, enviando una (respuesta 5xx)

SERVIDORES PROXY.

Corren un programa "intermediario" que actúa como servidor y como cliente. Respecto al llamante se comporta como servidor y, al llamado como cliente.



Un servidor proxy puede reenviar solicitudes hasta el destino final sin efectuar cambio alguno en ellas.

Puede cambiar alguno de sus parámetros si se requiere y desarrollan el ruteo de las solicitudes y respuestas SIP.

Servidor Proxy	Stateful	Retienen la información de la llamada durante el tiempo que esta dure
	Stateless	Procesan el mensaje SIP y luego "olvidan" todo hasta recibir nuevo mensaje

SERVIDORES DE REGISTRO.

Registran las direcciones SIP (SIP-URL) y las direcciones IP asociadas.

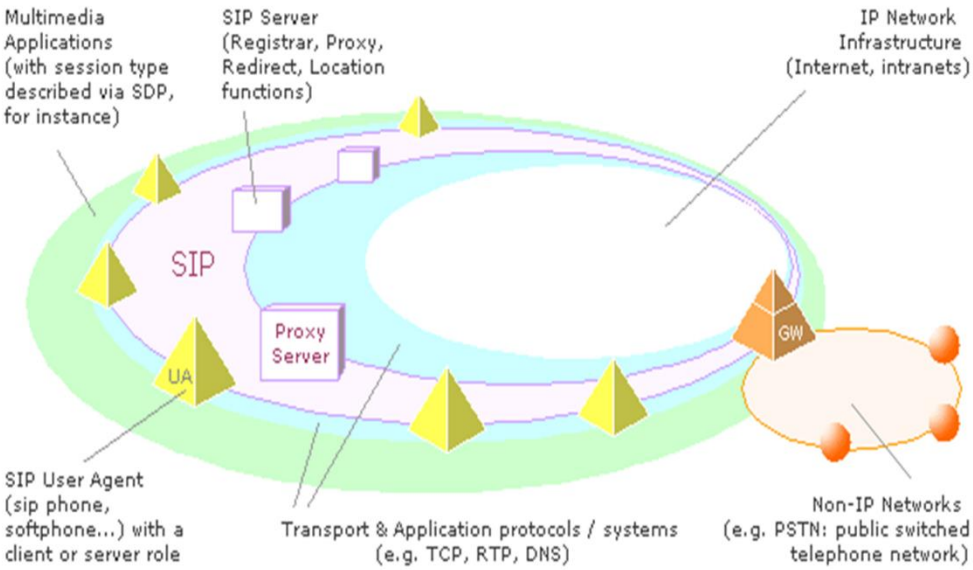
Garantizan el "mapping" entre direcciones SIP y direcciones IP.

Son servidores que sólo aceptan solicitudes REGISTER, posibilitando el registro correspondiente a la localización actual de los usuarios.

Se les denomina servidores de localización, pues son utilizados por los servidores proxy y de redirección para obtener información respecto a la localización o localizaciones posibles de la parte llamada.

Deben implementar el transporte sobre TCP y UDP.

EL MODELO SIP.



El protocolo SIP intercambia mensajes SIP (solicitudes y respuestas) a través de transacciones entre los entes funcionales (Agentes de Usuario y Servidores de Red).

Estos mensajes emplean el formato de mensaje definido en la RFC 822.

Los métodos SIP, esto es, mensajes de solicitud, son:

- INVITE
- ACK
- OPTIONS
- BYE
- CANCEL
- REGISTER

INVITE: invita a un usuario o servicio a participar en una sesión. El cuerpo del mensaje contiene una descripción de la sesión.

ACK: confirma que el cliente llamador ha recibido una respuesta final desde un servidor a una solicitud, p.e. a la solicitud INVITE, reconociendo la respuesta como adecuada.

OPTIONS: posibilita descubrir las capacidades del receptor.

BYE: finaliza una llamada o una solicitud de llamada. Puede ser enviado por el agente llamante o por el agente llamado.

CANCEL: cancela una solicitud pendiente, pero no afecta una solicitud completada. Este método finaliza una solicitud de llamada incompleta.

REGISTER: se utiliza este método como un servicio de localización que registra la localización actual de un usuario. También es necesario cuando hay varios servidores SIP en un mismo host, en cuyo caso solo uno de los servidores puede usar el número de puerto por defecto. Un servidor SIP que es capaz de aceptar mensajes REGISTER se denomina como Registrar.

Las posibles respuestas a estas solicitudes son códigos de tres enteros, e indican el resultado de comprender y satisfacer una solicitud.

- 1xx: Informativo. Solicitud recibida, que continua para procesar la solicitud. Por ejemplo, 180 RINGING,
- 2xx: Sucesos. La acción fue recibida de forma adecuada, comprendida y aceptada. Ej: 200 OK,

- 3xx: Redireccionado. Más acciones deben ser consideradas para completar la solicitud. Ej: 302 MOVED TEMPORARILY,
- 4xx: Error de cliente. La solicitud contiene mal la sintaxis o no puede ser resuelta en este servidor. Ej: 404 NOT FOUND,
- 5xx: Error de servidor. El servidor ha errado en la resolución de una solicitud aparentemente válida. Ej: 501 NOT IMPLEMENTED,
- 6xx: Fallo global. La solicitud no puede ser resuelta en servidor alguno. Ej: 600 BUSY EVERYWHERE.

MODELO BÁSICO DE LLAMADA SIP: (MODO DIRECTO)

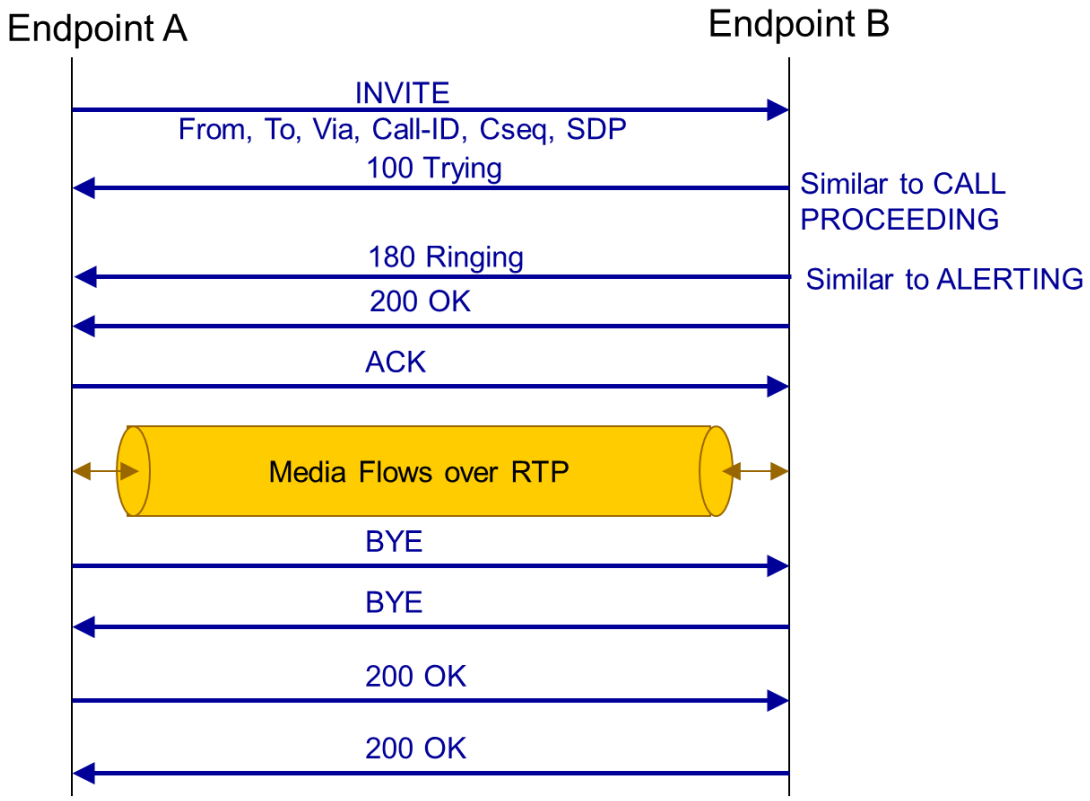
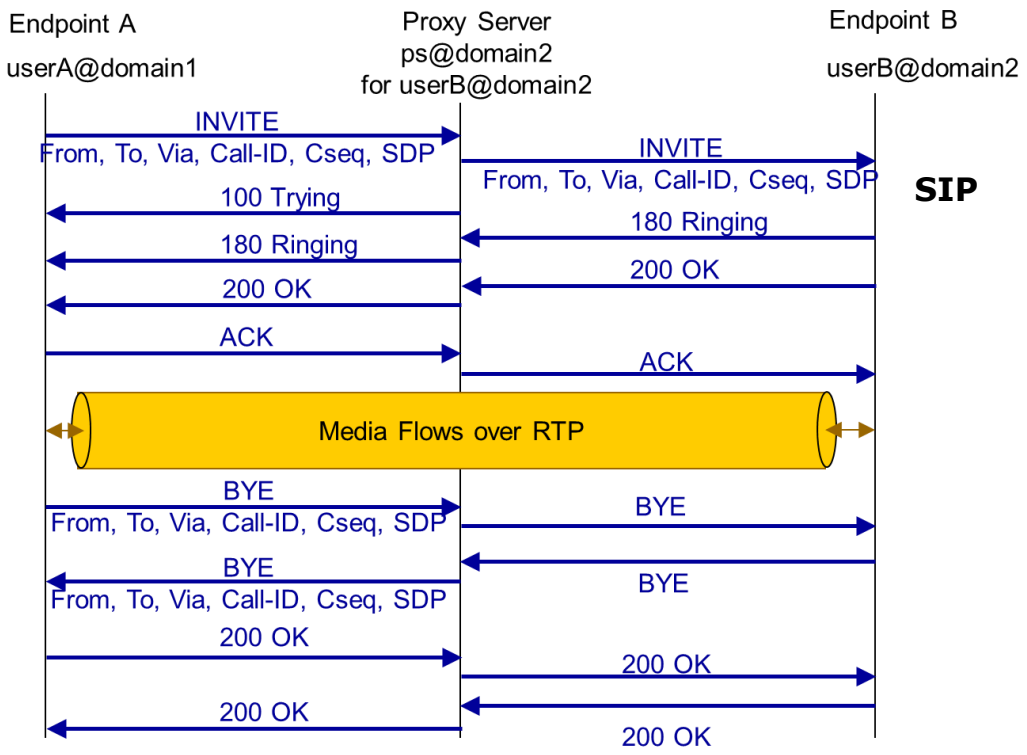
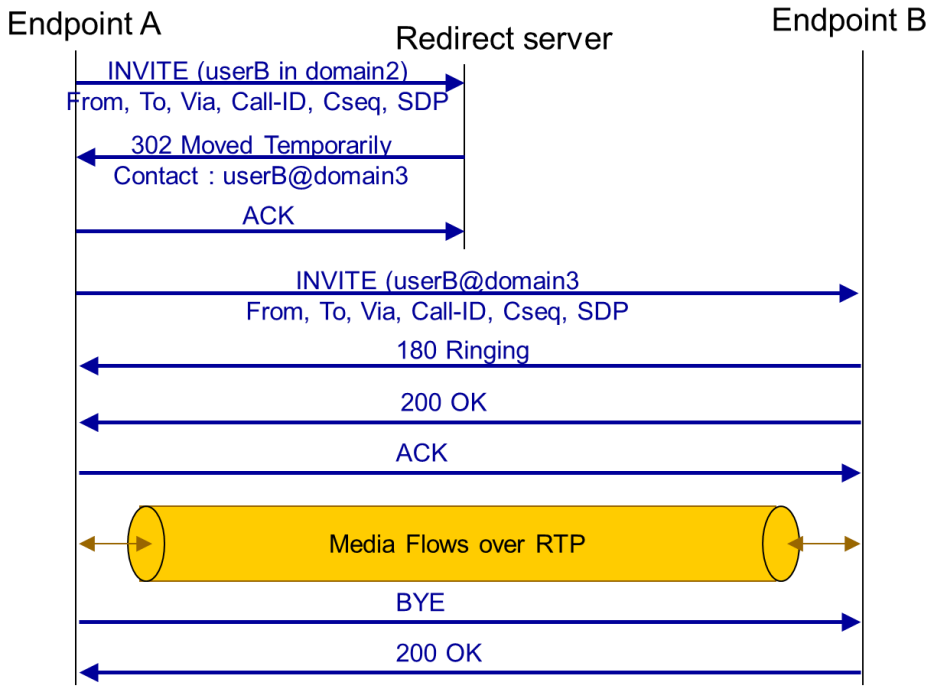


Ilustración 7 Modelo básico de la llamada SIP

SIP PROXY CALL MODEL.



REDIRECT CALL MODEL.



Fin de la clase
UAI
Universidad Abierta
Interamericana

REDES ADMINISTRATIVAS

UNIDAD 7: REDES DEFINIDAS POR SOFTWARE

CLASE 14

Claudio Milio 2020

En la clase 14 veremos una definición de las diferentes tecnologías sobre las redes SDN.

INTRODUCCION A LAS REDES SDN

Las redes definidas por software surgieron para automatizar las redes para las aplicaciones que se ofrecen a través de una nube privada virtual o como un servicio de nube pública.

Las redes definidas por software (SDN) están diseñadas para flexibilizar y agilizar la red. Permiten diseñar, desarrollar y administrar redes mediante la separación de los planos de control y reenvío de datos. Como resultado, el plano de control se puede programar directamente, y abstrae la infraestructura subyacente para las aplicaciones y los servicios de red.

La inteligencia de red se centraliza de manera lógica a través de controladores SDN programables. Implementados en el software, estos controladores mantienen una vista coherente del dominio de red. Para los motores de aplicaciones y políticas, las SDN son como un switch lógico.

Se considera a las SDN como una evolución fundamental de la tecnología de constitución de redes que permitirá a los operadores de red establecer y gestionar nuevos recursos y redes de carácter virtual, sin tener que instalar nuevas tecnologías de soporte físico (hardware).

También tiene implicancia, junto a la virtualización de las redes, como algo esencial para contrarrestar el aumento de la complejidad y de los costos de gestión y funcionamiento de las redes tradicionalmente asociados a la introducción de nuevos servicios o tecnologías. Esta abstracción dará paso a una mayor velocidad y flexibilidad de las

instrucciones de encaminamiento y a la gestión de la seguridad y la energía de los equipos de red, como los encaminadores y los conmutadores.

Tienen las siguientes características:

- Capacidad para automatizar mediante programación las configuraciones de red, aumentando la escalabilidad y la confiabilidad.
- Una Mayor flexibilidad para para habilitar una aplicación.
- Visibilidad centralizada de la topología, los elementos y el funcionamiento de la red.

Por supuesto que hay que solucionar algunas limitaciones. Las organizaciones requieren mayores capacidades de sus redes para administrar su propia transformación digital.

El área de tecnología debería esperar:

- Traducción automática de políticas comerciales a políticas de TI en cuanto a seguridad.
- Despliegue automatizado de estas políticas
- Garantía de recepción de notificaciones proactivas ante el incumplimiento de esas políticas.

Las redes no tuvieron cambios desde hace más de 30 años hasta este cambio de paradigma.

Los enrutadores y conmutadores convencionales tienen una estrecha integración entre los planos de control y de datos, que realizaba depuración de problemas de configuración o control del comportamiento del enrutamiento, una tarea muy desafiante y complicada. Para enfrentarse a dicha tarea, la idea de separar ambos planos empezó a florecer con distintos enfoques.

Debido al crecimiento de Internet, las empresas de equipos hardware comenzaron a implementar la lógica de reenvío de paquetes en hardware (plano de datos), separada del plano de control y los ISP a luchar para poder gestionar sus redes crecientes y poder aportar a sus clientes servicios que las hiciesen más seguras (como las VPN). Todo esto dio lugar a dos innovaciones principales: una interfaz abierta entre ambos planos.

El desarrollo de las SDN se iniciaron a partir de 1990, donde se incluye funciones programables en la red, en el 2001- 2007, se separó el plano de control y de datos mejorando con esta innovación, a partir del 2007-2010, se implementa los API Open Flow, se presenta como una interfaz abierta, presenta diversas maneras la separación del plano de control y de datos para que sea escalable, práctica donde virtualización jugó un rol importante en esta evolución de SDN.

Por qué deberíamos pensar en una SDN:

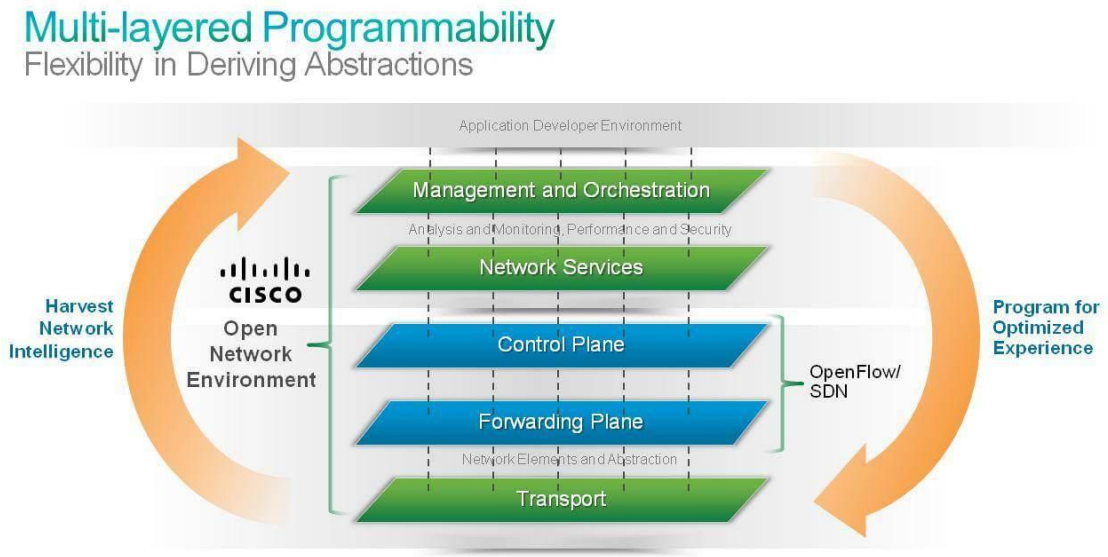
Cuando lo grandes centro de datos no pueden responder ante grandes picos de demanda.

Si pasara esto podríamos escalar la red, aumentando los costos de infraestructura y tiempo para la configuración.

Si necesitamos cambios rápidos SDN podría ser la solución. El tráfico de las redes por internet incluyendo redes sociales pueden necesitar cambios rápidos en determinado lugar geográfico.

Una red definida por software permite:

- Ser compatible con el movimiento dinámico, la duplicación y la asignación de recursos virtuales
- Facilitar la carga administrativa de la configuración y suministro de funciones como calidad de servicios y seguridad
- Implementar y ampliar con mayor facilidad las funciones de la red
- Diseñar el tráfico con una vista de extremo a extremo de la red
- Utilizar mejor los recursos de red
- Reducir el OPEX (costo operativo)
- Hacer que las funciones de red evolucionen más rápido basándose en el ciclo vital de desarrollo de un software
- Habilitar aplicaciones para solicitar dinámicamente servicios a la red
- Implementar una función de seguridad más efectiva
- Reducir la complejidad



En este tipo de redes, el administrador de red puede modificar el comportamiento de los conmutadores cuando sea necesario dando o quitando prioridad a paquetes hasta un nivel detallado.

Eso es especialmente útil en una arquitectura de computación en nube porque permite al administrador manejar cargas de tráfico de manera flexible y más eficiente. Esencialmente, esto permite al administrado usar menos conmutadores pequeños y costosos y tener más control que nunca sobre el flujo del tráfico de red.

En la actualidad, existe una especificación para crear una SDN. Es un estándar abierto llamado OpenFlow.

OpenFlow permite a los administradores de red controlar tablas de enrutamiento de forma remota.

OpenFlow no es lo mismo que SDN, es sólo un elemento que forma parte de la arquitectura SDN. OpenFlow es un estándar abierto para un protocolo de comunicaciones que permite al plano de control interactuar con el plano de datos (OpenFlow, sin embargo, no es el único protocolo disponible o en desarrollo para SDN)

SDN es posible porque los planos de red ya no están enlazados a los propios dispositivos de red. Sin embargo, otras entidades, usan los planos de red.

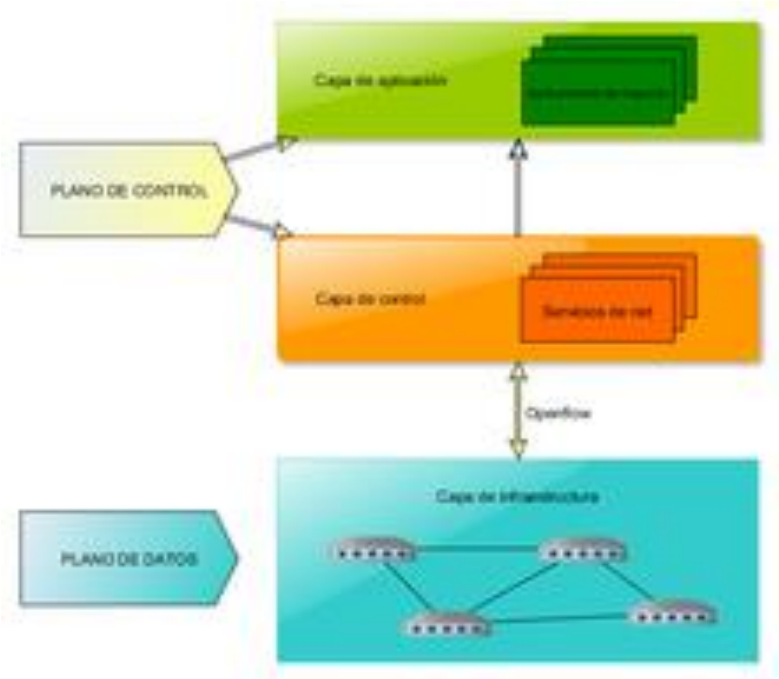


Ilustración 1 Arquitectura simplificada SDN utilizando openFlow

También permite administrar la red del centro de trabajo de forma dinámica, lo que proporciona una manera automatizada y centralizada de cumplir los requisitos de las aplicaciones y las cargas de trabajo.

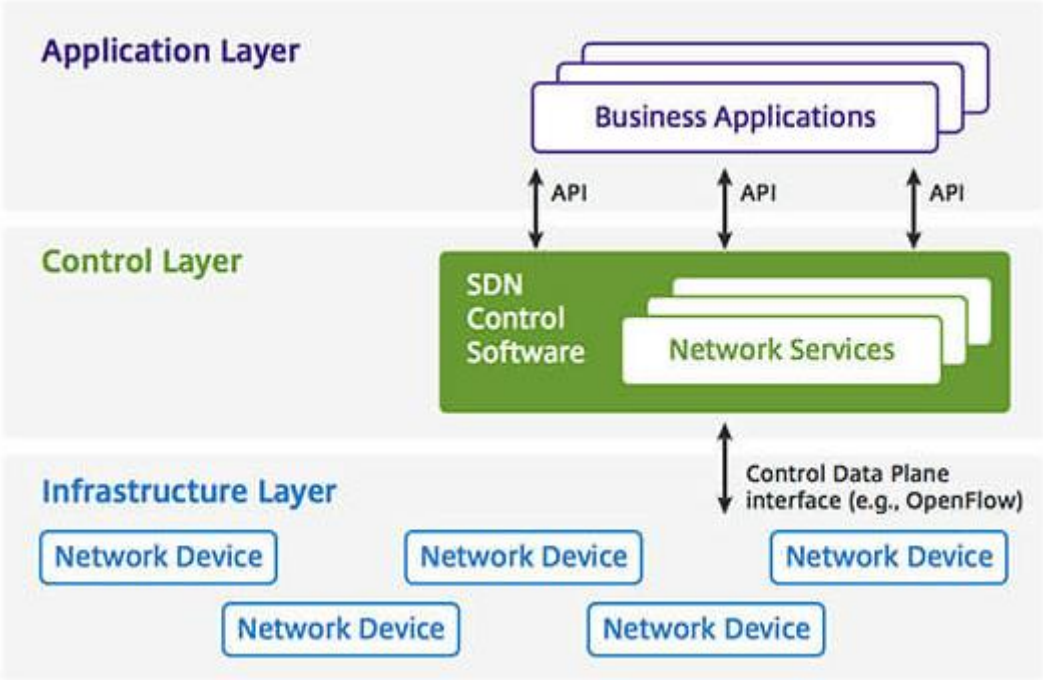


Ilustración 2 Arquitectura de SDN utilizando OpenFlow

Las redes definidas por software (SDN) ofrecen una red centralizada y programable que consiste en un controlador SDN, API descendentes y API ascendentes.

- Los controladores SDN son los cerebros de la red, ya que ofrecen una vista centralizada de toda la red.
- Las API descendentes transmiten información a los switches y routers de la red.
- Las API ascendentes se comunican con las aplicaciones y los servicios de implementación.

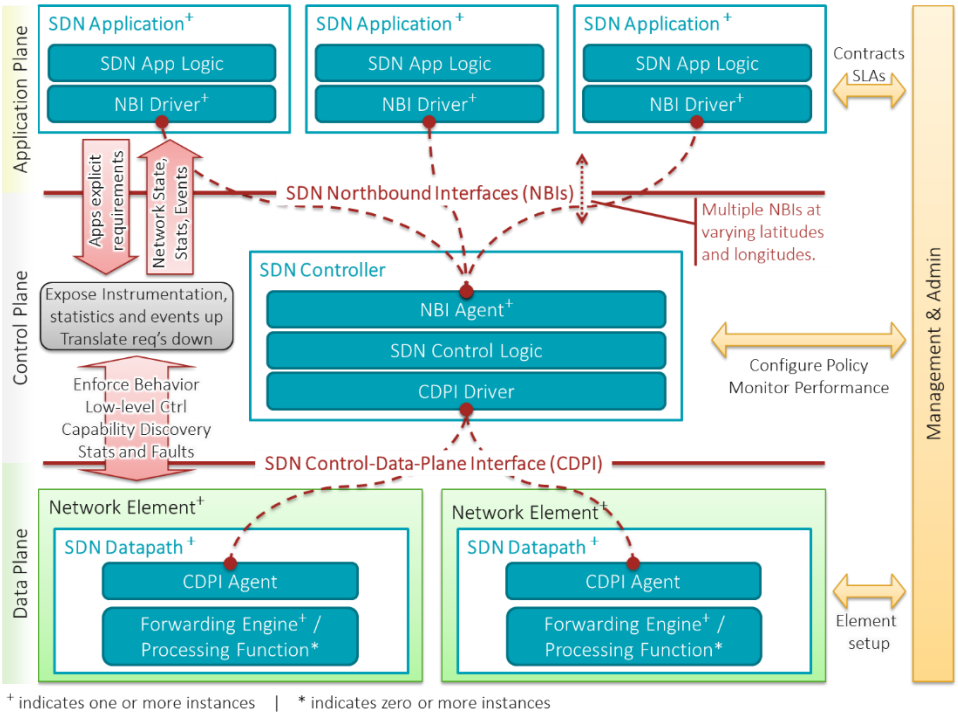


Ilustración 3 Visión esquemática de SDN

¿Cuál es la relación entre las SDN y la NFV?

La virtualización de funciones de red (NFV) utiliza tecnología de hipervisor y computación en la nube para la organización y la automatización de la red. La NFV funciona mejor en el contexto de los servicios de red (OSI nivel 4 y superior) que requieren una alta potencia de cálculo con un rendimiento del ancho de banda de bajo a medio.

Las SDN combinan la administración de servicios de redes y de aplicaciones en plataformas de organización centralizadas y

extensibles. Las SDN son óptimas para el reenvío de red de alto rendimiento (OSI niveles 0 a 3) donde las cargas de trabajo con uso intensivo del ancho de banda necesitan una administración de tráfico significativa.

Este es un desglose de los componentes vitales de una red definida por software:

Aplicaciones empresariales

Esto hace referencia a aplicaciones que sean directamente consumibles por los usuarios finales. Las posibilidades incluyen videoconferencias, administración de la cadena de suministro y administración de la relación con los clientes.

servicios de red y seguridad

Esto hace referencia a las funciones que permiten que las aplicaciones empresariales tener un rendimiento eficaz y seguro. Las posibilidades incluyen una amplia gama de funciones capacidades de seguridades como firewalls, ids/ips y protección frente a ataques de denegación de servicio.

Conmutador SDN puro

En un conmutador SDN puro, todas las funciones de control de un interruptor tradicional (como los protocolos de enrutamiento que se usan para crear bases de información de redireccionamiento) se ejecutan en el controlador central. La funcionalidad del conmutador está restringida por completo al plano de datos.

Conmutador híbrido

En un conmutador híbrido, las tecnologías SDN y los protocolos de conmutación tradicionales se ejecutan a la vez. Un administrador de redes puede configurar el controlador de SDN para descubrir y controlar ciertos flujos de tráfico mientras unos protocolos de redes tradicionales distribuidos siguen dirigiendo al resto del tráfico en la red.

Red híbrida

Una red híbrida es una red en la que los conmutadores tradicionales y los conmutadores SDN, tanto si son conmutadores SDN puros como híbridos, operan en el mismo entorno.

Api ascendente

El api ascendente permite comunicaciones entre la capa de control y la capa de aplicaciones empresariales. Actualmente no hay un api ascendente que se base en estándares.

Api descendente

El api descendente permite comunicaciones entre las capas de control y de infraestructura. Los protocolos que pueden permitir esta comunicación incluyen openflow, el protocolo de presencia y mensajería extensible (xmpp) y el protocolo de configuración de la red.

En el área de la administración de redes se han considerado como herramientas de evaluación de red además de OpenFlow, a ENVI y SAGE, que se desarrollaron para realizar la funcionalidad de gestión de SDN aplicado en la red de grado de operador, extendiendo la arquitectura SDN para admitir funciones de administración de red de múltiples proveedores.

Se ha presentado un marco de control de red basado en eventos, a saber, Lithium, que facilita la gestión de la red. También se usa bancos de pruebas llamado BISmark para implementar medidas y aplicaciones en redes de acceso de banda ancha.

Este banco de pruebas puede recopilar información sobre la topología de la red, la disponibilidad, la accesibilidad, etc.

De igual manera se ha diseñado e implementado "Procera" que simplifica diversos aspectos de las operaciones y de la administración de la red, y sirve como el enlace entre las políticas de red de alto nivel, y las configuraciones de red de bajo nivel.

En relación con las aplicaciones de calidad de servicio se utilizan APIs (application programming interface) QoS basadas en controladores SDN, que proporcionan control automatizado de QoS.

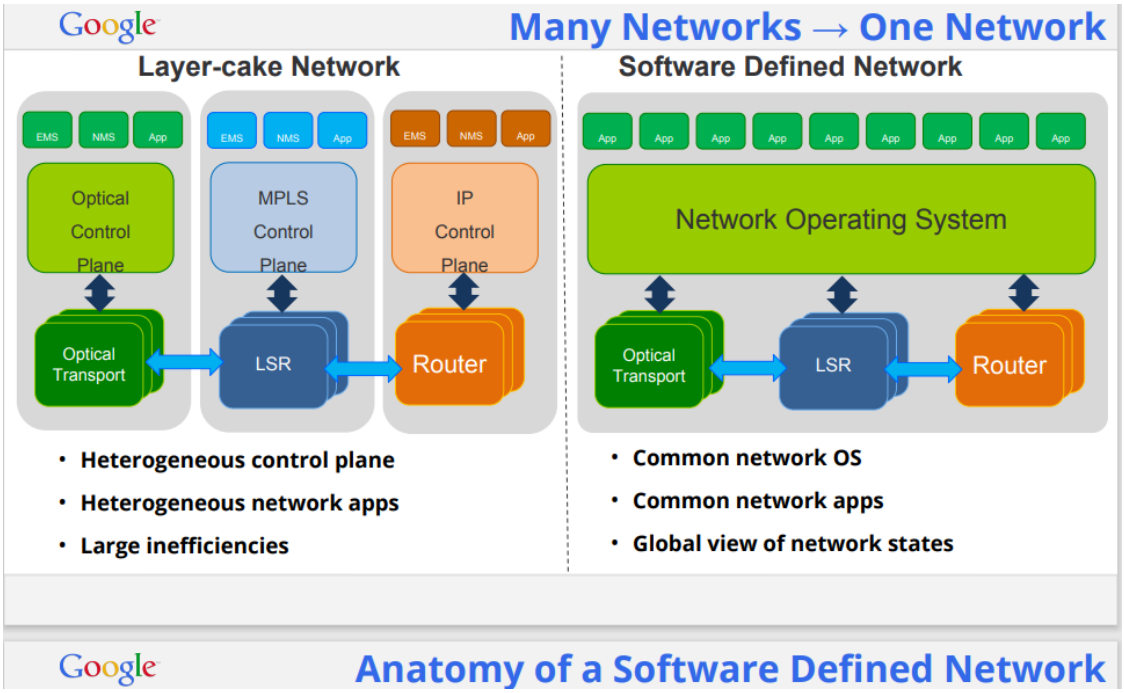
Se han propuesto el marco OpenQoS para garantizar la entrega de video sin interrupciones con soporte QoS de extremo a extremo.

También se diseñan marcos de optimización para el enrutamiento de la QoS. OpenQFlow ha sido propuesto para soportar SDN escalable y con estado, proporcionando QoS basado en micro flujo.

Se ha estado estudiando también una arquitectura que puede incorporar flujos de QoS en el entorno OpenFlow para admitir la transmisión de video escalable.

En SDN se está implementando redes de centros de datos con redes definidas por software (DCN - datacenter network) para mejorar el rendimiento de la red.

Google implementa SDN en una red privada de área amplia (WAN) que conecta centros de datos para construir la arquitectura B4, La WAN B4 se basa en enrutadores caseros que tienen cientos de puertos que se ejecutan a velocidades de 10Gb/seg, logrando un control total sobre toda la red para maximizar la utilización de enlaces.



Se ha estado utilizando el controlador NOX a DCN, abordando una variedad de requisitos de centros de datos. Igualmente se ha construido una plataforma de prueba con OpenFlow para medir y analizar el DCN (datacenter network) conscientes de la energía (energy-aware DCN).

Se ha propuesto también una nueva arquitectura de centro de datos con conmutación con filtros fijos en paquete (SiBF - switching with in-packet bloom filters), transformando los DCN en un problema de software.

También se ha utilizado la tecnología SDN para diseñar una solución para manejar la congestión de los centros de datos DCN.

La computación en la nube en redes definidas por software proporciona las denominadas infraestructura como servicio (IaaS - Infrastructure-as-a-Service), la plataforma como servicio (PaaS - Platform-as-a-Service) y el software como servicio (SaaS - Software-as-a-Service). Sin embargo, es difícil proporcionar una red como servicio (NaaS - Network-as-a-Service) debido al control limitado sobre los recursos de la red.

La SDN proporciona interfaces de usuario potentes para controlar redes, lo que hace posible implementar NaaS. Ha sido desarrollado un prototipo de una red basada en la nube al extender la arquitectura OpenFlow, para realizar un modelo de capacidad de red de pago por uso.

De forma similar se ha aprovechado las técnicas de la tecnología SDN para construir un novedoso sistema de red en la nube, denominado CloudNaaS, que proporciona muchas funciones de red virtual.

Se ha propuesto una nueva plataforma SDN, la denominada “Meridian” para soportar un modelo de servicio de red de computación en la nube. También centros de investigación han diseñado una biblioteca de algoritmos gráficos, que puede cargarse en un controlador SDN para la gestión de la red en la nube.

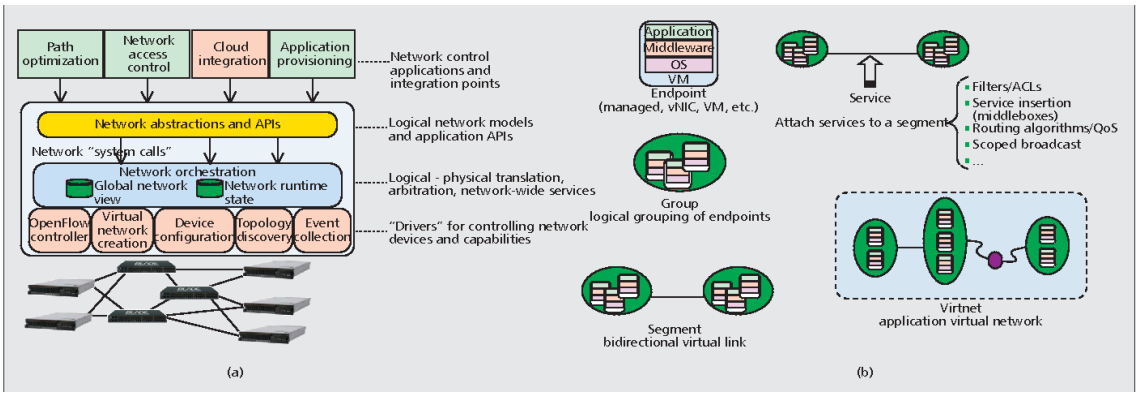


Ilustración 4 Merirdian SDN Cloud networking y b) Meridan service model

Diversas aplicaciones para la red definidas por software SDN se aplican en el desarrollo del Internet de las cosas (IoT). Ha sido construido un sistema de gestión móvil en la nube basada en SDN, que se beneficia de la configuración dinámica de los conmutadores OpenFlow.

Varios grupos de investigación han abordado los problemas de movilidad en las redes del Protocolo de Internet (IP) que utilizan SDN al diseñar un protocolo de movilidad basado en OpenFlow. Se ha presentado un marco de gestión de red basado en SDN llamado FlowComb para el procesamiento de la big data.

De la misma forma se ha integrado una función de control de red proporcionada por un controlador SDN en "Haddop" para optimizar el rendimiento del procesamiento de la big data y la utilización de la red.

Es muy importante el desarrollo y los estudios que se realizan sobre el diseño y la implementación de aplicaciones SDN en los centros de datos distribuidos.

Se debe aprovechar el control central proporcionado por la tecnología SDN para abordar el problema de asignación de solicitudes en centros de datos distribuidos. Primero, es primordial analizar los modelos de optimización conjunta desde la perspectiva de los proveedores de servicios y de los usuarios finales.

En segundo lugar, tener un dominio sobre el método basado en la solución de negociación de Nash (NBS - Nash bargaining solution) para modelar los requisitos tanto de los proveedores como de los usuarios finales. Tercero, se debe alcanzar un conocimiento referente

al desarrollo de algoritmos eficientes que combinen las ventajas de la técnica de suavizado logarítmico y del método de la variable auxiliar.

También es importante realizar muchos experimentos basados en trazas del mundo real, para mostrar la eficiencia de estos algoritmos de asignación de solicitudes.

En la implementación de las redes SDN en los centros de datos distribuidos, se tienen que plantear soluciones efectivas en la ubicación de los controladores SDN.

Primero, se debe adecuar la nueva métrica de ubicación, para poder implementar múltiples controladores en redes a gran escala. En segundo lugar, se debe reformular el problema de la ubicación óptima del controlador como un ILP (Integer Linear Programming) y utilizar un algoritmo de aproximación efectivo, para encontrar su solución.

Además, se deben realizar experimentos intensivos basados en muchos tipos de topologías reales, para demostrar que las estrategias se pueden mejorar significativamente, en cuanto al rendimiento sobre los métodos existentes.

La tecnología SDN busca garantizar el rendimiento de la gestión de la red en los centros de datos distribuidos, diseñando e implementando sistemas de gestión de controladores SDN.

Estos sistemas constan de módulos de gestión de un controlador heterogéneo (HCM - heterogeneous controller management), de un módulo de gestión de relaciones de dominio (DRM - domain relationships management), de un módulo de base de datos (database module) y de un módulo de terminal (front-end module).

Esto, con el fin de proteger las diferencias entre los controladores heterogéneos y proporcionar una interfaz gráfica de usuario (GUI - graphical user interface) unificada para los usuarios y los administradores.

Es muy importante en el diseño e implementación, el desarrollo de aplicaciones SDN para los centros de datos distribuidos, y también destacar el planteamiento futuro, de avanzar aún más en nuevas áreas de investigación y desarrollo, que estén relacionadas con la tecnología de las redes SDN, con la esperanza de proporcionar información y conocimiento valioso, a los investigadores e ingenieros en este campo, en constante expansión.

REDES ADMINISTRATIVAS

UNIDAD 4: PROTOCOLOS DE ENRUTAMIENTO Y TRANSPORTE

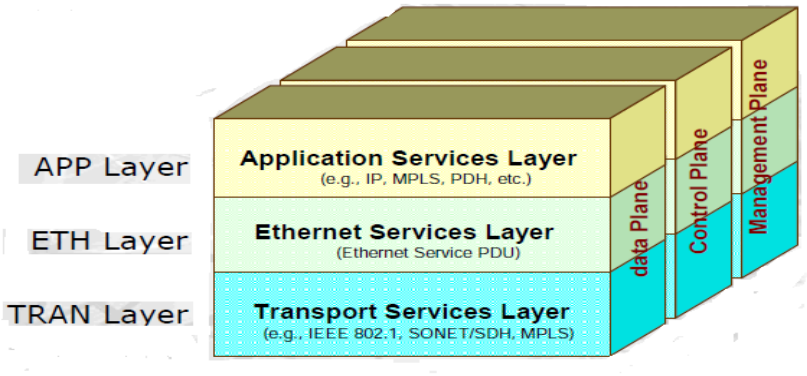
CLASE 10 METRO ETHERNET

Claudio Milio 2020

Bienvenidos a la clase 10, en esta ocasión verá conceptos de la red metro ethernet.

HISTORIA Y ESTANDARES de ETHERNET

Ethernet es un conjunto de estándares para la capa física y la capa MAC, para la transmisión de datos.



Fue Inventado por Robert M. Metcalfe en 1973 cuando trabajaba en Xerox y fue estandarizado por la IEEE bajo el estándar 802.3.

Los datos trasmitidos se encapsulan en tramas. Históricamente, existen dos tipos de tramas:

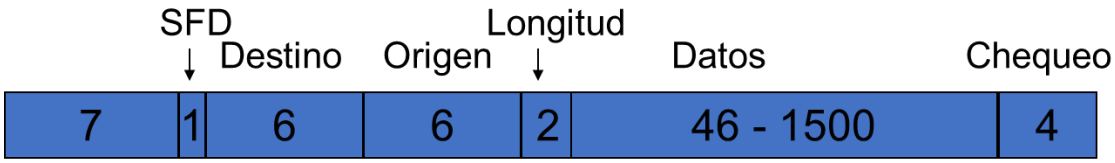
- 802.3 Framing usa en campo de longitud de trama (Length) después del campo de Source Address.
- Ethernet II (DIX) Framing usa (usaba) el campo de tipo de trama (type) despues del campo Source Address

Ambos tipos de tramas están definidos y soportados dentro de IEEE 802.3.

suplemento	año	descripción
802.3a	1985	Original 802.3: 10BASE-5 10BASE-2 10BROAD-36
802.3c	1986	Especificaciones de repetidores
802.3d	1987	FOIRL (enlace de fibra)
802.3i	1990	10Base-T Ethernet sobre par trenzado de cobre
802.3j	1993	10Base-F Ethernet sobre fibra
802.3u	1995	100Mbps Ethernet
802.3x e 802.3y	1997	operación full duplex
802.3z	1998	1000Base-X (Gigabit Ethernet)
802.3ab	1999	1000Base-T (GE sobre par trenzado)
802.3ac	1998	Extensiones de trama (hasta 1522 bytes) para VLANs
802.3ad	2000	link aggregation
802.3ae	2002	10 GE
802.3af	2003	PoE (Power over Ethernet). Hasta 15W
802.3ah	2004	Ethernet in First Mile
802.3an		10 Gbase-T (en draft)
		Bridging en 802.1D
802.1w		Cambios y mejoras en el spanning tree
802.1s		Múltiples spanning trees

Ilustración 1 Estándares 802.3 de la IEEE

El tamaño de la trama varía desde 64 a 1518 Bytes.



Casi el 100% del tráfico se inicia y termina en un puerto Ethernet. Metro Ethernet aparece como una elección por menores costos y por su performance.

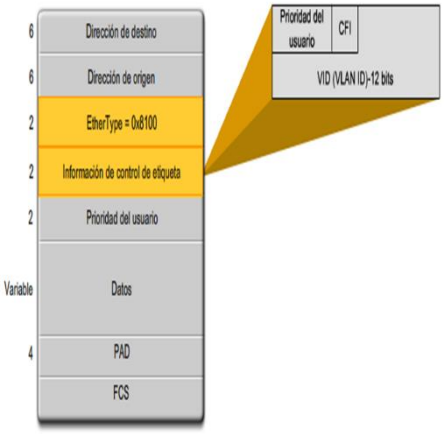
Es un diseño de red que proporciona conectividad de banda ancha para redes privadas y servicios de transporte necesarios, tales como Internet de alta velocidad dentro de un área metropolitana.

Metro Ethernet hoy en día es un servicio ofrecido por los proveedores de telecomunicaciones para interconectar LANs ubicadas a grandes distancias dentro de una misma ciudad, ejecutando un transporte WAN.

Esta red está basada en el estándar Ethernet, y que cubre un área metropolitana.

Es comúnmente usada como una red metropolitana de acceso para conectar a las empresas a los abonados y una red de área extensa, como la Internet.

Los switches son dispositivos de Capa 2. Sólo utilizan la información del encabezado de la trama de Ethernet para enviar paquetes.



El encabezado de la trama no contiene la información que indique a qué VLAN pertenece la trama.

Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen.

Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q.

Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama

METRO ETHERNET

Pero… ¿Qué es una red Metro Ethernet?

Red Metro Ethernet es cualquier red que está destinada a suministrar servicios Metro Ethernet.

Los servicios Metro Ethernet son servicios de conectividad MAN/WAN de nivel 2 a través de UNIs Ethernet.

La red del proveedor puede implementarse con varias opciones de transporte.

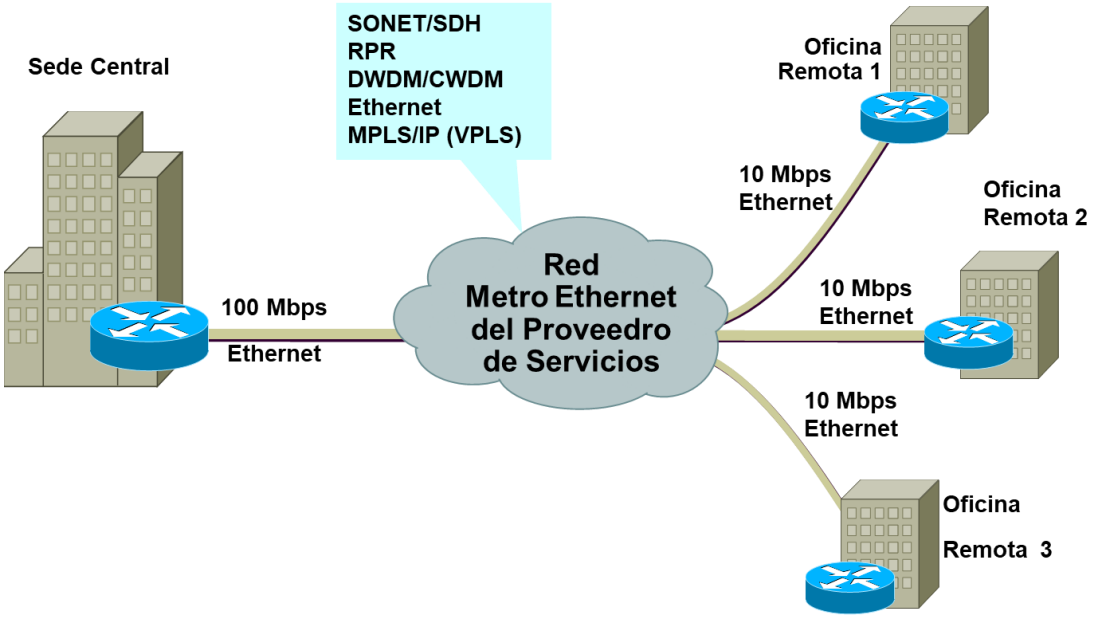
Ethernet se ha convertido en una tecnología única para LAN, MAN y WAN.

Es una arquitectura eficiente para redes de paquetes, punto a punto, punto multipunto y multipunto a multipunto

Ofrece flexibilidad de ancho de banda: 10/100/1000/10000 Mbps

Originalmente fue utilizada sólo en entornos LAN, pero hoy ofrece independencia geográfica: Ethernet óptico, sobre IP o MPLS.

Existe un precedente antiguo que es ELAN. ELAN es una emulación LAN (sobre ATM)



Las redes Metro Ethernet, están soportadas principalmente por medios de transmisión guiados, como son el cobre (MAN BUCLE) y la fibra óptica, existiendo también soluciones de radio licenciada.

La tecnología de agregación de múltiples pares de cobre, (MAN BUCLE), permite la entrega de entre 10 Mbit/s, 20 Mbit/s, 34 Mbit/s y 100 Mbit/s, mediante la transmisión simultanea de múltiples líneas de cobre, además esta técnica cuenta con muy alta disponibilidad ya que es imposible la rotura de todas las líneas de cobre y en caso de rotura parcial el enlace sigue transmitiendo y reduce el ancho de banda de forma proporcional.

La fibra óptica y el cobre se complementan de forma ideal en el ámbito metropolitano, ofreciendo cobertura total a cualquier servicio, a desplegar.

Algunos servicios son:

- Conectividad Internet
- Transparent LAN service (punto a punto LAN to LAN)
- L2VPN (punto a punto o multipunto a multipunto LAN to LAN)
- Extranet

- LAN a Frame Relay/ATM VPN
- Conectividad a centro de backup
- Storage area networks (SANs)
- Metro transport (backhaul)
- VoIP

Algunos se están ofreciendo desde hace años. La diferencia está en que ahora se ofrecen usando *conectividad Ethernet*

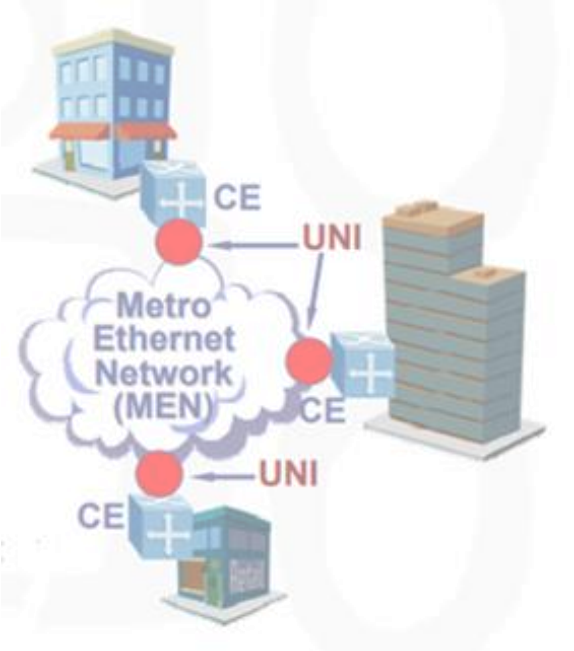
QUE OFRECE ETHERNET COMO TECNOLOGIA DE TRANSPORTE LAN/WAN/MAN

Ethernet se ha convertido en una tecnología única para LAN, MAN y WAN.

Además de la flexibilidad del ancho de banda, ofrece una arquitectura eficiente para redes de paquetes, punto a punto, punto multipunto y multipunto a multipunto.

También ofrece independencia geográfica: Ethernet óptico, sobre IP o MPLS.

A continuaciones muestra el modelo de referencia:



El equipamiento de usuario (CE) se conecta a través de la UNI.

El CE puede ser un router, un Bridge IEEE 802.1Q (switch)

El UNI es el User Network Interface. Corresponde al estandar IEEE 802.3 Ethernet PHY and MAC

Soporta varias clases de servicio (QoS).

ƒ Metro Ethernet Network (MEN), puede usar distintas tecnologías de transporte y de provisión de servicios como: ƒ SONET/SDH, WDM, PON, RPR, MAC-in-MAC, QiQ (VLAN stack), MPLS.

Sobre el anterior modelo, se añade un cuarto ingrediente: una Ethernet Virtual Connection (EVC).

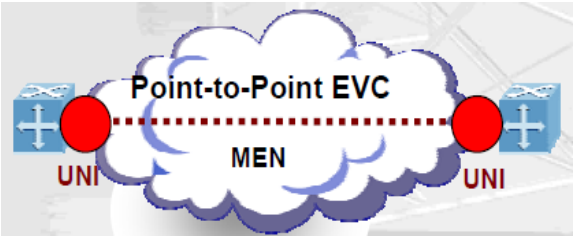
ETHERNET VIRTUAL CONNECTION (EVC)

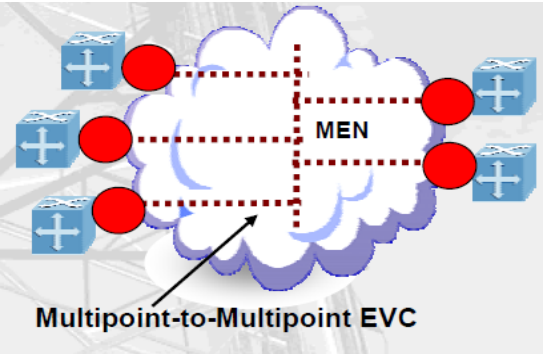
EVC es una asociación entre dos o más UNIs. Es creada por el proveedor del servicio para un cliente.

Una trama enviada en un EVC puede ser enviada a uno o más UNIs. Nunca será enviada de vuelta al UNI de entrada. tampoco será enviada a un UNI que no pertenezca al EVC.

Las EVC´s pueden ser:

- Punto a punto (E-Line)
- Multipunto a multipunto (E-LAN)
- Cada tipo de servicio ethernet tiene un conjunto de atributos de servicio y sus correspondientes parámetros que definen las capacidades del servicio. Servicio Ethernet – M

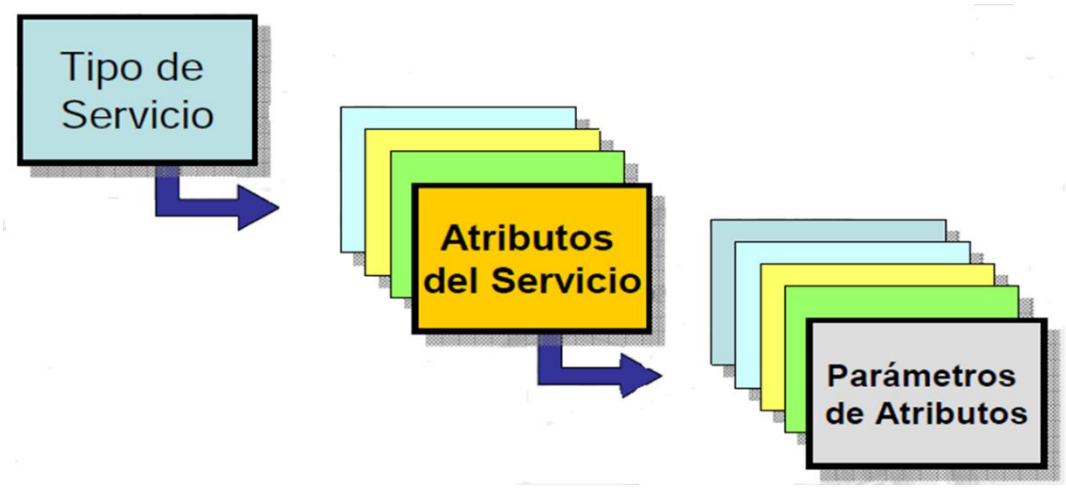




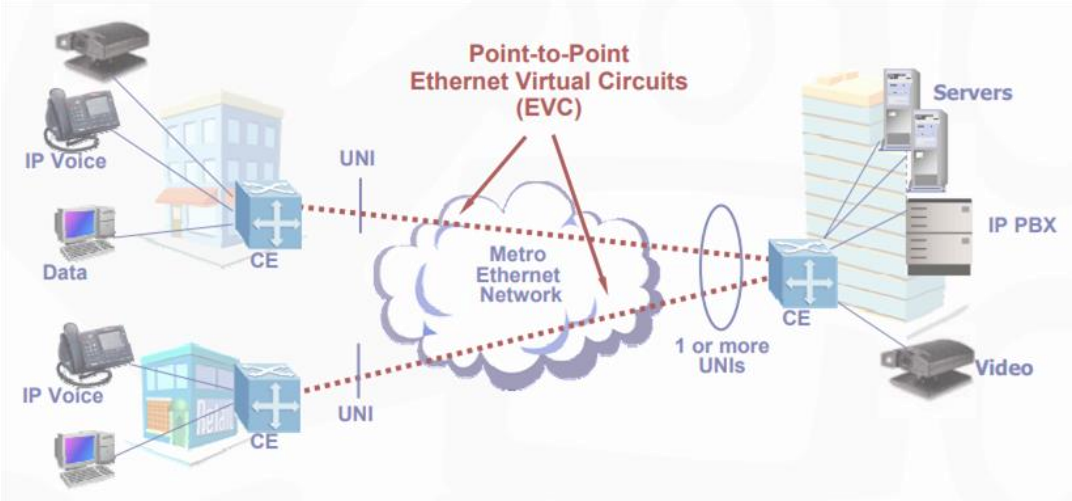
Los servicios Metro Ethernet services no necesitan que toda la red de nivel 2 sea ethernet; tambien puede ser:

- Ethernet over SONET/SDH (EOS)
- Resilient Packet Ring (RPR)
- Ethernet Transport
- Ethernet sobre MPLS

Los distintos servicios se rigen por una jerarquía para definir las capacidades de este:



SERVICIO ETHERNET E-LINE



Una E-Line puede operar con ancho de banda dedicado ó con un ancho de banda compartido.

EPL, Ethernet Private Line, es un servicio EVC punto a punto con un ancho de banda dedicado. El cliente siempre dispone del CIR.

Normalmente opera en canales SDH (en NGN) o en redes MPLS.

Es como una línea en TDM, pero con una interfaz ethernet

EVPL: Ethernet Virtual Private Line.

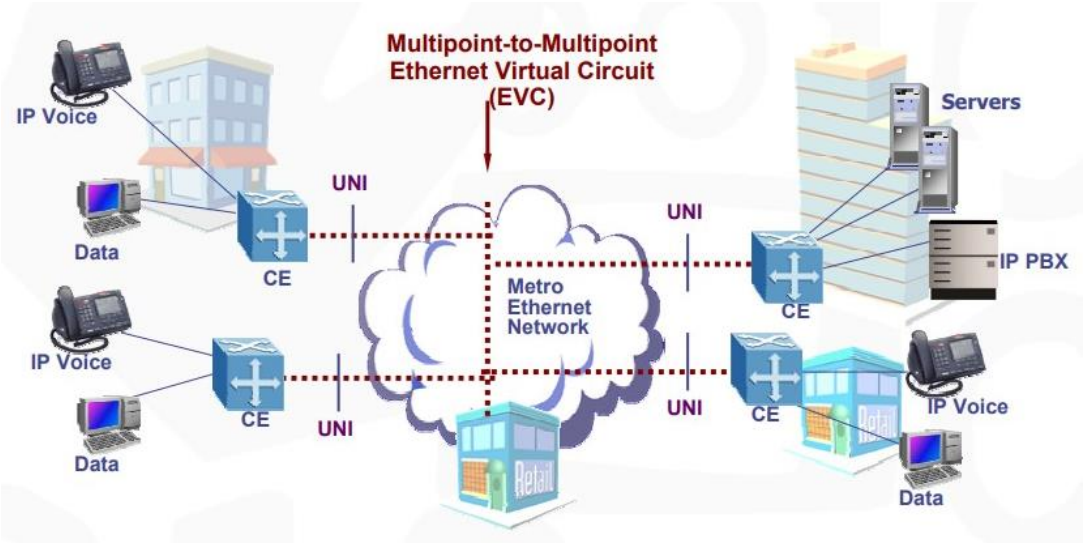
En este caso el cliente dispne de un CIR.

Es similar a Frame Relay. Se suele implementar con canales TDM compartidos o con redes de conmutación de paquetes usando Switchs y/o routers.

SERVICIO ETHERNET E-LAN

Servicio Ethernet LAN (E-LAN).

Este servicio provee conexión multipunto. Cada sitio (UNI) es conectado a el EVC multipunto y se pueden establecer diversos rate para cada UNI (ej: UNI 1 y 3 10Mbps - UNI 2 y 4: 100Mbps).



Una E-LAN puede operar con ancho de banda dedicado o con un ancho de banda compartido.

Red de SW´s interconectados por fibra ó WDM:

- Bueno para "best efforts"
- Redundancia por STP, FSTP ó EAPS. No hay proteccion sub-50 ms.
- También se puede implementar sobre SDH (NGN) (ITU-T)
- También se puede implementar sobre una red de paquetes usando MPLS (IETF), L2TP ó Q-in-Q

EPLan: Ethernet Private LAN

Suministra una conectividad multipunto entre dos o más UNI´s, con un ancho de banda dedicado.

EVPLan: Ethernet Virtual Private LAN

Otros nombres:

VPLS: Virtual Private Lan Service

TLS: Transparent Lan Service

VPSN: Virtual Private Switched Network

Está limitado a4.96 VLAN.

Es el servicio más rentable desde el punto de vista del proveedor.

CATEGORIAS Y ATRIBUTOS DE SERVICIO

Las categorías se agrupan en:

- Ethernet Physical Interface (UNI)
- Traffic Parameters (EVC)
- Performance Parameters (EVC)
- Class of Service (EVC)
- Service Frame Delivery (EVC)
- VLAN Tag Support (UNI)
- Service Multiplexing (UNI)

- Bundling UNI)
- Security Filters (UNI)

Atributos de UNI:

- identificador, tipo de medio, velocidad, duplex, etc)
- Atributo de soporte de VLAN tag
- Atributo de multiplexación de servicio
- Bundling attribute
- Security filters attribute

Atributos de EVC:

- Parámetros de tráfico (CIR, PIR, in, out, etc)
- Parámetros de prestaciones (delay, jitter, etc)
- Parámetros de Clase de Servicio (VLAN-ID, valor de .1p, etc)
- Atributo de Service frame delivery
- Unicast frame delivery
- Multicast frame delivery

Parámetros de tráfico

Se define un Bandwith Profile (B.P), que está compuesto por 4 parámetros que definen el bandwidth o throughput del servicio

- CIR (Committed Information Rate)
- CBS (Committed Burst Size)
- EIR (Excess Information Rate)
- EBS (Excess Burst Size)

Existe un Service Frame Color, el color de la trama determina qué tipo de B.P tiene.

Un servicio puede tener 2 o más colores.

CIR (Committed Information Rate) Es el rate promedio el cual las tramas pueden ser transmitidas por la red de acuerdo a una performance establecida (ej: SLA)

CBS (Committed Burst Size) Es el tamaño que deben tener las tramas para alcanzar ese CIR

EIR (Excess Information Rate) Es el rate promedio el cual las tramas pueden ser transmitidas por la red sin una performance establecida

EBS (Excess Burst Size) Es el tamaño que deben tener las tramas cumplir con él EIR

PARAMETROS DE PERFORMANCE

Frame delay (Retardo de trama)

Son retardos presentados en la transmisión, es un parámetro crítico y tiene un alto impacto en la QoS de las aplicaciones en tiempo real.

Frame Jitter

Es la variación de los retardos (delay), es un parámetro crítico en las aplicaciones de tiempo real, (Telefonía IP / video)

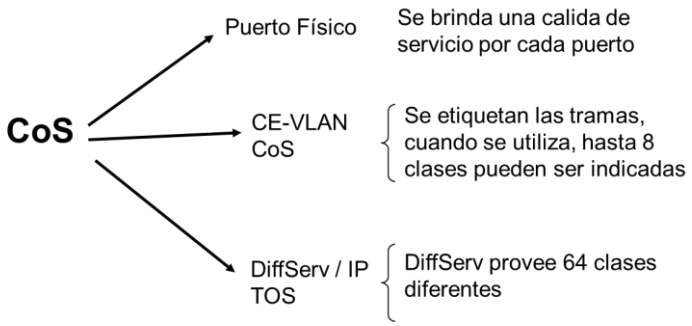
Frame loss (Pérdida de trama)

Es el porcentaje de tramas que no son transmitidas correctamente en un intervalo de tiempo, está definido como:

$$\left(1 \quad \frac{\textbf{Nro de Tramas entregadas al destino}}{\textbf{Total de tramas enviadas}} \right) \times 100$$

CLASE DE SERVICIO

Cada clase de servicio puede ofrecer diferentes niveles de desempeño, es utilizado por el proveedor de servicio para brindar distintas características de sus servicios



VLAN TAG SUPPORT

El cliente puede utilizar el etiquetado (tagged) en sus equipos y superponer dos VLAN ID (la propia y la del proveedor)

Para estos casos se ha detinido el término CE-VLAN ID (Customer Edge VLAN ID) en 802.

- CE-VLANID Presertavion

  Preserva el campo \rLAN ID del cliente sin alterarse a través del EVC .

- CE-VLANID CoS Presertavion

  Preserva los bits de Cos establecidos por el cliente sin alterarse a través del EVC.

Mapeo de VLAN IDs

Se da en los casos que una UNI soporta etiquetado y otra, donde el paquete irá, no los soporta

La red del proveedor debe quitar la etiqueta "VLAN cuando la trama irá a una UNI que no soporta etiquetado, para ello utiliza una tabla de mapeo de VLAND ID / EVC.

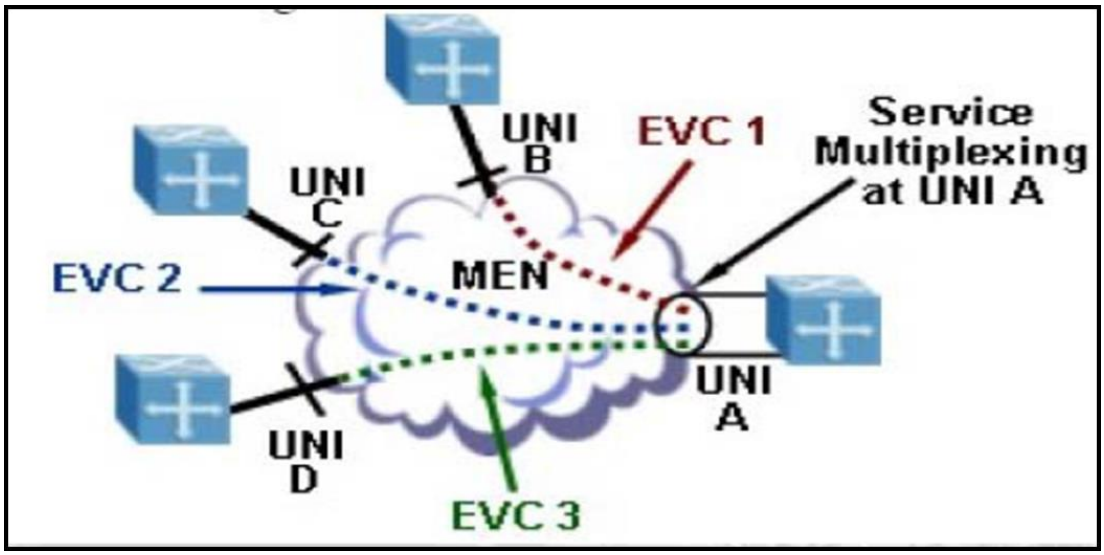
SERVICIO DE MULTIPLEXADO

Se utiliza para que una UNI soporte varios EVC

Reduce el costo de equipamiento

Ahorra espacio, energía y cableado

Simplifica las activaciones de nuevos



BUNDLING

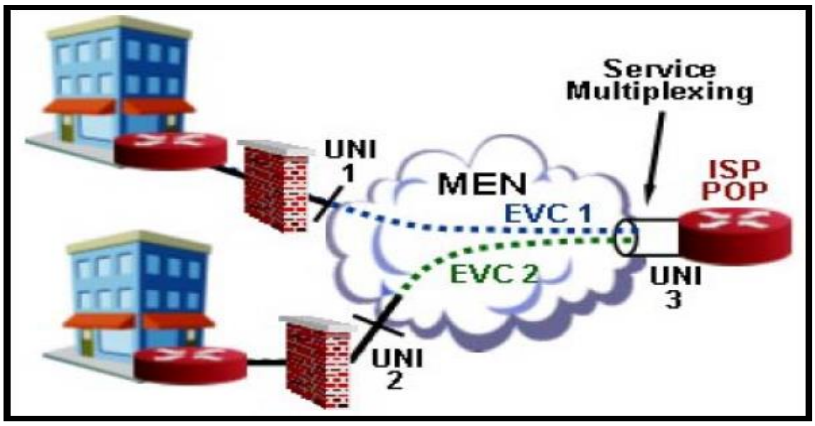
Este servicio permite que dos o mas CD VLAN Ids puedan ser mapeadas a un mismo EVC en la UNI

SECURITY FILTERS

Se pueden establecer Access Control List, para adicionar seguridad o administrar el tráfico.(por ej: lista de direcciones MAC a las cuales se les puede garantizar el acceso.

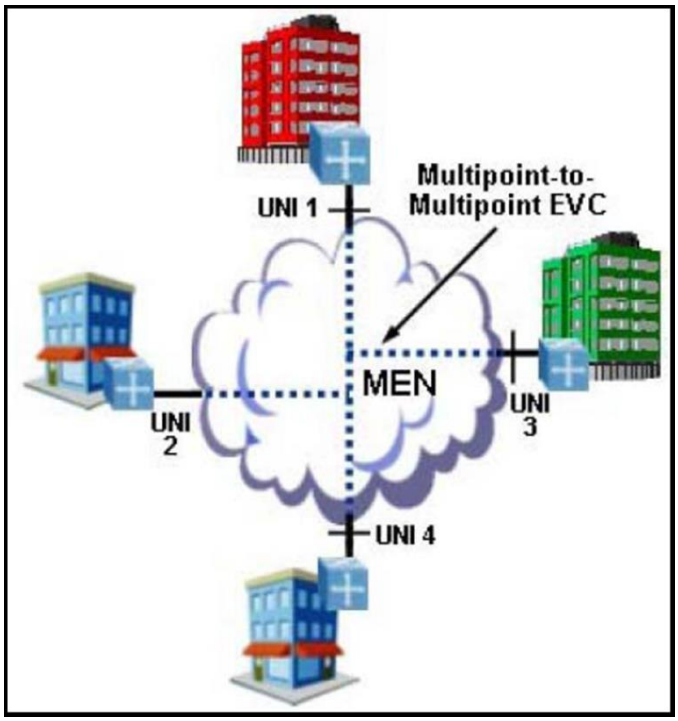
SERVICIOS OFRECIDOS

ACCESO A INTERNET DEDICADO.



El cliente tiene servicios E-Line separados (UNI 1 y 2), no es necesario el uso del tag VLAN ID y se utiliza el servicio de multiplexing (UNI 3).

EXTENSION DE LAN.



Lo más conveniente es usar un servicio E-LAN. Utiliza VLAN soportando (CE VLANIds).

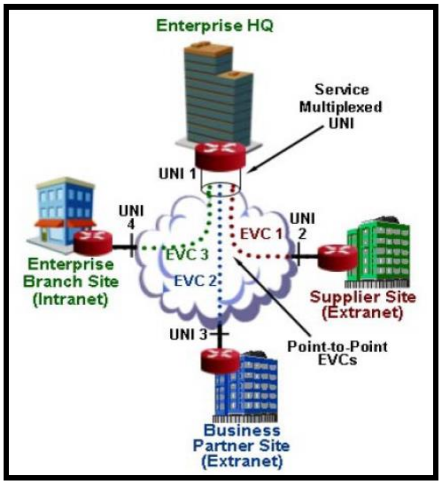
Todas las CE VLAN están mapeadas al mismo EVC y no utiliza multiplexing.

Si el cliente utilizará CoS se debe usar CoS preservation

INTRANET – EXTRANET L2 VPN.

En este caso se utilizan 3 EVC PtP. Utiliza VLAN soportando (CE VLAN Ids). Hay un mapeo de CE VLAN Ids con los EVC. También utiliza multiplexing.

Si el cliente utilizará CoS se debe usar CoS preservation



	CE-VLAN ID	EVC
CE-VLAN ID / EVC Map	10, 11, 12	1
	20, 21, 22	2
	30, 31, 32	3

METRO ETHERNET FORUM

La misión del FORUM es acelerar la adopción de la tecnología y servicios Ethernet a nivel de operador.

Objetivos.

Crear consenso y unir a los proveedores de servicios, proveedores de equipos y clientes finales sobre definición de servicio Ethernet, especificaciones técnicas y la interoperabilidad.

Facilitar la implementación de los estándares existentes y nuevos, la definición del servicio Ethernet, los procedimientos de prueba y las especificaciones técnicas del MEF para permitir la entrega de servicios

Ethernet y hacer una clase de operadores de redes de metro basadas en Ethernet.

Mejorar la conciencia mundial sobre los beneficios de los servicios Ethernet y las redes de transporte metropolitano basadas en la misma.

Las principales competencias del MEF son definir:

- Servicios Ethernet para las redes de transporte metropolitanas

  Dichos servicio deberán ser suministrados sobre redes Metro de Ethernet nativo y podrán estar soportadas por otras tecnologías de transporte

- Tecnologías de transporte de ethernet para áreas metro "carrier-class", especificando arquitecturas, protocolos y gestión
- Con menor prioridad el MEF también se encarga de definir:

  El trabajo que deben hacer otras organizaciones sobre otras tecnologías de transporte (actividad de enlace y coordinación)

  Interfaces no-ethernet, si no están definidas por otras organizaciones.

REDES ADMINISTRATIVAS

UNIDAD 5: REDES DE ACCESO RESIDENCIAL

CLASE 11 ADSL CATV

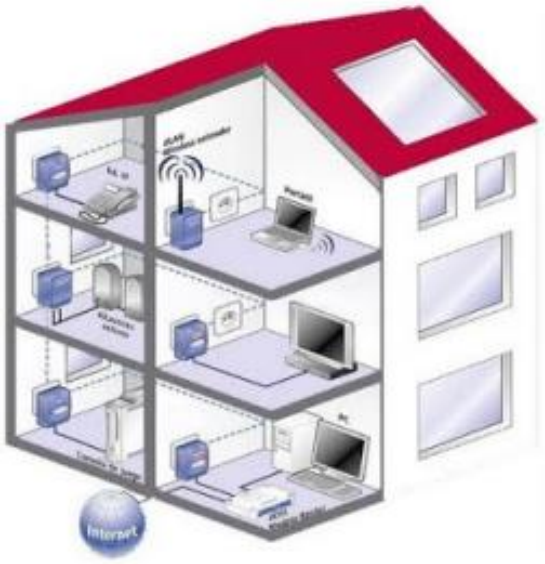
Claudio Milio 2020

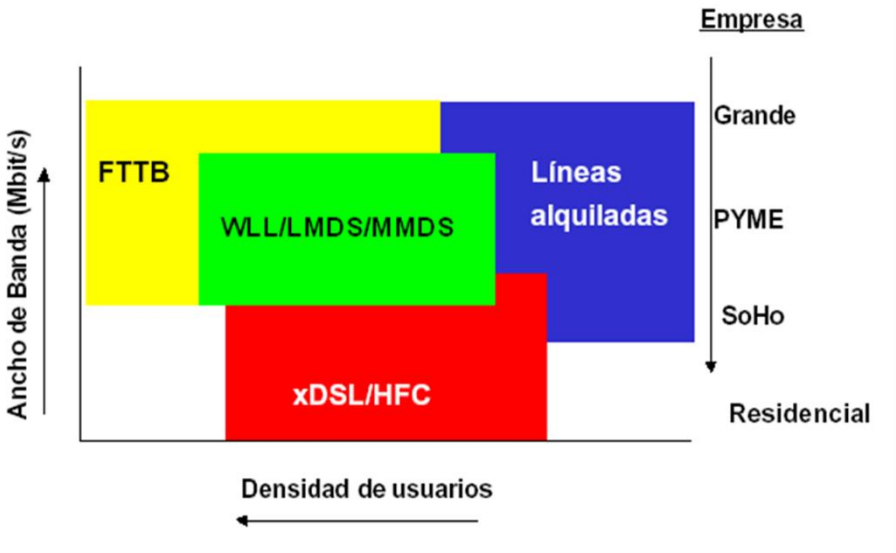
En esta clase vera las características de las redes de acceso residencial.

REDES DE ACCESO RESIDENCIAL

Parece trivial explicar el significado de una red doméstica. Todos tenemos uno o más dispositivos que están intercambiando información entre ellos y utilizando servicios de Internet.

En un principio, una computadora con un modem y una línea telefónica era suficiente para poder acceder a la información que estaba disponible. Luego, hemos ido sumando dispositivos y nuevas maneras de comunicarnos. Dispositivos como celulares, Tablet, televisores, impresoras, etc. conectados a través de switchs, router, cables UTP, Wi Fi, Bluetooth. Y todos esos dispositivos acceden de manera simultánea a internet. Los servicios de internet y cable actualmente llegan a nuestro hogar por medio del cable, de manera híbrida (cable y fibra) o por FTTH (Fiber To The Home).



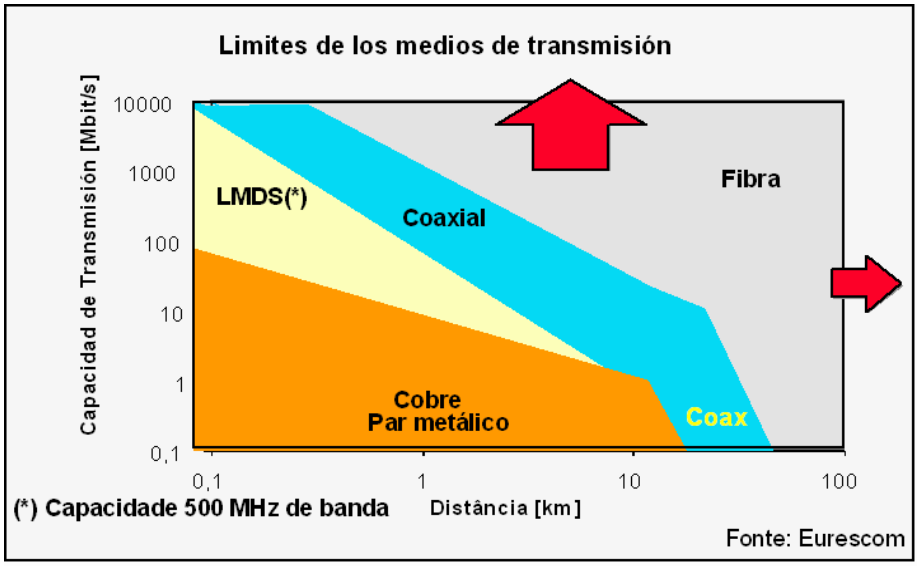


Referencias:

- FTTB – acceso a banda ancha sobre fibra óptica (fibra to building)
- WLL – bucle local inalámbrico.
- LMDS sistema de distribución local multipunto tecnología de conexión de radio.
- HFC híbrido de fibra y coaxial.

En el anterior gráfico podemos observar las distintas densidades de usuarios y el ancho de banda que consumen.

En la próxima figura se grafican los límites para cada medio.



TECNOLOGÍAS XDSL

Se define como una tecnología que permite el uso de la línea del teléfono (línea de cobre) para la transmisión de datos a alta velocidad y a la vez el uso de la línea telefónica.

Toda la información transmitida es digital y emplea el esquema del servicio tradicional de telefonía que consta de un bucle de abonado local.

Los últimos módems xDSL se aproximan a velocidades de 10 Mbit/s.

Existen tres técnicas de modulación para xDSL:

- La modulacion 2b1q donde una secuencia de dos bits se transmite como un pulso de cuatro niveles.
- Carrier-less amplitude phase modulation" (CAP). En este caso divide la señal modulada en segmentos que después almacena en memoria
- Discrete multitone modulation" (DMT) basado en el uso de múltiples portadoras. El rango de frecuencias usadas es dividido en bandas de frecuencia o canales.

DSL SIMETRICO

La velocidad de bajada como la de subida son iguales. Es ideal para aplicaciones que requieren simetría como Video Conferencia.

Existen diferentes tipos de DSL:

- High bit-rate DSL (HDSL)

  Es La primera tecnología simétrica DSL. Utiliza múltiples pares de cobre (2 o 3) para alcanzar altas velocidades.

  Su alcance es hasta hasta 4 Km a hasta 2 Mbps.

- SDSL: Línea Simple DSL (Single Line DSL). Es una versión de HDSL, también conocida como SHDSL, que utiliza un solo cable del par de cobre. Proporciona transferencia de datos

bidireccional y de alta velocidad, con un alcance máximo de 3 km y hasta 1.5 Mbps. En comparación con la HDSL, su despliegue es más fácil, ya que puede reservar un cable en el par trenzado.

- HDSL 2. Versión desarrollada para mejorar la interoperabilidad y compatibilidad espectral con otros servicios. (ISDN, T1, HDSL) 1.5 a 2 Mbps.

- Single-pair HDSL (SHDSL). Similar a HDSL 2, pero más generalizado. DSL para negocios, permite transportar T1/E1, ISDN, ATM, e IP.
- G. SHDSL. Desde 192 kbps hasta 2.312 Mbps en pasos de 8 Kbps.Dos hilos (Opcional 4 hilos: hasta 4624 Kbps). No soporta Splitters para POTS.

ADSL

Es el servicio de acceso a Internet por banda ancha que brindan, entre otras, las empresas telefónicas.

Se caracteriza por utilizar para el tráfico de datos el mismo cable telefónico que para las transmisiones de voz, pero en bandas de frecuencia diferentes logrando de esta forma la simultaneidad de ambos tipos de comunicación.

La evolución de la tecnología ADSL ha permitido aumentar considerablemente las velocidades ofrecidas a los consumidores abriendo un abanico de posibilidades en el uso de Internet en el hogar como por ejemplo transmisiones en vivo, transferencias de grandes volúmenes de datos, mayor calidad en las comunicaciones en línea, etc.
su velocidad de transmisión es distinta en los dos sentidos y la información transmitida es digital de extremo a extremo

ADSL opera sobre el bucle de abonado hasta la central más próxima.

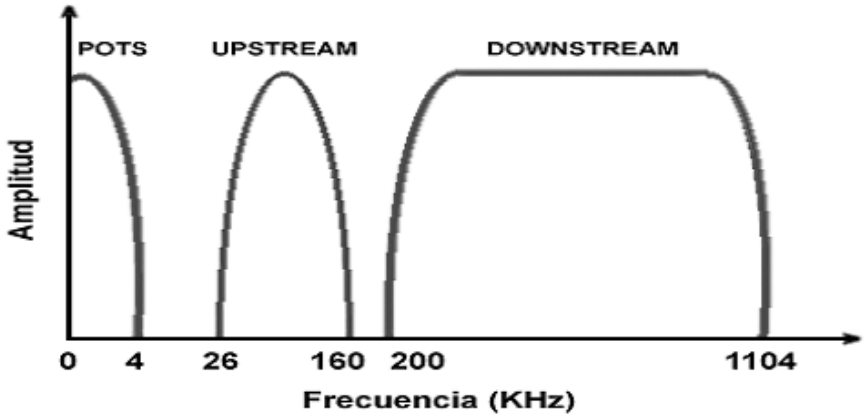
Características:

- utiliza dos hilos de cobre y pares de equipos.
- Tecnología no conmutada (siempre conectado)
- Velocidades diferentes de bajada y subida.
- Mercado: Hogares y Negocios.

Hace uso del par trenzado de cobre instalado para brindar servicio de telefonía básica.

Aprovechando que la telefonía básica utiliza únicamente bajas frecuencias (hasta 16 KHz), ADSL utiliza la porción del espectro que va desde 25 KHz, hasta 1,1 MHz.

De esta forma, dispone de un gran ancho de banda (>1MHz), exclusivo del abonado, y sin interferir con el servicio básico, ni depender de él.



Tiene sus límites físicos que le hace variar el alcance y calidad por el estado del par de cobre.

Otros equipamientos adicionales son lo Splitters y Microfiltros.

Fortalezas

Conexión dedicada.
Basada en Estándares.
Flexibilidad en opciones.

Debilidades

Rango Limitado.
Problemas con co-location y unbundling
Servicio de Contención.

Un sistema ADSL está compuesto por los siguientes dispositivos:

- Un ATU-C: ADSL transceiver unit-central office (Transceptor ADSL central) que es el modem situado en la casa del usuario.
- Un ATU-R: ADSL transceiver unit-remote (Transceptor ADSL remoto, módem ADSL, CPE), que es la terminal situada en la central.
- Un Splitter (Divisor). Es el filtro que separa las señales de ADSL y POTS
- Un DSLAM: Digital subscriber line access multiplexer (Multiplexor de acceso), que es el elemento de red que concentra el tráfico de los usuarios finales y estará conectado de alguna forma a la red de datos (backbone) del proveedor.

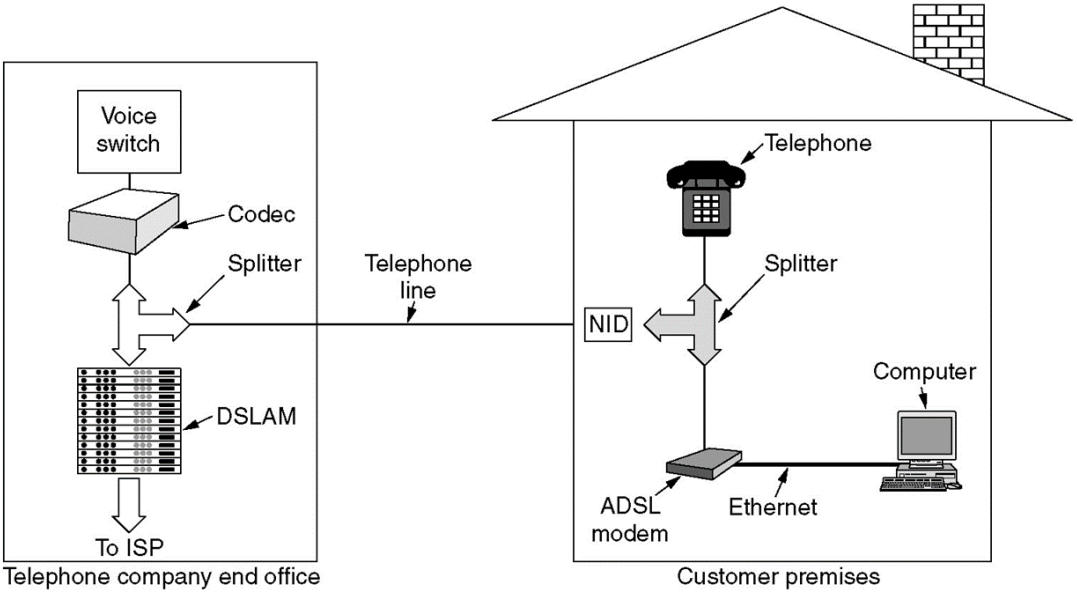
Las señales de ADSL y POTS son mezcladas en un splitter, y conectadas al tendido exterior a través del repartidor general.

El abonado que posea un servicio ADSL recibirá en su domicilio ambas señales en el mismo par.

Para discriminar ambas señales, deberá colocar un splitter en la entrada.

A su salida tendrá por un lado la señal de POTS, que utilizará normalmente, y por otro la señal ADSL, que conectará a su módem (ATU-R).

Es normalmente un filtro pasivo, que posee una entrada para la línea externa, y dos salidas. Una de ellas tendrá la señal de POTS, y otra la señal ADSL.

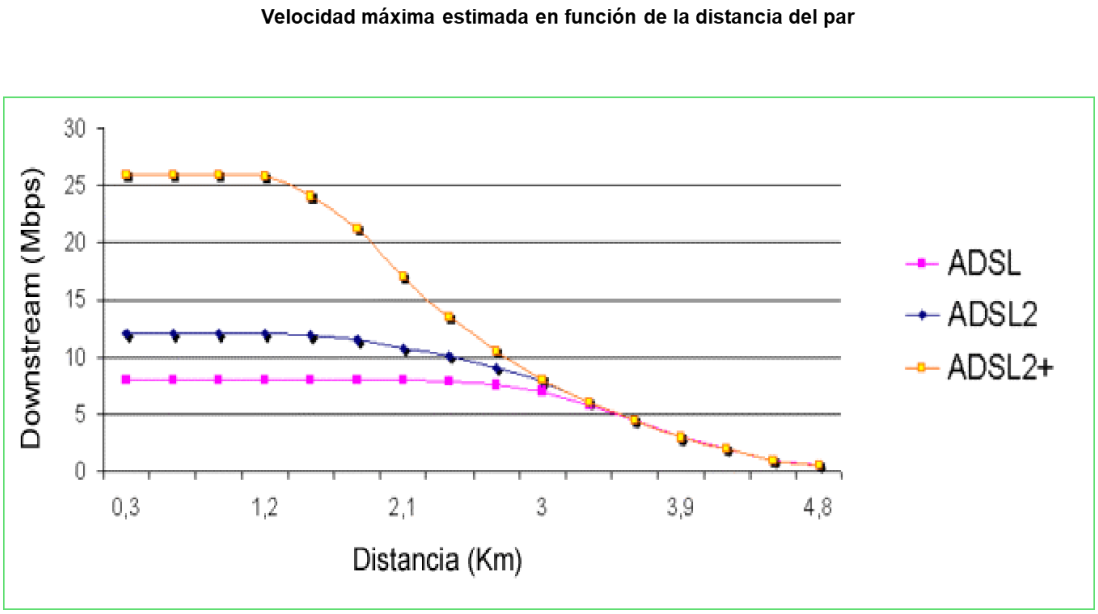


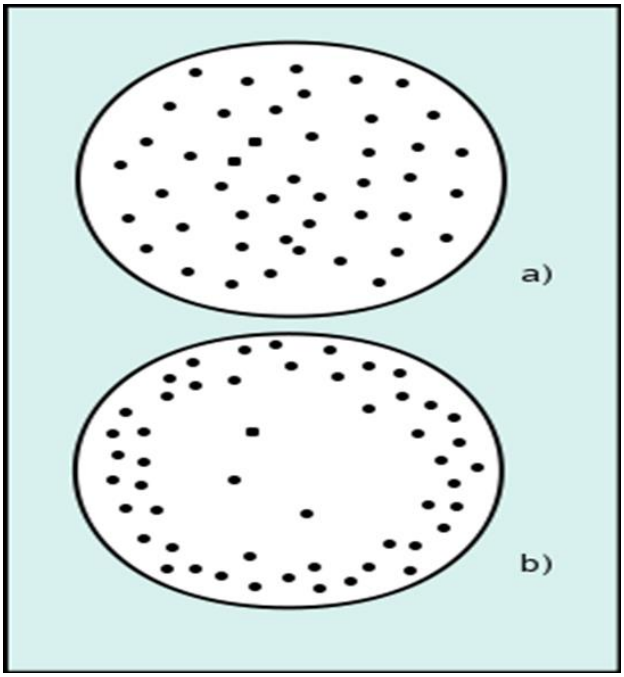
El medio utilizado para la transmisión de las señales es el tendido de cobre instalado para prestar servicio de telefonía básica.

De acuerdo a la calidad del tendido y a la sección del conductor, el medio presentará distintos valores de atenuación de la señal.

Un tendido de mejor calidad y de mayor sección dará lugar a una menor atenuación. La distancia será un factor decisivo, puesto que la atenuación total será mayor cuanto mas largo sea el cable.

En la figura siguiente, se observamos la atenuación de la señal respecto a la distancia.



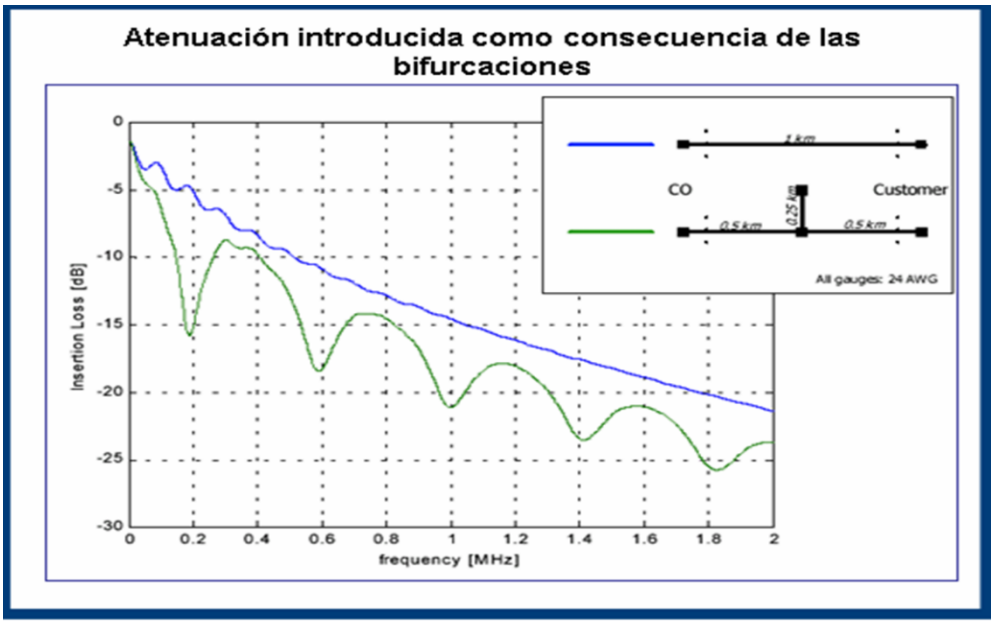


En corriente continua, la densidad de corriente es similar en todo el conductor (figura a), pero en corriente alterna se observa que hay una mayor densidad de corriente en la superficie que en el centro (figura b). Este fenómeno se conoce como **efecto pelicular**,**efecto skin** o **efecto Kelvin**.

Este fenómeno hace que la resistencia efectiva o de corriente alterna sea mayor que la resistencia óhmica o de corriente continua dando como resultado una disminución del conductor, y por lo tanto aumenta su atenuación.

Los siguientes son factores que afectarán a la calidad de la señal recibida:

- Calidad / sección del tendido
- Distancia central-abonado
- Frecuencia
- Las bifurcaciones en el tendido introducen una atenuación adicional.



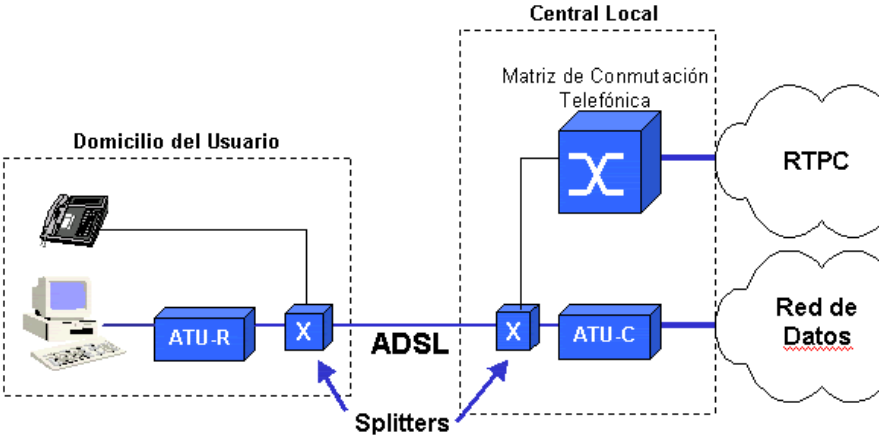


Ilustración 1 Instalación básica - bucle del abonado

Una vez instalado, el cableado es susceptible de interferencias o alteraciones de los siguientes parámetros:

- Emisiones de radiofrecuencia,
- Inducciones electromagnéticas
- Condiciones climáticas
- Instalaciones próximas

Anteriormente nombramos al dispositivo DSLAM y ahora lo verá con más detalle.

DSLAM, Digital Subscriber Line Access Multiplexer, es el elemento de red que concentra el tráfico de los usuarios finales. Su objetivo es almacenar la configuración y efectuar la conmutación. Tiene conjuntos de modems (AtU-C), uno para cada abonado.

La modulación asimétrica implica dos módems ATU (ADSL Terminal Unit) distintos:

- ATU-R (Remote) en el usuario, con un máx. de 32 subportadoras ascendentes.
- ATU-C (Central) en la central, con un máx. de 256 subportadoras descendentes, agrupados en tarjetas integradas dentro de un chasis de acceso múltiple DSLAM, que concentra el tráfico hacia una red WAN y permite un despliegue masivo del acceso.

Esta asignación de banda de datos (de 24KHz a 1'104 MHz) permite coexistir en el bucle de abonado con telefonía vocal POTS (hasta 4KHz)

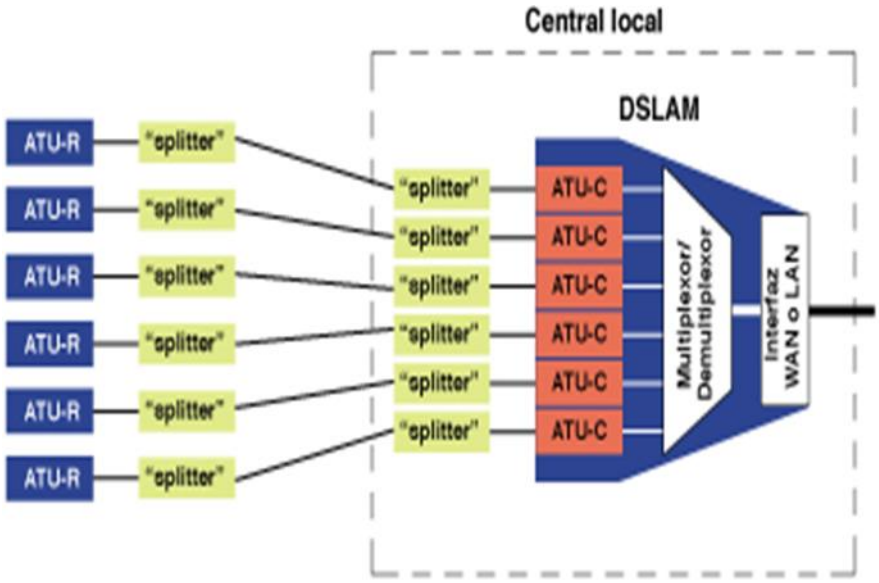


Ilustración 2 ATU-C de un DSLAM

TECNICAS DE MODULACION DE ADSL

En la actualidad, existen dos técnicas de modulación que coexisten:

CAP (Carrier-less Amplitude Modulation).

CAP es más antigua y sencilla.

Es más barata de implementar, pero consigue eficiencias menores y está más retrasada en el proceso de estandarización.

CAP es una implementación de QAM para xDSL, divide la señal modulada en segmentos que después almacena en memoria.

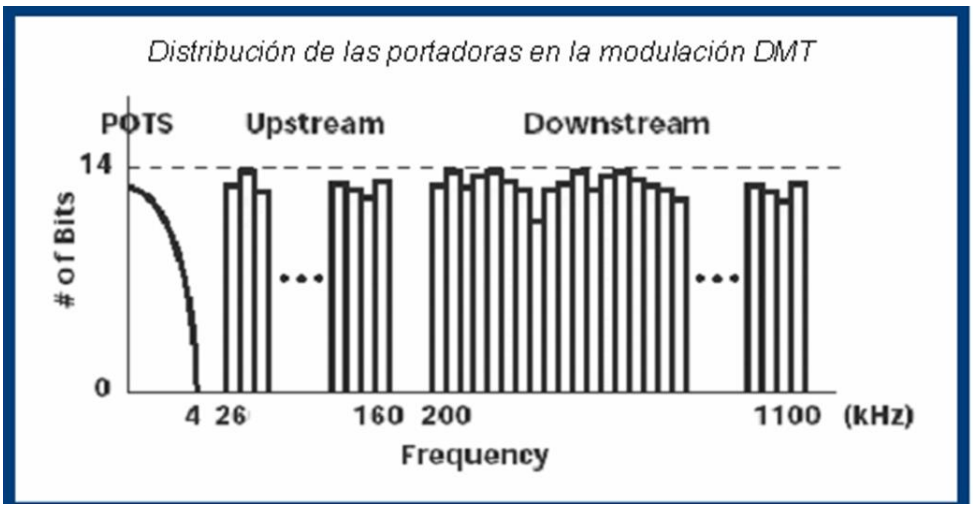
QAM,(modulación de amplitud en cuadratura), transporta dos señales independientes, mediante la modulación, tanto en amplitud como en fase, de una señal portadora

CAP es una modulación tipo QAM en la que la "constelación" es de rotación libre ya que no lleva portadora que nivele.

Así se puede utilizar todo el ancho de banda del bucle local (excepto los 4 Khz para la voz) para enviar todos los bits y olvidarnos de subportadoras y subcanales.

DTM (Discrete Multi-Tone modulation).

Es más compleja, pero consigue una mayor eficiencia. Actualmente parece que la tendencia de los fabricantes es hacia el uso de DMT.



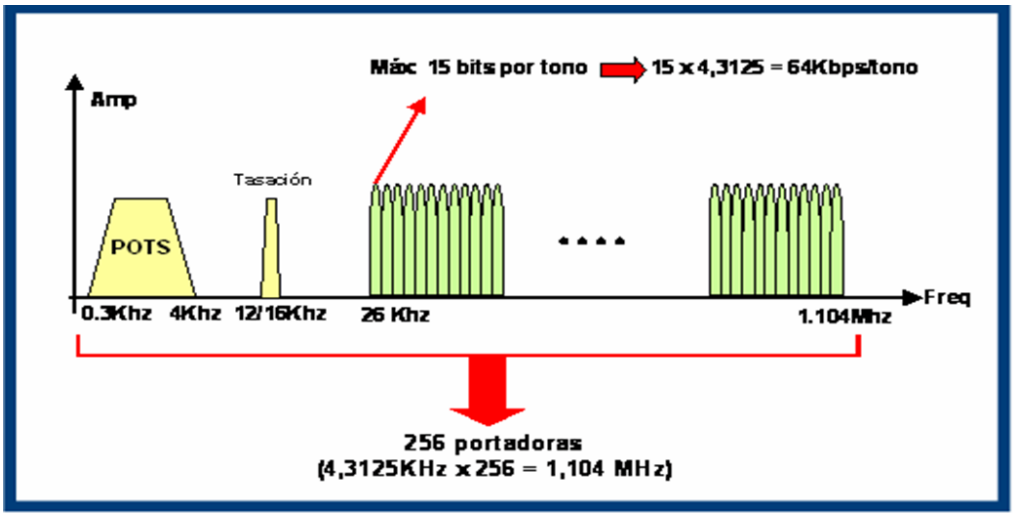
En el gráfico se puede observar que la porción que va desde 26 KHz a 160 KHz se utiliza para el tráfico ascendente (upstream), desde el módem del usuario hacia la central.

la porción desde 200 KHz hasta 1,1 MHz será utilizada para tráfico descendente (downstream) desde la central hacia el módem del usuario.

ADSL utiliza como máximo una constelación de 32768 símbolos, lo que representa un total de 15 bits. Esto significa que una portadora puede como máximo brindar una tasa de 64 Kbps.

Si se considerara el total de portadoras utilizadas para downstream, la tasa máxima podría ser de alrededor de 13 Mbps.

Sin embargo, y puesto que en la práctica no se alcanzan estos valores, ADSL determina un máximo de 8Mbps para el downstream, y aprovecha el margen restante para asegurar esta velocidad a distancias del orden de 2 Km.



DISTRIBUCION DE CANALES O BINS EN LA TECNOLOGIA ADSL DTM.

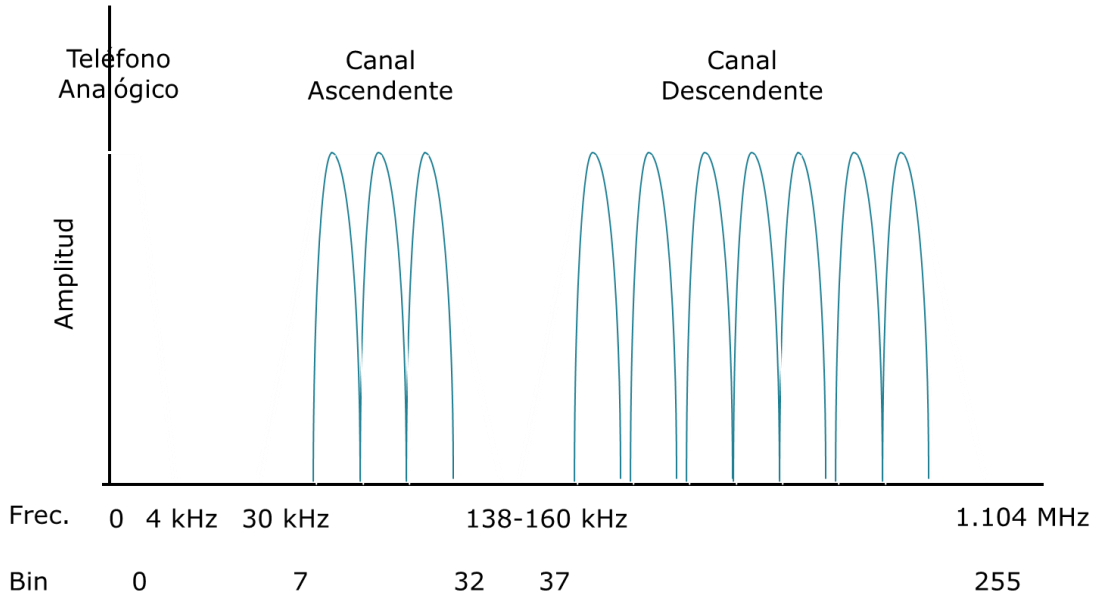
Uso	Bins Subcanales	Rango frecuencias (KHz)
Teléfono analógico	0-5	0-25,9
Tráfico ascendente	6-38	25,9-168,2
Tráfico descendente	33-255	142,3-1104

La asignación de bins al tráfico ascendente o descendente en ADSL DMT se realiza de acuerdo con lo indicado en el cuadro.

El canal ascendente puede llegar hasta el bin 38 y el descendente puede empezar en el bin 33; dentro de este rango se decide para cada caso concreto donde se pone la división entre ascendente y descendente.

Además, se reserva un bin en cada sentido para funciones de control.

ADSL DMT (ITU G.992.1) Frecuencia . 0 4 kHz 1.104 MHz Canal Descendente Canal Ascendente Teléfono Analógico 30 kHz 138-160 kHz Bin 0 32 37 255 7 Amplitud

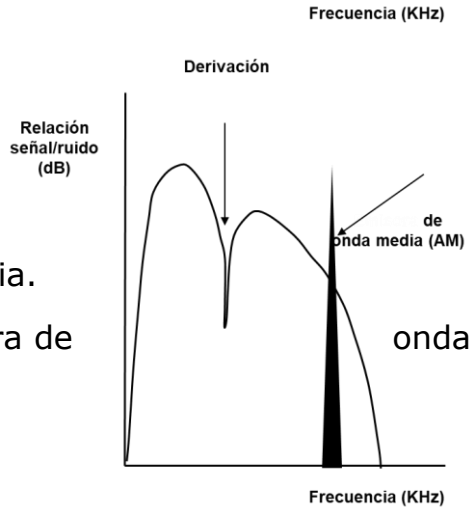


INTERFERENCIAS EXTERNAS EN ADSL.

Interferencia provocada por una derivación de un cable no retirado De una instalación anterior.

Esto produce una pérdida de calidad de la señal en una determinada frecuencia.

También hay una interferencia de emisora de onda media AM

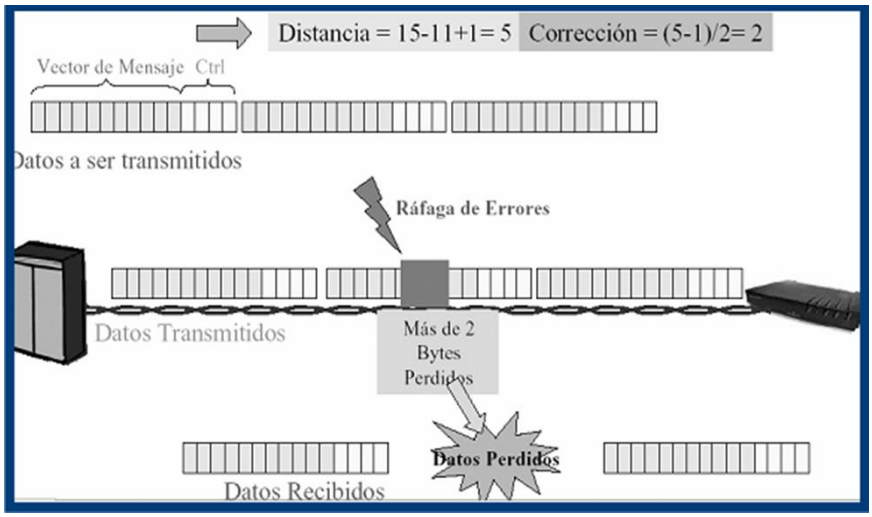


Como consecuencia de estos problemas los módems han decidido reducir la eficiencia en el bin correspondiente a la derivación, e inhabilitar por completo el bin correspondiente a la frecuencia de la emisora de onda media

INTERLEAVING.

El interleaving (o entrelazado) es una característica que permite disminuir la incidencia de interferencias o ruidos aleatorios, que típicamente afectan a la comunicación en forma de ráfaga ("burst").

El enlace ADSL utiliza una estructura de trama para transmitir la información, que contiene información de control.



Si, como se observa en el gráfico, una ráfaga afecta muchos bits (incluso bytes) de una trama, la información de control de la trama no permite reconstruir la información original.

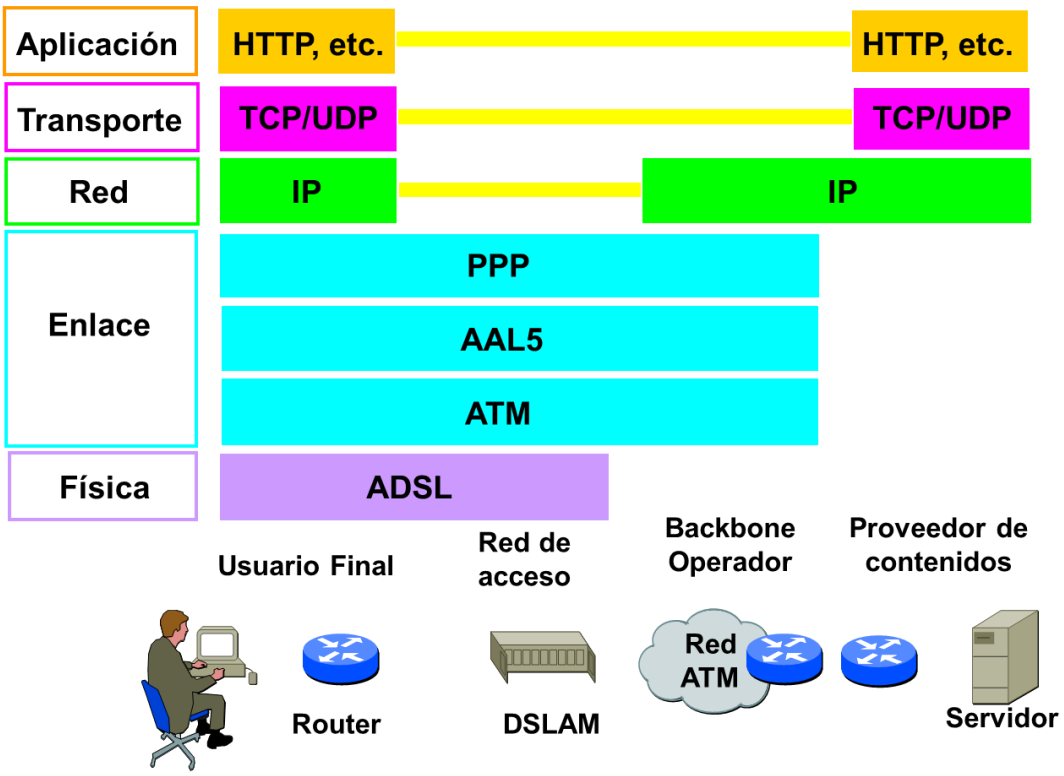
La transformación consiste en intercalar los datos de varias tramas, de manera que, si una ráfaga afecta a una porción de la información transmitida, al volver atrás el intercalado, tenga los bits errados dispersados entre varias tramas.

Si bien esto parecería afectar más la transmisión, no es así: valiéndose de la información de control, el receptor puede llegar a corregir todos los errores, dado que en cada trama a afectado a muy pocos bits.

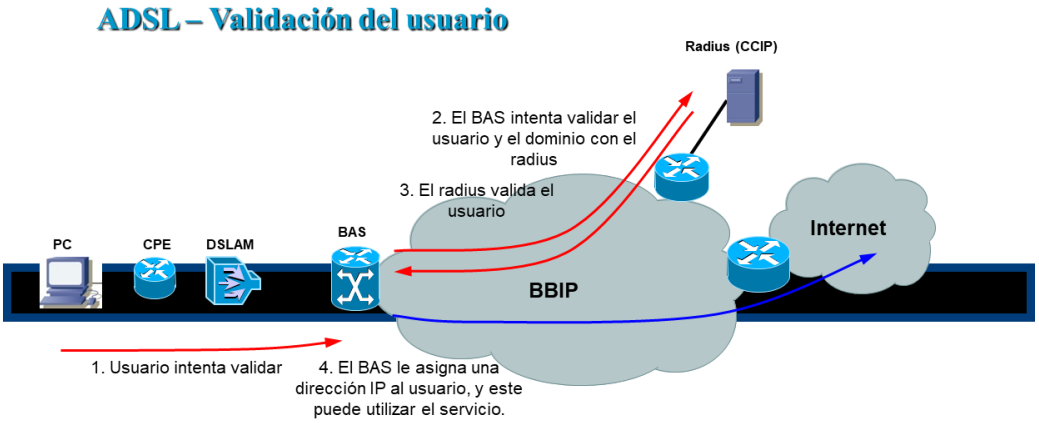
PROTOCOLO UTILIZADOS EN ADSL.

En el siguiente esquema, se muestra la forma como se integra normalmente ADSL con los protocolos de las capas superiores. ADSL utiliza el protocolo de adaptación AAL5 y sobre él el protocolo a nivel de enlace PPP (Point to Point Protocol) que es utilizado normalmente en conexiones de red telefónica tradicional. Esto permite aprovechar en conexiones ADSL de forma transparente todo el software de control de acceso habitual entre los ISP, como RADIUS. Por encima de PPP se

pueden utilizar los diversos protocolos habituales en el nivel de red, como IP.



¿COMO FUNCIONA?



Configuración de conectividad xDSL

Estas tecnologías salieron al mercado en el siguiente orden, con una compatibilidad variable para PPP:

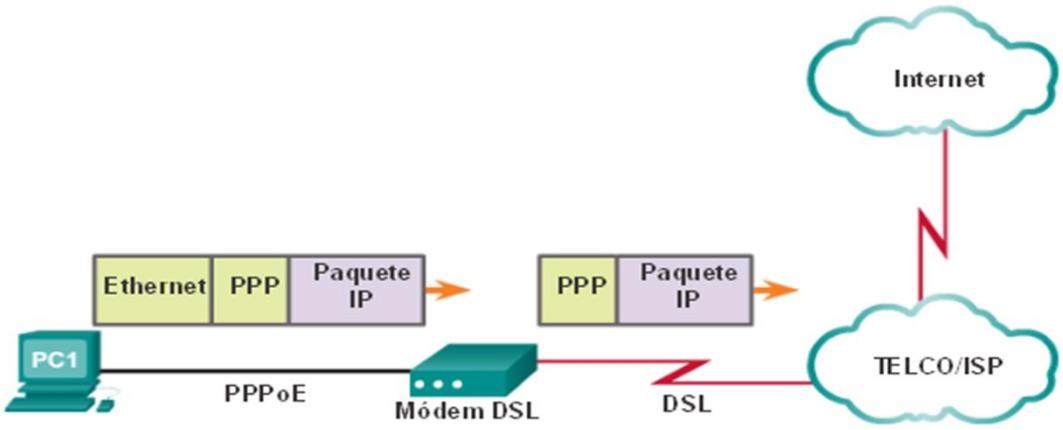
- Módems análogos para dial-up que podían utilizar PPP y CHAP
- ISDN para dial-up que podían utilizar PPP y CHAP
- DSL, que no establecía un enlace punto a punto y no admitía PPP ni CHAP

Los ISP consideran que PPP es valioso debido a las características de autenticación, contabilidad y administración de enlaces.

Sin embargo, los enlaces Ethernet no admiten PPP de forma nativa.

Como solución a este problema, se creó PPP por Ethernet (PPPoE).

Tramas PPP a través de una conexión Ethernet (PPPoE)



La pc1 se conecta directamente a un modem DSL. Mediante el uso del software adecuado (generalmente, un marcador o un cliente DSL que proporciona el ISP), la C1 encapsula tramas PPP dentro de las tramas de Ethernet y las envía al modem DSL.

PPOE.

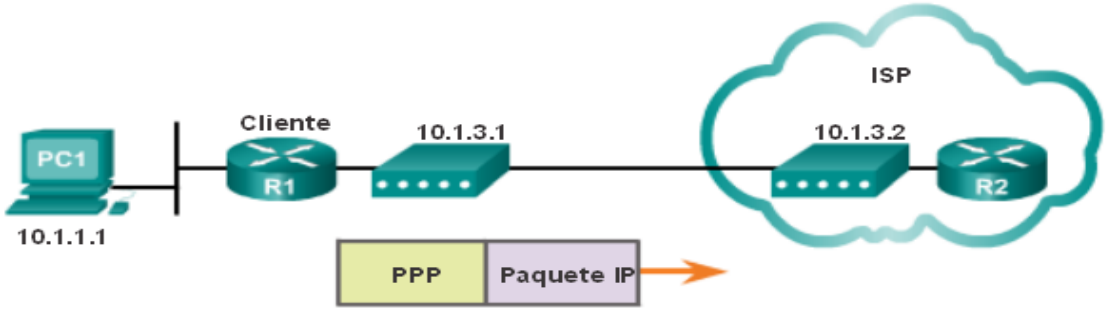
Como se muestra en la ilustración, el router del cliente generalmente está conectado a un módem DSL mediante un cable Ethernet.

PPPoE crea un túnel PPP a través de una conexión Ethernet.

Esto permite que las tramas PPP se envíen a través de un cable Ethernet hasta el ISP desde el router del cliente.

El módem convierte las tramas de Ethernet en tramas PPP mediante la eliminación de los encabezados Ethernet.

Después, el módem transmite estas tramas PPP en la red DSL del ISP.



REDES CATV

Las redes CATV aparecieron en los Estados Unidos al fines delos años 40 para resolver las malas condiciones de recepción de la señal de televisión que se daban en ciudades o barrios por orografía u otras razones.

La solución consistía en instalar una antena en un sitio elevado con buenas condiciones de recepción, y desde allí distribuir la señal mediante cable coaxial a los usuarios.

El hecho de que la antena se colocara en un lugar elevado dio lugar a la denominación 'downstream' o 'hacia abajo' que se utiliza para describir la comunicación en el sentido del centro emisor hacia el usuario.

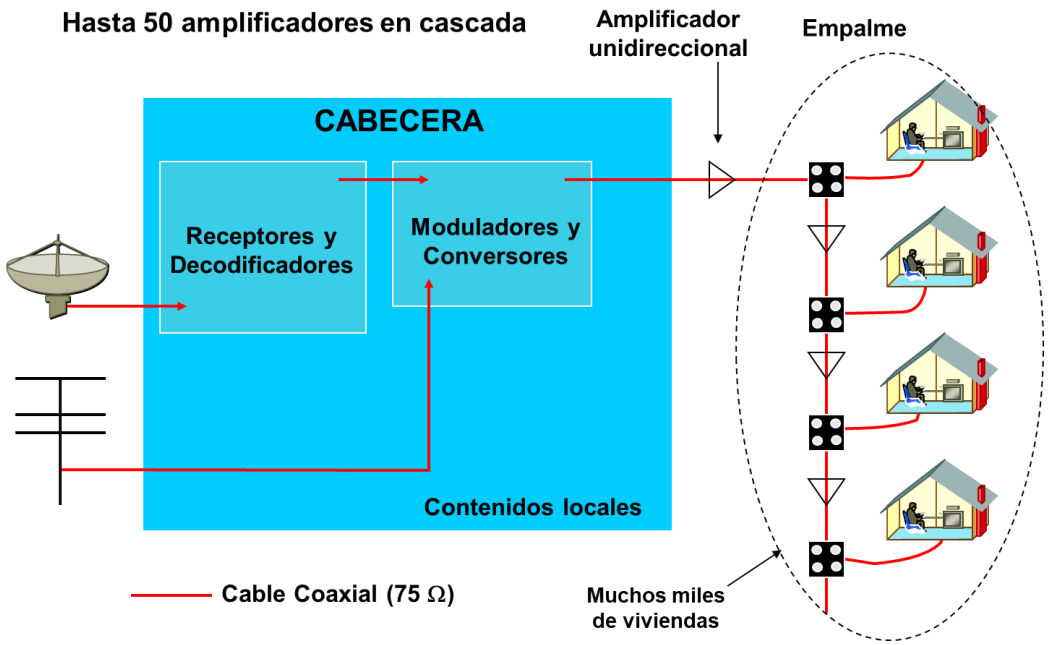
Se utiliza cable coaxial de 75 Ω como el de antena de televisión.

Para regenerar la señal se colocan amplificadores cada 0,5 – 1,0 Km.

La distancia entre amplificadores es función de la cantidad de usuarios en cada tramo (a más usuarios menor distancia) y de la frecuencia máxima que utilizara la red (a mayor frecuencia máxima menor distancia). Esta frecuencia máxima era de 300-400 MHz.

Las redes CATV antiguas eran unidireccionales. No se contemplaba la necesidad de utilizarlas en sentido 'ascendente', por lo que los amplificadores se diseñaban con la única función de amplificar la señal hacia abajo y actuaban como verdaderas válvulas que impedían cualquier propagación de señales en sentido ascendente.

Arquitectura típica de una red CATV coaxial tradicional



Aquí tenemos un ejemplo de red CATV 'clásica' unidireccional que utiliza cable coaxial únicamente.

El centro emisor, o cabecera de la red, puede tener una antena de superficie para captar la programación normal, varios receptores de canales vía satélite y una serie de canales de programación propia.

Todas estas señales se distribuyen a los abonados a través de la red de cable coaxial, que puede abarcar muchos miles de usuarios.

Debido a la necesidad de colocar amplificadores en las redes CATV coaxial la señal podía tener que atravesar hasta 50 amplificadores para llegar a algunos usuarios. Cada amplificador degradaba la señal un

poco, y la probabilidad de averías aumentaba al haber tantos elementos en serie. Desde el punto de vista del mantenimiento la red era muy compleja.

Muchos amplificadores en cascada degradan la señal, complican y encarecen mantenimiento. Solución: redes HFC (Hybrid Fiber Coax)

Redes CATV modernas.

Para resolver los problemas de gestión y mantenimiento de las redes CATV coaxiales a finales de los años 80 empezaron a aparecer redes CATV con la arquitectura denominada HFC (Hibrid Fiber Coax).

Esta consiste en dos niveles jerárquicos, el principal formado por un tendido de fibra óptica con topología de estrella que distribuye la señal desde el centro emisor hasta cada zona de la ciudad.

En cada zona hay un nodo (normalmente un armario ubicado en la acera) que se encarga de convertir la señal óptica en eléctrica para su distribución final en cable coaxial a los abonados.

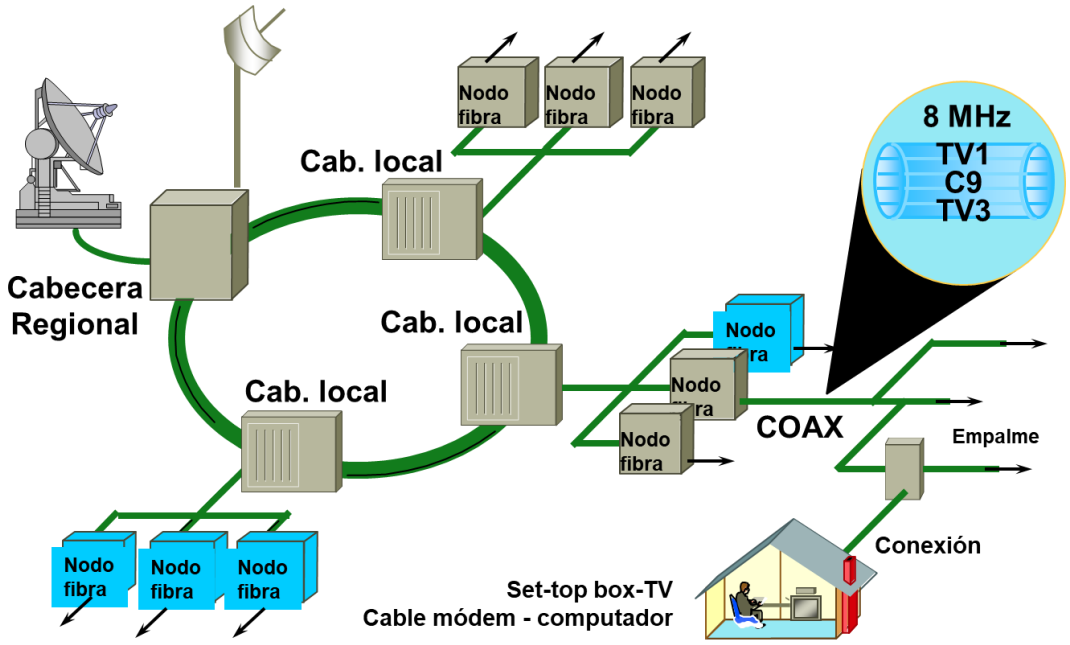
Cada zona abarca de 500 a 2000 viviendas. Debido a la menor distancia a cubrir el número de amplificadores máximo es de 5 (en muchas redes nunca hay más de 2 ó 3), con la consiguiente mejora en calidad de la señal y sencillez de mantenimiento.

Un elemento crucial en la implantación de redes HFC fue la posibilidad de enviar la señal analógica de televisión por fibra óptica sin necesidad de convertirla en digital.

Las redes HFC también facilitaron la utilización de la red para tráfico ascendente. Esto permitía labores de monitorización y servicios tales como el pago por visión.

Dado que la señal de televisión utiliza el rango de frecuencias altas (50-400 MHz) para el sentido descendente, se utilizan frecuencias por debajo de 50 MHz para el ascendente.

Se colocan amplificadores en sentido ascendente para el rango de bajas frecuencias, que no interfieren en la propagación de la señal descendente.



En esta figura tenemos un ejemplo típico de red HFC. Al nivel más alto tenemos un anillo de fibra óptica, seguramente por motivos de fiabilidad, que distribuye la señal del centro emisor a una serie de concentradores.

Cada uno de esos concentradores a su vez reenvía la señal, también por fibra óptica, a una serie de nodos que la convierten en señal.

En el esquema siguiente, eléctrica y la envían por cable coaxial a los abonados.

Este esquema representa la arquitectura típica de una red CATV HFC bidireccional preparada para ofrecer servicios de transmisión de datos.

Aparte de los equipos utilizados para la distribución de la señal de televisión encontramos en el centro emisor el CMTS (Cable Modem Termination System); en la vivienda además del televisor tenemos el Cable Módem, que conecta el computador.

Tanto el canal ascendente como el descendente son compartidos, pero gracias a la estructura de la red HFC los canales solo son compartidos por los usuarios de una zona, no entre zonas diferentes.

En función de la densidad de usuarios del servicio de datos de cada zona el operador puede adoptar las siguientes estrategias:

- Si la densidad es baja puede agrupar varias zonas en un mismo canal compartido, con lo que a efectos de datos se comporta todo como una misma zona.

- Si la densidad es alta puede asignar varios canales ascendentes y/o descendentes a una misma zona, con lo que el resultado es equivalente a dividir la zona en dos. En el caso de los canales ascendentes también es posible jugar con la anchura.

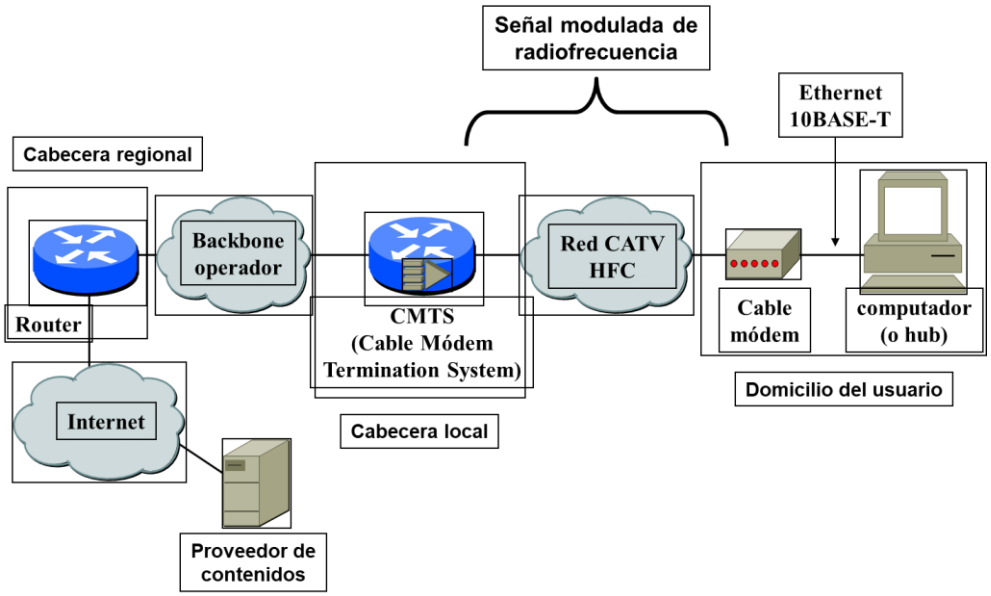


Ilustración 3 ARQUITECTURA TÍPICA DE UNA RED CATV HFC

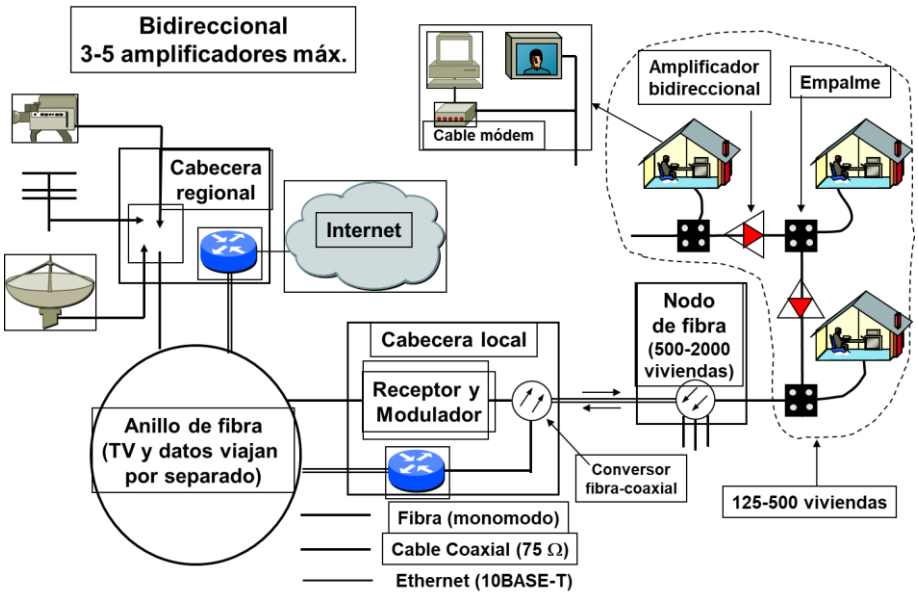


Ilustración 4 Elementos de comunicación en una red CATV HFC

Esta figura anterior, nos muestra los elementos básicos que permiten la comunicación en una red CATV HFC.

En primer lugar tenemos el denominado CMTS (Cable Modem Termination System) que es el dispositivo que se encarga de enviar los datos en sentido descendente modulados por el canal de televisión elegido al efecto, así como de recoger de los Cable Módems de los usuarios los datos que éstos envían a través del canal ascendente asignado.

El CMTS se ubica normalmente en el centro emisor o cabecera de la red. De allí se conecta al resto de la red (la red de transporte) y a la Internet por alguna tecnología de red de área extensa, por ejemplo POS (Packet over SONET).

Por su parte el usuario dispone de un cable módem, dispositivo que se encarga de sintonizar el canal de televisión elegido para los datos y extraer los que le corresponden, es decir los que van dirigidos a él.

También debe de enviar los datos de retorno por el canal ascendente correspondiente.

Existen diversas formas de conectar el Cable Módem al computador del usuario final. De entre ellas la más frecuente es utilizar una conexión Ethernet de 10 Mb/s, que es una interfaz de alta velocidad y bajo costo para prácticamente cualquier computador.

LA TRANSMISION DATOS.

Cuando se utiliza una red CATV para transmitir datos se reserva un canal de televisión para el sentido descendente. Según se utilice la norma americana (NTSC) o europea (PAL o SECAM) el canal tendrá una anchura de 6 u 8 MHz, respectivamente.

Para el retorno en las redes CATV coaxiales puras se emplea una conexión telefónica (módem analógico o RDSI) ya que la comunicación en sentido ascendente a través de la red CATV es imposible.

En las redes CATV HFC se utiliza para el sentido ascendente el rango de frecuencias bajas en el que los amplificadores actúan en sentido inverso. En este rango se pueden definir canales de diversas anchuras entre 0,2 y 3,2 MHz.

La red CATV es un medio compartido singular; al no ser simétrico el medio físico tampoco lo es su funcionamiento: el CMTS gobierna la red y los CMs se limitan a cumplir sus órdenes.

Debido a la forma como funcionan los cables módems la comunicación entre dos usuarios de la red CATV siempre se realiza a través del

equipo de cabecera, aun en el caso de que ambos usuarios se encuentren en la misma zona y compartan el canal ascendente y descendente. Así por ejemplo si en el ejemplo de la transparencia anterior el usuario 1 quiere transmitir algo al usuario 3 tendrá que utilizar el canal ascendente para enviar la información al CMTS, el cual la reenviarla por el canal descendente al destinatario. Por lo tanto dicha información pasará dos veces por el mismo cable.

.

CABLEMODEM

El nombre que recibe esta tecnología se basa por una parte en la contracción de "Red de Televisión por Cable" ("Cable TV Network" o lo que es lo mismo CATV) y la palabra MODEM ("modulador demodulador"), aunque realmente es un término es un tanto equivocado ya que la tecnología está más cercana a una interfaz LAN (MAN o WAN realmente) que a un módem en el sentido original de la palabra.

Una conexión del tipo "cable módem" están solapadas entre una conexión por modem tradicional y una conexión LAN.

Las velocidades que suele alcanzar están entre los 3 y 50 Mbps de manera básica y la distancia de aplicación alrededor de los 100 Km. y quizá más. Existe una terminal central (nodo) donde están conectados todos los módems y que se comunican entre si a través de ella.

El cable módem es un tipo especial de módem diseñado para modular la señal de datos sobre una infraestructura de televisión por cable.

El término Internet por cable (o simplemente cable) se refiere a la distribución de un servicio de conectividad a Internet sobre esta infraestructura de telecomunicaciones.

Los abonados de un mismo vecindario comparten el ancho de banda proporcionado por una única línea de cable coaxial. Por lo tanto, la velocidad de conexión puede variar dependiendo de cuanta gente este usando el servicio al mismo tiempo.

Una debilidad más significativa de las redes de cable al usar una línea compartida es el riesgo de la pérdida de privacidad, especialmente considerando la disponibilidad de herramientas de hacking para

cablemódems. De este problema se encarga el cifrado de datos y otras características de privacidad especificadas en el estándar DOCSIS

El Cablemodem se conecta al computador normalmente mediante Ethernet (10BASE-T). Así se consigue una interfaz de alta velocidad a bajo costo y una clara separación usuario-red.

Puede actuar como puente transparente o como router IP.

Se pueden conectar varios PCs a través de un mismo CM (algunos CM llevan hub incorporado).

Hay algunos módems internos (bus PCI) y conectables a USB

FUNCIONES DEL CABLEMODEM.

- Captar/generar señal de Radiofrecuencia
- Modular/demodular los datos
- Generar/verificar la información de control de errores (FEC)
- Encriptar/desencriptar la información
- Respetar protocolo MAC en Upstream
- Gestión y control del tráfico (limitación de caudal, número de computadores conectados, etc

ESTANDARES CATV.

- DOCSIS: estándar más extendido.
- Productos DAVIC 1.2 aproximadamente un año por detrás.

- DOCSIS: desarrollo USA. Caso europeo (Euro-DOCSIS) (solo cambia nivel físico).
- DAVIC: desarrollo europeo.
- CMs actuales: DOCSIS 1.0 (sobre todo), también DVB 1.2 y propietarios.
- ITU-T ha adoptado tanto DOCSIS 1.0 como DAVIC 1.2.

DOCSIS

DOCSIS es un estándar para la certificación de dispositivos de proveedores de cable (cable modem y sistema de terminación de modem por cable).

Especifica las capas físicas y MAC y define los requisitos de la interfaz rd para un sistema de datos sobre cable.

Los proveedores de equipos de cable deben aprobar la certificación dirigida por CableLabs.

Euro-DOCSIS es una variación del estándar para uso en Europa.

DOCSIS define los requisitos de interfaz de soporte de operaciones y comunicaciones para el sistema de datos por cable y permite la incorporación de transferencia de datos de alta velocidad a un sistema CATV existente.

Los operadores de cable emplean DOCSIS para proporcionar acceso a Internet por la infraestructura existente de fibra coaxial híbrida (HFC).

DOCSIS especifica los requisitos de Capa 1 y Capa 2 del modelo OSI:

- **Capa física**: para las señales de datos que el operador de cable puede usar, DOCSIS especifica los anchos de canales (anchos de banda de cada canal) como 200 kHz, 400 kHz, 800 kHz, 1,6 MHz, 3,2 MHz y 6,4 MHz. DOCSIS también especifica las técnicas de modulación (la manera de usar señales de RF para transmitir los datos digitales).
- **Capa Mac**: define un método de acceso determinista, acceso múltiple por división temporal (TDMA) o el método de acceso múltiple por división de código síncrono (S-CDMA).

EVOLUCION DE DOCSIS.

DOCSIS 1.0

La especificación DOCSIS consiste en varios documentos de especificación, que cubren todos los aspectos de la arquitectura requerida para ofrecer un servicio completo end-to-end, que incluye:

- Cable Módem to CPE interface (CMCI)
- Cable Modem termination System – Network Side Interface
- RF Interface Specification
- Telephone Return Interface
- Security (Baseline Privacy)
- Operations Support System Interface (OSSI)

DOCSIS 1.1

Posee interoperabilidad con DocSIS 1.0.

En cuanto a calidad de servicio (QOS), permite priorizar el tráfico de paquetes según la aplicación o la importancia del cliente.

- Garantiza el ancho de banda
- Clasifica los paquetes e identifica los flujos.

Con respecto a la mejora en la eficiencia del ancho de banda:

- Realiza fragmentación de paquetes grandes para facilitar la asignación de capacidad para servicios tipo DBR (voz y video).
- Agrupa paquetes pequeños para incrementar el throughput.
- Mejora la utilización del ancho de banda.
- Mejora de la Seguridad:
    - Reduce la posibilidad de "Robo de Servicio" mediante el downloading seguro de software.
    - Permite autenticación.
    - Seguridad y encriptación avanzada: Baseline Privacy Plus (BPI+)
    - Ecualización de la transmisión.

DOCSIS2.0

Agrega capacidades a nivel físico mediante modos de modulaciones avanzadas Enel upstream para ampliar su capacidad:

- 64 QAM vs 16 QAM (DOSCSIS1.1)
- A-TDMA (Advanced Time Division Multiple Access).
- S-CDMA (Sybchronous Code Division Múltiple Access).

Avances en la inmunidad al ruido mediante mejoras en las técnicas de FEC (Forward Error Correction)

También es efectivo para reducir los errores en la transmisión debido al ingreso de ruido impulsivo en la banda de retorno.

DOCSIS 3.0

Channel Bonding:

Agrupa varios canales de DS y US

- 160 Mbps o más en DS (4 canales de DS o más)
- 120 Mbps o más en US (4 canales de US o más)
- Posee la posibilidad de incorporar nuevos servicios corporativos

Soporte de IPv6:

- Provisioning y Management de CMs.
- Conectividad IPv6 para CPEs

IP Multicast:

- Soporte de SSM (Sourse Specific Multicast)
- Soporte de QoS para Multicast
- PHS para Multicast
- QoS y Autorización

Nivel físico:

- TFTP Proxy
- Certificate Revocation Management
- Configuration file learning

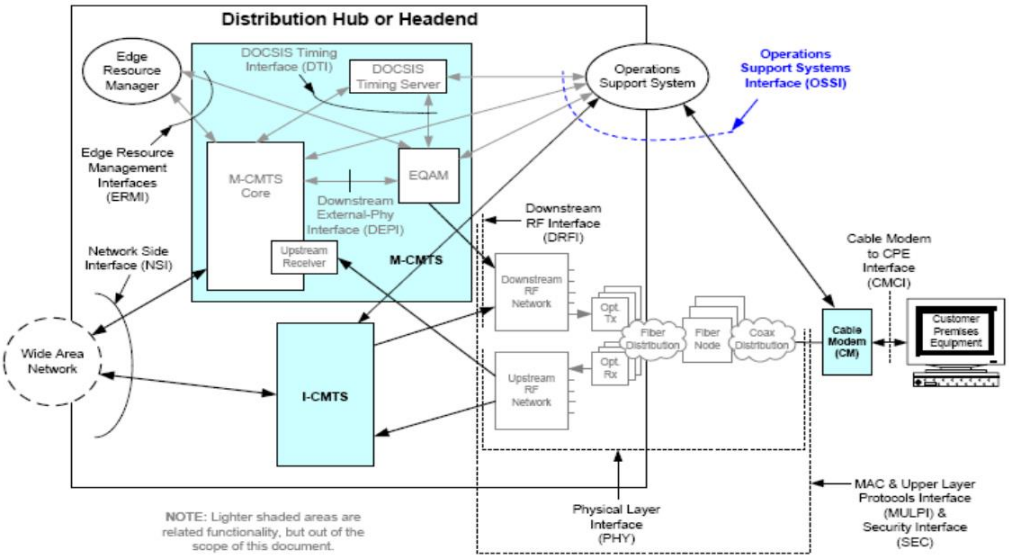
- Early autentication encriptation.
- Encriptación AES 128 bits.
- Source Address Verify: paquetes no provenientes de IPs válidamente otorgados son eliminados.

Manejo de la red.

- Mejoras en los diagnósticos
- Mejorass en la performance del data Collector

Bussiness Service Over DOCSIS

- VPN de nivel 2
- Emulación TDm(E1/T1)



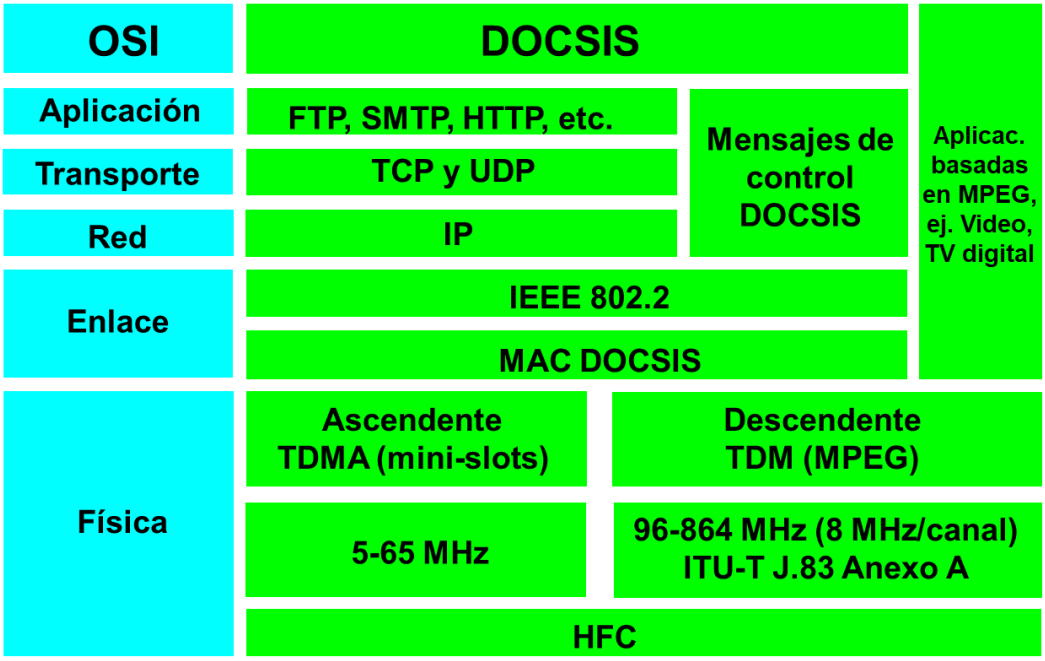
La siguiente figura muestra la correspondencia entre los protocolos utilizados en DOCSIS, que es el estándar más extendido en redes CATV, y el modelo OSI.

Podemos ver que las peculiaridades de redes CATV se limitan al nivel físico y a la subcapa MAC (mitad inferior de la capa de enlace), compartiendo el protocolo LLC 802.2 con el resto de redes IEEE 802. En este sentido podemos considerar las redes CATV como una más de las tecnologías LAN, al lado de Ethernet (802.3) o Token Ring (802.5).

Para el nivel de red y superiores DOCSIS sigue plenamente el modelo y la pila de protocolos TCP/IP, si bien añade una serie de mensajes de control para mejorar la gestión y mantenimiento de la red.

Por otro lado, las aplicaciones de televisión digital emplean una pila de protocolos propia a partir del nivel de enlace, compartiendo sólo el nivel

físico en la especificación de canal descendente; puesto que no se contempla la posibilidad de interacción en este caso no se requiere sentido ascendente.



Ampliación Redes 3-83

COMPARANDO ASDL Y HFC.

En ASDL el par telefónico es dedicado, en HFC el medio de bajada y el de subida son compartidos. Muchos usuarios simultáneos notarán una diferencia (mejor ASDL). Pocos usuarios, puede ser mejor HFC.

En HFC el canal de subida es compartido, luego HFC requiere de un protocolo para acceder al medio común de subida (protocolo de accedo múltiple distribuido).

Fin de la clase
UAI
Universidad Abierta
Interamericana