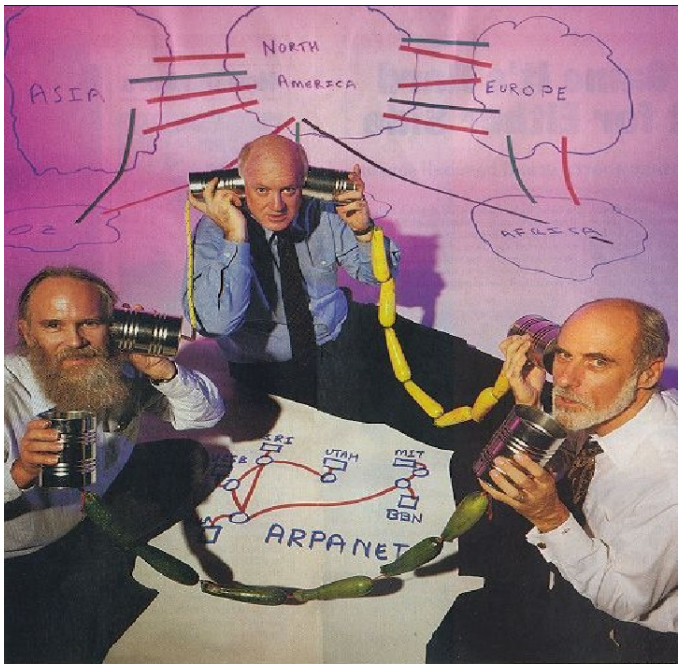
Redes de comunicaciones

Última modificación 2009/04



Se solía decir que TCP/IP debería funcionar incluso entre dos latas unidas por una cuerda.
En la foto vemos a Jon Postel, Steve Crocker y Vinton Cerf haciendo la prueba.

2004-2009 – Güimi (http://guimi.net)
Esta obra está bajo una licencia "Reconocimiento-Compartir bajo la misma licencia 3.0 España" de Creative Commons.
Para ver una copia de esta licencia, visite http://guimi.net/index.php?pag_id=licencia/cc-by-sa-30-es_human.html.

Reconocimiento tautológico: Todas las marcas pertenecen a sus respectivos propietarios.

Elaboración propia utilizando principalmente apuntes de trabajo, de distintas asignaturas universitarias, trabajos del profesor Montañana publicados en RedIRIS y artículos de la wikipedia (http://www.wikipedia.org).
Algunas partes son directamente copia o traducción de las fuentes.

Redes de comunicaciones

Contenido

1. INTRODUCCIÓN....4
1.1. Conceptos....4
1.2. Tipos de red....6
1.3. Redes de área local (LAN)....9
1.4. Redes de área extensa (WAN)....9
2. EL MODELO ISO OSI....10
2.1. Niveles de red del modelo OSI....11
3. EL MODELO INTERNET....13
3.1. Un poco de historia....13
3.2. Familia de protocolos de Internet....13
3.3. Protocolo Internet (IP)....15
3.4. Otros protocolos de la familia Internet....25
4. ETHERNET....29
4.1. Un poco de historia....29
4.2. Definición....30
4.3. Control de colisiones....30
4.4. Direccionamiento....31
4.5. Formato de trama....31
4.6. Tarjetas interfaces de red (NIC: Network Interface Card)....32
4.7. Repetidores y concentradores (Hubs)....32
4.8. Puentes (Bridges) y conmutadores (Switches)....33
4.9. Comunicación Dúplex (Full-Duplex)....33
4.10. Restricciones....34
4.11. La evolución de la familia Ethernet....35
4.12. Mejoras de rendimiento....39
5. IEEE 802.11 (Wi-Fi)....41
5.1. Definición....41
5.2. Otras definiciones....41
5.3. Problemas añadidos en redes inalámbricas....43
5.4. Control de acceso al medio (MAC: Medium Access Control)....43
5.5. Seguridad....44
5.6. Evolución del estándar 802.11....45
6. PROTOCOLOS WAN....48
6.1. Portadora-T y PDH (Plesiochronous Digital Hierarchy)....48
6.2. X.25....49
6.3. RDSI....49
6.4. FDDI (Fiber Distributed Data Interface) / CDDI....50
6.5. FRAME-RELAY....50
6.6. ATM (Asynchronous Transfer Mode)....52
6.7. Redes de fibra SONet / SDH....54
6.8. PoS (Packet Over SONet/SDH)....55
6.9. GSM (Global System for Mobile comunications)....55
6.10. GPRS (General Packet Radio Service)....55
6.11. UMTS (Universal Mobile Telecommunications System)....55
6.12. Redes de satélites....56
6.13. MPLS (Multi-Protocol Label Switching)....56
7. MÉTODOS DE ACCESO A REDES....57
7.1. Introducción....57
7.2. Módems....57

7.3. xDSL....57
7.4. CATV (Redes de TV por cable)....60
7.5. LMDS (Local Multipoint Distribution System)....61
8. REDES PRIVADAS VIRTUALES....62
8.1. Introducción....62
8.2. Autenticación de usuario....63
8.3. Protocolos para la realización de VPNs....64
9. SEGURIDAD EN REDES....65
9.1. Introducción....65
9.2. Algoritmos....69
9.3. Técnicas criptográficas y de seguridad....71
9.4. Autenticación de usuario....71
9.5. Esquemas de seguridad....73
9.6. Herramientas de seguridad de redes....76
10. TRANSMISIÓN MULTIMEDIA EN REDES IP....77
10.1. Introducción....77
10.2. El protocolo H.323....78
10.3. Protocolo SIP....82
11. VÍDEO-DIFUSIÓN Y VÍDEO BAJO DEMANDA....85
12. ANEXO I – Cortafuegos....86
13. ANEXO II – Comandos para la gestión de red....87
14. ANEXO III - La VC en el campo educativo....98
14.1. Introducción....98
14.2. Técnicas de realización....98
14.3. Elementos que el profesor tiene que contemplar....99

1. INTRODUCCIÓN

1.1. Conceptos

Red de comunicaciones

Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -*master/slave*-). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc.). La información se puede transmitir de forma analógica, digital o mixta, pero en cualquier caso las conversiones, si las hay, siempre se realizan de forma transparente al usuario, el cual maneja la información de forma analógica exclusivamente.

Las redes más habituales son las de ordenadores, las de teléfono, las de transmisión de audio (sistemas de megafonía o radio ambiental) y las de transmisión de vídeo (televisión o vídeo vigilancia).

Capacidad de transmisión

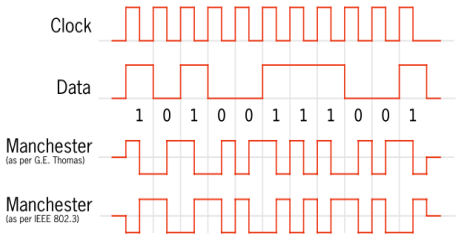
La capacidad de transmisión indica el número de bits por segundo que se pueden transmitir a través de una conexión. A menudo se llama erróneamente velocidad de transmisión (que depende de la capacidad y de otros factores) o ancho de banda (que es la amplitud de onda utilizable). En este texto usaremos ancho de banda como sinónimo de capacidad de transmisión excepto cuando se hable explícitamente de frecuencias de onda.
En el contexto de velocidades o capacidades de transmisión (caudales), los prefijos (K, M, G, ...) se utilizan con su significado métrico de potencias de 10 (10^3, 10^6, etc.).
En el contexto de almacenamientos, *buffers*, etc, los prefijos significan potencias de 2 (2^{10}, 2^{20}, etc.)[1].

Control de flujo

Capacidad del receptor de enviar un mensaje al emisor para indicarle que deje de enviar momentáneamente datos porque no se puede garantizar la recepción correcta de ellos (porque hay saturación de *buffers*, por ejemplo).

Codificaciones eléctricas

El código eléctrico más simple, el unipolar establece un valor de voltaje para indicar un 1 y otro valor para indicar un 0 (p.e.: bit 1=+0,85V y bit 0=-0,85V). Este código no tiene límites en su componente continua: si debemos enviar muchos bits consecutivos a 1, la señal debe mantenerse varios ciclos de reloj al voltaje necesario.
Esto hace que una señal continua se desincronice fácilmente si para emisor y receptor la señal no ha durado los mismos ciclos de su reloj. Además la mayoría de medios de comunicaciones de red no pueden transportar una componente continua. Por ello se utilizan códigos en línea (modulación en banda base o codificación eléctrica) que eliminan la componente continua y facilitan la sincronización de relojes de emisor y receptor.



Existen dos modos básicos de realizar la codificación eléctrica:

- Diseñar cada código transmitido de tal forma que contenga el mismo número de impulsos positivos que negativos, así se anularía la componente continua. Por ejemplo el código Manchester[2].
- Realizar una traducción de la señal usando un código de disparidades emparejadas o código alternante. Es decir, algunos o todos los símbolos están representados por dos conjuntos de dígitos, de disparidad opuesta, que se utilizan en una secuencia de manera que se minimice la componente continua y se facilite la sincronización[3].

1 La CEI definió en 1999 los símbolos para potencias de dos: kibi (Ki), mebi (Mi), gibi (Gi), tebi (Ti), pebi (Pi) y exbi (Ei).
2 El código Manchester, también denominado codificación bifase-L, es un método de codificación eléctrica de una señal binaria en el que en cada tiempo de bit hay una transición entre dos niveles de señal. Así 1 es una transición de alto a bajo y 0 es una transición de bajo a alto (o al revés). Es un código autosincronizado, ya que en cada bit se puede obtener la señal de reloj, lo que hace posible una sincronización precisa del flujo de datos. Una desventaja es que consume el doble de ancho de banda que una transmisión asíncrona.
3 La codificación de traducción utiliza un código en línea (modulación en banda base) que traduce símbolos para conseguir un balance de corriente y permitir la sincronización de la señal. 4B/5B utiliza MLT para traducir símbolos de 4 bits en símbolos de 5 bits. 8B/6T utiliza PAM para traducir 5 binarios en 6 ternarios. PAM 5x5 utiliza códigos quinarios (5 voltajes diferentes).

Encaminamiento (Enrutamiento o *Routing*)

Cada nodo intermedio de una comunicación debe conocer dónde ha de enviar el paquete que ha recibido. En el caso de los circuitos (conmutados o virtuales) solo se toma la decisión en el inicio de la conexión. En el caso de paquetes conmutados (datagramas) se toma la decisión con cada paquete.
Este proceso de decisión se denomina encaminamiento (*routing*).

La solución más sencilla pero ineficaz es enviar el paquete por todos los interfaces menos por el que llegó (inundación). Es el funcionamiento de los concentradores. Este sistema no se considera un protocolo de encaminamiento.
Para encaminadores (*routers*) sencillos se puede utilizar configuraciones estáticas de encaminamiento.
Los encaminadores más modernos permiten utilizar auténticos protocolos de encaminamiento dinámico que sirven para intercambiar información entre encaminadores y adaptarse a situaciones cambiantes de tráfico basándose en:

- Capacidad del enlace.
- Tráfico medio.
- Retardo.
- Fiabilidad.

Las técnicas básicas son:

- Vector de distancia: Cada encaminador mantiene una tabla con las distancias mínimas hacia cada posible destino y el interfaz de salida. Le pasa esta información a todos sus vecinos. Tiene el problema de la cuenta a infinito.
- Estado de enlace. Identifica a sus vecinos y su coste y manda esa información a todos los encaminadores de la red. Con esa información se calcula el mapa de la red.

Debido a que los protocolos de encaminamiento no son escalables se utiliza encaminamiento jerárquico. Esto simplifica el intercambio de información aunque puede no aprovechar todos los caminos mínimos.

Cada nodo intermedio de una comunicación puede utilizar variantes de dos técnicas de reenvío:

- ***Store-and-forward***: Almacena completamente el paquete y luego, si es correcto, lo reenvía.
- ***Cut-througth***: Conforme recibe el paquete, y una vez que sabe por que puerto lo tiene que reenviar, empieza su retransmisión. Si después el paquete resulta erróneo se propaga el error al siguiente nodo. Esta técnica es más rápida y sencilla para redes fiables.

Calidad de Servicio (QoS: *Quality of Service*)

La congestión es la situación en la que un equipo o una línea no puede procesar todo el tráfico que se le envía. La congestión puede provocar pérdida de datos y baja mucho el rendimiento de la red.
Para resolverla, en conexiones punto a punto se utiliza el control de flujo, que puede aplicarse a nivel de enlace o de transporte.
Un factor que propicia la congestión es la tendencia del tráfico a generarse a ráfagas.

Una red puede comprometerse a garantizar una serie de parámetros de una conexión o servicio. El contrato que especifica los parámetros de QoS se denomina Acuerdo de Nivel de Servicio (SLA: *Service Level Agreement*). Los parámetros que se pueden garantizar son:

- Ancho de banda (*Throughput*) mínimo.
- Retardo o latencia máximo.
- Fluctuación del retardo (*Jitter*) máxima.
- Pérdida de datos tolerable.
- Disponibilidad del servicio (en % del tiempo).

Los tipos de servicio que puede dar una red desde el punto de vista de la QoS son:

- Mejor esfuerzo posible (*Best Effort Service*): La red no se compromete a nada, pero intentará que los datos lleguen al otro extremo lo antes posibles.
- Con servicio diferenciado (*soft QoS o Differentiated Service*): Trata cierto tráfico con más preferencia que otro, pero no garantiza nada a ninguno de ellos.
- Con servicio garantizado (*hard QoS o Guaranteed Service*): Se definen unos valores límite requeridos al establecer una conexión extremo a extremo y todos los nodos de la red se comprometen a garantizarlos, reservando los recursos necesarios.

Para implementar QoS es necesario utilizar técnicas de:

- Gestión de tráfico individual en cada encaminador de la red:
  - Gestión de colas.
  - Perfilado de tráfico (*Traffic Shaping*)
  - Vigilancia de tráfico (*Traffic Policing*)
- Señalización entre los elementos de la red:
  - Marcado de paquetes descartables.
  - Envío de paquetes de asfixia.
  - Descarte selectivo de paquetes.
  - Marcado de Prioridad en paquetes.
  - Control de admisión y reserva de recursos.
- Mejora del aprovechamiento de enlaces lentos:
  - Fragmentación de paquetes grandes
  - Compresión de datos

1.2. Tipos de red

Las redes se pueden clasificar de diferentes maneras. Las principales clasificaciones son:

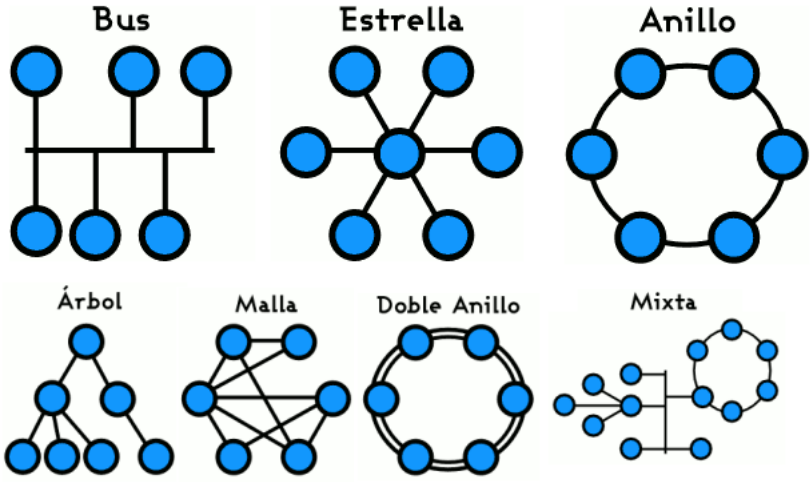
- **Por su extensión**: Redes de área personal (PAN), local (LAN), extensa (WAN)... (ver cuadro inferior).
- **Por su topología**: Estrella, bus, anillo, malla, mixta...
- **Por su conexión física**: se clasifican en redes punto a punto (*unicast*) y redes multipunto o de difusión (*broadcast*).
- **Por su técnica de transmisión de datos**: líneas dedicadas, circuito conmutado o paquetes conmutados.
- **Por su uso**: se clasifican en redes privadas o corporativas y redes públicas.
- ...

Por su extensión

Diámetro	Tipo
< 0,01 m	Paralelismo masivo. Procesadores multi-núcleo.
< 0,1 m	Multiprocesadores.
< 10 m	Redes de área personal (PAN: *Personal Area Network*). Redes de infrarrojos o *bluetooth*.
10 m – 3 km	Redes de área local (LAN: *Local Area Network*) y metropolitana (MAN). Ethernet, Wi-Fi.
> 3 km	Redes de área extensa (WAN: *Wide Area Network*) o redes interconectadas. Frame-Relay, RDSI, ATM, SONet/SDH.

Por su topología

La topología de una red es el diseño de las comunicaciones entre los nodos de la red. Las topologías principales son tipo bus compartido (o símplemente bus), estrella o anillo aunque existen más topologías.



Hay que diferenciar entre la topología física, que define como están conectados físicamente los nodos y la topología lógica que es como tratan los nodos las conexiones. Así por ejemplo se puede disponer de una red física en estrella donde el nodo central es un concentrador y el resto de nodos son equipos utilizando para comunicarse el protocolo Ethernet original, que considera el medio utilizado como una topología de bus compartido.

Por su conexión física

- **Redes punto a punto (*unicast*)**: basadas principalmente en cable y en cada conexión intervienen solo dos equipos. Tienen problemas de tipología. Se subdividen en:
  - **Simplex**: inútil en redes de computadores (monodireccional).
  - **Semi-dúplex *(Half-duplex)***: envía datos cada vez en un sentido.
  - **Dúplex *(Full-duplex)***: envía datos en los dos sentidos a la vez.

  En las redes semi-dúplex y dúplex se puede disponer de la misma capacidad en las dos direcciones de transmisión (conexión simétrica) o no (conexión asimétrica).

  Ejemplos de redes punto a punto: LANs en estrella con conmutadores centrales y la mayoría de las WAN (enlaces telefónicos, X.25, Frame Relay, RDSI, ATM, etc.).

- **Redes multipunto o redes de difusión (*broadcast*)**: basadas principalmente en bus compartido (cable bus y anillo) y redes inalámbricas (radio, satélites...); todos los equipos comparten el mismo medio de transmisión. Tienen problemas de colisiones que se pueden afrontar con una gestión:
  - Estática (TDM): No emite si alguien lo está haciendo.
  - Dinámica (Centralizada o Distribuida).

  Las emisiones pueden estar marcadas como *unicast*, *multicast* o *broadcast*, pero no garantizan la confidencialidad.

  Ejemplos de redes multipunto: transmisiones vía radio o satélite, redes CATV y la mayoría de las LANs originales (Ethernet original, FDDI, Token Ring, Inalámbricas, etc.).

Por su técnica de transmisión de datos

Líneas dedicadas. Enlace punto a punto permanente y siempre disponible. Se utilizan principalmente en redes WAN con velocidades prefijadas por el proveedor, generalmente simétricas y full-dúplex. Otro caso habitual es el radio enlace. El nivel de enlace utilizado suele ser HDLC o PPP. Suelen tener un coste elevado por lo que solo son adecuadas si hay mucho tráfico continuo.

Modelos de circuito conmutado (*Circuit Switching*). En ellos las comunicaciones no comparten los medios. Al iniciarse la comunicación se reserva los recursos intermedios necesarios para establecer y mantener el circuito. Si el canal se corta se corta la comunicación. Los dispositivos mantienen información sobre el estado de la comunicación (*statusfull*). Utilizado en la Red Telefónica Conmutada (RTC[4]) incluyendo:

- Red Telefónica Básica (RTB) -analógica-.
- Red Digital de Servicios Integrados (RDSI o ISDN) -digital-.
- GSM (*Global System for Mobile Comunications*) -digital por radioenlace-.

Una vez establecido el el circuito se comporta como una línea dedicada ofreciendo un transporte físico de bits sobre el que se puede utilizar cualquier protocolo de nivel de enlace.
El costo es proporcional al tiempo y la distancia de conexión.

Modelos de paquetes conmutados (*Packet Switching*). En ellos las comunicaciones se dividen en paquetes que comparten los medios. Se pueden utilizar varios enlaces en cada interfaz físico.
Ofrece un medio físico de transmisión de datos para los equipos. Existen dos submodelos:

- **Datagramas**: Cada paquete debe estar delimitado e identificado y llevar la dirección destino, y cada uno se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo. En este modelo no sabemos si los paquetes van a llegar todos ni si van a llegar por orden (ni si van a llegar sin errores). Los dispositivos no mantienen información sobre el estado de la comunicación (*stateless*). Es el modelo más sencillo de implementar y el único que soporta multidifusión (*multicast*). Se puede asimilar al sistema de correo tradicional.
- **Circuitos virtuales (VC: *Virtual Circuit*)**: Simula un circuito conmutado, pero compartiendo los medios. Primero se establece una conexión y los equipos intermedios reservan una parte de sus recursos; después todos los paquetes siguen la misma ruta ordenadamente. Este modelo es utilizado en telefonía digital GPRS y redes como X.25, Frame Relay o ATM.
  - **PVC (*Permanent VC*)**: Los PVC son circuitos virtuales definidos estáticamente y permanentes.
  - **SVC (*Switched VC*)**: Se establecen y terminan a petición del usuario de forma dinámica. La implementación de circuitos virtuales es más compleja que la de circuitos permanentes.

Otra división de redes por su técnica de transmisión de datos sería en **servicios orientados a conexión** – que incluiría los modelos de líneas dedicadas, circuito conmutado y circuito virtual- y **servicios no orientados a conexión** -el modelo de datagramas-.

La primera red (ARPANET) nació en 1964 y unía cuatro nodos con un protocolo de datagramas (NCP).

4 RTC o PSTN: *Public switched telephone network*

1.3. Redes de área local (LAN)

El comité de estándares IEEE 802 LAN/MAN es el encargado de desarrollar estándares de redes PAN, LAN y MAN. Los estándares ISO 8802.x se corresponden con los estándares IEEE 802.x. Los más utilizados son:

- 802.1 – Definición de interfaces
  - 802.1d – Puentes y conmutadores. Define el protocolo "*Spanning Tree*".
  - 802.1e – Gestión de la carga de la red
  - 802.1p (integrado posteriormente en 802.1q) – Tráfico por prioridades
  - 802.1q – VLANs
  - 802.1x – Control de acceso a redes en base a puertos
- 802.3 – Ethernet CMSA/CD
  - 802.3u – Fast-Ethernet
  - 802.3x – Full-Duplex
  - 802.3z – Gigabit Ethernet Fibra
  - 802.3ab – Gigabit Ethernet Cobre
  - 802.3ae – Gigabit Ethernet (En desarrollo)
- 802.4 – Token Bus
- 802.5 – Token Ring
- 802.8 – FDDI
- 802.11 – Inalámbrica (Wi-Fi)
  - Ver el apartado IEEE 802.11 para un detalle de las principales revisiones.
- 802.14 – Módems
- 802.15 – Inalámbrica PAN
  - 802.15.1 – Bluetooth
- 802.16 – Inalámbrica MAN (WMAN)
- 802.20 – Inalámbrica MAN con movilidad (Mobile Wi-Fi)

1.4. Redes de área extensa (WAN)

A diferencia de las redes locales, cuya infraestructura es generalmente propiedad y responsabilidad del usuario, las redes de área extensa (WAN) normalmente utilizan redes de proveedores. Inicialmente estas redes eran únicamente las instaladas para la transmisión de voz por las compañías telefónicas, pero hoy en día se utilizan también redes creadas específicamente para datos por distintos proveedores (compañías de telecomunicaciones).
Así las primeras redes se caracterizaban por su baja velocidad y su alta tasa de errores, además de por su alto costo. Hoy en día existen sin embargo redes de gran fiabilidad y velocidad, aunque el costo suele seguir siendo alto.
Casi siempre son redes punto a punto (excepto redes de satélites) sobre líneas E1/T1 o sobre la RTC dependientes de un proveedor de servicios. Por ello se utilizan servicios orientados a conexión: líneas dedicadas, circuitos conmutados y circuito virtuales.

Algunos ejemplos de WAN:

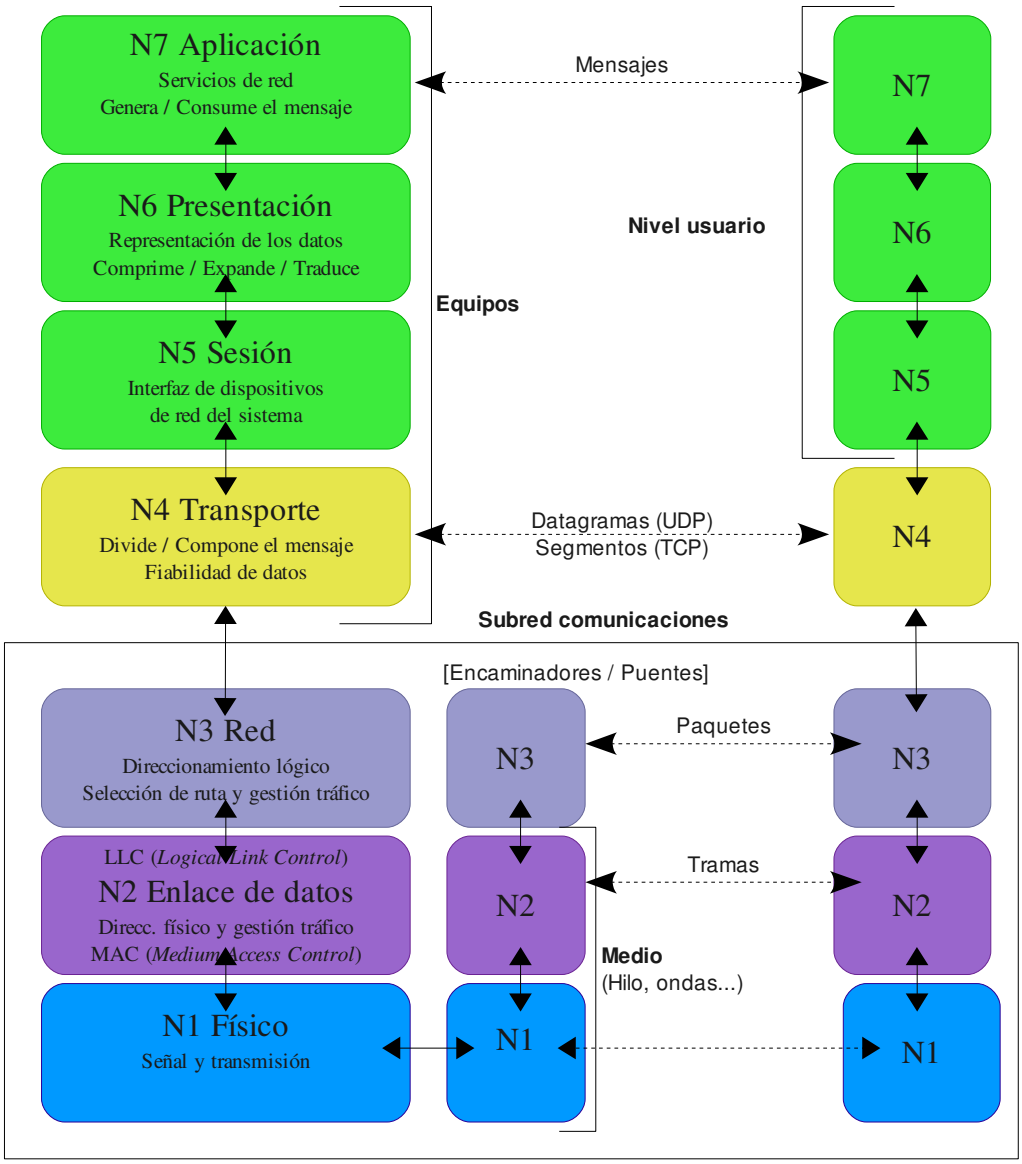
	Conexión permanente	**Conexión temporal**
Circuito Real	Líneas dedicadas E1/T1	Conmutación de circuitos RTB, RDSI, GSM
Circuito Virtual	Redes de conmutación con PVCs X.25, Frame Relay, ATM	Redes de conmutación con SVCs X.25, Frame Relay, ATM

2. EL MODELO ISO OSI

(*Open Systems Interconnection Basic Reference Model*)

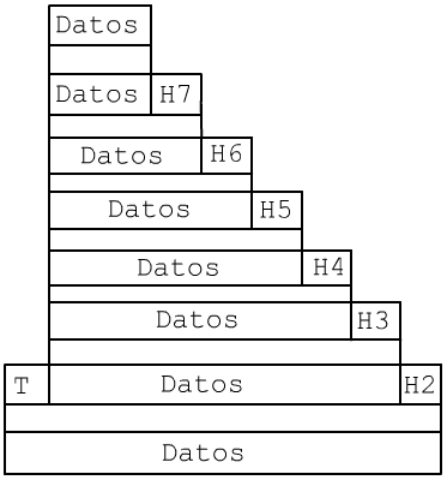
Este es el modelo de referencia para la descripción de las arquitecturas de redes (conjunto de capas y protocolos de red), aunque raramente se ha implementado por completo. Su objetivo es conseguir que un conjunto heterogéneo de equipos autónomos (no jerárquico -*master/slave*-) comunicados por medios de baja calidad también heterogéneos, aparezca ante el usuario como un medio homogéneo y fiable.

Antes de ISO OSI cada arquitectura de red dependía del fabricante y de protocolos propietarios (SNA, Appletalk, NetWare, DECnet...). ISO e ITU-T colaboraron a partir de finales de los 70 para estandarizar un modelo de referencia para redes que se aprobó en 1984 (ISO 7498:1984). Aunque OSI sigue siendo el modelo teórico de referencia, en 1996 se renunció definitivamente a su implementación práctica debido a que, mientras se desarrollaban los trabajos de diseño y estandarización de OSI, la pila TCP/IP se había ya convertido en el estándar de hecho en los niveles 3 y 4, mientras que en las capas 1 y 2 Ethernet y Token Ring asumían el mismo rol en las redes de área local.



Cada nivel es independiente de los demás y se comunica únicamente con los niveles inmediatamente superior y/o inferior por medio de interfaces. Así cada nivel aporta una cabecera, de forma que los datos realmente comunicados entre aplicaciones (N7) son solo una parte de los transmitidos físicamente (N1). Esto causa sobrecarga (*overhead*) pero aporta gran flexibilidad al sistema.

A nivel lógico cada capa se comunica con las aplicaciones de su misma capa en otra máquina a través de las capas inferiores.



2.1. Niveles de red del modelo OSI

Subred de comunicaciones (Niveles 1, 2 y 3)

La **capa física** (N1) se encarga de transmitir los bits de información a través del medio utilizado. Es responsable de las conexiones físicas del equipo con la red en lo que se refiere al medio físico (cable de distintos tipos, radio, infrarrojos...), características del medio (p.e. tipo de cable o calidad del mismo; tipo de conectores normalizados o de antena...) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, velocidad de transmisión, etc.). Para ello establece interfaces mecánicas, eléctricas y de procedimiento, en base a las características del medio de transmisión (Manchester, 4B/5B, DSSS...).
El medio de transmisión, por ejemplo un cable, se convierte en un almacén intermedio (*buffer*) lo que produce bastantes problemas de comunicación. Además esto hace que los ficheros grandes tengan más probabilidades de sufrir errores, por lo que se seccionan en paquetes. Al mejorar las conexiones físicas se puede utilizar tramas mayores (*Jumbo frames*).

La **capa de enlace** (N2) pretende ser capaz de proporcionar un tránsito de datos fiable a través de un enlace físico. Para ello debe crear y reconocer los límites de las tramas, así como opcionalmente resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas y colisiones en conexiones de multidifusión. También puede incluir algún mecanismo de control del flujo que evite la saturación de un receptor que sea más lento que el emisor.
Suele tener una conexión con el nivel físico (MAC -*Medium Access Control*-) y varias con el nivel de red (LLC -*Logical Link Control*-).
A este nivel se implementa la calidad del servicio de red o QoS (*Quality of Service*). Cada usuario contrata con la red un tipo de servicio y una calidad (p.e: mayor prioridad, mayor ancho de banda...).

Sistemas de control de errores

- *Unack conectionless*: ningún control. Fácil y rápido. Para redes de nivel 1 (físicas) muy fiables.
- *Ack conectionless*: informa de errores, pidiendo reenvíos al emisor.
- *Ack conection oriented*: informa de errores, pide reenvíos y ordena los paquetes.

Por tanto la capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red (MAC: *Medium Access Control*), de la distribución ordenada de tramas y opcionalmente del control del flujo, de la notificación de errores y de la calidad del servicio (QoS).

Los concentradores (*hubs*) actúan exclusivamente a nivel físico (N1) y, entre otras cosas, no controlan las colisiones; mientras que los conmutadores (*switches*) actúan a nivel de enlace.

El cometido de la **capa de red** (N3) es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Para ello se basan en dos aspectos: el direccionamiento y el encaminamiento (utilizando encaminadores (*routers*), a veces llamados "enrutadores").
Adicionalmente la capa de red debe gestionar la congestión de red.

Nivel de transporte (Nivel 4)

El **nivel de transporte** (N4) se encarga de efectuar y asegurar el transporte de los datos de la máquina origen a la máquina destino, independizándolo del tipo de red física que se esté utilizando. En el modelo de Internet los protocolos de transporte también determinan a que aplicación van destinados los datos.

Sesión y presentación (Niveles 5 y 6)

En la práctica el nivel de sesión (N5) nunca se implementa por separado, sino con el nivel de presentación (N6).
La **capa de sesión** (N5) establece, gestiona y finaliza las conexiones entre usuarios (procesos o aplicaciones) finales. Se encarga de controlar la sesión, la concurrencia y la reanudación en caso de interrupción.
La **capa de presentación** (N6) se encarga de la representación de la información. Esta capa es la primera en trabajar más el contenido de la comunicación que la forma en que se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible. Además permite cifrar los datos y comprimirlos.

Nivel de aplicación (Nivel 7)

El **nivel de aplicación** (N7) ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de red y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

El nivel de aplicación abstrae al usuario del acceso a la red. El usuario utiliza aplicaciones que son las que interactúan en este nivel. Así por ejemplo un usuario para utilizar el protocolo HTTP interactúa con un navegador, no manda una petición "`HTTP/1.0 GET index.html`" para conseguir una página en html, ni lee directamente el código html/xml.

3. EL MODELO INTERNET

3.1. Un poco de historia

Los protocolos TCP/IP (*Transmission Control Protocol / Internet Protocol*) fueron desarrollados por la agencia DARPA (*Defense Advanced Research Projects Agency*). En primavera de 1973 se unieron para desarrollar modelos de interconexión entre distintas arquitecturas[5] Robert E. Kahn y Vicent Cerf, el desarrollador del protocolo NCP (*Network Control Program*) que se utilizaba en ARPANET.
En verano de 1973 hicieron una reformulación fundamental del protocolo: las diferencias entre protocolos de red quedarían escondidas usando un protocolo común entre redes (*Internetwork Protocol*) y la responsabilidad de la fiabilidad caería sobre los equipos, en vez de sobre la red. Para ello se inspiraron en la red Cyclades desarrollada por Hubert Zimmerman y Louis Pouzin.
Un equipo de red especial llamado encaminador (*router*), con una conexión a cada red, se encarga de enviar paquetes entre ellas. El papel de los encaminadores está definido en el RFC 1812 (*Request For Comments* 1812).

Al reducir el papel de la red al mínimo se pudo conectar con cualquier red[6], solventando el problema inicial de Kahn para interconectar las redes de satélites y las de radio. Cerf y su equipo de Stanford desarrollaron con detalle el nuevo modelo, generando la primera especificación de TCP (RFC 675). En 1978 se publico la versión estable -TCP/IP versión 4- que aún se utiliza en Internet.
En 1980 David P. Reed diseñó el protocolo UDP (*User Datagram Protocol*, también llamado *Universal Datagram Protocol*) para trabajar sobre IP con un esquema de datagramas -no orientado a conexión-.
En 1982 el departamento de defensa de los EE.UU. seleccionó TCP/IP como su protocolo estándar y el 1 de enero de 1983 ARPANET mudó sus sistemas al nuevo protocolo.

En 1992 nace la ISOC (*Internet SOCiety*) una entidad pública internacional sin ánimo de lucro, para dirigir el desarrollo de Internet[7]. Así en Enero de 1992 el IAB (*Internet Architecture Board*) pasa a depender de esta nueva sociedad, dejando de depender del departamento de defensa de EE.UU.
El IAB es responsable de la edición y publicación de los RFCs (*Request For Comments*); es la autoridad oficial sobre los números de Internet (IANA[8]: *Internet Assigned Numbers Authority*)[9]; supervisa las actividades de las IxTF como la IETF (*Internet Engineering Task Force*) -que ratifica los estándares oficiales de Internet- o la IRTF (*Internet Research Task Force*)...

3.2. Familia de protocolos de Internet

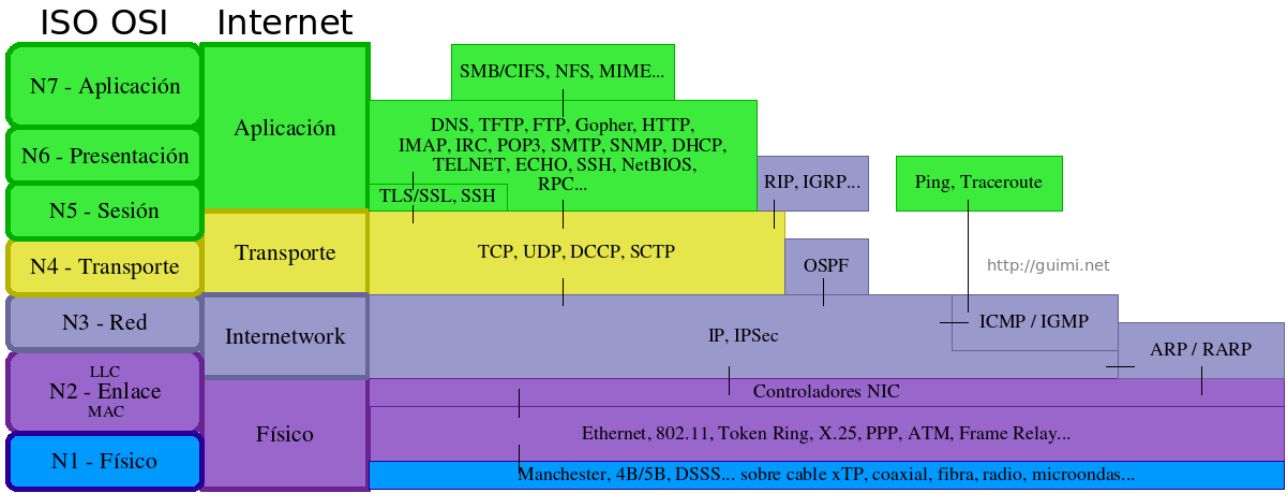
La pila IP forma un conjunto de protocolos que utiliza tanto el origen como el destino para la comunicación de datos a través de una red de paquetes conmutados. Este conjunto no está orientado a la conexión entre equipos, sino a la interconexión de redes que ya están implementadas en origen, por tanto no pretende competir con el modelo OSI, sino implementar una parte de sus niveles.
Así el conjunto TCP/IP no hace ninguna referencia al nivel de usuario ni al nivel físico, sino únicamente al nivel de encaminamiento entre redes (protocolo IP) y al de transporte (por medio de los protocolos TCP y UDP).
Sin embargo en la práctica la gran mayoría de redes, y en concreto Internet, se basan en IP para generar redes, es decir para conectar equipos, complementando TCP-UDP/IP con protocolos a nivel de usuario "por arriba" y a nivel físico "por debajo", generando una pila de protocolos conocida como familia de protocolos de Internet o modelo Internet.

5 Pretendían conectar con ARPANET una red de paquetes satelitales (SATNET -conectaba EE.UU., Noruega y Reino Unido-) con redes de paquetes de radio (PRNETs -como ALOHAnet de la Universidad de Hawaii-).
6 Se solía decir que TCP/IP debería funcionar incluso entre dos latas unidas por una cuerda. (Ver portada ;-).
7 "*...to assure the open development, evolution and use of the Internet for the benefit of all people throughout the world.*"
8 El primer IANA fue Jon Postel, que también era el editor de los RFCs. Protagonizó la rebelión de Internet frente al gobierno Clinton que dio pie a la creación de ISOC e ICANN (1998/02/28).
9 En la práctica es ICANN (*Internet Corporation for Assigned Names and Numbers*), quién desde su fundación en 1998 gestiona los dominios principales genéricos y de países (*generic -gTLD- and country code -ccTLD- Top-Level Domain*). La renovación del contrato (2006) fue polémica porque se solicitaba que el IANA fuese una agencia de la ONU en vez de una organización de EE.UU. -aunque sea no lucrativa- sobre cuyas decisiones el gobierno de EE.UU. tiene derecho de veto.

Efectivamente muchas redes van implementadas cada vez más sobre el protocolo Internet que no controla errores, ni congestión, ni disponen de garantías de QoS (*Quality of Service*); en parte confiando en la mejor calidad de los medios actuales, en parte obviando el control de errores para protocolos de tiempo real, como transmisión de audio y vídeo, donde por ejemplo no tiene sentido retransmitir parte del fotograma que se emitió hace 2 segundos.
De la misma manera, como TCP/IP no tiene un nivel de sesión unificado sobre el que los niveles superiores se sostengan, estas funciones son típicamente desempeñadas (o ignoradas) por las aplicaciones de usuario.

Comparación entre el modelo OSI y el modelo de Internet

El modelo OSI fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de ordenadores. En cambio el modelo de Internet fue creado como la solución a un problema práctico. Aunque la familia de protocolos de Internet puede describirse por analogía con el modelo OSI, en la práctica no se corresponden exactamente.
Concretamente hay protocolos de la familia Internet (ICMP, IGMP) que funcionan sobre IP pero se utilizan para control de comunicaciones, por lo que por pila estarían en el nivel OSI N4 (al ir encima de IP -N3-) pero por función estarían en parte como OSI N3 (red), en parte como OSI N2 (enlace, direccionamiento físico).
También existen protocolos de comunicación entre encaminadores (IGP: *Interior Gateway Protocol*) que funcionan sobre IP (OSPF) o sobre TCP-UDP (RIP, BGP, IGRP, EIGRP) y podrían llegar a considerarse parte del nivel de enlace.
Igualmente los protocolos ARP (*Address Resolution Protocol*) y RARP (*Reverse* ARP) que forman parte de la familia IP, operan por encima del nivel de enlace (N2 OSI) pero por debajo de IP (N3 OSI).



3.3. Protocolo Internet (IP)

Diseño de IP

La versión más utilizada de IP (*Internet Protocol*) todavía es la 4 (IPv4), la primera versión estable que se publicó. La versión 5 es experimental y la versión 6 está sustituyendo progresivamente a la versión 4.

IP utiliza un esquema de red no fiable de datagramas o paquetes independientes. En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes. Aunque IP define clases de paquetes, no provee ningún mecanismo para determinar si un paquete alcanza o no su destino, ni verifica la integridad de los datos transmitidos. Al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.
En v4 verifica la integridad de sus cabeceras (mediante *checksums* o sumas de comprobación), pero en v6 ya no.

Direccionamiento y encaminamiento

Los aspectos principales de IP son el direccionamiento y el encaminamiento. Cada interfaz de red (NIC: *Network Interface Card*) se identifica por medio de una dirección IP unívoca. Además cada NIC está asignado a una subred. La clasificación de redes estaba definida inicialmente en la propia dirección IP, pero en 1993 IETF definió el sistema CIDR (*Classless Inter-Domain Routing*) que estableció la gestión de subredes mediante el uso de la máscaras de red[10].

Una red IP (o una subred) comprende un rango de direccionamiento IP. Cuando un equipo va a enviar un paquete a otro equipo -identificado por su dirección IP- comprueba si la dirección del destinatario está en su misma subred. En caso de ser así emite el mensaje dando por supuesto que el equipo destinatario será capaz de escucharlo (como debería ser si la configuración es correcta y el otro equipo está operativo). Si el equipo destinatario está en otra red diferente a la del remitente, éste enviará el mensaje a la puerta de enlace (*gateway*) que tenga configurada -si la tiene-.
Podemos apreciar que un equipo sin puerta de enlace solo será capaz de comunicarse con su propia subred, y que la puerta de enlace de un equipo debe encontrarse en su misma subred.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los conmutadores de paquetes (*switches*) y los encaminadores (*routers*) para decidir el tramo de red por el que reenviarán los paquetes.

La configuración IP (dirección, máscara y pasarela) puede asignarse de manera estática (especificándose en cada equipo) o dinámica, mediante DHCP (*Dynamic Host Configuration Protocol*). Puede generar confusión el que se suele decir que un equipo tiene IP fija si siempre tiene la misma dirección IP y que tiene IP dinámica si su dirección IP varía con el tiempo. Sin embargo puede asignarse siempre la misma dirección al mismo equipo dinámicamente por DHCP.

Fragmentación en v4

En IPv4 si el paquete a transmitir supera el tamaño máximo negociado (MTU: *Maximum Transmission Unit*) en el tramo de red por el que va a circular, podrá ser dividido en paquetes más pequeños, y reensamblado luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de la congestión de las rutas en cada momento. Si uno de los fragmentos se pierde, todo el paquete original se considerará perdido, y los restantes fragmentos se descartarán.
Esto puede ocurrir por ejemplo con los protocolos ICMP o UDP, pero no con el protocolo TCP que adapta su tamaño de paquete para que no deba ser fragmentado. Para ello al inicio de la comunicación utiliza una técnica de tanteo enviando paquetes IP con el bit "No fragmentar" activado para encontrar el tamaño de MTU adecuado[11].
IP no establece un MTU máximo, pero sí establece un MTU mínimo de 576 bytes para v4 y 1280 bytes para v6 que no permite fragmentación (solo en origen)[12].

10 Máscaras de subred de tamaño variable (VLSM: *Variable-Length Subnet Masks*).
11 Para facilitar esto, los encaminadores actuales al recibir un paquete no fragmentable demasiado grande incluyen el MTU en el mensaje de error.
12 Nótese que la MTU de IPv6 es menor que la MTU de Ethernet (1518B), lo que permite que IPv6 se pueda encapsular sobre Ethernet sin problemas.

Direccionamiento v4

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de red (NIC). IPv4 utiliza un direccionamiento de 4 bytes que permite aproximadamente 4.295 millones de direcciones (2^{32}), un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos para cada coche, teléfono, PDA o tostadora, lo que obliga a usar direccionamientos privados y NAT; mientras que el direccionamiento de 16 bytes de IPv6 soporta aproximadamente 340 sextillones de direcciones (2^{128}) -aproximadamente 670 mil billones de direcciones por cada mm2 de la superficie de La Tierra-.

En IPv4 las direcciones de 4 bytes (32 bits) se escriben en formato decimal punteado, es decir, 4 números decimales separados por puntos, representando cada uno 8 bits. Por tanto cada número debe estar en el rango [0-255].
Por ejemplo: "127.0.0.1".

Rangos de direcciones IPv4 reservadas (Intranets)

Dado que no puede haber dos interfaces con la misma dirección IP, dichas direcciones las otorgan organismos y entidades especialmente designadas, que delegan dicha autoridad jerárquicamente[13]. De este modo, los ISPs (proveedores de Internet, *Internet Services Provider*) disponen de rangos de IP que pueden otorgar.
Cuando un equipo se conecta a Internet necesita una IP pública ya sea variable o fija, que le proporciona su ISP.

Existen rangos de direcciones IPv4 que no se utilizan en la red pública, sino que están reservadas para redes internas ("intranets") cuyos equipos no disponen de conexión directa a Internet. Al reutilizarse los mismo rangos en todas las organizaciones todavía se consigue disponer de suficientes direcciones IP públicas para todos... aunque el límite ya casi se ha alcanzado[14]. Al utilizar direccionamiento privado, si se conecta dicha red privada a Internet, la pasarela obtiene una IP pública con la se conectan todos los equipos de la red privada utilizando una técnica llamada NAT (*Network Address Translation*).
Los rangos de IP v4 reservados para intranets son:

- 1 rango clase A: 10.x.x.x
- 16 rangos clase B: 172.16.x-172.31.x
- 256 rangos clase C: 192.168.0.x-192.168.255.x
- 1 rango clase B para enlace local[15]: 169.254.x.x

Clases de direcciones IP v4

Originalmente existían cinco clases de direcciones IP, indicadas por el primer 0 de los 4 primeros bits, pero solo se utilizan las tres primeras:

- Clase A: 7 bits de red || 24 bits de equipo (*host*), indicada por un 0 en el primer bit de dirección IP
  `0xxx xxxx.||xxxx xxxx.xxxx xxxx.xxxx xxxx` (0.0.0.0-127.255.255.255)
- Clase B: 14 bits de red || 16 bits de equipo, indicada por un 0 en el segundo bit de dirección IP
  `10xx xxxx.xxxx xxxx.||xxxx xxxx.xxxx xxxx` (128.0.0.0-191.255.255.255)
- Clase C: 21 bits de red || 8 bits de equipo, indicada por un 0 en el primer bit de dirección IP
  `110x xxxx.xxxx xxxx.xxxx xxxx.||xxxx xxxx` (192.0.0.0-223.255.255.255)
- Clase D: Multicasting, no utilizable
  `1110 xxxx.xxxx xxxx.xxxx xxxx.xxxx xxxx` (224.0.0.0-239.255.255.255)
- Clase E: Experimental, no utilizable
  `1111 xxxx.xxxx xxxx.xxxx xxxx.xxxx xxxx` (240.0.0.0 - 255.255.255.255)

13 La autoridad superior es la IANA (*Internet Assigned Numbers Authority*) que en este momento es la organización ICANN. Después aparecen por debajo los distintos ISPs (*Internet Services Providers*).
14 El principal objetivo de IPv6 es subsanar el agotamiento de direcciones IP disponibles. Además introduce optimizaciones en el protocolo.
15 Este sistema configura automáticamente una NIC asignando una IP aleatoria en el rango de enlace local tras verificar mediante ARP que está disponible. No configura pasarela ni servidores DNS (por eso "enlace local"). Llamado por Microsoft APIPA (*Automatic Private IP Addressing*).

Máscara de red

Como ya se ha dicho, el sistema de clases de red de IP quedó pronto sobrepasado, por lo que la IETF estableció en 1993 el sistema CIDR (*Classless Inter-Domain Routing*) que eliminó el uso de clases de direcciones IP y estableció la gestión de subredes mediante el uso de la máscaras de red. En IPv6 el concepto de clases se ha abandonado definitivamente.

Una máscara de red es un prefijo de n bits de valor '1' que se aplica sobre las direcciones IP y que se indica "/n". Así en IPv4 una máscara puede tener hasta 32 bits y en IPv6 hasta 128 bits.
Para conocer si dos direcciones IPs se encuentran en la misma subred basta con realizar una operación binaria AND entre la máscara y cada dirección; si el resultado es el mismo es que están en la misma red.

En IPv4 la máscara se puede especificar con la notación CIDR (/n) o con la misma notación que las direcciones IP.
Para IPv4 se definen tres clases de red básicas basadas en máscaras:

- Clase A: máscara de 8 bits (/8) o 255.0.0.0
- Clase B: máscara de 16 bits (/16) o 255.255.0.0
- Clase C: máscara de 24 bits (/24) o 255.255.255.0

Por ejemplo, dada la dirección IP 192.168.1.4 con máscara de 24 bits (/24 o 255.255.255.0).
La dirección en binario es: `1100 0000.1010 1000.0000 0001.0000 0100`.
La máscara en binario es: `1111 1111.1111 1111.1111 1111.0000 0000`.

Realizamos un AND binario entre dirección y máscara para obtener la red en la que se encuentra dicha dirección:

```
    1100 0000.1010 1000.0000 0001.0000 0100 [192.168.1.4]    IP
AND 1111 1111.1111 1111.1111 1111.0000 0000 [255.255.255.0]  Máscara
-----------------------------------------------------------------
    1100 0000.1010 1000.0000 0001.0000 0000 [192.168.1.0/24] RED
```

Para indicar la red de la dirección 192.168.1.4 con máscara de 24 bits puede escribirse en el formato CIDR como 192.168.1.0/24 y en el formato decimal punteado como 192.168.1.0/255.255.255.0.

Es fácil ver por tanto que dada una dirección IP a.b.c.d:

- La red de clase A (/8) estará formada por todas las direcciones a.x.x.x (red a.0.0.0/8)
- La red de clase B (/16) estará formada por todas las direcciones a.b.x.x (red a.b.0.0/16)
- La red de clase C (/24) estará formada por todas las direcciones a.b.c.x (red a.b.c.0/24)

Direccionamientos reservados

IPv4 contempla una serie de direcciones con significado especial y que por tanto no pueden utilizarse en interfaces de red normales:

- 127.x.x.x -> *loopback* (p.e. 127.0.0.1)
- Todos los bits a 0 -> equipo local
- Todos los bits a 1 (255.255.255.255) -> todos los equipos (difusión, *broadcast*)
- Todos los bits de equipo a 1 -> todos los equipos de la red (difusión limitada, *multicast*)
- Todos los bits de red a 0 -> un equipo de la red local

Generación de Subredes

Cuando disponemos de redes grandes y complejas, es interesante crear subredes, lo que facilita su administración.
Para crear subredes modificamos las máscaras de red, incrementando la cantidad de bits a 1 de la máscara.
El número n de bits a 1 de la máscara nos proporciona la cantidad de subredes generadas (2^n-2) y el número m de bits a 0 el número de equipos permitidos (2^m-2).

Limitación

Se puede comprobar que en realidad se generan 2^n subredes de 2^m equipos, pero por las restricciones de direccionamiento, solo podemos utilizar 2^n-2 y 2^m-2, ya que no se permiten las direcciones con todos los bits de red y/o todos los bits de equipo (*host*) con el mismo valor (todos a 1 o todos a 0), ya que son direcciones especiales.
En concreto el octeto "`1000 0000`" (128) no se debe utilizar para crear subredes porque generaría dos subredes que no se deben usar (todo 0 o todo 1 en el bit de red). Del mismo modo 255.255.255.254 es una máscara inútil porque solo permite dos direcciones que no se pueden usar (todo 0 o todo 1 en el equipo).
Algunas implementaciones (llamadas "*subnet-zero*") sí utilizan esas dos subredes (y también la máscara 128), pero no es una utilización correcta y en redes complejas puede generar problemas inesperados.

Tabla resumen de subredes

Bits Subred / Equipo	1 / 7 * `sxxx xxxx`	2 / 6 `ssxx xxxx`	3 / 5 `sssx xxxx`	4 / 4 `ssss xxxx`	5 / 3 `ssss sxxx`	6 / 2 `ssss ssxx`	7 / 1 * `ssss sssx`	8 / 0 * `ssss ssss`
Subredes / Rango	2 / 128 * `sxxx xxxx`	4 / 64 `ssxx xxxx`	8 / 32 `sssx xxxx`	16 / 16 `ssss xxxx`	32 / 8 `ssss sxxx`	64 / 4 `ssss ssxx`	128 / 2 * `ssss sssx`	256 / 1 * `ssss ssss`
Máscara	128 * `1000 0000`	192 `1100 0000`	224 `1110 0000`	240 `1111 0000`	248 `1111 1000`	252 `1111 1100`	254 * `1111 1110`	255 * `1111 1111`
Rangos efectivos (utilizables)	[0] * Inútil	[2] 64-128	[6] 32-64-96-128-160-192	[14] 16-32-48-64-80-96-112-128-144-160-176-192-208-224	[30] 8-16-24-32-40-48-... 200-208-216-224-232-240	[62] 4-8-12-16-20-24-... 232-236-240-244-248	[126] 2-4-6-8-... 250-252 *Inútil en el último octeto de la máscara	[254] * Se pasa de una red a 254 redes de clase inferior.

- En la primera fila vemos los bits de la máscara de red que dedicamos a crear subredes, marcados con 's', y los bits que dedicamos a equipos, marcados con 'x' (p.e. en la tercera columna dedicamos 3 a subredes y 5 a equipos `sssx xxxx`).
- En la segunda fila vemos el número de subredes creadas (2^s) y el rango de equipos en cada subred (2^x). Recordemos que siempre hay dos subredes y dos equipos por subred que no son utilizables (todo 0 y todo 1).
- La tercera fila indica el valor decimal de la máscara. Se puede obtener para cada celda fácilmente sumando al valor de la celda izquierda con el rango de la celda superior. P.e.: 128 + 64 = 192; 240 + 8 = 248 ...
- La cuarta fila nos indica los rangos efectivos (utilizables). Por ejemplo en la columna 3 -máscara 224-, si los rangos son de 32 direcciones y no podemos usar ni el primer rango (todos los bits de red a 0) ni el último (todos los bits de red a 1), los rangos resultantes serán 32-64-96-128-160-192.
- Nótese que en ningún caso se utilizan ni la primera ni la última subred (la que empieza en 0 y la que acaba en 255). La penúltima columna (máscara 254) no se puede utilizar en el último octeto (obtendríamos redes inviables de 2 equipos).

Ejemplos de subredes

Ejemplo 1 con red tipo B:
Rango de direcciones: 172.16.x.x (máscara inicial /16 o 255.255.0.0)
Queremos crear 6 subredes -> Tomamos la máscara 255.255.224.0 (`111|0 0000`)
Cada subred tiene un rango de direcciones de 32*255 -2 (x xxxx): [32-64-96-128-160-192]
Rangos de direcciones IP obtenidos:

```
172.16. 32.1 - 172.16. 63.254 (001|0 0000.0000 0001 - 001|1 1111.1111 1110)
172.16. 64.1 - 172.16. 95.254 (010|0 0000.0000 0001 - 010|1 1111.1111 1110)
172.16. 96.1 - 172.16.127.254 (011|0 0000.0000 0001 - 011|1 1111.1111 1110)
172.16.128.1 - 172.16.159.254 (100|0 0000.0000 0001 - 100|1 1111.1111 1110)
172.16.160.1 - 172.16.191.254 (101|0 0000.0000 0001 - 101|1 1111.1111 1110)
172.16.192.1 - 172.16.223.254 (110|0 0000.0000 0001 - 110|1 1111.1111 1110)
```

Ejemplo 2 con red tipo A:
Rango de direcciones: 10.x.x.x (máscara inicial /8 o 255.0.0.0)
Queremos crear 2 subredes -> Tomamos la máscara 255.192.0.0 (`11|00 0000`)
Cada subred tiene un rango de direcciones de 64*255*255 -2 (`xx xxxx`): [64-128-192]
Rangos de direcciones IP obtenidos:

```
10. 64.0.1 - 10.127.255.254 (01|00 0000.0000 0000.0000 0001 - 01|11 1111.1111 1111.1111 1110)
10.128.0.1 - 10.191.255.254 (10|00 0000.0000 0000.0000 0001 - 10|11 1111.1111 1111.1111 1110)
```

Ejemplo 3 con red tipo B:
Rango de direcciones: 172.18.x.x (máscara inicial /16 o 255.255.0.0)
Queremos crear 14 subredes -> Tomamos la máscara 255.255.240.0 (`1111| 0000`)
Cada subred tiene un rango de direcciones de 16*255 -2 (`xxxx`):
[16-32-48-64-80-96-112-128-144-160-176-192-208-224-240]
Rangos de direcciones IP obtenidos:

```
172.18. 16.1 - 172.18. 31.254 (0001| 0000.0000 0000.0000 0001 - 0001| 1111.1111 1111.1111 1110)
172.18. 32.1 - 172.18. 47.254 (0010| 0000.0000 0000.0000 0001 - 0010| 1111.1111 1111.1111 1110)
172.18. 48.1 - 172.18. 63.254 (0011| 0000.0000 0000.0000 0001 - 0011| 1111.1111 1111.1111 1110)
172.18. 64.1 - 172.18. 79.254 (0100| 0000.0000 0000.0000 0001 - 0100| 1111.1111 1111.1111 1110)
172.18. 80.1 - 172.18. 95.254 (0101| 0000.0000 0000.0000 0001 - 0101| 1111.1111 1111.1111 1110)
172.18. 96.1 - 172.18.111.254 (0110| 0000.0000 0000.0000 0001 - 0110| 1111.1111 1111.1111 1110)
172.18.112.1 - 172.18.127.254 (0111| 0000.0000 0000.0000 0001 - 0111| 1111.1111 1111.1111 1110)
172.18.128.1 - 172.18.143.254 (1000| 0000.0000 0000.0000 0001 - 1000| 1111.1111 1111.1111 1110)
172.18.144.1 - 172.18.159.254 (1001| 0000.0000 0000.0000 0001 - 1001| 1111.1111 1111.1111 1110)
172.18.160.1 - 172.18.175.254 (1010| 0000.0000 0000.0000 0001 - 1010| 1111.1111 1111.1111 1110)
172.18.176.1 - 172.18.191.254 (1011| 0000.0000 0000.0000 0001 - 1011| 1111.1111 1111.1111 1110)
172.18.192.1 - 172.18.207.254 (1100| 0000.0000 0000.0000 0001 - 1100| 1111.1111 1111.1111 1110)
172.18.208.1 - 172.18.223.254 (1101| 0000.0000 0000.0000 0001 - 1101| 1111.1111 1111.1111 1110)
172.18.224.1 - 172.18.239.254 (1110| 0000.0000 0000.0000 0001 - 1110| 1111.1111 1111.1111 1110)
```

Ejemplo 4 con red tipo C:
Rango de direcciones: 192.168.2.x (máscara inicial /24 o 255.255.255.0)
Queremos crear 6 subredes -> Tomamos la máscara 255.255.224.0 (`111|0 0000`)
Cada subred tiene un rango de direcciones de 32 -2 (`x xxxx`): [32-64-96-128-160-192-224]
ATENCIÓN: Como trabajamos con el último octeto debemos descontar las direcciones todo 0 y todo 1.
Rangos de direcciones IP obtenidos:

```
192.168.2. 33 - 192.168.2. 62 (001|0 0000.0000 0000.0000 0001 - 001|1 1111.1111 1111.1111 1110)
192.168.2. 65 - 192.168.2. 94 (010|0 0000.0000 0000.0000 0001 - 010|1 1111.1111 1111.1111 1110)
192.168.2. 97 - 192.168.2.126 (011|0 0000.0000 0000.0000 0001 - 011|1 1111.1111 1111.1111 1110)
192.168.2.128 - 192.168.2.158 (100|0 0000.0000 0000.0000 0001 - 100|1 1111.1111 1111.1111 1110)
192.168.2.161 - 192.168.2.190 (101|0 0000.0000 0000.0000 0001 - 101|1 1111.1111 1111.1111 1110)
192.168.2.193 - 192.168.2.222 (110|0 0000.0000 0000.0000 0001 - 110|1 1111.1111 1111.1111 1110)
```

Ejemplo 5 con red tipo B:
Rango de direcciones: 172.16.x.x (máscara inicial /16 o 255.255.0.0)
Queremos crear 126 subredes -> Tomamos la máscara 255.255.254.0 (`1111 111|0`)
Cada subred tiene un rango de direcciones de 2*255 -2 (`x`): [2-4-6-8-10-12-...252]
Rangos de direcciones IP obtenidos:

```
172.16.  2.1  - 172.18.  3.254 (0000 001|0.0000 0000.0000 0001 - 0000 001|1.1111 1111.1111 1110)
172.16.  4.1  - 172.18.  5.254 (0000 010|0.0000 0000.0000 0001 - 0000 010|1.1111 1111.1111 1110)
172.16.  6.1  - 172.18.  7.254 (0000 011|0.0000 0000.0000 0001 - 0000 011|1.1111 1111.1111 1110)
                                          [...]
172.16.248.1  - 172.18.249.254 (1111 100|0.0000 0000.0000 0001 - 1111 100|1.1111 1111.1111 1110)
172.16.250.1  - 172.18.251.254 (1111 101|0.0000 0000.0000 0001 - 1111 101|1.1111 1111.1111 1110)
172.16.252.1  - 172.18.253.254 (1111 110|0.0000 0000.0000 0001 - 1111 110|1.1111 1111.1111 1110)
```

Ejemplo de mezcla de subredes en una red tipo B:
Para una mayor flexibilidad, a veces se utilizan rangos de subredes distintos, cuidando que no se solapen.
Dada la complejidad de mantenimiento de este sistema no se recomienda su uso.

Rango de direcciones: 172.16.x.x (máscara inicial /16 o 255.255.0.0)
Combinando máscaras de 18, 19 y 21 bits podemos obtener 3 subredes de 8 equipos, 3 de 32 y 1 de 64:

```
/21 (255.255.248.0) 172.16.  8.1  - 172.16. 15.254
/21 (255.255.248.0) 172.16. 16.1  - 172.16. 23.254
/21 (255.255.248.0) 172.16. 24.1  - 172.16. 31.254
/19 (255.255.224.0) 172.16. 32.1  - 172.16. 63.254
/19 (255.255.224.0) 172.16. 64.1  - 172.16. 95.254
/19 (255.255.224.0) 172.16. 96.1  - 172.16.127.254
/18 (255.255.192.0) 172.16.128.1  - 172.16.191.254
```

Cabecera de trama de IPv4

<table>
<tr><th>0</th><th>4</th><th>8</th><th>16</th><th>19</th><th>31</th></tr>
<tr><td>Version</td><td>Hdr. len.</td><td>Type of Service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time To Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="6">Source IP Address</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="6">Options & Padding</td></tr>
</table>

- **Version**: Versión del protocolo: v4.
- **Hdr. Len.**: Indica la longitud de la cabecera en palabras de 32 bits y, por tanto, dónde empiezan los datos. Esta longitud es de 5 palabras (20 Bytes) más el campo "Opciones" si existe.
- **Type Of Service**: tipo de servicio de calidad solicitado (QoS).
- **Total Length**: longitud total del datagrama -cabecera y datos- en bytes.
- **Identification**: número del datagrama asignado por el emisor. Los fragmentos de un datagrama tendrán el mismo número de identificación.
- **Flags**: 3 bits utilizados para el control de fragmentación.
  - bit 0 – reservado. Debe ser 0.
  - bit DF (Don't Fragment) – A 1 significa "no fragmentar".
  - bit MF (More Fragments) - 0 indica que es el último o único fragmento y 1 que hay más fragmentos.
- **Fragment Offset (FO)**: se usa en datagramas fragmentados. Indica el número de partes de datos de 64 bits contenidas en fragmentos anteriores. En el primer (o único) fragmento el valor es cero.
- **Time To Live (TTL)**: indica un tiempo en segundos -especificado por el protocolo de alto nivel que genera el datagrama- tras el cual se debe descartar el paquete -*timeout* del protocolo superior-. Cada encaminador actualiza el campo restando su tiempo de proceso. Como los encaminadores tardan menos de un segundo en procesar un paquete se convierte en una cuenta de saltos.
- **Protocol**: número oficial del protocolo de alto nivel al que IP debe entregar los datos.
- **Header Checksum**: código de control de la cabecera[16]. Si no es correcto se desecha el datagrama.
- **Source IP Address**: dirección IP del equipo emisor.
- **Destination IP Address**: dirección IP del equipo receptor.
- **Options & Padding (Opciones y relleno)**: este es un campo opcional de longitud variable para pruebas de red o depuración. No se requiere que las implementaciones de IP puedan generar las opciones, pero sí que puedan procesar los datagramas que contienen opciones saltando las opciones, gracias a que conocen la longitud de la cabecera. Esto hace que la longitud de las opciones deba ser múltiplo de 32bits, utilizándose bits de relleno si es necesario.

16 Se calcula como el complemento a uno de la suma de los complementos a uno de todas las palabras de 16 bits de la cabecera.

Direccionamiento v6

IPv6 utiliza un direccionamiento de 16 bytes. Las direcciones se escriben mediante 8 grupos de 2 bytes cada uno, escritos mediante 4 cifras hexadecimales y separados por el símbolo ":".
En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 8 bytes (16 cifras hexadecimales) y otra parte de 8 bytes que corresponde al identificador de interfaz. En el caso de Ethernet este identificador se genera automáticamente a partir de su dirección MAC -6 bytes-, insertando dos bytes (0xFFFF) entre los 3 bytes que identifican al fabricante y los otros 3 bytes.

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a 0000:0000:0000:0000:0000:0000:874B:2B34 con máscara de 96 bits, o ::874B:2B34/96[17] lo que se conoce como dirección “IPv4 compatible”.
Se puede utilizar una notación mixta, que siguiendo el ejemplo quedaría como ::135.75.43.52. Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

Representación de direcciones IPv6

Algunas reglas acerca de la representación de direcciones IPv6 son:

– Los ceros iniciales, como en IPv4, se pueden obviar.
  Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 -> 2001:123:4:ab:cde:3403:1:63
– Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación sólo se puede hacer una vez.
  Ejemplo válido: 2001:0:0:0:0:0:0:4 -> 2001::4
  Ejemplo no válido: 2001:0:0:0:2:0:0:1 -> 2001::2::1 (debería ser 2001::2:0:0:1 o 2001:0:0:0:2::1)
– Si la dirección es una dirección IPv4 “camuflada” o “mapeada”, los últimos 32 bits pueden escribirse en base decimal; así:
  ::ffff:192.168.89.9 es lo mismo que
  ::ffff:c0a8:5909 pero no lo mismo que
  ::192.168.89.9 (IPv4 compatible) o
  ::c0a8:5909 (IPv4 compatible)
  El formato ::ffff:1.2.3.4 se denomina dirección IPv4 mapeada, y el formato ::1.2.3.4 dirección IPv4 compatible.

Tipos de direcciones IPv6

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

- :: /128 – Dirección indefinida -todo ceros, máscara de 128 bits- se utiliza para indicar la ausencia de dirección, y no se asigna a ningún nodo.
- ::1 /128 – Dirección de *loopback* es una dirección que puede usar un nodo para enviarse paquetes a sí mismo. No puede asignarse a ninguna interfaz física.
- :: /96 – (La máscara cubre toda la dirección excepto los últimos 4 bytes) Dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo obsoleto.
- ::ffff:0:0 /96 – Dirección IPv4 mapeada es usada como un mecanismo de transición en redes duales.
- fe80:: /10 – Prefijo de enlace local específica que la dirección sólo es válida en el enlace físico local.
- fec0:: /10 – Prefijo de emplazamiento local específica que la dirección sólo es válida dentro de una organización. Declarado obsoleto (RFC 1918).
- ff00:: /8 – Prefijo de difusión (*multicast*).
- ff01::1 – Funcionalidad de "todos los nodos" (*broadcast*) utilizando difusión (*multicast*).

17 Nótese que la máscara cubre los 0's iniciales.

Sistema de Nombres de Dominio (DNS) en IPv6

Al diseñarse IPv6 se realizaron dos propuestas para el sistema de nombres de dominio, una basada en registros AAAA (*quad-A*) y otra basada en registros A6. Mientras que la idea de quad-A es una simple generalización del DNS IPv4, la idea de A6 es una revisión y puesta a punto del DNS para ser más genérico incluyendo otras innovaciones como las etiquetas de cadena de bits (*bit-string labels*) y los registros DNAME, de ahí su complejidad.

El RFC 3363 recomienda utilizar registros AAAA mientras se prueba y estudia exhaustivamente el uso de registros A6. El RFC 3364 realiza una comparación de las ventajas y desventajas de cada tipo de registro.

Cabecera de trama de IPv6

0	4	12	32	48	56 63
Vers.	*Traffic Class*	*Flow Label*	*Payload Length*	*Next Header*	*Hop Limit*
Source Address (128 bits)					
Destination Address (128 bits)					

El campo Longitud ya no es necesario, ya que la cabecera de IPv6 siempre tiene 40 bytes. Tampoco se realiza una suma de integridad de la cabecera.

- **Version**: Versión del protocolo: v6.
- **Traffic Class**: Equivale a "Type of Service". Indica la clase de tráfico para la gestión de QoS.
- **Flow Label**: Todos los paquetes pertenecientes al mismo flujo tienen el mismo valor de FL, haciendo que sea reconocible sin necesidad de estudiar el contenido del paquete. Esto puede ser útil para QoS, encaminamiento, filtros...
- **Payload Length**: Longitud de los datos transmitidos del paquete.
- **Next Header**: Indica el tipo de cabecera de los datos transportados.
- **Hop Limit**: Equivale a Time to Live (TTL). Indica un número de saltos -especificado por el protocolo de alto nivel que genera el datagrama- tras el cual se debe descartar el paquete.
- **Source IP Address**: dirección IP del equipo emisor.
- **Destination IP Address**: dirección IP del equipo receptor.

IPSec

Los protocolos de IPSec se definieron originalmente en las RFCs 1825 y 1829, publicadas en 1995. IPSec es obligatorio en IPv6 y opcional en IPv4. El objetivo principal de IPSec es proporcionar protección a los paquetes IP.
IPSec establece comunicaciones IP con seguridad de extremo a extremo, lo que significa que los nodos intermedios utilizan el protocolo IP, sin necesidad de una implementación específica para IPSec.

Antes de iniciar el envío de datos, IPSec realiza una autenticación de los extremos y negocia los parámetros de la comunicación. Durante la comunicación utiliza ISAKMP (*Internet Security Association and Key Management Protocol*) para realizar cambios dinámicos de las claves.

Para la comunicación IPSec permite utilizar dos protocolos diferentes: AH (*Authentication Header*) y ESP (*Encapsulation Security Payload*). El protocolo AH permite únicamente verificar la integridad del paquete (mediante firma). El protocolo ESP permite cifrar la información (DES, 3DES...) y opcionalmente verificar la integridad del paquete.

Los protocolos de IPSec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan en la capa de transporte o por encima (capas OSI 4 a 7). Esto hace que IPSec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. Así para que una aplicación pueda usar IPSec no es necesario modificarla, mientras que para usar SSL y otros protocolos de niveles superiores sí.

Hay dos modos de operación de IPSec: modo transporte y modo túnel.

- **Modo transporte**: El modo transporte permite que dos equipos se comuniquen entre ellos utilizando IPSec igual que utilizarían IP pero firmando y/o cifrando los datos que se transfieren (la carga útil del paquete IP). Este sistema añade poca sobrecarga de bytes y permite a los dispositivos de la red conocer el origen y el destino del paquete, lo que puede ser necesario para algunos servicios como QoS.
  El sistema de encaminamiento no varía respecto a IP, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza integridad con AH -que firma la cabecera IP-, las direcciones IP no pueden ser traducidas (p.e. con NAT), ya que eso invalidaría la firma del paquete (*hash*). Para encapsular mensajes IPSec a través de NAT se usa NAT Transversal (NAT-T).

- **Modo túnel**: En el modo túnel dos equipos establecen un canal de comunicación por el que otros equipos o procesos envían información. Es decir el emisor y el receptor originales siguen enviando y recibiendo sus datos sin cifrar ni firmar mediante las pasarelas del túnel IPSec (*IPSec Proxy*), que se encargan de cifrar y/o firmar todo el paquete IP original que debe ser encapsulado en un nuevo paquete IP.
  El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre encaminadores, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

<table>
<tr><th></th><th>Modo Transporte</th><th>Modo Túnel</th></tr>
<tr><td>Protocolo ESP</td><td>
<table>
<tr><td colspan="2"></td><td colspan="4">Firmado (Opcional)</td></tr>
<tr><td colspan="3"></td><td colspan="3">Cifrado</td></tr>
<tr><td>IP Header</td><td>ESP Header</td><td>TCP/UDP Header</td><td>DATA</td><td>ESP Trailer</td><td>ESP Auh</td></tr>
</table>
</td><td>
<table>
<tr><td></td><td colspan="5">Firmado (Opcional)</td></tr>
<tr><td></td><td colspan="5">Cifrado</td></tr>
<tr><td>New IP Header</td><td>ESP Header</td><td>Orig. IP Header</td><td>TCP/UDP Header</td><td>DATA</td><td>ESP Trailer</td><td>ESP Auh</td></tr>
</table>
</td></tr>
<tr><td>Protocolo AH</td><td>
<table>
<tr><td colspan="4">Firmado</td></tr>
<tr><td>IP Header</td><td>Auth Header</td><td>TCP/UDP Header</td><td>DATA</td></tr>
</table>
</td><td>
<table>
<tr><td colspan="5">Firmado</td></tr>
<tr><td>New IP Header</td><td>Auth Header</td><td>Orig. IP Header</td><td>TCP/UDP Header</td><td>DATA</td></tr>
</table>
</td></tr>
</table>

IPSec no define unos algoritmos específicos de cifrado sino que mediante ISAKMP permite utilizar IKE (*Internet Key Exchange*) para realizar un autonegociado del algoritmo a utilizar y del intercambio de claves. IKE funciona sobre UDP y aporta escalabilidad y flexibilidad ya que permite utilizar algoritmos de varios tipos:

- Claves Pre-Compartidas (PSK: *Pre-Shared Key*). Su mayor inconveniente es la distribución de la PSK.
- Kerberos.
- Criptografía de clave pública-privada.
- Certificados digitales.

El principal problema de IKE viene de que, aunque es un estándar abierto, la norma es admite distintas interpretaciones, lo que ha dado lugar a implementaciones ligeramente incompatibles. Este es uno de los motivos por el que se están imponiendo las VPNs sobre SSL. Actualmente está en desarrollo IKE v2.

3.4. Otros protocolos de la familia Internet

ARP y RARP

El protocolo ARP (*Address Resolution Protocol*) es el método estándar para obtener la dirección "física" (nivel 2 -de enlace-) de una NIC cuando únicamente se conoce su dirección "lógica" (nivel 3 -de red-). Una vez obtenida se guarda temporalmente la información en una tabla (tablas caché ARP) para reducir el número de consultas.
No es un protocolo de uso exclusivo con IP, aunque dada la gran implantación de dicho protocolo y de Ethernet, se utiliza principalmente para asociar una dirección IP a una dirección MAC de Ethernet. También se utiliza ampliamente con IP sobre otras tecnologías LAN como Token Ring, FDDI, IEEE 802.11 (*Wi-Fi*) o ATM.

Existe un protocolo, RARP (*Reverse ARP*), cuya función es la inversa.

ICMP e IGMP

ICMP (*Internet Control Messaging Protocol*) es parte fundamental y complementaria de IP y es empleado por éste para notificar mensajes de error o situaciones que requieren cierta atención. Debido a que los paquetes ICMP viajan en paquetes IP es a veces considerado un nivel por encima.
Los distintos mensajes ICMP posibles utilizan un identificador numérico, que en el caso de los mensajes de error es menor que 128. ICMP también permite adquirir información mediante pares de paquetes petición / respuesta, por ejemplo, para adquirir la máscara de red de un sistema o el valor de su reloj (*timestamps*). Por último, en numerosas ocasiones se emplea para comprobar la existencia de conectividad, como en la utilidad "ping", empleando paquetes ICMP "echo" (id. 128) y "echo reply" (id. 129).

Los mensajes de error de ICMP se generan cuando el destinatario o un encaminador no puede procesar un paquete IP e incluyen la cabecera del paquete IP que ha generado el error y los primeros 8 bytes del contenido del mismo, lo que es suficiente en TCP para conocer la comunicación que originó el paquete erróneo -recordemos que IP no garantiza la recepción de paquetes-.

Como IPv6 está diseñado para poder soportar múltiples protocolos de transporte, ICMPv6 incluye el inicio del paquete IP fallido original (incluyendo la cabecera) hasta generar un paquete de error de 1280 bytes, que es el MTU mínimo admitido por IPv6.

IGMP (*Internet Group Management Protocol*) se utiliza para informar a los encaminadores de la pertenencia de un equipo a un grupo de *multicast*. Es análogo a ICMP pero para conexiones *multicast* en vez de *unicast*. IGMP se puede usar para transmisión de vídeo, para juegos... Es un protocolo vulnerable, poco utilizado y opcional (mientras que ICMP es requerido por IAB) por lo que algunos cortafuegos lo bloquean opcionalmente.

TCP

TCP (*Transmission Control Protocol*) es el protocolo de transporte empleado actualmente por la mayoría de los protocolos de aplicaciones en Internet. Utiliza un esquema de circuito virtual para establecer un flujo de bytes sobre IP. El protocolo TCP utiliza la técnica de ventana deslizante -pudiéndose cambiar el tamaño de la ventana durante la comunicación- y la técnica de "*piggybacking*" es decir, incluye en la transmisión de paquetes, la confirmación de recepción de paquetes. Así un equipo que reciba correctamente los bytes 1, 3 y 4, emitirá el reconocimiento del byte 1 (ACK 1). Cuando reciba correctamente el 2 emitirá ACK 4, indicando que ha recibido correctamente hasta el byte 4[18].

Para permitir múltiples conexiones entre equipos e identificar a los destinatarios y remitentes de manera sencilla, TCP multiplexa las direcciones IP utilizando "puertos". Así una conexión TCP se identifica como:
<TCP, IP_local.Puerto_local, IP_destino.Puerto_destino>.

18 Dado que emisor y receptor han acordado un tamaño de ventana, el emisor no envía más bytes de los que puede almacenar el receptor.

Antes de comenzar la transmisión de datos, se debe establecer una conexión haciendo que los nodos reserven recursos y estableciendo parámetros como el tamaño de los mensajes (MTU del circuito virtual) o la ventana de transmisión. Una conexión TCP se establece en tres pasos (*three-way handshake*):

1. El equipo que inicia la conexión envía al destinatario un paquete de sincronización “SYN” con el número de secuencia inicial elegido para esta conexión[19] y el tamaño de ventana;
2. éste le responde con un paquete de reconocimiento “SYN-ACK”, confirmándole la recepción de su número inicial (ACK) y enviándole un número propio inicial de secuencia (SYN);
3. el equipo que ha iniciado la conexión reconoce la recepción de la señal “SYN-ACK” mediante una señal “ACK”. En este momento la conexión se ha establecido y puede tener lugar toda la transferencia de datos.

De igual modo, la finalización de la conexión se lleva a cabo mediante el intercambio de un par de paquetes TCP por parte de cada equipo: un paquete “FIN” y un paquete “ACK”. Esto puede llevarse a cabo en 4 pasos (FIN-ACK-FIN-ACK) o en tres pasos (FIN-FIN&ACK-ACK). Algunas implementaciones permiten finalizar en dos pasos o cerrar solo un lado de la comunicación...

Si bien una vez establecida la comunicación, TCP envía los bytes agrupados en conjuntos llamados "segmentos", el control de la transmisión, incluyendo la cuenta de envíos ("*Sequence Number*") o las recepciones correctas ("*Acknowledgment Number*"), se hace en base a bytes no a paquetes o segmentos.
Las aplicaciones que utilizan TCP pueden invocar a la función "*Push*" para solicitar que se envíe un segmento sin esperar nuevos bytes para incluir en él[20]. De manera similar la función "*Urgent*" solicita que los nuevos bytes añadidos al segmento se traten antes que los que ya estén en él esperando su envío[21].

Cabecera de trama de TCP

<table>
<tr><th>0</th><th>4</th><th>10</th><th>16</th><th>31</th></tr>
<tr><td colspan="3">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="5">Sequence Number</td></tr>
<tr><td colspan="5">Acknowledgment Number</td></tr>
<tr><td>Dat. Offset</td><td>Reserved</td><td>Flags</td><td colspan="2">Window</td></tr>
<tr><td colspan="3">Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="5">Options & Padding</td></tr>
</table>

- **Source Port**: Número de puerto de 16 bits del emisor, que el receptor debe usar para responder.
- **Destination Port**: Número de puerto de 16 bits del receptor.
- **Sequence Number**: Número de secuencia del primer byte de datos del segmento enviado en el paquete. Si el byte de control SYN está a 1, el número de secuencia es el inicial y el primer byte de datos será el n+1.
- **Acknowledgment Number**: Contiene el valor del último byte recibido correctamente. Este número implica que todos los bytes anteriores han sido recibidos correctamente ("reconocidos").
- **Data Offset**: Indica la longitud de la cabecera en palabras de 32 bits y, por tanto, dónde empiezan los datos. Esta longitud es de 5 palabras (20 Bytes) más el campo "Opciones" si existe.
- **Reserved**: bits reservados para un uso futuro; deben ser cero.
- **Flags**: 6 bits utilizados para el control de la conexión
  - URG (*Urgent*): Indica al receptor que los primeros bytes en tratar sean los bytes urgentes, cuyo inicio se indica en el campo "*urgent pointer*".
  - ACK (*Acknowledge*): Indica que el campo de reconocimiento es significativo en el segmento.
  - PSH (*Push*): Indica que se ha solicitado la función "*Push*".
  - RST (*Reset*): Reinicia la conexión porque el puerto destino no está en uso o el número de secuencia no se puede usar.

19 El número de secuencia inicial se elige de manera pseudoaleatoria para que no se pueda mezclar con otra comunicación por error.
20 Por ejemplo en una conexión telnet con eco remoto, al pulsar "Intro" se envía la información con "*Push*".
21 Por ejemplo en una conexión telnet, al pulsar Ctrl-C se envía como "*Urgent*".

  - SYN (*Syncro.*): Indica si el número de secuencia es el inicial.
  - FIN: Indica que el emisor desea terminar la comunicación.
- **Window**: Establece un nuevo tamaño de la ventana de bytes para la comunicación.
- **Checksum**: código de control de la cabecera[22]. Si no es correcto se desecha el paquete.
- **Urgent Pointer**: Apunta al primer byte de datos urgentes.
- **Options & Padding (Opciones y relleno)**: este es un campo opcional de longitud variable para pruebas de red o depuración. No se requiere que las implementaciones de TCP puedan generar las opciones, pero sí que puedan procesar los segmentos que contienen opciones saltando las opciones, gracias a que conocen la longitud de la cabecera. Esto hace que la longitud de las opciones deba ser múltiplo de 32bits, utilizándose bits de relleno si es necesario.

UDP

UDP (*User Datagram Protocol*) es un protocolo que utiliza un esquema de datagramas sobre IP. UDP no garantiza la comunicación, es decir, los paquetes pueden no llegar, llegar correctamente, duplicados o fuera de orden. Al evitar esas comprobaciones y su sobrecarga (*overhead*) el protocolo UDP es más sencillo, rápido y eficiente que TCP, pero solo sirve para aplicaciones que no necesiten garantías en la comunicación. Esto es muy práctico en aplicaciones en que es más importante la velocidad de transmisión (como comunicación de audio y vídeo: IPTV, VoIP, juegos en línea) o en aplicaciones servidoras sin estado que deben responder pequeñas consultas de un gran número de clientes (como DNS). A diferencia de TCP, UDP permite paquetes de difusión (*broadcast* y *multicast*).

Cabecera de trama de UDP

0	16 31
Source Port	*Destination Port*
Length	*Checksum*

La cabecera de trama de UDP únicamente indica puertos de origen y destino, longitud del datagrama -incluyendo la cabecera- y un código de control del paquete[23].

22 Para este código se utiliza el complemento a uno de 16 bits de la suma en complemento a uno del paquete con una pseudo cabecera IP "virtual".
23 Se calcula igual que en TCP.

Puertos de aplicaciones basadas en TCP/UDP

A continuación se indican algunos de los principales protocolos de aplicaciones y sus puertos habituales asociados[24].

Puerto	Protocol.	Descripción
7	tcp y udp	Echo - Responde con eco a llamadas remotas
20-21	tcp	FTP (*File Transfer Protocol*) - Transferencia de Ficheros [datos (20) y control (21)]
22	tcp	SSH, SCP, SFTP - Juego de protocolos de comunicación segura
23	tcp	Telnet - Protocolo de comunicación de inseguro
25	tcp	SMTP (*Simple Mail Transfer Protocol*) - Transferencia Simple de Correo
53	tcp y udp	DNS (*Domain Name System*) - Sistema de Nombres de Dominio
67-68	udp	BOOTP (Server-Client) / DHCP (*Dynamic Host Configuration Protocol*)
80	tcp	HTTP (*HyperText Transfer Protocol*) - Transferencia de HiperTexto (web)
88	tcp	Kerberos - Agente de autenticación
110	tcp	POP3 (*Post Office Protocol 3*) - Correo-e
123	tcp y udp	NTP - Protocolo de sincronización de tiempo
135	tcp	RPC (*Remote Procedure Call*)
137-139	tcp y udp	NetBIOS Servicio de nombres [nombres (137), datagramas (138), sesiones (139)]
143	tcp	IMAP4 (*Internet Message Access Protocol 4*) - Correo-e
161-162	tcp y udp	SNMP - Gestión Simple de Red [consultas (161) y señales (162)]
389	tcp y udp	LDAP - Protocolo de acceso ligero a Bases de Datos
443	tcp	HTTPS/SSL – HTTP sobre una capa SSL
631	tcp	CUPS - Sistema de impresión Unix
636	tcp	LDAPs – LDAP sobre SSL
993	tcp	IMAP4 sobre SSL
995	tcp	POP3 sobre SSL
1433-1434	tcp	Microsoft-SQL (Server-Monitor)
1512	tcp	WINS
1521	tcp	Oracle listener (por defecto)
1701	udp	Enrutamiento y Acceso Remoto para VPN con L2TP.
1723	tcp	Enrutamiento y Acceso Remoto para VPN con PPTP.
2049	tcp	NFS - Archivos del sistema de red
3128	tcp	Servidores intermediarios de HTTP, como Squid
3306	tcp	MySQL sistema de gestión de bases de datos
3389	tcp	RDP (Remote Desktop Protocol)
5060	udp	Session Initiation Protocol (SIP)
5432	tcp	PostgreSQL sistema de gestión de bases de datos
10000	tcp	Webmin (Administración remota web)

24 Puertos reservados [0-1.023]; Puertos registrados [1.024-49.151]; Puertos dinámicos [49.152-62.535].

4. ETHERNET

4.1. Un poco de historia

En 1970 Robert Metcalfe, recién graduado en el MIT, se encontraba realizando sus estudios de doctorado en la Universidad de Harvard trabajando para ARPANET. Encontró un artículo de Norm Abramson en el que describía la red Aloha en Hawaii y pensó que podía mejorarlo. Escribió un artículo que se convertiría en su tesis doctoral, presentada en 1973, con un idea básica simple: las estaciones antes de transmitir deberían detectar si el canal ya estaba en uso (es decir si ya había 'portadora'), en cuyo caso esperarían a que la estación activa terminara. Además cada estación, mientras transmitiera, estaría continuamente vigilando el medio físico por si se producía alguna colisión, en cuyo caso se pararía y retransmitiría más tarde. Este protocolo MAC recibiría más tarde la denominación Acceso Múltiple con Detección de Portadora y Detección de Colisiones, o más brevemente CSMA/CD (*Carrier Sense Multiple Access / Colision Detect*).

En 1972 Metcalfe se mudó a California para trabajar en el Centro de Investigación de Xerox en Palo Alto llamado Xerox PARC (Palo Alto Research Center). Allí se estaba diseñando lo que se consideraba la 'oficina del futuro', con las primeras impresoras láser y computadoras Alto, que ya disponían de capacidades gráficas y ratón y fueron consideradas las primeras computadoras personales... Se quería conectar las computadoras entre sí para compartir ficheros y con las impresoras y Metcalfe tenía la tarea de diseñar y construir la red que debía ser de muy alta velocidad, del orden de megabits por segundo. Contaba para ello con la ayuda de un estudiante de doctorado de Stanford llamado David Boggs.

El 22 de mayo de 1973 Metcalfe escribió un memorándum interno en el que informaba de la nueva red. En principio la red se llamaba *Alto Aloha Network*, pero para evitar que se pudiera pensar que sólo servía para conectar computadoras Alto se cambió el nombre de la red por el de Ethernet (en alusión al éter como portador de ondas en el espacio). Las dos computadoras Alto utilizadas para las primeras pruebas de Ethernet (11 noviembre de 1973) fueron rebautizadas con los nombres Michelson y Morley, en alusión a los dos físicos que habían demostrado en 1887 la inexistencia del éter.

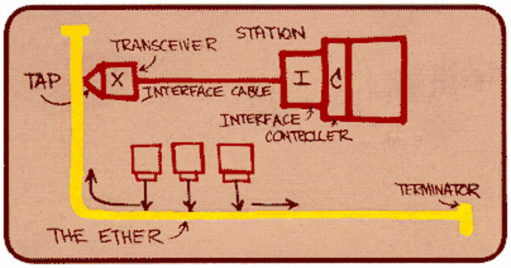


Diagrama de Ethernet realizado por Metcalfe

La red de 1973 ya tenía todas las características esenciales de la Ethernet actual. Empleaba CSMA/CD para minimizar la probabilidad de colisión, y en caso de que ésta se produjera utilizaba un mecanismo denominado retroceso exponencial binario para reducir gradualmente la 'agresividad' del emisor, con lo que éste se adaptaba a situaciones de muy diverso nivel de tráfico. Tenía topología de bus y funcionaba a 2,94 Mb/s sobre un segmento de cable coaxial de 1,6 Km de longitud. Las direcciones eran de 8 bits y el CRC de las tramas de 16 bits. El protocolo utilizado a nivel de red era el PUP (*Parc Universal Packet*) que luego evolucionaría hasta convertirse en el que luego fue XNS (*Xerox Network System*), antecesor a su vez de IPX (Protocolo Netware de Novell).

En vez de utilizar el cable coaxial de 75 ohms de las redes de televisión por cable se optó por emplear cable de 50 ohms que producía menos reflexiones de la señal, a las cuales Ethernet era muy sensible por transmitir la señal en banda base (es decir sin modulación). Cada empalme del cable y cada 'pincho' vampiro (transceptor o *transceiver*) instalado producía la reflexión de una parte de la señal transmitida. En la práctica el número máximo de transceptores, y por tanto el número máximo de estaciones en un segmento de cable coaxial, venía limitado por la máxima intensidad de señal reflejada tolerable.

En 1975 Metcalfe y Boggs describieron Ethernet en un artículo que se publicó en 1976 (en "Communications of the ACM"). En él ya describían el uso de repetidores para aumentar el alcance de la red. Ese mismo año Boggs construyó el primer encaminador. En 1977 Metcalfe, Boggs y otros dos ingenieros de Xerox recibieron una patente por la tecnología básica de Ethernet, y en 1978 Metcalfe y Boggs recibieron otra por el repetidor. En esta época todo el sistema Ethernet era propietario de Xerox[25]. En 1979 Metcalfe dejó Xerox y fundó 3Com.

25 Xerox se juntó con DEC e Intel para fundar DIX y promocionar el uso de Ethernet. Publicaron la versión 1.0 en el Libro Azul de Ethernet (1980). La licencia costaba $1000 anuales por cada rango de 24 bits de direcciones MAC (hoy controlado por el IEEEE a un precio similar).

4.2. Definición

Ethernet es un protocolo de nivel de enlace (N2) para redes de área local (LAN) basado en datagramas y definido en el estándar IEEE 802.3[26], de comunicaciones entre iguales (PTP o P2P: *peer to peer*) en el que no hay un control centralizado y todas las estaciones son tratadas por igual.
El protocolo original se basa en una topología de bus con medio compartido, es decir, varias estaciones que pueden enviar datos al mismo tiempo. Por tanto se debe arbitrar un mecanismo de control de acceso al medio y resolver los problemas que conllevan los accesos simultáneos (colisiones). Las nuevas versiones se basan en comunicaciones *full-duplex* sobre canales independientes, por lo que no pueden existir las colisiones.
Una vez una estación consigue enviar sus datos sin colisiones, supone un medio físico altamente fiable, por lo que no implementa confirmación de entrega de datos en destino. Si hay perdida de datos en el camino deben detectarla los niveles superiores. Esto hace que cuando realmente se pierdan datos en este nivel, las aplicaciones se vean bastante perjudicadas.

4.3. Control de colisiones

El mecanismo de control de colisiones de Ethernet es el CSMA/CD (*Carrier Sense Multiple Access/Colision Detect*) y se basa en escuchar si el medio está libre para empezar a transmitir y asegurarse que la señal transmitida no es alterada por otra señal. Una vez comprobado que el medio esta libre únicamente hay que dejar pasar un tiempo equivalente a 12 bytes antes de comenzar a transmitir. Esta pausa sirve para evitar que los datos transmitidos se concatenen con otra trama en la red y para dar tiempo a las estaciones a procesar una posible trama recibida y que vuelvan a la escucha.

Cuando dos estaciones transmiten a la vez se produce una "colisión" que supone una alteración de las señales enviadas. Esta alteración es detectada por las dos estaciones emisoras, que actúan de la siguiente manera:

1. Detienen la transmisión de la trama.
2. Envían una señal de atasco (*Jam*) durante el tiempo equivalente a 4 Bytes para que todas las estaciones se enteren de que ha habido colisión.
3. Ponen en marcha el mecanismo de retroceso exponencial binario[27] para decidir cuanto tiempo esperan a retransmitir. Ese tiempo será aleatorio para evitar que las dos esperaren el mismo tiempo y vuelvan a colisionar.
4. Transcurrido ese tiempo, si el medio esta libre, vuelven a intentar emitir.

Todas las estaciones que comparten el medio físico forman un dominio de colisión. Una estación compite por el medio con todas las de su dominio de colisión. No solo con las que estén en su mismo cable, también con las que estén al otro lado de repetidores y concentradores (*hubs*), pero no con las que estén al otro lado de puentes (*bridges*), conmutadores (*switchs*) o encaminadores (*routers*).
El diámetro de un dominio de colisión es la distancia máxima entre estaciones. Esta distancia debe ser lo suficientemente pequeña para que en el tiempo que tarda en ir y volver la señal de un extremo a otro no se pueda transmitir una trama de tamaño mínimo T (2τ propagación en el diámetro máximo $< \tau$ transmisión de T).

26 En general, los protocolos de la rama IEEE 802.x definen la tecnología de redes de área local. ISO los define como ISO 8802x.
27 Cada vez que hay una colisión la estación espera entre 0 y 2^i-1 veces el tiempo 2τ, siendo 'i' la iteración del algoritmo.

4.4. Direccionamiento

Cada nodo tiene una dirección de nivel 2 única, llamada dirección MAC (*Medium Access Control*). Esta dirección tiene 48 bits (6 bytes) y se suele representar con 12 caracteres hexadecimales separados por ":" o por "-" entre cada dos.
Las direcciones son asignadas por los fabricantes, que se identifican por los primeros 24 bits[28].

Una trama puede ir dirigida a:

- Una estación concreta (*unicast*). Lleva como dirección de destino la dirección MAC de la estación de destino.
- Todas las estaciones de su red (difusión o *broadcast*). Lleva como dirección de destino la dirección de difusión -todos los bits a uno- (FF:FF:FF:FF:FF:FF).
- Un grupo de estaciones que comparten una dirección especial (*multicast*). Estas direcciones especiales tienen un 1 en el ultimo bit de su primer byte. Típicamente, son de la forma 01:xx:xx:xx:xx:xx.

4.5. Formato de trama

La trama en Ethernet puede tener entre 64 y 1518 bytes y tiene el siguiente formato:

Preámbulo	Inicio (SoF)	Dir. Destino	Dir. Origen	Tipo / Long.	Datos	Relleno	CRC32	(Pausa)
7	1	6	6	2	0 – 1500	0 – 46	4	(12)

Donde:

- Preámbulo: Secuencia de 7 bytes 10101010 para estabilizar el medio.
- Inicio (*Start of Frame*): Byte 10101011 que indica que se va a iniciar la transmisión.
- Dir. Destino: es la dirección de destino.
- Dir. Origen: es la dirección de origen.
- Tipo/Long: es interpretado como:
  - Tipo de protocolo de nivel 3, si su valor es mayor de 1536 (formato original DIX[29]).
  - Longitud de la trama, si es menor que 1536 (formato IEEE 802.3).
- Datos: son los datos que lleva la trama.
- Relleno: existirá si no hay suficientes datos para que la trama tenga al menos 64 bytes.
- CRC32: es un código de redundancia cíclico para comprobar que no ha habido errores.
- El final de la trama se detecta por el hueco equivalente a 12 bytes que todas las estaciones deben respetar. Es decir tras cada trama el emisor hace una pausa por el tiempo equivalente a enviar 12 bytes.

En función del protocolo de nivel 3 que se utilice, dentro de los datos puede haber una cabecera LLC (*Logical Link Control*) para resolver a qué protocolo se le entrega la trama. Por ejemplo NetBEUI lo utiliza pero IP no.
El tamaño máximo de trama condiciona la cantidad de memoria que debe tener la interfaz de red.

En el caso de Gigabit Ethernet si se mantuviese una trama mínima de 64B, el diámetro del dominio de colisión sería de ~45m. Por ello mientras viajan por Gigabit las tramas deben tener un mínimo de 512B (diámetro ~330m), añadiéndose en caso necesario un relleno conocido como extensión de portadora que se elimina si la trama deja la red Gigabit.
Sin embargo el uso de extensión de portadora supone por un lado mayor proporción de datos enviados/colisiones[30] y por otro lado pérdida de eficiencia en el caso de tramas pequeñas -mayor proporción de datos de control-. Para este caso se prevé la posibilidad de que una estación que quiera enviar varias tramas pequeñas seguidas lo haga como una ráfaga.
Actualmente existen implementaciones que utilizan tramas Jumbo (*Jumbo-frames*) con MTU (*Maximum Transmission Unit*) mayor que 1518B, lo que permite reducir la sobrecarga de cabeceras presuponiendo una mayor calidad de los medios. El MTU típico de las tramas Jumbo es de 9000 B, pero existen distintas implementaciones.

28 OUI: Organization Unic Identifier.
29 DIX fue un consorcio creado por DEC, Intel y Xerox para hacer de Ethernet un protocolo abierto al que se pudiesen sumar distintos fabricantes. Cuando 802 sacó su estándar (1983), para permitir su convivencia DIX movió los tipos utilizados a valores mayores que 1536, sin embargo el sistema DIX es más eficiente y era el preferido por los fabricantes. En 1997 IEEE estandariza el uso de Tipo/Longitud.
30 Dado que se emiten más bits en el mismo tiempo límite de propagación de 2τ bits.

4.6. Tarjetas interfaces de red (NIC: *Network Interface Card*)

Las tarjetas interfaces de red (NIC: *Network Interface Card*) son la electrónica que utilizan las estaciones para acceder al medio físico para comunicar con otras estaciones. Implementan el subnivel MAC (*Medium Access Control*), mientras que el controlador de las mismas (*driver*) implementa el subnivel LLC (*Logical Link Control*).
En funcionamiento normal, sólo reciben y entregan al nivel superior las tramas que cumplen:

- La dirección de destino es su propia dirección MAC
- Son tramas de difusión (*broadcast*)
- Son tramas de *multicast* y alguna aplicación le ha indicado a la tarjeta que reciba tramas a esa dirección *multicast* en concreto.

Tienen un modo de funcionamiento especial llamado "modo promiscuo" en el que reciben y entregan al nivel superior todas las tramas que escuchan. Algunos programas configuran la tarjeta en este modo para analizar todo el trafico que pasa por su segmento.

En un principio, cada trama que se recibía en la tarjeta provocaba una interrupción a la CPU para pasársela al controlador y que éste la entregara al protocolo correspondiente de nivel 3. Hoy en día se pueden configurar para que esperen (durante un tiempo máximo) a recibir varias tramas para pasárselas todas juntas al controlador y así provocar menos interrupciones a la CPU.

Si se utilizan canales no compartidos (*full-duplex*) y el interfaz soporta varias velocidades, normalmente también es capaz de negociar su velocidad con el otro extremo del cable por medio de una señal especial intentando negociar primero la velocidad más alta. Esta negociación se lleva a cabo cuando se inicializa el enlace, antes de enviar datos.
En fibra óptica no se puede negociar la velocidad porque cada estándar utiliza transmisores diferentes.

Es muy importante que los interfaces que no usan *full-duplex* implementen correctamente el protocolo CSMA/CD para que no disminuya el rendimiento de la red.

4.7. Repetidores y concentradores (*Hubs*)

Los repetidores son componentes que actúan a nivel puramente físico (N1) y sirven para ampliar el alcance de la red. Simplemente repiten (y con ello amplían / regeneran) la señal recibida sin actuar a nivel lógico, esto es, sin realizar ningún control o análisis de la misma y sin aislar segmentos de la red. A nivel lógico son únicamente una parte más del medio (un trozo de cable, o parte del aire). Algunos permiten cambiar de medio físico (no de velocidad).

Los concentradores (*hubs*) son repetidores con varios puertos. Un concentrador simula un único segmento Ethernet entre todas las estaciones que se conectan a el. Como cualquier otro repetidor actúan a nivel físico (N1) retransmitiendo las tramas que se reciben en un puerto a todos los puertos restantes, independientemente de que estén libres u ocupados, por lo que también propagan las colisiones. Todos los puertos de un concentrador deben ser de la misma velocidad. En los inicios de Fast Ethernet, dado el alto coste de los conmutadores, aparecieron concentradores de doble velocidad (*dual-speed hubs*) que en realidad eran dos concentradores unidos internamente por un puente.

El estándar de IEEE define los puertos RJ45 para cable de par trenzado (xTP[31]) de los equipos como MDI (*Medium Dependent Interface*), mientras que los puertos de los concentradores son MDI-X (*Medium Dependent Interface – Crossover*). De los 4 pares del cable el interfaz MDI transmite por el par 2 (hilos 1-2) y recibe por el par 3 (hilos 3-6), mientras que el MDI-X lo hace al revés.
Para conectar una estación a un concentrador se utiliza un cable paralelo (*straight-through*), pero para conectar entre si dos concentradores o dos equipos se necesita un cable cruzado (*crossover*).

Con el tiempo los concentradores y conmutadores (*switches*) fueron incorporando un puerto MDI para interconectar (o "apilar") concentradores. Actualmente los conmutadores utilizan puertos propios o fibra para conectarse entre ellos y todos sus puertos se configuran automáticamente como MDI o MDI-X (además de negociar *Half* o *Full-duplex*, velocidad, control de flujo...).

31 Par trenzado no apantallado (UTP: *Unshielded Twisted Pair*) o par trenzado apantallado (STP: *Shielded Twisted Pair*).

4.8. Puentes (*Bridges*) y conmutadores (*Switches*)

Los puentes son nodos que unen dos o más redes a nivel de enlace de datos (N2) y permiten:

- Ampliar las distancias de la red.
- Separar dominios de colisión y aislar trafico *unicast* innecesario.
- Cambiar de protocolo de nivel de enlace (N2) entre dos redes (de FDDI a Ethernet, por ejemplo).
- Cambiar de velocidad.
- Transmisiones *full-duplex*.

Los conmutadores son puentes de múltiples puertos con circuitos integrados específicos de aplicación (ASIC[32]).
Desde el punto de vista MAC los puentes y conmutadores se comportan como una estación más. Durante su funcionamiento, cuando reciben una trama por un puerto, apuntan en una tabla que la dirección MAC de origen de la trama está en ese puerto. Así pueden saber en que puerto está cada estación y más tarde, cuando tienen que enviar una trama a esa estación la envían solo al puerto donde se detectó.

Las entradas en la relación MAC-puerto se renuevan cada pocos segundos. Si un puente o conmutador no conoce donde esta la estación de destino envía la trama a todos sus puertos (inundación o *flood*).
Aunque cada puente o conmutador produce un retardo en la señal, en principio no hay limite en cuanto al número de puentes que se pueden poner en una red ya que cada retransmisión regenera la señal.

Como los puentes y conmutadores aislan el trafico *unicast* enviándolo solo al puerto necesario, aumenta también la seguridad de la red ya que las estaciones conectadas a otros puertos no pueden capturar ese trafico. Para poder hacerlo, algunos conmutadores soportan configurar especialmente un puerto espejo (*mirror*) que transmite el mismo trafico que otro. De todas maneras este esquema puede atacarse por medio de inyecciones ARP (*ARP spoofing*) o inundación de MAC (*MAC flooding*), aunque los conmutadores (*switches*) más modernos implementan defensas al respecto.

Si los puentes soportan el protocolo *Spanning Tree* definido en el estándar 802.ld se pueden unir dos puentes a través de 2 o más caminos (pasando incluso por otros puentes) evitando los bucles, lo que permite tener un camino alternativo en caso de que haya una avería en el camino principal o poder repartir tráfico.

4.9. Comunicación Dúplex (*Full-Duplex)*

El protocolo Ethernet original transmite en semi-dúplex (*half-duplex*) porque el medio es compartido. La transmisión dúplex (*full-duplex*) en Ethernet esta normalizada por el IEEE en el estándar 802.3x. Una línea es dúplex si puede enviar y recibir datos al mismo tiempo, lo que puede ocurrir entre dos nodos conectados directamente.

Para que la transmisión pueda ser dúplex se deben cumplir:

- Que haya un medio de transmisión diferente del de recepción.
- Que solo haya dos nodos compartiendo el medio.
- Que los interfaces de los nodos lo soporten.

En transmisión dúplex no hay gestión CSMA/CD ya que no puede haber colisiones. Si la transmisión es dúplex se puede aumentar la distancia entre estación y conmutador, ya que tampoco hay que tener en cuenta el tiempo de ida y vuelta porque no hay control de colisiones. La única restricción es la atenuación de la señal. Con algunos emisores láser se ha llegado a 800km.

Cuando la comunicación es dúplex puede que uno de los extremos no sea capaz de procesar el trafico que le envía el otro. Para resolver este problema en el estándar IEEE 802.3x se define un método de control de flujo que consiste en que el extremo saturado le envía al otro una trama especial llamada *Pause* (con tipo 8808) donde le ordena dejar de enviar datos durante un tiempo indicado. Antes de que transcurra ese tiempo le puede enviar la orden *Pause-Release* para que vuelva a transmitir. La orden *Pause* debe darse antes de que se llenen los *buffers* ya que puede haber datos en el cable que todavía no se han recibido. El control de flujo puede ser simétrico (los dos extremos pueden ordenar parar al otro) o asimétrico (sólo puede ordenarlo un extremo).

32 ASIC: *Application-Specific Integrated Circuit*.

Normalmente un interfaz de red es capaz de negociar automáticamente con el otro extremo el modo de transmisión (*half* o *full-duplex*) y el control de flujo.

4.10. Restricciones

El estándar Ethernet impone las siguientes restricciones:

- Como máximo 100 m para cable de par trenzado.
- MTU (*Maximum Transmission Unit*) = 1518 bytes
- Restricciones en el estándar Ethernet original:
  - Como máximo 4 repetidores o concentradores entre dos equipos del mismo dominio de colisión.
  - Como máximo 1.024 estaciones de trabajo en el mismo dominio de colisión.
  - 2τ propagación en el diámetro máximo del dominio de colisión $< \tau$ transmisión de T (tamaño de trama mínima = 64 bytes = 512 bits)

4.11. La evolución de la familia Ethernet

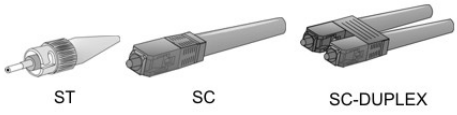
Ethernet

Transmite a 10Mbps. Utiliza codigo Manchester, que es sencillo y barato de implementar, pero poco eficiente ya que al utilizar el doble de frecuencia requiere un cable de altas prestaciones como el coaxial.
En Ethernet la codificación se realiza en el controlador, no en el transceiver, por lo que se ha de emplear en todos los medios físicos. En las siguientes especificaciones la codificación se realiza en el transceiver, con lo que para cada medio físico puede elegirse el código que más convenga.

Definido en el libro azul de Ethernet publicado por DIX en 1980. Al primer protocolo implantado en Palo Alto a 2,94 Mbs se le conoce como Ethernet Experimental.

Estándar	Medio y conectores	Repet. /Est.	Distancia / Transmisión
10Base-5 (1) Fue la primera versión comercial.	Coaxial amarillo de 50 Ω Transceptores vampiros y cable AUI (*drop*) de hasta 50 metros.	2 / 100	500 m. *Half-Duplex*
10Base-2 (1) Surgió para solucionar los problemas de coste y rigidez del coaxial amarillo.	Coaxial RG58 de 50 Ω Conectores BNC -conectores T-	4 / 30 separadas entre sí por 1 m. o más.	185 m. *Half-Duplex*
10Base-T (2) Surgió para reutilizar los cables de telefonía -par trenzado no apantallado (UTP)- para datos.	Par trenzado a partir de Cat. 3. Conectores RJ-45. De los 4 pares del cable solo utiliza dos: El 2 y el 3 (hilos 1, 2, 3 y 6).	4 / 1024	Cat. 3 – 100m Cat. 5 – 150m *Half-Duplex* y *Full-Duplex*
10Base-F (3) (**10Base-Fx**) Implementación del estándar. Se usan sus variantes FL, FB o FP.	Multimodo; LED en primera ventana. Luz visible. Conectores ST.		2000 m. *Half-Duplex* y *Full-Duplex*

(1) Basado en cable coaxial y topología lineal (o de bus). Se pueden unir varios segmentos con repetidores siempre que no haya más de 4 repetidores entre dos segmentos cualesquiera. Si se abre el coaxial o uno de los terminadores, deja de funcionar toda la red. Necesita terminadores de 50 Ω en los extremos del cable.
(2) Aunque su topología lógica sigue siendo lineal, su topología física es de estrella con un repetidor multipuerto (concentrador o *hub*) en su centro. Cada estación tiene un cable propio que lo une al concentrador. Se puede mezclar con 10Base-5 o 10Base-2 siempre que no se interconecten por más de 3 coaxiales.
Soporta 1024 estaciones en cada dominio de colisión.
(3) Implementación del estándar original Ethernet sobre fibra: FOIRL (*Fiber-Optic Inter-Repeater Link*). No se utiliza directamente, si no una de sus variantes (FL -la más utilizada-, FB -para espinazos (*backbones*)- o FP -nunca se usó-).



Fast Ethernet

Esta regulada por la norma IEEE 802.3u. Transmite a 100 Mbps. Utiliza codificación de traducción.

Estándar	Medio y conectores	Repetidores / Estaciones	Dist. / Trans.
100Base-Tx Variante de 100Base-T con cable cat. 5. Código 4B/5B.	Par trenzado (TP) de categoría 5. Usa los mismos hilos que 10Base-T.	2 Clase II[33] unidos con un cable de hasta 5m.	100m. - *Full-Duplex*
100Base-T4 (1) Variante de 100Base-T con cable cat. 3, usando 4 pares. Código 8B/6T.	UTP de categoría 3. Utiliza 3 pares para transmitir y uno para detección de colisiones.	2 Clase II unidos con un cable de hasta 5m.	100m. - *Half-duplex*
100Base-T2 (1) Variante de 100Base-T con cable cat. 3 *Full-Duplex*. Código PAM-5x5.	UTP de categoría 3. Utiliza los 4 pares.	Requiere procesadores de señal específicos muy sofisticados, ya que emiten y reciben *a la vez* por el mismo cable(*), por lo que era una opción cara que nunca se llegó a implementar.	100m. - *Full-duplex* *(* Dual-Duplex)*
100Base-Fx Código 4B/5B NRZ-I (*No Return to Zero - Inverted*).	Fibra óptica multimodo con LED en segunda ventana. Conectores SC.		400m. - *Half-duplex* 2000m - *Full-Duplex*

(1) Pensados para seguir utilizando el cableado telefónico existente (UTP Cat. 3).

Gigabit Ethernet

Esta regulada por las normas IEEE 802.3z para fibra e IEEE 802.3ab para cobre. Transmite a 1000 Mbps.

Estándar	Medio y conectores	Distancia / Transmisión
1000Base-T Código PAM-5x5.	Par trenzado (TP) Cat. 5, 5e o 6. Emite y recibe *simultáneamente* por los 4 pares (*).	100 m. - *Full-duplex* *(* Dual-duplex)*
1000Base-Lx Código 8B/10B NRZ. Se puede optimizar para conseguir hasta 10.000m. de alcance con fibras mono-modo.	Fibra óptica multi y monomodo con ILD en segunda ventana. Conectores SC.	En fibras multimodo: 330m - *Half-duplex* 550m - *Full-duplex* En fibras monomodo: 330m - *Half-duplex* 2000m – *Full-duplex*
1000Base-Sx Código 8B/10B (8 bits/10 baudios) NRZ. La optoelectrónica de LEDs en primera ventana lo hace mucho más económico que Lx	Fibra óptica multimodo con LED en primera ventana. Conectores SC.	62,5/125: 275m. 50/125: <~ 330m - *Half-duplex* <~ 550m – *Full-duplex* Depende de la calidad de la fibra.

33 Los concentradores pueden ser de Clase I o II en función del retardo que generan.

Aunque el estándar define el uso *half-duplex*, no se suele utilizar en fibras. En el caso de *half-duplex* solo se soporta un concentrador. Para poder alcanzar mayor distancia (330m) en *half-duplex* el tamaño mínimo de trama se amplia a 512B bits. Debido a la complejidad de la implementación *half-duplex*, se han diseñado concentradores especiales de fibra llamados *buffered repeaters* que funcionan en *full-duplex* pero sin aislar tráfico como hacen los conmutadores que son más complejos.
En caso de que por un puerto de un conmutador llegue una trama de menos de 512B y el conmutador tenga que enviarla por un puerto *half-duplex*, el conmutador podrá:

- Añadir una extensión de portadora para que la trama tenga 512B.
- Concatenar tramas (tramas Jumbo o *Jumbo frames*) y añadir luego la extensión de portadora si no llegan a tener 512B.

Cuando el conmutador recibe una trama con extensión de portadora y tiene que enviarla a un puerto *full-duplex* o un puerto no gigabit elimina la portadora.
En fibra óptica aparecen los Gbics que llevan la óptica del protocolo para hacer más flexibles los nodos.

Actualmente se está desarrollando el estándar IEEE 802.3ae a 10 Gbps. No funcionará en cable de par trenzado categoría 5, pero puede que si en categoría 5e o 6. Se están pensando hacer un estándar con velocidad variable como en los módems.

Problemas en Ethernet

- Su funcionamiento no permitía a los administradores un control centralizado de la red. Esto se soluciona con conmutadores programables.
- Ethernet considera el medio suficientemente fiable como para no ocuparse de la pérdida de tramas. Una trama perdida no se retransmite hasta que no vence el tiempo de espera (*timeout*) del nivel superior. Como el nivel de red también supone un nivel de enlace fiable, estos tiempos suelen ser altos.
- El mecanismo de retroceso exponencial binario intenta transmitir la trama hasta 16 veces. Si no lo consigue se reporta al nivel superior que hay excesivas colisiones, lo que suele ser debido a errores en el nivel físico.
- Efecto captura. Distintos paquetes pequeños de una máquina que los prepara y emite rápidamente pueden colisionar repetidamente *con el mismo* paquete de una máquina más lenta que irá aumentando su contador de retroceso, mientras que para la máquina rápida son distintas colisiones y cada vez pone su contador a 0, teniendo más probabilidades de enviar antes su paquete y mantener el uso del medio.
- La tasa de colisiones de una red es más o menos preocupante en función de los tamaños de trama que se utilicen. Normalmente debe ser menor del 10%.
- Ethernet no reparte equitativamente los recursos en condiciones de alta ocupación. Con una tasa de colisiones alta puede proporcionar más ancho de banda a aplicaciones que utilizan una trama más grande.
- En una topología no valida (diámetro excesivo del dominio de colisión), puede haber colisiones que se detecten después de haber enviado una trama mínima y haber dado la trama por transmitida. Este fenómeno se denomina "colisiones tardías" y es un síntoma de que pueden estar perdiéndose tramas mínimas.
- Un elevado numero de *broadcast* y/o *multicast* es indeseable. Algunos conmutadores pueden configurarse para filtrar estos paquetes si se supera un cierto umbral o no permitirlos.
- Si dos puntos de la red están unidos por dos caminos alternativos, la topología deja de ser un bus para contener un anillo. Por ese anillo circulan las tramas infinitamente sin ser nunca eliminadas lo que provoca una saturación inmediata de la red. En el caso de que el bucle se cree entre conmutadores sin *spannig tree* activado en al menos uno de ellos, aunque las tramas de *unicast* no entren en el bucle, si lo harán las tramas de *multicast* y de *broadcast*, saturando igualmente la red.
- Otro de los mayores problemas en Ethernet es que uno de los dos extremos este configurado en *full-duplex* y el otro en *half-duplex*. Aunque la mayoría de dispositivos actuales detecta automáticamente el tipo de envío, esto provocaría colisiones en el extremo *half-duplex* que tendrá que reenviar la trama y la pérdida de la trama del extremo *full-duplex* que presupone que no pueden existir colisiones.

Los problemas de colisiones se solucionan si los equipos se conectan a conmutadores *full-duplex*.

Resumen

Estándar	Medio / Conectores	Distancia	Codificación
10Base-5 (1) Primera versión comercial.	Coaxial amarillo de 50 Ω (grueso) y transceptores	500 m. *Half-Duplex*	Manchester
10Base-2 (1) Coaxial más económico.	Coaxial RG58 de 50 Ω (fino) y conectores BNC	185 m. *Half-Duplex*	Manchester
10Base-T (2) Reutiliz. cables de telefonía.	UTP Cat. 3 y RJ-45. UTP Cat. 5 y RJ-45.	Cat. 3 – 100m Cat. 5 – 150m *Half-Duplex* y *Full-Duplex*	Manchester
10Base-F (3) (**10Base-Fx**) Fibra óptica multimodo. FL / FB / FP	Multimodo; LED en primera ventana. Luz visible. Conectores ST.	2000 m. *Half-Duplex* y *Full-Duplex*	Manchester
100Base-Tx UTP Cat. 5.	UTP Cat. 5 y RJ-45.	100m. - *Full-Duplex*	4B/5B
100Base-T4 (1) UTP Cat. 3 Half no balanceado.	UTP Cat. 3 y RJ-45. 3 pares para transmisión 1 par para colisiones	100m. - *Half-duplex*	8B/6T
100Base-T2 (1) UTP Cat. 3 Full balanceado.	UTP Cat. 3 y RJ-45. Procesadores específicos.	100m. - *Full-duplex* *(Dual-Duplex)*	PAM-5x5
100Base-Fx Fibra óptica.	Multimodo; LED en segunda ventana. Conectores SC.	400m. - *Half-duplex* 2000m - *Full-Duplex*	4B/5B NRZ-I
1000Base-T Par trenzado.	UTP Cat. 5, 5e o 6 y RJ-45.	100 m. - *Full-duplex* *(Dual-duplex)*	PAM-5x5
1000Base-Lx Fibra más rápida.	Fibra óptica multi y monomodo con ILD en segunda ventana. Conectores SC.	En fibras multimodo: 330m - *Half-duplex* 550m - *Full-duplex* En fibras monomodo: 330m - *Half-duplex* 2000m - *Full-duplex*	8B/10B NRZ
1000Base-Sx Fibra más económica.	Fibra óptica multimodo con LED en primera ventana. Conectores SC.	62,5/125: 275m. 50/125: 330m - *Half-duplex* 550m - *Full-duplex*	8B/10B NRZ

4.12. Mejoras de rendimiento

Según estudios de Boggs[34] y colaboradores el rendimiento de una red Ethernet depende de:

- el tamaño de trama utilizado (a mayor trama, mayor rendimiento). Probablemente el más influyente dado que las colisiones siempre se producen en los primeros 2τ bits[35] (que su vez debe ser <= 512 bits por respeto a la trama mínima).
- el número de estaciones del dominio de colisión (a menor número de estaciones, mayor rendimiento).
- el tiempo de ida y vuelta (a menor diámetro del dominio de colisión, mayor rendimiento).

Recomendaciones para mejorar el rendimiento:

- no instalar “cables” largos (incluir puentes o conmutadores).
- no instalar demasiados ordenadores en un mismo dominio de colisión (incluir puentes o conmutadores).
- utilizar el tamaño de trama máximo posible.
- no mezclar aplicaciones de transferencia masiva de datos con aplicaciones de tiempo real.
- utilizar el protocolo correctamente -detección de colisiones, retroceso exponencial binario y pausa entre tramas- (detectaron que muchos de los principales fabricantes no lo hacían).

Agregación de enlaces

La agregación de enlaces (*Link Aggregation*) es una técnica también llamada "*Port trunking*", "*NIC bonding*" o "*Ethernet trunk*", entre otros. Consiste en agregar dos enlaces físicos en un único enlace lógico entre dos nodos. Estos nodos serán normalmente dos conmutadores o un conmutador y un equipo con tarjetas especiales que lo soporten.
El trafico se reparte entre los dos enlaces, consiguiendo más ancho de banda y más fiabilidad, puesto que si cae un enlace (rotura de un cable) se mantiene la conexión por los restantes.

VLANs

Las VLANs (Virtual LANs) aparecen para montar redes de nivel 2 independientes compartiendo la electrónica y el cableado. El estándar que las normaliza es el IEEE 802.1Q y su implantación más habitual es por puertos.
Si se configuran 2 puertos de un conmutador en VLANs diferentes, las estaciones conectadas a uno de los puertos no podrán comunicar (en este nivel) con las estaciones del otro puerto.
Se pueden configurar puertos por los que circulen tramas de varias VLANs con un campo especial que define a cual pertenece cada trama. Estos puertos se suelen llamar 'etiquetados' (*tagged*) y pueden utilizarse para unir dos conmutadores o un conmutador y un servidor con tarjetas especiales.

Destino	Origen	[Tag]	Tipo/Long.	Datos	Relleno	CRC
6	6	[4]	2	0 – 1500	0 – 46	4

El formato del campo Tag es el siguiente (en bits):

8100	Prioridad	CFI	VID
16	3	1	12

El campo 8100 se utiliza para identificar que esto es un campo *tag*. Si esto no fuera un campo *tag*, en su lugar estaría el campo Tipo/Longitud que nunca puede tener un valor 8100.
El campo de prioridad permite 8 niveles (3 bits).
El campo CFI (*Canonical Format Indicator*) se pone a 1 para indicar compatibilidad con Token-Ring.
El campo VID es el identificativo de la VLAN a la que pertenece el paquete. Si se conecta a un puerto etiquetado un equipo que no soporte 802.1Q, éste no funciona porque no entiende las tramas que le llegan.

34 (1988) Measured Capacity of an Ethernet: Myths and Reality. David Boggs colaboró con Robert Metcalfe en el diseño de Ethernet y construyó en 1975 el primer encaminador y el primer servidor de nombres de Internet.
35 Un número que crece con la velocidad de la red, ya que en el mismo tiempo se transmite más información.

Además de las VLAN por puertos, en que cada puerto de un concentrador pertenece a una VLAN, existen equipos que permiten realizar VLANs por direcciones MAC, por protocolo (inspeccionando datos de la capa 3 y formando redes según estos protocolos) o por direcciones IP (también de la capa 3), independientemente del puerto en que se conecten las máquinas.
Por coste y sencillez de gestión la gran mayoría de VLANs que se implementan son por puertos.

Prioridades

En redes Ethernet con conmutadores se pueden implementar prioridades para dar preferencia a un cierto tráfico de la red. Esto permite en cierta medida implementar aplicaciones de tiempo real sobre Ethernet.
El estándar que regula este mecanismo es el IEEE 802.1P que se integró más tarde dentro de IEEE 802.1Q.
Se puede aplicar una prioridad a cada puerto de un conmutador para que procese las tramas recibidas en cada puerto con más o menos rapidez.
Para poder aplicar prioridades entre concentradores, esta información es incluida en la trama en un campo especial añadido. Este campo aparece también en la trama 802.1Q.
Cuando un conmutador recibe una trama, la asigna a una cola con más o menos prioridad en función de la etiqueta que tenga la trama.
Como el campo de prioridad es de 3 bits, existen 8 niveles de prioridad diferentes.

5. IEEE 802.11 (Wi-Fi)

5.1. Definición

IEEE 802.11[36] es un conjunto de estándares de protocolo de nivel de enlace (N2) para redes inalámbricas de área local (WLAN: *Wireless* LAN), que trabaja en las bandas de 2.4 GHz y 5 GHz.
Aunque los términos 802.11 y Wi-Fi se intercambian habitualmente, no son exactamente lo mismo. 802.11 es el estándar de IEEE, mientras que "Wi-Fi" es una marca registrada de la alianza Wi-Fi (*Wi-Fi Alliance*), un grupo empresarial que inicialmente incluía empresas como 3Com, Cisco, Lucent, Nokia... y que actualmente engloba a casi todas las empresas del mercado en una u otra manera. Esta alianza nació para asegurar la compatibilidad entre dispositivos 802.11 y entrega certificados Wi-Fi. Sin embargo por cuestiones de mercado a veces se ha anticipado a los estándares certificando en base a borradores 802.11 ("futuros estándares").

Otras redes inalámbricas

IEEE 802.11 es el estándar para redes inalámbricas de área local (WLAN). Para redes inalámbricas de área personal (WPAN: *Wireless* PAN) se utiliza:

- IEEE 802.15.1 - Bluetooth: versión estandarizada de Bluetooth. Frec. 2'45 GHz. Entre 1 y 20 Mbps.
- IEEE 802.15.x: 4 estándares más de WPAN.
- Infrarrojo.

Para áreas metropolitanas (WMAN) se utiliza:

- IEEE 802.16: Conmutación de paquetes. Punto a multipunto.
- IEEE 802.20: WMAN *Mobile*.

5.2. Otras definiciones

Punto de acceso (AP: Access Point)

Un punto de acceso es un puente (N2) entre la red inalámbrica y otra red, que se encarga de realizar las conversiones de trama pertinentes.

Conjunto de Servicio Básico (BSS: *Basic Service Set*)

Bloque mínimo de una red WLAN. Se identifica mediante un BSSID (*BSS IDentifier*) y puede configurarse en dos modos:

- Infraestructura o gestionado: las estaciones se comunican a través de un punto de acceso. En este caso se conoce también como BSS la cobertura del AP -que es quien gestiona la red-. En este caso el BSSID es la dirección MAC del AP.
- Independiente o *ad-hoc* (IBSS): las estaciones se intercomunican directamente. Su precursor fueron las redes de paquetes de radio (*packet radio network*) de DARPA. En este caso el BSSID es un número aleatorio (PseudoMAC).

Conjunto de Servicio Extendido (ESS: *Extended Service Set*)

Conjunto de uno o más BSSs que funcionan como un único BSS para la capa lógica de red (N2 LLC). Este conjunto se identifica mediante una cadena de caracteres llamada ESSID (*ESS Identifier*) definida por el administrador. Este ESSID es a veces llamado simplemente SSID o "nombre de la red". Los distintos BSS del ESS pueden trabajar en el mismo canal o en distintos canales para ampliar la capacidad de la red.

Sistema de Distribución

Mecanismo que sirve para controlar a qué AP se envían las tramas. Proporciona movilidad entre distintos AP aunque las estaciones solo podrán cambiar de ubicación sin perder conectividad siempre que la transición se realice dentro de un mismo ESS.

36 En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

Señales Beacom

La sincronización de estaciones es muy importante y se hace a través de tramas especiales llamadas Beacom. El punto de acceso las emite periódicamente. Una estación puede esperarlos para sincronizarse (*passive scanning*) o emitir peticiones para recibirlas (*active scanning*).

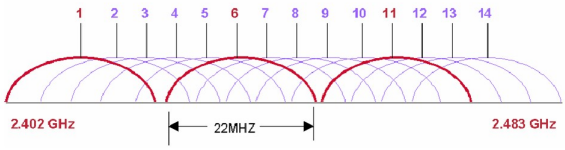
Las bandas ISM

Las bandas ISM (*Industrial Scientific Medical*) son bandas de radiofrecuencia electromagnética reservadas internacionalmente para uso no comercial en áreas de trabajo industriales, científicas y médicas. Estas bandas pueden utilizarse sin necesidad de licencia siempre que se respeten unos determinados límites de potencia.
Fueron definidas por la ITU (*International Telecomunications Union*) en el artículo 5 de las Regulaciones de Radio (RR 5.138, 5.150 y 5.280) y todo aparato que trabaje con ellas debe ser tolerante a errores y utilizar mecanismos de protección contra interferencias, como técnicas de ensanchado de espectro (RR 15.13). Por este motivo, las redes que funcionan en esta banda se les denomina redes de espectro ensanchado.

Algunos aparatos que usan la frecuencia de 2,4 GHz son los microondas, teléfonos inalámbricos, monitores de bebés, IEEE 802.15.1 (WPAN - Bluetooth) e IEEE 802.11 (WLAN)...

Además de utilizarse diferentes técnicas de espectro ensanchado, en función de la relación señal/ruido se puede utilizar una modulación (bits por símbolo) más o menos rica para alcanzar más velocidad, por lo que los aparatos realizan una negociación de velocidades.

Según la zona geográfica, en la banda de los 2.4GHz se utilizan de 7 a 14 canales (13 en Europa). El ancho de banda de la señal (22MHz) es superior a la separación entre canales consecutivos (5MHz), por eso se hace necesaria una separación de al menos 5 canales con el fin de evitar interferencias entre celdas adyacentes. Tradicionalmente se utilizan los canales 1, 6 y 11 o los canales 1, 5, 9 y 13.



Diversificación de la señal

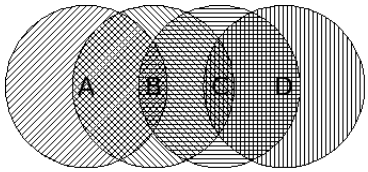
Como las señales viajan rebotando en las paredes y objetos, se produce autointerferencia de las señales al llegar desfasadas según el camino que recorren (multitrayectoria de la onda). Es decir se produce interferencia debido a la diferencia de tiempo entre la señal que llega directamente y la que llega reflejada por diversos obstáculos. Para minimizar este efecto, se suelen utilizar dos antenas ligeramente separadas y el receptor elige la señal de la antena donde se recibe con más claridad.

Codificación radioeléctrica

Las técnicas de codificación que se utilizan son variantes de CDMA (*Code Division Multiple Access*). A 5 GHz se utiliza OFDM (*Orthogonal Frequency Division Multiplexing*). A 2,4 GHz se utiliza DSSS (*Direct Sequence Spread Spectrum*) con diversidad de antenas (dobles antenas). El estándar original también permitía el uso de la técnica FHSS (*Frequency Hopping Spread Spectrum*) que reduce mejor la autointerferencia usando una sola antena.
Con dichas técnicas, si hay ruido en alguna frecuencia no afecta a una sola banda, sino que se reparte el efecto entre todas y su efecto es menor.

5.3. Problemas añadidos en redes inalámbricas

Además de los problemas habituales de acceso al medio existen dos problemas añadidos:



- **Nodos ocultos**: en que una estación cree que el canal está libre, pero en realidad está ocupado por un nodo al que no escucha.
  Por ejemplo el nodo A está en el rango del nodo B, pero queda fuera del rango del nodo C y no puede detectar si el nodo C está transmitiendo al nodo B.
- **Nodos expuestos**: en que una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría.
  Por ejemplo el nodo C puede retrasar sus transmisiones al nodo D mientras el nodo B transmite para A, que en realidad no interferiría.

5.4. Control de acceso al medio (MAC: *Medium Access Control*)

El sistema de control de acceso al medio (N2 capa MAC) de IEEE 802.11 es la pila de protocolos DFWMAC (*Distributed Foundation Wireless Medium Access Control*), aunque este nombre es poco utilizado en la literatura al respecto. La base de DFWMAC es una técnica de coordinación distribuida llamada DCF (*Distributed Coordination Function*), obligatoria en el estándar 802.11.
IEEE 802.11 también define una técnica de coordinación centralizada llamada PCF (*Point Coordinated Function*) que solo está disponible en modo infraestructura. Esta técnica es opcional y además no se exige para los certificados de la alianza Wi-Fi, por lo que muy pocos aparatos lo implementan.

PCF (*Point Coordinated Function*)

PCF alterna dos periodos de tiempo: periodos con conflictos (CP: *Contention Period*) y periodos libres de conflictos (CFP: *Contention Free Period*). Durante los CP las estaciones simplemente utilizan DCF. Durante los CFP el punto de coordinación (el AP) controla qué estación puede transmitir en cada momento de manera síncrona[37] con un algoritmo Round-Robin. Esta coordinación centralizada permite ciertas gestiones de QoS, por ejemplo para conexiones sensibles al tiempo, como emisiones de vídeo, y se puede utilizar para minimizar el problema de los nodos ocultos (si ningún nodo queda oculto al controlador). El principal inconveniente que se le achaca es que no define clases de tráfico.

IEEE 802.11e define una nueva función de coordinación HCF (*Hybrid Coordination Function*) con el objetivo de incorporar garantías QoS y permitir aplicaciones de tiempo real.

DCF (*Distributed Coordination Function*)

DCF utiliza un algoritmo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) con intercambio RTS/CTS opcional y acuse explícito de recibo. Usa comunicación asíncrona[38] entre estaciones.
La idea base de CSMA es que una estación que desea transmitir en un medio compartido primero escucha el canal para verificar si tiene actividad. En caso de que el canal esté libre la estación comienza a emitir inmediatamente.

Ethernet que utiliza CSMA/CD espera a que el canal quede libre (más la pausa requerida) y comienza a emitir. En caso de que otra estación estuviese también esperando para emitir se produce una colisión. Las estaciones emisoras detectan la colisión y esperan un tiempo aleatorio antes de volver a intentarlo.
Sin embargo dado que el rango dinámico de señales es muy amplio las NIC inalámbricas no son capaces detectar colisiones, por lo que no se puede usar CSMA/CD. En vez de ello se utiliza CSMA/CA.

37 Las comunicaciones síncronas utilizan ventanas de tiempo en las que se puede transmitir, y obligan a que las estaciones se mantengan sincronizadas para utilizar las mismas ventanas de tiempo (de manera centralizada o distribuida).
38 Las comunicaciones asíncronas utilizan ventanas variables y no sincronizadas de tiempo.

CSMA/CA hace varias cosas:
- verifica si el medio está libre u ocupado (CSMA);
- cuando la línea está ocupada espera un tiempo aleatorio antes de volver a intentar enviar (CSMA);
- incluye un mecanismo opcional de intercambio RTS/CTS antes de emitir el mensaje (CA);
- incluye un mecanismo de acuse explícito de recibo a nivel de MAC (CA);

Es decir, cuando una estación inalámbrica desea transmitir primero verifica que el canal está libre durante un tiempo predeterminado. Si está libre comienza a emitir inmediatamente y si está ocupado espera primero a que quede libre y después un tiempo aleatorio antes de volver a verificarlo (CSMA).
Una vez la estación puede emitir utiliza un intercambio RTS/CTS (éste intercambio no se utiliza para mensajes muy cortos en que la sobrecarga no vale la pena). Para este intercambio primero envía una trama corta de control de solicitud de transmisión RTS (*Request To Send*) indicando a las demás estaciones que no transmitan. Esta trama además especifica las estaciones origen y destino de la comunicación y el tamaño de la trama que se desea transmitir. Si la estación destinataria recibe correctamente esta señal devuelve una trama indicando que está ocupado -comunicándose con un nodo oculto- (RxBUSY) o una trama indicando que todo está preparado para la emisión (CTS: *Clear To Send*) y el tamaño de trama que va a recibir.
Si una estación recibe el mensaje RTS pero no la respuesta (CTS o RxBUSY) sabe que es un nodo expuesto y que puede comunicarse con otro nodo a la vez.
Si una estación no ha recibido un RTS pero recibe un CTS sabe que es un nodo oculto y que debe esperar y además sabe cuánto tiempo debe hacerlo porque conoce el tamaño de trama que se va a enviar.

Tras emitir el mensaje, la estación emisora espera a una respuesta del destinatario indicando una recepción correcta ("ACK") o incorrecta ("NACK"). En el segundo caso -o si no recibe respuesta- el emisor volverá a emitir el mensaje, existiendo un límite para el número de posibles reenvíos.

Sus principales inconvenientes son:
- Si muchas estaciones pretenden comunicar a la vez, ocurrirán muchas colisiones que disminuirán el ancho de banda disponible.
- No hay prioridades o clases de tráfico ni garantías de QoS.
- Cuando una estación gana el medio puede secuestrarlo. Por ejemplo una estación que transmita a 1Mb/s puede tardar mucho tiempo en enviar un paquete, perjudicando al resto de estaciones.
- Para poder garantizar la usabilidad del canal ha de sacrificar un porcentaje significativo de la capacidad incrementando el volumen de tráfico -con tráfico de control-.

5.5. Seguridad

Aunque la seguridad se contempló desde el principio, originalmente no era muy buena debido principalmente a las limitaciones para exportar productos de criptografía de muchos países (especialmente EE.UU.). Tras cambios normativos apareció una revisión del protocolo (802.11i) que mejora la seguridad del mismo. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores.

El sistema inicial se llamó WEP (*Wired Equivalent Privacy*) basado en el algoritmo de encriptación RC4 y clave pre-compartida (PSK). Ya en 2001 se presentaron trabajos que mostraban la debilidad de este sistema y hoy día existen programas que se encargan desatendidamente de romper la seguridad de una red basada en WEP.
IEEE creó un grupo -802.11i- dedicado a reemplazar el sistema de seguridad (anteriormente se encargaba el grupo 802.11e). La alianza Wi-Fi anunció una especificación llamada WPA (*Wi-Fi Protected Access*) basándose en el borrador de 802.11i que comenzó a utilizarse en 2003. Esta especificación era TKIP (*Temporal Key Integrity Protocol*) y se basaba también en RC4 con PSK. Sus mejoras en seguridad consistían principalmente en realizar un control de integridad de los paquetes (ya que en los ataques algunos paquetes se alteraban sin llegarlos a descifrar), un conteo de los mismos y utilizar una función de mezcla de la clave con el vector de inicialización de la red (en vez de una simple concatenación) para generar la clave RC4.
El sistema 802.11i final, conocido como WPA2, apareció en 2004. Permite nuevos mecanismos de distribución de la clave (como EAP), autenticación PSK o basada en servidores (como RADIUS) y CCMP (basado en AES) para cifrado. La configuración habitual recomendada es WPA2 con clave precompartida (AES *PreShared Key*) -en entornos domésticos o PyMES- o WPA2 con servidores RADIUS (EAP-TLS) en entornos corporativos.

En 2005 IEEE creó otro grupo -802.11w- que pretende asegurar las tramas de gestión y difusión, que en los estándares anteriores son inseguras. La fecha prevista de publicación es Marzo de 2008.

Muchos puntos de acceso permiten establecer un control por dirección MAC permitiendo o denegando el acceso únicamente a las tarjetas inventariadas. En algunos casos, la lista de MACs se puede mantener en un servidor RADIUS.

5.6. Evolución del estándar 802.11

Legacy

El estándar original IEEE 802.11 de 1997 -conocido como “legacy”-, especificaba dos ratios de transmisión de 1 y 2 Mbps sobre infrarrojos (IR) o sobre radiofrecuencia en la banda ISM de 2,4 GHz. Aunque la transmisión por infrarrojos sigue incluida en el estándar no hay en el mercado productos que la utilicen.
Permite usar codificación DSSS (*Direct Sequence Spread Spectrum*) o FHSS (*Frequency Hopping Spread Spectrum*).

802.11a

La revisión 802.11a al estándar original fue ratificada en 1999 y funciona en la banda de 5GHz utilizando 52 subportadoras OFDM (*Orthogonal Frequency-Division Multiplexing*).
802.11a tiene una velocidad teórica máxima de 54 Mbit/s, con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario.
802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto.
Los equipos 802.11a y 802.11b no pueden operar entre ellos.

La revisión 802.11a utiliza la banda de 5 GHz, que tiene restricciones -de hecho 802.11a no es utilizable en Europa-. Sin embargo la cantidad de canales disponibles y la ausencia de interferencias hacen de él una buena opción para profesionales y empresas que estén dispuestos a obtener (y pagar) una licencia para el uso de dicha banda. Sin embargo, la utilización de esta banda también tiene sus desventajas. Dado que sus ondas son más fácilmente absorbidas, los equipos 802.11a deben quedar en línea de vista y son necesarios un mayor número de puntos de acceso.
Los productos del estándar 802.11a aparecieron en el mercado en 2001.

802.11b

La revisión 802.11b del estándar original fue ratificada en 1999 y funciona en la banda de 2.4GHz. Fue la primera revisión que tuvo una amplia aceptación en el mercado.
802.11b tiene una velocidad teórica máxima de transmisión de 11 Mbit/s, pero debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica la velocidad máxima de transmisión es de aproximadamente 5.9 Mbit/s para TCP y 7.1 Mbit/s para UDP.
Los dispositivos 802.11b deben mantener la compatibilidad con la norma original IEEE 802.11 -utilizando DSSS-.

Aunque también utiliza una técnica de ensanchado de espectro basada en DSSS, en realidad la extensión 802.11b introduce CCK (*Complementary Code Keying*) para llegar a velocidades de 5,5 y 11 Mbps (tasa física de bit). El estándar también admite el uso de PBCC (*Packet Binary Convolutional Coding*) como opcional.

802.11g

La revisión 802.11g es la evolución del estándar 802.11b y fue ratificada en Junio de 2003. Es compatible con el estándar 'b' y utiliza las mismas frecuencias (2.4GHz) aunque con una velocidad teórica máxima de transmisión de 54 Mbit/s. La velocidad real de transferencia es de aproximadamente 22 Mbit/s, similar a la del estándar 802.11a.
En redes bajo el estándar 'g' la presencia de nodos bajo el estándar 'b' reduce significativamente la velocidad de transmisión.
Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación oficial. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar 'b'. A partir de 2005, la mayoría de los productos que se comercializan siguen la revisión 802.11g con compatibilidad hacia 802.11b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

802.11h

La especificación 802.11h se hizo pública en octubre de 2003 y soluciona problemas derivados de la coexistencia de las redes 802.11a con sistemas de Radares y Satélite. Aunque se utiliza en muchos otros países, fue originalmente desarrollada para incorporar directrices europeas que pretenden minimizar el impacto de abrir la banda de 5 GHz -utilizada generalmente por sistemas militares- a aplicaciones ISM.
Dichas directrices imponen la capacidad de gestionar dinámicamente tanto la frecuencia como la potencia de transmisión mediante funcionalidades DFS y TPC.

- DFS (*Dynamic Frequency Selection*) pretende evitar interferencias co-canal con sistemas de radar y asegurar una utilización uniforme de los canales disponibles.
- TPC (*Transmitter Power Control*) permite limitar la potencia transmitida para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

802.11i

Aprobado en 2004, está dirigido a mejorar la seguridad. El estándar abarca los protocolos 802.1x, TKIP (*Temporal Key Integrity Protocol*) -basado en RC4, conocido inicialmente como WEP2 y posteriormente como WPA- y AES (*Advanced Encryption Standard*). La versión definitiva del estándar, basada en AES, se conoce como WPA2, y se utiliza generalmente en la forma AES-PSK o EAP-TLS.

802.11e

La revisión 802.11e, aprobada en 2005, aporta mejoras en el sistema de control y servicios de 802.11.
Su objetivo es soportar tráfico en tiempo real con garantías de Calidad de Servicio (QoS). Para ello introduce clases de tráfico y un nuevo sistema de coordinación llamado HCF (*Hybrid Coordination Function*) con dos tipos de acceso:

- EDCA (*Enhanced Distributed Channel Access*): Sistema distribuido de control. Se basa en prioridades de tráfico. El tráfico más prioritario espera menos tiempo antes de emitir y utiliza marcos de tiempo de envío (TXOP *Transmit Opportunity*) más largos que el tráfico menos prioritario, que espera más antes de emitir y emite por menos tiempo (TXOP menores).
- HCCA (*HCF-Controlled Channel Access*): Sistema centralizado de control. De forma parecida al funcionamiento de PCF, HCF contempla periodos controlados o no, con la diferencia principal de que el AP puede iniciar un periodo controlado en cualquier momento y no de forma predeterminada. Análogamente a como ocurría en PCF, los periodos no controlados se rigen por el sistema EDCA. Además el controlador recibe información sobre el tráfico que desea enviar cada estación y en base a ellos y la QoS utiliza algoritmos de planificación complejos, no únicamente *Round-Robin*.
  También análogamente a PCF, su implementación es opcional y casi ningún equipo la soporta.

Además 802.11 incorpora otras mejoras como APSD (*Automatic Power Save Delivery*), BA (*Block Acknowledgments*), QoSAck / QoSNoAck y DLS (*Direct Link Setup*).

Certificación WMM

La certificación WMM (*Wireless MultiMedia*) de la alianza Wi-Fi, no es un estándar. Basándose en el borrador de 802.11e, prioriza el tráfico en base a 4 categorías de acceso AC (*Access Categories*): voz, vídeo, mejor esfuerzo (*best effort*) y fondo (*background*).
Para que un AP obtenenga el certificado WMM debe incorporar soporte para EDCA y TXOP así como *Power Save Certification*.

802.11n

Previsto para finales de 2009 802.11n debería ser capaz de trabajar tanto en banda de 2.4GHz como en banda de 5GHz, siendo compatible con todas las revisiones anteriores y alcanzando una velocidad teórica mayor de 600 Mbit/s.
También se espera que el alcance de operación de las redes sea mayor gracias a la tecnología MIMO (*Multiple Input – Multiple Output*), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.
Actualmente ya existen varios productos que cumplen el segundo borrador de la revisión 'n' con un máximo de 300 Mbps (80-100 estables).

802.11w

Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso al medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Se intenta extender la protección que aporta 802.11i en los datos a las tramas de gestión.

Resumen de revisiones

Aunque se usan los términos “estándar” y “revisión” (*amendment*) para referirse a las diferentes variantes de IEEE 802.11, oficialmente solo existe un estándar llamado IEEE 802.11, siendo la versión actual del estándar la IEEE 802.11-2007. Sin embargo el estándar se va actualizando con revisiones creadas por grupos de trabajo (TG: *Task Group*) identificados por una letra minúscula. Por ejemplo el grupo de trabajo TGm se encarga de actualizar 802.11 y realizar aclaraciones e interpretaciones de los documentos publicados para la industria.
Independientemente de los estándares están las certificaciones de la Wi-Fi Alliance, como WMM, que se basan en los estándares, revisiones y borradores de IEEE.

Revisión	Notas	Banda	Velocidad	Publicación
802.11-1997	*Legacy*	IR / 2.4GHz	1 o 2 Mb/s	1997
802.11a	Banda de 5 GHz	5 GHz	54 Mb/s	1999
802.11b	Primero con gran aceptación comercial	2.4 GHz	11 Mb/s	1999
802.11g	Revisión de b	2.4 GHz	54 Mb/s	2003
802.11h	Revisión de a para Europa	5 GHz	54 Mb/s	2003
802.11i	Mejoras en la seguridad (WPA, WPA2)			2004
802.11e	Mejoras QoS (EDCA y HCCA)			2005
802.11n	MIMO	2.4 y 5 GHz	>600 Mb/s*	2009*
802.11w	Seguridad en tramas de gestión			2008-2009*

* Previsto

6. PROTOCOLOS WAN

6.1. Portadora-T y PDH (*Plesiochronous Digital Hierarchy*)

El sistema portadora-T fue introducido por Bell System en los Estados Unidos en los años 60 y se utiliza principalmente en EE.UU. y Japón. A partir de ella e impulsada en Europa se desarrolló la jerarquía digital plesiócrona[39] o PDH (*Plesiochronous Digital Hierarchy*) también conocida como portadora-E. PDH tiene mayor capacidad porque presupone el uso de líneas más fiables, eliminando sobrecarga del control de errores.

El sistema PDH es un protocolo de capa física (N1) basado en líneas dedicadas enteramente digitales. Usando modulación de pulso y multiplexación de división de tiempo permite enviar varios canales sobre un mismo medio. Por tanto cada línea se compone de varios canales básicos. Al agrupar canales hay que añadir bits de sincronismo y entramado porque el reloj de cada canal es independiente.
El sistema utiliza conexiones full-dúplex, originalmente mediante dos pares trenzados de cobre y actualmente también sobre coaxial, microondas o fibra óptica. Sin embargo este diseño no obtiene un buen rendimiento sobre fibra, por lo que está siendo sustituido por las redes SONet/SDH.

La línea digital E1 consiste en 32 canales de 64 Kbps multiplexados (2 Mbps)[40]. Un enlace E1 estructurado utiliza un canal para sincronización y uno para entramado. Un enlace E1 no estructurado, utilizado como línea punto a punto, utiliza los 32 canales para datos.
En el sistema portadora-E al canal básico de 64 kbps se le llama a veces línea E0.

Protocolo	Capacidad	Canales por línea	Interfaz
E1	2 Mbps	30 canales + sinc. + entram.	V.35
E2	8 Mbps	4 x E1 + sinc. + entram.	-no se comercializan (se utilizan enlaces E1 en paralelo)-
E3	34 Mbps	4 x E2 + sinc. + entram.	HSSI (*High Speed Serial Interfaz*)
E4	140 Mbps	4 x E3 + sinc. + entram.	-no se comercializan-

Sus principales inconvenientes son:

- Los sistemas de portadora-T y portadora-E no son compatibles, aunque pueden interconectarse.
- Fue diseñado para utilizar señales eléctricas o microondas y no utiliza eficazmente la fibra óptica .
- No dispone de un buen sistema de gestión ni de redundancia.
- Los bits de relleno utilizados para forzar el sincronismo impiden extraer un canal de voz directamente cuando se encuentra en una trama de jerarquía superior (E1, E2, E3) necesitándose descomponer completamente la trama para extraer el canal y volver a componer una trama. Esto requiere equipos muy costosos y complejos en las centrales.

39 Deriva del griego *plesio* -cercano- y *chronos* -tiempo- y se refiere a que los canales de PDH están casi, pero no completamente, sincronizados.
40 La línea digital T1 utiliza 24 canales de 64 Kbps (1,5 Mbps).

6.2. X.25

El protocolo X.25 fue el primer protocolo que utilizaba la RTC en ser estandarizado por el antiguo CCITT (ahora ITU) en 1976. Diseñado para líneas de comunicación poco fiables (con muchos errores de transmisión), ofrece un servicio fiable orientado a conexión (circuitos PVC y SVC), que garantiza que los paquetes llegan en el mismo orden que salieron. Para ello utiliza la técnica de *store-and-forward* con confirmación de llegada en cada nodo, unido a un protocolo de ventana deslizante y un tamaño de trama pequeño (128 bytes).
Especifica los tres niveles inferiores del modelo ISO OSI:

- Define dos niveles físicos posibles: X.21 (digital) y X.21bis (analógico).
- El nivel de enlace se llama LAP-B (*Link Access Procedure-Balanced*).
- El nivel de red se llama PLP (*Packet Layer Protocol*) y el direccionamiento está estandarizado a nivel internacional (X.121).

Los protocolos de nivel 2 y 3 son complejos, por ello hay unos aparatos llamados PAD (*Packet Assembler Dissasembler*) que realizan las funciones de estos niveles para conectar equipos terminales poco potentes.

Sus velocidades típicas oscilan entre 9,6Kbps a 64kbps, siendo el costo proporcional al tiempo de duración del circuito y al número de paquetes enviados. No es apto para tráfico en tiempo real y en la actualidad está siendo totalmente reemplazado por otros protocolos como Frame-Relay.

6.3. RDSI

La Red Digital de Servicios Integrados (RDSI o ISDN: *Integrated Services Digital Network*) es una red que provee conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados, independientemente de la naturaleza de la información a transmitir y del equipo terminal que la genere.
Los protocolos de acceso RDSI presentan una arquitectura de capas que se puede hacer corresponder con la del modelo OSI, con gran variedad de configuraciones.
RDSI proporciona conexiones de conmutación de circuitos y de datagramas a 64 kbps bajo demanda, siendo su coste proporcional al tiempo de uso (aunque pueden contratarse tarifas planas).
Otras ventajas son:

- Establecimiento de conexión en un tiempo muy corto (entre ½ y 2 segundos) lo que permite que se realice la llamada cuando se necesite enviar datos para enviar.
- El receptor puede identificar al número que llama, con lo que se pueden establecer mecanismos de seguridad.

Existen dos tipos de canales:

- B -*bearer*- para transmisión de datos a 64Kbps
- D -*data*- de señalización y administración que siempre está activo. Puede ser de 16 (BRI) o 64 (PRI) kbps.

También existen dos tipos de acceso al servicio:

- Básico (BRI: *Basic Rate Interface*): 2B + 1D (16 kbps). Orientado a PyMEs y domicilios. El interfaz físico se llama TR1 (Terminador de Red 1 o NT1: *Network Terminator*) y se conecta mediante RJ45 usando dos pares para datos y dos para alimentación eléctrica.
- Primario (PRI: *Primary Rate Interface*): Si se implementa sobre T1 (EEUU y Japón) son 23B + 1D. Si se implementa sobre un E1 se utilizan 30B + 1D y el canal restante se utiliza para sincronismo.

Los canales B se pueden utilizar agregados o independientemente tanto para voz como para datos. Sus usos principales son: conexión de centralitas digitales privadas (PBX) a la red telefónica; videoconferencia (estándar H.320 con 2 canales B -128 kbps- o 6 canales B -384 kbps-); transmisión de varios canales de audio (conexiones de radio); y transmisión de datos, actualmente como servicio de apoyo a otras líneas en horas punta, o como conexión redundante.

6.4. FDDI (*Fiber Distributed Data Interface*) / CDDI

FDDI comenzó a ser desarrollado por el comité de estándares ANSI X3T9.5 en 1983 para constituir una LAN alternativa a Ethernet y Token Ring que además ofreciese una mayor fiabilidad. En la actualidad, en redes LAN se prefiere utilizar Fast/Gigabit Ethernet.
FDDI es un estándar de transmisión basado en un doble anillo con token bus en direcciones contrarias. Puede extenderse hasta 200 kilometros y permitir miles de usuarios, por lo que se ha utilizado también como WAN.
En caso de utilizarse cobre en vez de fibra como soporte, se llama CDDI.

6.5. FRAME-RELAY

Introducción

Frame-Relay es un protocolo de nivel 2 utilizado principalmente para interconectar redes LAN. Se basa en la utilización de la infraestructura de red disponible por los prestadores de servicio público, aunque puede ser también implementada sobre líneas dedicadas.
Frame Relay surgió como es el sucesor de la tecnología X.25, y está pensada para capas físicas con bajas tasas de errores y velocidades relativamente altas (de hasta 2 Mb/s, aunque podría funcionar sin problemas a velocidades mayores). El único control de errores que realiza es la verificación de tramas, sin realizar acuse de recibo. En caso de detectar una trama errónea la descarta, pero no solicita retransmisiones.

La tecnología Frame Relay se basa en la utilización de circuitos virtuales (VC: *Virtual Circuits*) tanto permanentes como conmutados (PVCs y SVCs). Los circuitos virtuales son caminos bidireccionales, establecidos entre dos puntos extremos de la red Frame Relay. Existen dos tipos de circuitos virtuales:

- **PVC (*Permanent VC*)**: Los PVC son circuitos virtuales permanentes -independientemente del tráfico- establecidos por el operador de red. Los PVC son definidos de forma estática, y se requiere la intervención de un operador para establecerlos y liberarlos. Son los más utilizados en Frame Relay.
- **SVC (*Switched VC*)**: Son circuitos que se establecen de forma dinámica en el momento de establecer la conexión. La implementación de circuitos virtuales es más compleja que la de circuitos permanentes, pero permite, en principio, conectar cualquier nodo de la red Frame Relay con cualquier otro.

Cada nodo dispone de un enlace Frame-Relay sobre el que se pueden establecer distintos circuitos. Cada nodo se identifica con un DLCI (*Data Link Connection Identifier*) local a cada conmutador, el cual lo puede cambiar cuando reenvía la trama. Para establecer circuitos conmutados se utiliza señalización fuera de banda a través del DLCI 0.

Características de los circuitos

Las características de los circuitos depende del servicio contratado. Las velocidades de acceso típicas están entre 64kbps y 2Mbps -aunque hay mayores-. Además en el contrato se fija un ancho de banda garantizado para el circuito virtual (CIR: *Commited Information Rate*) y un margen de tolerancia que se permite rebasar (EIR: *Excess Information Rate*) en caso de que haya ancho de banda disponible.
El usuario puede enviar hasta CIR+EIR bps, pero al exceder el CIR, los demás paquetes serán enviados en modo *Best Effort* y se marcarán con un bit llamado DE (*Discard Elegibility*) que indica que dichos paquetes se pueden descartar en caso de congestión en un nodo. Si se supera la cantidad CIR+EIR en un intervalo, las tramas se descartan directamente.

En realidad una de las ventajas de Frame Relay es que las limitaciones se hacen en base a velocidades medias, adaptándose muy bien al tráfico en ráfagas. De esta forma los valores CIR y EIR surgen de dividir por un tiempo prefijado “Tc” los valores Bc (*Committed Burst Size*) y Be (*Excess Burst Size*). Al basarse en velocidades medias se puede usar una mayor velocidad de la contratada en momentos puntuales (incluso por encima de CIR+EIR) siempre que la media en el intervalo Tc no supere la cantidad estipulada. Como habitualmente Tc es un segundo CIR=Bc y EIR=Be.

El contrato del CIR y EIR puede ser asimétrico y se establece de forma independiente para cada PVC.
En una configuración típica, un "nodo central" puede tener un enlace sobre el que se configuran varios PVCs hacia los "nodos secundarios", o sucursales. En el "nodo central" el enlace físico podría ser, por ejemplo, de 1 Mb/s, y cada PVC disponer de un CIR de 64 kb/s. Esto significa que la velocidad media garantizada de transmisión entre el nodo central y los nodos secundarios debe ser 64 kb/s (CIR), aunque la velocidad física del enlace central será de 1 Mb/s.

Se tarifica por cuota fija en función de la velocidad de acceso, de la distancia y del CIR/EIR del circuito contratado.
En España la red de Frame-Relay de Telefónica se llama Red Uno y permite establecer conexiones internacionales.

Tramas Frame-Relay

El tamaño de trama es variable. El máximo depende de las implementaciones (hasta 8kb). Una trama contiene: un indicador de comienzo de trama que facilita la sincronización (*Flag*), una cabecera (*Header*), los datos a transmitir (*Information*), y los campos FCS (*Frame Check Sequence Field*) -un CRC básico- y un nuevo Flag de sincronización que indica final de trama.
Dentro de la cabecera (2 o 4 bytes) existen muchos formatos diferentes que presentan los siguientes campos:

- DLCI destino: Identificador de 10 bits del destino de la trama.
- DLCI remitente: Identifica la conexión virtual de procedencia. Este valor DLCI es local y se modifica en cada salto.
- 2 bits AFE (*Address Field Extension*): Indica que la cabecera está utilizando direcciones más largas de lo habitual.
- bit FECN (*Forward Explicit Congestion Notification*): Este bit indica que el nodo que envía la trama ha detectado congestión en la red en el mismo sentido que va la trama.
- bit BECN (*Backward Explicit Congestion Notification*): Este bit indica que el nodo que envía la trama ha detectado congestión en la red en el sentido opuesto al que va la trama.
- bit DE (*Discard Eligibility Indicator*): Este bit indica que la trama es descartable en caso de congestión. Todas las tramas que exceden el CIR contratado, son marcadas como "DE".
- bit(s) EA (*Extension Bit*): Indica(n) si la cabecera es de 2 o 4 bytes.

Protocolos auxiliares

Aunque Frame-Relay aparece ante otros protocolos, por ejemplo IP, como un protocolo de enlace (N2), para gestionar los circuitos virtuales utiliza a su vez un protocolo de enlace llamado LAPF, que se encarga de gestionar los bits FECN, BECN y DE.

Por otra parte LMI (*Local Management Interface*) es un protocolo que se implementa de forma opcional, pero habitual, en las instalaciones de Frame-Relay y permite el intercambio de información entre equipos de clientes y equipos del prestador de servicios mediante el uso de tramas especiales de administración, que disponen de números de DLCI reservados para estos fines.
Esta información de administración incluye:

- Indicación de que la interfaz está activa (*keep alive*).
- Información de los DLCIs definidos en la interfaz.
- Información sobre el estado de cada circuito virtual, por ejemplo, si está congestionado o no.

6.6. ATM (*Asynchronous Transfer Mode*)

Introducción

ATM es una arquitectura de red de cuatro capas diseñada para presentar circuitos virtuales que permitan integrar voz, datos y vídeo (red multimedia). Surgió como respuesta a la necesidad de tener una red multiservicio que pudiera manejar velocidades muy dispares, con altos picos de transmisión y dispositivos de diferentes velocidades. Funciona tanto en medios ópticos como eléctricos.
A veces se llama RDSI de banda ancha y en cierto sentido es una evolución de Frame Relay.

Los protocolos de ATM están estandarizados por la ITU-T, con especial contribución del "ATM Forum[41]" y si bien pueden ser utilizados en LANs, se usan principalmente en las redes de espinazo (*backbone*) de los proveedores de servicios públicos. Sin embargo parece tener poco futuro debido a la aparición de GigaEthernet y de PoS (*Packet Over SONet/SDH*).

Algunas de las ventajas de ATM frente a otras tecnologías son:

- Alto rendimiento, realizando las operaciones de conmutación a nivel de hardware.
- Ancho de banda dinámico, para permitir el manejo de picos de tráfico.
- Soporte de "clase de servicio" para aplicaciones multimedia (QoS).
- Escalabilidad en velocidades y tamaños de redes. ATM puede utilizar desde redes E1/T1 hasta redes SONet/SDH soportando velocidades que oscilan entre 1.5 Mb/s y 2 Gb/s.
- Arquitectura común para las redes de LAN y WAN.
- Permite establecer conexiones punto a punto o punto a multipunto unidireccional. No soporta multicast, pero puede ser simulado.

Permite establecer circuitos virtuales permanentes (PVC) -configurados estáticamente- o conmutados (SVC) mediante señalización Q2931 a través de los circuitos reservados VPI 0 VCI 5.
Siguiendo el estándar OSI NSAP, las direcciones ATM son de 20 bytes: 13 bytes identifican la red, 6 el equipo y el último la entidad en el equipo.
El primer byte marca la utilización de uno de los 3 formatos posibles de dirección. Uno de los formatos incluye direcciones E.164 (tradicionales de telefonía internacional)[42] codificadas en los 20 bytes.

Permite contratar características diversas de un circuito virtual:

- Ancho de banda máximo
- Ancho de banda mínimo garantizado
- Margen de tolerancia
- Ancho de banda asimétrico
- Perfil horario
- Prioridades

Además define cuatro compromisos distintos de calidad (QoS):

- **CBR (*Constant Bit Rate*)**: Garantiza capacidad constante reservada en todo el trayecto.
- **VBR (*Variable Bit Rate*)**: Para tráfico a ráfagas. Se fija un caudal medio garantizado.
- **ABR (*Available Bit Rate*)**: Fija un mínimo garantizado y un máximo orientativo. Informa de congestión.
- **UBR (*Unspecified Bit Rate*)**: Sin garantías.

41 Organización voluntaria internacional, formada por fabricantes, prestadores de servicio, organizaciones de investigación y usuarios finales.
42 Por ejemplo 34961234567@timofonica.com, que se correspondería con el número 34961234567 en la RTC.

Los nodos de la red se llaman conmutadores ATM y los terminales equipos (*hosts*). De forma similar al modelo OSI, ATM también está diseñada en un modelo de capas. En el caso de ATM, el modelo de capas puede verse en dos "planos", uno de gestión con una sola capa y otro de transmisión dividido en 4 capas:

- **Física**. Dividida en:
  - PMD (*Physical Media Dependent*) Equivale a la física de OSI
  - TC (Transmisión Convergente) Equivale a enlace OSI
- **ATM**. Realiza tareas de señalización, transporte y control de congestión. Está a caballo entre las capas de enlace y de red de OSI.
  - El algoritmo de encaminamiento dinámico entre conmutadores se llama P-NNI y es parecido al OSPF.
- **AAL (*ATM Adaptación Layer*)**. Equivale a la de transporte OSI y se divide en:
  - SAR (*Segmentation and Reassembly*) Se encarga de fragmentar paquetes en celdas y reensamblarlos.
  - CS (*Convergence Sublayer*) Ofrece los tipos de servicio
- **Aplicación**. No se define. Se deja total libertad. En realidad hay muy pocas aplicaciones diseñadas para ATM. Se suele utilizar para transportar otros protocolos de nivel 3 (como IP).

Funcionamiento

No envía acuse de recibo. Los paquetes -llamados celdas- son de longitud fija y tienen 53bytes (5 de cabecera y 48 de datos). Esto permite dos cosas: que una celda de mayor prioridad no espere mucho tiempo porque hay otra de menos prioridad enviándose (y no se puede suspender el envío); y también reduce la complejidad del conmutador y puede ser más rápido. El inconveniente es una sobrecarga (*overhead*) de 5/53 (casi un 10%).

De los 5 bytes de la cabecera hay que destacar los campos VPI (*Virtual Path Identifier*) y VCI (*Virtual Channel Identification*) que son los campos que utilizan los conmutadores para saber por qué puerto hay que enviar la celda. Estos campos tienen sentido local al conmutador y pueden cambiarse al pasar de un conmutador a otro.
Hay un bit (CLP *Cell Loss Priority*) para identificar si la celda es más o menos susceptible de ser descartada en momentos de congestión y un campo HEC (*Header Error Control*) que es un *checksum* de cabecera.
La sincronización entre equipos para delimitar donde empieza cada celda se hace calculando los *checksums* de cabecera (HEC) hasta encontrar una secuencia de bytes que cumple la función del *checksum*.

Se definen dos tipos de interfaz:

- **UNI (*User-Network Interface*)**: entre el equipo de usuario y el conmutador. Normalmente versión 3.0 o 3.1.
- **NNI (*Network-Network Interace*)**: entre dos conmutadores.

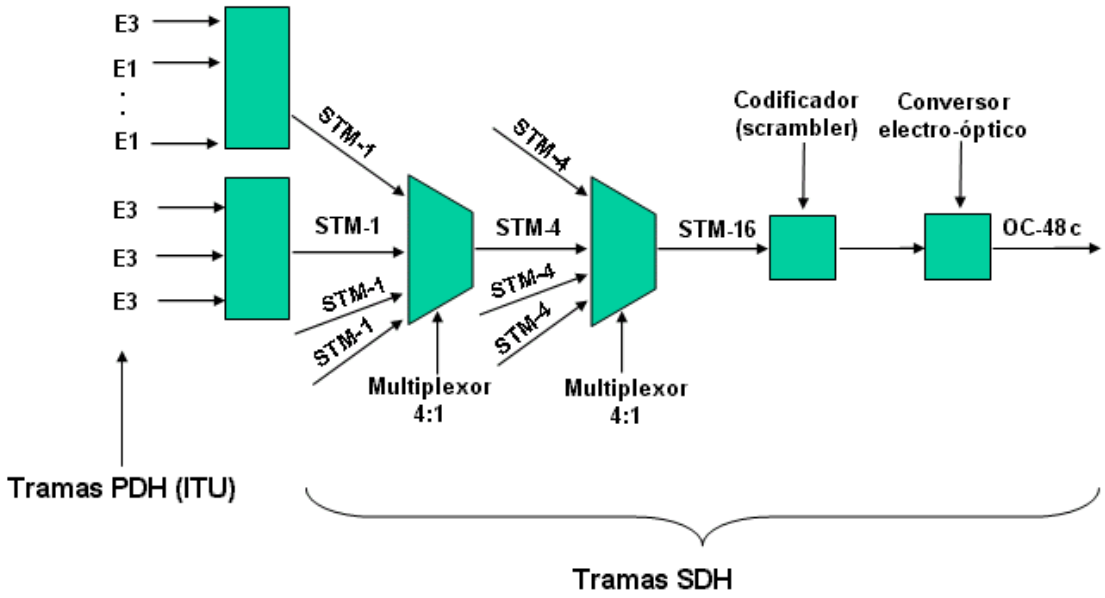
6.7. Redes de fibra SONet / SDH

Las redes SONet (*Synchronous Optical NETworking*) y SDH (*Synchronous Digital Hierarchy*), son protocolos de nivel 1 basados en multiplexado de tiempo (TDM: *Time Division Multiplexing*) para transferencia de datos sobre fibra óptica usando LEDs o ILDs. Están estandarizados por el ANSI y el ITU-T respectivamente y son compatibles, aunque una se utiliza sobre T3 y la otra sobre E3 -o sobre fibra-.
Ofrecen circuitos permanentes full-dúplex y se comporta como un medio físico de transmisión de bits. Se utilizan principalmente como nivel físico de ATM, PoS o 10GbE (Ethernet a 10 Gb).

Las tramas básicas de transmisión son:

SONet Eléctrico – STS (*Synchronous Transfer Signal*)	**SONet Óptico – OC (*Optical Carrier*)**	**SDH Óptico – STM (*Synchronous Transport Module*)**	**Velocidad (Mb/s)**
STS-1	OC-1	STM-0	51,84
STS-3	OC-3	STM-1	155,52
STS-12	OC-12	STM-4	622,08
STS-48	OC-48	STM-16	2.488,32
STS-192	OC-192	STM-64	9.953,28

De esta manera se garantiza la compatibilidad entre ambas si se utilizan múltiplos de 3. Cada trama STM está compuesta por 4 de las anteriores. Una trama STM4 lleva 4 tramas STM-1. Una trama STM-1 puede llevar 3 E3 o 1 E3 y 32 E1, etc.



Una red SDH está formada por repetidores, multiplexores y conmutadores interconectados por fibra óptica habitualmente con topología de doble anillo para mantener redundancia (como la de FDDI). El tiempo de reacción a un corte del anillo es de 50ms.
Los multiplexores se llaman ADM (*Add-Drop Multiplexor*) y se encargan de extraer e inyectar tramas de menor nivel en otras de mayor nivel. El tramo que recorre un circuito completo se llama ruta, el que comunica dos equipos sección y el que une dos ADMs contiguos línea.

6.8. PoS (*Packet Over SONet/SDH*)

Implementa PPP (*Point-to-Point Protocol*) directamente sobre SONet/SDH. Es una alternativa a ATM sobre SONet/SDH para redes IP[43] que reduce la sobrecarga (*overhead*) y la complejidad de ATM. Además, suprime la necesidad de conmutadores ATM y conecta los encaminadores directamente a los ADM de SONet/SDH. Sin embargo, al suprimir la capa ATM, no se puede establecer circuitos virtuales, solo redes de datagramas (p.e. IP).
La multiplexación se ha de hacer a nivel de circuitos SONet/SDH.

Si se dispone de un cableado de fibra entre dos encaminadores con interfaz PoS, se puede suprimir los equipos SDH y conectarlos directamente. Esto permite crear redes IP sobre PoS pero sin electrónica añadida.

6.9. GSM (*Global System for Mobile comunications*)

GSM es un protocolo de comunicaciones telefónicas móviles que permite formar circuito reales digitales por radioenlace. Se considera la segunda generación de sistemas de telefonía móvil, siendo la primera analógica y la tercera UMTS. Por tanto forma parte de la RTC.
El espacio geográfico es dividido en células con una estación base en su interior y un grupo de frecuencias propio. El usuario se comunica con la estación base que corresponde a la célula donde se encuentra. Si se desplaza a otra célula contigua cambia automáticamente de estación base (*roaming*).
Dos células contiguas no pueden utilizar el mismo grupo de frecuencias por lo que, siendo la estructura como la de un panal, se necesitan 7 grupos de frecuencias diferentes.
El rango de frecuencias de una célula se divide en canales de 200 KHz de anchura. Unos se utilizan para comunicación ascendente (hacia la estación base) y otros para la descendente (desde la base).
Cada canal soporta 8 circuitos de voz o datos multiplexados en el tiempo. La voz se transmite digitalizada y comprimida a 13,6 Kbps. Para datos sólo se puede transmitir a 9,6 kbps.
El número de usuarios simultáneos que soporta una célula está limitado por el número de canales que puede utilizar, que es fijo. Para aumentar este número hay que dividir la célula en otras más pequeñas poniendo más estaciones base con menos alcance (menos potencia). El teléfono adapta su potencia en función de la proximidad de la estación base.

En Europa se utiliza en dos bandas de frecuencia, entorno a 900 MHz y a 1800 MHz (GSM 900 y GSM 1800), mientras que en EE.UU. se utiliza en la banda de 1900 MHz (GSM 1900) y en el Sureste Asiático y Japón a 850 MHz (GSM 850).

6.10. GPRS (*General Packet Radio Service*)

GPRS es un protocolo de conmutación de paquetes sobre GSM, es decir para transmisión de datos sobre redes de móviles. Su velocidad máxima teórica es de 171,2 kbps, pero en la práctica es menor. A los dispositivos móviles que utilizan esta tecnología se les conoce como de generación 2.5 (2.5G).

6.11. UMTS (*Universal Mobile Telecommunications System*)

Red digital por microondas para teléfonos móviles. Se considera la tercera generación de sistemas de telefonía móvil, siendo la primera analógica y la segunda GSM. Por tanto forma parte de la RTC.
El estándar de ITU IMT-2000 (*International Mobile Telecommunications*-2000) garantiza que todas las redes 3G sean compatibles unas con otras.
Los servicios que ofrecen las tecnologías 3G son básicamente: acceso a Internet, servicios de banda ancha, *roaming* internacional e interoperatividad, con una velocidad máxima de 2 Mbit/s en condiciones óptimas.

43 En caso de querer enviarse tráfico no IP, debe encapsularse sobre IP.

6.12. Redes de satélites

Se utilizan para cubrir grandes distancias y para llegar a sitios donde no hay infraestructura de comunicaciones.
Utilizan frecuencias del orden de GHz y rangos distintos para comunicaciones ascendentes y descendentes.
Los satélites se comportan como repetidores con velocidades típicas de entre 300 kbps y 2 Mbps y pueden dirigir el haz a una zona concreta (250 km) pero todas las estaciones de esa zona recibirán la señal, por lo que los datos deben ir cifrados.

Hay satélites geoestacionarios que permanecen fijos en el cielo y permiten utilizar antenas parabólicas direccionales y fijas. Están a 36000 Kms de altura y eso hace que las comunicaciones tengan una alta latencia.
Hay proyectos de satélites de baja órbita (menor altura y por tanto menor latencia) pero al no estar fijos en el cielo aparecen y desaparecen, por lo que hay que crear una malla de satélites en el cielo para que en un punto de la tierra siempre haya alguno a la vista (como hace por ejemplo GPS).

Los problemas técnicos más importantes son debidos a que es un medio de multi-difusión y al control de acceso al medio (MAC) debido a que las estaciones no se ven entre sí y a las largas distancias del medio.

Dado que los equipos de emisión son caros, se pueden plantear para recibir información, utilizando las líneas telefónicas para las subidas de datos, creando una conexión altamente asimétrica.

6.13. MPLS (*Multi-Protocol Label Switching*)

Más que un protocolo de red es una técnica utilizada por los encaminadores del núcleo de Internet. Dado que el análisis de destino de un paquete IP es muy costoso, cuando la tabla de encaminamiento es muy grande, es más sencillo y rápido comparar etiquetas como hace ATM (con los campos VPI VCI). La etiqueta, como en ATM sólo tiene sentido local y cada encaminador la va cambiando.
Para agilizar el proceso, los llamados "*edge routers*" (encaminadores del borde de Internet) añaden a los paquetes, una vez resuelto su destino, una cabecera especial con una etiqueta identificando el flujo al que pertenece. Los siguientes encaminadores sólo tienen que fijarse en esa etiqueta. A la salida del núcleo, el último "*edge router*" elimina la cabecera MPLS.

7. MÉTODOS DE ACCESO A REDES

7.1. Introducción

Existen métodos diseñados para acceder a las redes de comunicaciones que se caracterizan por comunicar equipos de manera jerárquica: generalmente un equipo "usuario" o "cliente" y un equipo "proveedor", "servidor" o "central" que depende de los llamados "proveedores de acceso" cuyo servicios suponen un coste para el usuario. En algunos textos se les llama "Redes de Acceso", aunque en este se prefiere "Métodos de Acceso a Redes" por coherencia con la definición dada de redes de comunicaciones[44].

7.2. Módems

Un módem es un dispositivo que sirve para modular y demodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora.
Su uso más común y conocido es para realizar transmisiones de datos por vía telefónica ya que mientras las computadoras procesan datos de forma digital las líneas telefónicas de la RTB sólo transmiten señales analógicas.
Además de los módems telefónicos existen otros módems como los módems xDSL o módems utilizados para transmisiones radiofónicas y de televisión.

Los métodos de modulación y otras características de los módems telefónicos están estandarizados por el UIT-T (el antiguo CCITT) en la serie de Recomendaciones "V" que determinan la velocidad de transmisión. Así podemos encontrar desde el V.32. (transmisión a 9.600 bps) hasta el V.92 (transmisión a 56'6 kbps con compresión de datos y llamada en espera).

Las características que se pueden modificar de la señal portadora son:

- Amplitud, dando lugar a una modulación de amplitud (AM/ASK).
- Frecuencia, dando lugar a una modulación de frecuencia (FM/FSK).
- Fase, dando lugar a una modulación de fase (PM/PSK)

También es posible una combinación de modulaciones o modulaciones más complejas como la Modulación de amplitud en cuadratura.

7.3. xDSL

Introducción

La tecnología xDSL (*Digital Subscriber Line*: Línea de Abonado Digital) es una evolución de los módems telefónicos que utilizan un espectro de frecuencias situado por encima de la banda vocal (300 - 3.400 Hz) e incluso por encima de los 25 KHz ocupados en las líneas RDSI, y permiten alcanzar velocidades mucho mayores que un módem telefónico convencional, al mismo tiempo que se puede establecer comunicaciones telefónicas.
Por tanto permite utilizar para la transmisión de datos la infraestructura existente de RTB de manera transparente para su uso habitual, es decir sin interferir en el uso telefónico de la línea.
En el nivel de enlace utiliza celdas ATM. O dicho de otra manera, es un nivel físico para ATM. Por ello muchos proveedores pueden ofrecer servicios xDSL sin disponer de un bucle de abonado propio. En vez de ello contratan con la compañía proveedora de la RTB para que envíe el circuito ATM a sus conmutadores.

Aún así no se puede usar en cualquier cable de teléfono. Básicamente tiene que cumplir dos condiciones:

- que el cable esté en buen estado y no sea muy viejo, lo que impide su utilización en zonas y países con un mal mantenimiento de líneas telefónicas
- que el terminal (el módem) no esté a más de una distancia determinada de una central digital. En general se da por buena una distancia máxima de 5,5 Km, con una distancia óptima inferior a 2 Km.

Esto hace que xDSL resulte económico en países con una infraestructura adecuada e inviable en zonas con malas infraestructuras

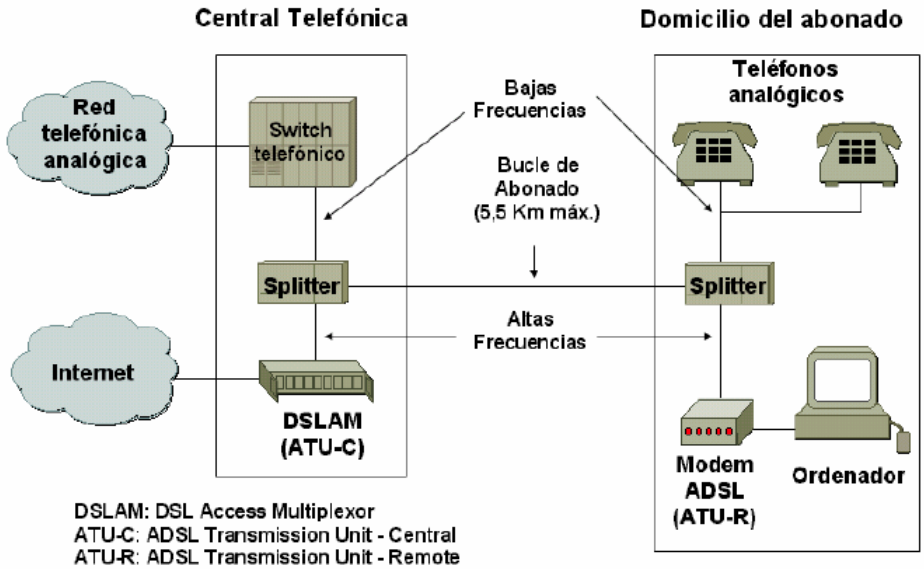
44 Conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (**no jerárquica** -*master/slave*-).

La voz humana usa normalmente frecuencias entre 0 y 4 Khz[45]. El sistema xDSL aprovecha la capacidad de la línea para transmitir datos en una banda de frecuencia más alta que la que se utiliza para transmitir voz. Así se puede transmitir voz y datos a la vez. Para evitar que se oiga un ruido de fondo en el teléfono se añaden filtros (*splitters*) a la conexión del teléfono. Al llegar a la central, los datos viajan por una red de datos separada de la de voz.

La banda de frecuencia utilizada para la transmisión de datos se divide en tres canales: subida, bajada y control. Es decir, en total se utilizan cuatro canales: el de voz y los tres de transmisión de datos.
La técnica de modulación más utilizada es la DMT (*Discrete Multi Tone*) estandarizada por el ITU-T. Consiste en dividir la gama de frecuencias en 256 subcanales denominados "bins" de 4,3125 KHz de anchura, que xDSL maneja de forma independiente. Esto permite que si hay ruido en una frecuencia se deje de utilizar solo un bin pero se siga aprovechando el resto. La capacidad exacta de datos por canal depende de la modulación.
Los 6 primeros se reservan para la voz y el RDSI (25,875 KHz), los siguientes se utilizan para subida (según la capacidad de subida contratada) y los últimos para bajada.

Otra técnica disponible llamada CAP (*Carrierless Amplitude Phase*) utiliza una filosofía similar pero sin dividir los rangos ascendentes en bins, con lo que da menor rendimiento, aunque los equipos son más sencillos.

xDSL utiliza transmisión full-duplex síncrona sobre una línea dedicada punto a punto, conocida como bucle de abonado, entre el módem del abonado (ATU-R) y la central digital del proveedor (ATU-C). Normalmente la central ATU-C se conecta un conmutador ATM con aparatos conocidos como DSLAM (*Digital Subscriber Line Access Multiplexer*).



45 Por teléfono analógico se suelen transmitir entre 300 y 3400 Hz.

Variantes de xDSL

ADSL

La variante de xDSL utilizada en España es el ADSL o *Asymmetric Digital Subscriber Line* ("Línea de Abonado Digital Asimétrica"). Esto significa que la velocidad de subida es distinta de la velocidad de bajada.
Por ejemplo, un ADSL2 en España para la subida utiliza las frecuencias 25,875 Khz a 138 Khz y para la bajada de 138-1104Khz. El canal de control se sitúa entre ambos (utiliza un ancho de banda pequeño).

Actualmente se están implantando tecnologías ADSL2 y ADSL2+ cuya diferencia fundamental es la utilización de un mayor ancho de banda (hasta 2,2 MHz), lo que permite en el caso del ADSL2 dar mayores velocidades de carga y descarga y en el caso del ADSL2+ utilizar uno de los rangos para enviar una señal de televisión.

	ADSL (T1.413)	**ADSL2 (G.992.3/4)**	**ADSL2+ (G.992.5)**
Frecuencia Máx.	0,5 MHz	1,1 MHz	2,2 MHz
Velocidad Máx. Subida	1 Mbps	1 Mbps	1,2 Mbps
Velocidad Máx. Bajada	8 Mbps	12 Mbps	24 Mbps
Distancia Máx.	2 Km	2,5 Km	2,5 Km
Tiempo Sincronización	10-30s	3 s	3 s
Corrección de Errores	No	Sí	Sí

ADSL G.Lite

Permite prescindir del filtro en la vivienda a costa de suprimir frecuencias y utilizar una modulación más pobre, obteniendo peores rendimientos.

RADSL (*Rate Adaptative ADSL*)

Negocia dinámicamente frecuencias con el otro extremo para suprimir o recuperarlas en función de las fluctuaciones del ruido.

VDSL (Very high speed DSL)

Permite velocidades muy grandes pero a muy cortas distancias.

HDSL (*High Data-rate DSL*)

Consigue altas velocidades sobre varios pares telefónicos en paralelo.
No es útil en el hogar porque no hay varios pares instalados y además no reserva las frecuencias de la voz.
Se suele utilizar para enviar líneas E1 sobre dos pares de hilos telefónicos.

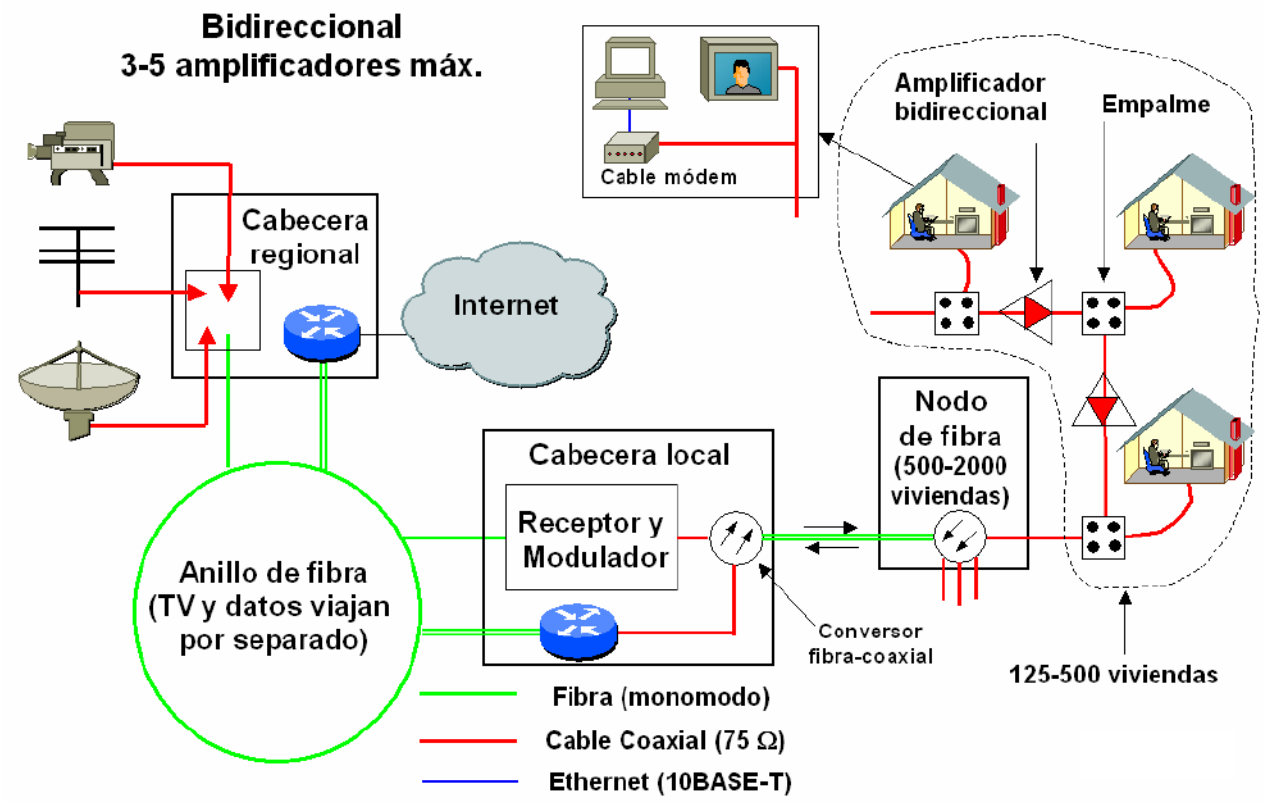
SDSL (*Symetric DSL*)

Similar a HDSL pero sobre un solo par de hilos.

7.4. CATV (Redes de TV por cable)

Las redes CATV surgen para distribuir la señal de TV a zonas donde no se recibían bien las ondas. Utilizaba cable coaxial de 75 ohmios y amplificadores cada ½ o 1 km. Los amplificadores degradaba la señal y se comportaban como válvulas que impedían señales ascendentes.
Las redes más modernas -entre ellas casi todas las europeas- son del tipo HFC (*Hibrid Fiber Coaxial*). Estas redes distribuyen la señal desde la cabecera -proveedor- hasta la manzana -residencias- por fibra y llegan a las viviendas por cable coaxial[46]. Tienen menos de 5 amplificadores y son de un tipo que permiten utilizar las frecuencias inferiores en sentido contrario (de subida), por lo que se pueden utilizar para transmisión bidireccional de datos.

En la cabecera de la red hay un equipo especial llamado CMTS (*Cable Modem Termination System*) y en las viviendas de los usuarios se instala un equipo llamado CM (*Cable Modem*). Normalmente, la compañía configura el cable módem para que no rebase un caudal contratado.



La transmisión de datos se hace modulada en un canal de TV reservado. Se utilizan frecuencias y modulaciones diferentes para las señales de subida y de bajada debido a la diferencia de relación señal/ruido de dichas frecuencias en el cable.
El medio de transmisión es asimétrico. Además es poco fiable, por lo que se utilizan códigos de corrección *Reed-Solomon* que suponen un 10% de sobrecarga.

Cada CM solo puede comunicarse con el CMTS que se comporta como un puente remoto. Todos los CMs de un segmento comparten el medio físico y tienen que compartir los canales de datos. Las emisiones del CMTS llegan a todos los CM del segmento, por lo que la información debe viajar cifrada.

Para competir por el canal ascendente hacia el CMTS se utiliza un protocolo basado en créditos. El canal ascendente se divide en intervalos de tiempo llamados “minislots”. El CMTS informa a los CM a través del canal descendente (junto con los datos) del mapa de asignación de minislots.

46 Según donde acabe la fibra: FTTN / FTTC / FTTB / FTTH (*Fiber to the Node / Curb / Building / Home*)

Hay tres tipos de minislots:

- **Asignados** a un CM en concreto para que envíe datos. Los demás deben permanecer callados.
- **De contención**, en los cuales los CM compiten por los minislots con un protocolo de tipo Aloha. Si hay colisión los CM no se enteran directamente, pero la detecta el CMTS y les informa.
- **De mantenimiento**. Para la inicialización de CM y el mantenimiento y sincronización de los relojes y la potencia de los CM. Debido a la distancia, es muy importante que se adapten los relojes y la potencia para que todos lleguen con la misma intensidad al CMTS y éste pueda detectar las colisiones.

7.5. LMDS (*Local Multipoint Distribution System*)

LMDS es una tecnología inalámbrica de red que se utiliza para transmitir voz, datos y servicios de vídeo en la banda de frecuencias superiores a 20 GHz (microondas), según licencias. Se diseñó para reemplazar las redes CATV con una mayor velocidad de despliegue. Sin embargo no llegó a cuajar en el mercado.
Para el canal descendente se utiliza emisión multidifusión omnidireccional y para el ascendente se puede utilizar telefonía o emisión dirigida con parabólica.
Su alcance se ve afectado por la lluvia y necesita visión directa. Entre 3 y 9kms.
Su despliegue puede ser mucho más rápido que otro tipo de redes, pero el retorno telefónico es lento y el de antena parabólica caro.

8. REDES PRIVADAS VIRTUALES

8.1. Introducción

Se entiende por VPN (*Virtual Private Network*) la construcción de una red privada (*intranet*) sobre otra red, generalmente pública como Internet, de manera que se utiliza la red inicial como un enlace de nivel 2 para montar sobre él una red privada de nivel 3 (transportando protocolos de nivel 3 como IP, NetBEUI, IPX, SNA…).

Para conseguir esta abstracción se basa en el concepto de túnel que consiste en un enlace punto a punto virtual entre dos extremos construido sobre una red compleja, de manera que los dos extremos se comportan a nivel lógico como si estuvieran unidos directamente por un enlace punto a punto.
Los paquetes se encapsulan en un extremo del túnel dentro de otros paquetes para cruzar la red. En el otro extremo se desempaquetan los datos que pueden haber viajado comprimidos y cifrados (para que la red sea "privada").

Desde el punto de vista de la seguridad, los protocolos que se utilizan para montar VPNs ofrecen:

- **Autenticidad de los extremos.** Cuando se utilizan certificados, se garantiza que tanto el emisor como el receptor son quienes dicen ser.
- **Cifrado de datos**. Permite que no puedan ser comprendidos por extraños que los pudiera interceptar.
- **Integridad de los datos**. Asegura que los datos no puedan ser alterados en algún punto del recorrido sin que el receptor lo detecte.
- **No repudio**. Cuando un mensaje va firmado el emisor no puede negar su emisión.

Se puede utilizar VPN sobre una red pública para realizar dos tipos básicos de conexión:

- **Acceso remoto**. También llamada *Remote Access VPN*, *client-gateway* o usuario-red. Permite unir virtualmente un equipo remoto a una red.
- **Interconexión de redes**. También llamada *Site to Site VPN*, *Router to Router VPN*, *gateway-gateway* o red-red. Permite unir virtualmente dos redes para crear una única red.

De manera similar, se puede utilizar VPN sobre una red privada para acceder a una subred protegida y/u oculta de dos maneras básicas:

- **Acceso privado**. Permite controlar el acceso a la subred oculta y cifrar el tráfico hacia dicha red.
- **Interconexión de redes privadas**. Permite unir dos subredes protegidas y/u ocultas cifrando el tráfico entre ellas.

Para poder configurar cualquier VPN hace falta al menos un servidor de VPN por cada red que forma parte de la VPN, y un cliente de VPN por cada cliente de acceso remoto que se conecta a la misma. El servidor VPN es el encargado de autenticar la conexión (o delegar dicha función) y permitir la comunicación entre la red y el otro extremo de la VPN.

TAP/TUN

Para la realización de VPNs se utiliza habitualmente dos controladores virtuales de red llamados TAP y TUN. TAP (de "*network tap*") simula un dispositivo de red de nivel 2 y opera con paquetes Ethernet. TUN (de "*network TUNnel*") simula un dispsitivo de red de nivel 3 y opera con paquetes IP. TAP se utiliza para crear el puente de red y TUN para encaminar los paquetes por dicho puente.

VPN de acceso remoto

En una conexión VPN de acceso remoto, el cliente, a través del protocolo IPCP (*IP Control Protocol*) de PPP (*Point-to-Point Protocol*) recibe del servidor VPN los parámetros de la configuración IP de su conexión virtual, incluyendo dirección IP, máscara de red y direcciones IP de los servidores DNS y WINS de la intranet.
Después de crear el túnel, el cliente pasa a tener 2 interfaces de red y 2 direcciones IP:

- La interfaz con la que conecta a la red principal (generalmente Internet) y que utiliza para conectar con el servidor VPN.
- La interfaz virtual PPP con la configuración IP que le ha dado el servidor de túneles y que establece una ubicación virtual dentro de la red destino.

Además la tabla de rutas se modifica para que el tráfico hacia la red privada se envíe por el túnel VPN y opcionalmente también el tráfico hacia Internet -lo que permite usar los filtros y servidores de la red privada, normalmente a cambio de reducir el rendimiento-.
De la misma manera el servidor VPN se encarga de recibir el tráfico destinado al equipo remoto y reenviárselo.

Antes de las VPN para conseguir un acceso remoto a una red se utilizaban sistemas RAS (*Remote Access Service*)[47] mediante PoPs (*Point of Presence*) de forma parecida al de las conexiones que ofrecían los proveedores de Internet (ISPs) a través de módems telefónicos. De esta forma un cliente llama mediante módem telefónico al servidor RAS de su organización, se valida mediante un servidor RADIUS o TACACS y establece la conexión. Opcionalmente el servidor RAS puede configurarse para devolver la llamada, cargando el gasto de la misma a la organización.

Las principales ventajas de la conexión VPN frente a la conexión mediante RAS son:
- Para clientes de acceso remoto vía módem supone una reducción del coste de las llamadas, ya que conecta a un proveedor local de Internet y no a un servidor RAS de la organización remota.
- Reducción del coste de los equipos y líneas de entrada (RDSI) que representa el RAS.
- Escalabilidad. Es mucho más fácil y barato de añadir servidores VPN que líneas de acceso y equipos de RAS.
- Permite acceso a mayor velocidad que la de un módem telefónico mediante el uso de cable-modems, xDSL u otras redes.

Otra diferencia es que al usar RAS se dispone únicamente de una sola interfaz de red, la del cliente RAS o PPP.

VPN de Interconexión de redes

La conexión de redes a través de Internet es una alternativa a las líneas alquiladas que permite reducir costes, ya que suele ser más barato conectar las dos redes a Internet que alquilar una línea para unirlas, sobre todo si están muy alejadas. Sin embargo esta alternativa tiene dos grandes inconvenientes, la falta de seguridad de Internet y el rendimiento, que es mucho menor que el de una línea dedicada. Para suplir el primero de ellos se utilizan las VPNs de interconexión de redes que ofrece seguridad en el túnel entre servidores VPN (no en las conexiones locales equipo-servidor).

Otras ventajas:
- Toda la configuración necesaria se realiza en los encaminadores o servidores VPN, de manera transparente al usuario.
- Permite transportar otros protocolos diferentes a IP que no pueden ser transportados sobre Internet si no es con túneles (IPX, Appletalk , SNA, NetBEUI, etc).
- Se puede introducir compresión de datos para aprovechar mejor los enlaces.
- Se puede utilizar el mismo rango -público o privado- de direcciones IP en todas las redes.

8.2. Autenticación de usuario

La autenticación del usuario se puede realizar mediante un usuario y contraseña, certificados digitales o tarjetas físicas (*tokens*) tanto contra el propio servidor VPN como utilizando otro servidor de autenticación, como servidores RADIUS, TACACS+ , LDAP (mediante NTLM) o Kerberos (en territorios sobre GNU/Linux).

Protocolos

Para realizar la autenticación se pueden usar distintos protocolos como:
- PAP (*Password Authentication Protocol*). La contraseña viaja en claro por la red.
- CHAP (*Challenger Authentication Protocol*).
- MS-CHAP (*Microsoft CHAP*) y MS-CHAP v2.
- Familia EAP (*Extensible Authentication Protocol*).
- SPAP (*Shiva Password Authentication Protocol*).
- Acceso sin necesidad de autenticación.

47 Actualmente el servicio de Windows que gestiona las VPNs se sigue llamando RRAS (*Routing and RAS*).

Aunque el protocolo Kerberos ha sido adoptado por Microsoft para la autenticación en el directorio activo, todavía utiliza NTLM en determinadas circunstancias:

- Si el cliente se autentica usando una dirección IP.
- Si el cliente se autentica en un servidor de otro bosque del directorio activo o no pertenece a ningún dominio o no existe ningún dominio.
- Si un cortafuegos corta los puertos necesarios para usar Kerberos.

8.3. Protocolos para la realización de VPNs

Protocolo PPTP (*Point to Point Tunneling Protocol*)

El protocolo PPTP fue desarrollado por el "PPTP Forum[48]" para encapsular otros protocolos, como IPX o NetBEUI, a través de Internet y se propuso al IETF en la RFC 2637. Así su función es encapsular tramas PPP[49] sobre IP.
Permite conexiones usuario-red y red-red con compresión y cifrado, pero no es muy seguro. Los servidores de Microsoft permiten usar MPPE (*Ms Point-to-Point Encryption*) para cifrar las conexiones VPN establecidas con PPTP.
No necesita infraestructura PKI (*Public Key Infraestructure*) ya que autentica con los mecanismos de PPP (usuario y contraseña) en base a EAP, MS-CHAP, MS-CHAPv2, SPAP y PAP.
Es multiprotocolo, permite NAT (*Network Translation Protocol*) y multidifusión.

L2TP sobre IPSec

El protocolo L2TP es una combinación de PPTP y L2F (protocolo propietario de Cisco). Utiliza UDP a través del puerto 1701 con dos tipos de paquetes: de transporte de tramas PPP y de control (creación, destrucción y mantenimiento del túnel). L2TP se encarga de realizar la autenticación de usuario, la asignación de direcciones y el encapsulado de tramas que pueden ser cifradas y comprimidas.
Permite encapsular tramas de diferentes protocolos sobre IP, X.25, Frame Relay o ATM... aunque en el caso de las VPNs se encapsulan los paquetes L2TP sobre paquetes IPSec, obteniéndose un sistema seguro de VPN multiprotocolo que permite NAT y multidifusión, tanto para conexiones usuario-red como conexiones red-red.
En el caso de conexiones VPN de acceso remoto, IPSec se utiliza en modo transporte.
En el caso de conexiones entre redes se utiliza IPSec en modo túnel.

Algunos servidores permiten usar IPSec sobre TCP o UDP (normalmente por el puerto 10000) para poder traspasar cortafuegos y servidores NAT.

48 En este foro participaron Microsoft, 3Com, Us Robotics entre otros.
49 Las tramas PPP a su vez encapsulan tramas de cualquier paquete de nivel 3.

9. SEGURIDAD EN REDES

9.1. Introducción

Criptología y esteganografía

La criptografía (literalmente "escritura oculta") es la disciplina que se ocupa del conjunto de técnicas para cifrar y descifrar información haciendo posible el intercambio de mensajes de manera confidencial, es decir de manera que sólo puedan ser leídos por aquellos a quienes van dirigidos.
El criptoanálisis es la disciplina que se ocupa del conjunto de técnicas para descifrar mensajes en ausencia de las claves ("romper el cifrado").
La criptología es la disciplina que engloba tanto la criptografía como el criptoanálisis.

La esteganografía es la disciplina que se ocupa del conjunto de técnicas que permiten el ocultamiento de mensajes dentro de otros, llamados portadores, de modo que no se perciba su existencia. En informática probablemente el sistema esteganográfico más utilizado sea el de ocultar mensajes en imágenes a nivel binario, alterando los bits de menor peso de determinados píxeles de la imagen e insertando en ellos el mensaje. Esta técnica hace indistinguible al ojo humano la imagen original de la alterada. Como además los mensajes se guardan cifrados en píxeles determinados por una clave no es posible saber si una imagen dada lleva un mensaje oculto o no.

Un ejemplo:

> Dos presos, Ana y Bob, planean fugarse y para organizarlo necesitan intercambiar mensajes. La única manera de enviar mensajes es solicitándole a la guardiana Eva que haga de portadora. Si Ana le da a Eva un mensaje para Bob que dice "Nos fugamos mañana a las 12" no es muy probable que la fuga tenga éxito. Ana puede utilizar la criptografía para enviar entonces el siguiente mensaje "gdtrhfuwjeldikarstyivh", pero Eva sospechará que algo ocurre, aunque no sepa qué. Por último Ana puede utilizar la esteganografía para enviar un mensaje en apariencia normal que oculte el mensaje real para Bob. Este mensaje podría ser, por ejemplo, un poema acróstico[50]. Para mayor seguridad Ana podría enviar un mensaje cifrado oculto mediante esteganografía.

En este capítulo nos ocuparemos solo de criptografía y sistemas de seguridad relacionados en redes informáticas.

Criptografía simétrica

La criptografía simétrica utiliza una clave para alterar un mensaje -"cifrado"- de manera que sea necesaria esa misma clave para recuperar el mensaje original -"descifrado"-. La criptografía de clave simétrica es la más antigua, la más sencilla (y por tanto la más rápida y eficiente) y la más utilizada. Los primeros sistemas se basaban simplemente en la trasposición o sustitución de las letras del alfabeto, desde la *scitala* espartana (cuya clave era la vara o "scitala"), el atbash utilizado por los hebreos (la trasposición se hace con el alfabeto invertido) o el método atribuido a Julio César y conocido como "cifrado del César" (la trasposición se hace con el alfabeto movido tres posiciones, la clave sería 3)[51].
Los algoritmos informáticos se basan principalmente en la trasposición de bloques[52] de bits en base a claves binarias.

50 Un acróstico es una composición poética en el que las letras iniciales, medias o finales de cada verso, leídas en sentido vertical, forman un vocablo o una locución. El acróstico más conocido de la lengua española está constituido por los versos que conforman el Prólogo de La Celestina (Fernando de Rojas, 1497), en cuyas octavas se puede leer: "El bachiller Fernando de Rojas acabó la comedia de Calisto y Melibea y fue nacido en la Puebla de Montalván".

51 Otro sistema de claves, por ejemplo "JULIOCESAR" (sin letras repetidas) nos daría el alfabeto de sustitución JULIOCESARBDFGHKMNÑPQTUVWXYZ

52 CBC (*Cipher-Block Chaining*) es el modo más utilizado de cifrado por bloques en contraposición al más simple y antiguo ECB (*Electronic CodeBook*). Su principal inconveniente es que el cifrado y descifrado es secuencial y no puede paralelizarse, mientras que en ECB el mensaje se divide en bloques que se cifran separadamente.

Criptografía asimétrica

La criptografía de clave pública se basa en la creación de "rompecabezas matemáticos" que son difíciles de resolver sin uno de los datos, pero fáciles de resolver con ese dato. El creador de las claves publica el rompecabezas (clave pública) y guarda el dato clave (clave privada). Ese rompecabezas matemático (clave pública) puede utilizarse para cifrar un número (mensaje) de manera que solo con el dato clave (clave privada) se pueda calcular el número original.
Por ejemplo es fácil multiplicar dos números primos pero es difícil factorizar el resultado. Lo mismo ocurre con el módulo de grandes números primos (DSA), los logaritmos discretos (ElGamal) o las matemáticas de las curvas elípticas. Por ejemplo si se usa la función "$g^a \bmod p = s$", es fácil calcular "s" a partir del resto de valores (g,a,p), pero es muy costoso computacionalmente calcular "a" a partir del resto de valores (g,p,s).

Se dice que un algoritmo de clave pública es reversible si se puede utilizar tanto la clave privada como la pública para cifrar y siempre es necesaria la clave contraria para descifrar.

La Criptografía de Curva Elíptica (ECC: *Elliptic Curve Cryptography*) es una variante de la criptografía asimétrica basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves más cortas que los métodos anteriores al tiempo que proporcionan un nivel de seguridad equivalente.

Firma de mensajes

Los algoritmos de firma aportan autenticación, integridad y no-repudio a la comunicación.
El sistema básico para firmar un fichero, un mensaje o un resumen es mediante su cifrado con una clave, de forma que solo podrá entenderse descifrándolo de nuevo. El hecho de que pueda descifrarse con la clave establecida garantiza su integridad (si se hubiese alterado una vez cifrado no se podría descifrar) y su autenticidad (ha sido cifrado con la clave -firma- correcta).

Para firmar un mensaje o un fichero se genera un resumen y se cifra únicamente el resumen, por varios motivos:
- Eficiencia: es más eficiente firmar un resumen de tamaño fijo y "pequeño" que largos ficheros de incluso varios GiB.
- Integridad: al firmar un resumen, éste no debe fraccionarse previamente
- Compatibilidad: los resúmenes siempre tienen el mismo tamaño y formato (para cada algoritmo de resumen) y es más fácil implementar algoritmos de firma sobre ellos
- Múltiples firmas: al mantener el mensaje original sin cifrar y firmar (cifrar un resumen) un mismo archivo puede ser firmado por diferentes entidades
- Firmado de datos públicos: El fichero original puede ser público (no necesita cifrarse) y basta con cifrar un resumen del mismo para garantizar su integridad y origen.

A cambio se introduce un nuevo punto de fallo (el algoritmo de resumen, que puede ser sensible a colisiones).

Además los protocolos de firma agregan mecanismos de estampado de tiempo, lo que aporta no-repudio a la comunicación, es decir el emisor no puede negar que es quién ha creado el mensaje si la clave no había sido comprometida con anterioridad.

Por tanto los protocolos de firma se componen de un algoritmo de cifrado de clave pública, un algoritmo de resumen y mecanismos de estampado de tiempo. En vez de algoritmos de clave asimétrica se pueden utilizar un algoritmo de clave simétrica con clave pre-compartida para realizar el cifrado.

Cuando se firman mensajes de comunicación dentro de un protocolo seguro, las firmas generadas se conocen como "código de autenticación de mensaje"(MAC o kHMAC *keyed-Hash Message Authentication Code*).

Comunicación segura

Cuando dos partes desean comunicarse de manera segura han de enviar sus mensajes cifrados, lo que permite garantizar la confidencialidad de la comunicación, es decir que solo quienes dispongan de la clave podrán entender el mensaje.
Además han de utilizarse técnicas de firmado para garantizar la integridad y autenticidad del mensaje.
Estas tres garantías (Autenticidad, Confidencialidad e Integridad) definen una comunicación segura.

Por tanto para establecer una comunicación segura las dos partes establecen una negociación en la que acuerdan el uso de un algoritmo de cifrado simétrico -son los más rápidos-, una clave para el algoritmo -que puede ir variando con el tiempo- y un sistema de firmado (mediante claves asimétricas o clave simétrica pre-compartida que también tendrán que acordar). Una vez realizada la negociación y establecidos los parámetros de una comunicación segura se dice que se ha establecido una asociación de seguridad (SA: *Security Association*).

Si ambas partes de la comunicación utilizan algoritmos asimétricos reversibles y disponen de la clave pública de la otra parte pueden realizar la negociación de manera segura usando un medio inseguro. Para ello el remitente debe firmar sus mensajes con su clave privada y utilizar la clave pública del destinatario para cifrar los mensajes que le envía.

Esto permite que:
- solo el destinatario puede leer el mensaje -descifrándolo con su clave privada- (confidencialidad)
- el mensaje no puede ser alterado y seguir siendo dado por bueno -fallaría el descifrado- (integridad)
- el destinatario puede verificar la firma del mensaje -mediante la clave pública del remitente- (autenticidad)

PKI (*Public Key Infraestructure*) y Redes de confianza (*Web of Trust*)

Si las partes no tienen conocimiento previo del otro no pueden simplemente solicitar a la otra parte su clave pública, ya que ésta podría ser alterada o intercambiada (ver más adelante el problema del hombre-en-medio). Para obtener las claves públicas de manera segura pueden utilizar una infraestructura de clave pública (PKI: *Public Key Infrastructure*). Estas infraestructuras se basan en la existencia de entidades certificadoras de claves públicas. Estas entidades emiten certificados que contienen el periodo de validez del certificado, datos del solicitante (datos de identificación y su clave pública) y están firmados por la entidad certificadora mediante la clave privada de la entidad. El principal formato de certificados utilizado es X.509, un estándar de ITU-T.

Para que una parte otorgue validez a un certificado de nuevo necesita conocer la clave pública de la entidad certificadora persistiendo el problema original. Por ello en última instancia las entidades certificadoras distribuyen su clave pública lo máximo posible mediante medios fiables, incluso en la propia instalación de los sistemas operativos y aplicaciones, por medio de certificados autofirmados. Además las entidades certificadoras deben certificarse unas a otras y crear listados de revocación de claves (para anular la validez de claves certificadas en su periodo de validez por haber quedado comprometidas).

Si no se dispone de PKI las partes deben acordar una clave para el algoritmo de cifrado simétrico sin llegar a comunicársela y sin que un tercero a la escucha pueda deducirla ya que entonces tendría capacidad para entender toda la comunicación. Este problema se conoce como "intercambio de claves" aunque, como se ha dicho, en realidad lo que se hace no es intercambiar una clave sino acordar una clave entre las partes.

Alternativamente las redes de confianza se basan en que cada usuario firme las claves públicas de usuarios de su entera confianza, que a su vez firman las claves públicas de otros exponencialmente, creando una red de claves públicas de confianza. Para obtener redes amplias y de calidad los usuarios deben conseguir que muchos terceros firmen su clave pública y, esto es muy importante, firmar solo la clave pública de terceros de confianza.

Intercambio Diffie-Hellman

El principal esquema teórico para acordar claves se conoce como intercambio Diffie-Hellman[53] (DH). Este esquema se basa, igual que la criptografía de clave pública en funciones cuya reversible es difícil de calcular.

Su funcionamiento se puede ver en el siguiente ejemplo con la función "$g^a \bmod p=s$":

Un extremo "Ana" quiere acordar una clave con "Bob" por un canal en el que escucha "Eva".
Ana informa a Bob (y a Eva) de que va a utilizar "g=5" y "p=23". En la práctica "g" suele ser 2 o 5, pero "p" debe ser un número primo de al menos 300 dígitos.
Entonces Ana elige un número aleatorio "a=6" (en la práctica "a" debe ser un número de al menos 100 dígitos), calcula "$5^6 \bmod 23=8$" y envía a Bob (y a Eva) el resultado (8).
Bob elige un número aleatorio "b=15" (que como el número aleatorio "a" de Ana debe ser en la práctica de al menos 100 dígitos), calcula "$5^{15} \bmod 23=19$" y envía a Ana (y a Eva) el resultado (19).
Con estos datos Ana calcula que la clave acordada con Bob es "$19^6 \bmod 23=2$". Bob calcula que la clave acordada con Ana es "$8^{15} \bmod 23=2$". Nótese que solo Ana conoce "a" y solo Bob conoce "b" pero ambos calculan el mismo valor para la clave "s=2".
Eva para conocer la clave acordada "s" sin conocer ni "a" ni "b" debería resolver el sistema de ecuaciones

- $5^a \bmod 23=8$
- $5^b \bmod 23=19$
- $19^a \bmod 23=8^b \bmod 23=s$

lo cual, con las restricciones dadas para los valores de "p", "a" y "b", actualmente es irresoluble computacionalmente.

El problema del hombre en medio

El esquema DH solo se ocupa de acordar una clave, pero no de autenticar a los extremos, por lo que es atacable mediante un esquema de hombre-en-medio (*man-in-the-middle*). Para realizar este ataque, el atacante debe conseguir interceptar la comunicación haciendo de intermediario, es decir debe conseguir que los mensajes que las partes envían lleguen al intermediario y no al destinatario original y después reenviarles los mensaje, sustituyendo la comunicación directa por una indirecta. Para que las partes no noten la interferencia el intruso finge ser en cada momento el remitente original.

Siguiendo el ejemplo anterior:

Si Eva en vez de solo escuchar quisiera hacer un ataque tipo hombre-en-medio, lo que haría es establecer una comunicación con Ana fingiendo ser Bob y establecer otra comunicación con Bob fingiendo ser Ana. Usando el esquema Diffie-Hellman acordaría una clave con Ana y otra con Bob. Después desencriptaría los mensajes enviados por Ana con la clave acordada con ella y los volvería a encriptar con la clave acordada por Bob para enviárselos a él. De la misma manera desencriptaría los mensajes enviados por Bob con la clave acordada con él y los volvería a encriptar con la clave acordada por Ana para enviárselos a ella.

En medio de una comunicación con claves asimétricas:

Si Eva quiere hacer un ataque tipo hombre-en-medio en una comunicación con claves asimétricas entre Ana y Bob, lo que haría es enviar a Ana su clave pública -una generada al efecto- como si fuese la de Bob y enviar a Bob otra clave pública -generada al efecto- como si fuese la de Ana. De nuevo establecería una comunicación segura con Ana y otra con Bob, reenviando los mensajes interceptados tras descifrarlos y volverlos a cifrar y firmar.
Como hemos visto, este ataque no es posible si previamente Ana y Bob conocen las claves públicas de la otra parte o si Ana y Bob verifican las claves públicas que reciben mediante certificados de una entidad que previamente hayan reconocido.

Este ataque de hombre-en-medio permite no solo conocer la información intercambiada sino también alterarla enviando al destinatario mensajes o ficheros totalmente diferentes de los enviados por el remitente original.

El uso de PKI con claves públicas certificadas por las partes hace innecesario el esquema DH. Pero ¿qué ocurre cuando un cliente sin certificado quiere comunicarse de manera segura con un servidor con certificado? Es decir ¿y si solo una de las partes usa PKI para certificar su autenticidad?

53 El esquema fue publicado por Whitfield Diffie y Martin Hellman en 1976.

En estos casos se utiliza el intercambio DH y el servidor firma todos sus mensajes. Esto hace que el hombre-en-medio pueda alterar los mensajes solo en una dirección (cliente sin certificar → servidor). Haciéndolo podría engañar al servidor pero no al cliente, con lo que la comunicación cliente-servidor no se establecería. Si no se altera ningún mensaje, como hemos visto, cliente y servidor podrán acordar una clave sin que ningún tercero sea capaz de averiguarla.

9.2. Algoritmos

Como hemos comentado existen tres tipos básicos de algoritmos:

- **Cifrado simétrico**. Permiten cifrar y descifrar mensajes mediante una misma clave.
- **Cifrado asimétrico -algoritmos de clave pública y privada-**. Estos algoritmos utilizan dos claves diferentes para cifrar y descifrar mensajes. Una de las claves se publica y la otra se mantiene privada.
- **Resumen -"*Digest*", "*Hash*", "*Cheksum*"-**. No son algoritmos de cifrado sino que generan un resumen que permite verificar la integridad del fichero o mensaje pero no permite obtener el original.

Cifrado simétrico (DES, 3DES, AES, RCx e IDEA)

Los algoritmos informáticos de cifrado simétrico se basan principalmente en la trasposición de bloques (*block cipher*) de bits en base a claves binarias.

DES y 3DES

El algoritmo DES (*Data Encryption Standard*) creado en 1976 requiere una clave de 64 bits, de los cuales utiliza únicamente 56 bits siendo los otros 8 un control de paridad.
Para mejorar la seguridad se creo Triple DES (TDES o 3DES), que consiste en utilizar tres veces DES, cifrando y/o descifrando con una, dos o tres claves diferentes. Así DES-EEE1 cifra tres veces con la misma clave, mientras que DES-EDE3 cifra-descifra-cifra con tres claves diferentes (al usar para "descifrar" una clave diferente que para cifrar, en realidad se complica el cifrado). Las variantes más seguras son DES-EEE3 y DES-EDE3[54].
Si se utilizan 3 claves diferentes la longitud de la clave usada es de 168 bits (56x3) pero la seguridad efectiva[55] es de 112 bits.
3DES es un algoritmo seguro pero lento, que permitió seguir utilizando dispositivos creados para DES. Sin embargo está siendo sustituido por AES (*Advanced Encryption Standard*).

AES

AES (*Advanced Encryption Standard*) es uno de los algoritmos más utilizados, ya que se convirtió en estándar en 2002. Utiliza un tamaño de bloque de 128 bits y claves de 128, 192 o 256 bits. AES es rápido tanto por *software* como por *hardware*, es relativamente sencillo de implementar y requiere poca memoria en el proceso.

RCx

RC4 (Rivest Cipher o Ron's Code) era el algoritmo de cifrado por software más utilizado en parte por ser el algoritmo utilizado por SSL y WEP. Este algoritmo utiliza un sistema de cifrado de flujo (*stream cipher*) no de trasposición de bloques. Esto hace que sea rápido y sencillo. Sin embargo este algoritmo es fácilmente atacable si la clave de flujo (*keystream*) no se descarta, o no es aleatoria o cambia en relación a la clave anterior o se usa varias veces la misma. Utiliza una clave de entre 40 y 256 bits y no se recomienda su uso ya que no aporta seguridad suficiente.
RC4 ha sido sustituido por RC5 y RC6 que utilizan trasposición de bloques. RC6 utiliza un tamaño de bloque de 128 bits y claves de 128, 192 o 256 bits (como AES), aunque puede parametrizarse con otros valores.
ARCFour (*Alleged RC4*) es un algoritmo libre al parecer compatible con RC4 (algoritmo patentado y cerrado).

IDEA

IDEA (*International Data Encryption Algorithm*) es un algoritmo de trasposición de bloques de 64 bits con clave de 128 bits. Se usa en PGPv2 (*Pretty Good Privacy*) y es opcional en OpenPGP dado que está sujeto a licencia en algunos paises.

54 Se puede observar que DES-EDE1 equivale a DES.
55 Se dice que un algoritmo tiene una seguridad efectiva de N bits si un ataque por fuerza bruta necesitaría del orden de 2^n intentos para tener éxito.

Cifrado asimétrico (RSA, ElGamal, DSA y ECDSA)

El esquema propuesto por Diffie-Hellman en 1976 era un modelo teórico. La primera realización robusta del modelo Diffie-Hellman apareció en 1978 (RSA78: Rivest-Shamir-Adleman 1978).
El algoritmo de cifrado RSA es reversible, es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la pública. Así se puede utilizar tanto para obtener confidencialidad (cifrando con la clave pública del destinatario) como para firmar (cifrando con la clave privada del emisor).

La primera versión de RSA (RSA base) no es suficientemente segura. En cambio "RSA Security" publica los PKCS (*Public Key Cryptography Standards*)[56] que definen los detalles de las implementaciones de RSA, y esquemas criptográficos de seguridad, incluyendo certificados, etc.
Se basa en la función "$m^e \bmod n = s$" con amplias restricciones para cada parámetro utilizado.
La clave pública se compone de "n" ($n=pq$) y "e" ($e=$mínimo común múltiplo$(p-1,q-1)$). La clave privada es un número "d" que cumple "$de \equiv 1 \pmod{\varphi(n)}$"[57] ("p" y "q" son números primos grandes).
Dado un número cualquiera "m" (el mensaje a cifrar) se obtiene el número "c" (mensaje cifrado) "$c \equiv m^e \pmod n$". A partir de "c" (mensaje cifrado), "d" (clave privada) y "n" (parte de la clave pública) se puede obtener "m" (el mensaje original sin cifrar) mediante "$m \equiv c^d \pmod n$".

El cifrado ElGamal (1984) es otra implementación, pero se basa en logaritmos discretos. Se utiliza en GPG y PGP.

DSA (*Digital Signature Algorithm*) es un algoritmo de clave asimétrica no reversible adoptado en 1993 para el estándar DSS (*Digital Signature Standard*)[58]. Como su nombre indica, sirve para firmar, no para cifrar información -dado que no es reversible-. Se basa en la dificultad de calcular logaritmos discretos en campos finitos -métodos de Schnorr y ElGamal-.
DSA primero selecciona un algoritmo de resumen (generalmente uno de la familia SHA) y una longitud de clave (inicialmente un múltiplo de 64 entre 512 y 1024, pero actualmente 1024, 2048 o 3072).
Utiliza la función "$g = h^{(p-1)/q} \bmod p$" y "$y = g^x \bmod p$" con varias restricciones sobre los parámetros, siendo (p,q,g,y) la clave pública y (x) la clave privada.

ECDSA (*Elliptic Curve DSA*) es una variante de DSA que utiliza CCE. En teoría es mucho más seguro que DSA y genera firmas del mismo tamaño.

Resumen (CRC-32, MD5 y SHA)

No son realmente algoritmos de cifrado sino que generan un resumen ("*Digest*", "*Hash*" o "*Checksum*") que permite verificar la integridad del fichero o mensaje pero no permite obtener el original[59]. Los principales son: MD5 (*Message-Digest* 5) y SHA (*Secure Hash Algorithm*). Tanto SHA-1 como MD5 descienden de MD4.
A este resumen a veces se le llama "firma de fichero" lo que puede llevar a confusión con los algoritmos de firma electrónica, que incluyen cifrado y estampado de tiempo.

MD5 (*Message-Digest algorithm* 5) es una función de resumen ampliamente difundida que genera resúmenes de 128 bits, expresada habitualmente como un número hexadecimal de 32 digitos. Actualmente se pueden generar colisiones arbitrariamente[60] por lo que está empezando a ser sustituido.
Los algoritmos SHA (*Secure Hash Algorithm*) son un conjunto de funciones (SHA-0, SHA-1 y SHA-2). SHA-1 es la versión más empleada y se utiliza entre otros en SSL y TLS, PGP, SSH, S/MIME e IPSec. SHA-1 genera resúmenes de 160 bits y se han encontrado debilidades teóricas.
Por su parte SHA-2 utiliza un algoritmo muy similar a SHA-1 pero genera resúmenes de tamaño variable conociendose las variantes como SHA-224, SHA-256, SHA-384 y SHA-512. Debido a las debilidades teóricas expuestas en SHA-1, y por tanto SHA-1, está en desarrollo SHA-3.

56 PKCS#1 (v 2.1) define el esquema RSA; PKCS#3 (v. 1.4) define el intercambio DH. Hasta PKCS#15 (algunos obsoletos) que definen varios esquemas más de seguridad criptográfica.
57 Relación de congruencia entre "de" y "1" con módulo "$\varphi(n)$". Es decir "de mod $\varphi(n)$ = 1 mod $\varphi(n)$".
58 Aunque ha sufrido también algunas modificaciones desde entonces.
59 P.e. la letra del NIF se calcula a partir del DNI.
60 Crear un archivo que genere el mismo resumen y por tanto permita sustituir al archivo original.

9.3. Técnicas criptográficas y de seguridad

Los diferentes algoritmos de cifrado se utilizan en diferentes técnicas criptográficas y de seguridad, principalmente:

- **Acuerdo de claves**. Permite a dos partes que no tienen un conocimiento previo el uno del otro, acordar una clave secreta -y establecer una comunicación cifrada- usando un canal inseguro.
- **Autenticación de las partes**. Permiten verificar que los extremos de una comunicación son quienes dicen ser.
- **Firma electrónica**. Permiten firmar un fichero, un mensaje o un resumen mediante su cifrado con una clave, de forma que se garantice la procedencia mediante un correcto descifrado.

Acuerdo de claves (PSK, DH, ECDH, RSA, SRP)

Estos esquemas se utilizan cuando no existe una clave pre-compartida (PSK: *Pre-Shared Key*). Los principales son los ya comentados DH (*Diffie-Hellman*), ECDH (*Elliptic Curve DH*) y RSA (*Rivest-Shamir-Adleman*), además del protocolo SRP (*Secure Remote Password*).

El protocolo SRP (*Secure Remote Password*) es un protocolo de acuerdo de clave basado en la autenticación por clave de una de las partes (cliente). Este protocolo acuerda una clave privada de manera similar a DH y después verifica que las dos partes tienen la misma clave y ambas conocen la clave del usuario (cliente).

Autenticación de las partes (PSK, RSA, DSA y ECDSA)

Para autenticar a las partes de la comunicación se utilizan bien PSK o bien algoritmos de clave pública apoyados en una PKI o una red de confianza (*web of trust*).

Firma electrónica (DSA, ECDSA, HMAC-MD5 y HMAC-SHA)

Los protocolos de firma se componen generalmente de un algoritmo de cifrado asimétrico (RSA, DSA y ECDSA) o cifrado simétrico con clave pre-compartida (PSK), un algoritmo de resumen (MD5 y SHA) y mecanismos de estampado de tiempo para incorporar no-repudio.

9.4. Autenticación de usuario

Una vez establecida una comunicación segura puede ser necesaria la identificación de una de las partes como cliente en la otra parte como servidor. Para ello se pueden utilizar diferentes algoritmos, protocolos y sistemas.

PAP, CHAP, Ms-CHAP

PAP (*Password Authentication Protocol*) es el mecanismo más sencillo de autenticación de usuario y lo que hace es enviar un par usuario/contraseña en claro por la red.

La familia de algoritmos CHAP (*Challenge-Handshake Authentication Protocol*) y en particular las implementaciones de Microsoft (MS-CHAP y MS-CHAPv2) se basan en mecanismos de "retos" para realizar la autenticación. En vez de solicitar la clave, que podría ser interceptada, se realiza una comunicación de acuerdo en tres partes ("*three-way handshake*") en la que el servidor "reta" al cliente basándose en la clave secreta, el cliente responde al reto y el servidor confirma o deniega la autenticación. Este proceso se repite regularmente durante la comunicación.
El protocolo original CHAP requiere que ambos extremos cliente y servidor conozcan la clave secreta aunque nunca sea trasmitida.

La versión MS-CHAP además permite al usuario cambiar la clave, permite autenticación mutua entre pares y no requiere que ambas partes conozcan la clave en claro, sino un resumen (*Hash*) de la misma.
PPP (*Point-to-Point Protocol*) utiliza CHAP para autenticar a los usuarios.

Kerberos

Kerberos es un protocolo de autenticación de partes cliente-servidor que permite autenticar ambas partes sobre un medio inseguro. Se basa en cifrado simétrico (DES) y un tercero en quien confían ambas partes (KDC *Key Distribution Center*). Este tercero provee las funciones de autenticación (AS: *Authentication Server*) y despacho de etiquetas (TGS: *Ticket Granting Server*). Todas las partes deben autenticarse en el AS. Algunas extensiones de Kerberos permiten el uso de PKI. La versión 5, vigente, permite el uso de AES en vez de DES.
Todos los equipos gestionados por un servidor forman un dominio o territorio Kerberos (*realm*).

Supongamos que Ana quiere solicitar un servicio de Bob y el KDC es Carlos. Tanto Ana como Bob deben ser conocidos por Carlos (tener un usuario y contraseña).
Primero Ana solicita a Carlos autenticarse mediante un mensaje en claro. Carlos le envía a Ana dos mensajes. El primer mensaje se llama TGT ("*Ticket-Granting Ticket*") y está cifrado con una clave privada de Carlos (indescifrable para Ana). El TGT incluye el identificador de Ana, el periodo de validez de la sesión y la clave de sesión Ana-Carlos.
El segundo mensaje que le envía Carlos a Ana es la "etiqueta de sesión Ana-Carlos" que contiene una clave de sesión Ana-Carlos y está cifrado con la clave de Ana. Al estar cifrado con la clave de Ana solo ella podrá acceder a la clave de sesión Ana-Carlos. Si Ana es capaz de usar la clave de sesión Ana-Carlos está autenticada.

Una vez autenticada Ana debe solicitar a Carlos el uso del servicio de Bob. Para hacer la solicitud envía a Carlos un mensaje con el TGT y el identificador del servicio de Bob al que quiere acceder. Además Ana envía un mensaje "Autenticador" que contiene su identificador y una marca de tiempo, cifrado con la clave de sesión Ana-Carlos.
Carlos utiliza su clave secreta para descifrar el TGT y obtener la clave de sesión Ana-Carlos. Con la clave de sesión Ana-Carlos descifra el "Autenticador" y lo da por válido (pues solo Ana lo ha podido enviar ya que es la única que conoce la clave de sesión Ana-Carlos).

Carlos verifica si Ana tiene permiso para acceder al servicio de Bob y en ese caso le envía a Ana dos nuevos mensajes. Un mensaje contiene una nueva clave de sesión Ana-Bob cifrada con la clave de sesión Ana-Carlos (que Ana puede descifrar).
Otro mensaje "petición de servicio" contiene los datos de Ana (identificador, periodo de validez) y la clave de sesión Ana-Bob cifrados con la clave de Bob (indescifrable para Ana).

Ana envía entonces a Bob el mensaje "petición de servicio" tal y como se lo envió Carlos.
Además le envía un nuevo mensaje "Autenticador" con su identificador y una marca de tiempo cifrado con la clave de sesión Ana-Bob.

Bob descifra con su clave secreta el mensaje "petición de servicio", lo que le garantiza que la petición proviene de un cliente autenticado (pues lo ha generado Carlos), y obtiene la clave de sesión Ana-Bob.
Con la clave de sesión Ana-Bob descifra el "Autenticador" suma uno a la marca de tiempo y lo devuelve a Ana, de nuevo cifrado por la clave de sesión Ana-Bob.
Ana descifra el "Autenticador" y verifica que la marca de tiempo es la que había indicado más uno, lo que sirve para autenticar a Bob.

NTLM

NTLM es un protocolo de autenticación similar a MS-CHAP, basado en retos sobre los datos de usuario. Utiliza algoritmos MD4/MD5, SHA y DES para los cálculos.
NTLMv2 utiliza HMAC-MD5 y separa el control de sesión en el protocolo NTLM-session (similar a MS-CHAPv2).

Aunque el protocolo Kerberos ha sido adoptado por Microsoft para la autenticación en el directorio activo, todavía utiliza NTLM en determinadas circunstancias:

- Si el cliente se autentica usando una dirección IP.
- Si el cliente se autentica en un servidor de otro bosque del directorio activo o no pertenece a ningún dominio o no existe ningún dominio.
- Si un cortafuegos corta los puertos necesarios para usar Kerberos.

Servidores AAA (RADIUS y TACACS)

Una función relacionada con la comunicación segura es la autenticación de los usuarios, diferenciándola de la autenticación de los extremos en una asociación de seguridad que permite evitar ataques de tipo hombre-en-medio. Una vez establecida una comunicación entre un cliente y un servidor, éste puede requerir una autenticación de usuario, para verificar que dicho usuario tiene acceso al servicio. Pero esta autenticación de usuario puede realizarse independientemente de si la comunicación es segura o no (aunque cada vez más, los servicios restringidos suelen realizarse a través de comunicaciones seguras).
Las funciones de los servidores de autenticación son en realidad tres, conocidas como triple A o AAA: *Authentication*, *Authorization*, *Accounting* (Autenticación, Autorización y Registro).

El sistema RADIUS (*Remote Authentication Dial-In User Service*) permite decidir la concesión de acceso a partir de una combinación de datos como la identidad del usuario, la pertenencia a un grupo, la hora del día, la fecha, el nivel de cifrado soportado, el tipo de túnel... Además permite la asignación de parámetros de conexión, como algoritmos de seguridad obligatorios.

RADIUS es escalable y permite configurarse para solicitar la autenticación a otro servidor (RADIUS o de otro tipo). El estándar de IETF (RFCs 2138 y 2139) define el puerto UDP 1812 para autenticación, pero se ha utilizado durante mucho tiempo el 1645.

Mientras que RADIUS combina la autenticación y autorización en el perfil de usuario, TACAS+ separa las dos operaciones. Además RADIUS utiliza UDP y TACACS+ utiliza TCP.

9.5. Esquemas de seguridad

Las diferentes técnicas criptográficas (algoritmos de cifrado y resumen, intercambio de claves, autenticación de equipos y usuarios y firma electrónica) vistas hasta ahora se combinan para crear diferentes esquemas de seguridad y protocolos de comunicación segura.

SSL y TLS

TLS (*Transport Layer Security*) es un protocolo estándar basado en SSL (*Secure Sockets Layer*), desarrollado por Netscape. TLS permite establecer comunicaciones seguras punto-a-punto por encima de la capa de transporte de la red (generalmente TCP/IP). TLS otorga autenticación (mediante PKI), confidencialidad e integridad. La autenticación puede ser unilateral (por ejemplo en un entorno web cliente-servidor) o bilateral, ya sea utilizando PKI, TLS-PSK o SRP.
Durante el inicio de la comunicación los extremos negocian el algoritmo de cifrado simétrico a utilizar, realizan el intercambio (o acuerdo) de clave y acuerdan los algoritmos de firma a utilizar. Una vez establecida la comunicación se utiliza el algoritmo de clave simétrica (con la clave acordada) para cifrar la comunicación y el algoritmo de firma para generar los códigos de autenticación de los mensajes (MAC: *Message Authentication Codes* o kHMAC).
Los algoritmos más utilizados en TLS son:

- Para intercambio de claves: RSA, Diffie-Hellman, ECDH, SRP, PSK
- Para autenticación de las partes: RSA, DSA, ECDSA
- Para cifrado: Triple DES, AES, IDEA
- Para firma de mensajes: HMAC-MD5 (SSLv2 en desuso) o HMAC-SHA (SSLv3).

IKE

IKE (*Internet Key Exchange*) o IKEv2 (la versión 1 es obsoleta) permite la creación de conexiones de seguridad que utiliza DH para el intercambio de claves y PSK, PKI o Kerberos para la autenticación de las partes. Permite negociar el cifrado simétrico y la firma de mensajes.
IKE funciona sobre UDP y, entre otros, es utilizado por ISAKMP y EAP-IKE.

ISAKMP (*Internet Security Association and Key Management Protocol*)

Es un esquema utilizado en IPSec para establecer comunicaciones seguras (crear asociaciones de seguridad) y renovar periódica y automáticamente la clave del cifrado simétrico entre las partes. ISAKMP generalmente utiliza IKE para crear la asociación de seguridad y negociar el algoritmo de cifrado y firma, aunque puede utilizar otros protocolos.

WEP, WPA (TKIP) y WPA2

El esquema de seguridad inicial de 802.11 se llamó WEP (*Wired Equivalent Privacy*) y se basaba en el algoritmo de cifrado de flujo RC4 y una clave pre-compartida (PSK: *Pre-Shared Key*).
El esquema original (WEP-40) para generar la clave de flujo de RC4 (64 bits) utiliza una clave PSK de 40 bits que se concatena con una cadena de 24 bits que identifica la red (vector de inicialización).
Tras aliviar las restricciones legales a los algoritmos de cifrado (año 2000) se comenzó a usar una clave de 128 bits (WEP-104). Sin embargo los problemas de WEP con RC4 tienen mucho que ver con el vector de inicialización y la obtención de la clave de flujo, por lo que el aumento de la clave no es útil ya que el sistema sigue siendo inseguro.

WPA (*Wi-Fi Protected Access*) comenzó a utilizarse en 2003. Esta especificación se basaba también en RC4 con PSK pero utiliza TKIP (*Temporal Key Integrity Protocol*) para mejorar la seguridad. TKIP realiza un control de integridad de los paquetes (ya que en los ataques algunos paquetes se alteraban sin llegarlos a descifrar), un conteo de los mismos y utiliza una función para obtener la clave de RC4 mezclando la clave de usuario con el vector de inicialización de la red (en vez de realizar una simple concatenación).
El sistema 802.11i final, conocido como WPA2, apareció en 2004. Permite utilizar nuevos mecanismos de distribución de la clave (comoEAP), autenticación basada en PSK o en servidores (como servidores RADIUS) y CCMP (basado en AES) para cifrado. CCMP (*Counter-mode with Cipher-block-chaining Message-authentication Protocol*), es opcional en WPA y sustituye totalmente a TKIP y WEP (obsoletos) en WPA2. CCMP utiliza AES tanto para la mantener la confidencialidad como para verificar la integridad.
La configuración habitual recomendada es WPA2 con clave precompartida (AES-PSK) -en entornos domésticos o PyMES- o WPA2 con servidores RADIUS (EAP-TLS) en entornos corporativos.

EAP, LEAP y PEAP

EAP (*Extensible Authentication Protocol*) es un esquema de autenticación utilizado en PPP y redes inalámbricas, siendo el esquema oficial de WPA y WPA2. No es un mecanismo de autenticación sino que define formatos de mensajes y mecanismos de autenticación para distintos protocolos (conocidos como EAP-MD5, EAP-SIM, EAP-AKA, EAP-TLS, EAP-IKEv2, EAP-TTLS...). Cada protocolo encapsula mensajes EAP.
El objetivo de EAP es generar una clave inicial llamada PMK (*Pair-wise Master Key*) a partir de la cual establecer la comunicación. Para ello básicamente realiza la autenticación de los extremos y el intercambio de claves para el algoritmo de cifrado acordado.

LEAP (*Lightweight Extensible Authentication Protocol*) es una versión de EAP creada por Cisco que utiliza MS-CHAP para autenticación de usuarios y actualmente obsoleta por insegura

EAP-PSK utiliza PSK para la autenticación y el intercambio de clave.

EAP-TLS es un esquema poco utilizado ya que requiere que ambas partes utilicen PKI (certificados) para su autenticación. Es universalmente soportado y considerado uno de los más seguros.

EAP-TTLS, conocido a veces únicamente como TTLS (*Tunneled Transport Layer Security*), es una extensión de EAP-TLS que permite que una de las partes (cliente) se autentique sin necesidad de certificado PKI. El cliente una vez autenticado el servidor crea con él un túnel cuyo uso sirve de autenticación del cliente.

EAP-IKEv2 se basa en IKEv2 para autenticar las dos partes cliente-servidor e intercambiar claves. El servidor puede autenticarse mediante PKI o algoritmos de clave simétrica. El cliente puede autenticarse además mediante una clave de cliente.

PEAP (*Protected EAP*) es un estándar de la industria similar a EAP-TTLS. Para autenticar las partes se puede utilizar PEAPv0 o v1. Microsoft solo implementa PEAPv0. Para autenticar a los clientes en el servidor se puede utilizar EAP-MSCHAPv2, EAP-TLS, EAP-GTC o EAP-SIM.
La versión más extendida y utilizada, que se conoce símplemente como PEAP, es PEAPv0/EAP-MSCHAPv2.

PGP / OpenPGP / GPG

PGP (*Pretty Good Privacy*), desarrollado originalmente por Philip Zimmermann en 1991, derivó en el estándar OpenPGP (1997). GPG o GnuPG (GNU Privacy Guard) es una implementación de OpenPGP.
OpenPGP es probablemente el sistema de cifrado personal más utilizado. Nació con el objetivo de cifrar correo-e, a lo que se añadió la firma de mensajes y el cifrado de archivos en disco.
GPG es una utilidad de línea de comandos, pero existen numerosos "*front-end*" gráficos y es la herramienta utilizada por múltiples programas para gestionar su cifrado, especialmente clientes de correo y navegadores.
GPG utiliza algoritmos de cifrados libres de patentes como 3DES, AES o Blowfish y ElGamal, mientras que PGP utiliza además algoritmos como IDEA o RSA que tiene restricciones de patentes en algunos países[61].

SSH

SSH es un protocolo cliente-servidor que permite la conexión segura con máquinas remotas para abrir sesiones y ejecutar comandos, crear túneles o reenviar puertos TCP y conexiones X11. Además puede trasferir ficheros mediante los protocolos asociados SFTP y SCP. El servidor generalmente escucha en el puerto TCP 22.

SSH-1 es un protocolo monolítico, mientras que SSH-2 es un protocolo de 4 capas: Una de transporte (que incluye el intercambio de claves, cifrado, compresión e integridad), Una de autenticación de usuario (mediante contraseña, clave pública, Kerberos y otros), Una de conexión (que permite múltiples canales en una sola conexión) y una llamada "SSHFP DNS" que se encarga de las firmas de los servidores ("*host key fingerprints*").

SSH-2 inicialmente utilizaba solo DSA como algoritmo de autenticación de equipos (y opcionalmente usuarios) y el intercambio DH para acordar la clave del algoritmo simétrico. Dado que actualmente RSA ha pasado a dominio público también puede utilizarse en OpenSSH para la autenticación de equipos y usuarios y el intercambio de claves.

SSH utiliza el cifrado asimétrico para la autenticación del servidor y el intercambio de claves (RSA o DSA + DH); el cifrado simétrico para la confidencialidad y los resúmenes para la integridad (mediante MACs: *Message Authentication Codes*). Además permite comprimir los paquetes para mejorar el rendimiento de la conexión.

	SSH-1	SSH-2
Cifrado asimétrico	RSA	RSA, DSA, DH
Cifrado simétrico	3DES, Blowfish, *IDEA*	3DES, AES, Blowfish, CAST-128, Twofish, *IDEA*
Resumen	MD5, CRC-32	MD5, SHA-1
Compresión	zlib	zlib

SSH nació como software libre pero cambió a privado como SSH-2 tras la versión 1.2.12. OpenSSH se desarrolló a partir de la última versión libre disponible. Más tarde SSH-2 se propuso como estándar de Internet. OpenSSH incluye:

- **sshd**, servidor
- **ssh**, cliente que reemplaza a rlogin y telnet para conectar con máquinas remotas
- **scp** y **sftp**, clientes que reemplazan respectivamente a rcp y ftp para copiar ficheros entre máquinas
- **ssh-keygen**, herramienta para generar y verificar las claves RSA y DSA utilizadas para la autenticación de equipos y usuarios.
- **ssh-agent** y **ssh-add**, utilidades para facilitar el uso y administración de claves públicas y privadas.
- **ssh-keyscan**, herramienta para analizar las claves de un servidor

61 GPG permite utilizar IDEA, mediante un "*plug-in*" sujeto a restricciones de licencia según países.

9.6. Herramientas de seguridad de redes

Las herramientas de seguridad de redes pueden utilizarse para revisar la seguridad de un sistema con buenas o con malas intenciones. *Si no revisas la seguridad de tu sistema, alguien lo hará por ti.*

Analizadores de red

Estas herramientas buscan equipos en la red, hacen barridos de puertos y descubrimiento de servicios, analizando los resultados para inferir información, como versión y tipo de sistema y/o servicios, y exponer deficiencias de seguridad. Algunos de los más utilizados son nmap, SATAN y SAINT.

Analizadores de seguridad

Otro tipo de herramientas se utiliza para analizar un equipo y localizar todo tipo de posibles problemas de seguridad. Permite detectar y exponer aplicaciones conocidas por su fragilidad, configuraciones particulares inseguras, uso de claves predefinidas y múltiples *bugs* y sus *exploits*.
Nessus es una aplicación gratuita para uso no comercial (en origen era libre). Sus desarrolladores producen decenas de nuevos análisis de vulnerabilidades a la semana. Estos análisis -llamados "*plug-ins*"- se publican para su uso gratuito una semana después de su puesta a disposición de los clientes de pago.
OpenVAS -inicialmente gnessus- es un analizador libre que nació como una ramificación del último Nessus libre. Los análisis de vulnerabilidades son llamados NVTs (*Network Vulnerability Tests*).

Analizadores de paquetes

Los analizadores de paquetes captan todos los paquetes que llegan a la tarjeta de red (NIC) configurándola en modo promiscuo. Después facilitan el análisis de dichos paquetes de red según los protocolos utilizados en los paquetes.
El más utilizado es WireShark, inicialmente llamado Ethereal, que dispone de interfaz gráfica. Otro analizador bastante utilizado es tcpdump, disponible solo en modo comando, aunque existen frontispicios gráficos como WinDump.

Descubrimiento de claves

Los programas de descubrimiento de claves analizan listados de claves cifradas o resumidas (mediante algoritmos como MD4) para intentar descubrirlas.
La herramienta más utilizada es "John The Ripper", que es libre. JTR autodetecta el tipo de resumen de la clave y puede atacar claves de multitud de algoritmos como DES, MD5, Blowfish, Kerberos o LM Hash (Windows) tanto en ficheros de texto como en repositorios sobre LDAP o MySQL. Puede trabajar con ataques de diccionario y alteraciones o mediante fuerza bruta usando tablas de caracteres frecuentes para marcar el orden.

10. TRANSMISIÓN MULTIMEDIA EN REDES IP

10.1. Introducción

El sistema tradicional de vídeo-conferencia es un conjunto de normas y protocolos definido como H.320, que se basa en la utilización de redes RDSI. Para poder realizar transmisiones multimedia en LANs basadas en IP se desarrolló el estándar H.323, basándose en tres ideas fundamentales:

- Utilizar los estándares existentes.
- Incorporar las ventajas de las redes de conmutación de paquetes para el transporte de voz y vídeo.
- Conseguir la transmisión de información multimedia en tiempo real a través de redes compartidas.

Los equipos tradicionales de vídeo-conferencia sobre RDSI (H.320) están formados por un ordenador con un códec *hardware* (H.26x) y una conexión RDSI, al que se le acopla un monitor de televisión y una serie de dispositivos de entrada/salida de altas prestaciones, tales como cámaras activadas por la voz, cámaras de documentos, micrófonos direccionales, micrófonos de ambiente, un sistema de altavoces de alta calidad, etc. Además incorporan sofisticados sistemas de supresión de eco para mejorar la calidad del sonido. Sin embargo su capacidad de multi-conferencia está limitada a un máximo de 5 usuarios por conexión RDSI, ya que con un flujo entrante y cuatro salientes se ocuparía toda la capacidad del acceso RDSI primario.

En el caso de H.323 la situación es similar salvo que se utiliza redes IP (principalmente Internet) en vez de RDSI. En muchos casos los terminales H.323 ofrecen una calidad inferior comparados con los H.320 debido al tipo de componentes utilizados: cámaras digitales de baja calidad, micrófonos baratos, carecen de supresión de eco, etc.

Si bien la familia de protocolos H.323 se diseñó para videoconferencia, los terminales H.323 implementan obligatoriamente únicamente un canal de audio y el resto de canales son opcionales. Por ello es posible utilizar H.323 para telefonía IP que utiliza únicamente Voz sobre IP (VoIP: *Voice over IP*) para realizar llamadas telefónicas tradicionales utilizando como terminales tanto equipos informáticos como teléfonos de la RTC.
Algunas ventajas de la telefonía IP son:

- Las llamadas de VoIP entre equipos de red IP no tienen coste adicional. El coste de una llamada de VoIP a la RTC se calcula en base a la ubicación de la pasarela utilizada (llamada local, nacional...) sin coste extra.
- Las llamadas pueden ser dirigidas a un terminal IP independientemente de su ubicación física real.
- Los terminales de VoIP pueden integrarse con otros servicios multimedia y de intercambio de datos.
- Dispone de múltiples servicios digitales: contestador automático, desvío de llamadas inteligente, bloqueo de llamadas salientes, filtrado de llamadas entrantes, multi-conferencia, marcación abreviada, extensiones virtuales, facturación de llamadas en tiempo real, identificador de llamada entrante, llamada en espera, transferencia de llamada en curso...

Sin embargo H.323 resulta excesivamente complejo en algunos aspectos para utilizarlo solo como VoIP. Esto motivó que la IETF desarrollara un protocolo alternativo denominado SIP (*Session Initiation Protocol*), con la intención de ser un estándar más sencillo y orientado a telefonía IP.
Más específicamente SIP está orientado a la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia. Así se utiliza para videoconferencias, mensajería instantánea, juegos en red...
En resumen actualmente H.323 y SIP realizan básicamente las mismas funciones, si bien son protocolos incompatibles. Para permitir la interconexión de redes existen pasarelas entre H.323 y SIP.

Aunque los protocolos multimedia más antiguos y utilizados son H.323 y SIP, existen otro muchos[62]. De la elección de uno u otro dependerá la eficacia y la complejidad de la comunicación.

62 Por orden de antigüedad (de más antiguo a más nuevo): H.323 (ITU-T), SIP (IETF), Megaco, Skinny CCP (Cisco), MiNet (Mitel), CorNet-IP (Siemens), IAX (Asterisk -obsoleto-), Skype (Skype), IAX2 (Asterisk), Jingle (abierto, Jabber), Telme (Woip2) y MGCP (Cisco).

10.2. El protocolo H.323

Introducción

El estándar H.323 es un conjunto de normas y protocolos recomendado por el ITU-T (*International Telecommunication Union*) diseñado para permitir transmisiones multimedia en LANs basadas en IP. Fue rápidamente adoptado por fabricantes de equipos para transmitir voz y videoconferencia sobre IP ya que define un modelo básico de llamada con servicios suplementarios (convergencia de voz, vídeo y datos en una sola red) y surgió en el momento adecuado. Forma parte de la serie de protocolos H.32x, los cuales también dirigen las comunicaciones sobre RDSI (H.320), RTC o SS7. Esta familia de protocolos ha ido evolucionando con el tiempo para permitir mejorar las transmisiones de voz y vídeo en LANs y WANs sobre distintos medios. La versión actual data de 2006 y se conoce como H.323v6.

Sus principales características son:
- No garantiza una calidad de servicio (QoS)
- Es independiente de la topología de la red
- Admite pasarelas
- Permite usar más de un canal (voz, vídeo, datos) al mismo tiempo.
- El estándar permite que las empresas añadan funcionalidades, siempre que implementen las funciones de interoperabilidad necesarias.

Los componentes principales del sistema H.323 son:
- **Terminales**: Equipamiento que utilizan directamente los usuarios. Se pueden implementar tanto por *software* (mediante un ordenador) como por *hardware* (dispositivo físico).
- **Guardianes (*GateKeepers*)**: Son el centro de toda organización VoIP y son el equivalente a las centralitas privadas o PBX (*Private Branch eXchange*). Normalmente se implementan por *software*.
- **Pasarelas (*Gateways*)**: Hacen de enlace con la red telefónica conmutada, actuando de forma transparente para el usuario.
- **Unidades de Control Multipunto (MCUs)**: se encargan de gestionar las multi-conferencias.

Los principales protocolos utilizados son:
- **RAS** (Registro, Admisión, Situación): Se utiliza sólo en zonas que tengan un guardián para la gestión de la zona de control del mismo.
- **H.225**: Mensajes de establecimiento y finalización de llamada entre terminales o con el guardián.
- **H.245**: Mensajes de control extremo a extremo. Negociación de las capacidades de ancho de banda (mensajes *TerminalCapabilitySet*), de la apertura y cierre de los canales lógicos (mensajes *OpenLogicalChannel*, *CloseLogicalChannel* y *EndSessionComand*), de los códecs y mensajes de control de flujo.
- **RTP/RTCP** (*Real-Time Transport Protocol / Real-Time Transport Control Protocol*): Transporte punto a punto de datos en tiempo real.

Componentes

Terminal

Un terminal es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal, con una pasarela (*gateway*) o con una unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, vídeo y/o datos entre los dos terminales. Conforme a la especificación, un terminal debe proporcionar audio (voz) y opcionalmente puede proporcionar más canales de audio (por ejemplo para emitir en varios idiomas), datos o vídeo. Además del códec de audio puede disponer de un códec específico para voz humana.

Generalmente el terminal receptor se encarga de incluir el retardo necesario en las tramas para obtener una buena sincronización. Por ejemplo retardando las tramas de audio para mantener la sincronización con las tramas de vídeo.

Un terminal H.323 consta de:

- Interfaces de usuario: cámaras, monitores, micrófonos, aplicaciones de datos...
- Códecs de vídeo (opcional) y audio.
- Canal de datos.
- Unidad de control que gestiona de los protocolos RAS, H.245 y H.225.
- Capa H.225 para definición de mensajes.
- Interfaz con la red por paquetes.

Guardián (*Gatekeeper*)

La función del guardián es gestionar una "zona de control" que consiste en un conjunto de equipos registrados (terminales, pasarelas y MCUs). Para las comunicaciones entre el guardián y los equipos de su zona se utiliza el protocolo RAS (Registro, Admisión, Situación).
Las funciones principales del guardián son:

- Gestión de la zona: Lleva a cabo el registro y la admisión de los equipos de su zona.
- Traducción de direcciones E.164: Existen varias formas de asignar direcciones E.164 a terminales H.323, siendo la más universal la asignación de números de extensión.
- Gestión del ancho de banda: Asignación de ancho de banda a terminales, pasarelas y MCUs, de manera que se garantice ancho de banda suficiente, o rechazo de la conexión (red saturada).

El guardián puede también ofrecer otros servicios de control:

- Restricciones de uso: Por tipo de conexión (entrante o saliente), por pasarela, por franjas horarias.
- Localización de las pasarelas: Si existen varias pasarelas registradas, encamina las conexiones salientes por la pasarela más conveniente (generalmente elige en base al coste una pasarela a telefonía móvil o fija en distintas ciudades o países...).

Un ejemplo de guardián es GNU Gatekeeper (GnuGk).

Pasarela (*Gateway*)

Una pasarela es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales de la red IP y otros terminales o pasarelas en una red conmutada. Además de realizar la conversión de protocolo puede realizar opcionalmente una conversión de formatos de audio y vídeo (transcodificación).
Una organización puede disponer de pasarelas a redes de telefonía móvil y de telefonía fija distribuidas por todo el mundo de tal manera que una llamada a la red convencional se realice desde la pasarela más conveniente.

Un ejemplo de pasarela (y guardián) es Asterisk (es tanto pasarela como PBX completo tanto para H.323 como SIP).

MCU (*Multipoint Control Unit*)
Para conectar dos o más terminales -para realizar una llamada o una vídeoconferencia- hace falta una Unidad de Control Multipunto (MCU).
Una MCU comprende dos unidades lógicas:

- Controlador Multipunto (MC: *Multipoint Controller*): gestiona las conexiones y se encarga de realizar la negociación entre los terminales para determinar las capacidades comunes para el proceso de audio y vídeo.
- Procesador Multipunto (MP: *Multipoint Processor*): mezcla, conmuta y procesa los diferentes canales de audio, vídeo y/o datos y los enviar a los participantes.

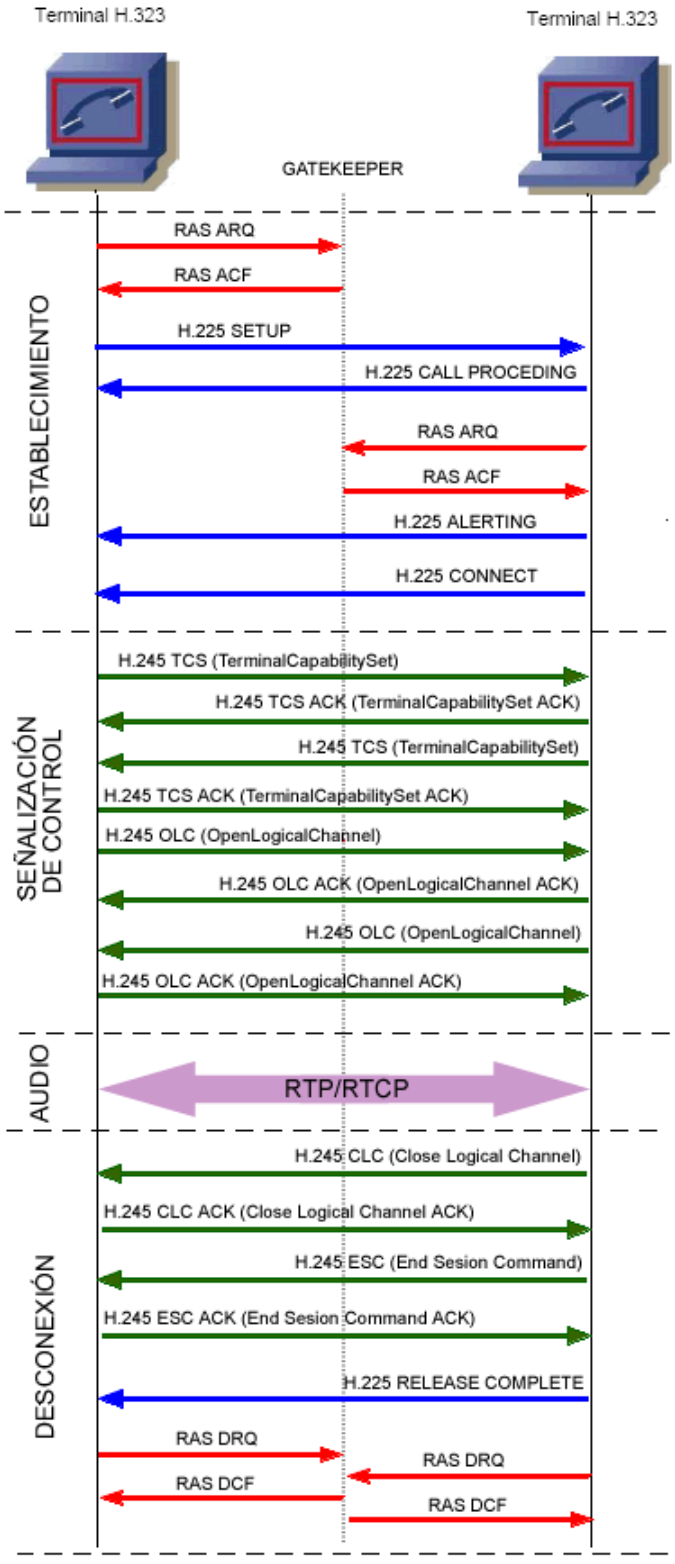
Las MCUs no son la única forma de realizar conferencias multipunto. Una alternativa muy interesante la constituye el uso de transmisión multicast, por ejemplo mediante el uso de la red MBone de Internet. En este caso en vez de encargarse un equipo de replicar los flujos de audio-vídeo es la propia red (más concretamente los encaminadores) la que se ocupa de replicar los paquetes en los puntos donde se producen las bifurcaciones del árbol multicast. Los estándares H.323 no contemplan la transmisión multicast, por lo que los terminales H.323 no pueden participar en este tipo de conferencias.
Existe una gran cantidad de usuarios que no tienen acceso a la red MBone, bien porque su proveedor de acceso no soporta encaminamiento multidifusión o porque la velocidad de su conexión no hace viable o interesante activar encaminamiento multicast. La solución es instalar en la red multicast una pasarela bidireccional que convierta el flujo multicast en flujos unicast y viceversa, generando un flujo diferente para cada usuario unicast. Los flujos unicast pueden ser transcodificados o no.
Desde el punto de vista de eficiencia la pasarela debería estar en el borde de la red multicast y tan cerca como sea posible de los usuarios unicast, ya que de este modo se aprovecha al máximo la optimización que supone la transmisión multicast.

Otro elementos
Los proveedores de servicios pueden tener dentro de su red cientos de pasarelas, teléfonos, terminales multimedia... En esos casos es útil dividir la red en zonas, por ejemplo por ciudades. A un conjunto de zonas controladas por una sola organización se le llama “dominio administrativo”.
Dentro de un dominio administrativo puede existir elementos llamados de borde o de frontera (*Border element*) que centralizan las comunicaciones con elementos de borde de otros dominios administrativos. Estas comunicaciones pueden incluir autorizaciones de acceso, información de costes de conexión y uso, y otros datos de gestión.
Además, dentro de un dominio pueden existir elementos (*Peer elements*) que ayuden a propagar a los guardianes la información útil sobre los elementos de bordes del propio dominio y de otros dominios.

Ejemplo de llamada H.323

(http://www.voipforo.com/H323/H323ejemplo.php)

A continuación se analizará detalladamente una llamada. Cada protocolo se muestra de un color diferente.



Una llamada H.323 se caracteriza por las siguientes fases:

1. ESTABLECIMIENTO
- Uno de los terminales se registra en el guardián utilizando el protocolo RAS (mensajes ARQ y ACF).
- Mediante el protocolo H.225 se manda un mensaje de inicio de llamada (*SETUP*) con los datos (IP y puerto) de llamante y llamado.
- El terminal llamado contesta con *CALL PROCEEDING*.
- El segundo terminal tiene que registrarse con el guardián de manera similar al primer terminal.
- *ALERTING* indica el inicio de generación de tono.
- *CONNECT* indica el comienzo de la conexión.

2. SEÑALIZACIÓN DE CONTROL
- Se abre una negociación mediante el protocolo H.245, para establecer quién será maestro y quién esclavo, las capacidades de los participantes y los códecs de audio y vídeo a utilizar. Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

3. AUDIO (+ DATOS y/o VÍDEO)
Los terminales inician la comunicación y el intercambio de audio (+ datos y/o vídeo) mediante RTP/RTCP.

4. DESCONEXIÓN
- Cualquiera de los participantes activos puede iniciar el proceso de finalización de llamada mediante mensajes *CloseLogicalChannel* y *EndSessionComand* de H.245.
- Posteriormente utilizando H.225 se cierra la conexión con el mensaje *RELEASE COMPLETE*
- Por último se liberan los registros con el guardián utilizando mensajes del protocolo RAS.

10.3. Protocolo SIP

Introducción

El protocolo SIP se concentra en el establecimiento, modificación y terminación de las sesiones. Se complementa, entre otros, con el SDP, que describe el contenido multimedia de la sesión, por ejemplo qué direcciones IP, puertos y códecs se usarán durante la comunicación. También se complementa con RTP (*Real-time Transport Protocol*), que es el verdadero portador del contenido de voz y vídeo que intercambian los participantes en una sesión establecida por SIP.

Aunque originalmente SIP tenía como objetivo la simplicidad, en su estado actual se ha vuelto tan complejo como H.323. El protocolo SIP permite el establecimiento de sesiones multimedia, implementa funciones típicas de telefonía (llamar a un número, provocar que un teléfono suene al ser llamado, escuchar la señal de tono o de ocupado), permite el establecimiento de sesiones multipunto, permite que un usuario esté registrado en diferentes ubicaciones (pudiendo realizar la búsqueda en paralelo o secuencial entre todas ellas).

SIP es similar a HTTP, comparte muchos códigos de estado (como 404: “no encontrado”) y comparte con él algunos de sus principios de diseño: es legible por humanos y sigue una estructura de petición-respuesta basado en el modelo cliente-servidor. Las respuestas llevan un código de estado que brindan información acerca de si las peticiones fueron resueltas con éxito o si se produjo un error. La petición inicial y todas sus respuestas constituyen una transacción.

Aunque dos terminales SIP puedan comunicarse sin intervención de infraestructuras SIP (razón por la que el protocolo se define como punto-a-punto o entre pares -p2p-), este enfoque es impracticable para un servicio público. En ese caso requiere de servidores intermediarios (*proxy*), elementos de registro y servidores de localización (DNS), utilizando un núcleo de red sencillo (y altamente escalable) con inteligencia distribuida en los extremos de la red, incluida en los terminales (ya sea mediante *hardware* o *software*).

El protocolo SIP diferencia entre dirección física (denominada "dirección de contacto"), que depende de la IP desde la que se conecte el usuario, y dirección lógica que es invariable para cada usuario. Al igual que en el correo-e, las direcciones lógicas de SIP tienen la forma usuario@dominio, gestionando cada dominio una compañía o proveedor de servicios de comunicaciones a través de un servidor (o varios).
Es habitual también, que exista un servidor que reciba las peticiones originadas por los usuarios de un dominio hacia otros dominios. Este recibe el nombre de Servidor Saliente.

Los principales elementos del sistema SIP son:

- Agentes de Usuario (Terminales)
- Servidores de Registro (*Registrar*)
- Servidores Intermediarios (*Proxys*)
- Servidores de Redirección (*Redirectors*).

Componentes

Agentes de Usuario (Terminales)

Son los puntos extremos del protocolo, es decir son los que emiten y consumen los mensajes del protocolo SIP. Un videoteléfono, un teléfono, un cliente de software (*softphone*) y cualquier otro dispositivo similar es para el protocolo SIP un agente de usuario.
Todos los agentes de usuario se comportan como clientes (UAC: *User Agent Clients*) y como servidores (UAS: *User Agent Servers*).

Algunos terminales por software que soportan charlas de audio y vídeo a través de SIP son Microsoft Windows Messenger, Apple iChat, AOL Instant Messenger, Ekiga, OpenWengo...

Servidores de Registro (*Registrar*)

Al iniciarse el agente de usuario SIP envía una petición con el método *REGISTER* a un Servidor de Registro, informando a qué dirección física debe asociarse la dirección lógica del usuario (*binding*). Esta asociación tiene un período de vigencia y si no es renovada, caduca. También puede terminarse mediante el método *DEREGISTER*.
El protocolo SIP no determinada la forma en que se debe gestionar los registros.

Servidores Intermediarios (*Proxy*) y de Redirección (*Redirectors*)

Para encaminar un mensaje entre un UAC y un UAS normalmente se recurre a los servidores (aunque puede utilizarse una estrategia tipo p2p). Estos servidores a su vez se sirven del sistema DNS para localizar los dominios y pueden actuar de dos maneras:

a) Como intermediario, encaminando el mensaje hacia destino
b) Como redirector, generando una respuesta que indica al remitente la dirección del destino o de otro servidor que lo acerque al destino.

La principal diferencia es que el servidor intermediario forma parte de la comunicación, mientras que el servidor de redirección una vez que indica al UAC cómo encaminar el mensaje ya no interviene más.

Un mismo servidor puede actuar como redirector o como intermediario dependiendo de la situación.

Esquema de comunicación

En este ejemplo se utiliza servidores, no un sistema entre pares (p2p).

- Un usuario indica a su terminal la dirección lógica de la persona con la que quiere comunicarse.
- El agente de usuario SIP actuando como UAC envía la petición (en este caso con el método *INVITE*) bien al servidor de registro local (si la llamada es a un miembro del mismo dominio) bien al servidor intermediario que tiene configurado como servidor saliente.
  - El servidor intermediario se vale del sistema DNS para determinar la dirección del servidor SIP del dominio del destinatario. Una vez obtenida la dirección del servidor del dominio destino, encamina hacia allí la petición.
- El servidor del dominio destino se vale de la información de registro de dicho usuario para establecer su ubicación física. Si la encuentra encamina la petición hacia dicha dirección.
- El agente de usuario destino, si se encuentra desocupado, comenzará a alertar al usuario destino y enviará una respuesta hacia el usuario llamante (código 180) que sigue el camino inverso de la comunicación. Cuando el usuario destinatario finalmente acepta la invitación, se genera una respuesta con un nuevo código de estado (200) cuya recepción es confirmada por el UAC llamante mediante el método *ACK*.
- Cuando cualquiera de las partes terminar la sesión, actuando como UAC, envía una petición con el método *BYE*.

Normalmente la petición con el método *INVITE* lleva un cuerpo donde viaja una descripción de la sesión que quiere establecer, esta descripción es realizada con el protocolo SDP. En ella se indica el tipo de contenido a intercambiar (voz, vídeo, etc.) y sus características (códecs, direcciones, puertos donde se espera recibirlos, velocidades de transmisión, etc.). Esto se conoce como "oferta de sesión SDP". La respuesta a esta oferta viaja, en este caso, en el cuerpo de la respuesta definitiva a la petición con el método *INVITE*. La misma contiene la descripción de la sesión desde el punto de vista del destinatario. Si las descripciones fueran incompatibles la sesión debe terminarse (mediante una petición con el método *BYE*).

11. VÍDEO-DIFUSIÓN Y VÍDEO BAJO DEMANDA

Los servicios de vídeo-difusión y vídeo bajo demanda se caracterizan por disponer de los contenidos multimedia previamente comprimidos en servidores. De esta forma el proceso de compresión puede realizarse en diferido con la optimización y compresión óptima.

Los servicios de vídeo-difusión son de tipo multidifusión (*multicast*), de forma que diferentes usuarios pueden seguir la misma emisión, lo que produce un ahorro de recursos. El uso de multidifusión es especialmente adecuado en LAN por su gran ventaja y sencilla implementación.
Los servicios de vídeo bajo demanda requieren el envío de la información en modo monodifusión (*unicast*), ya que se pretende que el receptor tenga un control total sobre el flujo generado, pudiendo por ejemplo parar la imagen o retroceder.

Los algoritmos de compresión preferidos para este tipo de servicio son los MPEG, ya que permiten conseguir una eficiencia máxima a cualquier caudal. Para caudales reducidos (0,8 Mb/s e inferiores) el más adecuado es MPEG-4, pudiéndose utilizar MPEG-2 para obtener una mayor calidad cuando el caudal disponible es de 2 Mb/s o mayor. Debemos tener en cuenta que el uso de MPEG-4 o MPEG-2 requiere una estación decodificadora potente.
MPEG-1 es una opción interesante para valores intermedios ya que es menos exigente.

En general es aconsejable mantener los caudales utilizados por debajo del 85% del caudal nominal de la conexión para dar cabida a la información de control que acompaña el tráfico de la aplicación.

La distribución de vídeo en directo es otra aplicación de las redes multimedia. En este caso si se utilizan los algoritmos de compresión MPEG es necesario disponer de un códec hardware para poder realizar la compresión en tiempo real, y aun en ese caso el retardo introducido por el proceso de compresión es apreciable. Otra opción es utilizar algoritmos más sencillos con menor compresión.

Diferencias entre vídeo-difusión y vídeo-conferencia:

	Vídeo-Difusión / Vídeo bajo demanda	**Vídeo-Conferencia**
Codificación	MPEG-1, MPEG-4	H.263
Caudal típico	750-1500 Kb/s	128-384 Kb/s
Retardo	4-5 s	200 ms
Fluctuación del retardo (*Jitter*)	5-6 s	20-70 ms

La vídeo-conferencia es más exigente con la Calidad de Servicio que la vídeo-difusión.

12. ANEXO I – Cortafuegos

Un cortafuegos es un elemento de monitorización y control del tráfico entre redes. Para poder realizar su función, todo el tráfico de entrada o salida debe de atravesarlo.

La función más básica y fundamental de un cortafuegos es determinar qué tramas deben transitar de una red a otra. El filtrado se basa en un conjunto de reglas ordenadas y políticas definidas por el administrador. Las acciones más generales son: aceptar la trama, rechazarla, registrarla, reenviarla o invocar tareas de autenticación. Además la mayoría de los cortafuegos permite realizar funciones de NAT y de pasarela IP.
El orden de aplicación de las reglas es fundamental.
Las políticas principales indican si las tramas que no encajan en ningún regla de aceptación o rechazo deben ser aceptadas o rechazadas. La política más segura, y más difícil de configurar, es la de rechazar todo lo que no sea aceptado expresamente.
El reenvío de tramas permite la instalación en la red de servidores intermediarios transparentes. Así por ejemplo se pueden redirigir todas las peticiones web a un intermediario web (Web Proxy) o filtrar todo el correo con herramientas antivirus y/o antispam, sin necesidad de configurar nada en los clientes e incluso sin que éstos se enteren.

Los cortafuegos más básicos filtran paquetes a nivel 3 y a nivel 4 (existen encaminadores con capacidades de filtrado a nivel 3, pero no se pueden considerar cortafuegos). También existen cortafuegos extendidos que trabajan a nivel de aplicación (nivel 7) y pueden añadir cifrado, autenticación y traducción de direcciones.
Estos cortafuegos extendidos utilizan más información para posibilitar un mayor refinamiento en la definición de los objetos a proteger. Esta nueva información se divide en:

- Información relativa al paquete en niveles superiores de la arquitectura; niveles del 4 al 7 (OSI).
- Información del estado actual y pasado de la comunicación.
- Información del estado actual y pasado de las aplicaciones.

Como ejemplo de filtrado basado en información de niveles superiores podríamos hablar de protección de URLs, recursos, ficheros, usuarios, etc. O dentro de la gestión del estado puede supervisarse el orden en el que se realizan los diferentes comandos de una conexión ftp: autenticación, apertura de canales, transferencias, etc.

Se puede ver un ejemplo de configuración de un servidor que actúa de pasarela y cortafuegos (iptables) con intermediario pop3 (P3Scan), antispam (SpamAssassin), antivirus (ClamAV) e intermediario web (Squid) en:
http://www.guimi.net/index.php?pag_id=tec-docs/firewall/fw-instalacion.html

13. ANEXO II – Comandos para la gestión de red

arp

El comando **arp** permite utilizar el protocolo del mismo nombre para resolver equivalencias entre direcciones MAC e IP.

En sistemas POSIX el comando **arp** solo puede ser utilizado por el administrador.

```
# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
maquina01.net2.upv.e     ether   00:09:97:xx:xx:xx   C                     eth1
maquina2.degi.upv.es     ether   00:15:F2:xx:xx:xx   C                     eth1
#
# arp -a
maquina01.net2.upv.es (158.42.222.x) at 00:09:97:xx:xx:xx [ether] on eth1
maquina2.degi.upv.es (158.42.222.x) at 00:15:F2:xx:xx:xx [ether] on eth1
#
# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
158.42.222.x             ether   00:09:97:xx:xx:xx   C                     eth1
158.42.222.x             ether   00:15:F2:xx:xx:xx   C                     eth1
```

```
W:\>arp -a

Interface: 158.42.222.x --- 0x50003
  Internet Address      Physical Address      Type
  158.42.222.x          00-09-97-xx-xx-xx     dynamic
```

- "-a" indica que se muestre toda la tabla.
- "-s" permite añadir una relación estática (`arp -s 192.168.1.1 xx-xx-xx-xx-xx-xx`).
- "-d" permite borrar una relación de la tabla (`arp -d 192.168.1.1`).

dig

dig es una herramienta avanzada de sistemas POSIX que obtiene información sobre consultas y servidores DNS.

```
$ dig guimi.net

; <<>> DiG 9.3.4-P1.1 <<>> guimi.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62659
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;guimi.net.                     IN      A

;; ANSWER SECTION:
guimi.net.              4345    IN      A       212.36.74.190

;; Query time: 0 msec
;; SERVER: 158.42.250.65#53(158.42.250.65)
;; WHEN: Tue Oct 14 12:39:53 2008
;; MSG SIZE  rcvd: 43

$ dig -x 212.36.74.190
 --> permite hacer búsquedas inversas
```

host

host es una herramienta de sistemas POSIX que obtiene información sobre consultas y servidores DNS.

```
$ host guimi.net
$ host -t MX guimi.net
$ host -a guimi.net
$ host 212.36.74.190
--> Respuestas similares a dig
```

ifconfig

`ifconfig` es un comando de los sistemas POSIX que permite configurar y gestionar las interfaces de red. El comando equivalente en sistemas Windows es **`ipconfig`**.

Este comando permite mostrar información:

```
# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:17:9A:xx:xx:xx
          inet addr:158.42.222.x  Bcast:158.42.222.255  Mask:255.255.255.0
          inet6 addr: fe80::217:9aff:fe39:xxxx/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5563 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3408791 (3.2 MiB)  TX bytes:743314 (725.8 KiB)
          Interrupt:50 Base address:0xe400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:229 errors:0 dropped:0 overruns:0 frame:0
          TX packets:229 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:246518 (240.7 KiB)  TX bytes:246518 (240.7 KiB)
```

- "-a" permite mostrar todos los interfaces, incluyendo los que no están activos.

Permite configurar una interfaz (en todos sus detalles, aquí se muestra un ejemplo simple):

```
# ifconfig eth0 10.0.0.3 netmask 255.0.0.0
```

Permite activar o desactivar una interfaz:

```
# ifconfig eth0 up / down
```

ipconfig

`ipconfig` es un comando de sistemas Windows que muestra información de la configuración TCP/IP en los distintos interfaces del sistema. Además permite renovar o liberar una configuración DHCP o limpiar la caché de DNS. El comando equivalente en sistemas POSIX es **`ifconfig`**.
Los parámetros más interesantes son:

- "/all" muestra toda la información de todos los interfaces, aunque no estén activos.
- "/release" libera la configuración IP recibida por DHCP.
- "/renew" renueva la configuración IP de DHCP.
- "/flushdns" limpia la caché de DNS.

```
W:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : dominio.es
   IP Address. . . . . . . . . . . . : 158.42.222.x
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 158.42.222.250

W:\>
W:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : maquina01
   Primary Dns Suffix  . . . . . . . : upvnet.upv.es
   Node Type . . . . . . . . . . . . : Hybrid
```

```
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : upv.es

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : upv.es
   Description . . . . . . . . . . . : Marvell Yukon 88E8001/8003/8010 PCI Gigab
it Ethernet Controller
   Physical Address. . . . . . . . . : 00-15-F2-xx-xx-xx
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . . . . . . . . : 158.42.222.x
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 158.42.222.250
   DHCP Server . . . . . . . . . . . : 158.42.xxx.x
   DNS Servers . . . . . . . . . . . : 158.42.250.195
                                       158.42.250.65
   Primary WINS Server . . . . . . . : 158.42.250.200
   Secondary WINS Server . . . . . . : 158.42.xxx.x
   Lease Obtained. . . . . . . . . . : martes, 14 de octubre de 2008 9:22:53
   Lease Expires . . . . . . . . . . : jueves, 16 de octubre de 2008 9:22:53
```

nbtscan

`nbtscan` es un comando de los sistemas POSIX que muestra estadísticas de NetBIOS y conexiones de NetBIOS sobre TCP/IP. El comando equivalente en sistemas Windows es **`nbtstat`**.

Los parámetros más interesantes son:

- "-v" indica que muestre una salida con más información (similar a **`nbtstat`**).
- "-h" hace que explique los servicios.

```
$ nbtscan 158.42.222.x
Doing NBT name scan for addresses from 158.42.222.x

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
158.42.222.x     MAQUINA01        <server>  <unknown>        00:15:f2:xx:xx:xx

$
$ nbtscan -v 158.42.222.x
Doing NBT name scan for addresses from 158.42.222.x


NetBIOS Name Table for Host 158.42.222.x:

Name             Service          Type
---------------------------------------
MAQUINA01        <00>             UNIQUE
MAQUINA01        <20>             UNIQUE
UPVNET           <00>              GROUP
UPVNET           <1e>              GROUP
UPVNET           <1d>             UNIQUE
__MSBROWSE__  <01>              GROUP

Adapter address: 00:15:f2:xx:xx:xx
---------------------------------------

$
$ nbtscan -vh 158.42.222.x
Doing NBT name scan for addresses from 158.42.222.x


NetBIOS Name Table for Host 158.42.222.x:

Name             Service          Type
```

```
----------------------------------------
MAQUINA01        Workstation Service
MAQUINA01        File Server Service
UPVNET           Domain Name
UPVNET           Browser Service Elections
UPVNET           Master Browser
__MSBROWSE__  Master Browser

Adapter address: 00:15:f2:xx:xx:xx
----------------------------------------
```

nbtstat

nbtstat es un comando de lo sistemas Windows muestra estadísticas de NetBIOS y conexiones de NetBIOS sobre TCP/IP. El comando equivalente en sistemas POSIX es **nbtscan**.
Los parámetros más interesantes son:

- "-n" indica que muestre la tabla de nombres del equipo local.
- "-c" indica que utilice la caché del equipo local.
- "-r" verifica que los nombres NetBIOS se resuelven correctamente mediante WINS.
- "-a nombre" o "-A dirección_IP" indica que utilice la tabla de nombres de un equipo remoto.

```
W:\>nbtstat -n

Local Area Connection:
Node IpAddress: [158.42.222.x] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    MAQUINA01      <00>  UNIQUE      Registered
    MAQUINA01      <20>  UNIQUE      Registered
    UPVNET         <00>  GROUP       Registered
    UPVNET         <1E>  GROUP       Registered
    UPVNET         <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered




W:\>nbtstat -c

Local Area Connection:
Node IpAddress: [158.42.222.x] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    TYNDAREUS      <20>  UNIQUE          158.42.250.x        587
    JUNO.UPVNET.UPV<2E>  UNIQUE          158.42.250.x        467

W:\>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 0
    Resolved By Name Server   = 4608

    Registered By Broadcast   = 0
    Registered By Name Server = 12
```

net

El comando net es uno de los más complejos por la cantidad de opciones diferentes que ofrece, tanto en sistemas Windows como POSIX. En el caso de Windows agrupa 22 comandos de gestión de redes Windows (net share, net use...). En el caso de POSIX es una herramienta para administrar servidores Samba y CIFS que en realidad agrupa 19 comandos (net time, lookup, user, group, sam, ...) de forma similar al comando de Windows.

```
W:\>net
NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

Algunos de los más interesantes son:

```
W:\>net share         <-- Permite ver y modificar los recursos compartidos del sistema

Share name   Resource                        Remark
------------------------------------------------------------------------------
C$           C:\                             Default share
ADMIN$       C:\WINDOWS                      Remote Admin
IPC$                                         Remote IPC
D$           D:\                             Default share
The command completed successfully.
```

```
W:\>net use           <-- Permite ver y modificar las conexiones del sistema
New connections will be remembered.

Status       Local     Remote                    Network
-------------------------------------------------------------------------------
OK           W:        \\maquina01\guimi         Microsoft Windows Network
Disconnected X:        \\maquina02\guimi         Microsoft Windows Network
The command completed successfully.
```

```
W:\>net start/stop           <-- Permiten iniciar/parar o ver los servicios iniciados del sistema
These Windows services are started:
[...]
   Workstation
The command completed successfully.
```

netdiag

`netdiag` es un comando de sistemas Windows que no se instala por omisión, pero está disponible en el paquete "*Resource kit*". Permite realiza una serie de pruebas para determinar el estado y la funcionalidad de la red del equipo.

```
netdiag [/q] [/v] [/l] [/debug] [/d:nombreDeDominio] [/fix] [/dcaccountenum] [/test:nombreDePrueba]
[/skip:nombreDePrueba]
```

Algunas pruebas interesantes son: Bindings, DcList, DefGw, DNS, IPSec, Kerberos, Route...

```
netdiag /test:ipsec
```

netsh

`netsh` en sistemas Windows permite de forma interactiva o por parámetros configurar la red de un equipo, incluyendo las interfaces, el cortafuegos, los sistemas ras, wins, dhcp...

```
W:\>netsh
netsh>help
<-- Se han eliminado la mayoría de lineas de ayuda -->
add            - Adds a configuration entry to a list of entries.
firewall       - Changes to the `netsh firewall' context.
interface      - Changes to the `netsh interface' context.
show           - Displays information.

The following sub-contexts are available:
```

```
 aaaa bridge dhcp diag firewall interface ipsec ras routing rpc wins winsock

netsh>quit
```

netstat

`netstat` muestra estadísticas de uso de TCP-UDP/IP y sus conexiones. Este comando tiene muchas opciones que además varían de sistemas Windows a sistemas POSIX.
En sistemas Windows los parámetros más interesantes son:

- "-a" muestra las conexiones y los puertos de escucha.
- "-r" muestra la tabla de encaminamiento (igual que el comando **`route print`**).
- "-e" muestra estadísticas de Ethernet.
- "-s" muestra estadísticas por protocolo.

```
W:\>netstat -s

IPv4 Statistics

  Packets Received                   = 31097937
[...]
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics
[...]
TCP Statistics for IPv4
[...]
UDP Statistics for IPv4
[...]


W:\>netstat -e
Interface Statistics
                           Received            Sent
Bytes                    3987777529       651861703
Unicast packets            30617810        32440422
Non-unicast packets          136910            9869
Discards                          0               0
Errors                            0               0
Unknown protocols             26122

W:\>
W:\>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       9924
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       784
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       1296
[...]
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    476
[...]
```

En sistemas POSIX los parámetros más interesantes son:

- "-p" muestra el PID del programa al que pertenece el *socket*.
- "-u" muestra datos de UDP.
- "-t" muestra datos de TCP.
- "-a" muestra todos los *sockets*, los que están a la escucha y los que no.

```
$ netstat -puta
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:2208          *:*                     LISTEN      -
tcp        0      0 *:vmware-authd          *:*                     LISTEN      -
[...]
tcp6       0      0 *:www                   *:*                     LISTEN      -
tcp6       0      0 *:ssh                   *:*                     LISTEN      -
[...]
udp        0      0 *:sunrpc                *:*                                 -
udp        0      0 *:ipp                   *:*                                 -
```

Además en sistemas POSIX **`netstat`** sustituye a nivel de usuario a otros comandos que son propios del superusuario. Por ejemplo `route`:

```
$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
158.42.xxx.0    0.0.0.0         255.255.255.0   U         0 0          0 eth1
0.0.0.0         158.42.xxx.250  0.0.0.0         UG        0 0          0 eth1
```

O `ifconfig`:

```
$ netstat -inet
Kernel Interface table
eth1      Link encap:Ethernet  HWaddr 00:17:9A:xx:xx:xx
          inet addr:158.42.xxx.x  Bcast:158.42.xxx.255  Mask:255.255.255.0
          inet6 addr: fe80::217:9aff:fe39:xxxx/64 Scope:Link
[...]
```

nmap

`nmap` es un analizador de puertos disponible en sistemas POSIX y Windows.
Ejemplos de uso:

```
$ nmap localhost      <-- Si no se indican puertos con -p analiza [0-1023]

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2008-10-17 14:34 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 1672 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
113/tcp  open  auth
631/tcp  open  ipp
902/tcp  open  iss-realsecure-sensor
3306/tcp open  mysql
5432/tcp open  postgres

nmap finished: 1 IP address (1 host up) scanned in 0.209 seconds$ nmap 192.168.1.1
```

```
$ nmap -sP xxx.xx.xxx.0/24    <-- Busca e identifica equipos en la red

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2008-10-17 14:34 CEST
Host maquina01 (xxx.xx.xxx.1) appears to be up.
[...]
Nmap finished: 256 IP addresses (5 hosts up) scanned in 2.258 seconds
```

nslookup

`nslookup` obtiene información sobre consultas y servidores DNS. Se puede utilizar interactivamente o proporcionando parámetros directamente en la invocación. Se utiliza igual en sistemas Windows y POSIX.

Ejemplo de uso interactivo:

```
W:\>nslookup
Default Server:  juno.cc.upv.es             <-- Nos indica el servidor DNS
Address:  158.42.250.195

> guimi.net                                 <-- Consultamos un dominio
Server:  juno.cc.upv.es
Address:  158.42.250.195
[...]
> set type=MX                               <-- Consultamos un subconjunto de entradas DNS
                                            <-- Podemos indicar: any, MX, NS, CNAME, A, SOA
> guimi.net
[...]
>
> server 213.0.184.85                       <-- Cambiamos el servidor DNS de consulta
Default Server:  85.red-213-0-184.static.ccgg.telefonica.net
Address:  213.0.184.85

> exit                                      <-- Terminamos la utilidad nslookup
```

Ejemplos de uso no interactivo:

```
W:\>nslookup guimi.net
Server:  juno.cc.upv.es
Address:  158.42.250.195

Non-authoritative answer:
Name:    guimi.net
Address:  212.36.74.190

$ nslookup 212.36.74.190
Server:         158.42.250.65
Address:        158.42.250.65#53

Non-authoritative answer:
190.74.36.212.in-addr.arpa      name = hc05.cdmon.com.
[...]
```

pathping

El comando **`pathping`** primero muestra los saltos hacia el destino como **`tracert`**, a continuación ejecuta varios pings hacia cada destino y calcula estadísticas.

Los parámetros más interesantes son:

- "-n" para que no resuelva nombres de máquina.
- "-h" indica la cantidad máxima de saltos.
- "-q" indica el número de pings a enviar a cada nodo.

```
W:\>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using Ipv6.
```

```
W:\>pathping -n guimi.net

Tracing route to guimi.net [212.36.74.190]
over a maximum of 30 hops:
  0  158.42.xxx.x
  1  158.42.xxx.xx
[...]
  8  212.36.74.190

Computing statistics for 200 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          158.42.xxx.x
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  158.42.xxx.xxx
                                 0/ 100 =  0%   |
[...]
  8    7ms     0/ 100 =  0%     0/ 100 =  0%  212.36.74.190

Trace complete.
```

ping

El comando **`ping`** utiliza paquetes "echo" (ping) y "echo reply" (pong) de ICMP para comprobar la conectividad con una IP.

En sistemas Windows "-n" establece el número de paquetes a enviar (por omisión 4).

```
W:\>ping guimi.net -n 1

Pinging guimi.net [212.36.74.190] with 32 bytes of data:

Reply from 212.36.74.190: bytes=32 time=6ms TTL=57

Ping statistics for 212.36.74.190:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

En sistemas POSIX el parámetro "-n" (*numbers*) indica que no resuelva los nombres y muestre solo los números de la dirección y el parámetro "-c" establece el número de paquetes a enviar (por omisión infinitos).

```
$ ping guimi.net -c 1 -n
PING guimi.net (212.36.74.190) 56(84) bytes of data.
64 bytes from 212.36.74.190: icmp_seq=1 ttl=57 time=6.90 ms

--- guimi.net ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.904/6.904/6.904/0.000 ms
```

route

El comando **`route`** permite consultar y gestionar las tablas de encaminamiento de red. Las posibilidades que ofrece son amplias y su sintaxis varía considerablemente de sistemas Windows a sistemas POSIX.

Ejemplos en un sistema POSIX (debe ejecutarse como superusuario):

```
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
158.42.xxx.0    *               255.255.255.0   U     0      0        0 eth1
default         rou-aulasiqn.ne 0.0.0.0         UG    0      0        0 eth1

# route add -net 192.56.76.0 netmask 255.255.255.0 eth0
--> Indica que los paquetes enviados a la red 192.56.76.0/24 salgan por la interfaz eth0

# route add default gw migw
--> Establece como pasarela por defecto "migw"
```

```
# route add -net 10.0.0.0 netmask 255.0.0.0 reject
--> Indica que se rechacen los paquetes con destino 10.0.0.0/8
```

Ejemplos en un sistema Windows:

```
W:\>route print

IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x50003 ...00 15 f2 d0 0c b8 ...... Marvell Yukon 88E8001/8003/8010 PCI Gigabit
Ethernet Controller - Trend Micro Common Firewall Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   158.42.222.250     158.42.222.1     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
[...]
Default Gateway:    158.42.222.250
===========================================================================
Persistent Routes:
  None
```

```
C:\> route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
             destination^      ^mask      ^gateway     metric^    ^
                                                       Interface^
```

tc

`tc` es un comando de sistemas POSIX que permite gestionar el control de tráfico, limitando las capacidades de una interfaz o generando prioridades de tráfico (QoS).

traceroute

`traceroute` es un comando de sistemas POSIX que determina la ruta y los saltos necesarios para alcanzar un destino IP utilizando por omisión paquetes UDP. También puede utilizar paquetes ICMP con el parámetro "-I". El comando equivalente en sistemas WINDOWS es **`tracert`**.
El parámetro "-n" (*numbers*) indica que no resuelva los nombres y muestre solo los números de la dirección.

```
$ traceroute guimi.net
traceroute to guimi.net (212.36.74.190), 30 hops max, 40 byte packets
 1  rou-aulasiqn.net2.upv.es (158.42.222.250)  0.631 ms  0.527 ms  0.521 ms
 2  cauac-1.net2.upv.es (158.42.254.94)  0.234 ms  0.205 ms  0.204 ms
 3  kukulcan.net.upv.es (158.42.255.58)  0.613 ms  0.538 ms  0.683 ms
 4  GE1-0-3.EB-Valencia0.red.rediris.es (130.206.211.153)  1.092 ms  1.011 ms  0.815 ms
 5  VAL.XE0-0-0.EB-Barcelona0.red.rediris.es (130.206.250.45)  15.142 ms  11.206 ms  5.661 ms
 6  adam.01.catnix.net (193.242.98.12)  7.375 ms  6.776 ms  6.758 ms
 7  sw2pp-rc1-dc.adam.es (195.219.118.3)  6.883 ms  7.623 ms  8.799 ms
 8  * * *

$ traceroute guimi.net -n -I
traceroute to guimi.net (212.36.74.190), 30 hops max, 40 byte packets
 1  158.42.222.250  0.674 ms  0.511 ms  0.508 ms
 2  158.42.254.94  8.106 ms  0.335 ms  0.212 ms
 3  158.42.255.58  0.786 ms  0.485 ms  0.341 ms
 4  130.206.211.153  0.802 ms  2.129 ms  15.974 ms
 5  130.206.250.45  7.915 ms  7.992 ms  7.917 ms
 6  193.242.98.12  8.017 ms  9.086 ms  14.754 ms
 7  195.219.118.3  8.104 ms  9.810 ms  6.707 ms
 8  212.36.74.190  7.284 ms  6.463 ms  6.530 ms
```

tracert

tracert es un comando de sistemas Windows que determina la ruta y los saltos necesarios para alcanzar un destino IP utilizando paquetes ICMP y su valor de TTL (*Time To Live*). El comando equivalente en sistemas POSIX es **traceroute**.

```
W:\>tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6]
target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

W:\>tracert guimi.net
Tracing route to guimi.net [212.36.74.190] over a maximum of 30 hops:

[...]
  6     8 ms     7 ms     7 ms  adam.01.catnix.net [193.242.98.12]
  7     7 ms     7 ms     6 ms  sw2pp-rc1-dc.adam.es [195.219.118.3]
  8     6 ms     6 ms     6 ms  hc05.cdmon.com [212.36.74.190]

Trace complete.
```

14. ANEXO III - La VC en el campo educativo

Extracto de “La videoconferencia en el campo educativo. Técnicas y procedimientos.” de Miquel Oliver Ribas, Universidad de las Islas Baleares. (http://www.uib.es/depart/gte/oliver.html).

14.1. Introducción

De entre la multitud de tecnologías de posible aplicación que posibilitan la interactividad en el campo de la formación, la vídeo-conferencia es, sin duda, una de las que mayor futuro tiene en lo referente a enseñanza no presencial, puesto que permite una interacción permanente, en tiempo real, con imagen y sonido entre diferentes puntos, haciendo posible que, diferentes profesores, diferentes alumnos, diferentes centros escolares, etc. participen en el proceso de comunicación.

Enseñar a través de vídeo-conferencia supone, no obstante, un cambio en cuanto a la metodología tradicional aplicada en los sistemas presenciales de enseñanza. Esta nueva tecnología necesita formas distintas de interacción, diferente comportamiento físico, distintas maneras de presentar la información y diferentes formas de juzgar los mensajes que se puedan transmitir en ambas direcciones.

La vídeo-conferencia puede ser punto a punto o multipunto. En el primer caso cada punto dispone de una consola que controla las diferentes funciones: como el movimiento de la cámara, el foco, el sonido, etc y cada lugar observa el otro a través de sus respectivos monitores. En la vídeo-conferencia multipunto no es posible lograr la denominada "presencia continua", es decir, todos los usuarios no pueden verse simultáneamente entre sí. En cada momento dado, sólo se puede ver a una persona.

La mayoría de equipos admiten cámaras auxiliares, de modo que la vídeo-conferencia pueda ser más flexible. La salida de vídeo puede ser conectada a un cañón de proyección y/o a un magnetoscopio, pudiéndose grabar la vídeo-conferencia. Además también pueden compartir datos y trabajar a la vez con un mismo documento, hacer anotaciones sobre él, modificar campos, tomar notas, etc.

14.2. Técnicas de realización

Los distintos elementos que componen un equipo de videoconferencia pueden ser controlados por el mismo conferenciante, o por un equipo de realización formado por técnicos.

Cuando se trata de vídeo-conferencia punto a punto, en la que el conferenciante utiliza pocos medios para complementar su exposición (a veces un solo PC con una cámara) puede controlarlo el mismo conferenciante.
En entornos más complejos, con multipunto, varias cámaras y micrófonos, salas de conferenciantes, etc ..., la realización puede pasar a uno o varios técnicos, que efectúan las conmutaciones de las diferentes cámaras, del sonido y de todos los demás elementos que se vayan a utilizar, así como la selección de la imagen a recibir (en multipunto).
Existen sistemas automatizados que permiten que la conmutación de vídeo se efectúe a través de la voz, de manera que cuando alguien habla, todos los demás participantes ven la imagen del orador en la pantalla. Incluso algunos sistemas permiten enfocar automáticamente la cámara hacia el orador en grandes salas con múltiples participantes.

Aspectos técnicos que hay que prever

- **Pantallas**. Lo ideal es que cada sala disponga de un sistema de vídeo-proyección, de forma que los alumnos presten atención a una sola pantalla.
- **Micrófonos**. Los micrófonos de solapa son los mejores, puesto que ofrecen una mayor libertad de movimiento. Es bueno disponer de uno o más micrófonos para captar el ambiente de la sala y para las intervenciones del público.
- **Cámaras**. En la sala donde se emite la vídeo-conferencia, lo mejor es disponer de dos: una para el profesor y otra para los alumnos presentes. En la sala(s) receptora(s) los alumnos el profesor debe poder ver a los alumnos mediante cámaras instaladas en cada sala. Cuando se trata de una videoconferencia punto a punto, el profesor debe poder controlar de forma remota la cámara de la otra sala.
- **Iluminación**. Es importante cuidar la iluminación. Es recomendable que sea cenital, fría o luz rebotada en superficies blancas. La temperatura de color ideal es de 3.200º K.

14.3. Elementos que el profesor tiene que contemplar

Antes de la vídeo-conferencia

- Planificar y ensayar la presentación.
- Familiarizarse con el equipo y los diferentes medios que utilizará (escáner, retro-proyector, vídeo-presentación...).
- Conseguir que todos los participantes se impliquen.
- Fomentar la interacción informal entre las distintas aulas que participen en la VC:
  - Hacer una introducción personal.
  - Recorrer la sala con la cámara, haciendo panorámica (si es posible).

Durante la vídeo-conferencia

Intentar involucrar a toda la audiencia (participación de alumnos de cada una de las aulas).

Nivel oral.

- Hablar claro e intentar mantener un volumen constante.
- Utilizar a menudo pausas.
- Permitir interrupciones por parte de los participantes.
- Indicar, claramente, cuándo ha terminado de hablar y se está esperando la réplica.

Nivel visual.

- Evitar excesivos movimientos o movimientos bruscos.
- Mantener a la vista los gráficos, imágenes o cualquier otro tipo de material que utilicemos durante un periodo de tiempo más largo de lo habitual. No moverlos una vez posicionados.
- Evitar el uso de imágenes, gráficos, etc. de baja calidad (no utilizar segundas generaciones de vídeo).
- Ir vestido con ropas de colores poco llamativos.
- La persona que quiera intervenir, en primer lugar tiene que esperar a que la cámara lo encuadre y enfoque, en segundo lugar tiene que identificarse.
- Utilizar diferentes medios para atraer la atención (transparencias, diapositivas, vídeo, etc.)

Después de la vídeo-conferencia

Una vez terminada la vídeo-conferencia evaluar la experiencia. Desde el punto de vista pedagógico, la evaluación comportaría dos vertientes: evaluación de la experiencia tecnológica, de la metodología empleada y del profesorado -por parte del alumno-, y evaluación de la eficacia del aprendizaje, -por parte del profesor o profesores-.