Sistemas de Transporte de Datos (9186)
Ingeniería en Informática (plan 2001)

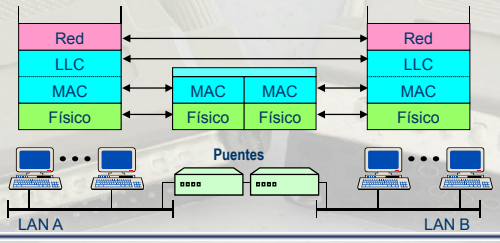
Bloque IV. Interconexión de Redes

Francisco Andrés Candelas Herías
Santiago Puente Méndez
Grupo de **I**nnovación **E**ducativa en **A**utomática (GITE-UA)

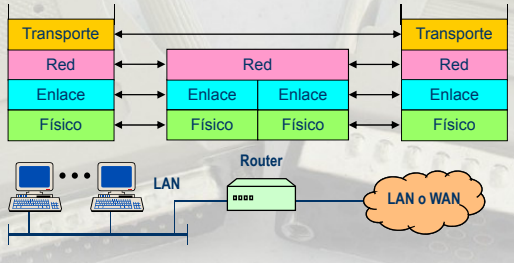
Universitat d'Alacant
Universidad de Alicante

Departament de Física, Enginyeria de Sistemes i Teoria del Senyal
Departamento de Física, Ingeniería de Sistemas y Teoría de la Señal

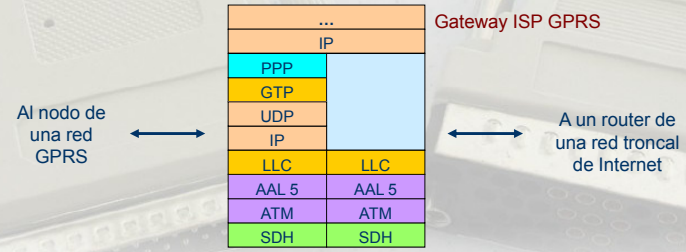
- Interconexión de redes
  - Interconexión de LANs:
    - Repetidores y hubs. Varios segmentos de red se unen en una misma LAN.
    - Puentes (bridges), conmutadores (switches), APs 802.11.
      - Conectan LANs del mismo tipo, con igual enlace (salvo APs).
      - Encaminan tramas a nivel de enlace, ampliando este nivel.
      - Puentes transparentes normales: conexión directa de LANs.
      - Puentes transparentes remotos: conexión de LANs a través de una WAN.



- Interconexión de redes
  - Interconexión de LANs:
    - Routers.
      - Permite conectar redes y LANs de diferentes tipos (diferente nivel de enlace), compartiendo un mismo nivel de red (típicamente IP).
      - Encaminamiento de paquetes de nivel de red.
      - Con túneles se pueden conectar equipos remotos a nivel de enlace.



- Interconexión de redes
  - Interconexión de LANs con WANs:
    - Pasarelas (gateways).
      - Permiten conectar redes a niveles superiores al de red.
      - Permiten intercomunicar redes con arquitecturas diferentes.
      - Usadas en conexión a Internet de proveedores de accesos ADSL, cable-módem y datos por telefonía móvil.



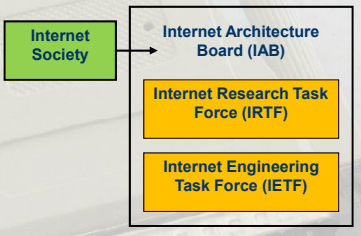
- Interconexión de redes
  - El protocolo usado por excelencia para la interconexión de redes con routers es IP. Hay dos versiones de IP:
    - IP (IPv4). Desde los orígenes hasta la actualidad.
    - IPv6. Nueva versión que está comenzado a funcionar.
  - IPv6 está en expansión:
    - Los routers y los S.O. actuales ya incorporan IPv6.
    - De momento, IPv6 se usa sobre todo en la interconexión de redes troncales, y a nivel de usuario final se emplea poco.
    - IPv6 es muy diferente de IPv4, y deben coexistir los dos protocolos.
  - Otra tecnología con éxito es MPLS (Multiprotocol Label Switching)
    - Trata de unificar características de datagramas y circuitos virtuales.
    - Se usa para enviar datagramas IPv4 sobre redes de circuitos virtuales.

17. Arquitecturas de Interconexión.
18. Versión 6 de IP.
19. MPLS.

- Problemas de IPv4.
- Origen.
- Características.
- Formato de los paquetes.
- Direccionamiento.
- ICMPv6.
- Despliegue.
- Normativas.

- Problemas de IPv4.
  - Dirección de 4 bytes: rango de direcciones muy limitado.
    - Se requiere el uso de NAT, que no funciona bien con algunos servicios (P2P, VoIP, juegos...).
    - Mala distribución de direcciones.
    - Tablas de encaminamiento complejas.
  - El encaminamiento de datagramas es complejo.
  - Difícil gestión de hosts móviles.
    - Si un equipo cambia de ubicación (aunque no de dirección), se requieren cambios en las tablas de encaminamiento de la red.
  - No es adecuado para tráfico de flujo de datos constante.
    - TCP: servicio fiable, pero muy costoso.
    - UDP: servicio ligero, pero no es fiable. Entrega desordenada.

- Origen.
  - Gestión de Internet.
    - Son varias las organizaciones que normalizan las tecnologías de Internet.
    - Las normas de Internet (RFC) siguen un proceso de aprobación.

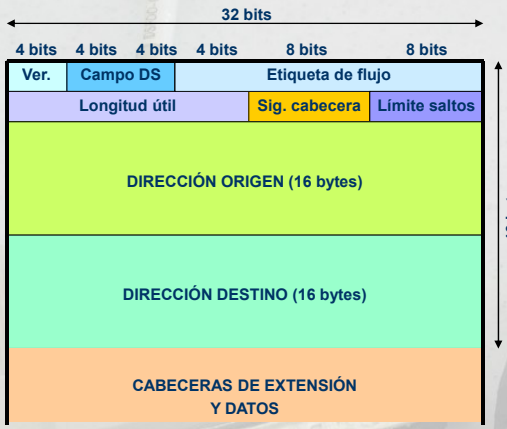


- Origen.
  - El IETF encargó una propuesta de opciones para la nueva versión. Destacaron dos opciones:
    - CLNP, basado en IP, pero fiel al modelo OSI. No gustó a los seguidores más fieles de IP.
    - SIPP (Simple Improved Internet Protocol). Se escogió esta, con modificaciones.
  - La nueva versión se numeró como 6 (IPv6), porque la versión 5 ya estaba definida como protocolo experimental para transmisión de señales digitales.
  - IPv6 fue aceptado por el IETF en 1994. Inicialmente se le llamó IPng (IP Next Generation).

- Características.
  - No es compatible con IPv4; IPv4 e IPv6 son muy diferentes.
  - Acepta los protocolos de transporte clásicos: TCP y UDP.
  - Emplea un nuevo formato de mensajes ICMP (ICMPv6).
  - Usa direcciones de 16 bytes (128 bits) y define un direccionamiento más flexible que IPv4.
  - La cabecera básica de un datagrama IPv6 es muy simple y de tamaño fijo.
  - Se puede ampliar la funcionalidad con cabeceras de extensión.
  - Con IPv6, la fragmentación solo se realiza en el equipo origen, y no en los routers de la red.

- Características.
  - Plantea mecanismos de seguridad internos al protocolo para autentificación y encriptación de los datos (no es necesario IPSec).
  - Soporta, además de datos, tráfico de flujo constante.
  - Dispone de opciones avanzadas para la gestión de la calidad de servicio (QoS).
  - Soporta dos modelos de gestión de QoS: DS e IS.
  - Implica menos trabajo en los routers y aumenta la eficiencia de la red.
  - Las últimas definiciones dan soporte para hosts móviles: los equipos pueden cambiar de red manteniendo su dirección.
  - Permite utilizar datagramas de más de 64Kbytes (Jumbogramas).

- Formato de los paquetes.



Versión: identifica si el datagrama es de IPv4 o IPv6.

DS (Differentiated Services): para clasificar los datos y aplicar QoS.

Etiqueta de flujo: para identificar todos los paquetes de un flujo de datos.

Longitud útil: número de bytes de datos (hasta 64KB), sin contar cabeceras.

Siguiente cabecera: identifica la primera cabecera de extensión, o el protocolo de nivel superior (ICMP, TCP, UDP…).

Limite de saltos: como el TTL de IPv4.

- Formato de los paquetes.
  - DS (Differentiated Services).
    - Ultima definición en RFC 2474.
    - Sirve para clasificar tipos diferentes de paquetes y establecer Control de Calidad de Servicio (QoS).
    - Con IPv4 también se utiliza hoy en día el campo DS, que sustituye al de ToS.
    - SI vale 0: simplemente hay que enviar el paquete sin control adicional, lo antes que la red pueda según su capacidad.

DSCP (DS Code-Point). Define 64 tipos de tráfico organizados en 8 categorías que se corresponden a los 8 valores de precedencia IPv4.

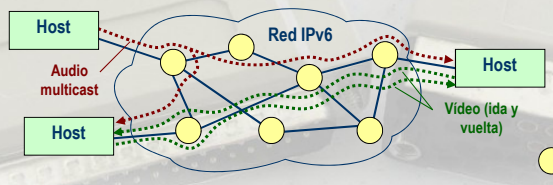
ECN (Explicit Congestion Notification). Para control de congestión y descarte de paquetes (RFC 3168).

- Formato de los paquetes.
  - DS (Differentiated Services).
    - Categorías de DSCP.
      - Los tres bits de mayor peso del campo DSCP de IPv6 se corresponden con los tres bits de precedencia del campo TOS de IPv4

Categorías (Bin)	Categorías (Dec)	Precedencia IPv4 equivalente	Significado
000 xxx	0 – 7	0	Mejor esfuerzo (valor por defecto)
001 dd0	8 – 15	1	Assured Forwarding (AF) clase 1
010 dd0	16 – 23	2	Assured Forwarding (AF) clase 2
011 dd0	24 – 31	3	Assured Forwarding (AF) clase 3
100 dd0	32 – 39	4	Assured Forwarding (AF) clase 4
101 xxx	40 – 47	5	Expedited Forwarding (EF)
110 xxx	48 – 55	6	Control de la red
111 xxx	56 – 63	7	Control de la red

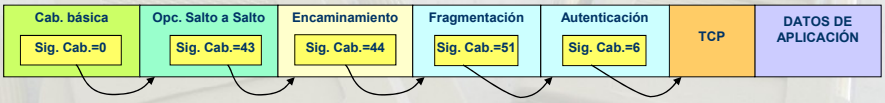
- Formato de los paquetes.
  - DS (Differentiated Services).
    - Categorías de DSCP.
      - Best Effort. Simplemente se reenvían los paquetes lo antes posible.
      - Assured Forwarding (AF). Aunque ofrece un trato preferente en la transmisión de datos, no ofrece garantías.
        - Se definen cuatro clases: 1 a 4 (4 es la más alta).
        - Cada clase AF tiene 3 opciones de descarte según bits “dd” (valores 1,2, 3). 0 significa no descartable.
        - Un tipo de tráfico AF se nombra como “AFcd” (c=clase, d=descarte).
      - Expedited Forwarding (EF) o Premium. Ofrece todas las garantías, como si se dispusiera de una línea dedicada:
        - Ancho de banda mínimo, retardo y variación de retardo acotados, y tasa de pérdidas máxima.

- Formato de los paquetes.
  - Etiqueta de flujo e IS (Integrated Services).
    - La etiqueta identifica todos los paquetes de un mismo flujo de datos.
    - Un flujo es una secuencia de paquetes enviados desde un mismo origen hacia un único receptor o varios receptores (multicast).
    - Un flujo es unidireccional.
    - Todos los paquetes de un flujo deben ser gestionados del mismo modo por los routers del camino:
      - Se debe aplicar el mismo control de QoS a todos los paquetes de un flujo.



- Formato de los paquetes.
  - Etiqueta de flujo e IS (Integrated Services).
    - Un flujo se comporta como un circuito virtual, y puede ser solicitado por protocolos de nivel superior.
    - La gestión de flujos está ligada a un control de QoS basado en reserva de recursos, lo que se conoce como “Integrated Services”.
      - Con “Integrated Services” los routers deben gestionar información de estado sobre los flujos establecidos y activos.
      - Se requiere protocolos adicionales para comunicar los routers y gestionar las reservas y el estado:
        - RSVP (Resource reSerVation Protocol): Protocolo de reserva de recursos.

- Formato de los paquetes.
  - Cabeceras de extensión.
    - Permiten incorporar funciones adicionales a los datagramas.
    - Las cabeceras de extensión se concatenan tras la cabecera básica, entre ésta y la cabecera del siguiente protocolo.
    - Un cabecera de extensión determinada solo puede aparecer una vez.



- Formato de los paquetes.
  - Cabeceras de extensión.

Cabecera	Función
Opciones salto a salto (0)	Para opciones que requieren ser procesadas en cada salto y para definir datagramas de más de 64Kbytes.
Encaminamiento (43)	Se indica las próximas direcciones de equipos por las que debe pasar el paquete, que son usadas por los routers.
Fragmentación (44)	Para gestionar paquetes fragmentados entre origen y destino. El origen debe determinar el MTU máximo.
Datos cifrados (50)	Se usa cuando el campo de datos está encriptado.
Autentificación (51)	Para verificar identidad del origen e integridad del paquete.
Opciones de destino (60)	Permite enviar Información adicional para el destino
RSVP (46)	Protocolo de reserva de recursos para gestionar flujos.
ICMP (58)	Protocolo de mensajes de control de IPv6.
TCP (6) y UDP (17)	Protocolos de transporte.

- Direccionamiento.
  - Gran espacio de direcciones:
    - Direcciones de 128 bits frente a los 32 de IPv4.
    - Si se considerasen todas las combinaciones se tendría $2^{128}=3{,}4\cdot10^{38}$ direcciones. En la superficie de la Tierra toca a $7\cdot10^{23}$ direcciones por m^2.
    - Esto se aprovecha para definir un orden jerarquico de direcciones que facilita el encaminamiento.
  - Se definen tres clases básicas de direcciones:
    - **Unicast**. Direcciones conocidas asignadas a interfaces de red.
    - **Anycast**. Hace referencia a un conjunto de interfaces (similar a la dirección de red de IPv4). El paquete se entrega en la interfaz más cercana del conjunto, en función de la métrica del protocolo de encaminamiento usado.
    - **Multicast**. El destino es un conjunto de interfaces de uno o más equipos. Se incluyen aquí las direcciones de broadcast, que no existen como tales.

- Direccionamiento.
  - Notación.
    - Se escriben 8 grupos de 4 cifras en hexadecimal:
      2001:0db8:85a3:0000:1319:8a2e:0070:7334
    - Los grupos de cuatro dígitos nulos se pueden resumir:
      2001:0db8:85a3**::**1319:8a2e:0070:7334
    - Los ceros a la izquierda en un grupo pueden ser omitidos:
      2001:**db8**:85a3::1319:8a2e:**70**:7334
    - Se pueden resumir más de dos grupos consecutivos de dígitos nulos. Solo se pude resumir una serie de grupos dentro de la misma dirección:
      2001:0db8:0000:0000:0000:8a2e:0000:7334 =
      2001:0db8:0000**::**0000:8a2e:**0000**:7334 =
      2001:0db8**::**8a2e:**0000**:7334

- Direccionamiento.
  - Notación.
    - En las direcciones IPv6 que representan direcciones de IPv4 se pueden escribir los últimos grupos en decimal:
      0000::0000::0000::0000::00AC:0014:002B:00E6 =
      ::AC:14:2B:E6 =
      ::172.20.43.230
    - También se puede usar en URLs:
      http://[FEDC:BA98:7654:1234:1319:5671:8F4E:2E4C]/
      http://[FEDC:BA98:7654:1234:1319:5671:8F4E:2E4C]:8080/
    - Para representar las redes se usa notación CIDR:
      Red con 48 bits de máscara: 2045:BA98:7654:: / 48
      Host: FEDC:BA98:7654:1234:1319:5671:8F4E:2E4C / 128

- Direccionamiento.
  - Tipos de direcciones más comunes:

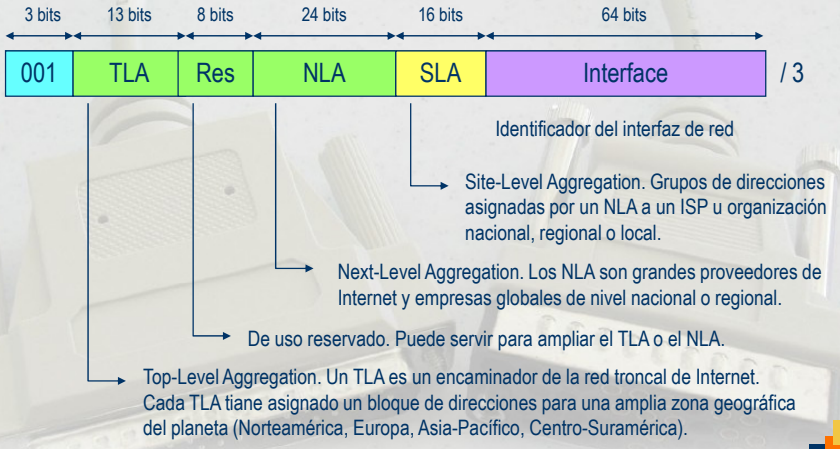
Rango	Prefijo CIDR	Función
::	/ 128	Indica que no hay dirección. Como 0.0.0.0 de IPv4.
::1	/ 128	Dirección de loopback. Como 127.0.0.1 en IPv4
::0000:X:X:X:X	/96	Direcciones IPv6 compatibles con IPv4 (o IPv4 empotradas). Define una conversión directa de direcciones IPv4 a IPv6.
::00FF:X:X:X:X	/96	Direcciones IPv4 mapeadas. Conversión indirecta.
::FFFF:X:X:X:X	/96	Direcciones de IPv4 representadas en IPv6 para usar nodos que sólo soportan IPv4 en una red IPv6. Usadas para enviar paquetes IPv6 con túneles sobre redes IPv4.

- Direccionamiento.
  - Tipos de direcciones más comunes:

Rango	Prefijo CIDR	Función
FE80::	/10	Direcciones locales, que solo son validas en un enlace físico local.
FEC0::	/10	Direcciones unicast de emplazamiento local: direcciones privadas de una organización. Este tipo se ha sustituido por el siguiente.
FC00::	/7	Direcciones unicast de uso local: direcciones privadas de una organización (RFC 4193, 2005). Para asegurar que son únicas incluyen 40 bits aleatorios.
FF00::	/8	Direcciones multicast. La dirección FF01::1, denominada "todos los nodos", equivale a un broadcast de IPv4.
2000:: a 3FFF:: (bits 001…)	/3	Direcciones unicast globales (públicas).

Nota: Las direcciones anycast usan los mismos rangos que las unicast. La diferencia es que las anycast son usadas por más de una interfaz de forma simultánea.

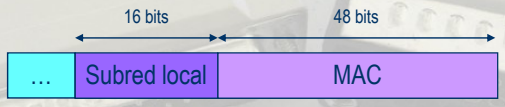
- Direccionamiento.
  - Formato de una dirección unicast global:



- Direccionamiento.
  - Formato de una dirección unicast global:
    - Algunas organizaciones de control de Internet y asignación de direcciones varían un poco el formato.
    - Ejemplo: Variación RIPE (Réseaux IP Européens), que coordina redes públicas y de investigación en Europa, incluida la española Red-IRIS:

  - Direcciones de RedIRIS: 2001:0720:0::/36 y 2001:0720:1::/36
    - TLA=0001, SubTLA RedIRIS=0720
    - NLA=Universidades en España. Ejemplo: 2001:0720:1E10::/48
    - SLA=Redes y subredes de una universidad. Ej.: 2001:0720:1E10:0101::/64

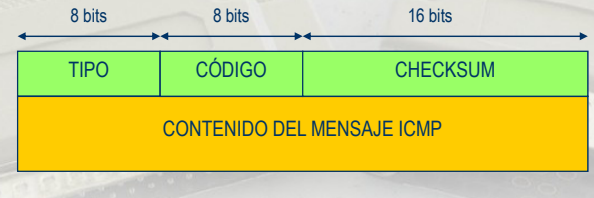
- Direccionamiento.
  - Asignación de direcciones
    - Un equipo escoge los 64 bits de menor peso de la dirección de cada interfaz y para configurar los 64 de mayor peso hay dos opciones:
      - Obtenerlos de un servidor DHCPv6 (Dynamic Host Configuration Protocol), de forma similar a como se hace con DHCP para IPv4.
      - Obtenerlos con ND (Neighbor Discovery). Más simple que DHCP y basado en mensajes ICMPv6. Actualizado en 2007.
    - No hace falta configurar máscara de red. El prefijo CIDR asociado depende del tipo de dirección (unicast global: /3, unicast local: /7, multicast: /8…)
    - Para los 64 bits de menor peso:



- Direccionamiento.
  - Asignación de direcciones
    - ND (Neighbor Discovery).
      1. El equipo genera una dirección temporal IPv6 a partir de su MAC y un prefijo estándar para los 64 bites de mayor peso.
      2. El equipo envía un ICMPv6 de "Router Solicitation" a la dirección de multicast "todos los encaminadores".
      3. El router configurado como puerta de enlace contesta la petición con un mensaje "Router Advertisement", que contiene el prefijo real que debe usar el equipo para los 64 bits de mayor peso y la dirección de la puerta de enlace.
      4. El equipo configura su dirección y la puerta de enlace.

- Direccionamiento.
  - DNS (Domain Name Service) e IPv6
    - DNS devuelve una dirección IP a partir de un nombre de dominio.
    - Se han definido modificaciones de DNS para trabajar con IPv6, principalmente en los tipos de registro que soporta DNS.
    - Tipos de registros de DNS:
      - Registros A y PTR: los clásicos para direcciones de IPv4.
      - Registros AAAA (RFC 3596). Para gestionar direcciones de IPv6 de forma similar a los registros A de IPv4.
        - Permite una adaptación sencilla y rápida de DNS.
      - Registros A6 (RFC 3363). Mejora aspectos de DNS y su uso es más complejo. Sigue en fase experimental.

- ICMPv6.
  - IPv6 usa una nueva definición de ICMP llamada ICMPv6:
    - ICMPv6 incorpora funcionalidad de ICMP, IGMP y ARP.
    - No se incluyen muchos mensajes ICMP obsoletos.
    - El formato de los mensajes de ICMPv6 es similar a ICMP clásico.
    - Ha habido diferentes especificaciones: la última es de 2006.
    - También se definen mensajes ICMPv6 especiales para ND.
    - Algunos mensajes de ND están firmados y son autentificados.



- ICMPv6.
  - Mensajes de error:

Tipo	Nombre	Notas
1	Destination Unreachable	Códigos 0-6: No route to destination, Communication with destination administratively prohibited (firewall), Beyond scope of source address, Address unreachable, Port unreachable…
2	Packet Too Big	Lo envía un router cuando no puede retransmitir un paquete por que el MTU de la siguiente red es demasiado pequeño. El mensaje informa de ese MTU y se usa en procesos de descubrimiento de MTU del camino.
3	Time Exceeded	Código 0: Hop limit exceeded in transit. Código 1: Fragment reassembly time exceeded.
4	Parameter Problem	Código 0: Erroneous header field encountered Código 1: Unrecognized Next Header type encountered. Código 2: Unrecognized IPv6 option encountered.

- ICMPv6.
  - Mensajes informativos:

Tipo	Nombre	Notas
128	Echo Request	Contiene un identificador y un número de secuencia para asociar las peticiones de eco a sus respuestas.
129	Echo Reply	Contiene el identificador y el número de secuencia de la petición correspondiente.

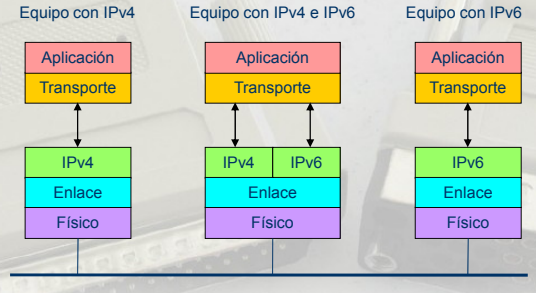
- ICMPv6.
  - Mensajes utilizados por Neighbor Discovery:

Tipo	Nombre	Notas
133	Router Solicitation	Usado por un router o equipo para solicitar información a otros. Se envía a un muticast específico atendido por routers IPv6.
134	Router Advertisement	Respuesta al anterior, o enviado de forma periódica. Un router informa a otros equipos de su precencia y de configuración de direccionamiento.
135	Neighbor Solicitation	Usado por un equipo para comprobar si otro existe, y poder resolver su dirección.
136	Neighbor Advertisement	Respuesta al anterior, que incluye información de la dirección de enlace del que responde.
137	Redirect	Similar al ICMP Redirect de IPv4.
138	Router Renumbering	Generado en un equipo de administración, contiene información para que los routers de la red cambien sus direcciones de forma automática. Está firmado y autentificado.

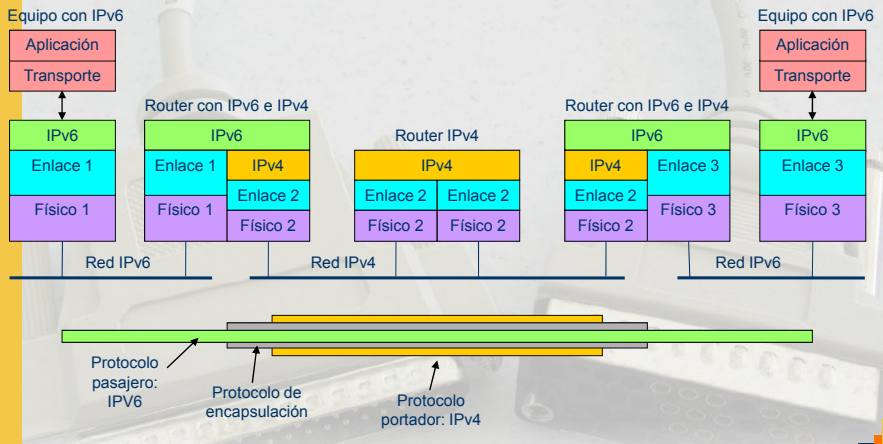
- Despliegue.
  - A tener en cuenta…
    - El gobierno de EE.UU. ordenó tener funcionando IPv6 en las agencias federales en 2008.
    - Los países asiáticos desarrollados (Japón, China, Corea del Sur…) son los más adelantados en el despliegue de IPv6.
    - La Unión Europea también promueve el desarrollo de IPv6.
    - Se espera que IPv4 conviva con IPv6 durante unos 20 años.
  - Mientras dure la transición, se necesita:
    - Pila de protocolos que soporte las dos versiones en Internet (pila dual).
    - Túneles, para llevar los paquetes IPv6 sobre redes IPv4, o viceversa.
    - NAT y otros mecanismos de traducción de direcciones, para convertir entre direcciones de IPv4 e IPv6. Además hay que convertir el protocolo.

- Despliegue.
  - La transición implica dos problemas:
    - Limita las características de IPv6
    - Mayor complejidad en la red.

Pila de protocolos dual:



- Despliegue.
  - Túnel de nivel 3 para transportar IPv6 sobre una red IPv4.



- Despliegue.
  - Los S.O. más comunes ya soportan IPv6:
    - MS. Windows:
      - Windows NT, 98. No hay soporte IPv6 de Microsoft.
      - Windows 2000-SP1. Requiere instalar “Microsoft IPv6 Technology Preview”, que un producto más de prueba que profesional. No se guarda la configuración y hay que hacer un script al arranque.
      - XP-SP1. Soportado, pero hay que habilitarlo. Se requiere “Advanced Networking Pack” para funciones adicionales y configuración gráfica.
      - Server 2003/.NET. Soportado, pero hay que activarlo. Sin soporte gráfico.
      - Vista y Server 2008. De forma nativa. La funcionalidad es mayor que en los anteriores.

- Despliegue.
  - Los S.O. más comunes ya soportan IPv6:
    - BSD. Gracias al proyecto KAME IPv6 es soportado de forma nativa en FreeBSD 4.0, NetBSD 1.5 y OpenBSD 2.7 por defecto, sin configuración adicional.
    - MAC OS X 10.2. Soporte completo, incluso con configuración gráfica. Al fin y al cabo, MAC OS X es esencialmente BSD.
    - Linux. El soporte IPv6 se incluye en el kernel a partir de la versión 2.1.8, bien directamente o como módulo. El kernel debe haber sido compilado con la opción de IPv6.
    - Sun Solaris 8. Soporte completo. Incluso ofrece túneles IPv6 sobre IPv4.

http://www.join.uni-muenster.de/Dokumente/Howtos/Howto_install_IPv6.php?lang=en

- Normativas
  - En evolución continua: Hay que tener cuidado con las RFCs.
    - RFC 1883. Primera versión del formato de paquete (1995).
    - RFC 1884. Última versión del esquema de direccionamiento (1995).
    - RFC 2375. Uso de multicast como broadcast.
    - RFC 2460. Versión actual del formato de paquete (1998).
    - RFC 2462. Configuración automática de direcciones.
    - RFC 2474, RFC 3168. Differentiated Services (QoS).
    - RFC 2526. Uso de las direcciones anycast.
    - RFC 2893. Implementación de pila dual IPv6-IPv4.
    - RFC 3363, RFC 3364. gestión de direcciones IPv6 en DNS (2002).
    - RFC 3596. Extensiones de DNS para soportar IPv6 (2003).
    - RFC 4193. Direcciones únicas locales (privadas) tipo FC00::
    - RFC 4291. Última versión del esquema de direccionamiento (2006).
    - RFC 4443. Última especificación de ICMPv6 para IPv6 (2006).
    - RFC 4861. Protocolo Neighbor Discovery (ND) (2007).
    - …

- Características
- Motivación.
- Historia.
- Etiquetado.
- Arquitectura.
- Encaminamiento.
- Gestión de etiquetas.
- VPNs con MPLS.

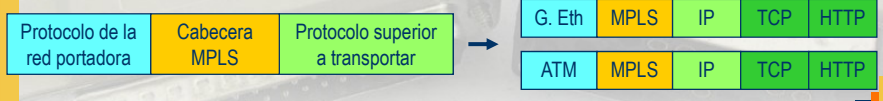
- Características.
  - MPLS: Multiprotocol Label Switching. Permite enviar diferentes protocolos (IP, Ethernet, ATM, SDH…) sobre una misma red.
    - Principalmente se usa para transportar IP (RFC 3031) y mejorar el rendimiento de redes IP grandes (WAN) simplificando el enrutamiento.
  - Emplea el concepto de túnel, donde hay un protocolo pasajero y otro portador. MPLS define el protocolo de encapsulación.
  - Ofrece servicios de conmutación de circuitos y de datagramas.
  - Basado en conmutación tipo ATM, pero con paquetes grandes de longitud variable.
    - Esto funciona bien en redes muy rápidas (Gbps).
  - Trabaja entre nivel de enlace y de red del OSI: nivel 2,5.

- Características.
  - La conmutación se basa en complementar los protocolos pasajeros, con unas cabeceras que gestionan etiquetas de forma parecida a las VLAN Ethernet.
  - Se realiza una gestión de tráfico eficaz, similar a la de Frame-Relay.
  - Proporciona servicios de VPNs, QoS y VoIP con fiabilidad y buen rendimiento.
  - Muy utilizado en redes WAN por proveedores de servicios de interconexión remota o de accesos de banda ancha.
  - MPLS no tiene tanto sentido con IPv6, ya que este protocolo ya incorpora etiquetas de flujo en su cabecera.

- Motivación.
  - El encaminamiento IP en redes WAN es muy complejo y disminuye el rendimiento de la red.
    - Para cada paquete, cada router de la red WAN debe aplicar el algoritmo de encaminamiento.
    - Las direcciones IPv4 son jerárquicas, basadas en subredes y máscaras.
    - La concordancia de direcciones destino y máscaras con las entradas de tablas de encaminamiento jerárquicas es compleja si hay muchas entradas.
    - Muchos protocolos de encaminamiento IP son complejos, y requieren tiempo y recursos.
  - Se necesita un método más sencillo y eficaz que las tabas de encaminamiento.

- Historia.
  - Toshiba CSR: Cell Switching Router (1994). Una de las primeras ideas para enviar IP sobre ATM (en Japón) aceptada por IETF.
  - IP Swithing (1996). Idea de Ipsilon Networks para IP sobre ATM. Los router-conmutadores de al red detectan cuando hay múltiples datagramas con mismos origen y destino, y entonces establecen un circuito virtual por donde enviarlos.
  - Tag Switching (1996). Versión de Cisco que no limitaba el uso a ATM para enviar paquetes IP en una red conmutada.
  - Label Switching (1997). Cuando IETF empezó a estandarizar la idea de Cisco.
  - MPLS (2001). El estándar de IETF recogió y consensuó a las ideas de varios fabricantes del sector
  - Desarrollo MPLS (2001-). Documentos sobre como aplicar MPLS con diferentes protocolos, mejoras de encaminamiento, control y señalización de QoS, y muchas otras opciones.

- Etiquetado.
  - Los paquetes de datos de un protocolo pasajero se etiquetan con números, de forma que se pueda identificar y distinguir los paquetes de un mismo flujo de datos, al enviarlos sobre una red portadora.
    - Al transportar datos sobre redes de circuitos virtuales (ATM o Frame-Relay) los identificadores de circuito (VCI-VPI, DLCI) podrían usarse como etiqueta de los datos que transportan.
    - Pero si la red portadora no usa circuitos virtuales (Gigabit Ethernet), se requiere añadir nuevos campos para el etiquetado.
  - Se ha definido una cabecera MPLS para etiquetas, independiente del protocolo portador:

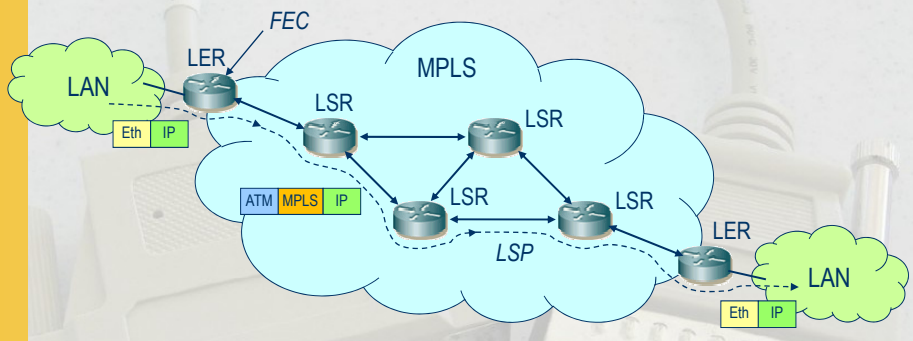


- Etiquetado.
  - Contenido de una etiqueta (32 bits):
    - Label (20 bits): valor numérico de la etiqueta.
    - Exp (3 bits): Experimental, sin definición concreta. Se pueden usar para QoS.
    - S o Stacking bit: vale 1 para la última etiqueta de una pila de etiquetas.
    - TTL (8 bits): Sustituye al TTL de la cabecera de IPv4 cuando los paquetes circulan por un flujo de MPLS.
  - Una cabecera MPLS puede contener una pila LIFO de etiquetas.

- Etiquetado.
  - FEC (Forwarding Equivalence Class). Para etiquetar los paquetes se pueden usar diferentes criterios, que definen clases de tráfico:
    - Direcciones IP, o patrones de direcciones (subredes).
    - Valores de ToS o DSCP de la cabecera IP.
    - Puertos de transporte.
    - Protocolos de aplicación.
  - Los paquetes que pertenecen a una misma FEC se encaminan por el mismo camino en la red, a modo de un circuito virtual.
  - La asociación entre etiquetas y FECs puede ser:
    - Estática. Cuando un administrador de la red define clases según aplicaciones.
    - Dinámica. Cuando los paquetes intercambiados entre pares de estaciones (igualdad de direcciones origen y destino) se envían por flujos independientes.

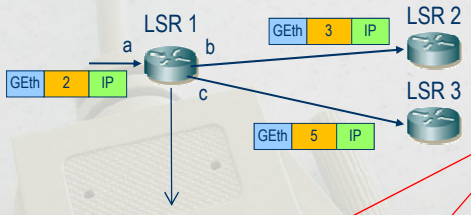
- Arquitectura.
  - Hay dos tipos básicos de conmutador-router:
    - LSR (Label Switching Router): elemento que encamina los paquetes dentro de la red MPLS.
      - Encamina en función de las etiquetas que ya tienen los paquetes.
      - Intercambia etiquetas de la cabecera MPLS.
    - Edge LSR o LER (Label Edge Router): equipo frontera entre la red MPLS y la red con el protocolo pasajero.
      - Puede ser de entrada (ingress LSR), de salida (egress LSR) o ambos.
      - Usa información clásica de encaminamiento de IP:
        - Para encaminar los paquetes de salida de la red MPLS.
        - Para crear FECs para los paquetes de entrada.
      - Es el que pone o quita las etiquetas.

- Arquitectura.
  - Esquema básico de red MPLS:



LSP (Label Switched Path): Camino MPLS por donde se envía el tráfico de paquetes correspondiente a un FEC (Forwarding Equivalence Class). Un LSP es unidireccional

- Encaminamiento.
  - Tablas de encaminamiento

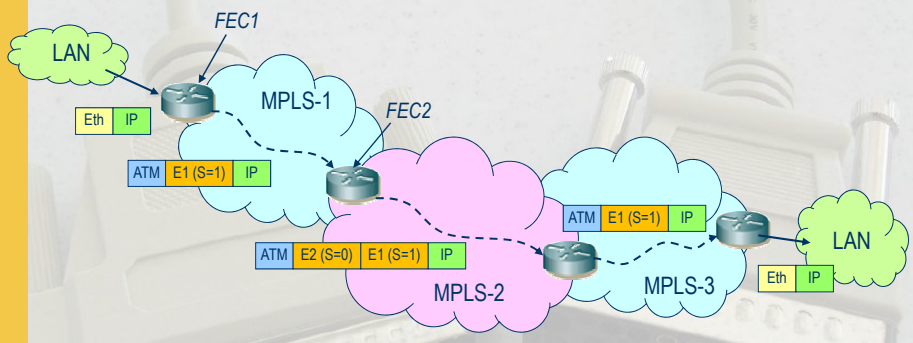


La red MPLS puede estar basada en protocolos con direcciones o en protocolos de circuitos virtuales

Etiqueta entrada	Etiqueta de salida	Interfaz de salida	Próximo salto
1	1	b	"LSR 2"
2	3	b	"LSR 2"
	5	c	"LSR 3"

Se puede enviar paquetes a múltiples destinos, lo que permite gestionar broadcast y multicast de IP

- Encaminamiento.
  - Es posible una jerarquía de redes MPLS, gracias a la pila LIFO de etiquetas en la cabecera MPLS:



- Gestión de etiquetas.
  - Los LSR de la red establecen los caminos para los flujos de paquetes usando el protocolo LDP (Label Distribution Protocol).
  - Las asociaciones FEC-etiqueta configuradas en un LSR se pueden propagar a otros LSR. Existen diferentes opciones de protocolos para la distribución de etiquetas:
    - BGP (Border Gateway Protocol). Protocolo de enrutamiento genérico.
    - RSVP (Resource reSerVation Protocol). Protocolo de reserva para Integrated Services usado con IPv6.
    - LDP. Especifico de MPLS.
  - Los LSR pueden fusionar varios flujos en uno sólo, agrupando los paquetes que le llegan con diferentes etiquetas en un flujo de salida con una misma etiqueta, o disgregar un flujo de paquetes.

- VPNs con MPLS.
  - MPLS permite gestionar eficazmente VPNs.
  - Ventajas de MPLS sobre las VPNs clásicas:
    - Los flujos LSP de MPLS son más eficaces que los túneles clásicos L2TP o PPTP.
    - Se puede realizar un buen control de QoS del tráfico de la VPN.
    - Es más fácil ampliar la VPN.
    - No se limita a conexiones punto a punto.
  - Muchos ISP que ofrecen servicios VPN usan MPLS.