

Redes y comunicaciones (tercera parte)

Autor: Jacinto Ruiz Catalán

[\[Ver curso online\]](#)

Presentación del curso

Este curso es la tercera y última parte de nuestro estudio técnico explicativo sobre redes y comunicaciones de transferencia de datos. En esta oportunidad podrás ampliar tus conocimientos aprendidos en los cursos previos siguiendo temas como: arquitectura, transmisión, funcionamiento, estructura de las ATM, RDSI-BA y SDH. También te ofrecemos información sobre la calidad de servicio en redes IP y la arquitectura TCP/IP.

Ampliarás tus conocimientos sobre protocolos ICMP, ARP, RARP, TCP, UDP, HTTP, entre otros. También tendrás todos los datos sobre redes ópticas y redes para móviles (wap) y mucha más información desarrollada en este nuestro curso sobre las distintas redes, incluidas las de internet y las inalámbricas, y todo lo referente a las comunicaciones de transferencia de datos.

Visita más cursos como este en mailxmail:

[<http://www.mailxmail.com/cursos-informatica>]

[<http://www.mailxmail.com/cursos-software>]



¡Tu opinión cuenta! Lee todas las opiniones de este curso y déjanos la tuya:

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/opiniones>]

Cursos similares

Cursos	Valoración	Alumnos	Vídeo
Amplificadores Operacionales Son llamados amplificadores operacionales porque podemos encontrar circuitos montados a base de estos amplificadores que realizan operaciones matemáticas, como por ejemplo... [13/09/05]		5.618	
Guía de Optimización de Windows XP Esta guía te servirá para optimizar tu Windows XP, para mejorar tanto en el trabajo como en la interpretación de juego sin peligro. Está diseñada para conocer todo aquello... [28/09/05]		6.316	
Eudora Light El correo electrónico en la actualidad se está convirtiendo en una forma de intercambio de información entre particulares y empresas muy potente. A través de un ... [09/03/04]		2.214	
Aprende Word Este curso está destinado a los principiantes. A todos aquellos que necesitan una introducción detallada para moverse dentro de este programa. Está basado en ejercicios prácticos... [27/09/05]		4.398	
Windows Vista Microsoft Windows Vista es la versión del sistema operativo Microsoft Windows que sucede a Windows XP. Windows Vista presenta una experiencia de usuario avanzada y está diseñada para... [21/11/07]		24.915	

1. Redes ATM. Principios de operación

[<http://www.mailxmail.com/...so-redes-comunicaciones-internet-3/redes-atm-principios-operacion>]

ATM, RDSI-BA y SDH. Principios de operación

*Los principios de las redes ATM

Conceptos de ATM:

- Conmutación de paquetes de longitud fija de 53 bytes (5 de cabecera y 48 de datos). Permite conmutación a alta velocidad.
- Orientado a conexión a bajo nivel.
- Asignación de ancho de banda bajo demanda.
- Mínimo control de errores y de flujo.
- Transparencia temporal (permite tráfico isócrono).
- Transmisión de células a intervalos regulares con o sin información.
- Llegada de células en orden al destino.

Hay que establecer una **conexión virtual** previa al envío de datos. Cada conexión tiene asignados una serie de parámetros de tráfico al establecerse la conexión.

Durante la **transmisión** también se controla que se cumplan los **parámetros** contratados.

Hay dos **interfaces**: la **UNI** es el interfaz entre un terminal y un nodo de la red ATM y la **NNI** es la interfaz entre dos nodos ATM.

Cada conexión lógica se llama conexión de canal virtual (CCV) y cada grupo de CCV que tienen el mismo destino se llaman conexión de trayecto virtual (CTV) lo cuál redundo en una disminución del coste en control y gestión de red.

2. Arquitectura de la RDSI-BA. Capas SDH

[<http://www.mailxmail.com/...so-redes-comunicaciones-internet-3/arquitectura-rdsi-ba-capas-sdh>]

Arquitectura de la RDSI-BA

*Configuración de referencia y modelo de referencia de protocolos RDSI-BA

Las tres capas más bajas de RDSI-BA son: capa física, capa ATM y capa de adaptación ATM (AAL). Por encima están las capas superiores. La AAL se encarga de adaptar la red a otros tipos de redes, como IP, etc.

*Capa física

Se divide en dos subcapas: subcapa dependiente del medio físico (PMD) y subcapa de convergencia de transmisión (TC).

- Jerarquías digitales en redes de banda ancha

En EEUU y Europa hay distintas jerarquías en la capa física. Para compensar esas diferencias, actualmente se rellenan las tramas con bits de relleno, lo que redundante en un menor rendimiento de las jerarquías más rápidas.

Para solucionar los problemas de las jerarquías actuales (PDH = Jerarquía digital plesiócrona o cuasi-isócrona) se ha creado la SDH (Jerarquía digital síncrona). La velocidad básica de SDH es 155'52 Mbps y engloba a todas las velocidades permitidas de la PDH.

- Jerarquía digital síncrona SDH

Se define la velocidad básica por el módulo de transporte síncrono STM-1 a 155'52 Mbps. La información está integrada en una estructura matricial de 270 x 9 bytes. De estas nueve filas y 270 columnas, las 9 primeras columnas son de control y gestión (TOH). Una de sus filas (9 bytes) es un apuntador a otra sección que consta de una columna y 9 filas que es la POH (función auxiliar del trayecto) y las otras 8 filas son la SOH (función auxiliar de sección).

Es decir, de sobrecarga hay $9 \times 9 = 81$ bytes más 1×9 bytes = 9 bytes, en total 90 bytes. El resto, es decir $270 \times 9 = 2430 - 90 = 2340$ bytes son la carga útil. La señal debe ser transmitida a 4 kHz, es decir 8000 células por segundo. Por lo tanto, la velocidad básica es $8000 \times 270 \times 9 \times 8 = 155'52$ Mbps. Para velocidades superiores, se utilizan múltiplos, es decir STM-n = n x STM-1. La especificación americana es la SONET, que es la tercera parte de la europea, es decir STM-n = 3 x STS-n.

Por lo tanto, por ejemplo, la velocidad de STS-3 = STM-1. Esto es así porque las células SONET son de 9 filas x 90 columnas. De las que $(9 \times 3) + 9 = 36$ bytes son de sobrecarga y el resto de carga útil.

- Contenedores virtuales en SDH

Para evitar multiplexar y demultiplexar la información, se utilizan los apuntadores.

*Capas SDH

La capa física de SDH se subdivide en varias subcapas, que son: interfaz física, sección de regeneración (RSOH), sección de multiplexación (MSOH), capa VC-4 y alternativamente VC-12, ATM o IP. De la carga útil, se emplean 27 bytes para RSOH y 45 para MSOH. Lo cuál implica que la carga útil se queda reducida a $2340 - 27 - 45 = 2358$ bytes. VC-4 y VC-12 se encargan de acomodar los actuales sistemas PDH a SDH.

- Ventajas de SDH

1. Alta velocidad

2. Estandarización
3. Simplificación y flexibilidad
4. Fiabilidad
5. Gestión de red

- Desventajas de SDH

1. Dificultades en la temporización
2. Formación del personal técnico



3. Capa ATM: Funciones y descriptor de tráfico

[<http://www.mailxmail.com/...s-comunicaciones-internet-3/capa-atm-funciones-descriptor-trafico>]

*Capa ATM: Funciones y descriptor de tráfico

Las **funciones** de la capa ATM son:

- Multiplexación/Demultiplexación de células
- Generación/Extracción de cabecera de la célula
- Traslación ITV/ICV
- Control de flujo genérico (CFG)

La célula ATM consta de 5 bytes de cabecera y 48 de carga. Los campos ITV y ICV son los identificadores de caminos virtuales y trayectos virtuales. En UNI, la ITV tiene 8 bits y la ICV 16. En NNI la ITV tiene 12 bits y la ICV 16.

El CFG tiene 4 bits, el campo de tipo de carga útil (PTI) tiene 3 bits. El campo de prioridad de pérdida de células (CLP) tiene 1 bit y el campo de control de error de cabecera (HEC) tiene 8 bits. Los canales y trayectos virtuales son unidireccionales. Se puede hablar también de enlaces y conexiones virtuales tanto para caminos como para trayectos. Además de conmutadores virtuales.

Hay células dedicadas sólo a gestión del tráfico, encargadas de monitorizar que el sistema atienda correctamente las necesidades contratadas. Estos flujos se llaman OAM. Ya que hay un contrato de tráfico previo a una conexión mediante ATM, se pueden elegir diferentes tipos de tráfico a contratar:

1. **CBR** (Velocidad binaria constante): Para tráfico isócrono.
2. **RT-VBR** (Velocidad binaria variable en tiempo real): Para tráfico isócrono.
3. **NRT-VBR** (Velocidad binaria variable en tiempo no real): Para tráfico transaccional.
4. **UBR** (Velocidad binaria no especificada): Semejante a datagramas. Para correo electrónico, etc.
5. **ABR** (Velocidad binaria disponible): Garantiza no pérdida de células pero a baja velocidad.

- Descriptor de tráfico

Consiste en todos los parámetros contratados. Son:

1. **PCR** (Tasa de pico de células): Velocidad máxima a que se pueden enviar células.
2. **MBS** (Tamaño máximo de ráfaga) y **BT** (Tolerancia de ráfaga): Número de células consecutivas a velocidad PCR en categoría VBR.
3. **MCR** (Mínima velocidad de las células): Velocidad mínima de envío de células en categoría ABR.
4. **SCR** (Tasa sostenida de células): Número medio de células medidas en una escala de tiempo grande por unidad de tiempo. Es una velocidad media.

Para prevenir la congestión, se utiliza el algoritmo de cubo de fichas. Se admite una profundidad máxima del cubo y conforme van llegando células se va llenando el cubo (cuando salen células se va vaciando). Cuando el cubo tiene células en número igual a su profundidad, las siguientes células se descartan.

4. Capa ATM: Variación de retardo, calidad de servicio y gestión de tráfico

[<http://www.mailxmail.com/...net-3/capa-atm-variacion-retardo-calidad-servicio-gestion-trafico>]

*Capa ATM: Variación de retardo, calidad de servicio y gestión de tráfico

- La tolerancia a la variación del retardo (CDVT)

Cuando dos células llegan a la vez a la capa ATM, una de ellas se debe retardar. Cada conexión tiene un indicador de su tolerancia al retardo. De esa manera, las conexiones con menor tolerancia van siendo servidas antes de sobrepasar ese indicador.

- Calidad de servicio

Hay seis parámetros para medir la calidad de servicio. Los no negociables son:

1. **CER** (Tasa de células erróneas): Células erróneas / células totales.
2. **CMR** (Tasa de células mal insertadas): Células mal insertadas consideradas como erróneas.
3. **SECBR** (Tasa de bloques severamente dañados): Número de bloques de células dañados.

El **retardo de transferencia** de la célula (**CTD**) indica el retardo que sufre una célula en una conexión ATM.

Los **parámetros negociables** son:

1. **CLR** (tasa de células perdidas): Células perdidas / células enviadas.
2. **CTDmax** (Retardo máximo de transferencia).
3. **CDV** (Velocidad máxima de retardo): CTDmax - retardo fijo en la conmutación.

Cada categoría de servicio utiliza unos parámetros de entre todos los señalados. Cuando se hace un contrato de tráfico, la red se compromete a servir lo contratado.

- Gestión de tráfico

El control de admisión se encarga de aceptar o declinar una petición de establecimiento de conexión. El control de flujo se encarga de ajustar la tasa de emisión de células en función de las características de la red.

La función de policía vela por el cumplimiento del perfil de tráfico contratado. La gestión de memoria decide las células a descartar en caso de desbordamiento de los buffers que hay en los conmutadores.

El planificador de células se encarga de decidir el orden de envío de células. Para controlar la congestión, se utiliza un sistema de créditos negociados entre emisor y receptor. Es el receptor el encargado de avisar al emisor para que cese en los envíos o los reanude.

- Gestión de tráfico ABR

Para acondicionar la velocidad del tráfico se utilizan células especiales RM. El control es retroalimentado dinámicamente entre emisor y receptor. Se suele utilizar un

algoritmo para el control de tráfico. Este algoritmo se llama GCRA. Es similar al cubo de fichas.

5. Capa AAL. Capa de adaptación ATM

[<http://www.mailxmail.com/...urso-redes-comunicaciones-internet-3/capa-aal-capa-adaptacion-atm>]

Capa AAL. Capa de adaptación ATM

*Capa AAL. Capa de adaptación ATM

- Funciones

Se ocupa de acomodar la capa superior de diversas tecnologías a la tecnología ATM. Implementa diferentes servicios, ya sea servicios de entrega en orden de datos, servicios de entrega a velocidad constante de datos, temporización, etc.

AAL se puede denominar AAL1, AAL2,... AAL5 en función de los servicios que preste. Las más utilizadas son AAL1 y AAL5.

- Estructura de la capa AAL

Consta de dos **subcapas**: subcapa de convergencia (**CS**) y subcapa de segmentación y reensamblado (**SAR**).

CS se encarga de servir a la capa superior prestando los servicios requeridos. La subcapa SAR sirve a ATM las células y las recibe a su vez de ATM. Como hay diferentes servicios posibles, pueden haber diferentes subcapas CS.

En AAL5 se ha subdividido CS en **dos subcapas más**, la parte común (**CPCS**) y la parte específica de servicio CS (**SSCS**).

Es decir, de arriba abajo, en **AAL1**:

Capas superiores
Subcapa CS
Subcapa SAR
Capa ATM
Capa física

En **AAL5**, tenemos:

Capas superiores
Subcapa SSCS
Subcapa CPCS
Subcapa SAR
Capa ATM
Capa física

- Introducción a la capa AAL1

Presta servicios CBR. Tiene una serie de mecanismos para recuperación, control de temporización, ordenamiento de células, etc. Para poder servir todas las estrictas características del servicio CBR. Transporta vídeo, señal de voz, audio de alta calidad, etc.

La capa SAR consta de 48 bytes, a los que ATM le añade los 5 bytes de cabecera. De los 48 bytes, 47 son de carga útil y 1 de cabecera utilizada por la subcapa SAR.

- Introducción a la capa AAL5

Se suele utilizar para datos, más restrictivos para pérdida de datos pero menos para velocidad. La subcapa SAR utiliza los 48 bytes para carga, pero los últimos 48 bytes los utiliza parcialmente para control. Es decir, la última carga de 48 bytes contiene una cola de 8 bytes, la carga sobrante y el resto hasta 48 se rellenan con basura.

6. Redes SDH

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/redes-sdh>]

Redes SDH

*Componentes de una red SDH

Las redes SDH están formadas por cuatro tipos de **elementos**:

1. **Regeneradores (R)**: Regeneran las señales que se han atenuado en la red.
2. **Multiplexores terminales (TM)**: Combinan señales síncronas y plesiócronas en señales STM de mayor velocidad.
3. **Multiplexor incrementador/decrementador (ADM)**: Insertan o extraen señales de baja velocidad en el flujo de alta velocidad de SDH.
4. **Transconectores digitales (DXC)**: Conmutan el tráfico entre la entrada y la salida.

Topologías SDH

Son las típicas, punto a punto, bus, malla, anillo, concentrador, clasificador. La bus se emplea en pequeñas redes, las estaciones extremas son normales, pero las intermedias tienen ADM's y DXC's.

La malla se emplea en grandes redes. Utiliza DXC's. El anillo es el más utilizado ya que permite tener anillos de protección (secundarios). Utiliza ADM's para insertar o extraer información en la red y DXC's para interconectar más anillos.

*Topología en anillo

El anillo tiene la ventaja que si utilizamos un anillo secundario, una ruptura en uno de ellos no implica una interrupción del tráfico.

Mediante la utilización de ADM's, podemos tener anillos unidireccionales o bidireccionales.

Si tenemos dos anillos, podemos utilizarlos de manera que podemos enviar la misma información por ambos, por lo que la redundancia es del 100% y la probabilidad de que ambas conexiones fallen es muy baja. También podemos tener el anillo secundario para tráfico de baja velocidad y para utilizarlo en caso de ruptura del principal.

- Anillos unidireccionales

Estos anillos envían información sólo en un sentido. Tienen el anillo secundario en el otro sentido para solventar los problemas de cortes en el principal.: su principal problema son los retardos ya que cada anillo utiliza recursos diferentes y está sometido a condiciones diferentes de retardo.

- Anillos bidireccionales

El tráfico siempre utiliza la ruta más corta. Se utiliza parte del ancho de banda de una dirección como reserva de la otra.

*Sincronización

Todos los elementos de la red deben estar sincronizados para que SDH cumpla sus funciones de calidad. Hay un reloj central que sincroniza a su vez a los relojes

secundarios esparcidos por la red.

7. Arquitectura y descripción de los protocolos TCP/IP

[<http://www.mailxmail.com/...unicaciones-internet-3/arquitectura-descripcion-protocolos-tcp-ip>]

Calidad de servicio en redes IP. Arquitectura TCP/IP

*El sistema de comunicaciones Internet

Internet está compuesto por múltiples redes de paquetes interconectadas por encaminadores. La capa de enlace y la capa de red son llamadas IP y por encima, la de transporte es la TCP.

- Direcciones Internet o direcciones IP

Cada host tiene asignada una dirección IP. Cada dirección IP se compone a su vez de dos partes, la dirección de red y la dirección de host. Como Internet opera sobre diversos tipos de redes, hay que traducir la dirección IP a la dirección de la red física.

*Descripción general de los protocolos TCP/IP

En Internet se habla de **5 niveles** (en vez de los 7 de OSI). DE arriba abajo, son:

- **Aplicación:** Aplicaciones de los usuarios.
- **Transporte (TCP o UDP):** TCP orientada a conexión y UDP no orientada a conexión.
- **Internet (IP):** No fiable no orientada a conexión.
- **Red e inferiores**
- **Físico**

Las unidades de datos intercambiadas en IP son los datagramas.

- TCP/IP y el modelo de referencia OSI

En TCP/IP los diferentes protocolos de cada capa prestan una serie de servicios a capas superiores y son servidos a su vez por las inferiores; igual que en OSI. Pero en TCP/IP no hay por qué utilizar todas las funcionalidades de la capa inferior, se utilizan sólo las necesarias.

IP no garantiza que los datos entregados sean correctos ni que lleguen en secuencia; estas funciones las deben garantizar los niveles superiores. IP es no orientado a conexión; esa capacidad la debe implementar algún nivel superior.

8. Protocolos del nivel Internet: IP ICMP ARP RARP (1)

[<http://www.mailxmail.com/...icaciones-internet-3/protocolos-nivel-internet-ip-icmp-arp-rarp-1>]

*Protocolos del nivel Internet

Son:

1. **IP** (Internet)
2. **ICMP** (Control)
3. **ARP** (Resolución de direcciones)
4. **RARP** (Resolución inversa de direcciones)

- El protocolo IP

Características:

1. No garantiza el control de flujo
2. No garantiza la recuperación de errores
3. No garantiza que los datos lleguen a su destino

Utiliza sólo datagramas. Y se encarga de seleccionar la trayectoria a seguir por los datagramas e incluso de su fragmentación y reensamblado.

- El mecanismo de direcciones IP

Cada host tiene una dirección única en Internet. Cada dirección se compone de un identificador de la red y otro del host. Se trata de 32 bits divididos en cuatro porciones separadas por un punto. Cada porción o campo consta de 8 bits en formato decimal (un número del 0 al 255).

Dirección IP (32 bits) = Dirección de Red + Dirección de Host

Debido al enorme crecimiento de Internet, se puede subdividir cada red en subredes. Estas subredes no existen para redes exteriores a su propia red (es una fragmentación interna de una red, opaca al exterior).

- Formatos de las direcciones IP

1. Clase A: Primer bit = 0, 7 bits de red y 24 de host.
2. Clase B: Primeros dos bits = 10, 14 bits de red y 16 de host.
3. Clase C: Primeros tres bits = 110, 21 bits de red y 8 de host.
4. Clase D: Primeros 4 bits = 1110.
5. Clase E: Primeros cinco bits = 11110.

Hay direcciones preasignadas: 0.0.0.0 = Esta red u ordenador local, 1.1.1.1 = Todas las redes u ordenadores, 127.0.0.1 = Bucle cerrado.

- Máscara en las direcciones IP

Para permitir flexibilidad, se ha creado un sistema de máscaras. De esta forma, localmente se puede subdividir la red en subredes. Cuando un bit de máscara está a 1, quiere decir que ese bit representa una subred y si es 0 es un host.

Mediante un encaminador específico, es posible traducir direcciones de una Intranet en direcciones de Internet. Esto hace posible un mayor grado de libertad en el

direccionamiento interno en subredes.

9. Protocolos del nivel Internet: IP ICMP ARP RARP (2)

[<http://www.mailxmail.com/...icaciones-internet-3/protocolos-nivel-internet-ip-icmp-arp-rarp-2>]

Protocolos del nivel Internet: IP ICMP ARP RARP (2)

- Los datagramas IP

Los datagramas se encapsulan en tramas, dependiendo del nivel inferior en que trabajen. Por ejemplo, si trabajan sobre Ethernet, se encapsulan en tramas de 1500 bytes a lo sumo.

Los datagramas IP contienen una cabecera IP. Esta cabecera contiene una serie de campos como pueden ser: versión, longitud de la cabecera, tipo de servicio, longitud total del datagrama, identificador (para cuando se subdivide en trozos), flags, offset, tiempo de vida, protocolo de nivel superior, etc. El tamaño máximo de un datagrama es de 65535 bytes (la cabecera es de 20 bytes).

- Fragmentación y reensamblado en IP

Ta que IP trabaja sobre distintos tipos de subredes, es necesario a veces fragmentar los datagramas en trozos más pequeños, aceptados por la subred específica. Para ello, IP debe fragmentar sus datagramas en trozos más pequeños y luego, en el destino reensamblarlos. La capa TCP no tiene conocimiento de ello ya que IP le sirve los datagramas completos.

Para el reensamblado, se utilizan los campos de la cabecera IP. Cada trozo en que se ha dividido el datagrama contiene una indicación de su lugar original en el datagrama, además se dispone de un temporizador. En el destino, IP va recibiendo trozos del datagrama y los va colocando en su lugar dentro del datagrama. Si ha expirado el temporizador y no han llegado todos los trozos, se descarta el datagrama (por eso decimos que IP no implementa conexiones seguras).

- El protocolo ICMP

TCP utiliza este protocolo para el envío de mensajes de control y de error. Por ejemplo ping se utiliza para ver si un ordenador está activo en la red.

Los mensajes ICMP están dentro de datagramas IP (IP los trata igual que los demás datagramas). Es decir, dentro de los datos del datagrama, hay una cabecera del protocolo ICMP que indica una serie de parámetros como código de error, tipo de mensaje, etc., (como ya se ha dicho, IP no tiene constancia de que sea un datagrama especial).

ICMP pueden enviar varios tipos de mensajes como por ejemplo, destino no alcanzable, control de congestión, redireccionamiento, tiempo excedido.

- El protocolo ARP

Convierte las direcciones IP en direcciones físicas de la red. Cada host tiene una tabla para realizar dicha conversión. Cuando una dirección pedida no figura en la tabla, ARP genera una petición por toda la red. Si alguna máquina de la red recibe esa petición y corresponde con la suya propia, avisa al host que ha realizado la petición y este incluye la nueva dirección en su tabla de direcciones.

- El protocolo RARP

Cuando un host desconoce su propia dirección, envía a la red su dirección física y si hay algún host a la escucha que la conozca, le envía al host peticionario su dirección IP. De esta manera, un host que arranca por primera vez, puede automáticamente conocer su dirección en Internet.



10. Protocolos del nivel de transporte: TCP, UDP

[<http://www.mailxmail.com/...des-comunicaciones-internet-3/protocolos-nivel-transporte-tcp-udp>]

*Protocolos del nivel de transporte

- El protocolo TCP

Es orientado a conexión y utiliza IP. Una conexión TCP puede ser utilizada a la vez por varios usuarios. La unidad de datos de TCP se llama segmento. La conexión TCP es dúplex y la entrega es en orden. TCP es fiable, garantiza la secuencia de entrega y se recupera ante errores. Para ello, tiene mecanismos de confirmación de recepción, retransmisión de segmentos, etc.

Para mantener varios usuarios a la vez conectados, cada uno debe utilizar una conexión virtual o puerto (caracterizado por 16 bits). Cada aplicación que utiliza TCP se llama Socket o zócalo y se caracteriza por dos campos, el host en el que corre la aplicación y el puerto que utiliza.

Para el control de flujo, TCP utiliza un mecanismo de ventanas deslizantes. Este mecanismo permite que el emisor pueda enviar un cierto número de segmentos si haber recibido confirmación. Aunque al final, todos deben ser confirmados. Cuando se emite un segmento, un temporizador cuenta un cierto tiempo y si no ha sido confirmada su llegada por el receptor, se reenvía.

Si la conexión se hace entre dos host muy diferentes en cuanto a velocidad, se puede llegar a una congestión. Cuando esto ocurre, es difícil recuperarse. Por eso hay que estudiar muy bien el mecanismo de control de flujo. Los segmentos TCP tiene una cabecera con una serie de campos de control y luego los datos. Para comenzar una sesión TCP hay que conectarse al receptor, cuando se ha confirmado la conexión ya se puede enviar datos en ambas direcciones. Cuando se cierra la conexión, el receptor ya no acepta datos pero el emisor los acepta hasta que termina de llegar la aceptación de cierre del receptor.

- El protocolo UDP

UDP permite el envío de datagramas aunque sea de la capa TCP (que trabaja con segmentos). El envío de estos datagramas no necesita tener abierta previamente una conexión. El datagrama contiene la suficiente información para poder llegar a su destino. Por lo tanto, UDP no garantiza lo que suele garantizar TCP (llegada en orden control de flujo, etc.). Aunque UDP maneja puertos y sockets.

* Nivel de aplicación

Todas las aplicaciones TCP/IP se basan en el modelo cliente/servidor.

- RPC (Llamadas a procedimientos remotos)

Una aplicación puede llamar a un procedimiento de otra aplicación (previo contrato de utilización). Este tipo de comunicación es la propia de programas de chat, de servidores de datos (MySQL), etc.

Hay dos **tipos de servidores**:

- **Servidor iterativo:** El servidor está en espera hasta que recibe la petición de un cliente, la procesa, y luego permanece otra vez a la espera.
- **Servidor concurrente:** El servidor está a la espera, cuando recibe una petición de un cliente, abre un puerto y coloca una subaplicación para servir al cliente y vuelve al estado de espera.

- Conexión remota (TELNET)

Un usuario puede acceder a otro ordenador en la red de manera que parezca que es su propio ordenador el que está manejando. Un terminal virtual de estas características utiliza un protocolo de terminal virtual para poder manejar diversidad de tipos de ordenador.

TELNET es uno de esos protocolos de terminal virtual de red. Para control TELNET utiliza secuencias de escape (códigos cortos). Hay una fase de negociación previa entre el que se conecta y el que debe aceptar la conexión.

- SMTP. Correo electrónico

El correo electrónico no es interactivo, por lo que debe de haber un lugar intermedio donde guardar la información. Una dirección de correo electrónico consta de un identificador de usuario, un símbolo de delimitación (@) y el nombre del servidor donde se aloja el correo.

SMTP también especifica el formato de los mensajes a enviar. SMTP se encarga de las gestiones de autenticación, control, etc. Se utiliza también el protocolo MIME (mensajes multimedia), POP (lectura de los mensajes en el servidor), IMAP (lectura de correo desde diversos terminales).

11. Acceso a ficheros (FTP-TFTP)

[<http://www.mailxmail.com/...curso-redes-comunicaciones-internet-3/acceso-ficheros-ftp-tftp>]

*Acceso a ficheros

Hay dos maneras de acceso remoto a fichero: o bien se accede al sitio remoto concurrentemente entre varios clientes o bien se hace una copia local y si se efectúan cambios en el fichero, se transfiere la copia al servidor de ficheros.

- Acceso mediante transferencia de ficheros (FTP-TFTP)

Un programa cliente, previa autorización del servidor, accede al servidor y descarga el fichero que desee en su ordenador local y luego cierra la conexión. FTP permite configurar una serie de parámetros para el acceso a los ficheros del servidor. Generalmente se permite el acceso concurrente de varios clientes. El control corre a cargo de la conexión que ha abierto el cliente, pero los datos van por nuevas conexiones abiertas por el servidor. Si se cierra la conexión de control, las demás también quedan cerradas.

TFTP es un subprotocolo de FTP en el que no es necesaria la autenticación del cliente. TFTP emplea UDP en vez de TCP. Se van enviando bloques de 512 bytes hasta que el último, de menos de 512 delimita el final del envío.

- NFS (Sistema de ficheros de red)

Permite acceder a ficheros remotos como si fueran locales (en cierto modo se parece a TELNET). Se realizan llamadas a procedimientos remotos mediante UDP. Cualquier cambio en los ficheros remotos, es visible para cualquier otro cliente.

- Asignación dinámica de direcciones

El protocolo DHCP permite asignar dinámicamente direcciones IP a los clientes. Estas direcciones no son permanentes y son eliminadas cuando el cliente se desconecta.

- Resolución de nombres de ordenadores

Cada host tiene su dirección IP y un nombre de equipo. Es posible conectar con sólo indicar el nombre de equipo. Los servidores DNS es un sistema distribuido a lo largo de la red que se encarga de traducir direcciones IP a nombres de host y viceversa. Hay distintas **categorías de servidores DNS**:

- 1. Servidor de nombre primario:** Mantiene nombres de una zona y direcciones de contacto de servidores de otras zonas.
- 2. Servidor de nombre secundario:** Obtiene nombres de otros servidores y los guarda en unas tablas.
- 3. Servidor de nombre maestro:** Se encarga de transferir archivos de nombres a servidores secundarios.
- 4. Servidor de nombre sólo de caché:** No guarda nombres, sólo se encarga de transferir nombres entre servidores y mantener los datos momentáneamente en memoria.

- El lenguaje HTML

Es el lenguaje utilizado para crear páginas Web. Sigue las consignas del metalenguaje XML.

- El protocolo http

Http realiza una conexión con un servidor mediante TCP para cada función que realiza. Primero se identifica el URL o dirección del cliente, después se solicita el nombre DNS de esa dirección, después se establece una conexión TCP con la IP recibida, después se emite la petición GET con la página deseada y después se envía la página del servidor al cliente. Una vez que se ha completado el proceso, el cliente puede visualizar la página.

Hay tres tipos de **sistemas intermedios**:

- 1. Representante (proxy):** Recoge las peticiones de sus clientes y las presenta al servidor.
- 2. Pasarela (gateway):** Es un servidor que puede representar a otros servidores (puede ser un cortafuegos).
- 3. Túnel:** Es sólo un punto de transmisión entre dos conexiones.

12. IP de nueva generación

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/ip-nueva-generacion>]

*IP de nueva generación

Debido al amplio crecimiento de la red, los 32 bits de dirección son insuficientes. Por ello se ha creado IP versión 6 (la normal es la 4).

- Mejoras de IP v6

1. Direcciones de 128 bits.
2. Mejoras en las opciones.
3. Asignación dinámica de direcciones.
4. Flexibilidad en el direccionamiento.
5. Facilidad para la asignación de recursos.
6. Capacidades de seguridad.
7. Eliminación de control de errores de cabecera.
8. Fragmentación sólo en la fuente.

- Estructura de la trama (PDU) en IPv6

Consta de una cabecera IPv6 de 40 bytes (IPv4 es de 20 bytes). Los campos de la cabecera son 8 frente a los 13 de IPv4. El campo de clase de tráfico permite diferenciar los datagramas en prioridades o clases para un mejor tratamiento. Desde el origen, hay una etiqueta de flujo que tienen todos los datagramas que pertenecen a la misma transmisión lógica.

- Direcciones IPv6

Consta de 128 bits. Cada nodo tiene una interfaz que identifica a múltiples destinos (o a uno sólo).

Hay tres **tipos de direcciones**:

- 1. Unidistribución:** Un identificador para una interfaz individual.
- 2. Monodistribución:** Un identificador para un conjunto de interfaces. Un paquete enviado a este tipo de dirección es captado por una interfaz de las identificadas por esa dirección.
- 3. Multidistribución:** Un identificador para un conjunto de interfaces. Un paquete enviado a una dirección de este tipo se entrega a todas las interfaces identificadas por esa dirección.

Las direcciones constan de grupos de 16 bits separados por ":". Estos 16 bits se codifican en hexadecimal. Cuando hay un grupo de 0, se sustituye por "::". Por ejemplo:

"5566:FFEE:54AB:F4F5:5434:09DE:43D5:FF00" o "6655:E443:87C6:6578::" que equivale a "6655:E443:87C6:6578:0000:0000:0000:0000".

- Cabeceras adicionales de IPv6

Entre la cabecera de TCP y la de IP se pueden incluir cabeceras adicionales de longitud múltiplo de 8 bytes. Estas cabeceras deben aparecer en orden (si las hay), Y Son:

1. **Cabecera nodo por nodo:** Contiene información de los nodos por los que ha viajado el paquete.
2. **Cabecera de encaminamiento:** Contiene una lista de nodos intermedios por los que debe viajar el paquete (la establece el emisor).
3. **Cabecera de fragmentación:** Permite enviar paquetes de un tamaño superior al normal. La fragmentación sólo se hace en IPv6 en el origen y no en los nodos intermedios.
4. **Cabecera de autenticación:** Sirve para autenticar y asegurar la integridad de los paquetes.
5. **Cabecera de confidencialidad:** Se encarga de encriptar los datos para hacerlos seguros en el camino. Si está presente, a partir de ella, toda la información está ya encriptada.
6. **Cabecera de extremo a extremo:** Da una información opcional controlada por el destinatario.

13. Internet. Calidad de servicio

[<http://www.mailxmail.com/...curso-redes-comunicaciones-internet-3/internet-calidad-servicio>]

*Calidad de servicio en Internet

Se define la calidad de servicio (CdS o QoS) como la capacidad que tiene un sistema de asegurar, con un grado de fiabilidad preestablecido, que se cumplan los requisitos de tráfico para un flujo de información dado.

Los proveedores de servicio son los encargados de prestar los servicios de Internet. Cada proveedor tiene una red propia dentro de Internet que provee una serie de servicios a sus clientes. Dentro de estos proveedores, los hay más grandes (que engloban a otros más pequeños) y más pequeños. Los más grandes son los proveedores troncales (ISPn1). Estos proveedores grandes, que prestan servicio a otros más pequeños (ISPn2) deben tener unas infraestructuras de alto rendimiento. Los ISPn1 prestan sus servicios a los ISPn2 (se llama servicio de tránsito). Los ISPn2 prestan sus servicios o bien a grandes corporaciones o a ISPn3. Los ISPn3 son los que prestan sus servicios a los pequeños clientes o particulares. Prestan el llamado servicio de acceso.

*Parámetros de calidad de servicio

- 1. El retardo:** En TCP, cuanto mayor es el retardo, más grande se hace y llega a no haber servicio. En UDP, el aumento de retardo hace que llegue a ser imposible la comunicación.
- 2. Variación del retardo de transmisión (jitter):** Es la fluctuación del retardo de tránsito entre extremos. TCP hace que si aumenta mucho la variación de retardo, las estimaciones se hagan conservadoras y disminuya mucho el rendimiento. En UDP puede llegar incluso a distorsionarse la señal en el destino.
- 3. Ancho de banda:** Es la máxima velocidad de transferencia de datos entre extremos de la red.
- 4. Fiabilidad:** Es la tasa media de error de la red. TCP corrige este problema con retransmisiones. En UDP, como no hay retransmisiones, la señal llega distorsionada (ya que UDP se encarga de transmisiones en tiempo real).

*Procedimientos de calidad de servicio

Las diversas **clases de servicio** son:

- 1. Colas basadas en clases (CBQ):** El tráfico se clasifica en clases y se pone en una cola diferente para cada clase. Cada clase tiene una prioridad y un rendimiento. Hay mecanismos para establecer esas colas. Cada clase tiene asignado su ancho de banda que puede ser dinámico o estático. Cada clase debe recibir aproximadamente su ancho de banda y si una clase no tiene tráfico, se debe distribuir proporcionalmente el ancho de banda disponible entre las demás clases.
- 2. Colas equitativas ponderadas (WFQ):** Se reparten equitativamente los recursos entre todas las colas. El tráfico de poco volumen tiene preferencia.
- 3. Tasa de acceso entregada (CAR):** Se distribuye el tráfico en diferentes niveles de prioridad. Los paquetes se clasifican según su prioridad. Al tráfico que está dentro

de los límites de su contrato de servicio, se le deja pasar y el resto se descarta o se transmite si sobra ancho de banda. Para ver si hay ancho de banda suficiente se utiliza el algoritmo del cubo de fichas. Cuando el tráfico es conforme se procede a su envío.

4. Descarte aleatorio anticipado (RED): Se le indica a los sistemas finales cuándo deben dejar de enviar paquetes (para evitar la congestión). Cuando se pasa un nivel de peligro se empiezan a descartar aleatoriamente paquetes y se le indica al emisor que disminuya su tasa de envío hasta que se descongestione el sistema. Si aún así se sobrepasa un límite máximo, se descartan todos los paquetes.

***Arquitectura de Cds**

La aplicación se encarga de pedir a la red el servicio que desea y si la red lo puede procesar, responde afirmativamente. La arquitectura de servicios integrados (ISA) utiliza este punto de vista. Es todo o nada, o la red admite la petición o no la admite.

La arquitectura de servicios diferenciados (DiffServ) utiliza otro sistema que es que no solicita un servicio preferencial a la red sino que marca cada datagrama con el tipo de servicio que se desea para él. Entonces serán sólo ciertos datagramas los que corran el riesgo de ser declinados por la red y no todo el tráfico como en ISA. La arquitectura MPLS es otro tipo de arquitectura que selecciona rutas acordes con el tipo de servicio que quiere.

14. Servicios integrados, protocolo RSVP y servicios diferenciados

[<http://www.mailxmail.com/...net-3/servicios-integrados-protocolo-rsvp-servicios-diferenciados>]

Servicios integrados y protocolo RSVP

*Planteamiento y objetivos

Hay varios niveles de calidad:

- 1. Mejor esfuerzo (BE):** El servicio normal de datagramas de Internet. No hay aseguramiento de llegada de paquetes.
- 2. Carga controlada (SCL):** Si minimiza el peligro de pérdida de paquetes aunque no se asegura un retardo pequeño.
- 3. Calidad garantizada (SG):** Se asegura que no hay pérdidas de paquetes un además que llegarán en un tiempo máximo establecido.

*Modelo de la arquitectura de servicios integrados

RSVP se encarga de gestionar reservas de recursos a lo largo de todos los nodos de la red. Por lo tanto, debe estar presente en todos ellos para que la calidad se garantice.

Cuando es aceptada una transmisión por parte del RSVP del emisor, se envía un paquete que informa a los nodos intermedios de que se va a proceder a transmitir. Una vez que el receptor es avisado, envía al emisor una confirmación. Es decir, se hace una reserva en cada nodo para la comunicación. Esta reserva debe refrescarse periódicamente.

ISA mantiene una comunicación simplex entre el emisor y el/los destinatarios. En cada nodo hay una serie de colas y un control de tráfico encargado de todo el proceso.

*Protocolo RSVP

Es el encargado del control de todo el sistema de envío de paquetes entre el emisor y el receptor (y los nodos intermedios) para poder implementar una calidad de servicio. Opera sobre IP y reserva recursos en cada nodo de la ruta. Una sesión RSVP consta de una dirección de destino, un identificador del protocolo IP y un puerto de destino.

Cada emisor que utiliza RSVP intenta reservar recursos a lo largo de todo el camino hasta el receptor, pero sólo se le reservarán sin en los nodos intermedios es el solicitante más prioritario. Cuando se ha conseguido la reserva y es confirmada, se procede al envío de datos. Para realizar reservas es necesario que haya una autorización y que haya recursos para atenderla.

Arquitectura de servicios diferenciados

*Definición y objetivos

Se trata de diferenciar cada paquete y darle un trato dependiendo del servicio que necesite. Los paquetes se marcan y clasifican para recibir un tratamiento específico por salto en la ruta. Esta política de clasificación sólo se implementa en las fronteras

de la red y no en los nodos intermedios.

Se trata de dividir los **paquetes** en distintas clases que requerirán distintos servicios. Los **4 básicos** son:

- 1. PHB por defecto:** Es el menos riguroso y equivale a enviar si se puede y si no, descartar.
- 2. PHB selector de clase:** Si no hay congestión, se asegura el envío y si la hay, no.
- 3. PHB de reenvío explícito:** Se garantiza un ancho de banda, se asegura que no hay pérdidas, poca latencia y variación de retardo (para videoconferencia, etc.).
- 4. PHB de reenvío asegurado:** Se garantiza que no hay pérdida de paquetes.

15. Dominio MPLS

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/dominio-mpls>]

Dominio MPLS

*Introducción

Cuando los nodos intermedios en una red IP deben manejar mucha información, hay que aumentar sus prestaciones, pero eso tiene un límite. Para intentar no tener que llegar al límite se ha creado una solución que se llama conmutación de etiquetas.

El nodo de entrada se encarga de decidir el camino a seguir por el paquete. Este camino se codifica en una etiqueta que se incluye en el paquete. Los nodos intermedios no inspeccionan toda la cabecera sino sólo la etiqueta (lo cuál es mucho más rápido y satura menos al encaminador o nodo intermedio).

*MPLS

MPLS trabaja sobre la capa de red y debe funcionar sobre cualquier capa de enlace. MPLS debe funcionar sobre IP y puede ser punto a punto o punto a multipunto (difusión).

- Descripción funcional

Conceptos:

- **Encaminamiento:** Son las acciones realizadas por los elementos de red para mover los paquetes a través de la red.
- **Conmutación:** Es el mecanismo de transferir información desde un puerto de entrada a uno de salida en la capa de enlace (la 2).
- **FEC:** Son los paquetes que van a llevar la misma etiqueta (llevan el mismo camino dentro de la red).
- **Etiqueta:** Es un identificador de longitud fija, y corto para describir un camino en la red.
- **Dominio MPLS:** Conjunto contiguo de nodos que soportan MPLS dentro del mismo dominio IP.
- **LER:** Nodo capaz de conectar con nodos externos al dominio.
- **LSR:** Nodo interno que admite MPLS.
- **LSP:** Camino de datos dentro de un dominio MPLS.

Los nodos de la frontera del dominio MPLS y los internos deben tener unas tablas de encaminamiento. Cuando un tráfico entra en la red, se le añade una etiqueta de encaminamiento, los nodos internos analizan esa etiqueta y van reenviando a otro nodo hasta que llega la información al nodo frontera de salida de la red MPLS, donde se le quita la etiqueta y se le envía a su destino.

Hay dos maneras de manejar las tablas de etiquetas, o bien se conservan para próximos envíos o bien se eliminan cuando a pasado el tráfico que las utiliza. Una de las aplicaciones de MPLS es la de solventar el problema del enrutado que hacen los algoritmos antiguos sobre IP (ya que el camino más corto hace que se saturen ciertos nodos de la red) al hacer posible un enrutado manual.

16. Redes ópticas

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/redes-opticas>]

Redes ópticas. DWDM (Multiplexación por división densa de ondas)

Se pueden hacer dos cosas para aumentar el ancho de banda de una fibra óptica: aumentar la velocidad de transmisión o aumentar el número de longitudes de onda que viajan por la misma fibra.

*DWDM

DWDM proviene de DWDM (Multiplexación por división en longitud de onda). Se trata de una tecnología que permite acoplar muchas longitudes de onda distintas en la misma fibra. DWDM es sólo una condensación mayor de longitudes de onda que DWDM. DWDM ha sido posible por el gran avance en la tecnología óptica, al disminuir los costes y aumentar las prestaciones de los componentes ópticos.

- Sistemas WDM opacos y transparentes

Los WDM opacos reciben información óptica de la fibra, la demultiplexan y la convierten en eléctrica. Un sistema electrónico trata la señal eléctrica y al final es multiplexada y convertida otra vez en óptica y pasada a la fibra. Los sistemas transparentes no convierten la señal en eléctrica sino que operan en el rango de la óptica.

*La fibra óptica

La fibra óptica es inmune a las interferencias electromagnéticas, no se oxida y tiene un amplísimo ancho de banda. Los cables de fibra óptica presentan varias capas que los hacen muy seguros y fiables y los aíslan de posibles interferencias y roturas. Dependiendo del grosor de la fibra, puede ser multimodo o monomodo.

La luz se propaga a lo largo de la fibra por un canal central cuyas paredes la reflejan, de forma que va "rebotando" por las paredes internas hasta que llega a su destino. En una misma fibra se pueden enviar rayos luminosos a diferentes longitudes de onda sin que haya apenas interferencias entre ellos. Si se quieren eliminar del todo las interferencias, se utiliza fibra monomodal, donde un solo rayo viaja por el centro de la fibra.

- Interconexión óptica

El gran problema a resolver en la tecnología óptica es cómo mantener la luz encajada en las interconexiones de dos fibras. ¿Cómo manejar la luz en los conmutadores ópticos para que no se "escape"? En los terminales de una fibra, se puede pasar la luz a electricidad o se puede mantener como luz. El método más empleado en la actualidad es el primero (debido a que hasta hoy no se había avanzado lo suficiente en la tecnología óptica).

- Los multiplexores ópticos

Son mecanismos capaces de unir varias longitudes de onda en una fibra para ser enviadas. Los demultiplexores hacen lo contrario. Estos aparatos se llaman OADM (Multiplexor incrementador/decrementador óptico).

***Sistemas DWDM**

La transmisión se divide en canales. Cada canal puede viajar a diferentes velocidades. Cada canal puede utilizar más de una longitud de onda. Son como circuitos virtuales. Cada canal tiene alrededor de la longitud de onda central, un espacio vacío para evitar interferencias entre longitudes de onda contiguas. La señal ha de ser amplificada cada 80 km aproximadamente.

Topologías de redes DWDM*- Redes punto a punto**

Se emplea para largas distancias por su gran velocidad de transmisión. Los multiplexores (OADM) permiten añadir o extraer canales a lo largo del trayecto.

- Redes en anillo y estrella

Se suele emplear en redes locales (con un anillo o dos para seguridad). Existe un nodo que es el concentrador. Cada nodo tiene su OADM para extraer e insertar canales al anillo. El concentrador es el comienzo y el fin de la señal que circula por el anillo. El concentrador administra los canales. Suele haber menos nodos que canales en la fibra (para que no se sature).

***Reconocimiento ultrarrápido de patrones**

Debido a la alta velocidad en que se opera, se necesitan dispositivos de reconocimiento de patrones muy rápidos. Estos reconocedores se llaman CAM y suelen ser memorias ultrarrápidas. También se pueden utilizar memorias convencionales RAM.

***Tendencias futuras**

Para trabajar IP sobre DWDM, se colocan capas intermedias, IP sobre ATM, sobre SDH y sobre DWDM. La tendencia actual es eliminar ATM. E incluso situar MPLS en vez de SDH. Otra tendencia es a utilizar NSDM que es una tecnología más avanzada que DWDM y que permite reducir el espaciado perdido entre canales consecutivos.

17. Redes para móviles. WAP

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/redes-moviles-wap>]

Redes para móviles

*WAP

El protocolo de aplicaciones inalámbricas (WAP) es un protocolo para desarrollar aplicaciones para móviles. Está basado en el modelo Web. El principal obstáculo es que los teléfonos móviles actuales no están adaptados para ello. Para poder hacer una adaptación de HTML a los lenguajes de WAP se han creado unos minilenguajes, descendientes de HTML y más simples que él.

*Arquitectura

Consta de las siguientes **capas**:

Capa de aplicación
Capa de sesión
Capa de transacciones
Capa de seguridad
Capa de transporte
Capas propias de los móviles

*Características

La comunicación se basa (como http) en cliente-servidor. Todas las transacciones van comprimidas y hay una optimización de todo el envío.

Existe un navegador, una pasarela y el propio servidor. El navegador traduce WML a la pantalla. Es un estándar libre, independiente de la tecnología de la red sobre la que se opera, ejecuta acciones en el servidor.

Ya se ha dicho que se compone del terminal, la pasarela (que se encarga de pasar las peticiones a la Web y de recibir las respuestas) y del servidor.

*Puntos fuertes y débiles Sus puntos fuertes son:

- Interoperatividad
- Seguridad
- Escalabilidad

Puntos débiles:

- Poca riqueza
- Necesidad de adaptar las páginas al sistema WAP
- Seguridad

18. Sistemas GPRS y UMTS

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/sistemas-gprs-umts>]

Sistema GPRS

*Introducción

Es un sistema de transmisión de paquetes sobre GSM. Se usa para datos y es muy parecido a IP.

GPRS utiliza los canales sólo cuando va a transmitir datos (GSM los abre durante toda la llamada). Por lo tanto, un mismo canal puede ser utilizado por varios usuarios.

GPRS permite casi todo lo que se permite en Internet más todo lo que se permite con GSM.

La facturación para datos se hace en función de la cantidad de datos transmitidos y no en función del tiempo utilizado (como GSM).

*Funcionamiento de GPRS

Funciona igual que IP, con paquetes que viajan a su destino troceados y ensamblados en él. Los datos comparten frecuencias por lo que puede haber varios usuarios utilizando las mismas antenas (células) móviles y las mismas frecuencias. GPRS permite al acceso limpio a Internet, por lo que tiene asignada su propia dirección IP.

La transmisión puede ser punto a punto (con datagramas independientes o con una conexión virtual entre cada extremo) o punto a multipunto. Para que se implante GPRS ha sido necesario que se creen nuevos nodos o células con funciones que no soportaba GSM.

*Tipos de servicio GPRS

El tipo PTP (punto a punto) puede asumir uno de los estados: dormido (sólo funciones de control), reposo (pendiente de comunicarse) y activo (enviando o recibiendo paquetes).

El paso de dormido a reposo implica que se establece una comunicación y autenticación entre los dos extremos (se establece una especie de canal virtual). En el estado de reposo hay que estar redituando el móvil en cada momento para estar a punto para poder enviar o recibir datos.

El tipo PTM (punto a multipunto) permite la difusión de información a varios destinatarios dentro del mismo área ya sea a todos o a un grupo de ellos (se utiliza para publicidad). Dependiendo del tipo de terminal, será posible la utilización o no de PTM.

Para GPRS funcione con suficiente calidad, es necesario que haya unas mejoras en la red y que se puedan emplear más capacidades de las asignadas en este momento para esta tecnología.

Sistema UMTS

***Introducción**

El UMTS (Sistema de comunicaciones móviles universal) pretende ampliar las funcionalidades de GPRS. UMTS las llamadas de voz y datos recorren el mismo camino en la red de acceso y se bifurcan en la red de conmutación. Hay una red para atender las llamadas de voz y otra para la de datos.

***Características generales de los sistemas 3G**

Los sistemas 3G o de tercera generación, como UMTS permiten la transmisión de datos a alta velocidad y garantía de calidad de servicio. Son una ampliación de GPRS.

***Arquitectura UMTS**

Se divide en tres capas: capa de acceso o física, capa de conectividad o de enlace de datos y capa de servicios o de red. Como ya se ha dicho, hay dos redes de conmutación, una para voz y otra para datos.

NOTA: Con este capítulo hemos llegado al final de nuestro curso.

Visita más cursos como este en mailxmail:

[<http://www.mailxmail.com/cursos-informatica>]

[<http://www.mailxmail.com/cursos-software>]



¡Tu opinión cuenta! Lee todas las opiniones de este curso y déjanos la tuya:

[<http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/opiniones>]

Cursos similares

Cursos	Valoración	Alumnos	Vídeo
Windows Vista Microsoft Windows Vista es la versión del sistema operativo Microsoft Windows que sucede a Windows XP. Windows Vista presenta una experiencia de usuario avanzada y está d... [21/11/07]		24.915	
Curso de E-Business En la actualidad esta surgiendo una nueva forma de hacer negocios. Esta se basa en la nueva tecnología conocida por muchos como Internet, aunque surgió antes que Internet... [12/01/06]		2.292	
DSSS Comunicaciones en banda base utilizando el espectro ensanchado Las comunicaciones en espectro ensanchado en la actualidad tienen bastantes aplicaciones entre las que se incluyen la telefonía celular y redes locales de datos, entre ot... [12/11/04]		1.505	
Aprende Word Este curso está destinado a los principiantes. A todos aquellos que necesitan una introducción detallada para moverse dentro de este programa. Está basado en ejercicios prá... [27/09/05]		4.398	

Windows XP. Sistemas operativos (primera parte)

En este curso sobre el Sistema operativo Windows XP estudiaremos el concepto del sistema operativo, sus funciones básicas y los tipos de sistemas operativos. Aprende el m...

[08/10/08]

●●●●● 12.431