1201

COMPONENTES DE REDES IP

Sobre los atributos de las redes de datos y los diferentes tipos de redes comerciales. Referido a las funciones de hub, switch y routers de red. Referido a los server para redes IP.

1- INTRODUCCIÓN

1.1- COMPONENTES DE UNA RED

Por una red de datos se entiende la posibilidad de comunicación entre elementos informáticos (entidades de un sistema). La selección de la red de datos apropiada debe atender a un componente estratégico (planeamiento a largo plazo) y otro táctico (desarrollo a corto plazo). La más simple de las redes de datos es la comunicación punto-a-punto entre PC mediante módem analógicos que funciona con el soporte de la red de telefonía **PSTN**. Desde Window 95 es posible la comunicación entre computadores mediante la puerta paralelo **LPT** (conector DB-25) sin requerir un hardware adicional.

COMPONENTES DE UNA RED. Los elementos que componen una red de datos son:
-Software. Se trata del software de comunicación que trabaja apoyado sobre el sistema operativo del computador.
-Server. Permite administrar la memoria, el backup de archivos (*file*), el servicio de correo electrónico (*mail*) y el facsímil electrónico, la comunicación con sistemas remotos, la base de datos y directorios, la administración de la impresora. El concepto de trabajo *client/server* se ha introducido en 1987 para ambientes de operación LAN.
-Sistema de cliente (Nodos y *Workstations*). Se trata de las PC que se conectan a la red LAN y que completan el concepto cliente/servidor. Se utiliza para procesador de palabra, diseño gráfico, base de datos, gestión de proyectos, etc.
-Interfaz de red **NIC** (*Network Interface Cards o Network Board*). Conecta una PC a la red de datos; se trata de un circuito conectado a la unidad maestra de la PC. Cumple funciones de capa 1 para conexión al medio físico de enlace.
-Hub/Bridge/Switch/Router/Gateway. Permite reunir en un punto los elementos de la red. Se trata de componentes activos que regeneran las señales de datos, direccionan paquetes, evalúan protocolos y pueden tener funciones de supervisión remota.

1.2- FUNCIONES DE LOS PROTOCOLOS

Un protocolo es normalmente un software que realiza un conjunto de funciones. Esto define las acciones que cumple cada capa de la red de datos. Las **funciones** de un protocolo son entre otras las siguientes:
-Segmentación y encapsulado en transmisión y ensamble en recepción de secuencias extensas de datos.
-Multiplexación e identificación de tramas de distintos usuarios de capas superiores.
-Control de conexión (inicio y final de llamada) y control de flujo de datos.
-Control de paridad para detección de errores y el descarte de tramas o pedido de retransmisión de las mismas.
-Selección de ruta (conmutación) o filtrado de direcciones cuando corresponde.
-El control de flujo de datos para detener la emisión cuando el receptor no está disponible.

SEGMENTACIÓN y ENSAMBLE. Las razones que son mencionadas para efectuar la segmentación de los datos a transmitir incluye:
-La distribución del medio de enlace en forma más equitativa entre los usuarios,
-La segmentación permite disminuir el retardo de acceso e impide la monopolización del medio de enlace,
-Permite que el tamaño del buffer requerido para los datos sea más pequeño,
-Se logra un control de errores más eficiente cuando los segmentos son pequeños,
-Permite la retransmisión de tramas más cortas.

Sin embargo, una segmentación en paquetes pequeños tiene sus desventajas:
-Reduce la eficiencia de datos al involucrar un encabezado proporcionalmente mayor,
-Los bloques pequeños pueden involucrar también un número mayor de interrupciones,
-Se requiere un tiempo mayor de procesamiento.

CONTROL DE FLUJO DE DATOS. Este concepto se refiere a la capacidad del receptor de controlar la emisión de datos desde el otro extremo. Los métodos usados son varios, dependiendo de la capa involucrada. Sobre la capa 1 es un control eléctrico (hardware) en tanto que sobre las capas superiores se realiza en forma de secuencia de datos (software).

Por ejemplo, sobre la interfaz RS-232 (Capa 1) se dispone de un hilo de solicitud de transmisión **RTS** (*Request to Send*) y otro de autorización **CTS** (*Clear to Send*) para la transmisión de datos. Otra técnica posible se denomina asincrónica y se conoce como **XON/XOFF**. Se aplica para conexión del computador con un módem de datos. De esta forma el módem puede controlar la llegada de datos desde la PC hacia la línea telefónica cuando el buffer se encuentra saturado (señal XOFF hacia el computador para detener la emisión y XON para reiniciarla; caracteres ASCII 19 y 17 respectivamente).

En varios protocolos de capas superiores se involucra el reconocimiento **ARQ** (*Automatic Request Repeat*) de las tramas recibidas. Se trata de numerar las tramas sucesivas emitidas y confirmar el número de la trama correctamente recibida. Tal caso se presenta sobre la capa 2 en los protocolos de tipo **HDLC** (por ejemplo, LAP-B en X.25). Para mejorar la eficiencia se adopta una **ventana o crédito** (*Window*), de forma que el emisor continúa emitiendo tramas, aún sin recibir el reconocimiento, hasta el valor del crédito establecido. En Frame Relay se adoptan **alarmas** enviadas hacia adelante y atrás para controlar el flujo de datos cuando existe congestión en un nodo de la red.

En el protocolo TCP/IP (capa 4/3 del modelo ISO) se adopta un control de flujo más sofisticado: con cada trama de TCP se envía el valor de la ventana (**WIN**) consistente en un campo de 2 bytes que indica la cantidad de bytes que pueden ser transferidos en el próximo paquete.

CONTROL DE ERRORES. Se involucra un campo de bits de paridad (*checksum* o CRC-16/32) que permite determinar las tramas con error. En este caso se puede efectuar el descarte de la trama de datos afectada (Frame Relay o ATM) o pedir la repetición automática **ARQ** (protocolos X.25 y redes LAN). El checksum se calcula como la suma binaria de los datos transmitidos y es menos eficaz que el chequeo de redundancia cíclica CRC.

CONTROL DE CONEXIÓN. El tipo de **Servicio ofrecido** por la red es:
-Orientado con-conexión (*Connection-Oriented*),
-Orientado sin-conexión (*Connection-less Oriented*).

El Servicio **orientado con-conexión** se modela de acuerdo con el sistema telefónico y el servicio **orientado sin-conexión** de acuerdo con el correo postal. En el primero se establece inicialmente una conexión (canal virtual) y se mantiene hasta la desconexión. En el segundo cada mensaje lleva la dirección completa y el enrutamiento es independiente para cada mensaje. Esto puede producir que el arribo de los mensajes esté fuera de orden. En el primero es más fácil el control de flujo para la congestión y el encabezado más corto.

El servicio sin-conexión es solicitado por los usuarios de redes de datos debido a que permite el arribo de las tramas aún con interrupción de ciertos enlaces en una red malla. En tanto el servicio con-conexión es el generalmente soportado por las empresas de telecomunicaciones por la simplicidad sobre los nodos de enrutamiento. Sin embargo, esta diferencia no es muy apreciable: en con-conexión es posible un re-enrutamiento automático (aplicado en X.25, por ejemplo) y en sin-conexión el trayecto en la red es mantenido a menos que exista una razón para cambiarlo.

DIRECCIONAMIENTO. En una red de datos se requiere la identificación de los usuarios que participan en la conexión mediante las direcciones de origen y destino. Estas direcciones pueden ser físicas (mediante *hardware* o *firmware* en una memoria EPROM) o lógicas (establecida mediante el sistema operativo de la red).

El direccionamiento provoca una característica denominada **Latencia**: Un switch no puede direccionar un paquete hasta recibir el campo de control de errores (contenido al final del paquete) y verificar su correcto estado. Si existiese un error y se encontrase en el campo de dirección, el enrutamiento sería incorrecto. La latencia incrementa el retardo y obliga a una mayor velocidad en las redes. Esta acción ha determinado un servicio especial en las redes conmutadas de paquetes que se denomina *Store-and-Forward* (memorizando los datos en la red y transmitiendolos en horarios de tarifa reducida).

1.3- ATRIBUTOS DE LAS REDES DE DATOS .

Al final de este trabajo se presenta una clasificación de las redes de datos. Los enlaces y las redes de datos poseen características (**atributos**) que permiten varias clasificaciones (ver **Tabla 01**). Debe tenerse en cuenta que el modelo de capas, surge de la secuencia de conceptos de enlace, de red y de servicio.

Tabla 01: Características (atributos) fundamentales de las redes de datos.

ENLACE.	Surge con la necesidad de comunicar dos puntos y lleva asociados los siguientes conceptos: Sistema: teoría de la información, teoría de señales y del ruido, Bidireccionalidad: considera la estabilidad, el eco, la atenuación y los equivalentes de referencia, Multiplexado: FDM (potencia, ruido, diafonía e intermodulación) y TDM (muestreo y codificación), Transmisión: medios de enlace y ecuación del enlace, la modulación y los errores.
RED.	Se desarrolla como una estructura bidimensional de enlaces que involucra: Topología y Enrutamiento (el tránsito, desborde y jerarquía). Conmutación y Concentración (el tráfico, la pérdida de información y la espera). Señalización (establecimiento, desarrollo e interrupción de servicio).
SERVICIO.	Se estructura sobre la red como un conjunto de 7 capas. Involucra: Protocolos: permiten realizar operaciones para servir a la capa superior.
	ATRIBUTOS
Duplexión	Simultaneidad en la transmisión y recepción de datos: -Simplex (conexión unidireccional). -Half-dúplex (conexión bidireccional con transmisión alternativa). -Full-dúplex (bidireccional simultánea).
Cadencia	Forma de la emisión de datos. -Asincrónicos (emisión por ráfagas de caracteres, start-stop). -Sincrónicos (emisión periódica y continua).
Sincronismo	Determinada por las redes de transporte. Tendencia desde PDH a SDH. -Plesiócronas (emisores con distinto reloj) PDH. -Sincrónicas (dependientes de un solo reloj) SDH.
Segmentación	Tipo de segmentación de datos. -Por paquetes/tramas/segmentos/datagramas (longitud variable de Bytes). -Por celdas (longitud constante).
Conmutación	Se refiere a la forma de mantener la conexión entre extremos. Ver también Orientación. -Punto a punto (E1/T1). -Redes con conexión virtual conmutada **SVC** por paquetes (X.25). -Redes con conexión permanente **PVC** (Frame Relay, ATM).
Extensión	-Redes de área local LAN (Ethernet y token ring), -Red de área metropolitana MAN (FDDI, DQDB). -Red de área extendida WAN (X.25, Frame Relay y ATM).
Topología	-Redes en estrella y malla (red conmutada WAN). -Bus (LAN Ethernet), y Doble-bus (MAN-DQDB; ATM). -Anillo (token ring) y Doble anillo (FDDI).
Estructura	-Enlace (unidimensional); Red (bidimensional) y Servicio (tridimensional).
Orientación	-Con-conexión (enrutamiento igual para todos los paquetes de la conexión virtual). -Sin-conexión (enrutamiento independiente para cada paquete).
Control flujo	Se refiere a la forma en que el receptor puede controlar la emisión de datos desde el transmisor. -Fuera de banda (del tipo RTS/CTS) y dentro de banda (Xon/Xoff). -Del tipo *Stop and wait* **ARQ** (ejemplo, protocolos LAP-B/D). -Mediante un crédito variable (ejemplo, protocolo TCP en capa 4).
Control error	-Mediante chequeo de paridad de la trama completa (Frame Relay) o solo del encabezado (ATM). -En base a los errores se puede retransmitir (X-25) o descartar la trama (Frame Relay).

2- REDES DE DATOS COMERCIALES.

En la **Tabla 02** adjunta se muestran las redes de datos comerciales. Las redes de área local **LAN** (Ethernet y Token Ring) permiten la interconexión en un área restringida de elementos informáticos. La interconexión de LAN se puede efectuar mediante redes punto-a-punto E1-Fraccional, mediante redes de área metropolitana **MAN** (FDDI y DQDB) y redes de área extendida **WAN** (X.25, Frame Relay y ATM). La red **Internet** involucra funciones de capas 3/4 y superiores; hacen uso de las redes anteriores que involucran las capas 1/2. La red **ISDN** ocupa la capa 1 para la integración de usuarios digitales; en tanto que la señalización se efectúa mediante la red **SS7** y **DSS1**.

Tabla 02: Comparación de las características principales de las redes de datos que se disponen comercialmente.

Denominación.	**Ethernet**	**Token R**	**FDDI**	**DQDB**	**E1-Frac**	**X.25/75**	**F. Relay**	**ATM**	**Internet**	**ISDN**	**SS7**	**DSS1**
Extensión de la red	LAN	LAN	MAN	MAN	WAN	WAN	WAN	WAN	WAN	WAN	WAN	WAN
Tipo de conexión	P-a-Punto	P-a-Punto	P-a-Punto	Conmutada	ADM	Conmutada	P-a-Punto	Conmutada	Conmutada	Conmutada	Dedicada	Dedicada
Normalización	IEEE 802	IEEE802	ANSI	IEEE 802		ITU-T X	ITU-T I	ITU-T I		ITU-T I	ITU-T Q	ITU-T I
Período de normalización	1973-85	1980-85	1985-88	1985-88		1976-88	1988-92	1984-92	1970-82	1976-88	1976-88	1976-88
Tipo de usuario	PC	PC	LAN	LAN	Varios	Telex/PC	PC/LAN	Todos	PC/LAN	Tel/Datos	Señaliz.	Señaliz.
Modelo de capas	1-2	1-2	1-2	1-2	1	1-2-3	1-2	1-2	3-4	1	1-2-3-4	1-2-3
Capa Física.												
Velocidad en bit/s	10 M	4/16 M	100 M	34/140 M	2 M	64 K	Nx64 K	Nx155 M		144 K	64 K	16 K
Medio físico	coaxial/par	par trenz.	F.Optica	F.Optica						Par		
Topología de red	bus/árbol	Anillo	Doble anilo	doble bus	malla/anilo	malla		malla/anilo	malla	Estrella	malla	estrella
Acceso al medio	CSMA/CD	Token	Token	Cola DQ		PAD	FRAD					
Capa de segmentación.												
Número de capa	2	2	2	2	---	2/3	2	2	3/4	---	2	2
Segmentación de datos	Trama	Trama	Trama	Celda		Paquete	Trama	Celda	Datagrama		Mensaje	
Mensaje:												
Tipo de capa 2	LLC	LLC	LLC			LAP-B	LAP-F				HDLC	LAP-D
Longitud de trama Byte	max 1536	max 4500	max 4500	53 By		max 141		53 Byte			max 70	
Delimitación de trama	Preámbulo	Preámbulo	Preámbulo	HEC		Bandera	Bandera	HEC			Bandera	Bandera
Enrutamiento	Dirección	Dirección	Dirección	VPI/VCI		Dirección	DLCI	VPI/VCI			Dirección	Dirección
Tipo de conexión	Sin-conex	Sin-conex	Sin-conex	Con-conex		C.Virtual	C.Virtual	C.Virtual	Sin-conex		Sin-conex	Sin-conex
Control de error	CRC-32	CRC-32	CRC-32	CRC-8		CRC-16	CRC-16	CRC-8			CRC-16	CRC-16
Corrección de errores	ARQ	ARQ	ARQ	No		ARQ	No	No	ARQ		ARQ	ARQ
Control de flujo de datos	RNR	RNR	RNR			RNR	B/FECN	No	Crédito		Crédito	RNR
Crédito de tramas	127	127	127			7			variable		7	7

3- COMPONENTES DE LA RED

Los objetivos del presente trabajo se centran en la descripción de los Routers que realizan funciones a nivel de capa 3, los componentes de una red IP y los servicios que la misma puede brindar. A fines de la década de los años `90 este tipo de red se presentaba como la más adaptada para las redes del primer decenio del siglo XXI.

Por redes IP se entiende aquellas redes que soportadas por el protocolo TCP/IP (o similar como el IPX) se interconectan mediante routers. Se trata en principio de redes corporativas de empresas y de redes públicas de datos de alta velocidad. Una tendencia detectada a fines de los años 90 muestra que el crecimiento de ATM como medio de transporte para servicios multimediales se reduce ante la posibilidad de trabajar con el protocolo IP sobre fibras ópticas con interfaz Gigabit Ethernet.

La interconexión (***internetworking***) de redes se efectúa de distintas formas dependiendo de los objetivos y tipos de redes involucradas. Los elementos usados para la extensión o comunicación de una red son: repetidores, bridge, **ROUTER** y gateway. Se indican a continuación las principales características de ellos.

3.1- *LAYER-1.* REPETIDORES.

Funcionan en capa 1; no actúan en el ámbito de protocolos (capa 2 y 3). Efectúan la repetición eléctrica de la señal (proceso de regeneración). Permiten de esta forma la aislación eléctrica entre extremos del cable y la extensión de la LAN en un área mayor. No permiten la aislación del tráfico; todo el tráfico de un extremo pasa al otro. Introducen un retardo de propagación a veces intolerable en redes extensas.

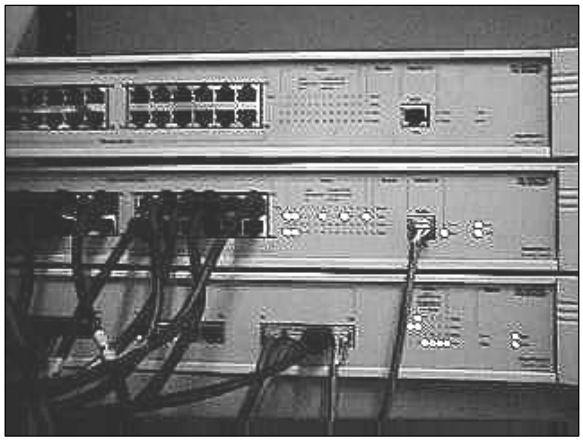
3.2- *LAYER-2.* HUB, BRIDGE Y SWITCH.

HUB.
Se han difundido los concentradores Hub con las redes 10BaseT debido a la facilidad de extensión de la red LAN mediante una configuración jerárquica en estrella. Se trata de una topología mixta con un columna *Backbone* de coaxial o fibra óptica y concentradores para usuarios en estrella. Un Hub es un concentrador, cuya versión más simple es un elemental conector tipo "T" (concentrador de 3 puertas pasivo).

La primer generación de Hub activos solo ofrece funciones de repetidor-regenerador de señal digital. Disponen de hasta 8/12 puertas activas. En la segunda generación de Hub se introducen las funciones de gestión de red. Mediante el protocolo SNMP se obtienen los estados de las puertas (se trata de un concentrador inteligente *Smart Hub*). Permite la generación de segmentos virtuales de LAN (puertas de acceso múltiple). Disponen de un microprocesador para la gestión y memoria MIB (base de datos de gestión).

La tercera generación de Hub poseen un *backplane* de alta velocidad (por ejemplo con celdas ATM). Posee puertas de diferentes técnicas para permitir modularidad LAN, FDDI, Router y Gestión. Incorpora funciones de conmutación para todas las necesidades de una empresa (*Enterprice Switching*). Las funciones de gestión permiten la desconexión de nodos con alarma y aislación de puertas para pruebas locales. Además permite la conexión horaria de puertas, el análisis de protocolo y obtener el estado de carga de enlaces.

BRIDGE.
Permiten interconectar distintas LAN del mismo tipo o generar varias desde una misma. Permite una mayor disponibilidad al generar LAN autosuficientes. Reducen el tráfico entre secciones de red LAN. Permiten solucionar problemas de congestión de paquetes mediante aislación de tráfico. Se puede generar una red de bridge con conmutación de paquetes (*Routing*) a nivel de capa MAC. Introduce retardo para medios de acceso de menor velocidad. Produce latencia de 1 mseg aproximadamente.



Normalmente un bridge posee dos puertas y un switch posee más de dos puertas. Un bridge puede utilizarse solo (como filtro entre dos secciones de LAN en la misma localización) o de a pares (uno en cada extremo para unir dos redes LAN distantes mediante un canal de comunicación dedicado como ser Nx64 kb/s en una WAN).

SWITCH-LAN
Un hub es un medio de interconexión plano (*Shared Media*) a nivel de capa 2. Un bridge es un filtro de direcciones MAC con dos puertas. Un switch consiste en una operación de Bridge de tipo multipuerta.

Simultáneamente con la creación de los switch se ha generado la operación **VLAN** (*Virtual LAN*) que consiste en agrupar los usuarios en la red en varias LAN por separado.

El switch funciona en el ámbito de capa 2 (MAC), procesan las direcciones MAC en una LAN y no modifican el contenido del paquete. Inspecciona la dirección de fuente y destino del paquete (*MAC Address*) para determinar la ruta de conmutación. La tabla de rutas se realiza mediante un compilador de direcciones MAC. La misma es dinámica y se actualiza sobre la base de la lectura de las direcciones contenidas en los paquetes que ingresan al switch (aprendizaje mediante lectura de direcciones). Cuando un switch recibe un paquete con dirección desconocida lo emite a todas las puertas (técnica conocida como *Flooding*).

Contiene suficiente memoria buffer para los momentos de demanda máxima (cola de espera). El overflow del buffer produce descarte de paquetes. Generalmente son estructuras no-bloqueantes y permiten que múltiples conexiones de tráfico se desarrollen simultáneamente. Permiten una estructura de red jerárquica en lugar de plana (uso de Hub). Un switch LAN dispone de varias puertas de interfaz con un ancho de banda dedicado, cada puerta representa un host o un segmento de red diferente. Trabajan sobre redes LAN del tipo Ethernet, token ring y FDDI.

Los switch tienen diversas estructuras de matriz de conmutación (*Switch Fabric*). El switch basado en un bus implementa un backplane monolítico donde se intercambia el tráfico de todos los módulos. El switch basado en memoria *shared* utiliza memorias RAM de alta velocidad para interconexión de módulos sobre el backplane. El switch punto-a-punto interconecta cada módulo con los demás no mediante un bus sino mediante conexiones individuales.

ETHERNET-CHANNEL. Una redundancia interesante se logra mediante la función ***Ether-channel***. En este caso dos switch pueden ser unidos mediante líneas paralelas con tráfico distinto. De esta forma, en caso de corte una sola línea abastece al medio, reduciendo la performance pero manteniendo el servicio.

3.3- *LAYER-3.* ROUTER Y SWITCH.

ROUTERS.
Funciona en el ámbito de capa 3 y por ello requiere un análisis del protocolo Internet IP. Debe soportar distintos tipos de protocolos; por ejemplo TCP/IP, DECnet, IPX (Novell), AppleTalk, XNS (Xerox). Interconectan LAN entre sí o una LAN con WAN (X.25, Frame Relay, ATM).

Permiten mejorar la eficiencia de la red ya que toleran distintos caminos dentro de la red. El Router puede segmentar datagramas muy largos en caso de congestión, en cambio no pueden ensamblar datagramas. Un router se utiliza muchas veces como conversor de interfaz (LAN hacia G.703 para 2 Mb/s o V.35 para Nx64 kb/s). En conexiones de datos de baja velocidad el router puede ser colocado en el extremo del circuito de acceso al usuario para obtener supervisión de línea. En este caso, mediante el protocolo SNMP asociado a UDP/IP se puede gestionar el punto de acceso de usuario (función PING por ejemplo).

Los router se pueden interconectar a alta velocidad mediante interfaces de 100 Mb/s (mediante pares o fibra óptica) y 1000 Mb/s (mediante Gigabit Ethernet) para formar redes de alta velocidad. En este caso el medio de transporte entre router es una conexión LAN extendida (MAN). Normalmente el protocolo IP usado en una LAN puede ser transportado mediante una red SDH, una red ATM o directamente sobre interfaz LAN por fibra óptica. Cuando la estructura de red usada es la descripta se observa una unión entre el concepto de switch LAN y router.

Algunas ventajas de los switch de capa 2 frente a los routers han determinado la idea de difundir el switch y usar el router solo una vez ("un switch cuando se puede, un router cuando se debe"). El switch tiene menor latencia, mayor capacidad de tráfico (*throughput*), fácil administración (concepto de gestión "*plug and play*") y menor costo por puerta. Los switch de capa 2 crean redes planas, en esencia se trata de un *bridging*. Un switch de capa 3 simula totalmente las operaciones de *routing*.

SWITCH-IP (*Layer 3 Switching*).
Se entiende por switch de capa 3 al equipo que realiza la operación de enrrutamiento mediante acciones de hardware; en tanto que es un router cuando las mismas se realizan mediante acciones de software. El switch-IP se fundamenta en circuitos *custom* del tipo **ASIC** (*Application-Specific Integrated Circuit*). Un switch de fines de los años `90 contiene 3 ASIC (para resolución de direcciones; para memoria de sistema y para memoria de puertas Gigabit). Con estos puede enrutarse 40 Mpps, soportar 1,5 millones de rutas y tomar decisiones a nivel de capa 2, 3 y 4.

Una diferencia de importancia entre un switch y un router es que este último permite optimizar la ruta cuando la red es muy grande. Permite además disponer de caminos alternativos y reconfigurar la tabla de rutas. Hacia fines de la década de los años `90 la diferencia entre router y switch se han reducido y reciben nombres combinados con ambas funciones.

La capacidad de procesamiento de un switch o un router se mide en Gb/s o Mpps (millones de paquetes por segundo) como capacidad de la matriz de conmutación. Cuando la suma de las entradas al equipo es igual a la capacidad de la matriz de

conmutación se dice que es no-bloqueante. Cuando es inferior se dice que se sobre-escribe el equipo y se supone que el tráfico no satura a la matriz.

NETFLOW SWITCHING. Esta técnica de *Cisco* combina las acciones de router y switch para mejorar la performance a alta velocidad (por ejemplo en Gigabit Ethernet). El primer paquete de la secuencia es enrutado en forma normal en capa 3; la información obtenida sirve para crear un camino (*flow forwarding*) y los paquetes siguientes son procesados mediante un switch de nivel 2 (se trata de una operación orientada con-conexión). El camino se genera en base a las direcciones IP y las ports de TCP/UDP. La información está contenida en un *cache* que se crea a tal efecto. Esta técnica de switch entre capas 2/3 se complementa en el *Core* de la red con *Tag Switching*.

Por otro lado, se utiliza este método para obtener información de performance de tráfico y proveer seguridad. Esta técnica utiliza los protocolos de routing normales y no requiere otros diseños especiales. Netflow entrega estadísticas de tráfico por cada usuario, protocolo, port y tipo de servicio. Esta estadísticas son útiles para análisis y diseño de la red y la facturación por departamentos en una empresa. La estadística de tráfico puede contener: la hora *Time-Stamp* del inicio y final, las direcciones IP y port de origen y destino, número de interfaz de entrada y salida, número de paquetes y total de bytes de la transacción.

***TAG SWITCHING* y *MPLS*.** Es un diseño de Cisco para el *Core* (*Backbone*) de una red IP cuando se trabaja a alta velocidad (por ejemplo, Gigabit Ethernet). Es un avance de la técnica **MPLS** (*Multiprotocol Layer Switching*). La arquitectura Tag Switch se encuentra en RFC-2105 del año 1997. Con posterioridad la denominación Tag se reemplazó por Label; Tag Switching se cambió por MPLS; el protocolo TDP por LDP.

Luego que la tabla de rutas converge (usando protocolos de routing convencionales) los distintos router asignan una etiqueta *Tag* para cada ruta posible (dicho tag se encuentra como *header* de capa 2 o 3). El tag es corto y de longitud fija que es mejor manejado que el tabla de rutas (se puede asimilar al identificador de trayecto virtual VPI de ATM). Los tag generados localmente en el router se intercambia con los otros mediante un protocolo **TDP** (*Tag Distribution Protocol*). Este protocolo permite distribuir, requerir y actualizar la información de tag.

El tag switching consiste de dos componentes: el *forwarding* (responsable de la transferencia de paquetes) y el control. La información de tag se memoriza en una base de datos de información realizada a tal efecto y denominada **TIB** (*Tag Information Base*). Los paquetes que circulan en la red llevan el tag de identificación y no requieren de acciones de tabla de rutas. El tag puede ser una simple ruta unicast o multicast, o un identificador de flujo de tráfico (por ejemplo, para el caso de *Netflow* donde se identifica el flujo mediante direcciones IP, ports y políticas administrativas). Por otro lado, el tag switching puede trabajar con QoS mediante información de prioridades.

3.4- *LAYER-4.* SWITCH

Se han reconocido hasta ahora dos tipos de switch: el switch de nivel 2 (funciona como un bridge de varias puertas) y el de nivel 3 (funciona como un router orientado al hardware). El switch de nivel 4 realiza funciones de conmutación de paquetes tomando en cuenta el *socket* (IP address y TCP/UDP port). De esta forma se puede tener acceso al tipo de servicio (capa de aplicación) transportado y realizar operaciones de prioridad (política de QoS) del tráfico con mayor precisión.

4- SERVIDORES

4.1- SERVER DE FIREWALL.

Es un sistema o grupo de sistemas que refuerzan la seguridad en las redes corporativas o proveedores de servicios con protocolos IP. El firewall determina los servicios que pueden ser accedidos desde el exterior de la red (desde la conexión a Internet). Todo el tráfico debe pasar por el firewall para ser inspeccionado.

FUNCIONES. El módulo de firewall instalado como un software sobre el router o servidor de acceso permite realizar las siguientes funciones:
-Control de acceso. Es el principal objetivo del firewall. Crea un perímetro de defensa diseñado para proteger las reservas corporativas. Acepta, rechaza y controla el flujo de paquetes basado en identificadores de capa 3 o aplicaciones. El principio de funcionamiento es: "todas las conexiones son denegadas a menos que estén expresamente autorizadas".
-*Logging*. Es el inicio de las conexiones entrantes y salientes. El uso de un sistema proxy y cache incrementa la velocidad de respuesta de estas operaciones.
-Traslación de direcciones. Permite realizar las funciones de **NAT** (*Network Address Translator*) asegura la supervisión de la información de entrada y salida. El NAT permite aliviar la escasez de direcciones IP y eliminar la necesidad de renumeración cuando se realiza un cambio de **ISP** (*Internet Service Provider*).
-Autentificación. El proceso de autentificación involucra a 3 componentes: el servidor, el agente y el cliente.
-Reportes. El firewall ofrece un punto conveniente para monitorear (*Audit and log*) y generar alarmas.

El firewall genera dos áreas en una red: el área pública con facilidad de acceso desde el exterior (para visita de Web, por ejemplo) y el área interna, detrás del firewall que se encuentra protegida contra la penetración no deseada. El perímetro de defensa se denomina zona desmilitarizada **DMZ** (*De-Militarized Zone*) y puede ser accedida por un cliente externo. El firewall puede trabajar sobre un server o sobre un router. La ventaja es que se concentra esta acción en un centro de la red consolidado en lugar de estar distribuido en cada host. Esta acción es más útil cuando es llevada a cabo por el router de entrada a la red. Por otro lado, ofrece un punto óptimo para instalar el Web y Server de FTP.

LIMITACIONES. Sin embargo, el firewall no puede controlar el tráfico que no pasa por él. Si existe un *Dial-out* irrestricto desde el interior de la red las conexiones PPP o SLIP a la Internet pueden generar una puerta no protegida. No protege contra robos mediante *Floppy Disks* o ataques internos a la red. No protege contra virus. Muchas veces los ataques internos son mayoría frente a los externos.

El firewall debe ser inmune a la penetración de ataques de *Hackers, Crackers* y espías. El hacker puede utilizar diversas herramientas para obtener información de la red interna y utilizarla en consecuencia. Así por ejemplo,
-el protocolo SNMP puede examinar la tabla de rutas;
-el programa *TraceRoute* puede relevar redes y router intermedios;
-el protocolo *Whois* puede entregar datos del DNS;
-el server DNS puede acceder a una lista de host;
-el protocolo Finger puede revelar detalles de usuarios (*login name*);
-el programa *Ping* puede emplearse para localizar un host desconocido, etc.

Algunos tipos de ataques a la red son el envío de paquetes no-ruteables al router (lo que degrada su performance) y el envío de actualizaciones de tablas de ruta espurias (conocido como *Spoofing*).

4.2 SERVER DE AUTENTIFICACION

El proceso de autentificar a un cliente puede ser realizado durante 4 etapas posibles: la conectividad del cliente, cuando se accede al software de autentificación del switch, mediante un servidos o cuando se autoriza a trabajar en una VLAN. Existen diversos métodos de autentificación de clientes. Se utilizan diversas herramientas como ser: *username*, *password*, claves (*key*), **RADIUS** (*Remote Access Dial In User Service*), **PIN** (*Personal Identification Number*), Kerberos, LDAPv3, etc.

S-Key es un método anunciado en 1981 (standard RFC-1760) y basado en una clave secreta aplicada a la función hash (algoritmo **MD4**). El algoritmo *Hash* tiene las versiones SHA-1 y MD4/5. Se trata de generar un código con el auxilio del algoritmo. El algoritmo genera un mensaje compacto conocido como *Digest*. Es un proceso criptográfico que genera una secuencia fija de 128 bits en MD y 160 bits en SHA-1. El resultado del algoritmo es usado para crear un password.

Otra técnica es el ***Smart Card*** consistente en una clave (PIN inicial) y una tarjeta que contiene información criptografiada. Este método es común en telefonía celular GSM. La información de autentificación puede ser memorizada en un servidor de directorio **LDAP** con los objetos referidos al tipo de cuenta, el horario de uso, etc.

Kerberos es desarrollado por el MIT como sistema de autentificación para sistemas abiertos en entornos distribuidos. El proceso se realiza cuando se inicia la sesión (*logon*) del tipo cliente-servidor. Se basa en *tickets* que se obtienen de un

servidor y que tienen una duración limitada de tiempo. El ticket contiene toda la información del cliente para asegurar su identidad.

4.3- SERVER DE CACHING

Existen 3 armas que utiliza el router para mejorar la eficiencia de la red reduciendo el tráfico que circula por la misma:
-el manejo de nombres y direcciones mediante **DNS**,
-los servicios *proxis* (se entiende por *proxi* a un elemento de la red que actúa en representación de otro) y
-el *cache* local.

Un *Cache* es un block de memoria para mantener a mano los datos requeridos frecuentemente por varios procesos. Cuando un proceso requiere información primero consulta el cache, si la información se encuentra allí se produce una mejora de la performance de funcionamiento reduciendo el retardo de procesamiento. Si no se la encuentra en el cache se buscará en otras alternativas de memoria y luego se lo encontrará disponible en el cache para una próxima oportunidad.

Una ventaja adicional de ciertos cache es la posibilidad de reducir el dialogo para transferencia de información. Por ejemplo una consulta web lleva una sesión de innumerable cantidad de objetos que son transferidos mediante un HTTP *Get-Request*. Puede reducirse la cantidad de paquetes transferidos mediante una sesión en paralelo de objetos.

Algunos tipos de memoria cache son:
-Cache del procesador: es parte del procesador y es de más fácil acceso que la memoria RAM y a una velocidad mayor.
-Disco cache: pertenece a la memoria RAM y contiene información del disco. En algunos casos se mueve en forma anticipada la información desde el disco al cache en la RAM.
-Cache cliente-servidor: se trata de un banco de memoria ubicado en el cliente para agilizar el movimiento de datos.
-Cache remoto: permite reducir los retardos cuando se accede a información de un sistema remoto en una WAN. Se resuelve mediante un *caching* de información del terminal remoto ubicado en el sistema local.
-Cache de servidor intermedio: entrega información a un grupo de clientes (*Local Workgroup*) en un sistema cliente-servidor.

WEB-CACHING. Para un ISP el uso de cache en el punto de presencia POP puede reducir el tráfico en su red (aumentando la velocidad de respuesta al usuario y el costo de la conexión WAN). Un tráfico muy común y apropiado para el cache es el Web. Un router que administra el cache dialoga con la memoria mediante un protocolo **CCP** (*Cache Control Protocol*). El cache se conecta directamente al router, el cual deriva todos los paquetes de requerimiento al cache (por ejemplo mediante la port 80 de TCP que indica el protocolo HTTP), de esta forma puede verificar si la información está disponible.

Los componentes de este complejo son los siguientes:
-La memoria cache que se denominan *Cache Engine*.
-El router conocido como *Home Router*. El cache posee suficiente memoria (ejemplo, 24 Gbytes) y capacidad de transacciones (algunos miles de sesiones TCP simultáneas).
-Un router puede poseer varios cache que se denominan *cache farm*. En este caso se forma una jerarquía entre cache para sucesivas investigaciones sobre el requerimiento del usuario.

La desventaja del Web-Caching es que pueden aparecer diferentes versiones de un documento en la web. La duración de un documento en el cache debe ser limitada en el tiempo para reducir este efecto. La introducción de firewall para seguridad de acceso a los web ha introducido la idea del *Caching-Proxy*. En este contexto el proxy es un programa que interactúa entre el cliente y los servers; se trata de **URL** (*Uniform Resource Locator*). Esta posición es ideal para general el cache del web; el primer software disponible para esta función fue el servidor de web del CERN en el año 1993.

4.4- SERVER DE WWW (*World Wide Web*).

Se inicia en **CERN**-1989 en Ginebra para implementar la idea de **hipertexto** en la actividad científica mediante la Internet. Web se popularizó a partir de 1993 cuando la Universidad de Illinois generó el programa gratuito **Mosaic**, con formato windows accesible a cualquier usuario. Para 1995 el número de programas "inspectores de Web" superaba la docena y el **NetScape Navigator** era usado por el 75% de los usuarios de Internet. En Windows 95 y 98 el programa **Explorer** es un software standard. En 1995 el crecimiento de servidores de Web era del 100% cada 53 días.

Las principales características del Web son las siguientes. En WWW se desarrolla el protocolo de hipertexto; por hipertexto se entienden enlaces entre datos, similar a una enciclopedia. Con la selección (pulsando 2 veces) de palabras y textos resaltados se accede a una otra página adicional. El salto entre páginas es independiente al lugar de almacenamiento (un server o varios en todo el mundo). Este proceso se denomina "navegación" (*Browsing, Cruising o Surfing*) en el ciberespacio.

No existe una RFC para el Web. Se trata de diferentes mecanismos: URL, HTTP, HTML, CGI y Cookies. Se indican varios detalles de los mismos a continuación.

-URL (*Uniform Resource Locators*). Obtenible desde RFC-1630. El URL es una forma de identificador de reservas en los servidores web. Un URL puede administrar a varios servidores de web desde un punto al que se dirige el usuario.

-HTTP (*Hypertext Transfer Protocol*). Obtenible desde RFC-2068. Se trata de una arquitectura cliente-servidor, donde el cliente utiliza un visualizador (*Browser Web*). El servidor de Web es uno o más servers que entregan texto, gráficos, imagen y sonido. Se utiliza el protocolo de hipertexto HTTP por ello la forma de identificación de un servidor de web inicia con el formato (*http://www*). El servidor se denomina *"HTTP server"* en el ambiente Windows NT o *"HTTP Daemon"* en el Unix. Las direcciones de los server de Web tienen el formato http://www.nombre.código que incluye la apertura, el nombre de empresa y el identificador de cierre (por ejemplo .com.ar para indicar una empresa comercial en Argentina).

-HTML (*Hypertext Markup Language*). Los enlaces de hipertexto se crean mediante el lenguaje HTML (RFC-1866). Es una variante de **SGML** (*Standard Generalized Markup Language*) de ISO-8879 del año 1986. Se lo utiliza para escribir los *Web-Server*. En la fotografía anexa se muestra la pantalla de un programa de escritura en HTML (el texto en la primer frase de este ítem y el programa se denomina *FrantPage Express*).

-CGI (*Common Gateway Interface*). Esta interfaz define como se comunica el server de HTTP con el programa ejecutable mediante un browser.

-***Cookies*.** Se trata de información que el servidor del web memoriza en el cliente para ser utilizada en una próxima sesión. Puede ser usada para memorizar información de configuración o password de subscripción (acceso) al servidor. Esto produce un consumo de memoria y una intromisión que puede ser considerada inaceptable por el cliente. Algunos cookies son utilizados para tomar información del cliente y enviarlas al servidor. Los navegadores de Internet permiten configurar la aceptación de cookies en el cliente.

4.5- SERVER DE DOMINIOS

La gestión de direcciones IP requiere de una serie de elementos interrelacionados: el servidor DNS permite asociar un nombre de usuario con la dirección IP; el servidor/router NAT permite asignar direcciones IP no-públicas en el interior de una red privada; el servidor DHCP permite asignar direcciones IP en forma dinámica a usuarios intermitentes y el *Dynamic DNS* permite actualizar el servidor de DNS cuando se asigna la dirección mediante DHCP. A continuación los detalles de estos elementos.

DNS (*Domain Name System*).
Este sistema permite organizar la información de routing entre una denominación (seudónimo) simple de recordar y el número de dirección IP verdadero (se denomina resolución de nombre). Hasta 1980 un solo computador (llamado Host.txt en California) realizaba esta función, pero el tráfico hacia la misma se tornó inmanejable. Entonces se introdujo un sistema distribuido. El nombre completo tiene como máximo 63 caracteres. De ellos 3 caracteres indican el domino (edu-educación, com-comercial, gov-gubernamental, org-organización, mil-militar, etc) y 2 el país (ar-Argentina, it-Italia, etc). La tabla de dominios memorizada en el servidor se denomina *DNS Cache*.

NAT (*Network Address Translation*).
El problema más complejo de Internet es el reducido número de direcciones. La solución a largo plazo el IPv6 con un mayor número de bytes por dirección. La solución instrumentada sobre IPv4 son dos: el **CIDR** (*Classless InterDomain Routing*) y el **NAT**. El proceso NAT propone reducir el número de direcciones IP mediante el re-uso de direcciones privadas en todas las redes. De esta forma una red privada utiliza un direccionamiento propio y el router en el borde (*Stub Router*) de la red realiza la función de traducción y direccionamiento hacia la red pública (llamadas dirección local y dirección global).

DHCP (*Dynamic Host Configuration Protocol*).
Cuando un nuevo usuario se agrega a la red o se cambia de posición se requiere asignar una dirección IP y actualizar la base de datos del DNS. El protocolo DHCP fue diseñado por el IETF (standard en RFC-2131) para reducir los requerimientos de configuración. Además de asignar la dirección IP realiza una configuración automática de los parámetros necesarios para funcionar en la red donde se encuentra. DHCP trabaja sobre TCP y está basado en el protocolo **BOOTP** (*Bootstrap Protocol*) de RFC-0951, con algunas diferencias. El BOOTP permitía que clientes sin capacidad de memoria (disco rígido) pueda funcionar en TCP/IP.

Se utiliza un modelo *Client/Server* por lo que se dispone de uno o varios servidores DHCP. No se requiere de un servidor por subred por lo que el protocolo DHCP debe trabajar a través de routers. Más de un servidor pueden realizar las tareas de asignación de direcciones con el propósito de mejorar la eficiencia del sistema.

DNS *UPDATE*.

Asociado a DHCP se encuentra el mecanismo *Dynamic DNS Update*. Permite la actualización automática del servidor DNS con el nombre y la dirección IP asignada en forma dinámica por el protocolo DHCP. Se refiere a RFC-2136 del año 1997. Este protocolo trabaja sobre TCP o UDP de acuerdo con el request. El formato del mensaje de actualización (*update*) contiene un encabezado de 12 Bytes que identifica al que efectúa el requerimiento y diversos campos

DHCP *FAILOVER*.

También en sociedad son DHCP se dispone de la técnica *DHCP Failover* que consiste en disponer de servidores duplicados funcionando como pares redundantes. Se dispone de un protocolo de comunicación simplificado para la operación en régimen normal, de interrupción de comunicación entre servidores y de falla del servidor asociado.

1202

PROTOCOLO IP

Referido al funcionamiento y la trama de los protocolos de capa 3. Sobre el protocolo IP de RFC y los protocolos Ipv6, IPX y CLNP asociados.

La intuición de lo particular, este será el conocimiento pleno. Estaba dispuesto a pensar en todo, no por la vastedad de mi intelecto, sino por la estrechez de mi intuición.
Umberto Eco-1980.

1- INTRODUCCION A TCP/IP

Los primeros antecedentes de TCP/IP e Internet son los siguientes:
-En 1961 se L. Kleinrock escribe el primer artículo sobre la teoría de conmutación de paquetes y en 1964 el primer libro.
-En 1965 se realiza en el MIT la primer interconexión entre computadores entre sí.
-En 1969 se escribe la primer RFC referida a "Host Software" para ARPA.
-En 1969 se inicia UNIX un sistema operativo original de K.Thompson y D.Ritchie en AT&T.
-En 1972 se inicia el protocolo TCP por B.Kahn y V.Cerf.
-En 1977 comienza a operar el protocolo TCP (incluía las funciones del actual IP).
-En 1978 se separan los TCP e IP. Las RFC correspondientes se escriben en 1983.
-En 1983 se separan la Milnet (45 nodos) y la Arpanet (68 nodos). Nace entonces la Internet actual
-En 1983 se introduce la versión UNIX 4.2 (*Berkeley Software Distribution*) y TCP/IP entra en la era comercial..

1.1- UNIX y TCP/IP.

Desde su formulación actual en 1983 los protocolos **TCP/IP** se han difundido extensamente. Se trata de **IP** (*Internet Protocol*) el protocolo de capa 3 y **TCP** (*Transmission Control Protocol*) de capa 4. Ambos protocolos operan independientemente de las capas de orden inferior (como ser redes de área local LAN IEEE 802.x, accesos mediante paquetes X.25 o Frame Relay, módem de datos *Dial-up* o accesos de alta velocidad ATM) y ofrecen servicios a las capas de aplicación (SMNP, FTP, HTTP, etc).

Existen otras variantes de protocolos de capas 3/4, como ser el proporcionado por el modelo ISO y propietarios de productores de computadoras como ser: el **SNA** de IBM; **DECNET/DNA** de Digital Equipment Corp; el **XNS** de Xerox; el **BNA** de Unisys; **AppleTalk** de Macintosh y **IPX/SPX** de Novell. TCP/IP se encuentra como protocolo de base para el sistema operativo **UNIX**. UNIX no dispone de las capas 5 y 6 (Sesión y Presentación), las cuales son introducidas en el modelo de la ISO.

El modelo de ISO entrega un protocolo más moderno pero menos experimentado que TCP/IP. Aunque se promovió una migración hacia el modelo ISO (recomendado por el *National Research Council* de USA en 1985) ha ocupado un período largo de tiempo y es probable que no se realice nunca debido a la extensión de la difusión de TCP/IP y a las mejoras introducidas en futuras versiones de los protocolos. TCP/IP recibe un impulso cuando **Sun Microsystems** publica la especificación **ONC** (*Open Network Computing*), también conocido como **NFS** (*Network File System*). Se trata de una simple interfaz de usuario para aplicaciones comerciales y está disponible para una gran variedad de computadoras.

INTERNET. La primer red fue desarrollada desde 1965 en el MIT para **ARPA** (*Advanced Research Projects Agency*). Se denominaba red **Arpanet** (precursor de la actual Internet). Desde 1972 se denomina **DARPA** (*Defence ARPA*). En 1983 se formaliza la red Internet al separarse de la órbita militar (red **Milnet**). La red **Internet** disponía de más 5 millones de host conectados en 1995 impulsado por el servicio de Web.

Para Internet se generan sucesivamente los siguientes organismos de normas: **ICCB** (*Internet Configuration Control Board*) entre 1981-84, **IAB** (*Internet Activities Board*) desde 1984 y **IETP** (*Internet Engineering Task Force*) junto con **IRTF** (*Internet Research Task Force*) desde 1989.

Las normas **MIL-STD** (*Militar Standard*) y **RFC** (*Request For Comments*) determinan los protocolos para la interconexión de redes Internet. MIL pertenece al Departamento de Defensa y RFC son las normas de **IAB** (*Internet Activities Board*) para el protocolo oficial de Internet. Los estándar RFC son normas preparadas para la red Internet en forma de artículos. Las normas RFC se distribuyen mediante mail electrónico y su actualización es mucho más veloz que las normas ISO. Por otro lado, el incremento de servicios Internet en la década de `90 ha retardado la conversión desde TCP/IP hacia ISO.

1.2- MODELO DE CAPAS.

Referido a las **Fig 01/02**. La red Internet es independiente de las capas inferiores. Sin embargo, es común el uso de redes LAN, X.25 o protocolos para modem de datos para el acceso. El protocolo X.25 para redes conmutadas de paquetes tiene una capa 3 involucrada. En este caso se trata de una sub-capa interna a la red, mientras que IP es una sub-capa entre redes. X.25 es un servicio orientado con-conexión donde se establece una llamada virtual en tanto que IP es un protocolo sin-conexión.

Las redes LAN involucran las capas 1 y 2 del modelo. Cuando la red es Ethernet el acceso a IP es directo; en tanto que en la IEEE 802.3/5 y FDDI se requiere de un campo adicional denominado **SNAP** (*SubNetwork Access Protocol*) que se coloca luego del campo **LLC** (dirección hexadecimal AA en LLC). El SNAP consta de 2 campos: 3 Bytes para el identificador de versión de protocolo **IP** y 2 Bytes para identificador de capas superiores (hexadecimal 0800 para TCP/IP).

Tabla 01: Modelo general de capas relacionadas con TCP/IP.

-Capa 7	Capa de aplicaciones **FTP, SMTP, Telnet, HTTP, VoIP, RSVP,** etc.
-Capa 6-5	No definidas.
-Capa 4	Capa de transporte Host-a-Host **TCP** para aplicaciones con control de errores o **UDP**.
-Capa 3	Capa de red Internet **IP** y protocolos asociados ARP/RARP/ICMP.
-Capa 1-2	Capa de acceso a red: generalmente una **LAN** (Ethernet), o X.25/FrameRelay/ATM.

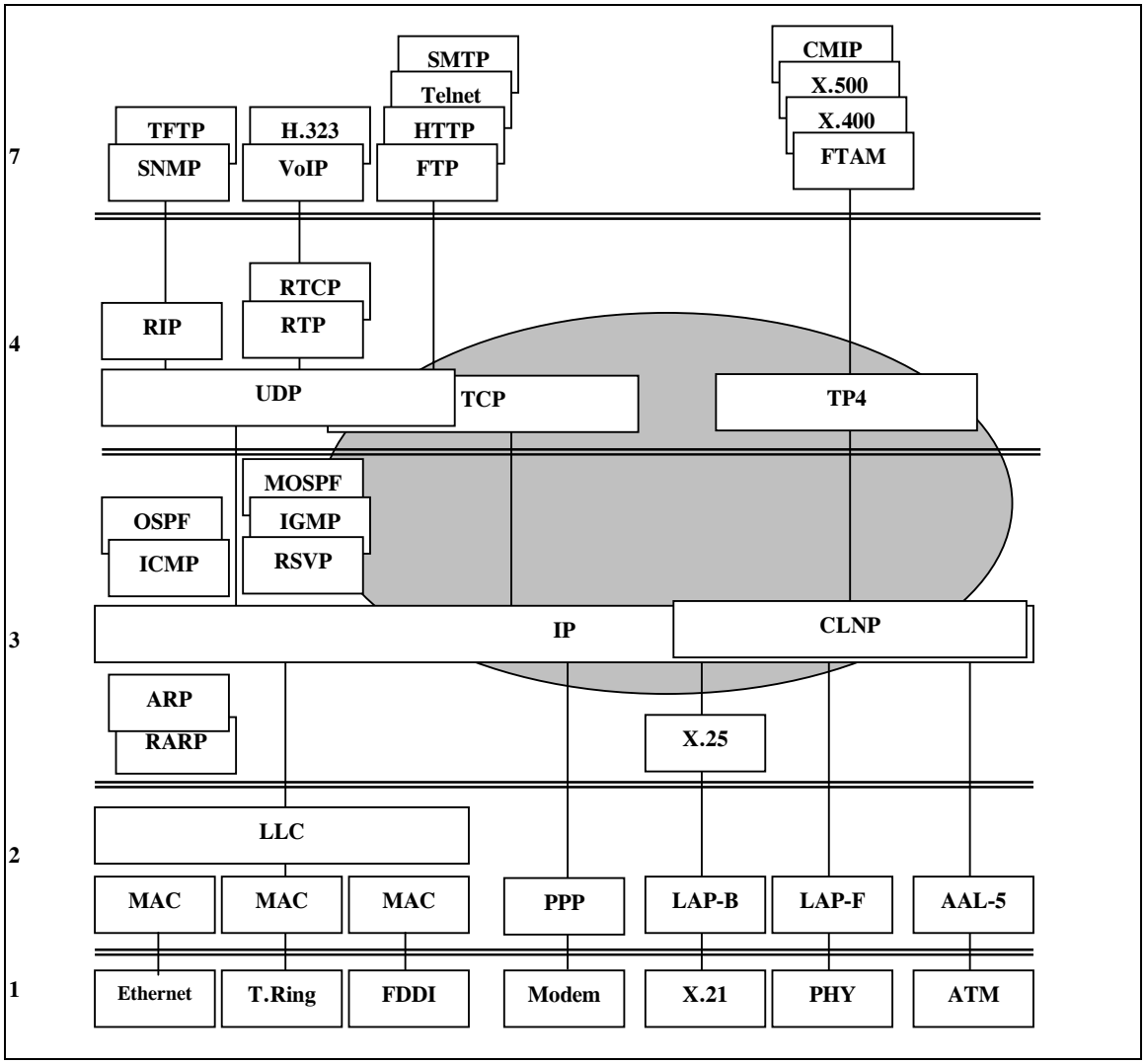


Fig 01. Modelo de capas para la suite TCP/IP.

1.3- FUNCIONES DE TCP/IP.

Los protocolos de capas 3/4 permiten efectuar las siguientes funciones generales:

-**Segmentación y ensamble:** El proceso de segmentación se aplica para mayor eficiencia en el control de errores, para un acceso más equitativo al medio de transporte y para requerir un tamaño de memoria buffer inferior. Sin embargo, la segmentación en paquetes de corta longitud genera un incremento en el tiempo de procesamiento y una menor eficiencia de datos. Se entiende por eficiencia la relación entre Bytes de datos **PDU** (*Protocol Data Unit*) y Bytes de encabezado. La segmentación en largos datagramas impide el acceso equitativo de distintos usuarios sobre el medio de transporte. La relación entre la velocidad y el tamaño del datagrama determina la eficiencia y el acceso equitativo.

-**Routing:** Cada PDU contiene, además de los datos de capas superiores, la dirección de protocolo IP de origen y de destino para el *Routing* sin-conexión.

-**Control de errores y de flujo:** Mediante campos de control apropiados se puede detectar la ausencia de datos y requerir la retransmisión. El protocolo IP detecta errores en el encabezado y descarta el datagrama. El protocolo TCP detecta errores en el encabezado y falta de segmentos de datos y solicita la retransmisión. El protocolo UDP no realiza la retransmisión de datos.

-Control de conexión: Se trata de servicios orientados con-conexión en TCP y sin-conexión en IP. En el primer caso se establece una conexión virtual con 3 fases: establecimiento de conexión, transferencia de datos y terminación de conexión.

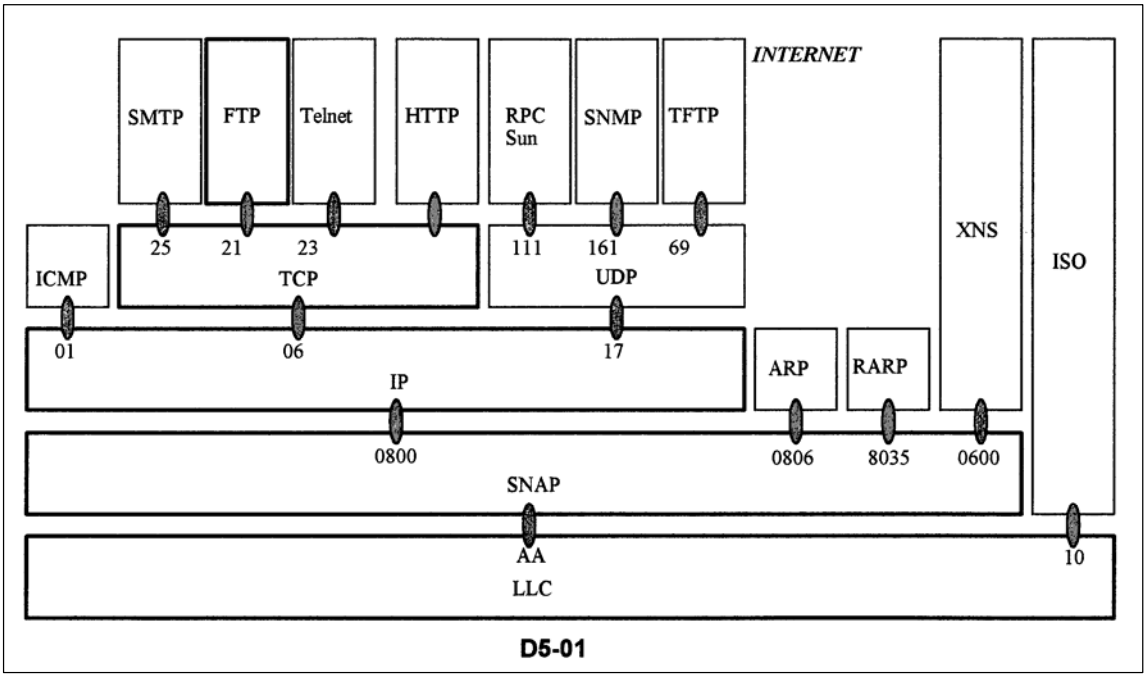


Fig 02. Direcciones de servicios entre capas.

2- PROTOCOLO IP

2.1- DIRECCIONES DE PROTOCOLO IP

Las normas **MIL-STD-1777** (*Militar Standard*) y **RFC-791** (*Request For Comments*) determinan el protocolo IPv4 (del año 1981) para la interconexión de redes Internet. En Internet se trata de conectar redes individuales mediante *Routers* (algunas veces denominados *Gateway* de red), el router realiza la operación de enrrutar el paquete sobre la base de las direcciones IP (4 bytes).

La identificación de un punto en la red requiere de vías simultáneas (direcciones MAC en capa 2, IP en la capa 3 y port en la capa 4; adicionalmente la identificación de usuario de un servicio en particular).
-La dirección de usuario Internet depende del servicio; en SMTP para mail-electrónico contiene los siguientes campos: "nombre", **@** (carácter arroba), "empresa". com . ar.
-La dirección de capa IP es de 4 Bytes. Generalmente es indicada mediante notación (*dotted*) punteada como ser 44.123.230.224. No es de tipo jerárquico como en la red telefónica o X.25, donde se distingue el país y ciudad, antes del usuario.
-La dirección MAC en la red LAN es de 6 Bytes (ejemplo en hexadecimal: 08.00.02.12.34.BF).

La dirección IP de origen y de destino ocupa 32 bits: Permite identificar la red y el host individual. El formato de las direcciones puede ser de 5 tipos de acuerdo con la **Tabla 02**.

Tabla 02. Clases de direcciones IP (IP-Address).

Clase A.	0+7bit+24bit. Corresponde a un número de dirección de Network (7 bit asignados por IANA) y otro número para el Host (24 asignados por el administrador de la red). Es aplicable solo para grandes redes. El IANA solo puede designar 128 (2^7) redes de este tamaño. Numera desde 0.0.0.0 hasta 127.255.255.255. Sin embargo, ante la falta de direcciones IPv4 se ha decidido particionar la clase A para asignarlas a varios usuarios (se conoce como direccionamienro *classless*). Por ejemplo, La dirección de HP de Argentina es del tipo 15.59.x.y. En tanto que, la dirección MAC de HP es 08-00-09 (la dirección MAC de Siemens es en cambio: 08-00-06).
Clase B.	10+14bit+16bit. Es aplicable a redes medianas y numera desde 128.0.0.0 hasta 191.255.255.255. Por ejemplo, la empresa Telefónica de Argentina tiene asignado un número de este tipo de red: 168.226.x.x (los dos bytes finales son asignados por el operador de la red).
Clase C.	110+21bit+8bit. Para pequeñas redes. Se trata de 4 Bytes: los 3 primeros Bytes indican la dirección de red y el último Byte numera el Host dentro del nodo. Un router de red IP se identifica mediante los 3 primeros Bytes (dados por IANA) y sus puertas con el Byte final. En esta configuración el primer valor válido es 192.0.0.0 y el último es 223.255.255.255.
Clase D.	1110+28 bits. Ocupa la numeración 224.0.0.0 hasta 239.255.255.255. Es utilizada para direcciones *multicast* (grupo de usuarios de servicios IP).
Clase E.	11110+27 bits. Ocupa desde 240.0.0.0 hasta 247.255.255.255. La dirección 255.255.255.255 es una dirección de *broadcast*.

La dirección IP puede escribirse mediante la notación decimal punteada *Dotted* (44.123.230.224) que esta es la preferida por su simplicidad. También se puede usar la notación hexadecimal (2C.7B.E6.E0), la notación estilo C de Unix (Cx2C7BE6E0) y la notación binaria (00101100.01111101.11100110.11100000).

La dirección IP contiene 4 sectores:
-***Prefijo*** desde 1 a 5 bits para identificación del tipo de Clase (A a E). Así la secuencia 110 determina la clase C).
-Identificación de ***Network*** (de 7, 14 o 21 bits para las clases A a C); entonces la secuencia 110 inicial determina que la dirección de red es de 21 bits.
-Identificador de ***Sub-network***. Se trata de la diferencia con la dirección de host.
-Identificador de ***Host***. Para conocer la secuencia que identifica al host es necesario leer la máscara de red. Esta máscara identifica los bits que determinan el host y por ello, la subnetwork.

Estos dos últimos campos ocupan en total los 24, 16 o 8 bits que completan la dirección. Para poder distinguir entre la identificación de subnetwork y host se requiere una filtro de direcciones denominado *Mask Net*. Por ejemplo, para una dirección clase C (inicio 110) se tiene el siguiente formato (x para Network; y para Subnetwork; z para el Host):

Dirección:	110x.xxxx	xxxx.xxxx	xxxx.xxxx	yyyz.zzzz	
Mask Net:	1111.1111	1111.1111	1111.1111	1110.000	(255.255.255.224)

La gestión de direcciones la realiza el **IANA** (*Internet Assigned Numbers Authority*). Asigna el número de red al usuario, dejando al usuario la numeración de host que debe ser única. El registro se opera desde el **DDN/NIC** (*Department of Defense Network/Network Information Center*) de Chantilly-Virginia.

NAT (*Network Address Translation*). El problema más complejo de Internet es el reducido número de direcciones. La solución a largo plazo el IPv6 con un mayor número de bytes por dirección. La solución instrumentada sobre IPv4 son dos: el **CIDR** (*Classless InterDomain Routing*) y el **NAT**. El proceso NAT propone reducir el número de direcciones IP mediante el re-uso de direcciones existentes en la red pública dentro de redes privadas. De esta forma una red privada utiliza un direccionamiento propio y el router en el borde (*Stub Router*) de la red realiza la función de traducción y direccionamiento hacia la red pública (llamadas dirección local y dirección global).

El uso de NAT en el router de borde requiere el manipuleo de la información; por ejemplo, los checksum de IP y TCP cambian, además existen protocolos que llevan la dirección IP en el contenido y debe ser cambiada, etc.

2.2- TRAMA DE IP.

El formato de la trama (denominado datagrama) contiene los campos de la **Tabla 03** para el protocolo IPv4; ver también la **Fig 03/04**. Obsérvese que el protocolo IP no tiene previsto el control de flujo, la protección de la secuencia de datos u otros servicios ofrecidos del tipo host-a-host.

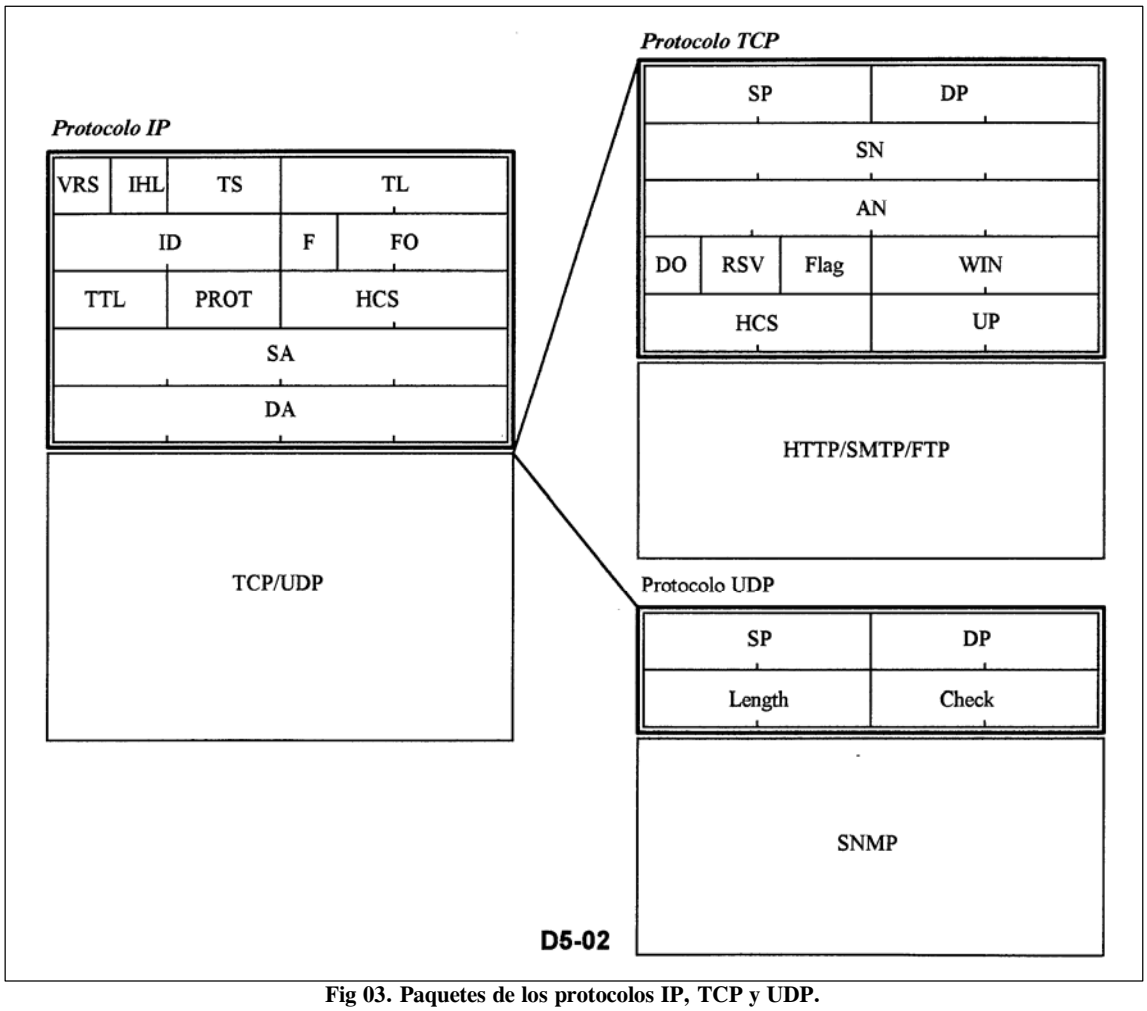


Fig 03. Paquetes de los protocolos IP, TCP y UDP.

Tabla 03: Campos del Datagrama del protocolo IPv4.

	CAMPOS DE INFORMACIÓN GENERAL.
-VRS	4 bits. Indica la versión del protocolo IP. La versión actual es la IPv4.
-IHL	4 bits. (*Internet Header Lenght*). Indica la longitud de encabezado en unidades de 4 Bytes. El valor típico es 5 (corresponde a 20 Bytes sin campo opcional).
-ToS	1 Bytes. (*Type of Service*). Contiene información para procesamiento de información por prioridad, retardo, etc. Permite gestionar la calidad de servicio **QoS** dentro de una red IP. En detalle son:
.PROC	3 bits. Procedencia; permite designar a datagramas de alta prioridad con 8 niveles. Se trata de los siguientes casos: control de red; control de internetwork; crítico; pasaje rápido (*Flash Override*); *Flash*; inmediato; prioritario y rutina.
.D	1 bit. Retardo admitido sobre el datagrama. Se admite el estado normal o bajo.
.T	1 bit. Conectividad admitida (*throughput* normal o alto).
.R	1 bit. Pérdida de datagramas (probabilidad para descarte de datagrama normal o bajo).
	INFORMACIÓN PARA LA SEGMENTACIÓN.
-TL	2 Bytes. (*Total Length*). Se indica la longitud total del datagrama, incluyendo el encabezado, en unidades de Bytes. Por razones de fragmentación se usa un valor muy inferior al máximo permitido de 65535 Bytes (máximo 2^{16}). Se puede programar a los router para aceptar datagramas de 576 Bytes como máximo. Es conveniente que la longitud total del datagrama no supere la utilizada en la red de transporte (por ejemplo: 1492 Bytes en IEEE 802.3, 4352 Bytes en FDDI, 9180 Bytes en SMDS, 128 Bytes en X.25, 256 Bytes en Frame Relay). Con esto se logra reducir los problemas de fragmentación en capas inferiores.
-ID	2 Bytes. Identificador de dirección de origen, destino y protocolo de usuario. La identificación es única mientras dura el datagrama en la Internet.
-Flags	3 bits. Para informar de la segmentación y facilitar el ensamble de datagramas en el destino. Contiene la siguiente información mediante 2 bits de los 3 bits:
.MF	1 bit. (*More Flag*). Indica si es el final de la segmentación final o si existen más datagramas.
.DF	1 bit. (*Do not Fragment*). Indica si se ha efectuado o no una fragmentación de datos y si ella es autorizada para los routers.
-FO	13 bits. (*Fragment Offset*). Indica la posición del datagrama en el mensaje original en unidades de 8 Bytes. En los segmentos sucesivos se señala la cantidad de Bytes transmitidos hasta el presente. La longitud máxima del mensaje recibido desde TCP y segmentado por IP es $8x2^{13}$ Bytes.
-TTL	1 Bytes. (*Time To Live*). Tiempo de vida medido en intervalos de 1 segundo. En muchos casos es configurable y el valor recomendado es de 32 seg. Permite liberar la red de datagramas que no llegan a destino y que ocupan reservas de memoria.
-PROT	1 Bytes. (*Protocol*). Indica el nivel de protocolo de capa superior; actúa como dirección de servicio **SAP**. Corresponde al valor siguiente (decimal 0…255): TCP lleva 6; UDP:17; ICMP:0; EGP:08; OSPF:89.
-HCS	2 Bytes. (*Header Checksum*). Para detección de error en el encabezado. HCS cambia en cada router debido al cambio de TTL y Flags. Si se detecta error en el encabezado el datagrama se descarta. TCP detecta falta de datos y solicita la retransmisión. IP no detecta errores en los datos; esto lo hacen TCP y UDP.
	CAMPO DE DIRECCIONES Y OPCIONAL.
-SA	4 Bytes. (*Source Address*). Dirección de origen con formato w.x.y.z (0 a 255).
-DA	4 Bytes. Dirección de destino del datagrama, con igual formato.
-PAD	N Bytes. (*Padding*). Para final de encabezado (completa el número de Bytes).
-Data	Campo de datos del datagrama (mensaje segmentado desde capa superior).
-OPT	Campo de información opcional.

2.3- FUNCIONAMIENTO DE IP

ENRUTAMIENTO. El datagrama puede ser direccionado mediante una tabla de ruta estática (solo dispone de alternativas en caso de indisponibilidad de un enlace o router) o dinámica (responde a errores, congestión de la red, costo y retardo). Puede soportar también requerimientos de seguridad y prioridad de datagramas. Estos aspectos pueden demorar a un datagrama en la red, consumiendo buffer de memoria y capacidad de transporte e incluso puede mantenerlo en loop entre routers indefinidamente (por ello se requiere el tiempo de vida TTL).

La operación de redes como X.25 o Frame Relay es en el modo orientado con-conexión; lo cual corresponde a un circuito virtual (conexión lógica permanente establecida entre dos puntos en una red de paquetes). La operación en modo sin-conexión corresponde a un datagrama que lleva toda la información necesaria para el enrutamiento en la red. La operación

sin-conexión requiere del análisis del nivel de protocolo Internet IP (función del router), en tanto en la operación con-conexión una vez establecido el circuito virtual no requiere dicho tratamiento.

TIEMPO DE VIDA. Para reducir el riesgo de demora o pérdida del datagrama se define el **TTL** (*Time To Live*). Indica el tiempo que el datagrama puede permanecer en la Internet. Como el datagrama consume memoria y recursos en la red, al transcurrir este tiempo (indicado en el campo TTL en segundos) el mismo se descarta. Cada ingreso de un datagrama a un router le descuenta una unidad de TTL; además en tanto el datagrama permanece en el buffer de un nodo se descuenta el valor de TTL en una unidad por seg. En IP el tiempo de vida es indicado en saltos de 1 seg, mientras que en el modelo ISO es en intervalos de 0,5 seg.

El protocolo de capa 3 no se ocupa de la retransmisión, el encargado es el protocolo de capa 4 (TCP). El protocolo de destino debe detectar la ausencia de un datagrama correlativo mediante la información TL, Flag y FO, con lo que se interrumpe el ensamble. Un router intermedio no está autorizado a efectuar ensamble ya que no posee la seguridad que los distintos segmentos pasan por dicho router. El protocolo IP dispone del protocolo ICMP para enviar reportes cuando se produce un descarte debido a finalización de TTL. Un datagrama puede ser descartado por varias razones: final del tiempo de vida, congestión de la red y errores de bits en el encabezado.

CALIDAD DEL SERVICIO. En IP se tiene la oportunidad de definir la Calidad del Servicio **ToS** (*Type of Service*) en los siguientes términos:
-Procedencia (importancia relativa del datagrama, 8 niveles),
-Retardo admitido del datagrama (2 niveles),
-Importancia para la seguridad del datagrama (2 niveles).

ENSAMBLE DE DATOS FRAGMENTADOS. Mediante la información de longitud y offset del datagrama se facilita el ensamble. Para este funcionamiento se utilizan los siguientes recursos: longitud de datos TL, Offset de fragmentación FO y Flag MF que indica si se trata del último datagrama. Para el ejemplo de la **Tabla 04** la longitud total del mensaje TCP es de 860 Bytes. Se ha fragmentado en 4 datagramas (240+200+320+100) por razones de simplicidad. En la realidad la fragmentación mínima de datagramas es de 576 Bytes y los fragmentos son múltiplos de 8 Bytes.

Tabla 04. Fragmentación de un mensaje TCP.

Orden del Datagrama	**1**	**2**	**3**	**4**
Tamaño del fragmento en número de Bytes	240	200	320	100
Longitud total TL del datagrama en número de bytes	260	220	340	120
Fragmentación MF (existencia y final de fragmentación)	0	0	0	1
Offset de fragmentación FO	0	30	55	95

IP es responsable por la ruta de los datos pero no lo es por la integridad de los mismos. De esto se ocupa la capa 4 (TCP requiere la retransmisión automática). No permite el secuenciamiento, control de flujo, apertura y cierre de la conexión y reconocimiento del servicio. TCP se encarga de reconocer cuando un datagrama se ha perdido (por tiempo de vida o errores) en la Internet.

COMANDOS PARA PROTOCOLO IP. El protocolo IP permite entre muchos otros los comandos de la **Tabla 05**. La interpretación de varios de estos comandos requiere el conocimiento del concepto de routing y del protocolo ICMP.

Tabla 05. Algunos comandos del protocolo IP

Add	Añade interfaces, servidores, *hostname*, routers, etc.
Change	Modifica la tabla programada mediante el comando Add.
Delete	Elimina las configuraciones realizadas mediante el comando Add.
Cache	Muestra la tabla de destinos enrrutados recientemente.
Counter	Diversos contadores pueden ser configurados para obtener estadísticas (paquetes con error, etc).
Dump	Enlista el contenido de la tabla de rutas del router.
Enable	Habilita diversas facilidades (routing ARP, broadcast, información RIP, etc).
Interface	Enlista las direcciones IP de las interfaces del router.
Show arp	Muestra la lista de direcciones IP y las direcciones MAC asociadas.
List	Muestra la lista de comandos que permiten la configuración de IP.
Ping	Emite un comando ICMP *Echo Request* para verificar el estado del elemento con IP Address requerida. La respuesta es un comando ICMP *Echo Replay*.
Route/Trace	Enlista la ruta seguida por los datagramas en la red hacia un destino específico. Se envían datagramas con TTL sucesivamente creciente para que sean descartados e informados mediante ICMP.
Static	Muestra las rutas estáticas especificadas mediante configuración.
Security	Permite la configuración de seguridad (*keyword*, *password*, etc).

3- OTROS PROTOCOLOS DE CAPA 3

Entre una amplia variedad de protocolos en capa 3 se encuentran los siguientes:
-**ICMP** (*Internet Control Message Protocol*). Utiliza datagramas de IP para llevar mensajes de estado entre nodos; es por ello parte integrante de IP. Luego del encabezado IP (20 Bytes) se colocan los datos ICMP. En el trabajo referido a la gestión de redes el ICMP se define con mayor detalle.
-**ARP** (*Address Resolution Protocol*). Permite comunicarse con un usuario IP sin conocer la dirección MAC del mismo.
-**RARP** (*Reverse ARP*). Funciona con estaciones sin disco que no pueden guardar las direcciones IP. Su función es requerir la dirección IP cuando se conoce la dirección MAC. ARP y RARP no utilizan datagramas IP, generan su propio datagrama. Para más detalles ver el ítem relacionado con protocolos de Routing.

3.1- VERSION DE PROTOCOLO IPv6.

Las versiones de IPv1 y IPv3 fueron reemplazadas por la actual IPv4. La IPv5 funcionaba con **SP** (*Stream Protocol*) en algunos routers. La versión IPv6 se inicia en 1992 con el llamado de propuestas. Es menos compleja y tiene un mayor tamaño de direcciones. Considera un mecanismo de autentificación y privacidad. Su implementación se demora por diversas razones; entre ellas las continuas mejoras que se introducen en la versión 4. El encabezado de IPv6 es el indicado en la **Tabla 06**.

En IPv6 no es posible que un router realice la segmentación de datagramas como en IPv4; la segmentación sola es posible en la fuente de información. En IPv6 la dirección es compatible con IPv4. En este caso 12 bytes iniciales llevan la dirección 00…0 y los 4 finales la dirección IPv4.

Tabla 06. Campos definidos en el encabezado del protocolo IPv6.

VRS	4 bits. Identifica la versión IPv6.
PRY	4 bits. Identifica la prioridad entre datagramas de la misma fuente.
FL	3 Bytes. *Flow Label*. Es el nivel de flujo de datos.
Length	2 Bytes. *Payload Length*. Identifica la longitud de la carga útil del datagrama.
Next	1 Byte. *Next Header*. Identifica al encabezado de longitud variable que sigue a continuación.
HL	1 Byte. *Hop Limit*. Reemplaza al TTL de Ipv4. Es el número máximo de router de tránsito.
Address	2x16 Bytes. para identificar la dirección de la fuente de origen y de destino. Las direcciones de Ipv6 contienen 16 Bytes. Se inicia con 010 y contiene: -Identificación del registro de la autoridad que asigna la dirección. -Identificación del proveedor de Internet. -Identificación del subscriptor. -Identificación de la subred conectada al subscriptor. -Identificación de la interfaz conectada a la subred.

3.2- PROTOCOLO CLNP

Se trata de la norma **ISO-8473** que define el protocolo **CLNP** (*ConnectionLess Network Protocol*). La versión del protocolo Internet para el modelo de ISO es distinta a la versión de la norma RFC de Internet. Se dispone de información similar a IP para el ensamble de los datagramas provenientes de una fragmentación. En la **Tabla 07** se enumeran los campos del protocolo. Cada opción en el datagrama debe ser especificada mediante 3 campos: el código del parámetro, la longitud del parámetro y el valor del parámetro.

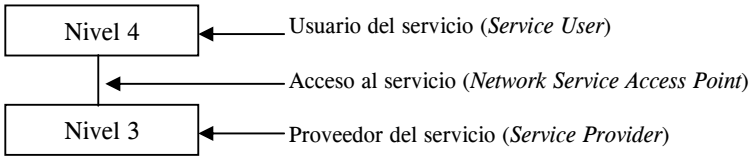
Los posibles parámetros definidos son:
-Compensación (*Padding*) para extensión del encabezado.
-Seguridad: definido por el usuario.
-Fuente de ruta: define las entidades de red que deben ser visitadas.
-Memoria de ruta: identifica las entidades que fueron visitadas para un reporte en pantalla.
-Calidad del servicio: define la disponibilidad y retardo.
-Prioridad: especificado entre 0 y 14.

DIRECCIONES NSAP. Esta dirección está normalizada por ISO y permite el direccionamiento entre equipos de la red SDH. Trabaja sobre el protocolo de capa 3 de ISO/ITU-T **CLNP**. Las funciones de router en este caso son desarrolladas por la tabla de ruta (*Routing Table*) que se actualizan en forma automática. El protocolo que permite actualizar esta tabla de rutas en TCP/IP es el OSPF y para el modelo ISO se denomina IS-IS.

Tabla 07: Elementos del protocolo ISO-8473 para Capa 3 CLNP.

	LONGITUD FIJA:
-PI	1 Byte. Es el identificador de protocolo de servicio Internet. Si la fuente y destino se encuentran en la misma red el encabezado se reduce a este único Byte.
-HL	1 Byte. Indica la longitud del encabezado en número de Bytes.
-VRS	1 Byte. Identifica la versión del protocolo.
-LF	1 Byte. Se trata del tiempo de vida del datagrama en unidades de 0,5 seg.
-Flag	3 bits. Contiene la siguiente información:
.S/P	1 bit. Indica si la segmentación está permitida.
.M/S	1 bit. Indica si existen más tramas.
.E/P	1 bit. Indica que se requiere un reporte de error a la fuente del datagrama si éste es descartado por error o porque expira el tiempo de vida.
-Type	5 bits. Indica si existen datos de usuario o un mensaje de error de PDU.
-SL	2 Bytes. Longitud de encabezado extra.
-HCS	2 Bytes. *Checksum* aplicado al encabezado para detección de error.
	CAMPO DE DIRECCIÓN VARIABLE:
-DAL	1 Byte. Indica la longitud en Bytes de la dirección de destino.
-DA	N Bytes. Especifica la dirección de destino.
-SAL	1 Byte. Indica la longitud de la dirección de origen.
-SA	N Bytes. Identifica la dirección de origen.
	INFORMACIÓN DE SEGMENTACIÓN:
-ID	2 Bytes. Identificador único para fuente y destino.
-SO	2 Bytes. Corrimiento (*off-set*) de Bytes en unidades de 8 Bytes.
-TL	2 Bytes. Longitud total original del mensaje PDU en Bytes.
	PARTE OPCIONAL:
-OPT	Opción: Servicios adicionales de longitud variable.
-Data	Datos de capa 4 de longitud variable.

La dirección **NSAP** (*Netwotk Service Access Point*) consiste en un una secuencia jerárquica de bytes (entre 14 y 20 bytes). El significado de este nombre proviene de los nombres dados al modelo de 7 capas. Así la interfaz entre la capa 3 y 4 genera un punto de acceso al servicio SAP que por corresponder a la capa 3 de red (Network) se denomina NSAP.



Los Bytes de numeración NSAP disponen del significado indicado en la **Tabla 08**.

Tabla 08. Componentes de la dirección NSAP.

-IDP	(*Initial Domain Part*). Contiene dos partes:
.AFI	(*Authority and Format Identifier*). Es 1 Byte para actuar como identificador de formato de dirección según norma ISO 6523 (hexadecimal 47), ISO 3166 (39), X.121 (37 o 53).
.IDI	(*Initial Domain Identifier*). El IDI identifica el inicio del dominio que sigue a continuación.
-DSP	(*Domain Specific Part*). Parte específica de dominio que incluye los campos de Area, Estación. Incluye la dirección MAC. La longitud total de la dirección se encuentra entre 14 y 20 Bytes.
-NS	1 Byte para Selector de NSAP (valor hexadecimal fijo 01).

3.3- PROTOCOLO IPX/SPX

Los protocolos de capa 3/4 **IPX/SPX** (*Internetwork Packet Exchange/Sequenced Packet Exchenge*) fueron patentados por Novell a semejanza de **XNS** (*Xerox Network System*). En la **Tabla 09** se enumeran los campos del protocolo IPX/SPX. Este protocolo disponía de 20 millones de usuarios en 1993. Novell introdujo microcomputadores en los años 1970 con el procesador Z80 y en los años 1980 con el procesador Motorola 68000.

Tabla 09. Contenido del datagrama de capa 3 en el protocolo IPX/SPX.

-IPX	30 Bytes. Son usados para el direccionamiento en capa 3; su descripción particular es la siguiente:
.CS	2 Bytes. Checksum para control de paridad sobre el encabezado.
.Length	2 Bytes. Longitud del datagrama. Hasta 576 Byte con el encabezado incluido.
.TC	1 Bytes. Para control de transporte.
.PT	1 Bytes. Tipo de paquete.
.DNE	4 Bytes. Identifica a la red de destino.
.DNO	6 Bytes. Identifica al nodo de destino.
.DS	2 Bytes. Indica el protocolo de destino del datagrama; semejante a la dirección SAP.
.SNE	4 Bytes. Identifica a la red de origen.
.SNO	6 Bytes. Identifica al nodo de origen.
.SS	2 Bytes. Indica el protocolo de origen del paquete.
-SPX	12 Bytes. Para el mecanismo de retransmisión ARQ. Reconoce la ausencia de paquetes y los cambios de posición. Realiza el control de conexión en el ámbito de capa 4.
-Data	Campo de información. La longitud del datagrama se encuentra entre 512 y 6500 Bytes.

El protocolo IPX en la capa 3 genera datagramas en la versión sin-conexión. No espera el reconocimiento del estado de recepción; basta la respuesta del otro extremo para confirmar la transmisión. Por otro lado, SPX en la capa 4, dispone de retransmisión automática en caso de falta de respuesta por un determinado tiempo. Se trata de un protocolo con-conexión. En la **Tabla 10** se presenta una lista de protocolos relacionados con IPX/SPX.

Tabla 10. Protocolos de capas superiores a IPX/SPX.

-NCP	(*Netware Core Protocol*). Es el protocolo principal para la transferencia de información entre el cliente y servidor en la red LAN Netware.
-SAP	(*Service Advertising Protocol*). Es usado por el servidor y Router como mensajes broadcasting sobre la red cada 1 minuto. Indica el tipo de servicios que puede proveer sobre la red.
-RIP	(*Routing Information Protocol*). Utiliza un algoritmo para calcular el trayecto entre Router y utiliza mensajes RIP cada 1 minuto para planear e informar cambios en la tabla de enrrutamiento.

1203

PROTOCOLOS TCP-UDP

Sobre el funcionamiento y la trama de datos de los protocolos de transporte en capa 4. Referido a los protocolos de RFC (TCP y UDP) y los protocolos ISO (TP4).

1- PROTOCOLO TCP

1.1- TRAMA TCP PARA INTERNET

El protocolo TCP puede entregar los siguientes servicios: multiplexación para varias puertas de usuario (varias puertas de aplicación en TCP sobre una TCP/IP); gestión de la conexión (inicio, mantenimiento y terminación). transporte de datos (full-dúplex, ordenamiento, control de flujo, chequeo de errores). Tratándose el protocolo TCP de un servicio orientado con-conexión el funcionamiento incluye el establecimiento y finalización de la llamada. La estrategia de transferencia de datos incluye la retransmisión, la detección de duplicación y el control de flujo. En la **Fig 01** se indica el modelo de capas y en la **Fig 02** la trama RFC-0793. En la **Tabla 01** se indican las funciones de cada campo del paquete TCP. En la **Tabla 02** se muestra una traza de mensaje intercambiado entre entidades TCP/IP.

Tabla 01: Elementos de protocolo RFC-793 para Capa 4 (TCP).

-SP	2 Bytes. Identifica la puerta (*Port TCP*) de acceso al servicio origen en TCP. Se trata de direcciones TSAP que numeran desde 1 a 225 los protocolos más conocidos (Echo:7, SMTP:25; FTP:21; Telnet:23; Gopher:70; y Web:80). El protocolo UDP identifica las aplicaciones SNMP:161; TFTP:69 y RPC-Sun:111. Desde la port 256 a 1023 se reserva para aplicaciones UNIX. Las aplicaciones propietarias llevan la dirección de port desde 1024 hasta 49151; las direcciones superiores a 40152 se asignan en forma dinámica. La combinación de la dirección IP y la port TCP/UDP es conocida como ***Socket*** cuya asignación puede estar predeterminada (para protocolos conocidos) o se asigna entre los valores no utilizados (para las aplicaciones nuevas).
-DP	2 Bytes. Identifica la puerta de acceso al servicio de destino. Tiene igual estructura a SP.
-SN	4 Bytes. (*Sequence Number*) Número secuencial del primer octeto de datos en el segmento para la puerta correspondiente. Permite el proceso de requerimiento de retransmisión automática **ARQ**. La longitud máxima del mensaje de capas superiores que puede segmentar TCP es de 2^{32} Bytes; la longitud máxima del segmento que puede entregar a IP es de 2^{16} Bytes.
-AN	4 Bytes. Contiene el número de secuencia del próximo Byte que el TCP espera recibir. Es un reconocimiento ACK de los Bytes recibidos.
-DO	4 bits. (*Data Offset*) Número de palabras de 4 Bytes del encabezado.
-RSV	6 bits. Reservados.
-Flags	6 bits. Son bits utilizados para señalar la validez de otros campos y para el control de conexión.
.URG	1 bit. Indica la existencia del puntero urgente en los datos (UP al final del header). Se trata de la función *Break* que notifica a la aplicación del TCP receptora que los datos son urgentes y deben ser presentados de inmediato en pantalla.
.ACK	1 bit. Indica la existencia del campo de reconocimiento (AN al inicio del header).
.PSH	1 bit. Función *push* envía los datos desde un usuario (login remoto) cuando se presiona *Return*. Los datos son transferidos por TCP y presentados en la aplicación del otro extremo.
.RST	1 bit. Indica que se debe realizar un *Reset* de conexión debido a un error grave.
.SYN	1 bit. Usado para iniciar el seteo de conexión entre nodos. Se usa solo en el primer paquete de la conexión; en éste el primer byte de datos se numera como SN+1. El valor SN es un número de 4 bytes (se incrementa cada 4.10^{-6} seg; período de 5 hs).
.FIN	1 bit. No más datos desde el emisor. Usado para iniciar la desconexión del enlace TCP.
-WIN	2 Bytes. (*Window*). Crédito para control de flujo. Una PC tiene una capacidad de buffer limitada (4 kBytes) equivalente a 4 tramas de Ethernet de 1 kByte. Un crédito 0 detiene la emisión de datos.
-CS	2 Bytes. (*Checksum*) Control de error sobre el encabezado y la carga útil. Permite la detección de errores para realizar la retransmisión.
-UP	2 Bytes. (*Urgent Pointer*). Puntero que indica la cantidad de datos urgentes (identifica el final de los datos urgentes en el campo de datos que deben tratarse con prioridad).
-OPT	Opcional de longitud variable.
-Data	Datos de capas superiores.

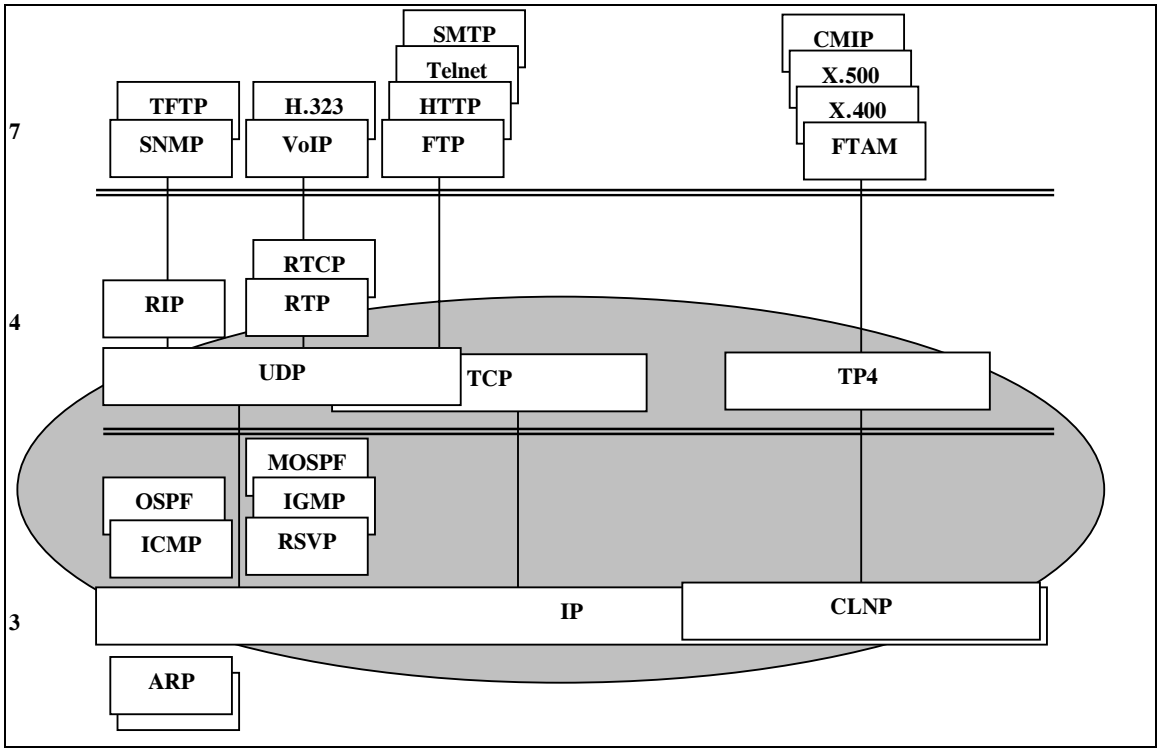


Fig 01. Modelo de capas para los protocolos TCP y UDP.

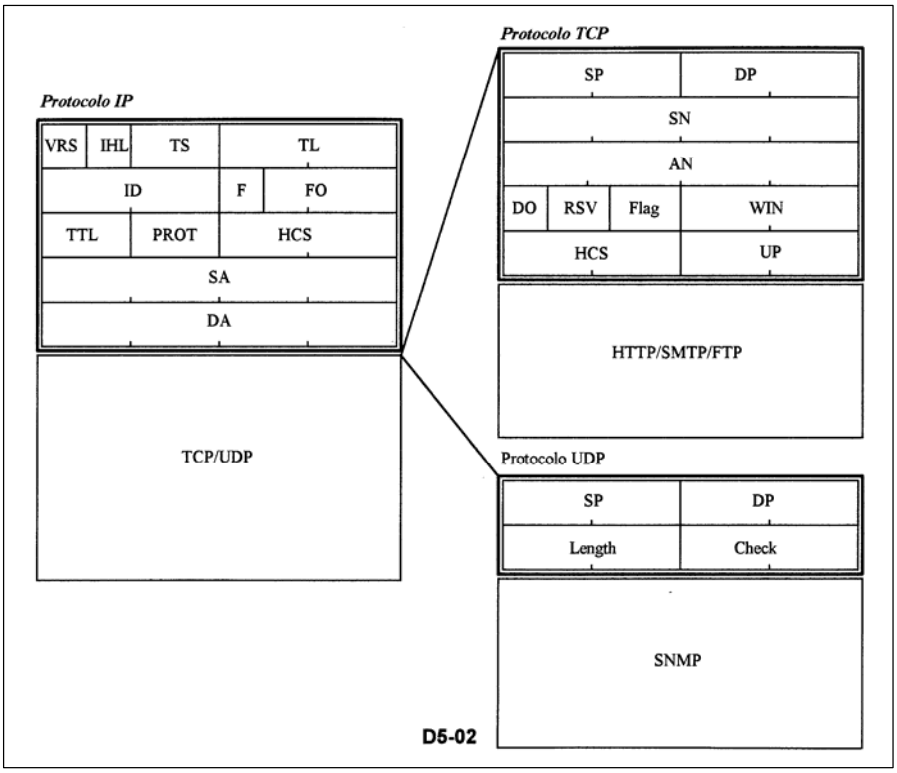


Fig 02. Campos de los protocolos TCP y UDP.

PROTOCOLOS TCP/UDP

Si la conexión al medio de enlace se supone mediante una LAN del tipo IEEE 802.3, se dispone de los campos de dirección **SAP** dentro del protocolo LLC y **SNAP** adicional. Las direcciones son:
-En Ethernet IEEE 802.3: el Type: IP=0800; ARP=0806 y RARP=8035.
-En SNAP (*Sub-Network Address Point*). Consta de 2 campos: 3 Bytes para el identificador de versión de protocolo **IP** y 2 Bytes para identificador de SAP (0800 para TCP/IP y 0600 para XNS).
-La dirección SAP en la capa IP se determina mediante el campo *Protocol* y en TCP/UDP se identifican mediante dos Bytes de *Port*.

Tabla 02. Traza de protocolos TCP-IP-Ethernet

HEWLETT-PACKARD Network Advisor		
Measurement: Network Stack Decode	Prínt Type: Frames 1	Open Views: Summary Detailed Data
Display Mode: Viewing All Frames	Print Date: 10/03/95	Print Time: 21:45:31
DETAILED FORMAT TCP		
Source port	1208	User prog. port
Destination port	23	Telnet
Sequence number	0	Initial sequence number
Data offset	6	Number of 32-bit words in header
Flags:	..00-0010	
Urgent flag	..0.....	
Ack flag	...0....	
Push flag	....0...	
Reset flag	.....0..	
Syn flag	......1.	Synchronizing sequence numbers
Fin flag	0	
Window	512	
Checksum	20-D9	
Urgent pointer	0	Not used
Option type	2	MaxiTnilm segment size
Option length	4	
Max seg size	1460	
DETAILED FORMAT IP		
Version	4	
Internet header length	5	(32 bit words)
Precedence	000.....	Routine
Delay	...0....	Delay normal
Throughput	....0...	Throughput normal
Reliability	......0..	Reliability normal
Reserved	00	
Total Length	44	
Identification	198	
Reserved	0.......	
May/Do Not Fragment	.0.....	
Fragmentation allowed		
Last/More Fragments	..0.....	
Last fragment		
Offset	0	
Time To Live	31	
Next Protocol	6	TCP
Checksum	2A-88	
Source	160.1.131.180	
Destination	132.0.200.200	
DETAILED FORMAT ETHERNET		
Destination address	00-20-8A-00-28-4F	Individual, global
Source address	HP---------82-E9-DC	
Individual, global		
Type	08-00	IP

1.2- FUNCIONAMIENTO DE TCP

INICIO DE CONEXIÓN. Se trata de un saludo de 3 pasos. Cada extremo informa el número secuencial SN que pretende utilizar. El primer paquete lleva la bandera SYN=1 y el número secuencial SN=X (se genera mediante un contador de 32 bits que se incrementa cada 4 μseg y de período 5 horas). La respuesta a este paquete consiste en SYN=1 y ACK=1 más el propio número secuencial SN=Y y el acuse de recibo AN=X+1 (acuse de recibo del valor X). El tercer paso es responder al paquete anterior con ACK=1 y el acuse de recibo AN=Y+1.

RETRANSMISIÓN. Mediante el mecanismo de reconocimiento se puede pedir la retransmisión de segmentos cuando estos llegan corruptos por errores o faltan segmentos intermedios. Es de fundamental importancia cuando las capas inferiores de la red no prevén la retransmisión (tal es el caso de Frame Relay y ATM). Las redes Ethernet (IEEE 802.3) y el protocolo PPP tienen desactivado el mecanismo de control en el protocolo LLC (tampoco corrigen errores).

La capa 3 (Internet) no se ocupa de la confirmación de datagramas. Es TCP quien confirma, para cada puerta individual, los segmentos recibidos. La combinación de los campos AN y WIN permite el reconocimiento y el control de flujo.

Cuando se requiere emitir una secuencia de N bytes de datos, el TCP coloca la bandera PSH=1 (empujando la emisión inmediata) y SYN=1; en tanto que la numeración secuencial SN=X. El receptor retorna un mensaje con ACK=1 y la confirmación AN en el valor X+N+1 y el valor de la ventana WIN. Cuando existe un error se envía las banderas RST,SYN,ACK=1. En la siguiente **Tabla 03** se indica un ejemplo.

Tabla 03. Ejemplo del proceso de retransmisión entre los terminales A y B.

Transmisión desde A hacia B		**Condiciones de enlace**	**Respuesta desde B hacia A**	
SN= 1	TL= 1093	⇒	AN= 1093	WIN= 2000
		⇐		
SN= 1093	TL= 1217		AN= 2310	WIN= 2000
SN= 2310	TL= 310	Error de comunicación	AN= 2310	WIN= 500
SN= 2310	TL= 310		AN= 2620	WIN= 20
SN= 2620	TL= 20		AN= 2640	WIN= 0
		…tiempo de espera…		
			AN= 2640	WIN= 2000
SN= 2640	TL= 1060			

CONTROL DE FLUJO. El mismo mecanismo de reconocimiento permite regular el flujo de datos en el protocolo TCP. El control de flujo de datos se complica debido al retardo entre entidades TCP y por la pérdida de segmentos. Además debe considerarse la posibilidad de arribo de segmentos fuera de orden y a la pérdida de segmentos con información de crédito. Sin el control de flujo los datos pueden superar la capacidad del buffer de recepción antes de ser procesados.

Se hace uso de dos elementos AN y el crédito o ventana (*Window*):
-AN=H reconoce hasta la secuencia (H-1) e indica que espera la secuencia H;
-el crédito WIN=K autoriza la transmisión hasta la secuencia (H-1)+K.

Obsérvese que los mecanismos de control de flujo se complican sucesivamente desde la capa 1 a la capa 4.
-En la capa 1 en la interfaz RS-232 se utilizan dos hilos. El **RTS** solicita permiso para transmitir, el **CTS** responde aceptando o no la recepción de datos. -Se trata de un mensaje mediante niveles de tensión sobre hilos metálicos.
-En la capa 2 en los protocolos de tipo HDLC (LAP-B, LAP-D, LLC) utilizan dos bits del campo de control. Mensaje **RR** para indicar la aceptación de recepción y **RNR** para indicar que no está preparado para recibir. -La capa 2 en Frame Relay y ATM implementan alarmas para desencadenar un control de flujo de los extremos.
-En la capa 4 en TCP implementa un control de flujo mediante **WIN** que indica el buffer disponible para la recepción. Cuando TCP detecta errores o falta de datos y realiza la retransmisión reduce el tamaño de la ventana para descongestionar la red (posteriormente la incrementa en forma sucesiva).

TIME-OUT. El valor de time-out de retransmisión es crítico. Si es muy corto incrementa el tráfico inutilmente y si es muy largo genera largos períodos de espera. Existen formas de realizar un tiempo time-out dinámico; en otros casos el mismo es configurable y fijo.

CIERRE DE CONEXIÓN. Se trata de un proceso de 3 pasos. Cuando la aplicación se cierra (*Close*) el TCP envía un mensaje con la bandera FIN=1. Se envían 2 mensajes de respuesta, el primero confirma mediante ACK=1 y el segundo cierra la conexión mediante SYN=FIN=1. A esto se responde con un mensaje de reconocimiento ACK=1 y otro de terminación.

2- OTROS PROTOCOLOS

2.1- PROTOCOLO UDP

El protocolo **UDP** (*User Datagram Protocol*) se ubica en la capa de transporte. El encabezado UDP ocupa 4 campos de 2 Bytes cada uno y se identifica en la **Tabla 04**. UDP es un protocolo minimalista, obsérvese que muchas de las funciones de TCP han sido eliminadas. Dispone de los campos de port para identificar a los usuarios de UDP (protocolos como SNMP, RTP, etc.); indica además la longitud del paquete y realiza un chequeo de errores sobre todo el paquete. Sin embargo no retransmite en caso de falta de datos, lo cual es útil en el caso de servicios de tiempo-real (voz y vídeo) donde esta función no es deseada.

Tabla 04: Campos de información de UDP (capa 4) y SNMP.

	Protocolo UDP.
-SP	2 Bytes. Identifica al número de puerta (*Port*) de origen del mensaje.
-DP	2 Bytes. Identifica al número de puerta de destino del mensaje.
-Length	2 Bytes. Determina la longitud total del datagrama UDP (incluyendo el encabezado y datos).
-Check	2 Bytes. Es un *Checksum* para control de errores del mensaje completo.

2.2- PROTOCOLO ISO-8073.

Se trata de una familia de protocolos que contiene 10 tipos de unidades de datos. Los campos que lo componen se identifican en la **Tabla 05**. Solo se dispone de un tipo de trama en TCP mientras que ISO-TP4 tiene 10 tipos. Esto determina mayor simplicidad en TCP pero un encabezado más extenso (20 y 5 Bytes respectivamente).

En tanto en TCP se establece una conexión independiente en cada sentido, en TP4 se requiere una doble conexión en full-dúplex. En tanto, TCP usa 16 bits de dirección de port, el TP4 no especifica la dimensión. Cada trama contiene un encabezamiento fijo y otro variable. El encabezado variable consta de una secuencia de campos de parámetros. Cada campo contiene: el código del parámetro (8 bits), la longitud del parámetro (8 bits) y el valor (1 o más Bytes).

Tabla 05: Elementos de protocolo ISO-8073 para Capa 4 Transporte (TP4).

	Composición de la trama	**Función**
-CR =	LI+CR+CDT+SR+Class+Opt	Pedido de conexión
-CC =	LI+CC+CDT+DST+SR+Class+Opt	Confirmación de conexión
-DR =	LI+DR+DST+SR+Reason	Pedido de desconexión
-DC =	LI+DC+DST+SR	Confirmación desconexión
-DT =	LI+DT+DST+EOT+TPDU	Datos
-ED =	LI+ED+DST+EOT+EDTPDU	Datos urgentes
-AK =	LI+AK+CDT+DST+YR	Reconocimiento de trama
-EA =	LI+EA+DST+YR	Reconocimiento urgente
-RJ =	LI+RJ+CDT+DST+YR	Trama descartada
-ER =	LI+ER+DST+Cause	Trama con error
	Campos de encabezado fijo contenidos en TP4.	
-LI	1 Byte. Longitud del encabezado fijo y variable en Bytes.	
-**TT**	4 bits. Código del tipo de TPDU (trama de protocolo CR a ER).	
-CDT	4 bits. Crédito (*window*) para el control de flujo. Crédito inicial en CR y CC y los siguientes en AK.	
-Class	4 bits. Clase de protocolo.	
-Opt	4 bits. Opción para el control de flujo.	
-Reason	1 Byte. Razón para la desconexión.	
-EOT	1 bits. Indica el último segmento de TPDU.	
-TPDU	7 bits. Número de secuencia de segmento emitido.	
-YR	1 Byte. Próximo número de secuencia esperado.	
-Cause	8 bits. Razón por la cual se descarta una trama.	
	Campos de parámetros para TP4.	
-TSAP	Identificador de punto de acceso al servicio de origen y destino.	
-Size	Tamaño en Bytes de la trama TPDU (128 a 8192 en potencia de 2).	
-Version	Versión del protocolo.	
-Checksum	Algoritmo para detección de errores.	
-ACT	Tiempo estimado para el reconocimiento.	
-Priority	Prioridad de esta conexión.	
-Delay	Especifica el retardo en mseg.	

2.3- TCP/IP over ETHERNET

En la **Fig 03** se muestra el empaquetado del protocolo TCP/IP (20 Bytes de encabezado para cada caso) sobre el paquete de Ethernet de acuerdo con la RFC-1042. En este caso Ethernet está representado por 14 Bytes de encabezado MAC (no se incluye el preámbulo de 8 Bytes); por 4 Bytes del protocolo LLC y por 5 Bytes del SNAP.

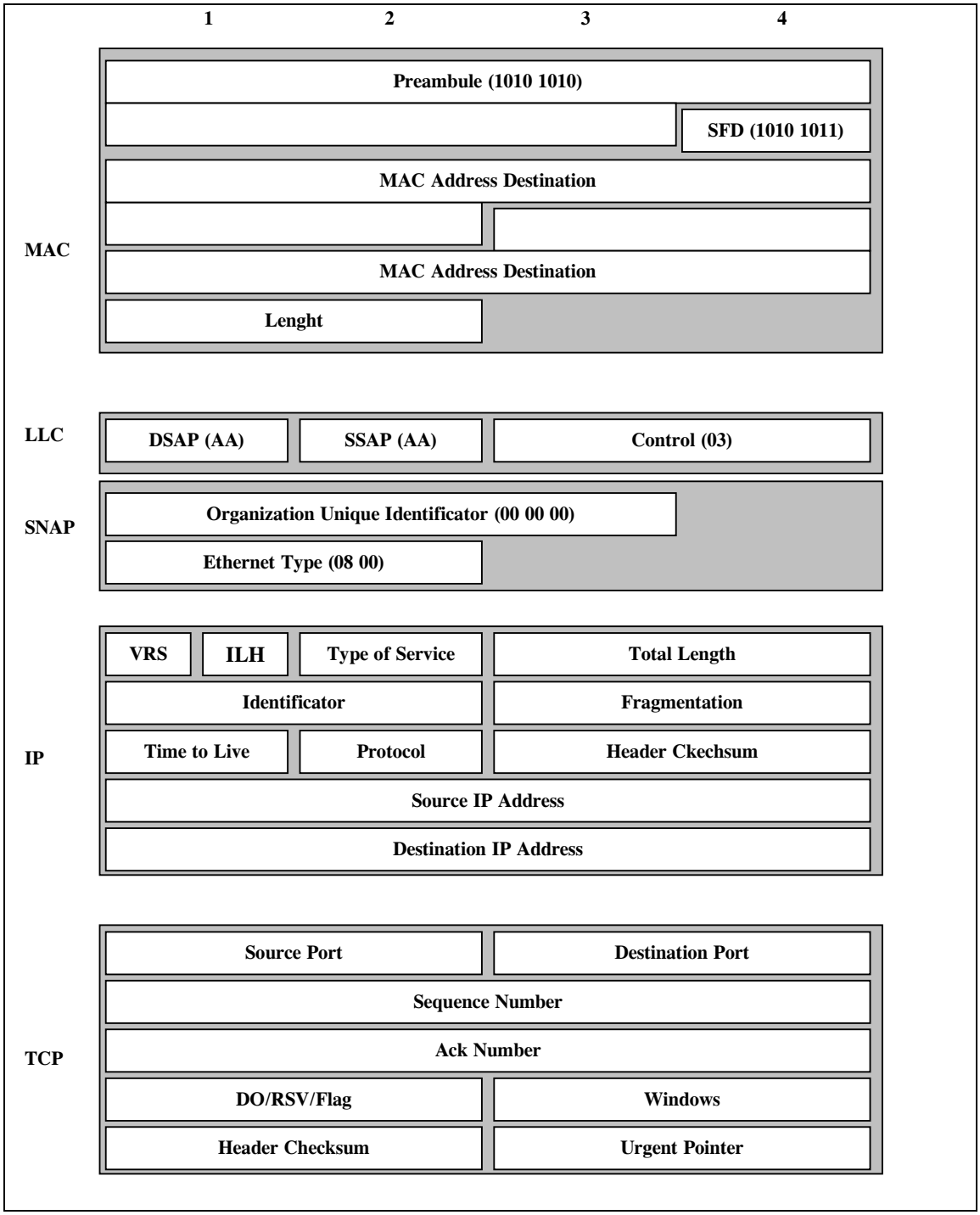


Fig 03. Campos del protocolo TCP/IP/Ethernet.

1204

ACCESO A INTERNET

Con referencia a los métodos de acceso disponible a la red Internet.

1- ACCESOS A INTERNET

El protocolo IP de routing es independiente del soporte físico de transporte. De esta forma se disponen de soluciones para los diversos casos enumerados en la **Tabla 01**. Normalmente se habla en términos de "IP sobre …", así **IP-over-SDH** significa que el protocolo IP se ingresa en la carga útil del contenedor VC-4 en la trama STM-1.

Tabla 01. Soportes físicos para redes IP.

DDR	-(*Dial-on-Demand Routing*). Entrega una conexión de la red IP a la red pública telefónica **PSTN**. Se implementa sobre líneas conmutadas de circuitos para reducir el costo de conexión. Puede ser desarrollada sobre interfaz serial sincrónica o asincrónica o sobre líneas ISDN usando interfaz **BRI** (*Basic Rate Interfaz*) o **PRI** (*Primary RI*). El protocolo soporte puede ser el PPP o X.25. La topología es muy simple: generalmente punto-a-punto entre routers hacia un router central que funciona de concentrador. El router dispone de una mapa estático de direcciones telefónicas (*Dialer Map*) que actúa en forma similar a ARP en las LAN; relaciona la dirección IP con un número telefónico. Utiliza la señalización dentro de banda de la norma **ITU-T V.25** para equipos DCE síncronos.
Dial-up	**PROTOCOLO PPP** (*Point-to-Point Protocol*). Standard de Internet que puede obtenerse desde RFC-1661. Requiere una conexión bidireccional del tipo full-dúplex; multiplexa distintos protocolos de red; realiza una configuración de enlaces; realiza un test de calidad de enlaces; detecta errores, puede criptografiar la carga útil de la trama y comprimir los datos.
X.25/F.Relay	-Se refiere a accesos de baja velocidad (desde 19,2 kb/s hasta Nx64 kb/s, máximo de 2 Mb/s). Normalmente se utilizan las líneas de acceso metálicas al usuario. Para ello se utilizan las redes de multiplexores PDH. Para permitir la gestión remota del extremo en el usuario se coloca un router conversor de interfaz (red LAN a V.35) gestionable mediante protocolo SNMP. Las líneas X.25 se utilizan hasta 64 kb/s, mientras que la Frame Relay se aplica para Nx64 kb/s. En la **Fig 01** se muestra el modelo de capas para el acceso a una red LAN mediante un router extremo para convertir LAN en X.25 (interfaz V.35). La red de transporte indicada en la figura es ATM.
ATM	-Esta alternativa ha recibido un gran impulso para redes de alta velocidad. En este caso se refiere a la emulación de redes LAN. La conexión de servicios Internet sobre ATM se ha propuesto mediante 2 alternativas. La primera (RFC-1577) tiene en cuenta el *Classical IP over ATM* que se trata de segmentar el datagrama IP en celdas de tipo AAL5. La otra alternativa determina la *LAN Emulation* (interfaz LAN para usuario-nodo **LUNI**) que dispone las capas IP/LLC sobre las capas LUNI/AAL5. La conexión desde una LAN hacia la ATM (interfaz UNI) se puede efectuar mediante dos formas. En la primera se utiliza la función *LAN Emulation* donde el concentrados ATM realiza las funciones de router para ingresar la LAN sobre AAL5. En la segunda se utiliza un acceso mediante router externo con el protocolo **DXI** (*Data Exchange Interface*). DXI es un protocolo de capa 2 (debajo de LLC) con trama similar a Frame Relay y campo de direcciones **DFA** (*DXI Frame Address*).
SDH/Sonet	-Los router pueden disponer de una interfaz hacia redes SDH. Los paquetes IP se encapsulan sobre PPP/HDLC y luego se mapean en la carga útil del VC-4, donde el puntero H4 (para celdas ATM) pierde sentido.
E1/Nx64 kb/s	-Los routers pueden disponer de interfaces E1 a 2048 kb/s o interfaz V.35 a Nx64 kb/s. En ambos casos el protocolo IP se encapsula en PPP/HDLC.
Ethernet	-La aplicación tradicional de utilizar el protocolo IP sobre LAN se incrementa ante la variante de velocidades de 100 y 1000 Mb/s utilizando fibras ópticas como medio de soporte. Así mediante unidades **Fast Ethernet** y **Gigabit Ethernet** con fibras ópticas monomodo es posible realizar enlaces entre router de decenas de kilómetros y formar una red MAN directamente soportado en protocolos TCP/IP/LLC/MAC. De esta forma un router se vería como una interfaz entre dos redes (LAN y MAN) con igual protocolo (Ethernet) pero distinta velocidad (10/100 Mb/s del lado usuario y 100/1000 Mb/s del lado MAN) y medio (cable UTP del lado usuario y fibra óptica del lado MAN).

GigabitEthernet vs. ATM. A fines de la década de los años `90 estas dos formas de transporte de protocolo TCP/IP se encontraban en competencia. El estado del arte determinaba las siguientes características:

-Gigabit Ethernet lleva ventaja en cuanto hace a la comprensión de la tecnología, la capacitación del personal, la operación y management del mismo. El diseño de red desde el punto de vista de la ingeniería y el mantenimiento es más simple. El precio también es menor.
-Sus prestaciones son idénticas desde el punto de vista de la resilencia (tolerancia a las fallas), la escalabilidad y la seguridad de la red. Son similares en cuanto hace a la posibilidad de definir QoS, los accesos VLAN y los servicios multicast.

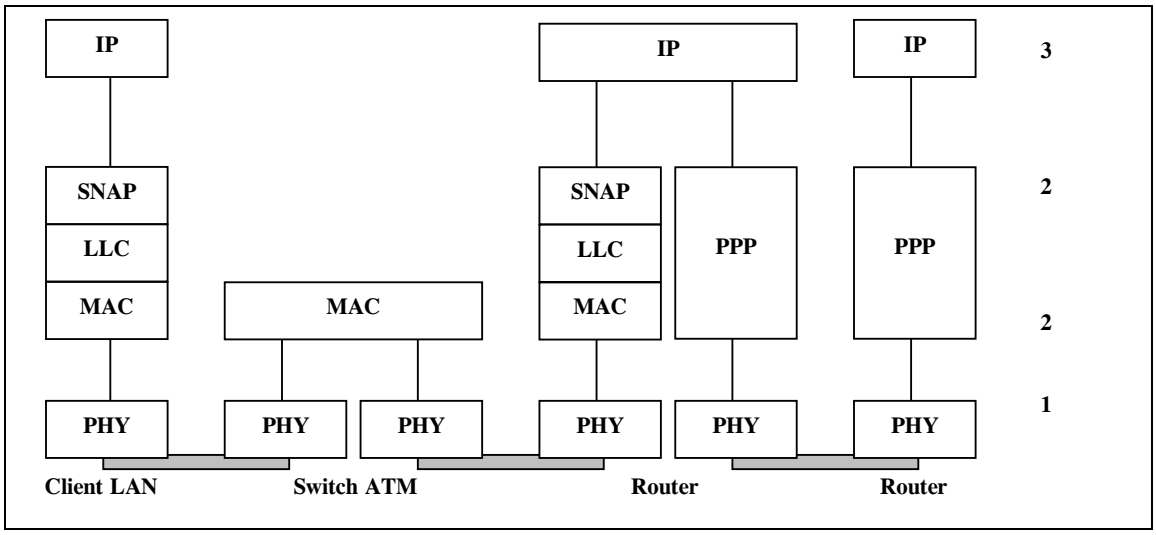


Fig 01. Modelo de capas de accesos a redes IP (Internet).

2- CONEXION DIAL-UP A INTERNET

2.1- MODEM DE DATOS

Los protocolos Módem para la transferencia de archivos entre computadores mediante la línea telefónica incluyen varios desarrollos. En el ámbito Internet se han definido dos protocolos de acceso al nodo mediante módem de datos: SLIP y PPP. La velocidad recomendada es de 14,4 o 28,8 kb/s y sus características se describen a continuación en la **Tabla 02**.

Tabla 02. Protocolos de acceso dial-up a Internet.

-Xmodem.	-Se trata de un desarrollo de **W.Christensen**-1977 que permite la transferencia de *file* binario y de texto entre micro-computadoras. El bloque consta de un carácter de encabezado, 128 Bytes de datos y uno de paridad para control de error. En los años '90 la popularidad continúa sobre la base de nuevas versiones y la aplicación en PC portátil.
-Ymodem.	-Desarrollado por **C.Forsberg**-1981 se ha convertido en un elemento esencial en un software de comunicación de PC. Posee un encabezado inferior a Xmodem y permite transferir bloques de datos de 1024 Byte. Si la calidad de transmisión es mala se reducen los bloques a 128 Byte para reducir el número de Byte a ser retransmitidos.
-Zmodem.	-Fue desarrollado por C.Forsberg-1986. Incluye el chequeo de errores CRC-32 y el rearranque (cuando una conexión se interrumpe, al reiniciarse se continua desde el punto de corte).
-Kermit.	-Original de **Columbia University**-1981. Diseñado para conexión de computadoras distintas con estructura de trama similar a Xmodem. Los bloques son de longitud variable de hasta 96 caracteres. Posee un código detector de errores checksum y un protocolo de repetición automática ARQ.
-LAP-M.	-(*Link Access Protocol-Modem*). Pertenece al **ITU-T V.42** desde 1988. Se trata de un protocolo del tipo HDLC denominado Protocolo de Acceso al Enlace del Módem. Trabaja con módem desde 1200 b/s en forma sincrónica. Permite el empaquetado de datos start-stop en tramas sincrónicas (protocolo BOP) con detección de error y retransmisión de tramas.
	PROTOCOLOS DIAL-UP DE INTERNET
-SLIP	-(*Serial Line Internet Protocol*). Normalizado en RFC-1055 permite la conexión punto-a-punto, sin utilizar direcciones ni control de errores. Permite la conexión en capas 2 hacia la red Internet mediante módem de hasta 19200 b/s por línea telefónica, con datagramas de hasta 1006 Bytes de largo. En este protocolo se definen los Bytes *Slip End y Slip Esc*. El byte *Slip End* inicia y cierra un datagrama de TCP/IP. Si un byte simula la secuencia *Slip End* (hexadecimal C0) se envía *Slip Esc* (DB) y (DC); si se simula *Slip Esc* se envía *Slip Esc* (DB) y (DD).
-PPP	-(*Point-to-Point Protocol*) Normalizado en RFC-1171. Preparado para una línea serial, permite la conexión de datos asincrónicos (start/stop) o asincrónicos BIP. Es más avanzado que SLIP y como está adaptado para redes LAN dispone de direcciones y control de error. Requiere una conexión full-dúplex. Mejora a SLIP en los siguientes aspectos: Asigna direcciones para acceso del tipo *Dial-up*; multiplexa distintos protocolos de red; realiza una configuración de enlaces; realiza un test de calidad de enlaces; detecta errores y comprime datos. Se ha previsto la criptografía y compresión de datos en PPP. Este protocolo se utiliza para realizar tunelización en el servicio VPN.

MODEM DE DATOS. Son usados para transmitir datos digitales por la red de conexión analógica y no son tratados en este trabajo. Los módem se iniciaron en 1962 a 2400 b/s, en 1967 se trabajaba a 4800 b/s, en 1971 a 9600 b/s, en 1980 a 14400 b/s y 1985 a 19200 b/s. En la red digital los datos son multiplexados en un canal de 64 kb/s. Solo a modo de referencia se muestra la siguiente **Tabla 03** del ITU-T en la Serie V referida al módem de datos.

Tabla 03: Características de los módem de datos en la red telefónica.

ITU-T	Velocidad	Modulación	Observaciones
V.21	300 b/s	FSK	Full-Dúplex asíncrono. Tx: 1080 ±100 Hz Rx: 1750 ±100 Hz
V.22	600-1200 b/s	4PSK	Start-stop asíncrono. Línea 2 hilos.
V.22 bis	2400 b/s	16QAM	Full-Dúplex. Tx: 1200±300 Hz Rx: 2400±300 Hz
V.23	600-1200 b/s	FSK	Datos 1700±400, supervisión 420±30 Hz. Línea 2 o 4 hilos.
V.26 bis	2400 b/s	4PSK	Datos 1800 Hz. Dúplex a 4 hilos.
V.27 ter	4800 b/s	8PSK	Datos 1800 Hz. Dúplex a 4 hilos.
V.29	9600 b/s		Full-Dúplex a 4 hilos.
V.32	9600 b/s	16QAM	Full-Dúplex
V.33	14400 b/s	TCM	
V.35	48 kb/s	AM-SSB	60-108 kHz sincrónico, dúplex a 4 hilos.
V.36	48-56-64 kb/s		60-108 kHz sincrónico, dúplex a 4 hilos.
V.37	96-128-144 kb/s		60-108 kHz sincrónico, dúplex a 4 hilos.

2.2- PROTOCOLO PPP (*Point-to-Point Protocol*).

Se trata de un standard de Internet que puede obtenerse desde RFC-1661. Es más avanzado que SLIP y como está adaptado para redes LAN. Dispone de direcciones y control de error. Requiere una conexión bidireccional del tipo full-dúplex. Asigna direcciones para acceso del tipo *Dial-up* (acceso telefónico por la red PSTN); multiplexa distintos protocolos de red; realiza una configuración de enlaces; realiza un test de calidad de enlaces; detecta errores, puede criptografiar la carga útil de la trama y comprimir los datos.

El modelo de capas de PPP incluye:
-En la capa 1 se aceptan conexiones desbalanceadas RS-232 y balanceadas RS-422 y V.35. Utiliza algunas de las alternativas de módem de datos de alta velocidad (hasta 56 kb/s).
-En la capa 2 se genera un paquete del tipo HDLC que contiene: bandera, campo de dirección, campo de control, identificador de protocolo, datos y paridad (ver la **Tabla 04**). Posteriormente se encapsula los protocolos LCP o los datos en dicha trama.
-Se dispone de un protocolo **LCP** (*Link Control Protocol*) para el control del enlace de datos. Tiene diversos formatos de paquetes: para la configuración inicial del enlace (*Request, Ack, Nack, Reject*), para el test del enlace y el cierre de la conexión (*Requst, Ack*). El protocolo LCP dispone de la trama indicada en la **Tabla 04**.

Tabla 04. Campos del paquete para protocolo LCP de control.

	Overhead PPP.
-Flag	1 Byte. Bandera (hexadecimal 7E) para inicio y final de trama.
-Address	1 Byte. Dirección de destino (hexadecimal FF). Solo posee la función broadcasting. Se trata de una conexión punto-a-punto.
-Control	1 Byte. Para el secuenciamiento de la información similar a LLC o un valor fijo para tramas no-secuenciadas (03 hexadecimal).
-Protocol	2 Bytes para identificar el protocolo de capa superior (punto de acceso al servicio SAP por ejemplo, (hexa) 0021 para IP, 0023 para ISO, 802B para IPX). Cuando se dispone del protocolo de control LCP indica C021.
	Campo LCP.
-Code	1 Byte para identificar el tipo de paquete LCP. Se trata de *Configure* (*Request, Ack, Nack* y *Reject*); *Terminate* (*Request, Ack*); *Echo* (*Reject, Replay*); *Reject* (*Code, Protocol, Discart*).
-ID	1 Byte de identificador que se utiliza para los requerimientos y respuestas.
-Length	2 Bytes para indicar la longitud del campo LCP y los datos.
-Data	Los paquetes del tipo *Reject* contienen la copia de los datos rechazados para ser interpretados por el emisor.
	Trailer PPP.
-FCS	Control de error de 2 (*default*) o 4 Bytes por configuración.
-Flag	1 Byte. Bandera (7E) para delimitación final de la trama.

Cuando los routers negocian la conexión inicial se intercambian paquetes del tipo *Configure Request* con diversas alternativas de opciones hasta que se recibe una respuesta *Configure Ack*. En una fase posterior se realiza la autentificación **PAP** (*Protocol Authentication Protocol*). En el protocolo PPP es posible la compresión del encabezado de TCP/IP con el objetivo de reducir la cantidad de bytes e incrementar la eficiencia de transporte de datos. Por encima de LCP y debajo de IP se utiliza el protocolo **NCP** (*Network Control Protocol*) para la configuración inicial del enlace.

2.3- CABLE-MODEM.

Este sistema permite el acceso de alta velocidad digital para servicios de Internet por el mismo cable coaxial de la red CATV. Trabaja con el criterio FDMA donde la señal digital se integra a un espectro compartido con la TV. Las señales de entrada y salida al usuario ocupan distintas bandas de frecuencia. En este caso en acceso se realiza mediante celdas ATM y con detección de colisión similar a Ethernet (CDMA/CD).

Se han ensayado sin embargo, otras formas de acceso como ser CDMA. Como referencia en la **Tabla 05** se entregan las características tomadas del sistema de cable-modem ComUNITY usado en Buenos Aires.

Tabla 05. Características más importantes del CableModem.

Dirección de la señal	**DownStream**	**Upstream**
Rango de frecuencia de operación	300-800 MHz o 88-450 MHz	5-40 MHz
Resolución	250 kHz	50 kHz
Ancho de banda del canal	6 MHz	1,8 MHz
Modulación	64QAM	QPSK
Velocidad digital	30,336 Mb/s	2,56 Mb/s
Nivel de red de transporte	ATM AAL5. Acceso MAC/SNAP	Ethernet (802.2/3).
Corrección de error	Viterbi+Reed-Solomon	Reed-Solomon

1205

SERVICIOS SOBRE LA INTERNET

Acerca de los servicios disponibles mediante la red Internet. Referido al servicio de e-mail; los servidores de web; la transferencia de archivos, los directorios, etc.

1- INTRODUCCION A INTERNET

La primer red fue desarrollada desde 1965 en el MIT para **ARPA** (*Advanced Research Projects Agency*). Se denominaba red **Arpanet** (precursor de la actual Internet). Desde 1972 se denominó **DARPA** (*Defence ARPA*). En 1983 se formaliza la red Internet al separarse de la órbita militar (red **Milnet**) y disponer de standard propios. Para Internet se generan sucesivamente los siguientes organismos de normas: **ICCB** (*Internet Configuration Control Board*) entre 1981-84, **IAB** (*Internet Activities Board*) desde 1984 y **IETP** (*Internet Engineering Task Force*) junto con **IRTF** (*Internet Research Task Force*) desde 1989.

Las anteriormente conocidas como normas **MIL-STD** (*Militar Standard*) y las actuales **RFC** (*Request For Comments*) determinan los protocolos para la interconexión de redes Internet. MIL pertenece al Departamento de Defensa y RFC son las normas de la **IETF** para el protocolo oficial de Internet. Los estándar RFC son normas preparadas para la red Internet en forma de artículos. Las normas RFC se distribuyen mediante mail electrónico en formato texto (.txt) y su actualización es mucho más veloz que las normas ISO. Por otro lado, el incremento de servicios Internet en la década de `90 ha retardado (e impedido para siempre) la conversión desde TCP/IP hacia ISO. La red **Internet** disponía de más 5 millones de host conectados en 1995 impulsado por el servicio de Web.

La **Fig 01** anexa muestra la Figura 2 del standard RFC-0793 referido al protocolo TCP de 1981. Obsérvese ya la presencia del protocolo RTP para servicio de voz sobre IP. La tecnología lo hizo posible 15 años después. En la **Fig 02** se presenta un esquema de protocolos relacionados. Entre ellos se encuentran los que se analizan en este capítulo: acceso a Internet mediante enlaces de tipo dial-up mediante la red telefónica pública y las aplicaciones sobre TCP y UDP.

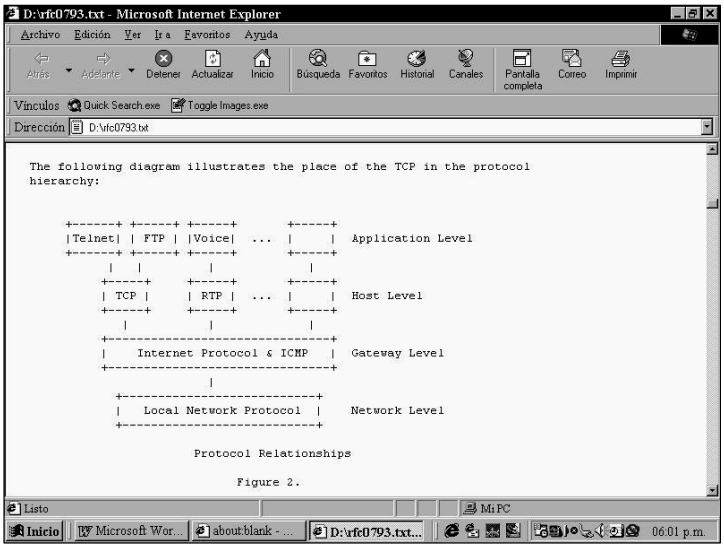


Fig 01. Se muestra la figura 2 del standard RFC-0793 del IETF.

SERVICIOS SOBRE LA INTERNET

La red Internet está formada por los siguientes operadores:

Tabla 01. Operadores de la red Internet.

-**ISP**	(*Internet Service Provider*). Se trata de las empresas que admiten el acceso de usuarios a un router de entrada a cambio de un valor económico mensual. Normalmente el acceso es dial-up mediante la red telefónica.
-**POP**	(*Point of Presence*). Se define así a los router de acceso a la red del ISP que se colocan en distintos lugares del país para dar cobertura a usuarios mediante acceso dial-up más cercano.
-**NAP**	(*Network Access Point*). Es el punto de interconexión entre distintos ISP.
-**NSP**	(*Network Service Provider*). Es el proveedor de conexiones para los distintos ISP y NAP.

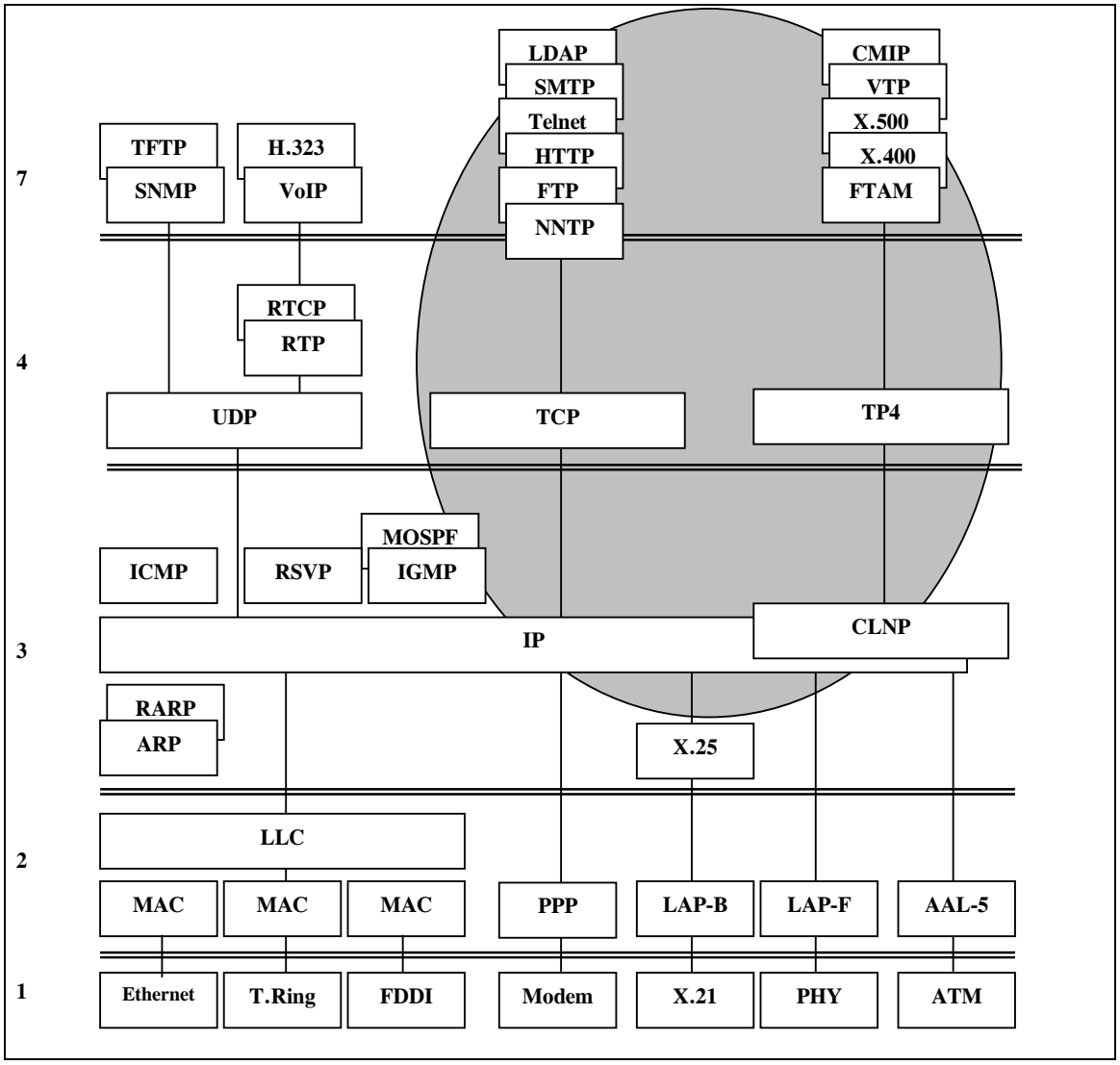


Fig 02. Protocolos de servicios de aplicación en Internet.

2- PROTOCOLOS DE APLICACION

Los protocolos **TCP/IP** nacieron con la red Internet pero se usan también fuera de ella. TCP/IP se ha implementado en el sistema operativo **UNIX**, pero no solo en UNIX. La red **Internet** es una red de computadoras que permite una variedad de funciones y que utiliza el protocolo TCP/IP y el sistema UNIX, pero no exclusivamente. Ha continuación se analizan las capas de procesos (equivalente a la capa 7 del modelo ISO) y se determinan los servicios ofrecidos al usuario de la red. Se trata de una suite de protocolos asociados al TCP/IP.

Este capítulo analiza solo las aplicaciones más utilizadas sobre la Internet. Aquellas aplicaciones que corresponden a redes corporativas soportadas en protocolo IP son analizadas en un capítulo por separado (por ejemplo, VoIP, H.323, VPN, VLAN). Por otro lado, el protocolo de management SNMP soportado sobre UDP/IP se analiza también en un capítulo independiente.

2.1- TRANSFERENCIA DE ARCHIVOS

FTP (*File Transfer Protocol*).
El standard se encuentra en RFC-0959. Mediante el sistema operativo permite la transferencia de archivos desde un sistema a otro. Esta fue la primer aplicación para conectar host en la red Arpanet. El protocolo es complejo, porque el problema también lo es: existen diferentes computadoras que deben conectarse entre sí (desde la PC *notebook* hasta *mainframe*). FTP se encuentra implementado para los sistemas operativos Unix, IBM-VM y MS-DOS. En MS-DOS la implementación de usuario incluye un *driver* y hardware para conexión X.25 y Ethernet. ***Archie*** es un directorio indexado de nombres de los archivos anónimos del tipo FTP.

Los comandos del protocolo FTP se clasifican en:
-Comandos de control de acceso: *name*, *password*, *logout*, *close* (termina la conexión), *bye* (cierra la conexión y se sale de FTP).
-Comandos de transferencia de parámetros: *get file* (transfiere un archivo desde el remoto al sistema local), *passive*, estructura de archivo, *cd dir* (se mueve un directorio hacia arriba en el sistema remoto).
-Comandos de servicio: *store*, *restart*, *rename* (redenomina archivos), *abort*, *delete* (borra el archivo en el sistema local), *remove*, *print* (sirve para administrar la impresora), *list*, *status* (entrega un status del FTP), *system*, *help* (ofrece un listado de comandos).

FTP Anonymous. Los servidores del FTP anónimo son una gran base de archivos ordenados por directorio. Para acceder a los mismos se selecciona *ftp://nombre del servidor*, el sistema responde requiriendo el *login* a lo cual se responde con la palabra *anonymous* y el *password* se indica la dirección de *e-mail*. Archie permite la búsqueda entre servidores de FTP.

FTAM (*File Transfer Access and Management*).
En el modelo ISO se dispone del protocolo de transferencia de archivos denominado FTAM. Trabaja sobre un entorno cliente-servidor y con características descriptas en la Serie X.400 del ITU-T. El protocolo FTAM es similar al FTP y **NFS** (*Network File System*). El FTAM es el protocolo estándar del ITU-T para aplicaciones en telecomunicaciones. Utiliza el concepto de almacén virtual de archivos y oculta las diferencias entre sistemas de distintos fabricantes. Entre las funciones que cumple se encuentran la transferencia, eliminación y recuperación de archivos desde un server-FTAM. Actúa sobre directorios FTAM y lee los atributos de los archivos.

NFS (*Network File System*).
Es también conocido como **ONC** (*Open Network Computing*) y es original de **Sun Microsystems Inc** en 1984. Es un sistema de operación de red que permite la conexión transparente entre computadoras en una red. Se trata de la más simple interfaz transparente de datos. En esencia el NFS provee una conexión de tipo memoria de disco virtual. Extiende el sistema operativo UNIX a otras PC y entrega servicios similares a Novell Netware, por ejemplo. El NFS trabaja en la mayoría de las PC y redes instaladas por lo que es el más familiar y simple de los sistemas.

El modelo de capa incluye 3 capas superiores:
-**NFS,** es el nivel de aplicación para transferencia de archivos, acceso y gestión;
-**XDR** (*eXternal Data Representation*), representa los datos de máquinas con distintas arquitecturas de procesadores CPU y permite el funcionamiento cliente/servidor y por último
-**RPC** (*Remote Procedure Call*), define el formato del mensaje usado en el proceso de llamada remota. Estos protocolos se encuentran sobre UDP/IP/IEEE802.3.

2.2- CORREO ELECTRONICO

SMTP (*Simple Mail Transfer Protocol*).
Se trata del correo electrónico definido en RFC-0821. Este protocolo es similar al **MHS** (*Message Handling System*) de Novell y a la serie **X.400** del ITU-T. Desde el punto de vista del modelo de capas SMTP opera sobre TCP para disponer del servicio de control de errores y retransmisión. El protocolo **IRC** (*Internet Relay Chat*) es un software que hace posible conversaciones en tiempo-real y simultáneas basadas en un server que actúa de centro de los clientes. Fue creado en 1988 en Finlandia y se describe en RFC-1459.

En SMTP cada usuario con acceso al sistema dispone de un *mailbox* que se sitúa en un *Server*, de forma que pueden intercambiarse mensajes aún en ausencia del corresponsal. La especificación del *Mailbox* del usuario se realiza como una dirección con la estructura: usuario@dominio. Por ejemplo se puede obtener la dirección del autor: rares@teleinfo.com.ar (Roberto Ares "en" Teleinfo, una entidad comercial en argentina).

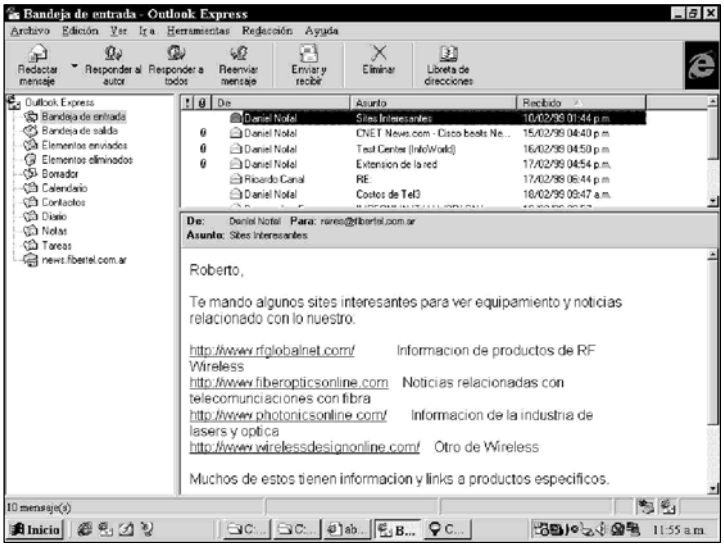


Fig 03. Ejemplo de pantalla de e-mail.

DNS (*Domain Name System*).
Este sistema permite organizar la información de routing entre una denominación (seudónimo o alias) simple y el número de dirección IP verdadero. El nombre completo tiene como máximo 63 caracteres. De ellos 3 caracteres indican el domino (edu-educación, com-comercial, gov-gubernamental, org-organización, mil-militar, etc) y 2 el país (ar-Argentina, it-Italia, etc). En USA no se coloca la sigla .us y en Europa no se utiliza el dominio (solo el país).

La tabla de dominios guardada en el servidor se denomina *DNS Cache*. Por ejemplo, cuando un usuario de Internet selecciona un dominio (dirección DNS) de e-mail (rares@teleinfo.com.ar) o de la dirección de web (www.teleinfo.com.ar) el servidor realiza un chequeo de la base de datos para encontrar que esta dirección DNS es un seudónimo de la dirección IP (ejemplo 192.168.1.4). La dirección IP se envía hacia atrás para asegurar un mensaje que pueda ser reconocido en la red. Existen servidores que permiten reconocer la dirección DNS y reporta la IP correspondiente.

COMANDOS DE SMTP. Este protocolo establece una conexión desbalanceada entre emisor y receptor donde cada uno dispone de una *port* distinta en TCP. Los datos se codifican en ASCII (7 bits) y se transmite en caracteres de 1 byte (el octavo bit en cero). Los comandos que se intercambian entre el emisor y receptor del mensaje SMTP son descriptos en la **Tabla 02**.

Tabla 02. Comandos definidos en el protocolo SMTP.

-Hello	Comando usado para identificar el emisor al receptor. Contiene el nombre del host. Se responde con OK.
-Mail	Comando para iniciar la transacción al *mailbox*.
-Recipient	Comando que se utiliza para identificar un recipiente RCPT de datos de mail.
-Data	Este comando sirve para la transferencia de 128 caracteres de código. Se confirma con OK.
-Send	Se utiliza para iniciar la transacción de datos.
-Reset	Se utiliza para informar que la conexión ha sido abortada. Todos los buffer se borran.
-Quit	Este comando especifica que el receptor debe enviar un OK y cerrar el canal de transmisión.

Por ejemplo, un e-mail es emitido desde el usuario roberto ubicado en el host denominado alpha.com.ar hacia el usuario ángel ubicado en el host beta.com.ar. Los comandos intercambiados son:

```
Send:     MAIL from: <roberto@alpha.com.ar>
Resp:     250 ok
Send:     RCPT to: <angel@beta.com.ar>
Resp:     250 ok
Send:     DATA
Resp:     354 start mail input
Send:     blah, blah, blah, ...
Send:     <CRLF>
Resp:     250 ok
```

X.400 (**ISO-10021**).
Los protocolos X.400 pertenecen al ITU-T y se encuentra como estándar desde 1984 con el nombre **MOTIS** (*Message Oriented Text Interchange System*). La integración entre los distintos tipos de E-mail se efectúa mediante el protocolo **API** (*Application Program Interface*). X.400 ha tenido cierto auge en Europa a mediados de los años `90 pero no ha tenido un desarrollo sustancial como SMTP.

Se basa en un modelo cliente-servidor distribuido que incluye los siguientes componentes:
-Agente de usuario UA: para permitir el trabajo en el computador cliente. Permite generar y leer mensajes.
-Agente de transferencia de mensaje MTA: permite la memorización y el enrutamiento hacia otros MTA.
-Memoria de mensajes MS: para guardar los mensajes hasta la consulta.
-Unidad de acceso AU: permite el acceso de otras entidades como facsímil y teletex.
-Sistema de directorio DS: para obtener la dirección y nombre de usuarios según ITU-T Serie **X.500**.

2.3- TERMINAL VIRTUAL

TELNET (*Remote Login*).
Permite el acceso remoto a un terminal conectado a la red Internet mediante RFC-0854. El protocolo equivalente para el modelo de ISO es el **VTP** (*Virtual Terminal Protocol*). Se trata de crear un **Terminal Virtual** (concepto original de 1972 sobre Arpanet) para el teclado e impresora. De esta forma se puede acceder a la computadora deseada desde cualquier lugar del mundo. Cuando un terminal inicia la conexión asume que el funcionamiento es el básico (teclado, impresora y protocolo ASCII).

Los comandos más comunes usados en Telnet son los siguientes: *close* (cierra la conexión), *open host port* (abre la conexión utilizando un puerto opcional), *quit* (sale de telnet), *status* (da un estado de la información de telnet), *type character* (ingresa carácter por carácter en el remoto), *type line* (entre línea por línea), *?* (sumariza los comandos de telnet).

2.4- DOCUMENTOS CON HIPERTEXTO

WWW (*World Wide Web*).
Se inicia en **CERN**-1989 en Ginebra para implementar la idea de **hipertexto** en la actividad científica mediante la Internet. Web se popularizó a partir de 1993 cuando la Universidad de Illinois generó el programa gratuito **Mosaic**, con formato windows accesible a cualquier usuario. Para 1995 el número de programas "inspectores de Web" superaba la docena y el **NetScape Navigator** era usado por el 75% de los usuarios de Internet. En Windows 95 y 98 el programa **Explorer** es un software standard. En 1995 el crecimiento de servidores de Web era del 100% cada 53 días.

Las principales características del Web son las siguientes. En WWW se desarrolla el protocolo de hipertexto; por hipertexto se entienden enlaces entre datos, similar a una enciclopedia. Con la selección (pulsando 2 veces) de palabras y textos resaltados se accede a una otra página adicional. El salto entre páginas es independiente al lugar de almacenamiento (un server o varios en todo el mundo). Este proceso se denomina "navegación" (*Browsing, Cruising o Surfing*) en el ciberespacio [1]).

No existe una RFC para el Web. Se trata de diferentes mecanismos: URL, HTTP, HTML, CGI y Cookies. Se indican varios detalles de los mismos a continuación.

---

[1]) El término *Cyberspace* fue introducido por William Gibson en la novela fantástica denominada "*neuromancer*" para describir el mundo de los ordenadores y la sociedad cercana.

-URL (*Uniform Resource Locators*). Obtenible desde RFC-1630. El URL es una forma de identificador de reservas en los servidores web. Un URL puede administrar a varios servidores de web desde un punto al que se dirige el usuario.

-HTTP (*Hypertext Transfer Protocol*). Obtenible desde RFC-2068. Se trata de una arquitectura cliente-servidor, donde el cliente utiliza un visualizador (*Browser Web*). El servidor de Web es uno o más servers que entregan texto, gráficos, imagen y sonido. Se utiliza el protocolo de hipertexto HTTP por ello la forma de identificación de un servidor de web inicia con el formato (*http://www*). El servidor se denomina *"HTTP server"* en el ambiente Windows NT o *"HTTP Daemon"* en el Unix. Las direcciones de los server de Web tienen el formato http://www.nombre.código que incluye la apertura, el nombre de empresa y el identificador de cierre (por ejemplo .com.ar para indicar una empresa comercial en Argentina).

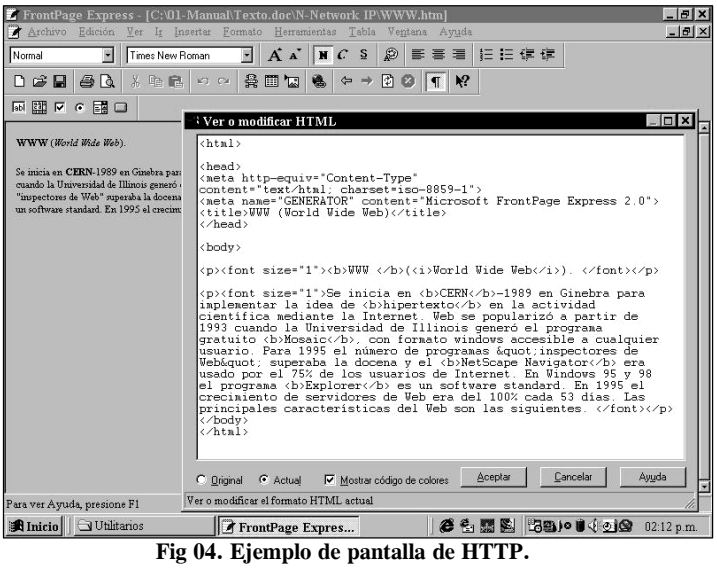


Fig 04. Ejemplo de pantalla de HTTP.

-HTML (*Hypertext Markup Language*). Los enlaces de hipertexto se crean mediante el lenguaje HTML (RFC-1866). Es una variante de **SGML** (*Standard Generalized Markup Language*) de ISO-8879 del año 1986. Se lo utiliza para escribir los *Web-Server*. En la fotografía anexa se muestra la pantalla de un programa de escritura en HTML (el texto en la primer frase de este ítem y el programa se denomina *FrantPage Express*).

Fig 05. Ejemplo de pantalla de HTML.

-CGI (*Common Gateway Interface*). Esta interfaz define como se comunica el server de HTTP con el programa ejecutable mediante un browser.

-***Cookies*.** Se trata de información que el servidor del web memoriza en el cliente para ser utilizada en una próxima sesión. Puede ser usada para memorizar información de configuración o password de subscripción (acceso) al servidor. Esto produce un consumo de memoria y una intromisión que puede ser considerada inaceptable por el cliente. Algunos cookies son utilizados para tomar información del cliente y enviarlas al servidor. Los navegadores de Internet permiten configurar la aceptación de cookies en el cliente.

2.5- DIRECTORIOS

En este caso el servicio de directorio nace dentro de las normas ISO/ITU (Serie **X.500** del ITU-T); su formato es demasiado complejo y se adapta para la comunidad de Internet en el servicio **LDAP**. Un directorio es una base de datos especial con información de varias reservas disponibles en la red. Se forma una base de datos del directorio **DIB** (*Directory Information Base*) donde los objetos del DIB se estructuran como un árbol (similar al directorio de archivos en el administrador de archivos de Window). Son objetos los usuarios y los recursos (impresoras, memorias). Cada usuario dispone de una ventana con toda la información (localización, direcciones de teléfono, facsímil, E-mail, etc.).

Se define una arquitectura del tipo cliente-servidor. Un directorio es una base de datos muy especial ya que no está estructurada para una actualización (escritura) permanente sino para consultas (lectura) periódicas. Por ello es más rápido en lectura que en escritura; es apto para soportar información estática.

X.500 (**ISO-9594**).
Es conocido también como **DS** (*Directory Services*) e iniciada en 1988 con actualización en 1993. El objetivo es generar un directorio global donde la información contenida en cada servidor es parte de la información de todos los servidores de este servicio. En X.500 se describen:
-La jerarquía de nombres (referencias organizacionales);
-El modelo de información (formato y estructura de los datos);
-El modelo funcional (protocolo de acceso al directorio);
-El modelo de autentificación (protección de datos para accesos de escritura no autorizados) y
-El modelo de operación distribuida (para mantener información distribuida en forma global).

Se trata de una solución compleja e implementada por muy pocos software. Requiere de reservas intensivas en la PC cliente. Por estar desarrollado sobre los protocolos ISO es de difícil implementación en TCP/IP. Una versión simplificada de X.500 para Internet se encuentra en el protocolo LDAP.

LDAP (*Lightweight Directory Access Protocol*).
Nace originalmente en la Universidad de Michigan como una versión simple de X.500. Es un standard de 3 versiones (RFC-1487 del año 1993; RFC-1777 del año 1995 y RFC-2251 en la versión 3 del año 1997). Se trata del servicio de directorio de fácil implementación en el cliente, manteniendo las funciones definidas en X.500. Mediante el servicio de directorio LDAP es posible generar bases de datos para autentificación de clientes en la red.

2.6- CONSULTA DE BASE DE DATOS

WAIS (*Wide Area Information Service*).
Permite la selección mediante el uso de "palabras clave" de textos útiles dentro de una colección de datos. Funciona como índice de textos. Son variantes del servicio de directorio. Los más conocidos son Yahoo y Altavista pero se encuentra una amplia variedad de buscadores especializados.

GOPHER.
Es el nombre de la mascota de la Universidad de Minnesota. Es un protocolo cliente-servidor para acceder a un host donde se encuentra una base de datos estructurada en forma de árbol. Entrega un índice de documentos de texto que permite "navegar" entre varios servidores de Gopher. Se entiende como una aplicación sin mayor éxito. Un ejemplo de dirección de acceso es *<gopher://lucano.uco.es>*.

ARCHIE/VERONICA.
Son sistemas que permiten localizar archivos. En el caso de Archie, un file memorizado en los server de FTP y, en el caso de Verónica, un file en el servidor de Gopher (es una opción del menú de Gopher para hacer una búsqueda en otros). Son aplicaciones con reducido éxito.

2.7- GRUPOS DE NOTICIAS

USENET (*User Network*).

Se fundamenta en el protocolo **NNTP** (*NetNews Transport Protocol*). Es original de 1979 (RFC-0977) y corresponde a una colección de grupos de discusión sobre los más variados temas (la subscripción al grupo asegura recibir toda las novedades intercambiadas). Ya en 1995 eran más de 5000 los grupos formados. Por ejemplo, el grupo de noticias "comp.security.unix" permite acceder a novedades en lo referente a seguridad en redes IP.

Existe una cierta jerarquía en las denominaciones de los grupos que forman las siguientes categorías: *comp*. (para computadoras y redes), *news*. (discusión sobre la misma Usenet), *talk*. (para distintos tipos de charlas), *soc*. (para sociales y culturales), *alt*. (para temas alternativos de diversos tipos). Las direcciones se encuentran mediante la sintaxis *<news://alt.cad.autocad>* que corresponde al grupo de discusión sobre autocad.

2.8- SERVICIOS EN REDES IP

Una amplia gama adicional de servicios pueden ser ofrecidos sobre redes IP. Estas redes tienen conexión hacia la Internet y trabajan con los mismos protocolos pero se encuentran protegidas para incrementar la seguridad (**IPsec**). Los servicios ofrecidos requieren además de la seguridad, asegurarse una apropiada calidad de servicio (retardo, latencia y jitter). Se encuentran entonces protocolos para servicios en tiempo-real (RTP y RTCP) y de reservación de ancho de banda (RSVP). Una interesante aplicación en redes IP es la posibilidad de acceso a usuarios mediante la formación de grupos multicast. Para ello se han previsto protocolos de gestión de grupos (IGMP) y de routing para la red. Estos servicios son analizados en un capítulo aparte.

VoIP (*Voice over IP*). Los servicios en redes IP incluyen todos aquellos que corresponden a la Internet, más otros de reciente implementación. Por ejemplo, se trata de la transmisión de voz **VoIP** en redes de paquetes. Utilizan como soporte cualquier medio basado en routers y los protocolos de transporte UDP/IP.

FoIP (*Fax over IP*). Se trata de la emisión de facsímil mediante protocolos IP en tiempo real (ITU-T **T.38**) o en formato *Store-and-Forward* (**T.37**). Ambas normas datan del año 1998 y el T.38 es el adoptado en H.323 para multimedia en LAN (también aplicado a VoIP).

ITU-T H.323. Esta tecnología permite la transmisión en tiempo real de vídeo y audio por una red de paquetes. Es de suma importancia ya que los primeros servicios de voz sobre protocolo Internet (**VoIP**) utilizan esta norma. En la versión 1 del protocolo H.323v1 del año 1996 se disponía de un servicio con calidad de servicio (**QoS**) no garantizada sobre redes LAN. En la versión 2 del año 1988 se definió la aplicación VoIP. Una versión 3 posterior incluye el servicio de fax sobre IP (**FoIP**) y conexiones rápidas entre otros.

VPN (*Virtual Private Network*). Una VPN es una conexión que simula las ventajas de un enlace dedicado (*leased*) pero ocurre sobre una red compartida (acceso remoto sobre una estructura pública con todas las ventajas de un enlace privado). Diversas redes (Frame relay y ATM) permiten formar redes VPN; sin embargo la posibilidad de realizarlos mediante redes IP tiene algunas ventajas. Por ejemplo, la posibilidad de accesos remotos mediante líneas dial-up, la posibilidad de realizar conexiones VPN esporádicamente y entre varios puntos (normalmente los VPN mediante Frame Relay y ATM son canales permanentes PVC).

VLAN (*Virtual LAN*). Existen diversas definiciones de VLAN. Se puede interpretar como un grupo de estaciones de trabajo que no se encuentran en la misma localización física y que se conectan mediante un switch IP. También se dice que una VLAN es un grupo de nodos que residen en un dominio de broadcast común sin saltos de router. Se puede entender como una red conmutada que está segmentada lógicamente por función o aplicación. En todos los casos VLAN se forma mediante switch agrupando ciertos usuarios sobre la base de alguna razón en común. Las redes LAN obtenidas son virtuales porque se obtienen mediante agrupaciones lógicas en el *Switching Fabric*.

1206

DOMINIOS Y DIRECCIONES EN REDES IP

Referido a la administración de dominios y direcciones IP; a la asignación dinámica y al manejo de los sockets.

1- DIRECCIONES IP

1.1- CLASES DE DIRECCIONES IP

Dentro de una red IP las direcciones son gestionadas tanto por el **IANA** (*Internet Assigned Numbers Authority*) que asigna las direcciones públicas, como por el usuario que maneja las direcciones en el interior de su red. La dirección IP ocupa 32 bits (4 Bytes) que permite identificar la red y el host individual. El formato de las direcciones puede ser de 5 tipos de acuerdo con la Clase que se indica en la **Tabla 01**.

Tabla 01. Clases de direcciones IP (IP-Address).

Clase A.	0+7bit+24bit. Corresponde a un número de dirección de Network (7 bit asignados por IANA) y otro número para el Host (24 asignados por el administrador de la red). Aplicable solo para grandes redes. El IAB solo puede designar 128 (2^7) redes de este tamaño. Numera desde 0.0.0.0 hasta 127.255.255.255. Sin embargo, ante la falta de direcciones IPv4 se ha decidido particionar la clase A para asignarlas a varios usuarios. Por ejemplo, La dirección de HP de Argentina es del tipo 15.59.x.y. En tanto que, la dirección MAC de HP es 08-00-09 (la dirección MAC de Siemens es en cambio: 08-00-06).
Clase B.	10+14bit+16bit. Aplicable a redes medianas y numera desde 128.0.0.0 hasta 191.255.255.255. Por ejemplo, la empresa Telefónica de Argentina tiene asignado un número de este tipo de red: 168.226.x.x (los dos bytes finales son asignados por el operador de la red).
Clase C.	110+21bit+8bit. Para pequeñas redes. Se trata de 4 Bytes: los 3 primeros Bytes indican la dirección de red y el último Byte numera el Host dentro del nodo. Un router de red IP se identifica mediante los 3 primeros Bytes y sus puertas con el Byte final. En esta configuración el primer valor válido es 192.0.0.0 y el último es 223.255.255.255.
Clase D.	1110+28 bits. Ocupa la numeración 224.0.0.0 hasta 239.255.255.255. Es utilizada para direcciones *multicast* (grupo de usuarios de servicios IP).
Clase E.	11110+27 bits. Ocupa desde 240.0.0.0 hasta 247.255.255.255. Este set de direcciones se encuentra sin aplicación. La dirección 255.255.255.255 es una dirección de *broadcast*.

IP

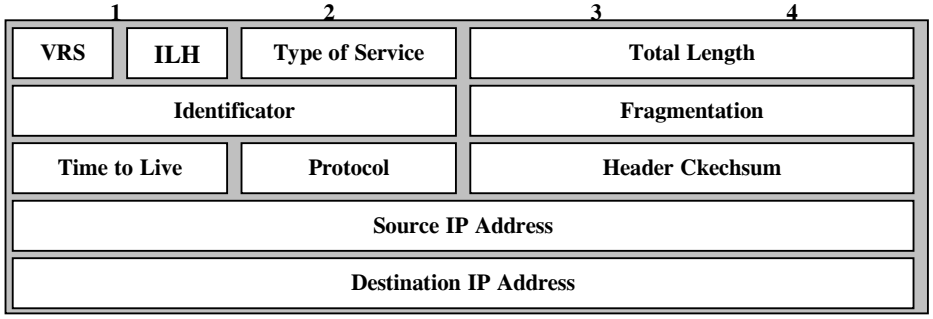


Fig 01.Campos del protocolo IP.

La dirección IP puede escribirse mediante la notación decimal punteada *Dotted* (44.123.230.224) que esta es la preferida por su simplicidad. También se han usado la notación hexadecimal (2C.7B.E6.E0), la notación estilo C de Unix (Cx2C7BE6E0) y la notación binaria (00101100.01111101.11100110.11100000).

CLASE D (*Multicast*). El IANA ha reservado la clase D de direcciones IP para grupos multicast. Esta clase de direcciones consiste en la secuencia 1110 y 28 bits de dirección (5 bits no usados y 23 de dirección). Expresado en la notación normal se trata desde 224.0.0.0 hasta 239.255.255.255. Algunas direcciones se encuentran reservadas y no pueden ser utilizadas.

En las direcciones MAC se ha reservado el prefijo 01-00-5E (hexadecimal) para direcciones IP multicast. De esta forma casi todos los últimos 3 Bytes de IP y MAC son idénticos. Por ejemplo, la dirección IP: 224.10.8.5 corresponde a la dirección MAC: 01005E0A0805. En la siguiente secuencia, los bits en negrita no son usados y separan la zona de identificación multicast (anterior) de la dirección propiamente dicha de usuario (posterior).

IP Address			224=1110 **0000**	10=**0**000 1010	8=0000 1000	5=0000 0101
MAC Address	0.1=0000 0001	0.0=0000 0000	5.E=0101 **1110**	0.A=**0**000 1010	0.8=0000 1000	0.5=0000 0101

MASK NET. La dirección IP contiene 4 sectores; el sector que define al host está determinado por la máscara de subnetwork. Los componentes son los siguientes:
-***Prefijo*** desde 1 a 5 bits para identificación del tipo de Clase (A a E). Así la secuencia 110 determina la clase C.
-***Network*** (de 7, 14 o 21 bits para las clases A a C); entonces la secuencia 110 inicial determina que la dirección de red es de 21 bits.
-***Sub-network***. Se trata de la diferencia con la dirección de host.
-***Host***. Para conocer la secuencia que identifica al host es necesario leer la máscara de red (*mask net*). Esta máscara identifica los bits que determinan el host y por ello, la subnetwork.

Estos dos últimos campos ocupan en total los 24, 16 o 8 bits que completan la dirección. Para poder distinguir entre la identificación de subnetwork y host se requiere una filtro de direcciones denominado *Mask Net*. Por ejemplo, para una dirección clase C (inicio 110) se tiene el formato (x para Network; y para Subnetwork; z para el Host) de la **Tabla 02**. Una dirección por el estilo se debe expresar como W.X.Y.Z/27; donde el /27 se refiere a la cantidad de unos en la máscara de red utilizada.

Tabla 02. Ejemplo de máscara de red.

	Byte 1	Byte 2	Byte 3	Byte 4	Decimal
Dirección IP	110x.xxxx	xxxx.xxxx	xxxx.xxxx	yyyz.zzzz	(192…) a (223…)
Mask Net	1111.1111	1111.1111	1111.1111	1110.0000	(255.255.255.224)

1.2- DIRECCIONES SIN CLASES

El crecimiento de las direcciones IP ocupadas ha obligado a dos tipos de soluciones: el VLSM y CIDR a corto plazo sobre el protocolo IP versión 4 y la ampliación del campo de direcciones en IP versión 6.

VLSM (*Variable Length Subnet Mask*).
En RFC-1009 se autoriza la construcción de redes donde la longitud de la máscara es variable dentro de la red. La limitación de utilizar siempre la misma máscara de subred es que se está limitado a un número fijo de direcciones de subred. Conceptualmente una red es dividida en subredes, cada subred es dividida en subredes y así sucesivamente. Esto puede reducir sustancialmente las tablas de ruta de los routers. El protocolo de routing OSPF soporta VLSM; el algoritmo que lo permite se denomina "*longest match*".

Ejemplo.
-El proceso se inicia sobre la red **140.25**.0.0/16 (binario: **10001100-00011001**-00000000-00000000) que permite los últimos 16 bits para direcciones de subred VLSM. En negritas se indican los bits fijos para la red; subrayado se indican los bits relacionados con /16.
-Se divide en subredes del tipo 140.25.0.0/20. Es decir que se han creado 16 subredes (4 bits).
-Se selecciona en el ejemplo la subred 140.25.**224**.0/20 (10001100-00011001-**1110**0000-0000000).
-Se la divide en subredes del tipo 140.25.224.0/24. Es decir se han creado 16 subredes (4 bits).
-Se selecciona en el ejemplo la subred 140.25.**238**.0/24 con la secuencia (10001100-00011001-1110**1110**-00000000).
-Se divide en subredes del tipo 140.25.238.0/27. Es decir se han creado 8 subredes (3 bits).
-Se selecciona en el ejemplo la subred 140.25.238.**64**/27 (10001100-00011001-11101110-**101**00000).
-Esta subred dispone de 30 direcciones de host (desde 140.25.238.66/27 a 140.25.238.94/27). La dirección inicial (140.25.238.65/27) se reserva para indicar la subred completa y la final (140.25.238.95/27) para broadcasting. Por ejemplo, la dirección de broadcasting en esta subred es (10001100-00011001-11101110-101**11111**).

CIDR (*Classless Inter-Domain Routing*).
En el año 1992 el IETF decide subdividir las direcciones clase A debido a que las direcciones clase C se encuentra casi exhausta. Por ejemplo, para el año 1992 se habían asignado 46 de las 126 direcciones clase A y 5467 de la 16382 de clase B. Para el año siguiente estos valores eran de 52 y 7133 respectivamente. En RFC-1519 del año 1993 se instruye el CIDR

que elimina la división entre clase lo cual equivale en esencia a VLSM. Con posterioridad el crecimiento de direcciones fue incrementándose. De 130 web en junio de 1993 se pasó a 646.162 en enero de 1997.

2- ASIGNACION DE DIRECCIONES IP

2.1- DOMINIOS

La gestión de direcciones IP requiere de una serie de elementos interrelacionados: el servidor DNS permite asociar un nombre de usuario con la dirección IP; el servidor/router NAT permite asignar direcciones IP no-públicas en el interior de una red privada; el servidor DHCP permite asignar direcciones IP en forma dinámica a usuarios intermitentes y el *Dynamic DNS* permite actualizar el servidor de DNS cuando se asigna la dirección mediante DHCP. A continuación los detalles de estos elementos.

DNS (*Domain Name System*).
Este sistema permite organizar la información de routing entre una denominación (seudónimo) simple de recordar y el número de dirección IP verdadero (se denomina resolución de nombre). Hasta 1980 un solo computador (llamado Host.txt en California) realizaba esta función, pero el tráfico hacia la misma se tornó inmanejable. Entonces se introdujo un sistema distribuido. El nombre completo tiene como máximo 63 caracteres. De ellos 3 caracteres indican el domino (edu-educación, com-comercial, gov-gubernamental, org-organización, mil-militar, etc) y 2 el país (ar-Argentina, it-Italia, etc). La tabla de dominios memorizada en el servidor se denomina *DNS Cache*.

Por ejemplo, cuando un usuario de Internet selecciona un dominio (dirección DNS) de e-mail (rares@nss.com.ar) o de la dirección de web (www.nss.com.ar) el servidor realiza un chequeo de la base de datos para encontrar que esta dirección DNS es un seudónimo de la dirección IP (ejemplo 192.168.1.4). La dirección IP se envía hacia atrás para asegurar que el mensaje pueda ser reconocido en la red. Existen servidores que permiten reconocer la dirección DNS y reporta la IP correspondiente.

DNS opera sobre UDP por lo cual no existe una conexión propiamente dicha; solo sirve para resolver la relación entre dominio en formato de texto y la dirección IP asignada. Con posterioridad, la conexión es establecida sobre TCP hacia el servidor (por ejemplo de web).

Existe también la resolución inversa. Si se conoce solo la dirección IP (por ejemplo 192.168.1.0) mediante el comando inverso (1.1.168.192.in-addr.arpa) se obtiene el seudónimo.

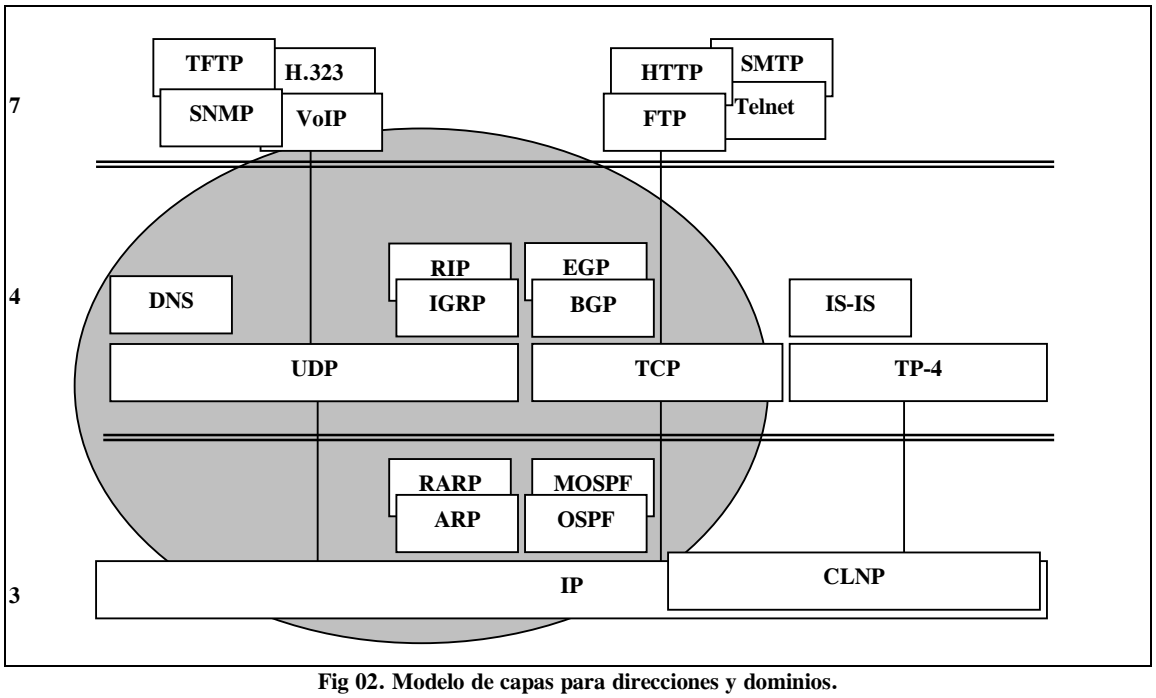


Fig 02. Modelo de capas para direcciones y dominios.

NAT (*Network Address Translation*).
El problema más complejo de Internet es el reducido número de direcciones. La solución a largo plazo el IPv6 con un mayor número de bytes por dirección. La solución instrumentada sobre IPv4 son dos: el **CIDR** (*Classless InterDomain Routing*) y el **NAT**. El proceso NAT propone reducir el número de direcciones IP mediante el re-uso de direcciones

privadas en todas las redes. De esta forma una red privada utiliza un direccionamiento propio y el router en el borde (*Stub Router*) de la red realiza la función de traducción y direccionamiento hacia la red pública (llamadas dirección local y dirección global).

El uso de NAT en el router de borde requiere el manipuleo de la información; por ejemplo, los checksum de IP y TCP cambian, además existen protocolos que llevan la dirección IP en el contenido (FTP lleva la dirección en código ASCII) y debe ser cambiada, etc. Esto introduce un retardo y un incremento de procesamiento pero a cambio se simplifica notablemente la gestión de direcciones. El funcionamiento de NAT puede ser estático o dinámico; en el estático el mapeo desde el conjunto de direcciones internas al conjunto externo se realiza manualmente. En el funcionamiento dinámico responde a diversas estrategias.

Una vez asignadas las direcciones privadas en el interior de la red, las mismas no cambian aun si se conectan a distintos ISP, con distintas direcciones públicas. Cuando NAT está implementado nunca el esquema de direcciones internas debe ser enviado al exterior pero lo contrario es deseable para que la Intranet tenga un conocimiento de la Internet.

El IANA determinó un set de direcciones para uso privado. Estas direcciones no son ruteadas por la Internet y se asignan para los componentes del interior. Como los router no distinguen las direcciones privadas se requiere el NAT para efectuar la traducción. Las direcciones reservadas por el IANA son las indicadas en la **Tabla 03.**

Tabla 03. Direcciones IP reservadas para aplicaciones en Intranet (NAT).

Clase	Desde	Hasta	Prefijo
A	10.0.0.0	10.255.255.255	10/8
B	172.16.0.0	172.16.255.255	172.16/12
C	192.168.0.0	192.168.255.255	192.168/16

NAT tiene la ventaja de conservar la legalidad de direcciones; es flexible para la conexión a nuevos ISP; impide el problema de superposición de direcciones IP debido al filtrado de direcciones privadas. Lamentablemente, el NAT reduce las opciones de seguridad debido a que tiene que intervenir sobre el paquete por lo que limita las posibilidades de la criptografía. Por otro lado se pierde la posibilidad de trazabilidad entre extremos y se incrementa el retardo por procesamiento de software.

2.2- ASIGNACION DINAMICA

DHCP (*Dynamic Host Configuration Protocol*).
Cuando un nuevo usuario se agrega a la red o se cambia de posición se requiere asignar una dirección IP y actualizar la base de datos del DNS. El protocolo DHCP fue diseñado por el IETF (standard en RFC-2131) para reducir los requerimientos de configuración. Además de asignar la dirección IP realiza una configuración automática de los parámetros necesarios para funcionar en la red donde se encuentra. DHCP trabaja sobre TCP y está basado en el protocolo **BOOTP** (*Bootstrap Protocol*) de RFC-0951, con algunas diferencias. El BOOTP permitía que clientes sin capacidad de memoria (disco rígido) pueda funcionar en TCP/IP.

Se utiliza un modelo *Client/Server* por lo que se dispone de uno o varios servidores DHCP. No se requiere de un servidor por subred por lo que el protocolo DHCP debe trabajar a través de routers. Más de un servidor pueden realizar las tareas de asignación de direcciones con el propósito de mejorar la eficiencia del sistema.

Las características generales de funcionamiento son las siguientes:
-El administrador de la red define en el servidor DHCP el set de direcciones IP que pueden ser asignadas. También se seleccionan los valores de los parámetros que deben ser seteados en el cliente.
-No requiere indicarse cuales de la direcciones IP están en uso; el protocolo RARP puede ayudar en esta función. Las direcciones IP que permanentemente se asignaban a la subred son distribuidas en forma dinámica entre los host. Otra forma es la asignación manual por parte del operador de la red con lo cual la asignación es permanente.
-Cuando un host se enciende realiza un pedido en forma broadcast a los servidores DHCP. El cliente puede seleccionar una de las respuestas (sin son varias) y enviar el requerimiento adicional de configuración. El server DHCP no fuerza los parámetros, es el host cliente el que solicita los parámetros configurables.
-El servidor asigna la dirección IP (y la mask de subred) por un tiempo determinado. El tiempo de asignación corresponde a un mensaje de 4 Bytes (*Timestamp*) en unidades de segundos; la secuencia FF.FF.FF.FF identifica a una asignación permanente sin límite de tiempo.
-En forma periódica el cliente debe renovar la solicitud de permanencia. Si no se renueva o el cliente efectúa un *shut-down* la dirección queda libre y será reciclada para se asignada a otro host.

Existen otros protocolos que se relacionan con la asignación dinámica de direcciones. El protocolo **RARP** permite descubrir cuales son las direcciones IP que han sido a signadas en la red. El protocolo **TFTP** provee un mecanismo de transporte de información desde el servidor de *Boot*. El **ICMP** provee información de host desde otros router mediante mensajes como el *redirect*.

DNS *UPDATE*.
Asociado a DHCP se encuentra el mecanismo *Dynamic DNS Update*. Permite la actualización automática del servidor DNS con el nombre y la dirección IP asignada en forma dinámica por el protocolo DHCP. Se refiere a RFC-2136 del año 1997. Este protocolo trabaja sobre TCP o UDP de acuerdo con el request. El formato del mensaje de actualización (*update*) contiene un encabezado de 12 Bytes que identifica al que efectúa el requerimiento y diversos campos

DHCP *FAILOVER*.
También en sociedad son DHCP se dispone de la técnica *DHCP Failover* que consiste en disponer de servidores duplicados funcionando como pares redundantes. Se dispone de un protocolo de comunicación simplificado para la operación en régimen normal, de interrupción de comunicación entre servidores y de falla del servidor asociado.

3- PORT y SOCKETS.

Mediante 2 Bytes se identifica la puerta (*Port*) de acceso al servicio origen en TCP/UDP. Se trata de direcciones TSAP que reservan la numeración desde 1 a 225 para los protocolos más conocidos (denominados *well-known*), como ser Echo:7, SMTP:25; FTP:21; Telnet:23; Gopher:70; y Web:80. El protocolo UDP identifica las aplicaciones SNMP:161; TFTP:69 y RPC-Sun:111. Desde la port 256 a 1023 se reserva para aplicaciones UNIX. Las aplicaciones propietarias llevan la dirección de port desde 1024 hasta 49151; las direcciones superiores a 40152 (hasta 2^{16}) se asignan en forma dinámica.

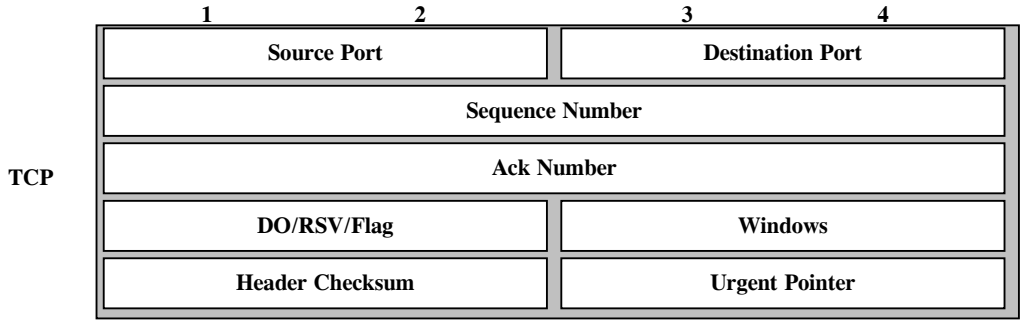


Fig 03. Protocolo TCP y Port de origen y destino.

La combinación de la dirección IP y la port TCP/UDP es conocida como ***Socket*** cuya asignación puede estar predeterminada (para protocolos conocidos) o se asigna entre los valores no utilizados (para las aplicaciones nuevas). Por ejemplo IP= 199.238.200.110 y port= 80 identifica al servidor de web identificado como *www.technologypreview.com*.

Un problema se genera cuando una misma máquina abre dos o más sesiones desde la misma aplicación (por ejemplo, varias ventanas de web simultáneas sobre la miasma máquina). Para eliminar esta discordancia en el socket se utiliza la numeración de port *well-known* solo en el servidor de web; en tanto que el cliente selecciona una port no asignada distinta para cada sesión. Por esta razón es que las direcciones IP y la port (el socket) es incluido en cada datagrama entre ambas máquinas. Solo los servicios que operan entre pares pueden usar la misma dirección socket en ambos extremos.

Para completar el concepto de NAT se dispone del **PAT** (*Port Address Transation*) consistende traducir una dirección de puerta interna hacia el exterior de la red. En este caso la transacción se realiza entre rangos de direcciones originales (convención BSD): 1…511; 512…1023; 1024…4999; 5000…65535. Esto permite crear varias conexiones desde el interior de la red hacia el exterior con pocas direcciones públicas.

1207

PROTOCOLOS DE ROUTING EN IP

Acerca de los algoritmos de routing, las métricas disponibles y el funcionamiento de los protocolos de resolución interior y exterior.

1- ROUTING BASICO.

1.1- GENERALIDADES DE ROUTING.

Se entiende por ***routing*** el proceso que permite la interconexión de redes. Se puede efectuar mediante Switch (capa 2 o 3) o Router de acuerdo con el tipo de redes involucradas. El Bridge o Switch se prefiere por el mínimo retardo; bajo costo; pocas conexiones y mínimo planeamiento. El bridge solo es posible para interconectar LAN. Mientras que Router se prefiere para protocolos aislados en cada segmento y flexibilidad futura; requiere configuración para interpretar la dirección IP de capa 3.

El Bridge, Switch y Router son elementos que "aprenden de la red". Como analizan la dirección de cada paquete pueden formar una tabla de direcciones. Cuando se conecta un nuevo terminal a la red LAN este envía un paquete indicando la activación con lo que puede integrarse a la tabla de direcciones. La dirección MAC es el número de hardware (grabado en EPROM) asignado por IEEE-ISO. El Router debe poseer un set de direcciones IP. Tiene la capacidad de enrutamiento para optimizar el camino del paquete de datos (analiza el costo; retardo de tránsito; congestión de red y distancia en número de Router en el trayecto). La tabla de ruta (*Routing Table*) contiene solo el "próximo paso" en la red[1]). Se han definido 2 tipos de protocolos para Router: el interior y el exterior al AS. Se denomina sistema autónomo **AS** (sistema interior o dominio) a un conjunto de sub-redes y Router que utilizan el mismo protocolo y el mismo control administrativo.

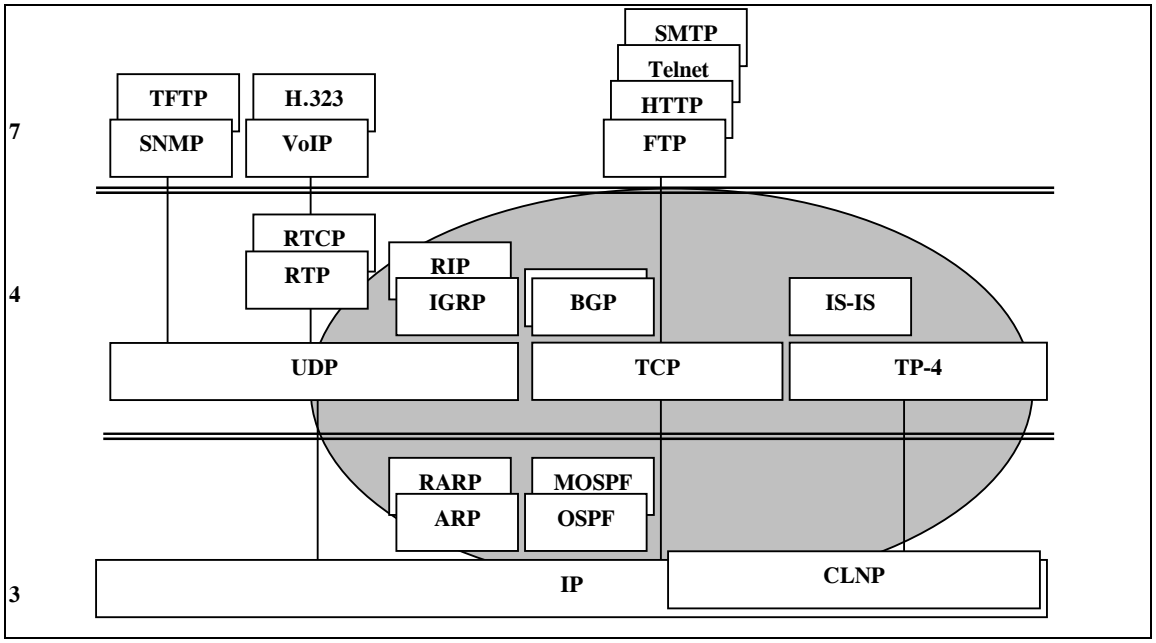


Fig 01. Modelo de capas para los protocolos de routing.

[1]) Los Router determinan un camino para el mensaje que sigue el principio de *Mínima Acción*. Los algoritmos para determinar esta mínima acción son diversos. En la teoría de la Relatividad fue **Einstein** quien, basado en la geometría no-euclideana de **G.Riemann**-1854, determinó que la luz se mueve en línea recta y es el propio espacio el que se curva en presencia de masas. De esta forma los rayos de luz determinan las líneas del mapa tetradimensional de la cartografía del espacio. Cada objeto en este mapa (el espacio-tiempo) sigue una línea de *mínima acción* (la geodésica) que no requiere energía. Los mensajes en una red de Routers sigue la geodésica (línea de mínima acción). La manzana de **Newton** cae del árbol porque sigue la línea geodésica, mantenerla en una posición requiere de un gasto de energía.

En la **Tabla 01** se resumen las características de los algoritmos de routing. En base a las mismas es posible obtener los protocolos de routing que son estudiados más adelante en este trabajo. Uno de los elementos más interesantes es la **métrica.** La métrica es un standard de medida que permite efectuar las operaciones de routing. Entre las métricas se encuentra por ejemplo, la longitud del trayecto en número de routers utilizado en RIP (el primer protocolo de routing).

La Tabla de Rutas es la responsable del enrutamiento del paquete en la red. Esta Tabla realiza un mapa de la topología de la red para determinar el próximo paso hacia el destino final. La métrica para una ruta particular es el agregado de varias características asignadas a un enlace. Existen diversos tipos de métricas; algunos protocolos de routing utilizan solo una de ellas mientras que otros usan varias alternativas. Algunas posibles métricas de los protocolos de routing son las siguientes:

-Calidad del enlace: referido a la existencia de errores en el trayecto.
-Longitud del trayecto: referido al número de saltos o routers intermedios en la red. Es el caso más común.
-Retardo de tránsito: referido al tiempo de propagación (medible mediante un *Ping* de ICMP).
-Ancho de banda del enlace: referido a la capacidad de tráfico disponible entre routers.
-Disponibilidad: referido al grado de ocupación del CPU del router.
-Costo: toma en cuenta el valor de conexión de la ruta.

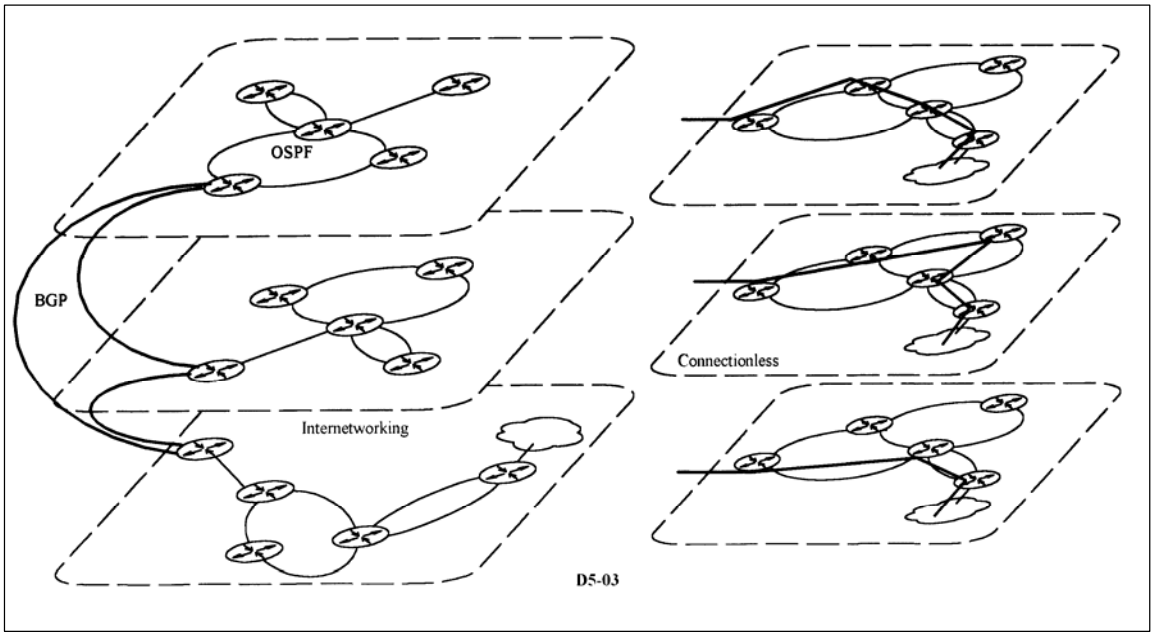


Fig 02. Aplicación de los protocolos de routing para internetworkimg.

Tabla 01. Características de los algoritmos de routing.

	CARACTERISTICAS DE CLASIFICACION
Estático/dinámico	Esta característica se refiere a la posibilidad de fijar una ruta determinada en el caso estático (*Route of last resort*) o routing variable para una adaptación en tiempo real.
Simple/múltiple	Referido a la posibilidad de permitir la multiplexación por varias líneas. Cuando es posible el múltiple-trayecto las vías para distribuir los paquetes son dos: balance por paquete (distribuidos de acuerdo con la métrica) y balance por destino (se asignan rutas por cada nuevo destino). -El balance por paquete es similar al esquema *round-robin* (todos-contra-todos; con el mismo nivel de métrica frente a los demás) para rutas de igual costo. -El balance por destino tiende a preservar el orden de los paquetes. TCP acomoda en orden los paquetes pero puede degradarse la performance. Si bien IP es un protocolo orientado sin-conexión (*connectionless*) los router que implementan el routing preservan en lo posible la ruta.
Plano/jerárquico	En la topología plana todos los router tienen igual jerarquía; en la jerárquica los router forman un *Backbone* para el tráfico principal. Los protocolos OSPF y IS-IS son ejemplos de protocolos de routing que utilizan estructura jerárquica.
Hardware	Referido al tipo de hardware utilizado. Es realizado por Host o Router inteligentes.
Domain	Los protocolos de routing son distintos si trabajan en el mismo dominio (intra-dominio) o entre dominios (inter-dominio).
Algoritmo	Se disponen de dos tipos de algoritmos para obtener la tablas de rutas. **-RIP** utiliza el algoritmo "vector-distancia" originario de Bellman-Ford. Requiere de datos sobre el número de saltos y el costo. El costo puede indicar un valor en $/min o bien preferencia (ponderación debido a retardo: por ejemplo un peso de 1 para 128 kb/s y de 10 para 64 kb/s). Es usado en RIP, Hello y BGP. **-SPF** que es utilizado se denomina *Dijkstra Algorithm*. Es un protocolo de estado de enlace **LSA** (*Link State Advertisements*). Acumula información que es usada por el algoritmo **SPF** (*Shortest Path First*) para reconocer el camino mas corto a cada nodo. Es usado en OSPF y IS-IS. El protocolo IGRP (de Cisco) utiliza un algoritmo híbrido.
	CARACTERISTICAS DE SELECCIÓN
Eficiencia	La eficiencia es la habilidad para seleccionar la mejor ruta con una utilización del CPU mínima.
Sumarización	La sumarización de ruta se refiere a la posibilidad de estructurar la Tabla de Rutas con sets de rutas sobre un mismo enlace. Esto permite reducir sustancialmente la capacidad de memoria utilizada por la tabla.
Simplicidad	Se refiere al software mínimo requerido y el uso del encabezado de paquete. Debe tenerse presente que el protocolo utiliza una parte de las reservas de enlace. De esta forma, protocolos como el RIP realizan actualizaciones periódicas, mientras que el OSPF o IS-IS lo hacen solo en caso de falla. Son más complejos pero solo ocupan al CPU en caso necesario. En funcionamiento normal minimiza la ocupación del ancho de banda.
Robustez	La robustez se refiere a la habilidad para soportar fallas de hardware, condiciones de pérdidas de paquetes e implementación incorrecta. Obsérvese en la **Fig 1** que algunos protocolos trabajan directamente sobre IP mientras que otros lo hacen sobre TCP o UDP.
Flexibilidad	Se refiere a la adaptación a diversas circunstancias.
Convergencia	Es la velocidad de actualización de la Routing Tabla cuando se requiere una actualización (recálculo de rutas para optimización). El problema es la formación de loop de rutas en caso de disponer de una convergencia lenta. El tiempo de convergencia depende de la velocidad de detección de cambios en la red, selección de la ruta y propagación de los cambios. Los cambios realizados en un router y que por el momento no generan cambios en otros routers, pueden provocar loop de routing. Algunos problemas son detectados rápidamente como la interrupción (pérdida de portadora) de una línea serial. En cambio sobre una Ethernet no existe indicación de interrupción (semejante a la pérdida de carrier). Si sobre un router se efectúa un reset tampoco se dispone de una indicación inmediata. Una forma de detectar problemas es mediante la ventana de temporización luego de un mensaje *Hello*.
Escalabilidad	La escalabilidad de la red: se refiere a la posibilidad de crecimiento. Normalmente la escalabilidad se encuentra limitada por razones operacionales más que técnicas.
Seguridad	Referido al uso de medios para protección de la información de routing. El mecanismo de autentificación reduce potenciales inestabilidades.

2- PROTOCOLOS EN CAPA 2

El más simple de los procesos que permiten definir direcciones y rutas es el de resolución de direcciones MAC en una red LAN. Se trata de alguno de los protocolos que se indican en la **Tabla 02**.

Tabla 02. Resolución de direcciones MAC.

ARP	(*Address Resolution Protocol*) de RFC-0826. Este protocolo es usado para anunciarse mediante direcciones de capa IP. Permite comunicarse con un usuario IP sin conocer la dirección MAC del mismo. ARP emite un datagrama de pedido (mensaje *ARP Request*) para todas las unidades MAC en la red LAN. Utiliza la dirección *broadcast* (hexadecimal FF.FF.FF.FF.FF.FF). La respuesta es un paquete (mensaje *ARP Respond*) con la dirección MAC que corresponde a la dirección IP indicada.
Proxy ARP	Definido en RFC-1027. Un router utiliza el proxy ARP para ayudar a un host en el reconocimiento de direcciones de otras redes y subredes vecinas.
RARP	(*Reverse ARP*) de RFC-0903. Funciona con estaciones sin disco rígido que no pueden guardar las direcciones IP. Su función es requerir la dirección IP cuando se conoce la dirección MAC. Los protocolos ARP y RARP no utilizan datagramas IP en forma directa, sin embargo generan un datagrama propio de características similares.
Hello	Este protocolo habilita a los elementos de red para reconocer las direcciones MAC mediante paquetes pequeños de presentación. Cuando un nuevo elemento se conecta a la red genera un mensaje Hello en forma broadcast, el mismo es emitido en forma periódica para indicar que continúa activo. Para cada *Hello message* se responde con un *Hello replie* para configurar la tabla de direcciones.

Un datagrama ARP es un paquete de corta longitud que contiene los siguientes campos:
-Identificador de tipo hardware (2 Bytes);
-Identificador de protocolo (2 Bytes; 0800 para IP);
-HLEN/PLEN (2 Bytes) indica la longitud de dirección MAC e IP (la longitud normal es 6 y 4 Bytes respectivamente);
-Identificador de mensaje (2 Bytes para indicar ARP request o response; RARP request o response);
-direcciones de hardware (MAC) e IP de origen y de destino.

Cada nodo mantiene una memoria denominada *ARP Cache* con las direcciones de las puertas IP y las correspondientes direcciones MAC. Esta es actualizada cada 15 minutos. Se entiende por *Cache* una memoria que contiene los datos corrientemente utilizados, en este caso referido a direcciones y rutas. Un ARP Cache tiene el formato de la tabla inferior (el valor de *Age* corresponde al tiempo de permanencia del dato en el cache expresado en minutos). El requerimiento y respuesta se realiza en forma broadcasting y por ello todos los componentes pueden actualizar la información en el cache.

Protocol	Address	Age (min)	Hardware Address	Type	Interface
Internet	131.108.62.193	187	0800.2010.a3b6	ARPA	Ethernet3
Internet	131.108.1.140	187	0800.200e.33ce	ARPA	Ethernet3

STP (*Spanning-Tree Protocol*). En las redes construidas mediante Switch-Ethernet se debe cuidar que no ocurran loop debido a que los caminos duplicados pueden generar paquetes duplicados. El uso de STA permite eliminar el problema de los loops y mantener las ventajas (redundancia de enlaces). STA es desarrollado originalmente en Digital DEC y luego fue incorporado a **IEEE 802.1d**. Este protocolo permite identificar los loop y mantener activa solo una puerta del switch; se asigna a cada puerta un identificador (la dirección MAC y una prioridad). La prioridad de la puerta se puede asignar en términos de costo.

El STP consiste en un intercambio de mensajes de configuración en forma periódica (entre 1 y 4 seg). Cuando se detecta un cambio en la configuración de la red se recalcula la distancia (sumatoria de costos) para asignar una nueva puerta. Las decisiones se toman en el propio switch. Los mensajes son *Configuration* y *Topology-change*. Los campos del mensaje de configuración incluyen 35 Bytes y el de cambio de topología solo 4 Bytes iniciales. El mensaje de configuración contiene:

-3 Bytes para indicar el Identificador de Protocolo (2) y la Versión (1).
-1 Byte para identificar el Tipo de Mensaje (0 para configuración y 128 para cambio de topología).
-1 Byte de Flag para indicar el cambio de configuración de la red.
-8 Bytes para identificar la raíz (*Root*) y 4 Bytes para identificar el costo de la ruta.
-8 Bytes para identificar el switch y 2 Byte para identificar la puerta del mismo.
-2 Byte para identificar el tiempo de emisión del mensaje (*Age*) y 2 Byte para indicar el tiempo máximo de vida.
-2 Byte para indicar el período de intercambio de mensajes de configuración *Hello*.
-2 Byte para indicar el tiempo de espera para emitir un mensaje en caso de detectar un cambio de configuración.

3- PROTOCOLOS EN CAPA 3

PROTOCOLOS DE ROUTING IP. La mayor jerarquía de routing es el **AS** (*Autonomous System*) que es una colección de redes bajo una administración de dominio común. Los protocolos de resolución interior **IGP** (*Interior Gateway Protocol*) permiten la comunicación interna del dominio AS, en tanto que, los de resolución exterior **BGP** (*Border Gateway Protocol*) lo hacen entre dominios distintos. Así un AS es un grupo de router que utilizan un mismo protocolo de routing. Cada AS puede ser dividido en una número de *Areas*; un router con múltiples interfaces puede participar de múltiples áreas. Estos router se denominan router de borde y mantienen separadas las bases de datos topológicas de cada área.

Un área puede contener a todos los router que inician con la misma dirección IP (por ejemplo, 150.98.05.x), en este caso el uso de la *mask net* (255.255.255.0) puede ser de utilidad. La expresión Dominio se refiere a la porción de red donde los router poseen la misma base de datos topológica. La topología del área es invisible a elementos fuera del área. El dominio es usado para intercambios con AS. Sucesivamente se estudian los siguientes protocolos: para resolución interior el RIP, IGRP y OSPF y para resolución exterior los EGP y BGP. Se informa también sobre IS-IS para resolución interior en el modelo OSI y el HSRP para resolución entre router en hot standby.

3.1- PROTOCOLO RIP (*Routing Information Protocol*)

El protocolo de routing RIP es del tipo de resolución interior IGP indicado como inter-AS. Es originario de Xerox (GWINFO) en la suite XNS. En 1982 pasa a formar parte de UNIX **BSD** (*Berkeley Software Distribution*). Es definido en RFC-1058 en el año 1988. La métrica utilizada es del tipo número de saltos (vector distancia de 4 bits); un número de saltos superior a 15 se entiende como inalcanzable. Por ello el RIP es válido para redes pequeñas.

Desde el punto de vista del modelo de capas RIP trabaja sobre UDP con el número de port 520 (decimal); en cambio BGP trabaja sobre TCP (realiza una conexión con control de errores y de flujo). El paquete RIP contiene la información que se enumera en la **Tabla 03**. El máximo tamaño del mensaje es de 512 Bytes (sin contar UDP/IP). Los mensajes son de *Request* (pedido de transferencia de la tabla de rutas) y la *Response* (respuesta al pedido). Normalmente el request es un mensaje con dirección broadcast. RIP no puede manejar direcciones con máscara de subred variable.

El paquete del protocolo RIP permite la actualización de la *Routing Table* en los routers, el contenido en la dirección IP y el valor de la métrica (utiliza cantidad de saltos desde 1 a 15). La *Routing Table* formada por RIP contiene la siguiente información: Dirección de destino, próximo paso, distancia, *Timer*, *Flag*. La tabla de rutas solo mantiene la mejor ruta al destino. Cuando una ruta mejor es detectada se reemplaza la anterior. Cada router actualiza un cambio y lo propaga a los demás. El tiempo de convergencia alto.

RIP requiere datos de ruta para actualizar las tablas y periódicamente anuncia la presencia y difunde los cambios que detecta en la red. Utiliza el algoritmo "vector distancia" originario de Bellman-Ford. Requiere de datos sobre el número de saltos y el costo; el costo puede indicar un valor en $/min o bien una preferencia (debido a retardo, etc). Este tipo de algoritmo es usado en RIP (Novell y Xerox) y IGRP (*Interior Gateway Routing Protocol* de Cisco).

Los paquetes de RIP son intercambiados en forma periódica cada 30 seg (*Upgrade*). Este mecanismo de transmisión periódica carga la red con información de routing. Si el tiempo de upgrade supera el valor de 90 seg la ruta de salida se considera inválida. Si se supera el tiempo de 270 seg (denominado *Flush Timer*) la ruta se elimina de la tabla de rutas. Obsérvese que el campo de métrica permite un máximo de 15 saltos (*Count Hop*). Si es mayor se considera un destino inalcanzable. Se utiliza un mecanismo denominado *Spli Horizont* que permite evitar información sobre rutas que retornan al origen generando loop de routing entre 2 nodos.

Tabla 03. Campos del protocolo de routing RIP

-Command	1 Byte. Identifica si se trata de un requerimiento o una respuesta. Se solicita el envío de la tabla de rutas y se responde con toda o parte de la misma.
-Version	1 Byte. Identifica la versión del protocolo RIP.
-Reserved	2 Bytes no utilizados.
-Address	2 Bytes. Identifica la dirección de familia de protocolo (para Internet IP el valor decimal es 2).
-Reserved	2 Bytes no utilizados.
-Address	4 Bytes. Dirección IP del destino a la que corresponde la métrica inferior. En un mensaje RIP de respuesta pueden reportarse un máximo de 25 destinos por paquete. Las tablas de ruta más grandes requieren múltiples paquetes.
-Reserved	8 Bytes no utilizados.
-Metric	4 Bytes. Indica el número de saltos al router de destino. El valor 16 corresponde a inalcanzable.

3.2- PROTOCOLO IGRP (*Interior Gateway Routing Protocol*).

Este protocolo es original de *Cisco* para routing en AS. Es un protocolo que usa el vector distancia como RIP. Emite la totalidad de la tabla de rutas al inicio y solo los cambios en períodos preestablecidos como actualización. Mientras RIP usa solo una métrica (con un número de saltos máximo de 16) el IGRP utiliza una combinación de métricas: retardo, ancho de banda, confiabilidad y carga del enlace (estos dos últimos se evalúan mediante un número desde 1 a 255).

Todos los routers mantienen la tabla de rutas de los vecinos para usarlo en el algoritmo de convergencia. Los tipos de paquetes involucrados se denominan: *Hello* (paquete multicast emitido para indicar la presencia)*; acknowledgment* (paquete de reconocimiento)*; update* (paquete emitido en forma unicast a un nuevo router en la red)*; querry; replay and request* (solicita información en forma unicast). Una muestra de una impresión de Tabla de Rutas es el siguiente:

```
Routing entry for 131.108.1.0
      Know via "igrp 109", distance 100, metric 1200
      Redistributing via igrp 109
      Last updata from 131.108.6.7 on Ethernet0, 35 seconds ago
      Routing Descriptor Blocks:
            131.108.6.7, from 131.108.6.7, 35 seconds ago, via Ethernet0
            Route metric is 1200, traffic share count is 1
            Total delay is 2000 microseconds, minimun bandwidth is 10000 Kbit
            Reliability 255/255, minimun MTU 1500 bytes
            Loading 1/255, Hops 0
```

Una tablas de ruta contiene la fila de destino denominada *Default*. Por la misma se enruta cualquier dirección de gateway que es desconocida. Una tabla de rutas extensa complica el mantenimiento y hace más lento.

3.3- PROTOCOLO OSPF (*Open Shortest Path First*).

OSPF es desarrollado en la suite de IP (no enruta en ambiente IPX por ejemplo) como protocolo de gateway interior **IGP**. Este protocolo se creó para mejorar el **RIP**. El OSPF es un protocolo abierto (especificación de dominio público) y se encuentra en RFC-1583 para la versión 2. El algoritmo utilizado se denomina *Dijkstra Algorithm*. Es un protocolo de estado de enlace **LSA** (*Link State Advertisements*) que acumula información usada por el algoritmo **SPF** (*Shortest Path First*) para reconocer el camino mas corto a cada nodo. OSPF es un protocolo intra-AS que dispone de una base de datos topológica que contiene la información recibida mediante LSA.

Cuando se inicia el algoritmo SPF espera que las capas inferiores informen de la operabilidad del enlace; cuando las interfaces están operacionales utiliza el mensaje *Hello* para adquirir información de los router vecinos. En una red pequeña la dirección de los routers vecinos puede ser configurada manualmente; sobre una red mayor se utiliza la dirección multicast 224.0.0.5 reservada para esta aplicación de Hello. Los routers reconocen la dirección y las redes LAN también; no puede ser usada para dirección de usuarios.

Cada router en operación normal emite los mensajes de LSA en forma periódica (valor típico 5 seg). OSPF soporta routing del tipo *multi-path* y **ToS** (*Type-of-Service*). El ToS permite efectuar operaciones de prioridad para datos urgentes sobre protocolo IP. Soporta además diferentes métricas (requiere el número de saltos, la velocidad de comunicación, congestión de tráfico, costo y prioridad). La métrica por default de OSPF está basado en el ancho de banda (el valor de métrica es inverso al ancho de banda).

El protocolo OSPF se adapta mejor a redes jerárquicas (**Fig 03**). La principal decisión es indicar que router se incluyen en el backbone y cuales en cada área. Una topología jerárquica incluye:
-el nivel de **acceso** (conexión a usuarios mediante routers o switch de capa 2),
-el nivel de **distribución** (que conecta a los router de borde de área e implementa mecanismos de seguridad y DNS) y
-el nivel ***Core*** para formar el backbone de la red (este nivel dispone de acceso a la Internet mediante routers de Borde).

Se debe considerar que el OSPF utiliza un algoritmo CPU-intensivo donde el número de cálculos aumenta más rápido que el número de routers. Por ello existen ciertos límites al tamaño de la red.
-Generalmente un área no debe superar los 50 routers.
-El número de routers vecinos (pares en la jerarquía) no debe ser mayor a 60.
-El número de áreas soportadas por un router no debe ser mayor a 3.

Los dos aspectos más críticos respecto de las áreas es la determinación de la dirección y la conexión al backbone. Una forma de localizar direcciones IP en un medioambiente OSPF es asignar números de red separados por áreas. Se asigna dirección de Network por área y de Subnetwork y Host en el interior del área. El router que conecta al área con el

backbone se denomina router de borde (*Bourder*). Es conveniente tener más de un router por borde de área. La redundancia permite prevenir la partición de redes y además permite obtener ancho de banda adicional en caso de tráfico elevado.

El tiempo de convergencia depende del número de router y el tamaño del área (entre 6 y 46 seg). La convergencia en OSPF es mejor que en otros protocolos y se logra mediante dos componentes:
-La detección de cambios de la topología de la red (por detección de falla del enlace o por ausencia del paquete *Hello* luego de un tiempo denominado *dead time*).
-El recálculo de routers (el router que detecta la falla del enlace emite a los otros un paquete de estado de enlace).

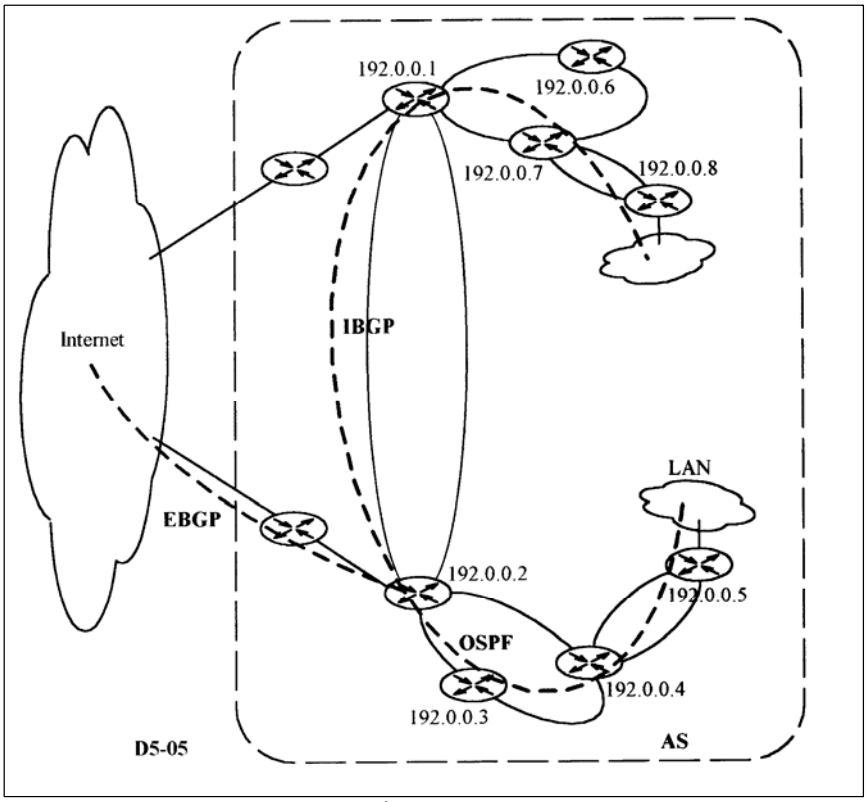


Fig 03. Protocolos de resolución de routing interior al AS y exterior.

El paquete OSPF trabaja sobre IP (protocol= 89) y contiene 24 bytes de encabezado de longitud. El contenido del mismo se indica en la **Tabla 04**. Obsérvese la posibilidad de proveer seguridad mediante el mecanismo de autentificación.

Tabla 04. Campos del protocolo de routing OSPF.

-Version	1 Byte. Indica la versión de OSPF utilizada.
-Type	1 Byte. Especifica uno de los 5 tipos de paquetes OSPF: -*Hello*. Emitido en forma regular para establecer relaciones con router vecinos. -*Database Description*. Describe la base de datos topológica y se intercambia con router adyacentes. -*Link State Request*. Requiere partes de la base de datos topológica cuando se descubren cambios. -*Link State Update*. Responde al mensaje anterior. Existen 4 tipos de campos del tipo LSA: .*Router Link Advertisements*. Describe el estado de enlace entre router de un área. .*Network LA*. Describe todos los router que se conectan a la red multiacceso. .*Summary LA*. Resume las rutas y destinos de salida del área. .*AS External LA*. Describe las rutas de destino al exterior de la AS. -*Link State Acknowledgment*. Reconoce el mensaje anterior para confirmar la recepción.
-Length	2 Bytes. Especifica la longitud total del paquete incluido el encabezado.
-Router ID	4 Bytes. Identifica el router que emite el paquete.
-Area ID	4 Bytes. Identifica el área. En OSPF los paquetes se asocian a un área solamente.
-Checksum	2 Bytes. Realiza un chequeo del paquete completo.
-Authen Type	2 Bytes. Contiene el tipo de autentificación. Ejemplo, simple password. Es obligatoria y configurable.
-Authen	8 Bytes. Información de autentificación.

3.4- PROTOCOLO EGP (*Exterior Gateway Protocol*).

Este protocolo es del tipo interdominio documentado en RFC-0904 (año 1984). Ha sido reemplazado en la práctica por el BGP que se indica a continuación. Inicialmente determina los routers vecinos, verifica luego la presencia on-line y envían periódicamente información de actualización de la red. Los campos de este protocolo involucran 10 Bytes fijos y una carga útil de datos variable. Los bytes fijos indican la versión del protocolo (1 Byte), el tipo y subtipo de mensaje (2 Bytes), información de estado (1 Byte e indica problemas, violaciones, etc), información de *checksum* (2 Bytes para detección de error), número de sistema AS (2 Bytes), numeración secuencial de paquete (2 Bytes) y datos (longitud variable).

3.5- PROTOCOLO BGP (*Bourder Gateway Protocol*)

El protocolo BGP reemplaza al EGP en la Internet y trabaja sobre TCP. El BGP se encuentra normalizado en RFC-1771 para la versión 4. Este tipo de protocolo permite el tráfico sin loop entre sistemas autónomos **AS**. Permite el tráfico dentro de un AS entre router pares (**IBGP** para *Interior*) o entre sistemas autónomos (**EBGP** para *External*) y el pasaje por un sistema autónomo que no opera con BGP. Normalmente es usado entre operadores ISP. La versión IBGP es más flexible, entrega varias vías de conexión en el interior del AS y dispone de una vista del exterior gracias a EBGP. En área de aplicación se muestra en la **Fig 03**.

Cuando un router se conecta a la red el BGP permite intercambiar las *Routing Table* completa. Pero las mismas se intercambian en forma parcial cuando existen modificaciones. BGP utiliza como protocolo de transporte el TCP (port 179). Cuando dos router intercambian información de routing (con la port TCP activa) se denominan *Peers* o *Neighbors*. Una actualización de la tabla de rutas se propaga a los routers pares vecinos. El mapa de rutas es usado en BGP para controlar y modificar la información de routing y para definir las condiciones de redistribución de rutas entre dominios de routing.

BGP utiliza la información de routing intercambiadas para generar un mapa de rutas AS libre de loops. Solo un camino es conservado en la tabla de rutas y es el que se propagada a otros routers. La decisión entre distintos caminos al mismo destino se realiza mediante los siguientes atributos:
-el próximo paso (*Next Hop*),
-la ponderación de peso (por lista de acceso o mapa de ruta; se prefiere el camino de mayor peso ponderativo),
-la preferencia de ponderación local asignada por el operador (para selección de caminos con igual ponderación),
-el origen de la ruta y la longitud del camino.

BGP4 soporta el routing interdominio del tipo *classless* **CIDR**; es decir con una máscara de red. Por ejemplo, una dirección 192.213.0.0/16 significa una máscara del tipo 25.255.0.0. En BGP se utiliza también el concepto de routers *Cluster* que consiste en una secuencia route-reflector-cliente. El router intermedio refleja los paquetes entre route y cliente. El encabezado del paquete ocupa 19 Bytes y el mensaje tiene longitud variable. Los Bytes involucrados en el encabezado se indican en la **Tabla 05**.

Tabla 05. Campos del protocolo de routing BGP.

-Marker	16 Bytes. Mensaje de autentificación que el receptor puede predecir.
-Length	2 Bytes. Longitud total del paquete en número de bytes.
-Type	1 Byte. Identifica el tipo de mensaje de datos que sigue a continuación.
-Data	Mensaje de longitud variable con los siguientes casos. -*Open Message*. 14 Bytes. Provee los criterios para el intercambio entre router. Contiene el tiempo en seg que se espera para declarar un enlace no-funcional; este tiempo se conoce como *hold-time*. Contiene la lista de parámetros opcionales: información de autentificación, etc. -*Update Message*. Sirve para actualizar las tablas de ruta; su longitud es variable. Algunos tipos de mensajes de up-date son: longitud total de un trayecto, atributos de un trayecto (origen, próximo-paso, grado de preferencia, etc), rutas agregadas, etc. -*Notification Message*. Indica condiciones de error a otros equipos. Por ejemplo: error en el encabezado del mensaje, finalización del tiempo (*Hold Time*), evento no esperado, error de datos (error en la lista de atributos, próximo-paso inválido, etc). -*Keep-alive Message*. Se utiliza para informar que el equipo está activo.

3.6- PROTOCOLO IS-IS (*Intermediate System*).

Este protocolo permite el intercambio de información de routing entre sistemas intermedios (intradomain). Corresponde a la norma ISO-10747. Está basado en un desarrollo original de DECnet. Desde el punto de vista de las funciones es similar a OSPF (pero no son compatibles); ambos son del tipo estado de enlace (*Link State*). Permite funciones no soportadas en RIP, como ser: jerarquías de routing, separación de trayectos, tipo de servicio ToS, soporta la autentificación, soporta una

máscara de subred de longitud variable. El protocolo que permite el routing interdomain es el **IDRP** (*Interdomain Routing Protocol*) que es similar al BGP. Los IS-IS y IDRP trabajan sobre el protocolo de red CLNP.

Utiliza una métrica con valor máximo de 1024; es arbitraria y es asignada por el administrador de red. Un enlace simple puede tener un valor máximo de 64. La longitud del enlace es calculada por la suma de las ponderaciones individuales. Otras métricas adicionales son: retardo del enlace, costos de expensas asociado al enlace y errores en el enlace. Un mapa de estos 4 tipos de métrica permite formar la QoS en el encabezado del paquete **CLNP** (protocolo de capa 3 en el modelo ISO) y computar la tabla de rutas de la internetwork.

Existen 3 tipos básicos de paquetes en IS-IS: el *Hello* para el IS-IS; el paquete de *Link State* y el paquete de número secuencial. El formato de los paquetes es complejo y contiene en esencia 3 diferentes partes lógicas. El formato común se enumera en la **Tabla 06**.

Tabla 06. Campos del protocolo de routing IS-IS.

-OH	8 Bytes de *OverHead*. Encabezado común contiene un byte para cada uno de los siguientes mensajes:
.IDE	-Identificador del protocolo IS-IS (corresponde a 1 Byte con valor 131).
.LEN	-Longitud del encabezado (corresponde a los 8 Bytes de longitud).
.PRO	-Versión del protocolo.
.ID	-Identifica la longitud de la porción de dominio ID en la dirección NSAP.
.PAC	-Tipo de paquete: hello, link state o numeración secuencial.
.VRS	-Versión del protocolo (repetición).
.RSV	-1 Byte Reservado (todos ceros).
.AR	-Dirección de área máxima: número máximo de direcciones en el área.

3.7- PROTOCOLO HSRP (*Hot Standby Routing Protocol*)

Este protocolo de *Cisco* entrega una protección hot standby automática entre dos routers. Cuando el router de trabajo falla el otro toma el control. Un router configurado con HSRP posee 4 estados posibles: activo, standby, *speaking* (recibe y emite mensajes *hello*) y *listening* (solo recibe mensajes *hello*).

HSRP trabaja mediante el intercambio de 3 tipos de mensajes multicast:
-*Hello*. Este mensaje se envía cada 3 seg para indicar información de estado y prioridad. El router con mayor prioridad es el que trabaja en un instante; los otros se encuentran en hot standby.
-*Coup*. Este mensaje indica que un router pasa de la función standby a la función activo.
-*Resign*. Este mensaje es emitido por el router activo cuando pasa al estado *Shutdown* o cuando un router de mayor prioridad ha enviado un mensaje *hello*.

1208

SERVICIOS EN REDES IP

Sobre los servicios para redes corporativas ofrecidos mediante redes de transporte IP. Referido a multicast, videoconferencia, VoIP, VPN, VLAN.

1- INTRODUCCION

Los objetivos del presente trabajo se centran en la descripción de los Routers que realizan funciones a nivel de capa 3, los componentes de una red IP y los servicios que la misma puede brindar. A fines de la década de los años `90 este tipo de red se presentaba como la más adaptada para las redes del primer decenio del siglo XXI. Los protocolos estudiados se muestran en la **Fig 01**.

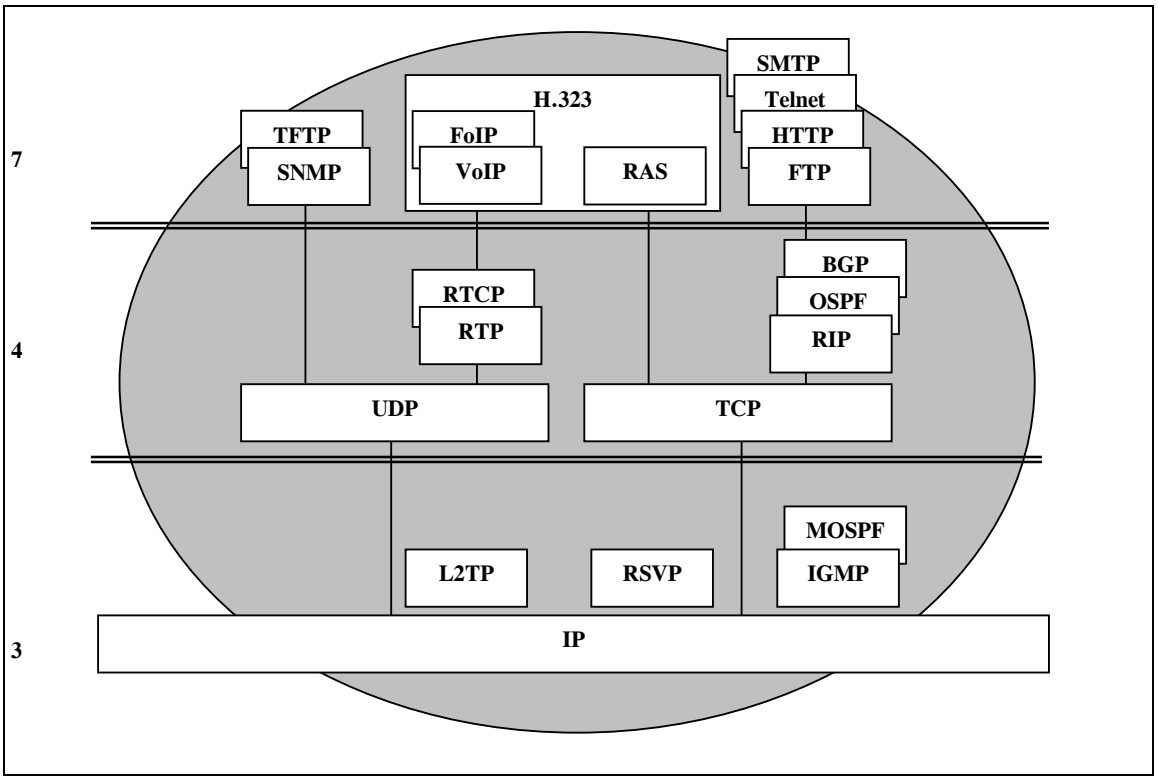


Fig 01. Modelo de capas y protocolos para servicios sobre IP.

2- PROTOCOLOS PARA IP MULTICAST

IP Multicast se aplica cuando una misma información debe ser proporcionada a un grupo de clientes en forma simultánea. Así una emisión de videoconferencia (H.323) puede ser recibida por varios clientes y ocupar una sola vez el canal de transporte. El switch (IEEE 802.1p) que conecta a los usuarios replica los paquetes a los clientes finales. Esta técnica permite la conservación del ancho de banda de una red IP. Otras técnicas de conservación son la compresión de datos y el ancho de banda por demanda **BoD** (*Bandwidth-on-Demand*).

2.1- PROTOCOLO IGMP (*Internet Group Management Protocol*).

Este protocolo standarizado en la RFC-1112 para la versión 1 y en RFC-2236 para la versión 2 se utiliza para la gestión de enlaces multicast. Las direcciones IP pueden ser individual (*unicast*) o grupal para algunos miembros o todos los de la red (*multicast* o *broadcast*). El grupo multicast puede ser permanente o transitorio (armado para un evento en especial).

DIRECCIONES MULTICAST. El **IANA** ha reservado la clase D de direcciones IP para grupos multicast. Esta clase de direcciones consiste en la secuencia 1110 y 28 bits de dirección (5 bits no usados y 23 de dirección). Expresado en la notación normal se trata desde 224.0.0.0 hasta 239.255.255.255. Algunas direcciones se encuentran reservadas y no pueden ser utilizadas. Por ejemplo, 224.0.0.1 corresponde a "todos los sistemas de esta subnetwork" y 224.0.0.2 a "todos los router de esta subnetwork".

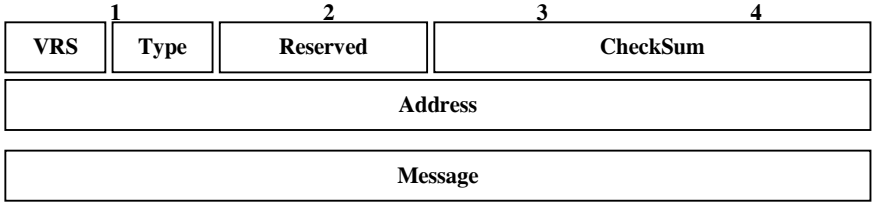
En las direcciones MAC se ha reservado el prefijo (hexa) 01 para MAC-multicast y (hexa) 01005E para direcciones IP multicast. De esta forma casi todos los últimos 3 Bytes de IP y MAC son idénticos. Por ejemplo, la dirección IP: 224.10.8.5 corresponde a la dirección MAC: 01005E 0A0805. En la siguiente secuencia, los bits en negrita no son usados y separan la zona de identificación multicast (anterior) de la dirección propiamente dicha (posterior).

IP Address			1110 **0000**	**0**000 1010	0000 1000	0000 0101
(Decimal)			224	10	8	5
MAC Address	0000 0001	0000 0000	0101 **1110**	**0**000 1010	0000 1000	0000 0101
(Hexadecimal)	0 1	0 0	5 E	0 A	0 8	0 5

El protocolo IGMP determina un servicio sin conexión con el mismo criterio de "best effort" de IP unicast. Se denomina **MBONE** (*Multicast Backbone*) a un set de routers y subredes interconectadas que soportan el servicio IP multicast. El protocolo permite la comunicación entre routers y host conectados en la red. Los mensajes intercambiados en el IGMP v.1 son de capa 3 y ocupan los 20 bytes de IP más 8 bytes de IGMP. Los 8 bytes de IGMP v.1 llevan la información de la **Tabla 01**. En IGMP v.2 agrega a los mensajes *Query* y *Report* (de la v.1) los mensajes *Leave Group* y *Membership Report*.

Tabla 01. Protocolo de grupo multicast IGMP (versión 1).

-VRS	4 bits. Identifica la versión del protocolo.
-Type	4 bits. Identifica el tipo de mensaje (*query* o *report*). Pueden existir mensajes de los protocolos de routing (DVMRP corresponde a decimal 3).
.*Query*	Mensaje emitido periodicamente por el router para determinar que host están conectados a la subred. Este mensaje tiene dirección 224.0.0.1 y un TTL=1 (es decir no puede salir de la subred; se trata de un único trayecto sin relevo).
.*Report*	Mensaje de respuesta del host. La emisión de un mensaje de report se realiza con un retardo random; la presencia de un mensaje de report produce el reset de los temporizadores random de otros host. De esta forma se reduce la concentración de trafico como picos de reportes. Si el router no recibe reportes de respuesta a varios query consecutivos se asume que existe una desconexión y se remueve de la lista de miembros del grupo multicast.
-RSV	1 Byte. Reservado sin aplicación en IGMP v.1. En la v.2 se utiliza para indicar el tiempo máximo de respuesta (unidad de 0,1 seg) en el mensaje Report.
-CKS	2 Bytes. Checksum para detección de errores (calculado de igual forma que en el protocolo ICMP).
-ADR	4 Bytes. Dirección IP de tipo multicast (clase D). En un mensaje query este campo vale cero y es ignorado. En un mensaje report lleva la dirección IP de multicast del grupo reportado.
-Message	Query o Report.



Las operaciones de multicasting en las redes LAN son soportadas por protocolos standard y propietarios. Por ejemplo, en IEEE 802.1p se definen los protocolos para registración **GMRP** (*Group Multicast Registration Protocol*) y gestión de direcciones **GARP** (*Group Address Registration Protocol*).

2.2- ROUNTING MULTICAST.

Los protocolos que se utilizan para el routing en los servicios multicast son derivados de los utilizados para direcciones unicast. De esta forma se toman como origen el RIP y OSPF. Los algoritmos de routing disponibles son: algoritmo broadcasting en reversa RPB o multicast en reversa RPM; algoritmo *Spanning Trees* o el *Core-Based Trees*. Las variantes de protocolos de routing son las siguientes:

PROTOCOLO DVMRP (*Distance Vector Multicast Routing Protocol*).
Este protocolo está definido en RFC-1075. Es derivado del RIP y utiliza una variante del algoritmo **RPB** (*Reverse Path Broadcasting*). El RIP provee un solo tipo de métrica por lo que el OSPF (mantiene más de un tipo) tiene mejor performance. Sin embargo, DVMRP es más simple que MOSPF. Y se utilizó anticipadamente. DVMRP se encuentra sobre IGMP en el modelo de capas.

La principal diferencia entre RIP y DVMRP es que, en tanto RIP calcula el próximo paso hacia el destino, en DVMRP se calcula la cantidad de pasos hacia el origen. DVMRP requiere de una periódica actualización para detectar nuevos receptores en el grupo y por ello tiene un problema de escala. El protocolo DVMRP dispone de diferentes tipos de mensajes: comando *Null*; indicador de familia de formato AFI; comando *Submask*; comando *Metrica*; *Destination Address Request & Responce*.

PROTOCOLO MOSPF (*Multicast OSPF*).
Se define en RFC-1584 como extensión del OSPF de la RFC-1583 y solo trabaja asociado al protocolo OSPF. El MOSPF provee el servicio de multicast pero no el servicio de tunelización del mismo (tampoco lo hace el DVMRP). En un protocolo de routing de tipo unicast la ruta se define en base a la dirección de destino, en tanto que en MOSPF se define en base al origen y los destinos.

La definición de ruta se realiza en base al costo basado en la métrica de estado de enlace. Una vez definida la ruta se forma el árbol en la red y se descarta cada ruta individual. Se define una única ruta, no existe alternativas de igual-costo. MOSPF permite modificar la ruta basado en el ToS del datagrama IP. La optimización de ruta para un grupo no asegura la optimización en el uso de la red.

PROTOCOLO PIM (*Protocol Independent Multicast*).
Si bien es independiente del protocolo de routing de tipo unicast implementado, requiere del mismo para formar la tabla de rutas. Este protocolo mejora la deficiencia de DVMRP aplicando dos técnicas: modo-denso (protocolo diseñado para operar en un medio con miembros de distribuidos con alta densidad y ancho de banda elevado) o modo-distribuido (baja densidad de miembros -no significa pocos miembros- y ancho de banda reducido). El uso de una o de otra depende de la distribución de routers en la red.

3- SERVICIOS EN TIEMPO-REAL

3.1- VoIP (*Voice over IP*).

Los servicios en redes IP incluyen todos aquellos que corresponden a la Internet, más otros de reciente implementación. Por ejemplo, se trata de la transmisión de voz **VoIP** y vídeo en redes de paquetes. Utilizan como soporte cualquier medio basado en routers y los protocolos de transporte UDP/IP. El modelo de capas previsto en 1981 tenía voz sobre RTP/IP; el modelo actual agrega UDP/IP, como sigue:
-Capa de aplicación: protocolo de voz y vídeo H.323; VoIP; FoIP; etc.
-Capa de transporte: protocolo de transporte para tiempo real RTP/RTCP.
-Capa de transporte: protocolo de transporte UDP.
-Capa de red: protocolo de reservación RSVP e internet IP.

Los problemas que se tienen en VoIP son los siguientes:

-Latencia. El gap existente en la conversación debido a los retardos acumulados en la matriz de switch. Se trata del retardo producido por el proceso *store-and-forward* y el retardo de procesamiento (cambio de encabezado, etc). A esto se suman los retardos propios del proceso de compresión de datos. Los retardos en la red pueden ser reducidos mediante el protocolo de reservación RSVP.

-El jitter del retardo. Se entiende por jitter el efecto por el cual el retardo entre paquetes no es constante. Se trata de una latencia variable producida por la congestión de tráfico en el backbone de red, por distinto tiempo de tránsito de paquetes debido al *connectionless*, etc. Se puede utilizar un buffer para distribuir los paquetes y reducir el jitter, pero introduce un retardo adicional. Lo correcto es incrementar el ancho de banda del enlace; solución posible en un backbone pero de menor posibilidad en los enlaces WAN. Otra posibilidad es la formación de colas para prioridad de tráfico.
-Otro problema es la pérdida de paquetes por errores en los routers intermedios de la red IP. Puede utilizarse una corrección de errores FEC pero no del tipo ARQ (retransmisión a pedido).

Por un lado se tienen los servicios de VoIP que ingresan en la red telefónica PSTN y por otro los servicios de datos que provienen desde la red PSTN. En muchas de estas interacciones se requiere la implementación del sistema de señalización SS7. Se trata de una suite de protocolos para el manejo de las comunicaciones por la red PSTN y la gestión de los centros de conmutación.

FoIP (*Fax over IP*).
Se trata de la emisión de facsímil mediante protocolos IP en tiempo real (ITU-T **T.38**) o en formato *Store-and-Forward* (**T.37**). Ambas normas datan del año 1998 y el T.38 es el adoptado en H.323 para multimedia en LAN (también aplicado a VoIP).

El mayor problema de transmitir fax sobre redes de paquetes es la dificultad de mantener la temporización del modem del fax. Los retardos involucran un elevado número de abortos de conexiones. Por otro lado, en tanto con VoIP la pérdida de paquetes se compensa con interpolación, en el caso de FoIP los paquetes deben ser retransmitidos mediante el uso de TCP, por ejemplo. Un terminal para FoIP consiste en 3 partes:
-La unidad modem fax para convertir la señal analógica de salida de un facsimil grupo 3.
-La unidad de protocolo de fax que compensa los efectos de temporización y pérdida de paquetes.
-La unidad de *driver* de red que permite el ensamble de paquetes hacia la red IP.

3.2- VIDEOCONFERENCIA (ITU-T H.323)

Esta tecnología permite la transmisión en tiempo real de vídeo y audio por una red de paquetes. Es de suma importancia ya que los primeros servicios de voz sobre protocolo Internet (**VoIP**) utilizan esta norma. En la versión 1 del protocolo H.323v1 del año 1996 se disponía de un servicio con calidad de servicio (**QoS**) no garantizada sobre redes LAN. En la versión 2 del año 1988 se definió la aplicación VoIP. Una versión 3 posterior incluye el servicio de fax sobre IP (**FoIP**) y conexiones rápidas entre otros.

Los componentes del servicio H.323 son indicados en la siguiente **Tabla 02a**:

Tabla 02a. Componentes para el servicio H.323

LAN	Donde se conectan los terminales, los elementos de interconexión al exterior (router, proxy o gateway) y el gatekeeper con el sistema de gestión.
Terminal	Se realiza en forma bidireccional en tiempo real; se trata de una PC o un equipo a medida. Normalmente se encuentran conectados a una LAN.
Gateway	Provee la conectividad entre la red H.323 y otra distinta (PSTN por ejemplo). Se encuentra conectado a la LAN por un lado y a las líneas de la PSTN por el otro.
Proxy	Es un tipo especial de gateway que conectado a la LAN por un lado, se comunica con otra red en tiempo-real (RTP). El router también tiene esta característica pero lo hace mediante la Internet sin usar protocolos de tiempo real.
Gatekeeper	Es el centro de control para el procesamiento de la llamada, direccionamiento, autentificación, gestión de ancho de banda, tarifación, etc. Aplica las políticas de **AAA** (*Authorization, Authentication and Accounting*). El Gatekeeper debe realizar la traslación de dirección IP a la ITU-T E.164 de la red telefónica; es decir, actúa de interfaz desde la red IP hacia la red telefónica PSTN . El proceso de admisión utiliza mensajes de protocolo **RAS** (descripto a continuación) para el requerimiento de admisión, la confirmación y el rechazo de admisión.
Sistema de gestión	Permite identificar el tráfico H.323 y aplicar las políticas apropiadas. Limita el tráfico H.323 sobre la LAN y WAN. Entrega un sistema de facturación (*Billing*) mediante un server apropiado. Inserta calidad de servicio e implementa seguridad.
Control multipunto	Esta unidad permite realizar conferencias entre varios usuarios.

Algunos términos relacionados con esta técnica son los siguientes:
-**PSTN** (*Public Switched Telephone Network*). Se refiere a la compañía de telefonía local.
-**POST** (*Plain Old Telephone Service*). Se trata del servicio de telefonía básica a dos hilos brindado por la PSTN.
-**FXO** (*Foreign Exchange Office*). Interfaz conectada a la PSTN para servicio POST.
-**FXS** (*Foreign Exchange Station*). Interfaz conectada al aparáto telefónico POST.

Los protocolos especificados por H.323 para efectuar las funciones entre componentes son los siguientes:

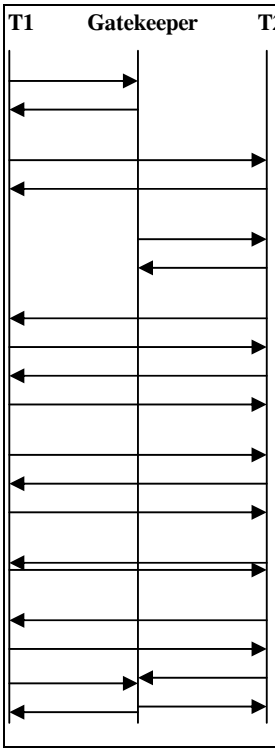
Señales de tráfico. Trabajan sobre UDP/IP.
-Codificación de audio: G.711 a velocidad de 64 kb/s; G.722 para 48, 56 y 64 kb/s; G.728 para 16 kb/s y G.729 para 8 kb/s. En tanto el ITU-T ratificó en 1995 a G.729, el VoIP Forum en 1997 (liderado por Intel y **Microsoft**) seleccionó a **G.723.1** con velocidad de 6,3 kb/s para la aplicación VoIP.
-Codificación de vídeo: de acuerdo con **H.263**.

Protocolos de señalización. Trabajan sobre TCP/IP.
-Protocolo **RAS** (*Registration, Admission and Status*) según H.225 para la comunicación entre terminal, gateway y gatekeeper. Sirve para registración, control de admisión, control de ancho de banda, estado y desconexión.
-Señalización de llamada: para establecer la conexión y desconexión mediante protocolo **H.225**.
-Señalización de control: mediante protocolo **H.245** para comandos, indicaciones, control de flujo, gestión de canales lógicos, etc. Los protocolos H.225/245 trabajan sobre protocolos TCP/IP.

Protocolos de calidad de servicio.
-Protocolo **RTP** (*Real-Time Transport Protocol*): usado con UDP/IP para identificación de carga útil, numeración secuencial, monitoreo, etc. Trabaja junto con **RTCP** (*RT Control Protocol*) para entregar un feedback sobre la calidad de la transmisión de datos.
-Protocolo de reservación de ancho de banda **RSVP**.

PROCEDIMIENTO DE COMUNICACION. Se describe en la **Tabla 02b** el procedimiento de conexión, comunicación y desconexión de una llamada mediante H.323. Intervienen dos terminales T1 y T2 y el Gatekeeper en el centro.

Tabla 02b. Canal de señalización mediante el protocolo RAS en H.323.



T1 requiere el uso de señalización de llamada directa (mensaje ARQ en protocolo RAS).
El Gatekeeper confirma la admisión con el mensaje ACF.

T1 emite en H.225 un mensaje de señalización "setup" requiriendo la conexión.
T2 responde con "call proceeding" en el mismo protocolo.

T2 se registra con el gatekeeper sobre el canal RAS mediante ARQ.
El Gatekeeper confirma la registración mediante ACF.

T2 envía los mensajes de "alerting" y "connect" en protocolo H.225.
T1 envía un mensaje para informar sobre las capacidades del terminal.
T2 reconoce la capacidad del terminal T1 y envía su propia capacidad de terminal.
T1 reconoce la capacidad de T2.

T1 envía un mensaje de canal abierto con dirección RTCP.
T2 reconoce y envía su propia dirección RTCP.
T1 reconoce y envía la dirección RTP. La conexión bidireccional está establecida.

T1 y T2 intercambian mensajes de RTP y RTCP durante la fase de comunicación.

T2 inicia el proceso de cierre de llamada.
T1 confirma la desconexión a T2.
Ambos terminales se desconectan del Gatekeeper mediante el mensaje DRQ.
El Gatekeeper confirma la desconexión mediante el mensaje DCF.

H.263 over RTP. A continuación se describe la paquetización de la señal de vídeo H.263 (videoconferencia por Internet) sobre protocolo RTP. El formato de la señal de vídeo H.263 es denominado **CIF** (*Common Intermediate Format*) y posee 352x288 pixel de luminancia (la mitad de crominancia). H.263 es similar a H.261 pero permite 4 opciones programables: la predicción avanzada (de 1 a 4 vectores de movimiento); tramas PB (un bitstream lleva una trama P y otra B); codificación aritmética basada en sintaxis (para DCT con coeficientes codificados en VLC) y vector de movimiento irrestricto. La estructura del paquete contiene 4 Bytes de encabezado de RTP y 4 Bytes de encabezado para H.263 antes de los datos.

4- SERVICIOS DE PRIVACIDAD

4.1- VPN (*Virtual Private Network*).

Una VPN es una conexión que simula las ventajas de un enlace dedicado (*leased*) pero ocurre sobre una red compartida (acceso remoto sobre una estructura pública con todas las ventajas de un enlace privado). Diversas redes (Frame relay y ATM) permiten formar redes VPN; sin embargo la posibilidad de realizarlos mediante redes IP tiene algunas ventajas. Por ejemplo, la posibilidad de accesos remotos mediante líneas dial-up, la posibilidad de realizar conexiones VPN esporádicamente y entre varios puntos (normalmente los VPN mediante Frame Relay y ATM son canales permanentes PVC).

Utilizando la técnica denominada tunelización los paquetes de datos son transmitidos en una red de routers públicos simulando la conexión punto-a-punto. El ingreso generalmente se realiza en el **POP** (*Point of Presence*) de un **ISP** (*Internet Service Provider*) conectado a una LAN del usuario. El VPN puede proveer mecanismos de seguridad como criptografía, autentificación y eventualmente firewall. La interconexión de puntos en la VPN se realiza mediante el direccionamiento con la técnica **NAT** (*Network Address Translation*) para la distribución de direcciones IP.

Una red IP con accesos VPN consta de los siguientes elementos:
-El cliente con acceso PPP (es el iniciador de la conexión VPN). Puede realizarse mediante la red pública PSTN o mediante ISDN. En este caso el protocolo es IP/PPP.
-El concentrador de acceso **LAC** (*L2TP Access Concentrator*) que se conecta directamente al cliente como medio de tránsito hacia el servidor. Esta denominación LAC es sinónimo de **NAS** (*Network Access Server*). Está localizado generalmente en el punto de presencia **POP** del ISP.
-El servidor de la red **LNS** (*L2TP Network Server*).

Para iniciar y mantener la conexión VPN se requiere de protocolos que realicen la función denominada Túnel. El túnel es una conexión protegida con ancho de banda asegurado que se efectúa entre el concentrador NAS y el servidor LNS. Estos mensajes de control del túnel disponen de dos alternativas. El túnel preserva a lo largo de toda la conexión tanto la información de usuario como el protocolo de acceso PPP. Se realiza una autentificación de usuario VPN; el LAC y LNS forman un túnel para atender los requerimientos. A continuación se genera una sesión L2TP para el usuario final.

PROTOCOLOS DE TUNELIZACIÓN. Los protocolos de tunelización trabajan en capa 2 y permiten una conexión del tipo conmutada **SVC** y aplicar las políticas de seguridad (firewall) sobre cada conexión. Se han definido para establecer y gestionar el proceso de tunelización (túnel virtual en la red) y son el PPTP y L2TP.

-PPTP (*Point-to-Point Tunneling Protocol*).
Es desarrollado por 3Com y Microsoft para Windows95 y NT4.0. Se trata de un protocolo de tunelización voluntario (el usuario decide realizar el túnel desde la configuración de su computadora). Un método de criptografía para VPN realizado mediante PPTP es el **MPPE** (*Microsoft Point-to-point Encryption*). Está diseñado para PPTP con una longitud de 40 bits (también disponible para 128 bits).

-L2TP (*Layer-2 Tunneling Protocol*).
Se trata de un mecanismo del tipo *"Off-Load"* donde el usuario realiza un *Dial-up* para acceso a otro punto de la red mediante el servidor de acceso a la red LAC. Dispone de una tunelización compulsiva (el túnel es creado sin intervención del usuario) utilizando el protocolo PPP. El protocolo L2TP es un standard del IETF que surgió como combinación del PPTP de Microsoft y el L2F (*Layer 2 Forwarding*) de Cisco. En el ámbito de **IPsec** (*IP Security*) el IETF desarrolla la seguridad (autentificación, privacidad e integridad) para trabajar en forma compatible con L2TP y más robusta que MPPE.

En una llamada entrante el usuario remoto inicia la conexión mediante el protocolo de comunicación PPP hacia el proveedor del servicio ISP usando la red telefónica o ISDN. El LAC del ISP acepta la conexión y lo informa al punto de presencia POP; la conexión PPP queda establecida.

L2TP posee mecanismos de autentificación negocidos. Sin embargo, bajo protocolo PPP no existe autentificación por paquete. El cliente es el responsable por la criptografía; puede utilizarse el mecanismo de PPP criptografiado. L2TP posee información de secuenciamiento que puede ser usada para control de flujo dentro del túnel (paquetes hacia el usuario controlados mediante *window* en IP). También puede negociarse la compresión de datos en PPP (por ejemplo mediante LSZ).

4.2- VLAN (*Virtual LAN*).

Existen diversas definiciones de VLAN. Se puede interpretar como un grupo de estaciones de trabajo que no se encuentran en la misma localización física y que se conectan mediante un switch IP. También se dice que una VLAN es un grupo de nodos que residen en un dominio de broadcast común sin saltos de router. Se puede entender como una red conmutada que está segmentada logicamente por función o aplicación. En todos los casos VLAN se forma mediante switch agrupando ciertos usuarios en base a alguna razón en común. Las redes LAN obtenidas son virtuales porque se obtienen mediante agrupaciones lógicas en el *Switching Fabric*.

El agrupamiento de los usuarios de puertas del switch se realiza mediante las siguientes formas:
-por puertas en el switch; cada puerta soporta una VLAN distinta,
-por direcciones MAC (permite el movimiento de la estación dentro de la LAN),
-por direcciones IP (por network o subnetwork o por dirección de host unicast o multicast),
-por protocolo de aplicación.
Trabajando por direcciones se logra una topología de red distinta para cada servicio. Todas las direcciones están asociada a una o más VLAN.

Las ventajas de utilizar VLAN son diversas. Se simplifica las acciones de añadir, mover o cambiar estaciones en la red; se controla mejor la actividad de tráfico (se reduce la circulación de tráfico del tipo broadcast y multicast); se incrementa la seguridad de la red y grupos de trabajo.

VTP (*VLAN Trunk Protocol*).
El protocolo que permite la configuración de VLAN en la red se denomina VTP. Maneja los cambios realizados en la VLAN a nivel de sistema. Automáticamente comunica los cambios a otros switch de la red minimizando la posibilidad de inconsistencias. Este protocolo está acompañado del *VTP Pruning*. Se trata de un método de control de tráfico que disminuye el tráfico de paquetes del tipo broadcast, multicast y unicast; reduciendo las vías de conexión en la topología en árbol por donde se envían los paquetes.

IEEE 802.1Q/p.
Los standard IEEE 802.10 y 802.1Q fueron propuestos para el manejo de las redes VLAN; este último es el utilizado con regularidad. En el standard 802.1Q se define el VLAN *Tagging Switch* que permite una identificación de la VLAN y la posibilidad de priorización del servicio (**CoS** *Class of Service*). La trama del paquete en capa MAC incluye 4 Bytes adicionales al IEEE 802.3 que se colocan luego de las direcciones MAC y antes del *Type/Length*. Los 4 Bytes son indicados en la **Tabla 03**. Obsérvese la presencia de 3 bits para prioridad de tráfico y 12 bits para identificación de VLAN.

El mecanismo que se define para la CoS (clase 0 a 7 desde alta a baja prioridad) se compone de las colas de recepción y transmisión. El umbral para extraer los paquetes de la cola de recepción son:
-Clase de servicio CoS 0/1: umbral del 50% (máxima prioridad).
-CoS 2/3: umbral al 60%.
-CoS 4/5: umbral al 80%.
-CoS 6/7: umbral al 100% (mínima prioridad).

En transmisión existen dos colas la de alta y baja prioridad. Su relación con la CoS es la siguiente:
-Cola de baja prioridad (corresponde al umbral del 80%) y CoS 0/1: umbral al 40%; con CoS 2/3: umbral al 100%.
-Cola de alta prioridad (corresponde al umbral del 20%) y CoS 4/5: umbral al 40%; con CoS 6/7: umbral al 100%.

Por ejemplo, una puerta del switch que no fue configurada para CoS tiene un valor por default de umbral del 100%. Un servicio clase CoS=2/3 en el buffer de recepción (entrada al switch) tiene un umbral al 60% para la extracción de paquetes, mientras que en el de transmisión se coloca en alta prioridad (umbral al 20%) y con CoS=2/3 tiene una prioridad adicional del 80%.

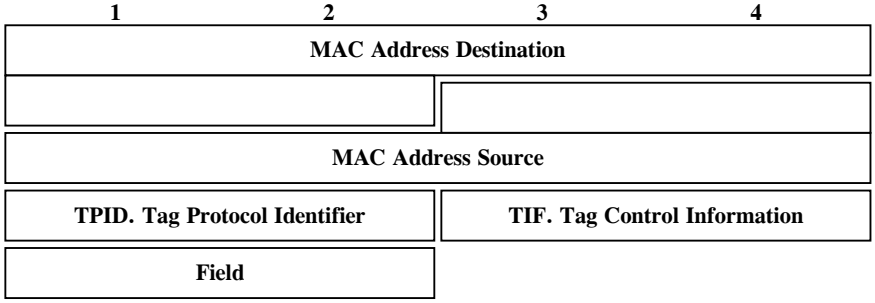
IEEE 802.1D.
En este standard de la IEEE se define el protocolo **STP** (*Spanning-Tree Protocol*). Se diseñó para permitir que en una red de bridge y switch de muchos componentes se formen enlaces cerrados para protección de caminos. Se intercambia información de la topología de la red que permiten construir el árbol.

De esta forma se crean puertas redundantes en el cableado, el protocolo STP deshabilita automáticamente una de ellas y la habilita en caso de falla de la otra. Se evita de esta forma la generación de loop pero se administra la protección en casos de fallas.

IEEE 802.3z.
Este standard se encarga de definir la operación full-dúplex de la interfaz Gigabit Ethernet y del control de flujo. El control de flujo es desarrollado por el switch mediante el protocolo 802.3x. Cuando se llega a un umbral de congestión determinado dicho protocolo informa al emisor que reduzca la transferencia de paquetes.

Tabla 03. Campos del protocolo MAC para satisfacer el servicio VLAN.

-PRE	7 Bytes. Preámbulo para el nivel físico (1010…10) para sintonizar el reloj de la estación receptora. Como la Ethernet se usa a 10 Mb/s en codificación Manchester el reloj es de 10 MHz.
-SFD	1 Byte (10101011). Delimitador de inicio de trama.
-DA	6 Bytes. Dirección de destino para identificar al terminal destinatario. Contiene:
-SA	6 Bytes. Identifica la dirección MAC del terminal de origen. Idéntico a DA.
-TPID	(*Tag Protocol Identifier*). 2 Bytes. Usados para identificación del protocolo. En Ethernet es hexa=8100.
-TIF	(*Tag Control Information*). 2 Bytes usados para las siguientes funciones:
.UP	3 bits para prioridad del usuario (*User Priority*). Se trata de CoS desde 0 a 7. Esta información permite poner en práctica la CoS definida en IEEE 802.1p.
.CFI	(*Canonical Format Indicator*). 1 bit para ser usado por Token Ring.
.VLANI	(*VLAN Identifier*). Este campo de 12 bits permite identificar la VLAN (válido desde 1 a 1005). Permite la interoperación entre diferentes productores.
-Field	2 Bytes con las siguientes alternativas:
.Type	Para Ethernet: Campo que identifica el tipo de protocolo superior de capa 3. Se trata de: IP (hexadecimal 0800), ARP (0806) y RARP (8035).
.Length	Para IEEE 802.3. Longitud del campo de información de usuario LLC.



1209

SEGURIDAD EN REDES IP

Una visión acerca de la política de autentificación del usuario, integridad de datos, privacidad de la red; el uso de firewall y la disponibilidad en las redes corporativas.

1- INTRODUCCION

POLÍTICAS DE SEGURIDAD. Se entiende por redes IP a aquellas redes que soportan como medio de transporte la suite de protocolos TCP/IP. Estas redes son corporativas (internas a una empresa) o públicas (permiten la conexión de redes privadas). Estas redes soportan los servicios de interconexión entre LAN y la conexión a Internet; pueden formar conexiones del tipo tunelizadas y redes LAN virtuales **VLAN** según IEEE 802.1Q.

La estructura es jerárquica formada por routers (conmutación en capa 3) y switch (conmutación en capa 2/3/4). Además de estos componentes se encuentran otros que permiten ofrecer servicios de capas superiores (server, cache, firewall, etc). Este trabajo se ocupa de los componentes que garantizan la seguridad en la red. Los mismos se encuentran cercanos al centro de la red corporativa.

En una red corporativa la seguridad involucra una política que contiene los elementos generales informados en la **Tabla 01**. En ítems sucesivos se trata la forma de asegurar la privacidad e integridad de la información, así como el control de acceso y el firewall.

Un *Site* es una organización de elementos de red (server, computadoras, routers, etc) que tienen acceso a Internet y que requieren una política de seguridad. Para que una política de seguridad sea viable a largo plazo debe ser flexible (independiente del hardware y software involucrado). Los servicios ofrecidos por el Site (se requieren servidores para realizar dicha tarea) son: *Name* (DNS), *Password/Key* (autenticación), SMTP (*E-Mail*), WWW (web), FTP, NFS, *News*, *Firewall*, etc. Estos servidores ofrecen servicios diversos a los clientes de la red.

Tabla 01. Componentes de la Política de Seguridad.

Responsabilidad	-La principal regla de la política de seguridad es la de informar al usuario de red y entrenarlo en los problemas de seguridad.
Autentificación	-Se utiliza para garantizar la identidad de los que intervienen en la conexión.
Control de acceso	-Se trata de asegurar que los que acceden a la red (luego de la autentificación) solo lo realicen sobre los recursos autorizados y no efectúen un manejo impropio. Se trata de una extensión del proceso de autentificación.
Integridad	-Es la condición de recibir los datos completos, sin modificación, falta o inserción de información. Una forma de asegurar la integridad es mediante el uso de *signature* digital; una extensión de la criptografía.
Privacidad	-Pretende asegurar la Confidencialidad de la información. Se utiliza la criptografía (*scrambler*) de los datos para la protección de privacidad. Algunos tipos especiales de criptografía se utilizan para la *Signature* de datos.
Emisión de reportes	-Se trata de alertas en tiempo-real de actividades sospechosas de forma que permite actuar al operador de la red a tiempo.
Antivirus	-Realizar la protección del tipo antivirus impide el ingreso de problemas mediante discos flexibles o programas que se bajan de la red (*Download*).
Firewall	-Permite realizar un seguimiento y filtrado de las aplicaciones y conexiones que se establecen. Se disponen de varias generaciones de firewall funcionando de acuerdo con la complejidad.
Direcciones NAT	-La traslación de direcciones NAT es una función que puede ser desarrollada por el firewall y consiste en reasignar direcciones entre la intranet y la internet. La política de seguridad puede involucrar la protección de direcciones internas.

STANDARD DE SEGURIDAD. La seguridad en redes IP dispone de versiones "propietarias" y una intento de standard que se conoce como **IPsec** (*IP Security*) y está desarrollado en IETF (RFC-2401). Se trata de un conjunto de standard que se ocupan de la confidencialidad, integridad de los datos y autenticación en redes con protocolo IP. IPsec incluye la criptografía y el firewall. Estos procesos deben funcionar en conjunto con una política global de seguridad de la empresa, entre ellas la criptografía de datos y el firewall.

Relacionado con IPsec se encuentra **IKE** (*Internet Key Exchange*). Es un protocolo de management que utilizado sobre IPsec mejora la flexibilidad. En forma automática negocia las asociaciones de IPsec (no requiere configuración manual). Permite especificar el tiempo de duración de la seguridad. Permite cambiar la clave de criptografía durante una seción de IPsec. Permite la autentificación dinámica entre pares.

Adicional a IPsec se implementan otros tipos de standard. El **AH** (*Authentication Header* de RFC-2402) es un protocolo de seguridad para autentificación. AH está embebido en los datos para su protección. El **ESP** (*Encapsulation Security Payload* de RFC-2406) se usa para privacidad y autentificación.

2- AUTENTIFICACION.

2.1 DIVERSOS METODOS

El proceso de autentificar a un cliente puede ser realizado durante 4 etapas posibles: la conectividad del cliente, cuando se accede al software de autentificación del switch, mediante un servidos o cuando se autoriza a trabajar en una VLAN. Existen diversos métodos de autentificación de clientes. Se utilizan diversas herramientas como ser: *username*, *password*, claves (*key*), **RADIUS**, **PIN** (*Personal Identification Number*), Kerberos, LDAPv3, etc.

Tabla 02. Formas de autentificación.

S-Key	Es un método anunciado en 1981 (standard RFC-1760) y basado en una clave secreta aplicada a la función hash (algoritmo **MD4**). El algoritmo *Hash* tiene las versiones SHA-1 y MD4/5. Se trata de generar un código con el auxilio del algoritmo. El algoritmo genera un mensaje compacto conocido como *Digest*. Es un proceso criptográfico que genera una secuencia fija de 128 bits en MD y 160 bits en SHA-1. El resultado del algoritmo es usado para crear un password.
Smart-Card	Otra técnica es el ***Smart Card*** consistente en una clave (**PIN** inicial) y una tarjeta que contiene información criptografiada. Este método es común en telefonía celular GSM. La información de autentificación puede ser memorizada en un servidor de directorio **LDAP** con los objetos referidos al tipo de cuenta, el horario de uso, etc.
Kerberos	Es desarrollado en el MIT como un sistema de autentificación para sistemas abiertos en entornos distribuidos. El proceso se realiza cuando se inicia la sesión (*logon*) del tipo cliente-servidor. Se fundamenta en *tickets* que se obtienen de un servidor y que tienen una duración limitada de tiempo. El ticket contiene toda la información del cliente para asegurar su identidad. También se generan tickets para una sesión en particular que permiten la criptografía entre pares. Utiliza DES para criptografiar y autentificar. La versión Kerberos-5 es un standard de Internet (RFC-1510). Kerberos tiene 3 fases. En la primera el usuario obtiene una credencial para ser usada en el proceso de requerimiento de acceso a otro servicio. En la segunda el usuario requiere la autentificación para el servicio especificado. En la tercera el usuario presenta sus credenciales al servidor. Existen tickets y autenticadores (este contiene información adicional del cliente). Ambos usan criptografía de clave privada pero con diferentes claves (key). El ticket contiene: los nombres del cliente y servidor, la dirección IP del cliente, el timestamp y lifetime de IP y una clave random para la sesión.
RADIUS	(*Remote Access Dial In User Service*) Es un método de autentificación para acceso a Internet en dial-up. Se remite a 1996 (RFC-2058). Los componentes del proceso son tres: el cliente (generalmente el NAS), el agente de autentificación (módulo de software localizado en el router o switch de acceso) y el servidor RADIUS (utiliza un modelo client/server donde el server opera sobre UNÍS o NT). RADIUS opera sobre UDP.
TACACS	(*Terminal Access Controller Access Control System*). Es una familia de protocolos de control de acceso basado en TCP o UDP (port 49). Utiliza el modelo client/server; el cliente es el NAS y el server trabaja sobre UNÍS o NT. Resume los procesos de autentificación, autorización y contabilidad (*accounting*). Como autentificación puede usar los protocolos para PPP (PAP, CHAP o EAP) o Kerberos. La autorización es la acción para determinar que acciones pueden ser desarrolladas, mientras que el accounting es la acción de memorizar que hace el usuario.

RADIUS. El procedimiento de autentificación utilizado en RADIUS es el siguiente:
-el cliente realiza un logon (pedido de inicio de sesión) al agente enviando el username y el password;
-el agente emite un *Request* de verificación al servidor RADIUS para efectuar la autentificación;
-el servidor responde con la autentificación *Acknow* en caso afirmativo o *Reject* en caso negativo;
-por fin, el agente interconecta al cliente con el servidor del servicio requerido (Web, por ejemplo).

El RADIUS es un software organizado en una estructura jerárquica con varios archivos y directorios agrupados en una base de datos **raddb** (*Radius Database*). Se disponen de los siguientes archivos:
-*Users*. Contiene el perfil del usuario: información de seguridad y configuración, nombre de usuario, método de autentificación, dirección y máscara, etc.
-*Dictionary*. Define los atributos y valores que se memorizan en el archivo de usuario.
-*Clients*. Contiene la lista de username y password de la red. Se utiliza para la autentificación de acceso.

Por ejemplo, a continuación se da un modelo de base de datos de usuario RADIUS:

```
   Password = "testing",
   Expiration = "31 Dec 1999",
   Service-Type = Framed-User,
      Framed-Protocol = PPP,
      Framed-Address = 172.16.3.33,
      Framed Netmask = 255.255.255.0,
      Framed-Routing = Broadcast-Listen,
      Filter-Id = "std.ppp",
      Framed-MTU = 1500,
      Framed-Compression = Van-Jacobsen-TCP-IP
```

AAA (*Authentication, Authorization, Accounting*). Este paradigma permite la configuración de las funciones de:
-autentificación: para identificación de usuarios (incluye login y password), etc. Es una vía para identificar acceso a la red.
-autorización: para controlar el acceso remoto en forma de RADIUS o TACACS.
-cuentas: para servicios de recolección de datos, similar a *billing*.

3- PRIVACIDAD E INTEGRIDAD

La criptografía es el empleo de la escritura para inducir a un error intencional. Se aplicó en Egipto a partir del 700 aC creando infinidad de jeroglíficos (escritura monumental o cursiva) que pierden conexión con la escritura cotidiana (hierática) y permitiendo la lectura solo por parte de la minoría sacerdotal. La codificación criptográfica permite la protección contra ataques pasivos (sobre la señal de datos PDU) a la comunicación. El término *cipher* y *cryption* se refiere al proceso de "cifrado" o "encriptado" de datos.

3.1- TIPOS DE CRIPTOGRAFIA.

En RFC-1827 se indica la **ESP** (*Encapsulation Security Payload*) como mecanismo para proveer seguridad en Internet. Algunos métodos usados en redes IP son enumerados en la **Tabla 03**. Se disponen de dos formas de cifrado genéricas:

-CLAVE PUBLICA (asimétrica).
La criptografía para Internet se inicia en 1976 por Diffie y Hellman cuando se estableció el concepto de "criptografía de clave pública". Para realizar este proceso se recurre a un número público (**g**), dos números privados (**x** en un extremo, **y** en el otro) y un módulo (**p**). El extremo A envía la clave ($\mathbf{g^x}$) y el extremo B la clave ($\mathbf{g^y}$) en ambos casos módulo-p. En recepción se realizan las operaciones $(g^x)^y$ y $(g^y)^x$ respectivamente. Ambas resultados son idénticos y pasan a ser la clave de criptografía secreta y única. El problema de la criptografía de clave pública es la lentitud de cálculo y la posibilidad de ser descifrada mediante el criptoanálisis. Se disponen de dos métodos de clave pública el DH y RSA (**Tabla 03**).

-CLAVE PRIVADA (simétrica).
La criptografía de clave privada consiste en utilizar en cada extremo un mismo código de cifrado. El problema es intercambiar el código entre extremos con seguridad y una vez utilizado debe ser actualizado (cambiado) en forma periódica. Es un método fácil y muy utilizado. Entre los métodos reales se encuentran **DES** (*Data Encryption Standard*) (o 3DES), **RC-4** (*Riverst Cipher*), **IDEA** (*International Data Encryption Algorithm*) y **FWZ-1**. Los métodos difieren en la longitud de bits de la clave (key), lo cual se asocia con la "fortaleza" del sistema criptográfico. La fortaleza se refiere al esfuerzo que se requiere mediante un ataque de "fuerza bruta" (el uso combinado de diferentes computadores para calcular todas las posibles combinaciones) para descifrar el algoritmo.

El protocolo **IKE (*Internet Key Exchange*)** es un protocolo de gestión de claves (key) que trabaja en conjunto con el standard IPSec. IKE permite mejorar las funciones de IPSec permitiendo flexibilidad y configuración. Elimina la necesidad de configuración manual de parámetros; permite el intercambio seguro de claves key para criptografía y la autentificación dinámica entre pares.

EJEMPLO: TELEFONIA GSM. Un tipo similar de criptografía se aplica en telefonía móvil celular en GSM (también en AMPS). Se autentifica el ingreso a la red y se criptografía la información para protección de escuchas no autorizadas. Se tienen algoritmos distintos pero similares para el proceso de autentificación y cifrado de datos de usuario. El cifrado se realiza sobre pares de grupos de 57 bits (con una codificación de interleaver ya realizada para distribuir las ráfagas de errores).

La red GSM (desde el centro de switching MSC) envía un número random **RAND** de 128 bits. El móvil utiliza a RAND para mezclarlos con un parámetro secreto Ki disponible también en el centro de autentificación. La mezcla se realiza mediante un algoritmo denominado A8 y permite obtener la señal Kc de 64 bits. El número de trama (numeración secuencial de 22 bits) y Kc (correspondiente a 64 bits) generan, mediante el algoritmo de criptografía A5, la señal S2 de 114 bits. La numeración secuencial de tramas se recibe por el canal de control de sincronismo SCH. Esta señal S2 se usa para componer los datos (2x57 bits) a ser transmitidos desde el móvil mediante compuertas exclusive-Or.

Tabla 03. Métodos de criptografía.

DES	-(*Data Encryption Standard*). El sistema DES fue desarrollado por IBM y adoptado por el **NBS** (*National Boreau of Standard*) como standard de criptografía en el año 1977; solo está disponible bajo licencia del gobierno de USA. Está fundamentado en bloques de códigos conocidos **ECB** (*Electronic Code Book*). El método standard utilizado se basa en segmentar la información en bloques fijos de 64 o 128 bits de longitud para realizar una criptografía por bloques. La clave para el cifrado (*Key*) es un código de 56 bits y se trata de un tipo de clave privada. Para reducir la probabilidad de detección se realiza un proceso de concatenación de forma que el resultado de un bloque influye sobre el siguiente (para el inicio se adopta un vector iniciación **IV**).
3DES	-En RFC-1851 se describe el uso de una variante de criptografía del algoritmo DES. La versión 3DES corresponde a un proceso de triple convolución mediante 3 claves distintas (denominadas k1, k2 y k3) de 56 bits cada una. Determinan en conjunto una longitud efectiva de 168 bits. Si las 3 claves de 56 bits son las mismas la convolución resulta en el algoritmo DES. Cada conjunto de 56 bits es memorizado en 8 bytes, cada uno de ellos contiene 7 bits del código algorítmico y 1 de paridad. El 3DES opera en bloques de 8 bytes, por ello requiere un vector iniciación (IV) de 8 bytes al inicio del datagrama y un *padding* al final del mismo (para obtener un número múltiplo de 8 bytes). La trama resultante dispone de los siguientes campos: .**SPI** (4 bytes) que indica el parámetro de seguridad. .**IV** (Nx4 bytes) es el Vector Iniciación. .**Payload**. Campo de datos criptografiados. .**Padding**. Es un campo de longitud variable para entregar un múltiplo de 8 bytes. .**PL** (1 byte) para indicar la longitud del campo de padding. .**PT** (1 byte) para indicar el tipo de payload.
DH	-(*Diffie-Hellman*). Este algoritmo se debe a Diffie-Hellman y es del tipo clave pública. Tiene las opciones de 768 y 1024 bits (grupos 1 y 2). Mayor cantidad de bits genera un código más robusto pero requiere mayor capacidad de cálculo.
RSA	-(*Riverst-Shamir-Adleman*) original del año 1978. Es un método de clave pública y utiliza una clave de 512 bits. Normalmente las claves para RSA se configuran manualmente. Se utiliza también como firma digital. El concepto es utilizar una clave privada y otra pública en cada extremo.
Signature	-(*Digital Signature*). La firma digital es un block de datos emitido al final de un mensaje para atestiguar la autenticidad del archivo. Si algún cambio se ha efectuado, la autenticidad de la firma no se verifica, sirviendo como autentificador y verificador de integridad de los datos. Está disponible en PGP y RSA.
PGP	-(*Pretty Good Privacy*). Emerge para datos memorizados o emitidos mediante e-mail.
Hash; SHA-1; MD4/5	-El algoritmo *Hash* tiene las versiones **SHA-1** (*Secure Hash* Algorithm) y **MD4/5** (*Message Digest* de RFC-1320/1321). Se trata de generar un firma digital con el auxilio del algoritmo Hash y tomando el mensaje completo como entrada. El algoritmo genera un mensaje compacto (conocido como *Digest*) que, convenientemente criptografiado mediante una clave privada, genera la firma digital. El mensaje y la firma digital son transferidas simultáneamente para su verificación. La firma digital es de longitud constante (64 o 128 bits). MD5 procesa entradas de 512 bits y entrega una salida de 128 bits; SHA-1 también ingresa 512 bits pero entrega un mensaje de 160 bits. SHA es un algoritmo intenso para el uso del procesador.

3.2- PPP: AUTENTIFICACIÓN Y CRIPTOGRAFIA

El protocolo **PPP** (*Point-to-Point Protocol*) entrega un método de conexión para datagramas IP con un procedimiento de autentificación y criptografía (RFC-1969 del año 1996).

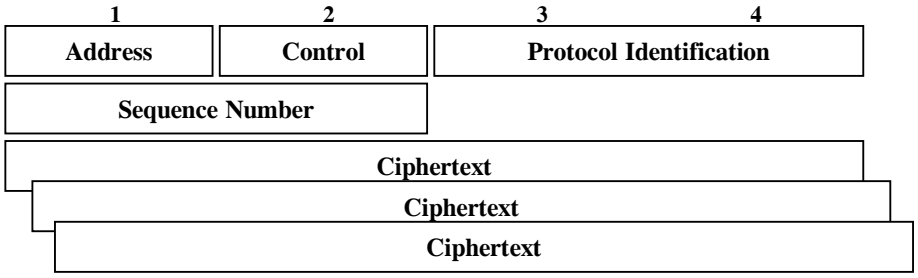
En PPP se dispone de los protocolos **LCP** (*Link Control Protocol*) y **NCP** (*Network Control Protocol*). El LCP es responsable de establecer, mantener y terminar la conexión. La autentificación no es obligatoria y se realiza luego de la primera fase de LCP, mediante el NCP. Los protocolos de autentificación disponibles son:

-**PAP** (*Password Authentication Protocol*). El protocolo PAP se ingresa en el campo de datos del paquete PPP y contiene 3 posibles funciones: requerimiento de autentificación y las respuestas de autenticación positiva o negativa.
-**CHAP** (*Challenge Handshake Protocol*). Mientras que el PAP no es un protocolo robusto ya que solo se emite un password, en el CHAP se realiza una verificación periódica. En CHAP se aplica una función Hash entre un número aleatorio y un identificador ID. La función Hash es típicamente la MD5.
-**EAP** (*Extensible Authentication Protocol*). El protocolo EAP soporta múltiples protocolos de autentificación.

El protocolo que permite controlar la criptografía se denomina **ECP** (*Encryption Control Protocol*). El ECP genera una trama para la negociación de los parámetros de criptografía. El formato del paquete PPP criptografiado contiene los campos enumerados en la **Tabla 04**.

Tabla 04. Campos del protocolo PPP criptografiado.

-ADR	1 Byte. Campo de dirección de PPP. No es criptografiado ni comprimido.
-CTR	1 Byte. Campo de control de PPP. No es criptografiado ni comprimido.
-PID	2 Bytes. (*Protocol Identification*). Campo de direcciones (hexa 0053).
-SN	2 Bytes. (*Sequence Number*). Numera en forma secuencial desde cero los paquetes criptografiados.
-CT	*Ciphertext*. Los datos criptografiados se realiza mediante el procedimiento DES



SEGURIDAD EN TCP/IP. La seguridad involucra diversas herramientas disponibles para distintos servicios. Para los servicios de web se dispone de **SHTTP** (*Secure HTTP*) que involucra la autentificación, criptografía y signature. Utiliza un código **MAC** (*Message Authentication Code*) que utiliza una clave Hash. Para segurizar un socket se recurre a **SSL** (*Secure Socket Layer*), protocolo diseñado por Netscape. Trabaja sobre aplicaciones del tipo http, Telnet, TNP o FTP. El protocolo **SSH** (*Secure Shell Protocol*) permite segurizar los accesos login remoto.

4- CONTROL DE ACCESO Y SEGUIMIENTO.

4.1- EL FIREWALL.

Es un sistema o grupo de sistemas que refuerzan la seguridad en las redes corporativas o proveedores de servicios con protocolos IP. El firewall determina los servicios que pueden ser accedidos desde el exterior de la red (desde la conexión a Internet). Todo el tráfico debe pasar por el firewall para ser inspeccionado.

FUNCIONES. El módulo de firewall instalado como un software sobre el router o servidor de acceso permite realizar las siguientes funciones:
-Control de acceso. Es el principal objetivo del firewall. Crea un perímetro de defensa diseñado para proteger las reservas corporativas. Acepta, rechaza y controla el flujo de paquetes basado en identificadores de capa 3 o aplicaciones. El principio de funcionamiento es: "todas las conexiones son denegadas a menos que estén expresamente autorizadas".
-*Logging*. Es el inicio de las conexiones entrantes y salientes. El uso de un sistema proxy y cache incrementa la velocidad de respuesta de estas operaciones.
-Traslación de direcciones. Permite realizar las funciones de **NAT** (*Network Address Translator*) asegura la supervisión de la información de entrada y salida. El NAT permite aliviar la escasez de direcciones IP y eliminar la necesidad de renumeración cuando se realiza un cambio de **ISP** (*Internet Service Provider*).
-Autentificación. El proceso de autentificación involucra a 3 componentes: el servidor, el agente y el cliente.
-Reportes. El firewall ofrece un punto conveniente para monitorear (*Audit and log*) y generar alarmas.

El firewall genera dos áreas en una red: el área pública con facilidad de acceso desde el exterior (para visita de Web, por ejemplo) y el área interna, detrás del firewall que se encuentra protegida contra la penetración no deseada. El perímetro de defensa se denomina zona desmilitarizada **DMZ** (*De-Militarized Zone*) y puede ser accedida por un cliente externo, el cual no puede acceder al interior de la red. El firewall puede trabajar sobre un server o sobre un router. La ventaja es que se concentra esta acción en un centro de la red consolidado en lugar de estar distribuido en cada host. Esta acción es más útil cuando es llevada a cabo por el router de entrada a la red. Por otro lado, ofrece un punto óptimo para instalar el Web y Server de FTP.

LIMITACIONES. Sin embargo, el firewall no puede controlar el tráfico que no pasa por él. Si existe un *Dial-out* irrestricto desde el interior de la red las conexiones PPP o SLIP a la Internet pueden generar una puerta no protegida. No protege contra robos mediante *Floppy Disks* o ataques internos a la red. No protege contra virus. Muchas veces los ataques internos son mayoría frente a los externos.

El firewall debe ser inmune a la penetración de ataques de *Hackers, Crackers* y espías [1]). El hacker puede utilizar diversas herramientas para obtener información de la red interna y utilizarla en consecuencia. Así por ejemplo,
-el protocolo SNMP puede examinar la tabla de rutas;
-el programa *TraceRoute* puede relevar redes y router intermedios;
-el protocolo *Whois* puede entregar datos del DNS;
-el server DNS puede acceder a una lista de host;
-el protocolo Finger puede revelar detalles de usuarios (*login name*);
-el programa *Ping* puede emplearse para localizar un host desconocido, etc.

Algunos tipos de ataques a la red son el envío de paquetes no-ruteables al router (lo que degrada su performance) y el envío de actualizaciones de tablas de ruta espureas (conocido como *Spoofing*).

4.2- GENERACIONES DE FIREWALL.

Son 5 los tipos posibles de implementaciones de firewall; se trata de una historia corta, cerca de una década, pero muy variada. Los sistemas son:

1- ***Packet Filter***. El router examina cada datagrama para determinar si se adapta al filtro de paquetes definido. Los elementos analizados con el propósito de determinar su pertenencia son: la interfaz de red física, las direcciones IP de origen y destino, el tipo de protocolo encapsulado (TCP, UDP, ICMP), las puertas de nivel de transporte TCP/UDP de origen y destino, el tipo de mensaje ICMP, etc.

Esta técnica es la primer generación de sistemas de firewall y data de 1985/88. El defecto es que normalmente no interviene sobre el protocolo de aplicación y por ello los paquetes pasan con un mínimo de escrutinio y convierte a este tipo

[1]) Se entiende por *Cracker* una persona que intenta acceder a un sistema sin autorización. A menudo lo hacen con malas intensiones en contraposición con el *Hacker* que es una persona que disfruta el conocimiento profundo de un sistema.

de firewall en el menos seguro. En el kernel TCP/IP se mantienen las listas de lo permitido y lo denegado lo cual hace del proceso relativamente rápido frente a los otros tipos de firewall. Puede ser implementado a nivel hardware sobre el router. Otro problema es la posibilidad de ataques del tipo *Spoofing*: consistente en enviar desde el exterior de la red paquetes con direcciones IP correctas del interior de la red.

2- ***Circuit Level***. Se trata de utilizar un Gateway a nivel de Circuito. Es la segunda generación de firewall y data de 1989/90. Este método releva las conexiones TCP sin realizar un filtrado o procesamiento de paquetes adicional. Esto permite detectar la conexión con la red protegida. Revisa el proceso de iniciación de conexión para verificar si existe al procedimiento extraño. Se mantiene una tabla de cada conexión durante el tiempo que se mantiene activa. Luego es borrada de la memoria.

Nuevamente no interviene sobre el protocolo de aplicación sino sobre el secuenciamiento del nivel de transporte. Solo trabaja sobre el protocolo TCP y por ello tiene las mismas ventajas y desventajas que el Packet Filter. Entrega un método muy rápido pero poco seguro.

3- ***Application Layer (Proxy Service)***. Se trata de un Gateway a nivel de Aplicación. Esta versión es más estricta que el filtro de paquetes y se desarrolló entre 1990/91 (tercera generación). Se trata de instalar un código particular para cada aplicación, si el código no corresponde no pasa por el firewall. Esta operación se realiza mediante un *proxy services* (un *proxi server* y un *proxi client* que dialogan en representación de los servidores y clientes reales).

El proxy es un firewall especial que gestiona tráfico de HTTP o FTP, por ejemplo. Trabaja solo con los protocolos para los que fue diseñado. Las conexiones que salen de la intranet pasan por el servidor proxy antes de ir a la internet. El cliente interno realiza el pedido al servidor proxy que evalúa la factibilidad y decide si permite o rechaza la conexión. El cliente proxy se sitúa a la entrada de la intranet antes del cliente real para las operaciones entrantes.

Se define como un *bastion host* porque está armado contra ataques. Este método da al administrador un control completo de cada aplicación. El firewall examina los paquetes de aplicación de forma que mantiene el secuenciamiento y conexión de la sesión; además puede validar otros ítem de seguridad como el password. Además puede actuar de cache para operaciones del tipo HTTP. Entre las desventajas se encuentra el retardo debido al procesamiento del nivel de aplicación. No provee protección sobre UDP y RPC.

4- ***Dynamic Packet Filter.*** El tipo de técnica de filtro de paquetes dinámico se utiliza para control de aplicaciones sobre el protocolo UDP. Se analizan los paquetes de *Request* de salida y la respuesta a los mismos es interceptada. Si la respuesta no aparece en un cierto tiempo se descarta la conexión. Se trata de una cuarta generación y data de 1991/94. Tiene las mismas ventaja y desventajas que el primer tipo solo que no permite la entrada de paquetes UDP no solicitados.

5- ***Kernel Proxy***. El último método de crear un firewall se estructura en el Kernel del Windows NT. Data de 1996/97 y es la quinta generación de firewall.

ESTRUCTURA DEL FIREWALL. El firewall tiene una arquitectura cliente-servidor (alta performance, escalabilidad y control centralizado). Tiene dos módulos primarios: el módulo de firewall y el módulo de management. El módulo de firewall incluye el módulo de inspección y el de seguridad. En estos se implementa la política de seguridad de la empresa. Manejar el firewall mediante una política de seguridad significa determinar con precisión las acciones que serán adoptadas en cuanto a los protocolos que transitan por el mismo.

El módulo de management utiliza una interfaz gráfica que facilita la aplicación de la política de seguridad. Se trata de una base orientada-al-objeto donde se definen objetos y a cada uno se le asignan propiedades y atributos. Entre los objetos se encuentran: los elementos de red (router, host, etc); usuarios; servicios; recursos (servidores HTTP, FTP, etc); objetos temporales; claves (key); etc.

Con los firewall se pueden generar protecciones en paralelo para redundancia en caso de fallas. Los firewall se interconectan mediante un cable para formar una estructura denominada como *Failover*.

5- DISPONIBILIDAD

La seguridad también tiene que ver con la disponibilidad permanente del sistema sin pérdidas de información. Cuando se evaluar los costos de indisponibilidad del sistema debe considerarse los siguientes aspectos: el costo del tiempo sin red, los problemas de la recuperación del servicio normal, comprender la vulnerabilidad de los sistemas, etc. Se puede determinar un rango subjetivo desde "inconveniente" a "catastrófico" con respecto a los problemas de indisponibilidad. Algunos problemas se presentan sobre procesos (interrupción, pérdida, corrupción de datos), sobre programas, sobre los negocios de la empresa (ventas, proyectos y operaciones) o sobre los propios empleados.

Se considera a este punto el grado de pérdida aceptable y el tiempo que se requiere para la recuperación del sistema. Las tecnologías vulnerables son: el hardware (memorias, procesadores, fuente de alimentación, etc), el sistema operativo, las bases de datos, la red o el management. Para solucionar los problemas de alimentación se recurre a **UPS** (*Uninterruptible Power Supple*); se procede al la duplicación de componentes (tolerante a fallas); a enlaces WAN de tipo redundante por distintos proveedores, etc.

DISASTER RECOVERY. Se trata de métodos que permiten recuperar a un sistema cuando existe una falla. Se disponen de los siguientes métodos:
-*Backup.* Puede realizarse mediante una localización externa. Puede realizarse fuera de línea o en-línea.
-Transacción. Se trata de actualizar los reportes de la base de datos. Un monitoreo de la transacción permite evitar sobre-escrituras de la base de datos con datos corruptos.
-Duplicación del disco. Los datos son escritos en dos discos simultáneamente.
-Servidores espejados. El servidor completo es duplicado para prevenir fallas. Los datos son sincronizados en ambos mediante un enlace de alta velocidad.
-Si se produce un corte en el vínculo de comunicación, *disaster recovery* se refiere a una selección automática de una vía alternativa.

1210

CALIDAD DE SERVICIO EN REDES IP

Sobre los problemas de calidad de servicio en la redes IP; los umbrales de QoS definidos, las herramientas disponibles para hacerlo posible y protocolos necesarios para servicios de tiempo-real.

1- CALIDAD DE SERVICIO QoS (Quality of Service)

1.1- DEFINICIONES.

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (jitter) acotados a valores contratados con el cliente. En las redes Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de **CIR** (*Commitated Information Rate*) con el usuario. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como ser los protocolos de tiempo-real RTP y de reservación RSVP. Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (VoIP) por ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado **LFI**. Mediante **QoS** (*Quality os Service*) se tiende a preservar los datos con estas características.

Los servicios tradicionales de la red Internet (SMTP o FTP) disponen de una calidad denominada "*best effort*"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real como el web. Para servicios del tipo "*real-time*" (voz y vídeo) se requiere una latencia mínima.

LATENCIA-JITTER. Se denomina **latencia** a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo por el procesamiento "*store-and-forward*" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para reconocimiento de encabezado, errores, direcciones, etc). Un tiempo de latencia variable se define como **jitter** (fluctuación de retardo) sobre los datos de recepción.

La solución al jitter es guardar los datos en memorias buffer, lo cual introduce un retardo aun mayor. Se han implementado diversas formas de buffer garantizados mediante software:
-Cola prioritaria: donde el administrador de la red define varios niveles (hasta 4) de prioridad de tráfico.
-Cola definida: donde el administrador reserva un ancho de banda para cada tipo de protocolo específico.
-Cola ponderada: mediante un algoritmo se identifica cada tipo de tráfico priorizando el de bajo ancho de banda. Esto permite estabilizar la red en los momentos de congestión.

1.2- VARIANTES DE SERVICIOS.

Los servicios de datos y multimediales tienen distintos requerimientos de calidad referido a latencia y jitter. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del tráfico. Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

En La **Tabla 01** se encuentran las siguientes variantes de servicios: clase de servicio en redes LAN, tipo de servicio sobre protocolo IP y calidad de servicio sobre redes IP. Por otro lado se han definido las características de la calidad de servicio que se entregan en la misma Tabla: servicio garantizado (mediante reservación de nacho de banda), diferenciado (mediante prioridad de tráfico) y el "mejor esfuerzo".

Tabla 01. Calidad de servicio: variantes y clasificación.

	VARIANTES EN CAPA 2, 3 y 4
-CoS	-(*Class of Service*). CoS se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes en total dentro del protocolo MAC. Estos 3 bits permiten definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del switch LAN para la descarga de paquetes. Para más detalles ver el servicio VLAN que es soportado por esta versión de funcionamiento para servicios de capa 2. Se ocupa la IEEE 802.x en los siguientes standard.
.IEEE 802.1p	-Se define el protocolo para registración de CoS **GARP** (*Generic Attribute Registration Protocol*). Las aplicaciones específicas del GARP son la registración de direcciones multicast **GMRP** (*Multicast GARP*) y de usuarios VLAN con protocolo **GVRP** (*LAN GARP*).
.IEEE 802.1Q	-Servicio VLAN para realizar enlaces troncales reduciendo el efecto de expansión en árbol de paquetes y el control de broadcasting.
.IEEE 802.3x	-Este standard examina el control de flujo en enlaces Ethernet del tipo full-dúplex. Se aplica en enlaces punto-a-punto (Fast y Gigabit Ethernet). Si existe congestión se emite hacia atrás un paquete llamado "*pause frame*" que detiene la emisión por un período de tiempo determinado. Una trama denominada "*time-to-wait zero*" permite reiniciar la emisión de paquetes.
.IEEE 802.1D	-Define el protocolo **STP** (*Spanning-Tree Protocol*). Se diseñó para permitir que en una red de bridge y switch de muchos componentes se formen enlaces cerrados para protección de caminos. Se intercambia información de la topología de la red que permiten construir el árbol. De esta forma se crean puertas redundantes en el cableado, el protocolo STP deshabilita automáticamente una de ellas y la habilita en caso de falla de la otra. Cada puerto tiene una ponderación en costo (el administrador de la red puede modificar el costo para dar preferencia a cierta puerta).
-ToS	-(*Type of Service*). Es sinónimo de CoS en la capa 3. Sobre el protocolo IP se define el ToS con 3 bits (del segundo byte del encabezado IP) para asignar prioridades. Se denomina señal de precedencia.
-QoS	-(*Quality of Service*). En redes IP se define la tasa de acceso contratada **CAR** (*Committed Access Rate*) en forma similar al CIR de Frame Relay y ATM. La calidad QoS se ve garantizada mediante protocolos de reservación **RSVP** y de tiempo real **RTP** que se describen en este mismo capítulo.
	CLASIFICACION DE LA QoS
Guaranteed	-El servicio garantizado es utilizado para requerir un retardo máximo extremo-a-extremo. Se trata de un servicio análogo al CBR (*Constant Bit Rate*) en ATM. Se puede aplicar un concepto de reservación de tasa de bit (utiliza RSVP) o el método *Leaky-bucket*. Al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo aún en momentos de congestión. Se lo conoce como *Hard QoS*.
Differentiared	-El servicio diferenciado utiliza la capacidad de particionar el tráfico en la red con múltiples prioridades o **ToS** (*Type of Service*). Se dispone de 3 bits de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IPv4). Es por lo tanto un *Soft QoS*. El control de aplicación es del tipo *leaky-bucket*. Se puede soportar la función **CAR** permite un management del ancho de banda (política de tráfico). La primer línea de defensa frente a la congestión es el uso de buffer de datos; lo cual implica el armado de una cola de espera y el retardo correspondiente dependiendo de la prioridad asignada en dicha cola.
***Best-effort*.**	-Este es un servicio por *default* que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo FIFO. Por ejemplo, el software Microsoft NetMeeting para aplicaciones multimediales utiliza la norma H.323 (E.164); trabaja sobre redes LAN y redes corporativas. Esta norma no tiene previsto garantizar la calidad de servicio QoS.

1.3-.BITS DE PRECEDENCIA

El campo de precedencia en el encabezado de IPv4 permite definir varios tipos de servicio ToS. Se trata de 3 bits que por razones históricas tienen diferentes nombres (routing, priority, etc) y que pueden ser usados para signar prioridad. Se aplica un control de acceso extendido EACL para definir la política de la red en términos de congestión. En redes heterogeneas se debe mapear este tipo de servicio en equivalentes (tag switch, Frame Relay y ATM).

Con Los bits de precedencia se pueden realizar 3 tipos de acciones: routing basado en políticas **PBR** (*Policy-Based Routing*) (por ejemplo direcciones IP, port de TCP, protocolo, tamaño de paquetes, etc); propagar la política de QoS mediante el protocolo de routing BGP-4 y la tasa de acceso contratada CAR. La **CAR** (*Committed Access Rate*) se ofrece especificando políticas de tráfico y ancho de banda. El umbral de CAR se aplica a la puerta de acceso para cada puerta IP o por flujo de aplicación individual. Una técnica disponible para manejar el CAR es el *netflow switch* que se comenta más adelante.

Algunas opciones de política de CAR son:
-Política de prioridad:

CAR máximo (el exceso de ancho de banda es descartado);
CAR premium (el exceso es señalado con un nivel de preferencia más bajo);
CAR best effort (por encima de un umbral se cambia la preferencia y sobre otro los paquetes son eliminados);
-Política de asignación:
CAR por aplicación (diferentes políticas son usadas en distintas aplicaciones; por ejemplo bajo nivel para HTTP).
CAR por puerta (los paquetes que ingresan por un port son clasificados con alto nivel de prioridad).
CAR por dirección (puede diferenciarse entre la dirección IP de origen y destino y asignar la prioridad en cada caso).

1.4- CACHING.

Existen 3 armas que utiliza el router para mejorar la eficiencia de la red reduciendo el tráfico que circula por la misma:
-el manejo de nombres y direcciones mediante **DNS**,
-los servicios *proxis* (se entiende por *proxi* a un elemento de la red que actúa en representación de otro) y
-el *cache* local.

Un *Cache* es un block de memoria para mantener a mano los datos requeridos frecuentemente por varios procesos. Cuando un proceso requiere información primero consulta el cache, si la información se encuentra allí se produce una mejora de la performance de funcionamiento reduciendo el retardo de procesamiento. Si no se la encuentra en el cache se buscará en otras alternativas de memoria y luego se lo encontrará disponible en el cache para una próxima oportunidad.

Una ventaja adicional de ciertos cache es la posibilidad de reducir el dialogo para transferencia de información. Por ejemplo una consulta web lleva una sesión de innumerable cantidad de objetos que son transferidos mediante un HTTP *Get-Request*. Puede reducirse la cantidad de paquetes transferidos mediante una sesión en paralelo de objetos.

Algunos tipos de memoria cache son:
-Cache del procesador: es parte del procesador y es de más fácil acceso que la memoria RAM y a una velocidad mayor.
-Disco cache: pertenece a la memoria RAM y contiene información del disco. En algunos casos se mueve en forma anticipada la información desde el disco al cache en la RAM.
-Cache cliente-servidor: se trata de un banco de memoria ubicado en el cliente para agilizar el movimiento de datos.
-Cache remoto: permite reducir los retardos cuando se accede a información de un sistema remoto en una WAN. Se resuelve mediante un *caching* de información del terminal remoto ubicado en el sistema local.
-Cache de servidor intermedio: entrega información a un grupo de clientes (*Local Workgroup*) en un sistema cliente-servidor.

WEB-CACHING. Para un ISP el uso de cache en el punto de presencia POP puede reducir el tráfico en su red (aumentando la velocidad de respuesta al usuario y el costo de la conexión WAN). Un tráfico muy común y apropiado para el cache es el Web. El cache se conecta directamente al router, el cual deriva todos los paquetes de requerimiento al cache (por ejemplo los paquetes con port-TCP de destino 80 -indica el protocolo http-), de esta forma puede verificar si la información está disponible. Su ventaja se incrementa en la medida que el número de usuarios es mayor.

Los componentes de este complejo son los siguientes:
-La memoria cache que se denominan *Cache Engine*. El cache posee suficiente memoria (ejemplo, 24 Gbytes) y capacidad de transacciones (algunos miles de sesiones TCP simultáneas).
-El router conocido como *Home Router*. El cache se conecta directamente al router de borde de la red (en la conexión hacia la Internet).
-Un router puede poseer varios cache que se denominan *cache farm*. En este caso se forma una jerarquía entre cache para sucesivas investigaciones sobre el requerimiento del usuario.
-Un router que administra el cache dialoga con la memoria mediante un protocolo **WCCP** *(Web Cache Control Protocol)*. El cache puede trabajar también en modo *Proxy* sin el protocolo WCCP y dialogando con un *Browser* configurado en forma manual.

La desventaja del Web-Caching es que pueden aparecer diferentes versiones de un documento en la web. La duración de un documento en el cache debe ser limitada en el tiempo para reducir este efecto. La duración normalmente está especificada por el generador de la página web.

La introducción de firewall para seguridad de acceso a los web ha generado la idea del *Caching-Proxy*. En este contexto el proxy es un programa que interactúa entre el cliente y los servers; se trata de **URL** (*Uniform Resource Locator*). Esta posición es ideal para general el cache del web; el primer software disponible para esta función fue el servidor de web del CERN en el año 1993.

2- HERRAMIENTAS PARA QoS.

En la **Tabla 02** se relacionan los distintos tipos de herramientas que se disponen para asegurar una QoS dentro de una red IP. Se trata de mecanismos que previenen o manejan una congestión, distribuyen el tráfico o incrementan la eficiencia de la red. Los protocolos involucrados en asegurar la calidad de servicio son los indicados en la misma Tabla; a los mismos se refiere como mecanismos de señalización. En el ítem siguiente se analizan con detalle a los mismos.

Tabla 02. Herramientas disponibles para asegurar la QoS.

	CONTROL DE CONGESTION EN EL BUFFER DE DATOS.
-**FIFO**	-(*First In, First Out*). El primer mensaje en entrar es el primero en salir. Este es el mecanismo de QoS por *Default* en las redes IP. Es válido solo en redes con mínima congestión. No provee protección, no analiza el ancho de banda ni la posición en la cola de espera.
-**PQ**	-(*Priority Queuing*). Este mecanismo de control de congestión se basa en la prioridad de tráfico de varios niveles que puede aportar el encabezado del datagrama IP (**ToS** *Type of Service*). Se trata de 3 bits disponibles en el Byte 2 del encabezado de IPv4 (bits de precedencia).
-**CQ**	-(*Custom Queuing*). Este mecanismo se basa en garantizar el ancho de banda mediante una cola de espera programada. El operador reserva un espacio de buffer y una asignación temporal a cada tipo de servicio. Es una reservación estática.
-**WFQ**	-(*Weighted Fair Queuing*). Este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino y tipo de protocolo en IP, número de *Socket* -port de TCP/UDP-) y por el ToS en el protocolo IP. En este esquema la menor ponderación es servida primero. Con igual ponderación es transferido con prioridad el servicio de menor ancho de banda. El protocolo de reservación RSVP utiliza a WFQ para localizar espacios de buffer y garantizar el ancho de banda.
	CONTROL DE TRAFICO
-WRED	-(*Weighted Random Early Detection*). Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma random si la congestión aumenta. Está diseñada para aplicaciones TCP debido a la posibilidad de retransmisión. Esta pérdida en la red obliga a TCP a un control de flujo reduciendo la ventana e incrementándola luego en forma paulatina. Un proceso de descarte generalizado, en cambio, produce la retransmisión en "olas" y reduce la eficiencia de la red. La versión ponderada WRED realiza el drop de paquetes de forma que no afecta al tráfico de tipo RSVP. Una versión superior debería considerar el tráfico de aplicación.
-GTS	-(*Generic Traffic Shaping*). Provee un mecanismo para el control del flujo de tráfico en una interfaz en particular. Trabaja reduciendo el tráfico saliente limitando el ancho de banda de cada tráfico específico y enviándolo a una cola de espera. De esta forma permite una mejor performance en topologías con tasa de bit diferentes. Este control de tráfico se relacióna con **CAR**.
	INCREMENTO DE LA EFICIENCIA. SEÑALIZACIÓN.
-**LFI**	-(*Link Fragmentation and Interleaving*). El tráfico interactivo como Telnet y VoIP es susceptible de sufrir latencia y jitter con grandes paquetes en la red o largas colas en enlaces de baja velocidad. Se basa en la fragmentación de datagramas y el intercalado de los paquetes de tráfico.
-RSVP	-(*Resource Reservation Protocol*). Se trata de implementar el concepto de Señalización. Se dispone de dos tipos de señalización: en-banda (por ejemplo los bits de precedencia para ToS) y fuera-de-banda (mediante un protocolo de comunicación como el RSVP). Este protocolo permite que un host o un router asegure la reservación de ancho de banda a lo largo de la red IP.
-**RTP-HC**	-(*Real-Time Protocol-Header Compression*). El protocolo de tiempo real RTP es estudiado por separado más adelante. La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de RTP/UDP/IP a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los datagramas.

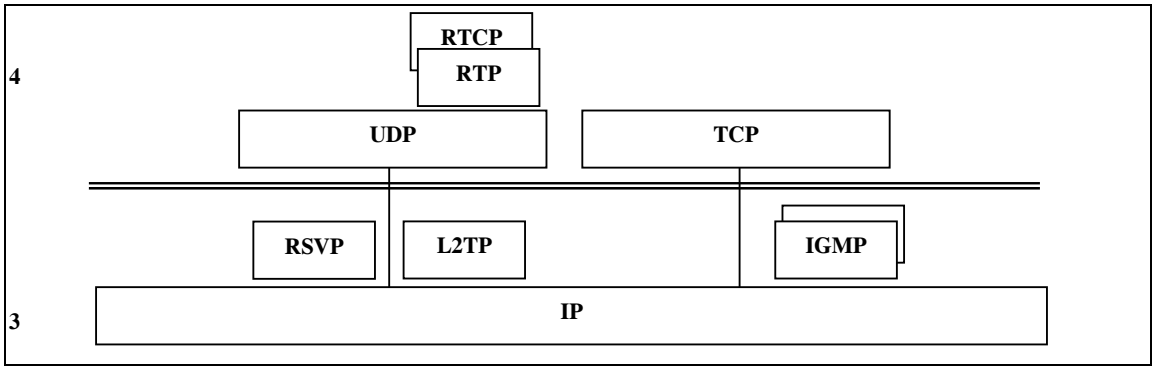
No todas las herramientas disponibles son usadas en los mismos routers. Por ejemplo, la clasificación de paquetes, el control de admisión y el manejo de la configuración se usan en los router de borde (*eage*), en tanto que en los centrales (*backbone*) se gestiona la congestión. El tratamiento de la congestión se fundamenta en el manejo de las colas en buffer mediante diferentes técnicas. El buffer es la primer línea de defensa frente a la congestión. El manejo correcto (mediante **políticas de calidad** de servicio) del mismo permite determinar el servicio de calidad diferenciada. Una segunda defensa es el control de flujo. El problema del control de flujo en TCP es que se ha planea de extremo-a-extremo y no considera pasos intermedios. En TCP cada paquete de reconocimiento (*Acknowledgment*) lleva una crédito (*Window*) con el tamaño del buffer disponible por el receptor. Un sobreflujo de datos en los routers de la red se reporta mediante el mensaje *Source Quench* en el protocolo ICMP. Estos mecanismos son ineficientes y causan severos retardos en la conexión.

3- PROTOCOLOS RSVP/RTP

En la **Tabla 03** se enumeran los protocolos que se estudian a continuación para asegurar la calidad de servicio en aplicaciones de tiempo-real.

Tabla 03. Protocolos para asegurar la calidad de servicio QoS.

RSVP	-(*Resource Reservation Protocol*). Este protocolo permite que un host o un router asegure la reservación de ancho de banda a lo largo de la red IP. Es del tipo orientado al receptor (el receptor solicita la reservación) y es útil para aplicaciones de tipo símplex (unidireccional). Puede funcionar como unicast o multicast.
RTP	-(*Real-time Transport Protocol*). Se utiliza sobre el protocolo UDP para aplicaciones como H.323 o VoIP.
RTCP	-(*Real-Time Transport Control Protocol*). Este protocolo se utiliza para control de calidad de servicio sobre aplicaciones que trabajan sobre RTP.
IGMP	-(*Internet Group Management Protocol*). Este protocolo se utiliza para aplicaciones del tipo multicast cuando se requiere distribuir la misma información sobre un grupo (multicast) de usuarios y reduciendo el ancho de banda ocupado. Se emite un mismo paquete con dirección multicast en lugar de uno para cada dirección unicast. Es estudiado en otro trabajo.



3.1- RESERVACION DE ANCHO DE BANDA (RSVP)

Los servicios del tipo SMTP o FTP en Internet son con calidad "best effort"; es decir, no prevén una calidad de servicio. Esto tiene como consecuencia una latencia variable y jitter sobre la información del tipo tiempo-real (audio o vídeo). RSVP permite la reservación de ancho de banda para asegurar una QoS. El protocolo RSVP trabaja en conjunto con el protocolo de transporte **RTP** para servicios de voz y vídeo en tiempo-real. El RSVP está disponible en RFC-2205.

Existen dos formas de reservación del ancho de banda: estática y dinámica. La reservación estática permite asignar un porcentaje fijo del canal de comunicación a cada tipo de protocolo (por ejemplo, 10% a HTTP, 15% a FTP, 3% a Telnet, etc). El protocolo RSVP permite reservar el ancho de banda en forma dinámica para asegurar una calidad de servicio **QoS** en las redes IP. La QoS permite garantizar el servicio en forma CAR similar al CIR de Frame Relay.

El protocolo RSVP se define para los servicios integrados en Internet. Es utilizado por el host para solicitar una QoS al router para una aplicación particular y es usado por el router para establecer un ancho de banda con todos los nodos intermedios del trayecto.

Opera tanto sobre IPv4 como sobre IPv6; no es un protocolo de routing y solo se lo utiliza para reservar ancho de banda y buffer. En el modelo de capas el protocolo RSVP ocupa la función de la capa 3 sobre IP, en la misma forma que los protocolos de routing (OSPF y BGP), de multicast (IGMP), de gestión (ICMP) y de transporte (TCP y UDP). Una sesión manejada por del protocolo RSVP está definida mediante 3 direcciones: la dirección IP de destino (receptor), el identificador de protocolo y la port de UDP.

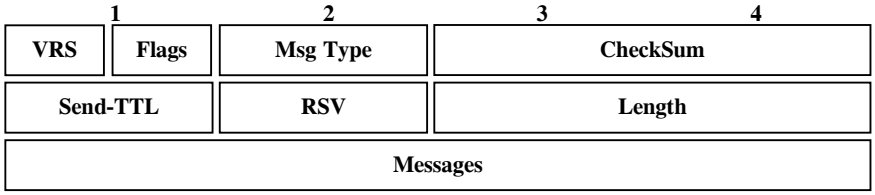
Está definido para operar en forma de unicast o multicast. En el caso de operar con protocolo multicast primero se establece el enlace mediante IGMP (para establecer el grupo) y luego mediante RSVP (para establecer la reservación). Por otro lado el RSVP es un protocolo de carácter símplex, es decir unidireccional. Está orientado-al-receptor; en el sentido que es el receptor el que solicita la reservación y la interrumpe.

CONTROL DE TRAFICO. La QoS es implementada por un mecanismo de flujo de datos denominado "control de tráfico". Este mecanismo incluye 3 etapas:
-la clasificación del paquete para determinar la QoS y la ruta de cada paquete;
-el control de admisión para asegura la disponibilidad de la reservación y
-el proceso de determinación temporal de emisión (*Packet Scheduler*).
El requerimiento de reservación es iniciado por host receptor y pasa por los distintos router de la red. Si algún mecanismo intermedio falla se genera un reporte de error. Se dispone de dos mensajes de error: *ResvErr* y *PathErr*.

Este protocolo mantiene en forma "soft" el estado de los routers y host, entregando un soporte dinámico para cambios de miembros y adaptación automática de cambios de routing. No es un protocolo de routing pero depende de los mismos. Los mensajes de *Path* y *Reservation* se utilizan a estos propósitos. Una lista más completa de los tipos de mensajes (denominado *State Block*) del protocolo RSVP se encuentran en la **Tabla 04**.

Tabla 04. Campos que componen el paquete de RSVP (*Reservation Protocol*).

-VRS	4 bits. Versión del protocolo (actualmente la versión 1).
-Flags	4 bits. No se han definido bits de flag hasta el momento.
-Msg Type	1 Byte. Identifica el tipo de mensaje que ocupa el campo de longitud variable al final del paquete. Se dispone de los siguientes casos: Path, Reser, PathErr, ResvErr, PathTear, ResvTear, ResvConf.
-Checksum	2 Bytes. Chequeo de paridad del protocolo RSVP.
-Send-TTL	1 Byte. Se trata del tiempo de vida de IP con que se emite el paquete de RSVP.
-RSV	1 Byte. No usado.
-Lenght	2 Bytes. Longitud total del mensaje en bytes incluyendo la longitud variable.
-Messages	Nx4 Bytes. Mensaje de longitud variable en palabras de 32 bits.
.Resv	-Mensaje emitido paso-a-paso desde el receptor al emisor para reservación de ancho de banda.
.Path	-Mensaje emitido en forma regular para cada flujo de datos del emisor al receptor. No se enruta mediante RSVP para asegurar la llegada al receptor mediante las direcciones IP.
-Teardown	-Mensajes (*Path and Reservation*) usados para desarmar el camino y la reservación efectuada.
-Error	-Reporta errores en el procesamiento del mensaje *Path* o *Resv*.
-Resv Conf	-Mensaje emitido como respuesta al *Resv*.



3.2- PROTOCOLO DE TIEMPO-REAL (RTP) (*Real-Time Transport Protocol*).

Tanto el protocolo de transporte en tiempo-real RTP como el protocolo de control RTCP se encuentran disponibles en RFC-1889 del año 1996. El protocolo RTP tiene como objetivo asegurar una QoS para servicios del tipo tiempo-real. Incluye la identificación del payload, la numeración secuencial, la medición de tiempo y el reporte de la calidad (protocolo RTCP). Entre sus funciones se encuentran la memorización de datos, la simulación de distribución interactiva, el control y mediciones de aplicaciones.

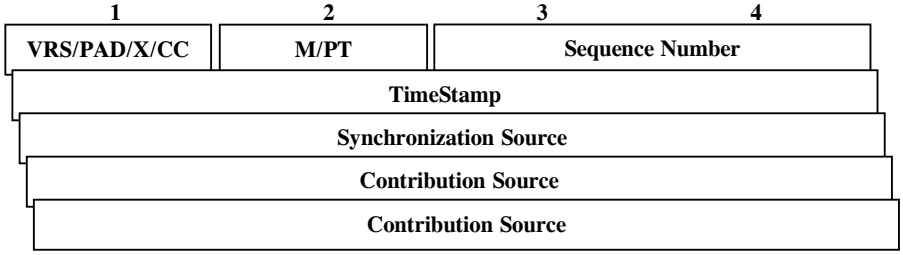
Este protocolo **RTP** es de transporte (capa 4) y trabaja sobre **UDP** de forma que posee un checksum para detección de error y la posibilidad de multiplexación de puertas (port UDP). Las sesiones de protocolo RTP pueden ser multiplexadas. Para ello se recurre a un doble direccionamiento mediante las direcciones IP y el número de port en UDP. Sobre RTP se disponen de protocolos de aplicación del tipo H.320/323 para vídeo y voz (H.32x forma una familia del ITU-T de normas para videoconferencia). El protocolo de H.323 se detalla entre los servicios de las redes IP. Junto a RTP se dispone del protocolo de control **RTCP**.

El RTP funciona en conjunto con **RSVP** (capa 3) para la reservación de ancho de banda y asegurar de esta forma la calidad del servicio QoS del tipo Garantizada. La QoS del tipo Diferenciada se logra mediante la priorización de tráfico que puede adoptar dos alternativas. En IP se pueden asignar diversos alternativas de prioridad para formar una cola de espera en routers. Un algoritmo particular de gestión de prioridad de tráfico es el **WFQ** (*Weighted Fair Queuing*) que utiliza un modelo de multiplexación TDM para distribuir el ancho de banda entre clientes. Cada cliente ocupa un intervalo de tiempo en un *Round-Robin*. El **ToS** (*Type of Service*) en IP puede determinar un ancho de banda específico para el cliente. Un servicio sensible al retardo requiere un ancho de banda superior. En IP además del ToS se puede utilizar la dirección de origen y destino IP, tipo de protocolo y número de *socket* para asignar una ponderación.

RTP además provee transporte para direcciones unicast y multicast. Por esta razón, también se encuentra involucrado el protocolo **IGMP** para administrar el servicio multicast. El paquete de RTP incluyen un encabezado fijo y el payload de datos; RTCP utiliza el encabeza del RTP y ocupa el campo de carga útil. Los campos del encabezado fijo del protocolo RTP se muestran en la **Tabla 05**.

Tabla 05. Protocolos para Tiempo-Real RTP (*Real-Time Protocol*).

-OH	2 Bytes de encabezado fijo para aplicaciones de identificación.
.VRS	2 bits. Es la versión del protocolo. Actualmente se utiliza la versión 2 (RFC-1889).
.PAD	1 bit. El bit de padding activo informa que luego del encabezado existen bytes adicionales (por ejemplo para algoritmos de criptografía).
.X	1 bit. Con el bit de extensión activado existe solo una extensión del encabezado.
.CC	4 bits. (*CSRC Count*). Identifica el número de identificadores CSRC al final del encabezado fijo.
.M	1 bit de *Marker*. La interpretación está definida por el perfil.
.PT	7 bits. (*Payload Type*). Identifica el formato de payload y determina la interpretación de la aplicación.
-SN	2 Bytes. (*Sequence Number*). Numera en forma secuencial los paquetes de RTP y permite la identificación de paquetes perdidos.
-TS	4 Bytes. (*TimeStamp*). Refleja el instante de muestreo del primer Byte en el paquete RTP. Permite el cálculo del tiempo y jitter en la red. Por ejemplo, en una aplicación de audio que comprime cada 160 muestras, el reloj se incrementa en 160 en cada bloque.
-SSRC	4 Bytes. (*Synchronization Source*). Identifica la fuente de sincronismo de forma que dos sesiones del mismo RTP tengan distinta SSRC.
-CSRC	Nx4 Bytes. (*Contribution Source*). Identifica la fuente que contribuye al payload contenido en el paquete. El valor de N lo da el campo CC.



RTP-HC (*Real-Time Protocol-Header Compression*). La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de RTP/UDP/IP a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los datagramas. (*RTP*). Como los servicios de tiempo-real generalmente trabajan con paquetes pequeños y generados en forma periódica se procede a formar un encabezado de longitud reducida que mejore la eficiencia de la red.

3.3- PROTOCOLO DE CONTROL RTCP (*Real-Time Control Protocol*).

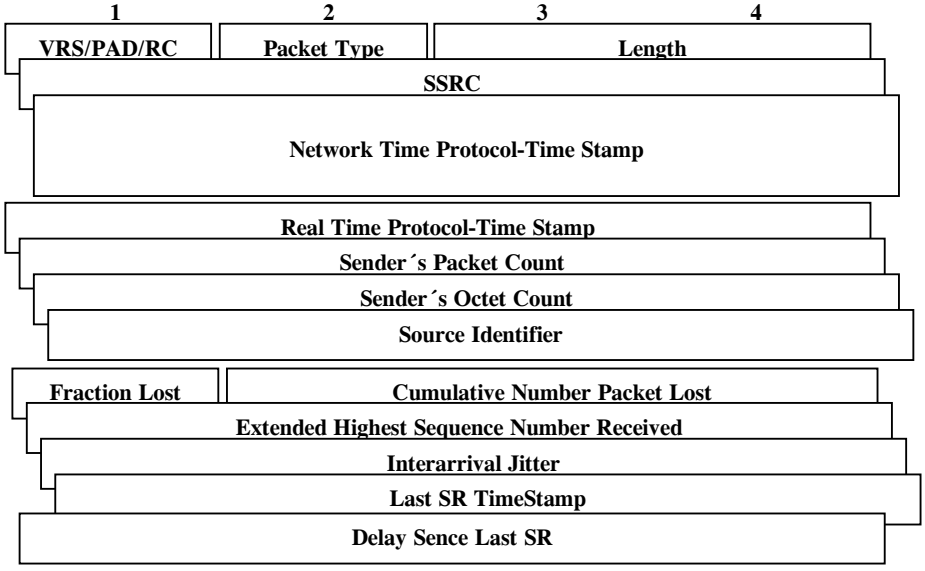
Este protocolo permite completar a RTP facilitando la comunicación entre extremos para intercambiar datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión. RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participante en la sesión usando el mismo mecanismo RTP de distribución de paquetes de datos. El protocolo UDP dispone de distintas puertas (*UDP Port*) como mecanismo de identificación de protocolos. La función primordial de RTCP es la de proveer una realimentación de la calidad de servicio; se relaciona con el control de congestión y flujo de datos.

RTCP involucra varios tipos de mensajes (uno de los más interesantes el *send report* se informa en la **Tabla 06**):

-*Send report*	para emisión y recepción estadísticas (en tiempo random) desde emisores activos.
-*Receiver Report*	para recepción estadísticas desde emisores no activos.
-*Source Description*	para un identificador de nivel de transporte denominado CNAME (*Canonical Name*).
-*Bye*	para indicar el final de la participación.
-*Application*	para aplicaciones específicas.

Tabla 06. Protocolo de control RTCP (*Real-Time Control Protocol*). Mensaje *Sender Report*.

	ENCABEZADO COMUN
-OH	1 Byte de encabezado con las siguientes funciones:
.VRS	2 bits. Identifica la actual versión (2) del protocolo.
.PAD	1 bit. Indica si luego de este paquete existe un padding adicional (por ejemplo, para completar el número de Bytes para criptografía en múltiplo de 8).
.RC	5 bits. (*Reception Report Count*). Contiene el número de bloques de reportes (unidades de 6x4 Bytes) que contiene el paquete. Un paquete puede contener más de un reporte de retorno.
-PT	1 Byte. (*Packet Type*). Identifica el tipo de paquete (decimal=200 para el paquete *Sender Report* que se enumera en este ejemplo).
-Length	2 Bytes. Indica la longitud del paquete en unidades de 4 Bytes.
-SSRC	4 Bytes. Identifica la fuente de temporización para el generador del reporte.
	INFORMACION PARA EVALUACION DE PARAMETROS
-NTP-TS	8 Bytes. (*Network Time Protocol-TimeStamp*). Es el tiempo relativo al UTC 00:00:00 horas del día 01-01-1900. Este campo de 8 Byte y es el *TimeStamp* completo. Para otras aplicaciones se utiliza una versión reducida de 4 Bytes con la información de tiempo más significativa.
-RTP-TS	4 Bytes. Se refiere al *TimeStamp* que es emitido en el RTP.
-SPC	4 Bytes. (*Sender´s Packet Count*). Es el total de paquetes emitidos por el transmisor desde el inicio de la sesión.
-SOC	4 Bytes. (*Sender´s Octet Count*). Es el total de Bytes transmitidos desde el inicio de la sesión como carga útil. Es usado para estimar la tasa de datos promedio de payload en conjunto con SPC.
	REPORTES DE PARAMETROS EVALUADOS
-SSRC-n	4 Bytes. (*Source Identifier*). Identifica la fuente SSRC de información en el reporte de recepción.
-FL	1 Byte. (*Fraction Lost*). Indica la relación fraccional (paquete perdido/total de paquetes) de paquetes perdidos desde el último reporte.
-CNPL	3 Bytes. (*Cumulative Number Packet Lost*). Indica el total de paquetes perdidos desde el inicio de la recepción.
-EHSNR	4 Bytes. (*Extended Highest Sequence Number Received*). Indica la numeración secuencial de recepción. Si el inicio de la recepción es distinto implica que los distintos posibles receptores (multicast) tienen un campo EHSNR diverso.
-IJ	4 Bytes. (*Interarrival Jitter*). El jitter se mide como la desviación de recepción respecto de la transmisión (en unidades de timestamp). Equivale a la diferencia de tiempo de tránsito relativo.
-LSR-TS	4 Bytes. (*Last SR TimeStamp*). Es el último *timestamp* (información más significativa) de los paquetes recibidos.
-DLSR	4 Bytes. (*Delay Since Last SR*). Es el retardo (entre la emisión y recepción) en unidades de 1/65536 seg del último paquete recibido.



El mensaje *Send Report* disponen de 3 secciones bien diferenciadas:
-Los primeros 8 Bytes (desde la versión hasta el identificador de la fuente de temporización SSRC) se refieren a un encabezado común.

-La segunda parte de 20 Bytes (desde el tiempo universal de emisión NTP-TS hasta el conteo de octetos emitidos SOC) permite la evaluación de diferentes parámetros (retardo, jitter, eficiencia de datos, etc).
-La tercera parte de 24 Bytes lleva reportes que han sido obtenidos desde el último reporte informado. Obsérvese la presencia de reporte referido a la cantidad total de paquetes RTP perdidos y a la proporción de los mismos; la cantidad de paquetes recibidos y el jitter entre paquetes; el horario del último paquete recibido y el retardo de transmisión del mismo.

La medición de tiempo se realiza mediante la emisión del **NTP-TS** (*Network Time Protocol-TimeStamp*) de 8 Bytes de longitud. Es el tiempo relativo al UTC 00:00:00 horas del día 01-01-1900. La precisión es de 32 bits a cada lado de la coma para el segundo. Como esto puede ser innecesario en diversas aplicaciones se utilizan variantes reducidas de Byte. Por ejemplo para la medición de jitter se utiliza unidades de 1/65536 seg (2^{16}).

El lector informado sobre redes ATM puede comparar este formato de RTCP con el utilizado en AAL5/ATM para reportes y mediciones de calidad de servicio (tasa de error, tasa de celdas perdidas, etc). La riqueza de lo proyectado en RTCP es sustancialmente superior.

1211

GESTION DE REDES RFC

Relativo a los protocolos de gestión disponibles en RFC. Sobre el ICMP para reporte de fallas en la red; el SNMP para management de componentes de la red y RMON para monitoreo remoto.

1- INTRODUCCION

Si bien la red Internet tiene su origen en el final de los `60, la difusión masiva se posterga hasta la divulgación de redes LAN en los `80. Solo a partir del año 1988 los host conectados a Internet han sufrido un incremento abrupto. También a la misma época se remonta la necesidad de la gestión de la red.

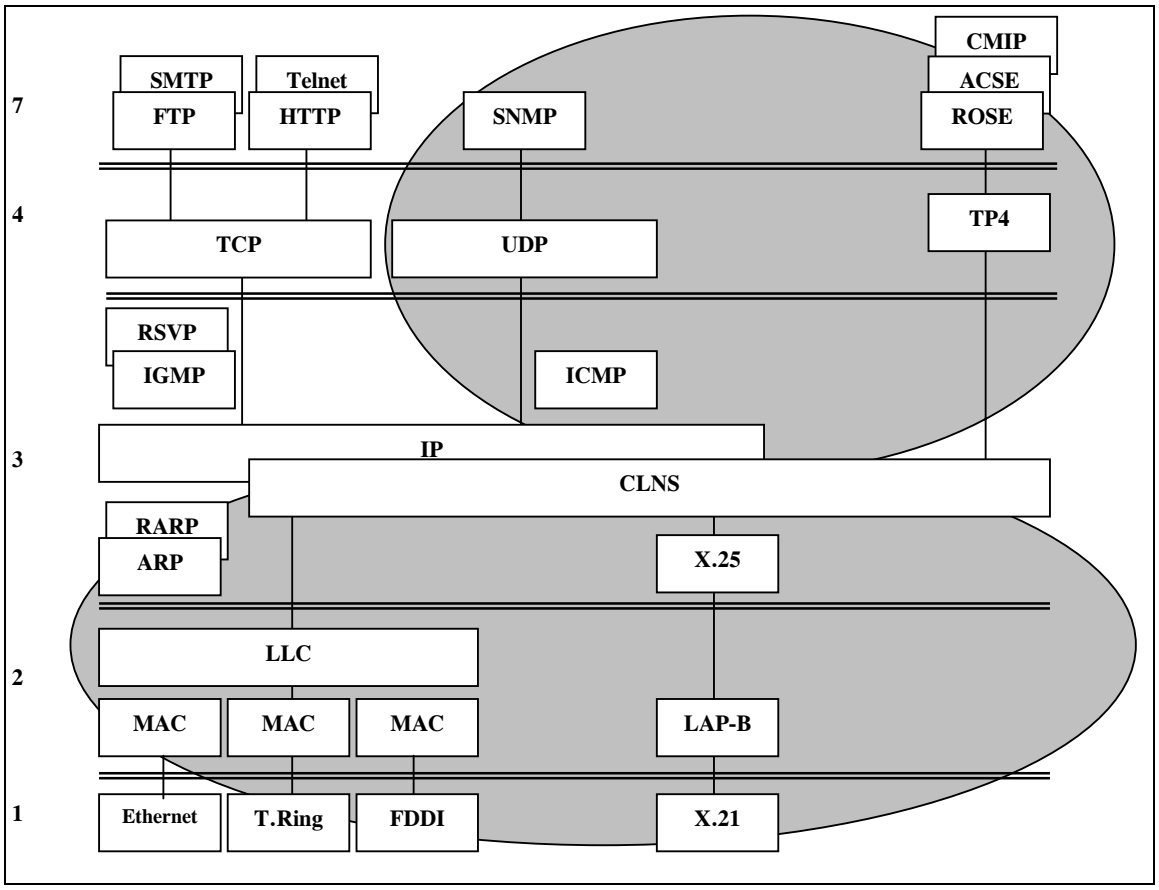


Fig 01. Modelo de capas de sistemas de gestión.

La **suite de protocolos** TCP/IP incluyen las capas de transporte, los protocolos de procesos de gestión de red. Estos últimos se tratan de ICMP y SNMP. La información que se debe disponer puede ser: estática (con cambios poco frecuentes como ser la configuración), dinámica (cambios de estado o volumen de transmisión de paquetes) y estadística (promedio de paquetes por hora o día). Las **motivaciones** para disponer de una gestión de la red son: el control del incremento de complejidad de la red, la mejora de servicios y el balance de necesidades. En la **Tabla 01** se detallan las funciones previstas para la gestión de redes.

En la **Fig 01** se observa la posición en el modelo de capas de los protocolos RFC (ICMP y SNMP) y los ITU-T (CMIP) para efectuar la gestión de redes. Obsérvese que los protocolos de capa 3 son IP y CLNS respectivamente. Ambos protocolos funcionan sobre redes LAN o líneas X.25.

Tabla 01. Funciones de la gestión de redes

Fallas	Permite detectar la localización de fallas, aislar partes de la red, correlacionar alarmas múltiples, administrar test de diagnóstico rutinarios y sobre la base de esto reconfigurar o modificar la red y reparar la falla.
Cobro	Se refiere a la determinación de costos de operación para cambiar procedimientos. Permite detectar el uso abusivo o ineficiente por parte de componentes de la red.
Configurar	Se trata de una comunicación hacia y desde los elementos de red. Permite el inventario, la asignación de recursos, la activación y el *back-up* para la restauración futura. La información sobre configuración describe la naturaleza y el estado de los recursos involucrados en la red. Incluye la descripción de atributos de los recursos físicos (hardware) y lógicos (software: circuitos virtuales, contadores, temporizadores, etc). La gestión de configuración puede realizarse mediante una lista de datos como en SNMP o mediante una base de datos orientado-al-objeto como en ISO.
Performance	Se pueden obtener indicadores de performance orientados al servicio (disponibilidad, tiempo de respuesta, porcentaje de segundos sin errores EFS) e indicadores orientados a la eficiencia (cantidad de eventos de transacción ocurridos -*Throughput*- y la utilización como porcentaje del recurso utilizado. Esta gestión permite la colección de estadísticas, cambiar parámetros, generar tráfico artificial, etc.
Seguridad	Permite la autentificación y control de acceso para protección contra intrusos no autorizados.

2- GESTION STANDARD RFC.

2.1- ICMP (*Internet Control Message Protocol*)

Es un protocolo que usa el protocolo IP para mensajes de estado entre host y gateway. El primer protocolo se definió en 1970. Cada mensaje se refiere a un datagrama anterior y constituye un canal de retorno (*Feedback*) para informe de estado y fallas en el canal de comunicación. Desde el punto de vista del modelo de capas ICMP utiliza el IP como soporte. El encabezado del protocolo IP lleva el parámetro de protocolo=1 para identificar al ICMP.

En esencia permite un canal de retorno para la detección de problemas en la red de comunicaciones; por ejemplo, cuando un datagrama no puede alcanzar el objetivo o cuando una gateway no dispone de un buffer suficiente. En general un mensaje ICMP se emite como respuesta a un datagrama. La descripción de los campos que constituyen el paquete de ICMP se dan en la **Tabla 02**.

Obsérvese que existe un encabezado fijo y otro variable que depende del tipo de mensaje.
Mediante una combinación de datagramas con distinto tiempo de vida TTL y los mensajes de *Time_Exceeded* es posible obtener la ruta seguida por los datagramas en la red. Cada datagrama es eliminado en un router distinto y se reporta un mensaje de error. Este proceso se denomina *IP Trace*.

IRDP (*ICMP Router Discovery Protocol*). Este protocolo utiliza mensajes de solicitud y aviso (*solicitation and advertisement*) para descubrir direcciones de router en la subnetwork conectado. Cada router en forma periódica emite mensajes de aviso tipo multicast desde cada una de sus interfaces. El host descubre la dirección del router de esta forma. El host también puede usar mensajes de solicitud para recibir el de aviso. IRDP tiene la ventaja que el host no requiere conocer protocolos de routing para reconocer al router.

2.2- SNMP (*Simple Network Management Protocol*)

SNMP (standard del IETF en RFC-1157) es un protocolo de la suite UDP/IP para soportar mensajes de control y gestión. Virtualmente todos los productores de host, workstation, bridge/router y hub ofrecen el protocolo SNMP como estándar. SNMP fue adoptado en 1989 en la versión 1 (en 1993 se adopta la versión 2). Comercialmente se encuentran distintas versiones: por ejemplo, NetView-6000 (trabaja sobre IBM RS-6000), HP OpenView (trabaja sobre una estación HP o Sun) y SunNet (trabaja sobre Sun SPARC). En la fotografía vecina se muestra la pantalla de gestión de routers en Uruguay.

SNMP dispone de un número limitado de órdenes para obtener información de los elementos de red. El modelo de capas ubica a SNMP en la capa de aplicación y utiliza mensajes de tipo **UDP** (*User Datagram Protocol*) en la capa de transporte. Se trata de un protocolo sin-conexión que dispone de la dirección decimal 161 en UDP. El encabezado UDP ocupa 4 campos de 2 Bytes cada uno y se identifica en la **Tabla 03**. También usa UDP el protocolo NFS.

SNMP funciona en forma de ***Polling*** donde la estación de gestión interroga en forma cíclica a cada elemento de la red. Sobre una red LAN del tipo Ethernet (funcionando a 10 Mb/s) con 400 elementos de red NE cada circuito de polling se realiza en 5 minutos y requiere un ancho de banda de 51,2 kb/s en promedio. Estos valores son distintos en una WAN, donde los tiempos de tránsito son mayores y el ancho de banda disponible es menor. Por ello en redes WAN el sistema de polling requiere una subdivisión en pequeñas redes. Una frecuencia de polling mayor alerta al sistema de gestión en forma más certera pero a cambio consume mayor ancho de banda.

Los objetos gestionados forman una base de datos denominada **MIB** (*Management Information Base*). Se denomina agente ***Proxis*** al que, usado por agentes que no soportan SNMP, realiza la traducción desde el protocolo propietario al estándar.

Tabla 02: Formato general del mensaje del protocolo de control ICMP.

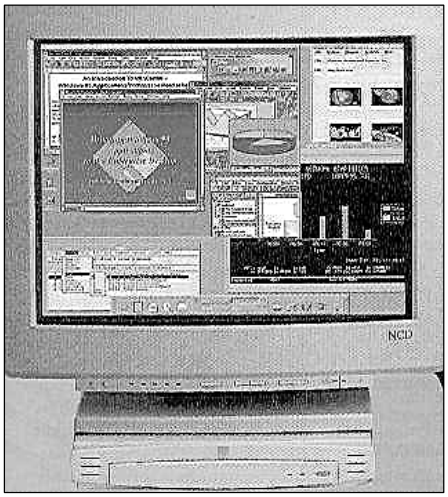
-Type	1 Byte. Identifica el tipo de mensaje en particular. Por ejemplo el mensaje *Time Exceeded* se identifica con el tipo 12 (decimal). Más abajo se encuentra la lista completa de mensajes.
-Code	1 Byte. Usado para parámetros que solo requieren pocos bits. En el caso del mensaje *Time Exceeded* este código toma dos estados: 0 cuando el TTL fue excedido en tránsito o 1 cuando fue excedido durante el proceso de reensamble.
-CS	2 Bytes. (*Checksum*) Para verificación de errores. Es del mismo tipo que IP.
-PAR	4 Bytes. En algunos tipos de mensajes no está usado; en otros es usado para parámetros de identificador y número secuencial. Cambia de acuerdo con el Type.
-Message	N Bytes. Es el mensaje de control propiamente dicho. En la mayoría de los casos (por ejemplo en el mensaje *Time Exceeded* este campo lleva los 20 Bytes de encabezado IP del datagrama descartado más 8 Bytes de la carga útil del mismo datagrama. Esto permite obtener el número de port si el protocolo es TCP/UDP.
	TIPO DE MENSAJES DE CONTROL
Echo Requ/Reply	Se trata de los mensajes *Echo Request* y *Echo Reply*. En el sistema operativo UNIX el diagnóstico se efectúa mediante el **PING** (*Paket Internet Groper*). Se emite el mensaje de *Echo Request* y se espera como respuesta el *Echo Reply*. Prueba la comunicación entre entidades IP. Sirve para el análisis de problemas de redes y verifica que la máquina esté encendida y operando, además de testear el estado del enlace.
Unreachable.	Se trata del mensaje *Destination_Unreachable*. Un Router puede retornar al origen un mensaje por encabezado incorrecto o fragmentación equívoca. Indica destino no es alcanzable: entre ellos la Red, el Host, el protocolo SAP, la puerta TCP, etc.
Source_Quench.	Este datagrama identifica a los router que no disponen de suficiente memoria para la cola de espera. Permite detectar las fuentes apagadas para evitar el envío de datos y efectuar un control de flujo. Impide la existencia de datagramas en la red de destinos no alcanzables.
Route_Change	Algunos Router pueden generar un datagrama para informar que no son la vía correcta de ruta. Se requiere un cambio de ruta mediante *Route_Change_Request* (también indicado como mensaje *Redirect*).
Time_Exceeded	Indica el descarte de un datagrama por final del tiempo de vida TTL en IP. Un rescarte de datagramas puede indicar un seteado bajo de TTL para el número de Router en red. El mensaje informa si el TTL ha expirado en el tránsito del datagrama o durante el proceso de ensamble final.
Parameter	*Parameter_Problem_Message* indica problemas de parámetros por error de sintaxis o semántica en el datagrama.
TimeStamp	Se trata de los mensajes *Time_Stamp_Request & Time_Stamp_Replay*. Al mensaje *Request* se responde con el *Replay*. Permite medir el retardo en la transmisión en la Internet y adaptar la tabla de ruta en el Router. a medición de tiempo se realiza mediante la emisión del **NTP-TS** (*Network Time Protocol-TimeStamp*) de 4 Bytes de longitud. Es el tiempo relativo al UTC 00:00:00 horas del día 01-01-1900. La precisión es de 32 bits a cada lado de la coma para el segundo. Como esto puede ser innecesario en diversas aplicaciones se utilizan variantes reducidas de Byte. Aquí se utilizan solo 4 Bytes. En este caso el campo de mensaje ocupa 2x4 Bytes en total: 4 Bytes para indicar el *TimeStamp* del mensaje original; otros 4 Bytes para indicar el *TimeStamp* de recepción y los últimos 4 Bytes para indicar el *TimeStamp* de transmisión.
Information	Los mensajes *Information_Request.& Information_Replay* permiten descubrir la dirección de red de IP o de port en TCP/UDP.
Address Mask	*Address_Mask_Request & Address_Mask_Replay* permiten descubrir la dirección en una sub-red. La máscara de dirección IP se refiere a la identificación del host. Por ejemplo, en una dirección clase B (168.23.4.1) los dos primeros bytes corresponden a la identificación de red, el tercero a la identificación de sub-red y el último identifica al host. La máscara de dirección IP identifica la dirección del host dentro de la dirección IP, por ello es: 255.255.255.0.

COMPONENTES DE UNA RED SNMP. Los distintos componentes de una red SNMP son los siguientes:
-Elemento de red **NE** (*Network Element*). Es el hardware (computadora, servidor, router, etc) bajo observación.
-Agente. Es el módulo de software que reside en el NE y que guarda la información de gestión.
-Objeto gestionado. Es una característica que puede ser gestionada en el agente (por ejemplo puertas TCP activas).
-Variable. Es el valor instantáneo de un objeto gestionado.
-Base de información de datos **MIB**. Colección de objetos gestionados en el NE.
-Notación sintáctica. Lenguaje utilizado para escribir el MIB (por ejemplo, ASN.1).
-Estación de gestión de red. Es la conocida consola de gestión.
-Protocolo de management. Propiamente dicho el protocolo SNMP que permite la comunicación entre la consola y los NE.

Tabla 03: Campos de información de UDP (capa 4) y SNMP.

	Protocolo UDP.
-SP	2 Bytes. Identifica al número de puerta de origen del mensaje.
-DP	2 Bytes. Identifica al número de puerta de destino del mensaje.
-Length	2 Bytes. Determina la longitud total del datagrama UDP.
-Check	2 Bytes. Es un *Checksum* para control de errores del mensaje completo.
	Protocolo SNMP.
-VRS	Se trata del identificador de la versión del protocolo.
-COM	(*Community String*) Define el nivel de autentificación para leer o escribir información en el MIB
-PDU	Se trata de 5 tipos de mensajes de operaciones (Get, Next, Set, Get Response, Tap).
.Type	Identifica el tipo de PDU entre las 5 alternativas.
.Req	Identifica al destino y al origen.
.Error	Responde al requerimiento de *status* e *index*.
	Mensajes de control del protocolo SNMP.
Get_Request	Usado por el manager SNMP para obtener información de gestión desde el MIB del agente SNMP. SNMP utiliza un mecanismo de Polling entre *server* (*manager*) y *client* (agente).
GetNext_Request	Utilizado para requerir información desde una tabla MIB que no se conoce el *Entry*. No requiere especificar el MIB.
Get Response	Usado por el agente SNMP para responder a Get_Request; GetNext_Request y Set_Request.
Set_Request	Usado por el manager SNMP para modificar datos de gestión en el MIB.
Trap	Usado por el agente SNMP para notificar un evento no solicitado. Contiene solo algunos datos limitados para describir un problema. No existe reconocimiento y por ello no se tiene la garantía de recepción de un Trap.

LA CONSOLA DE GESTIÓN. El protocolo SNMP funciona con el sistema operativo UNIX (por ejemplo HP-UX A.09.05, versión de HP para UNIX) y visualización Xwindow (HP OpenView 3.3). Se trata de una interfaz gráfica tipo window que opera con el criterio cliente-servidor para clientes remotos.



Ha sido desarrollado por el MIT (RFC-1013) y permite X-Terminal remotos que utilizan TCP/IP en capas 4/3 y a nivel de enlace de datos el protocolo PPP o X.25. El hardware que soporta este sistema operativo es el sistema HP9000 (serie 700 y 800) y Sun SPARCstation; con 1 GB de hard disk y 64 MB de RAM.

La plataforma de aplicaciones que envuelve a SNMP puede ser el HP OpenView. Las funciones de esta consola son:
-Obtener la topología de la red.
-Detectar fallas, alarmas y diagnosticar problemas.
-Controlar el tráfico y la congestión.
-Generar informes, registros históricos y análisis de tendencias.

El operador dispone también del analizador de protocolo. Sirve para el diagnóstico y seguimiento de la actividad de la red. Es un software que trabaja sobre una computadora y realiza las siguientes actividades:
-Realiza una estadística de paquetes, volumen de tráfico y congestión de la red.
-Prueba los enlaces de comunicación de todos los nodos.
-Verifica alarmas y problemas de software de aplicación.

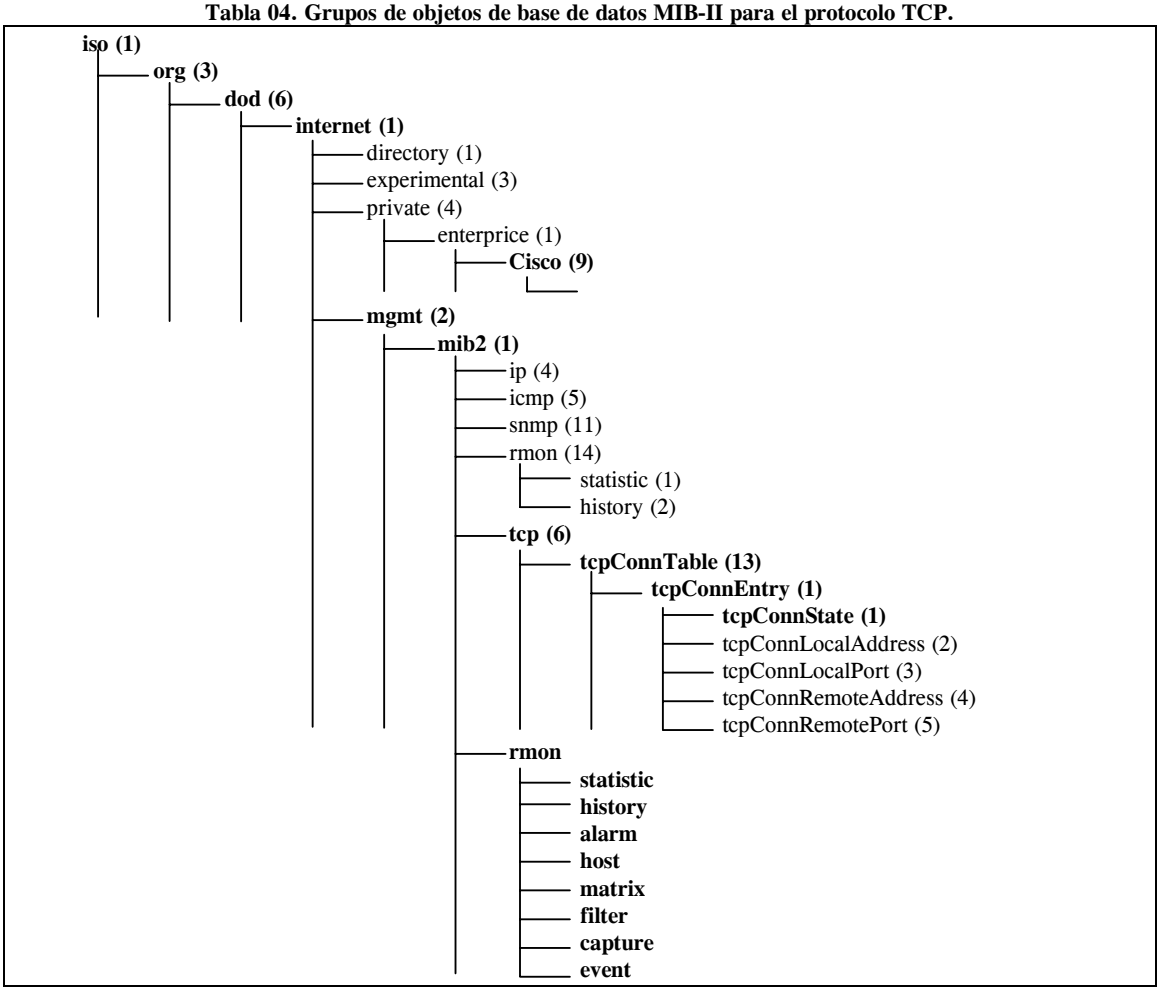
BASE DE DATOS MIB. Es una representación lógica de una entidad física que contiene: nombre, propiedades y atributos. En SNMP es una simple lista de datos escalares que pueden formar tablas. Cada objeto del MIB se define usando la notación abstracta **ASN.1** (*Abstract Syntax Notation One*) de la norma **ITU-T X.208**. Tiene similitud con el lenguaje de programación C o Pascal. En la **Tabla 04** se muestra un sector del MIB-II para el protocolo TCP en la línea tcpConnTable.

El **MIB-II** (RFC-1158) permite construir tablas de conexiones en TCP como la que se muestra anexa. Para cada conexión realizada se identifica el estado, las direcciones IP y las puertas TCP. Por ejemplo la secuencia de números 1.2.6.1.2.1.6.13.1.2 identifica en la conexión TCP a la dirección IP de origen (tcpConnLocalAddress).

Tabla. Ejemplo de direcciones IP y puertas TCP.

	tcpConnState	*TcpConnLocalAddress*	*tcpConnLocalPort*	*tcpConnRemoteAdd*	*TcpConnRemotePort*
tcpConEntry	5	10.0.0.99	12	9.1.2.3	15
	2	0.0.0.0	99	0	0
	3	10.0.0.99	14	89.1.1.42	84

Tabla 04. Grupos de objetos de base de datos MIB-II para el protocolo TCP.



LIMITACIONES DE SNMP. El protocolo original SNMP se realizó de manera muy simplificada de forma que se pueden detectar varias limitaciones. A cambio, debido a la simplicidad, ha tenido un éxito muy amplio. Sus deficiencias son:
-Utiliza un mecanismo de *Polling* para interrogar lo cual es limitativo para grandes redes (modelo *client-server*).
-El mensaje *Trap* pretende reducir esta limitación al permitir una notificación no requerida.
-Sin embargo, Trap no dispone de reconocimiento y no se está seguro que se ha recibido.
-No es útil para transferir gran número de datos como ser una tabla de rutas.
-El sistema de seguridad es elemental (dispone de autentificación trivial). Es útil para monitoreo más que para control.
-No soporta comandos imperativos. Actúa seteando objetos en el MIB remoto.
-No soporta la comunicación manager-to-manager.

En la versión **SNMPv2** se han introducido las siguientes mejoras sobre la versión 1:
-Introduce nuevos tipos de datos mediante el **SMI** (*Structure Management Information*).
-Introduce la capacidad manager-to-manager para la arquitectura de gestión distribuida.
-El protocolo de operación agrega los comandos:
  .*GetBulkRequest* para habilitar la emisión de gran volumen de datos.
  .*InformRequest* para habilitar la emisión de Trap desde un manager a otro.
-Mejora las condiciones de seguridad. Se aplica autentificación, criptografía, *scrambler*.

2.3- RMON *(Remote Network Monitoring).*

Este protocolo tiene la versión **RMON1** en RFC-1271 del año 1991. RMON1 consiste en el uso de un agente remoto para colectar información de gestión bajo demanda. Se diseñó para redes LAN Ethernet (posteriormente para Token Ring) y entrega las funcionalidades de los analizadores de redes y protocolos.

Opera *Off-Line* recolectando información sin *polling* de entrada y puede generar un trap de SNMP. Puede correr programas de diagnóstico y performance para entregar informes de fallas. Puede además detectar problemas en forma pasiva sin intervenir la estación principal. Permite visualizar la actividad en redes remotas. Puede además ser accedido desde varios centros de gestión.

COMPONENTES. La implementación consiste en una configuración *Client/Server*. El cliente es el equipo que presenta la información al usuario de la red de gestión. El servidor es el equipo que en forma remota reune la información y análisis de paquetes; se lo denomina *Probe* y desarrolla el programa de software denominado *RMON-Agent*. El agente-RMON está embebido generalmente en los switchs y routers. El protocolo de comunicación es el SNMP. Los datos son coleccionados y procesados en el servidor remoto de forma que se reduce el tráfico SNMP en la red de datos. De esta forma un segmento de red LAN es gestionable desde cualquier lugar de la red.

La mejora que se ha introducido sobre SNMPv1 se relaciona con la base de datos MIB del RMON. En el MIB se dispone de 9 grupos con las funciones que se indican en la **Tabla 04/05**.

Con posterioridad, en 1994, aparece el **RMON2**. El objetivo es entregar estadísticas sobre las capas de red y aplicación; es decir, extender el monitoreo de tráfico a las capas superiores (capas 3 a 7). Es decir, en tanto RMON1 opera sobre LAN (capa 2) el RMON2 opera sobre las capas superiores. Con el incremento de las estadísticas de tráfico la potencia del procesador CPU y la capacidad de la memoria del agente se han incrementado. Sobre RMON2 se disponen de dos tipos soluciones: el tipo A ocupa memos memoria que el tipo B. El tipo A realiza funciones de *Statistics/Host/Matrix* sobre la capa 3 y *Statistic* solo en la capa de aplicación; el tipo B realiza las 3 funciones en las capas de red y aplicación.

Tabla 05. Funciones del protocolo RMON (*Remote Network Monitoring*).

-Statistics.	Provee estadísticas desde una red, hub de LAN o usuario. Por ejemplo, la cantidad de errores en una puerta específica.
-History.	Forma la historia de las estadísticas anteriores. Es útil para establecer la actividad en la red.
-Alarm.	Entrega un mecanismo de selección para el seteo de umbrales o intervalos para enviar *Trap*.
-HostTable Group.	Soporta estadísticas de tráfico para la red, hub o usuario.
-HostTopNTable.	Soporta estadísticas del host para tabla de direcciones.
-TrafficMatrixGroup	Indica el tráfico en una matriz para cada par de estaciones.
-Filter.	Provee un filtro programable para datos, contador o para ejecutar eventos.
-PacketCaptura.	Captura paquetes de acuerdo con el criterio seleccionado en el *Filter*.
-Event.	Crea entidades, envía alarmas y ejecuta acciones.

1212

PROTOCOLOS DE GESTION ISO/ITU

Relacionado con los protocolos para la gestión de redes de las normas ISO/ITU-T. Sobre el protocolo CMIP y ejemplos de aplicación para las redes de transporte sincrónico.

1- STANDARD ISO/ITU-T

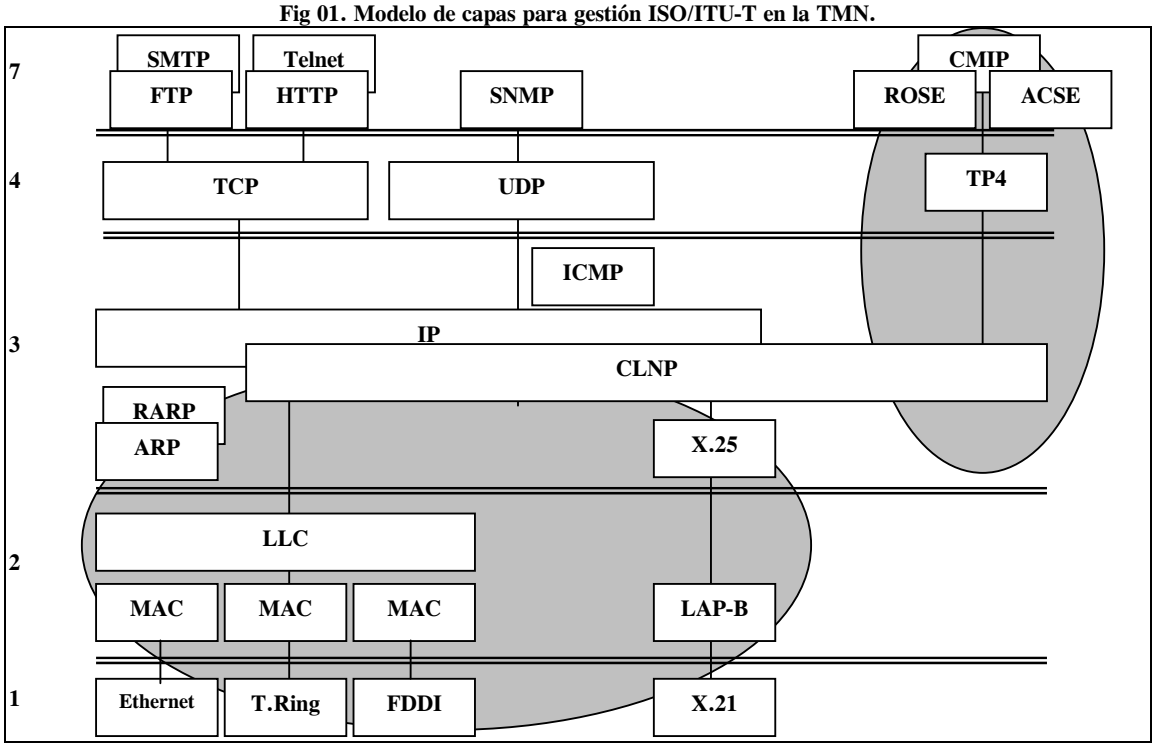
1.1- FUNCIONES GENERALES

En la **Tabla 01** se detallan las funciones previstas para la gestión de redes. En la **Fig 01** se observa la posición en el modelo de capas de los protocolos RFC (ICMP y SNMP) y los ITU-T (CMIP) para efectuar la gestión de redes. Obsérvese que los protocolos de capa 3 son IP y CLNS respectivamente. Ambos protocolos funcionan sobre redes LAN o líneas X.25.

Tabla 01. Funciones de la gestión de redes

Fallas	Permite detectar la localización de fallas, aislar partes de la red, correlacionar alarmas múltiples, administrar test de diagnóstico rutinarios y sobre la base de esto reconfigurar o modificar la red.
Cobro	Se refiere a la determinación de costos de operación para cambiar procedimientos. Permite detectar el uso abusivo o ineficiente por parte de componentes de la red.
Configurar	Se trata de una comunicación hacia y desde los elementos de red. Permite el inventario, la asignación de recursos, la activación y el *back-up* para la restauración futura. La información sobre configuración describe la naturaleza y el estado de los recursos involucrados en la red. Incluye la descripción de atributos de los recursos físicos (hardware) y lógicos (software: circuitos virtuales, contadores, temporizadores, etc). La gestión de configuración puede realizarse mediante una lista de datos como en SNMP o mediante una base de datos orientado-al-objeto como en ISO.
Performance	Se pueden obtener indicadores de performance orientados al servicio (disponibilidad, tiempo de respuesta, porcentaje de segundos sin errores EFS) e indicadores orientados a la eficiencia (cantidad de eventos de transacción ocurridos -*Throughput*- y la utilización como porcentaje del recurso utilizado. Esta gestión permite la colección de estadísticas, cambiar parámetros, generar tráfico artificial, etc.
Seguridad	Permite la autentificación y control de acceso para protección contra intrusos no autorizados.

Fig 01. Modelo de capas para gestión ISO/ITU-T en la TMN.



1.2- PROTOCOLOS DE COMUNICACIÓN.

La **ISO-7498** y **ITU-T-X.700** han determinado un modelo de arquitectura generales de estándar para la gestión de redes. En particular dan lugar a la red de management de telecomunicaciones **TMN**. En la **Tabla 02** se elencan los protocolos definidos en las normas ISO relacionados con funciones de gestión de redes. En particular los protocolos de capa superior **CMIP/CMIS** tienen los mensajes que son indicados en la misma Tabla.

Tabla 02. Protocolos de management para las normas ISO e ITU-T.

-SMAP	(*System Management Application Process*). Es el software local responsable de la gestión. Puede ser coordinado con SNMP. Permite normalmente una visualización en formato Windows (*Open View*).
-CMIP	(*Common Management Information Protocol*). Protocolo a nivel de aplicación para comunicación entre funciones CMIS.
-CMIS	(*CMI Service*). ISO-9595. Los servicios definidos en CMIS se efectúan mediante el protocolo de comunicación CMIP. Permite cambios de atributos o estado de objetos y recibe reportes (*Trap*). Opera sobre los protocolos ACSE y ROSE en la misma capa 7. Ver la **Tabla N5-05**.
-ACSE	(*Association Control Service Element*). ISO8649. ACSE permite iniciar y terminar una conexión entre 2 aplicaciones (capa 7).
-ROSE	(*Remote Operation Service Element*). ISO 9072. ROSE permite realizar una operación en otro sistema (origen *invoker* y recipiente *performer*). Además informa de la misma (resultado o informe de error en la transacción). El protocolo ROSE es original de 1984 (X.229) para mail **MHS** (*Message Handing System* X.410). Luego se aplicó para transferencia de archivos **FTAM** (*File Transfer and Access Management*) y CMIP.
-LME	(*Layer Management Entity*). Lógica incorporada a cada capa del modelo para permitir la gestión de la red. Estas entidades se encuentran distribuidas.
-**MIB**	(*Management Information Base*). Colección de información que cada nodo entrega a la gestión de la red. MIB obtiene información de cada capa del modelo. Utiliza la técnica orientada-al-objeto **OOD** (*Object Oriented Design*) que data desde los años 70. En 1983 se crea el lenguaje *Small-Talk* para comunicar objetos sin conocer su operación interna. Consiste en definir Objetos abstractos cuyas características dinámicas se modelan con un Comportamiento. Se define al objeto gestionado en términos de atributos que son una variable a la cual se le asignan valores. Los valores son: características operacionales, estado corriente, condiciones de operación, etc. El objeto gestionado se describe mediante su comportamiento (*Behavior*). En una red real la función completa envuelve la interacción de todos los objetos asociados. La totalidad de los objetos se la conoce como base o modelo de datos MIB. La programación orientada-al-objeto se asocia con mejoras de calidad y productividad del software. Las fases de construcción del software son: -Análisis: identificar los requerimientos del sistema; -Diseño: Identificar objetos; asignar funciones y datos (atributos); -Clasificar objetos y jerarquías e implementación con lenguaje CHILL; -Integración (de los componentes de software) y prueba del sistema.
	CMIS/P (*Common Management Information Service/Protocol*).
Event-Report	Permite reportar un evento desde un manager a otro. Es una indicación asincrónica de eventos importantes y lleva la información necesaria para reconocerlo. Puede ser confirmada la recepción de Event_Report.
Get	Requiere un reporte desde un manager a otro. Es un servicio confirmado. Esta formado por una lista de pares de valores-atributos.
Set	Requiere un seteo (modificación de información de gestión) de otro usuario. Tiene previsto el reemplazo de valores, la adición o borrado de valores y seteo al valor de *default*. Es un servicio confirmado o no-confirmado. En el caso confirmado se reporta el resultado. Se tienen disponibles distintos tipos de reportes de fallas: error, inválido, no soportado, no reconocido.
Action	Requiere una acción en otro usuario. Es un servicio confirmado o no-confirmado.
Create	Requiere que se cree un componente en el objeto de gestión. Es un servicio confirmado.
Delete	Requiere que se borre un componente en el objeto. Es un servicio confirmado.
Cancel_Get	Cancela un get previo cuando el envío de información es excesiva. Es un servicio confirmado.

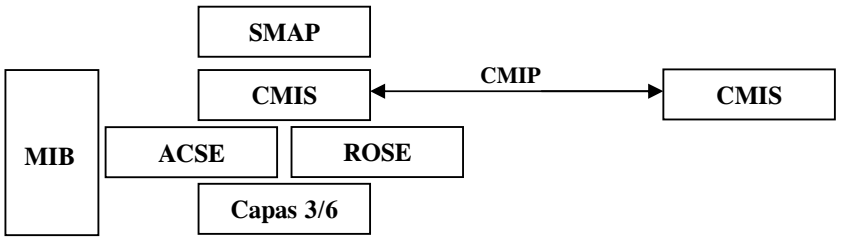
1.3- ARQUITECTURA DE LA TMN

La arquitectura típica de la TMN se remonta a 1988. La definición se encuentra en **ITU-T M.30** desde 1988. A partir de 1992 adopta el modelo de la Serie X.700 en **ITU-T M.3000**. Los componentes de la red TMN se elencan en la **Tabla 03**.

Tabla 03. Componentes de la TMN.

-NE	(*Network Element*). Los elementos de red poseen hacia el exterior las interfaz F y Q. Los distintos componentes de la red permiten acceder a una interfaz para mensajes de TMN mediante un canal **DCC** (*Data Communications Channel*) entre distintos elementos de red NE y una **interfaz Q** que permite la conexión de un sistema de operaciones (gestión exterior). Se dispone además la **interfaz F** adaptada para la conexión de una estación de trabajo PC (sistema operativo DOS, OS o UNIX) a cualquier elemento de la red para la configuración de la misma. Se disponen de las siguientes interfaces de conexión: -Canal de Comunicación de Datos **DCC** entre **NE**; -Interfaz de operaciones **F** hacia una PC; -Interfaz de Red Local de Comunicación **Q2**; -Interfaz de red TMN **Q3**.
-F	Interfaz F. Corresponde a una conexión hacia el terminal de operaciones (PC) mediante una salida ITU-T V.24 (RS-232) a 9,6 o 19,2 kb/s (conector tipo-D, de 9 pin). El diagrama de capas para una Interfaz F incluye los niveles de aplicación -capas 4 a 7- con protocolo propiedad del productor.
-QA	(*Q Adapter*). El adaptador de interfaz Q permite adaptar un elemento de la red NE ya existente a la TMN que se introduce. Téngase en cuenta que la interfaz Q3 es normalizada y la Qx es propietaria (protocolo interno de un fabricante).
-Q2	Interfaz de red Q2. Conecta al elemento de red con el elemento de mediación. La Capa 1 se trata de un bus o anillo, dúplex o semidúplex, mediante pares apantallados balanceados de 120 ohm (interfaz V.11). La velocidad es de 19,2 a 64 kb/s en código NRZ Invertido. La Capa 2 determina el protocolo LAP-B de X.25 con un 1 byte de direcciones. El campo de información tiene una longitud máxima de 128 o 256 Byte.
-**Q1/Q2/Q3**	La interfaz Q1/Q2 se indican en **ITU-T G.771** y Q3 en la **Q.513**. En **G.773** se identifican las capas del modelo ISO para la interfaz de red Q3. Existen 5 variantes para Q3 propuestas y denominadas A1/A2/B1/B2/B3. La variante **Q3/B2** se usa para comunicación con protocolo X.25 mientras que la variante **Q3/B3** se usa para una salida LAN Ethernet (la LAN pertenece al sistema de operación). La **Interfaz Física** es del tipo semidúplex con 2 pares balanceados uno en cada sentido de transmisión. La velocidad será de 19,2 o 64 kb/s con código NRZ Invertido. La capa 2 se determina en base a **ITU-T X.25 (LAP-B)** para la transferencia de datos por paquetes (interfaz y conector V.11/X.21) en **Q3/B2**. En el caso de **Q3/B3** se trata de la **IEEE 802.2** para la red de área local LAN tipo CSMA/CD (Ethernet). La capa 3 se encuentran conforme a **X.25** en Q3/B2 y a **ISO-8473** en el segundo. Se adopta, para X.25, el funcionamiento en módulo 8 y módulo 128 como opcional. La longitud máxima por trama es de 131 y 256 Byte.
-**M**	Elemento de Mediación. Permite la conexión entre el elemento de red y el sistema de operaciones mediante un canal de comunicación de datos normalizado. El proceso de mediación involucra las siguientes funciones de comunicación entre el elemento de red y el sistema de operaciones: -Control de la comunicación: interrogación secuencial para recopilación de datos, direccionamiento y encaminamiento de mensajes, control de errores; -Conversión de protocolos y tratamiento de datos: concentración de usuarios, compresión y recopilación de datos, formateo y traducción de información; -Transferencia de funciones: secuencición y eventual envío de alarmas, reporte de los resultados de las pruebas, carga de informes de estado; -Proceso para toma de decisiones: fijación de umbrales de alarma, encaminamiento de datos, funciones de seguridad, y selección de circuitos; -Almacenamiento de datos: configuración de redes, copia de memorias, identificación de equipos, etc.
-**OS**	Sistema de operaciones. Se trata de componentes informáticos para el proceso y presentación de la información. Está constituido por una o varias estaciones de usuario donde el Hardware es: -Sistema controlador (workstation): capacidad de memoria RAM (256 MBytes); -Monitor color: resolución (1280x1024 pixels de 256 colores); -Disco de memoria: sistema operativo UNIX y el software (4 GBytes); -Conexión a LAN (Ethernet a 10 Mb/s): interfaz Q3/B3 para varias gateway de red; -Impresora (salida RS-232-C a 9600 b/s).

1.4- ARQUITECTURA DEL SOFTWARE



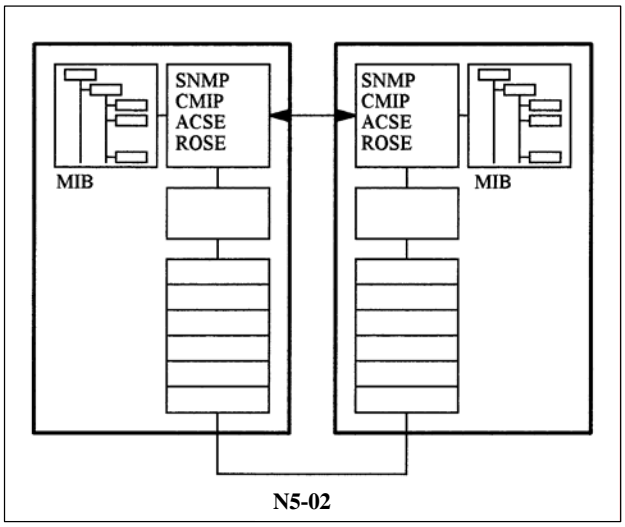
Se define un modelo de 7 capas para la TMN. Las inferiores se han detallado en la **Tabla 02**. Las capas complementarias son las siguientes:
-Capa de Transporte (capa 4/ISO 8073): clase de servicio, retransmisión de datos.
-Capa de Sesión (capa 5/ITU-T X.215): aceptación, rechazo, desconexión, aborto, transporte y segmentación.
-Capa de Presentación (capa 6/ITU-T X.216/226): reglas de codificación para sintaxis de transferencia.
-Capa de Aplicación (capa 7/ITU-T X.217/227): sintaxis abstracta (protocolos CMIP y ROSE).

Las funciones generales de la TMN son:
-Transporte de información entre distintos elementos;
-Almacenamiento de la información;
-Seguridad para garantizar un control de acceso;
-Consulta para permitir el acceso a la información;
-Tratamiento para permitir el análisis;
-Soporte para garantizar la entrada/salida de datos.

Dichas funciones se estructuran en 4 niveles (es decir, cada tipo de gestión se realiza en estratos diferentes) de acuerdo con **ITU-T M.3010**:

-**BML**	(*Business Management Layer*). Gestión del sistema para modelos de largo plazo, servicios y tarifas.
-**SML**	(*Service ML*). Gestión del servicio para la administración de órdenes de servicio.
-**NML**	(*Network ML*). Gestión de red para gestión de alarmas, tráfico, performance y configuración de la red.
-**EML**	(*Element ML*). Gestión del elemento de red para alarmas, tráfico, performance y configuración del equipo.

De esta forma la función de gestión de averías en el elemento de red es detectar alarmas, las cuales son "filtradas" (seleccionada de acuerdo con prioridad y origen) en la gestión de avería de red y presentadas en la gestión de avería de servicio. Un ejemplo más detallado de la gestion TMN aplicada a las redes de transporte SDH se puede encontrar en el Capítulo correspondiente (ver la fotografía anexa).



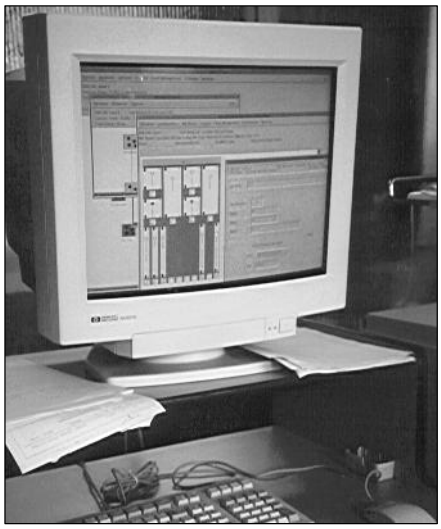


Fig 02. Modelo de capas y sistema de gestión para TMN.

2- EJEMPLOS

2.1- GESTION DE RED SDH

Se hace referencia al sistema de gestión **EM-OS** (*Equipment Management Operation System*) de *Siemens*. Los componentes que constituyen la red de gestión SDH son los siguientes:

1- UNIDAD DE CONTROL. Un equipo de la red SDH (multiplexor Add-Drop, terminal de línea óptica o radioenlace, Cross-connect, etc) puede visualizarse como una serie de unidades con distintas misiones y funciones. La unidad de control mantiene actualizada la base de datos del equipo y permite la comunicación con el operador del Terminal Local. Sus funciones en particular son:
-Comunicación con las distintas unidades del aparato.
-Actualización de la Base de Datos. En esta base de datos se sostiene la información de alarmas, configuración, reportes de performance, etc.
-Comunicación con el terminal local PC. Esto permite realizar las operaciones de gestión local desde una PC.
-Comunicación con la Unidad de Gestión de red TMN.

2- TERMINAL LOCAL. La interfaz F permite comunicar al equipo con una PC (*Notebook* o *Laptop*) exterior de forma tal que pueden realizarse funciones de programación local. Esta función es necesaria en la configuración inicial del equipo cuando aún no se han ingresado los parámetros de comunicación de red (direcciones MAC, NSAP e IP) que permiten la conexión remota. Las funciones son:
-Interfaz de conexión F. Corresponde a una conexión hacia el terminal de operaciones (PC) mediante una salida ITU-T **V.24** (similar a RS-232) a 9,6 o 19,2 kb/s. Se trata de un conector tipo-D de 9 pin (DB-9).
-Software de aplicación. Permite realizar casi las mismas funciones que la gestión TMN.
-El software disponible mediante el terminal local es suficiente para operar una red de equipos pequeña.

3- UNIDAD DE GESTION. Para efectuar las funciones de gestión remota TMN se requiere de una unidad de gestión que procesa los protocolos de comunicación apropiados (normas ISO para la TMN). Esta unidad puede ser la misma o distinta a la unidad de control. Realiza las siguientes funciones:
-Proceso de comunicación entre estaciones mediante el canal DCC embebido en la trama STM-1.
-Interfaz Q de conexión al exterior. Normalmente se trata de una red LAN-Ethernet.
-Interfaz hacia otros equipos idénticos de la misma estación.

4- COMUNICACIÓN ENTRE ESTACIONES. La comunicación entre los equipos que forman un enlace SDH ubicados en distintas estaciones se realiza mediante un canal de comunicaciones dedicado en la trama STM-1. Dicho canal se llama **DCC** (*Data Communication Channel*). Las características de esta comunicación son las siguientes:
-Se disponen de dos canales de datos embebidos en el encabezamiento SOH de la trama STM-1.
-El modelo de capas para el stack de protocolos se encuentra determinado en ITU-T **G.784**. En la Capa 2 se adopta el protocolo HDLC **LAP-D** usado en el sistema de señalización DSS1 para usuarios de la ISDN. En la Capa 3 se adopta el protocolo de la norma **ISO 8473** (**CLNP**). La capa 4 de Transporte es **ISO 8073** (TP4) y realiza funciones de retransmisión de datos. La capa 5 de Sesión ITU-T **X.215** (kernel dúplex) permite realizar las funciones de aceptación de conexión, rechazo y desconexión, aborto, transporte y segmentación. La capa 6 de Presentación ITU-T **X.216**/226 (kernel ASN.1) entrega las reglas de codificación para sintaxis de transferencia. La capa 7 de Aplicación utiliza las normas ITU-T **X.217** (ACSE), **X.219** (ROSE) y **ISO 9595** (CMIS). Permite la acción del los software de aplicación de cada elemento de red. Una misma plataforma permite visualizar diferentes equipos. El protocolo de comunicación entre CMIS es el CMIP.

5- COMUNICACIÓN ENTRE DISTINTOS EQUIPOS. En una estación pueden coexistir distintos tipos de equipos SDH (multiplexores, terminales de FO, radioenlaces, etc) y distintos enlaces que conforman la red. Para efectuar la interconexión de los mismos se requiere de la interfaz Q desde la Unidad de Gestión:
-INTERFAZ **Q1/Q2/Q3.** Q1/Q2 se indican en la norma ITU-T **G.771** y Q3 en **Q.513**.
-LAN ETHERNET. Normalmente los equipos SDH disponen de una interfaz física de conexión **AUI** que permite acceder al equipo mediante una LAN (10BaseT o 10Base2).

6- ELEMENTO DE ADAPTACION. Permite la conexión entre un equipo no adaptado a la red TMN y que desea ser gestionado por el mismo sistema de operaciones mediante un canal de comunicación de datos normalizado. El proceso de adaptación involucra las siguientes funciones de comunicación entre el elemento de red y el sistema de operaciones:
-Control de la comunicación: interrogación secuencial para recopilación de datos, direccionamiento y encaminamiento de mensajes, control de errores.
-INTERFAZ **Q2.** Conecta al elemento de red con el elemento de adaptación.

7- CENTRO DE GESTION REGIONAL. En el Centro de Gestión Regional se concentra la gestión remota de los equipos en un sector de la red. Se trata de una red LAN del tipo Ethernet (10Base2 o 10BaseT) que interconecta los siguientes elementos:
-Equipos de red SDH. Se trata de los extremos de enlaces que confluyen en la estación central regional.
-SISTEMA DE OPERACIONES. Está constituido por una o más (por razones de seguridad) estaciones de usuario **WS** (*WorkStation*). Esta WS puede funcionar con varios terminales **X-Terminal** para abastecer a diversos operadores simultáneamente.
-BRIDGE. Permiten interconectar distintas LAN del mismo tipo o generar varias desde una misma.
-SWITCH. Funciona en el ámbito de capa 2a (MAC), procesan direcciones y no modifican el contenido.
-ROUTER. Funciona en el ámbito de capa 3 y por ello requiere un análisis del protocolo correspondiente IP (ISO o UNIX).

8-CENTRO DE GESTION NACIONAL. Este centro de gestión se comunica con todos los otros centros de gestión regionales mediante una red extensa WAN generada con routers. El protocolo de comunicación es el TCP/IP de UNIX. El canal de comunicación es una señal tributaria de 2 Mb/s (noestructurada) que se envía dentro de la misma red SDH. La protección del tráfico se logra mediante una malla entre router por distintas vías. Sus componentes son:
-GATEWAY. Se denomina así a la WorkStation que funciona en el ámbito de todo el modelo de capas para convertir los protocolos de ISO a UNIX. Interconectan redes de características diferentes con simulación de protocolos.
-ROUTING. Se entiende por *routing* el proceso que permite la interconexión de redes.
-SISTEMA INFORMATICO. Posee características similares a la del Centro Regional. Mediante sucesivos *Password* es factible administrar las funciones que pueden ser desarrollados por ambos tipos de Centros.

9-DIRECCIONAMIENTO. La configuración inicial de la red de Gestión involucra la programación de los parámetros de comunicación. Se trata de las capas 2/3/4. Se disponen de tres estructuras de suite de protocolos: LAN, ISO y UNIX. Las direcciones disponibles en UNIX (IP) e ISO (NSAP) son distintas:
-DIRECCION IP. Disponible para direccionamiento entre componentes informáticos (Wokstation, X-Terminal, Routers, Impresoras, etc).
-DIRECCION NSAP. Esta dirección está normalizada por ISO y permite el direccionamiento entre equipos de la red SDH.
-DIRECCIÓN MAC. El enrutamiento dentro de una LAN contiene 2 direcciones: una LLC y otra MAC.

2.2- EJEMPLO DE BASE DE DATOS.

Una red de telecomunicaciones se representa mediante una jerarquía de ambientes a cada uno de los que se asocia objetos dinámicos e información estática. En un análisis inicial se jerarquiza la red de la siguiente manera. El nivel más alto es el **Sistema** en su globalidad que se divide, en el nivel inmediato inferior, en **Lugar** (asociado a un punto físico o localidad) y **Enlace**. Cada enlace, en la jerarquía inferior, se divide en **Canales** y **Direcciones** (ida y vuelta). El conjunto definido por un lugar o enlace, un canal o dirección determina un **Contexto**.

Posteriormente se identifican los **Objetos**. La red bajo gestión se observa entonces como un conjunto de objetos (ítem físico o lógico bajo gestión) definidos cada uno mediante un contexto. Los objetos constituyen la única entidad dinámica del sistema. A los objetos lógicos se los conoce como virtuales. Junto al contexto cada objeto tiene asociado 3 **Atributos** denominados **Tipo, Instancia** (tiene en cuenta la identidad en sistemas redundantes) y **Área**. El conjunto de estos elementos se denomina **Identificación** de un objeto. La identificación debe ser unívoca para cada objeto. Cada objeto está caracterizado por el comportamiento que puede adoptar. Varios objetos pueden tener un mismo comportamiento en común. El Comportamiento es una entidad de software que simula a un sistema de estados finitos. Para un sistema de transmisión se pueden mencionar, entre otros, los comportamientos de la **Tabla 04.**

Tabla 04: Comportamientos asignados a los elementos bajo supervisión.

Estado de alarmas:	On, Desconocido, Off, Habilitado, Deshabilitado.
Operación telecomandos:	On, Desconocido, Off, Operando, Problemas, Accionado.
Contador de errores:	Inactivo, Desconocido, Contando, Disponible, Problema.
Or/And de alarmas:	Ok, Prealarma, Alarma, Desconocido, Alarma normalizada.
Estado punto analógico:	Desconocido, Central, Bajo, Alto, Problemas.
Estado telesupervisión:	Habilitado, Deshabilitado, Desconocido.

2.3- EJEMPLO DE GESTION: CAMMESA.

En la **Fig 03** se muestra un diagrama a bloques de la red de gestión del sistema eléctrico nacional de la Argentina. Los componentes y canales de comunicación son indicados en la **Tabla 05**.

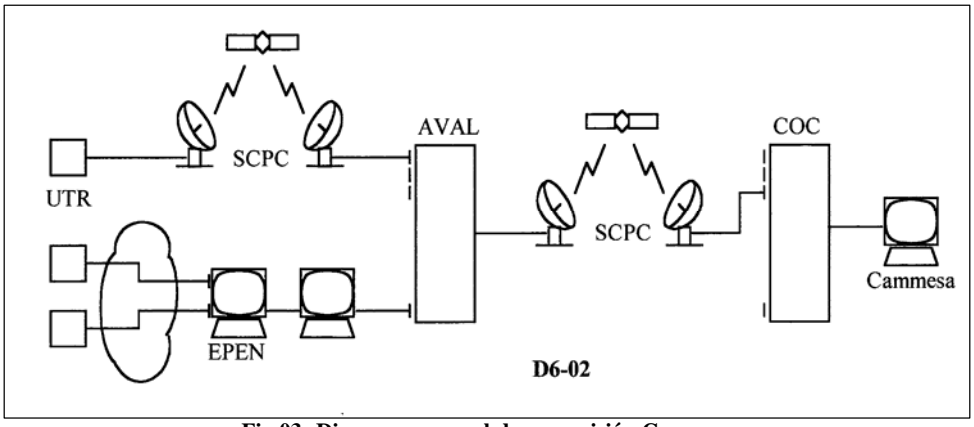


Fig 03. Diagrama general de supervisión Cammesa.

Tabla 05. Componentes y canales de comunicación de Cammesa.

-COC	(*Centro de Operaciones Cammesa*). La empresa **CAMMESA** (*Compañía Administradora de Mercado Mayorista Eléctrica SA*) fue creada en el proceso de apertura del mercado eléctrico en Argentina. Posee en la ciudad de Perez (Provincia de Santa Fe) el COC que reune las informaciones de operación de la red nacional de producción y transporte de energía. Desarrolla funciones de **SOTR** (*Sistema Operativo en Tiempo Real*). Mediante un Swicth con protocolo X.25 se concentran cerca de 200 puertas de entrada. Muchas de ellas se reciben mediante enlaces terrestres (**EPEC** de Córdoba lo hace mediante un radioenlace de 4x2 Mb/s como capacidad total) y otros mediante enlaces satelitales (**EPEN** de Neuquén).
-**AVAL**	(*Alto Valle*). La central de monitoreo de Alto Valle se encuentra en la Ciudad de Neuquén y posee un canal de comunicación satelital del tipo **SCPC** a velocidad de 19,2 kb/s con el COC. En AVAL se dispone de un switch con protocolo X.25 con 8 puertas. En él se concentran varios tipos de señales; por ejemplo, un canal satelital del tipo SCPC de 9,6 kb/s.
-**EPEN**	(*Ente Provincial de Energía de Neuquén*). Esta empresa realiza funciones de transporte provincial y distribución de energía. Posee cerca de 13 U **N5-03** *l Terminal Remota*) en localidades del interior provincial (Zapala, Chocón, Arroyito, Centenario, etc). Las UTR se encuentran unidas al AVAL mediante canales por cable (onda portadora en la red de alta tensión) o radioenlaces. La concentración de canales X.25 se realiza sobre una PC acondicionada especialmente para esta función de PAD en X.25. La capa de transporte de datos que utiliza EPEN para llegar al COC se basa en enlaces punto-a-punto de baja confiabilidad. Para incrementar la misma se proyectó en 1998 una red de transporte X.25 con switch en anillos para obtener enrutamientos alternativos. Es de notar que el COC debe recibir los datos con una disponibilidad del 99,5% o en caso contrario las empresas (EPEC, EPEN, etc) pagarán múltas al centro Cammesa.
-**ELCOM.**	La suite de protocolos contiene en las capas inferiores los protocolos X.25 y en la capa 7 el ELCOM. Este software de aplicación permite: -Realizar mediciones (tensión de red, potencia, corriente, etc); -Obtener el estado de los elementos de maniobras (interruptores, secuenciadores, etc); -Actualizar el estado de alarmas y -Realizar las funciones de correo electrónico (novedades y órdenes).

1213

CONFIGURACIÓN DE SWITCH-ROUTER

Sobre la ruptura de divisiones entre las funciones de switch y router en las capas 2, 3 y 4.
Este capítulo se fundamenta en productos Cisco para redes IP.

1- LOS COMPONENTES

1.1- LAYER 2: HUB, BRIDGE y SWITCH.

1.1.1- HUB. Se han difundido los concentradores Hub con las redes 10BaseT debido a la facilidad de extensión de la red LAN mediante una configuración jerárquica en estrella. Se trata de una topología mixta con un columna *Backbone* de coaxial o fibra óptica y concentradores para usuarios en estrella.

Un Hub es un concentrador, cuya versión más simple es un elemental conector tipo "T" (concentrador de 3 puertas pasivo). La primer generación de Hub activos solo ofrece funciones de repetidor-regenerador de señal digital. Disponen de hasta 8/12 puertas activas. En la segunda generación de Hub se introducen las funciones de gestión de red. Mediante el protocolo SNMP se obtienen los estados de las puertas (se trata de un concentrador inteligente *Smart Hub*). Permite la generación de segmentos virtuales de LAN (puertas de acceso múltiple). Disponen de un microprocesador para la gestión y memoria MIB (base de datos de gestión).

La tercera generación de Hub poseen un *backplane* de alta velocidad (por ejemplo con celdas ATM). Posee puertas de diferentes técnicas para permitir modularidad LAN, FDDI, Router y Gestión. Incorpora funciones de conmutación para todas las necesidades de una empresa (*Enterprice Switching*). Las funciones de gestión permiten la desconexión de nodos con alarma y aislación de puertas para pruebas locales. Además permite la conexión horaria de puertas, el análisis de protocolo y obtener el estado de carga de enlaces.

1.1.2- BRIDGE. Permiten interconectar distintas LAN del mismo tipo o generar varias desde una misma. Permite una mayor disponibilidad al generar LAN autosuficientes. Reducen el tráfico entre secciones de red LAN. Permiten solucionar problemas de congestión de paquetes mediante aislación de tráfico. Se puede generar una red de bridge con conmutación de paquetes (*Routing*) a nivel de capa MAC. Introduce retardo para medios de acceso de menor velocidad. Produce latencia de 1 mseg aproximadamente.

Normalmente un bridge posee dos puertas y un switch posee más de dos puertas. Un bridge puede utilizarse solo (como filtro entre dos secciones de LAN en la misma localización) o de a pares (uno en cada extremo para unir dos redes LAN distantes mediante un canal de comunicación dedicado como ser Nx64 kb/s en una WAN).

1.1.3- SWITCH. Un hub es un medio de interconexión plano (*Shared Media*) a nivel de capa 2. Un bridge es un filtro de direcciones MAC con dos puertas. Un switch consiste en una operación de Bridge de tipo multipuerta. Simultáneamente con la creación de los switch se ha generado la operación **VLAN** (*Virtual LAN*) que consiste en agrupar los usuarios en la red en varias LAN por separado.

El switch funciona en el ámbito de capa 2 (MAC), procesan las direcciones MAC en una LAN y no modifican el contenido del paquete. Inspecciona la dirección de fuente y destino del paquete (*MAC Address*) para determinar la ruta de conmutación. La tabla de rutas se realiza mediante un compilador de direcciones MAC. La misma es dinámica y se actualiza sobre la base de la lectura de las direcciones contenidas en los paquetes que ingresan al switch (aprendizaje mediante lectura de direcciones). Cuando un switch recibe un paquete con dirección desconocida lo emite a todas las puertas (técnica conocida como *Flooding*).

Contiene suficiente memoria buffer para los momentos de demanda máxima (cola de espera). El overflow del buffer produce descarte de paquetes. Generalmente son estructuras no-bloqueantes y permiten que múltiples conexiones de tráfico se desarrollen simultáneamente. Permiten una estructura de red jerárquica en lugar de plana (uso de Hub). Un switch LAN dispone de varias puertas de interfaz con un ancho de banda dedicado, cada puerta representa un host o un segmento de red diferente. Trabajan sobre redes LAN del tipo Ethernet, token ring y FDDI.

Los switch tienen diversas estructuras de matriz de conmutación (*Switch Fabric*). El switch basado en un bus implementa un backplane monolítico donde se intercambia el tráfico de todos los módulos. El switch basado en memoria *shared* utiliza memorias RAM de alta velocidad para interconexión de módulos sobre el backplane. El switch punto-a-punto interconecta cada módulo con los demás no mediante un bus sino mediante conexiones individuales.

1.2- LAYER 3: ROUTER Y SWITCH.

1.2.1- ROUTERS. Funciona en el ámbito de capa 3 y por ello requiere un análisis del protocolo Internet IP. Debe soportar distintos tipos de protocolos; por ejemplo TCP/IP, DECnet, IPX (Novell), AppleTalk, XNS (Xerox). Interconectan LAN entre sí o una LAN con WAN (X.25, Frame Relay, ATM).

Permiten mejorar la eficiencia de la red ya que toleran distintos caminos dentro de la red. El Router puede segmentar datagramas muy largos en caso de congestión, en cambio no pueden ensamblar datagramas. Un router se utiliza muchas veces como conversor de interfaz (LAN hacia G.703 para 2 Mb/s o V.35 para Nx64 kb/s). En conexiones de datos de baja velocidad el router puede ser colocado en el extremo del circuito de acceso al usuario para obtener supervisión de línea. En este caso, mediante el protocolo SNMP asociado a UDP/IP se puede gestionar el punto de acceso de usuario (función PING por ejemplo).

Los router se pueden interconectar a alta velocidad mediante interfaces de 100 Mb/s (mediante pares o fibra óptica) y 1000 Mb/s (mediante Gigabit Ethernet) para formar redes de alta velocidad. En este caso el medio de transporte entre router es una conexión LAN extendida (MAN). Normalmente el protocolo IP usado en una LAN puede ser transportado mediante una red SDH, una red ATM o directamente sobre interfaz LAN por fibra óptica. Cuando la estructura de red usada es la descripta se observa una unión entre el concepto de switch LAN y router.

Algunas ventajas de los switch de capa 2 frente a los routers han determinado la idea de difundir el switch y usar el router solo una vez ("un switch cuando se puede, un router cuando se debe"). El switch tiene menor latencia, mayor capacidad de tráfico (*throughput*), fácil administración (concepto de gestión "*plug and play*") y menor costo por puerta. Los switch de capa 2 crean redes planas, en esencia se trata de un *bridging*. Un switch de capa 3 simula totalmente las operaciones de *routing*.

1.2.2- SWITCH-IP (*Layer 3 Switching*). Se entiende por switch de capa 3 al equipo que realiza la operación de enrrutamiento mediante acciones de hardware; en tanto que es un router cuando las mismas se realizan mediante acciones de software. El switch-IP se fundamenta en circuitos *custom* del tipo **ASIC** (*Application-Specific Integrated Circuit*). Un switch de fines de los años `90 contiene 3 ASIC (para resolución de direcciones; para memoria de sistema y para memoria de puertas Gigabit). Con estos puede enrutarse 40 Mpps, soportar 1,5 millones de rutas y tomar decisiones a nivel de capa 2, 3 y 4.

Una diferencia de importancia entre un switch y un router es que este último permite optimizar la ruta cuando la red es muy grande. Permite además disponer de caminos alternativos y reconfigurar la tabla de rutas. Hacia fines de la década de los años `90 la diferencia entre router y switch se han reducido y reciben nombres combinados con ambas funciones.

La capacidad de procesamiento de un switch o un router se mide en Gb/s o Mpps (millones de paquetes por segundo) como capacidad de la matriz de conmutación. Cuando la suma de las entradas al equipo es igual a la capacidad de la matriz de conmutación se dice que es no-bloqueante. Cuando es inferior se dice que se sobre-escribe el equipo y se supone que el tráfico no satura a la matriz.

1.3- LAYER 4: SWITCH

Se han reconocido hasta ahora dos tipos de switch: el switch de nivel 2 (funciona como un bridge de varias puertas) y el de nivel 3 (funciona como un router orientado al hardware). El switch de nivel 4 realiza funciones de conmutación de paquetes tomando en cuenta el *socket* (IP address y TCP/UDP port). De esta forma se puede tener acceso al tipo de servicio (capa de aplicación) transportado y realizar operaciones de prioridad (política de QoS) del tráfico con mayor precisión.

2- CONFIGURACIONES Y PROTOCOLOS

En los ítems que siguen se estudian los diferentes protocolos y herramientas disponibles en los actuales equipos que reunen las funciones de switch y router en una combinación de capas 2, 3 y 4.

2.1- CONFIGURACIONES POSIBLES

Sobre los equipos switch-router se puede configurar una amplia variedad de funciones que permiten asegurar el funcionamiento normal y en caso de fallas, además de asegurar la calidad del servicio y la seguridad. En la **Tabla 01** se enumera una lista de funciones a ser configurables en los switch; en la **Tabla 02** se enumeran las configuraciones en los routers. Más adelante se indican los protocolos asociados a algunas de estas funciones.

Tabla 01. Funciones configurables en los switch-LAN.

CONFIGURACIÓN	DESCRIPCIÓN
Port del switch	Las configuraciones posibles sobre la port del switch son: -Velocidad. Se trata de 10 o 100 Mb/s sobre la puerta RJ45. La configuración de velocidad se realiza en forma manual (fija) o automática. -Operación duplex. Normalmente Ethernet funciona en forma half-duplex; para un mejor rendimiento de la red se puede realizar en forma full-duplex (los port de tipo Gigabit-Ethernet solo son full-duplex). -Nombre del port. Identifica una puerta del switch con su función o elemento conectado. -Prioridad de acceso al bus del switch (normal o alta).
Control de flujo	Está solo disponible sobre las puertas Gigabit-Ethernet. Se trata de tramas de pausa que inhiben la transmisión de paquetes desde una puerta por un período de tiempo. Las tramas de pausa no son conmutadas a través del sistema. Las port en un enlace Gigabit-Ethernet deben tener el mismo seteo, en cuanto a control de flujo, operación duplex y reporte de falla remota.
Tabla de direcciones	La *Address Table* se construye en forma automática de forma que la entrada de un paquete implica la memorización de la dirección MAC de origen.
Protección EtherChannel.	Opera sobre Fast y Gigabit Ethernet. Se pueden configurar varios enlaces paralelo para agregar tráfico. Se trata de un enlace de mayor velocidad y en caso de falla de uno de ellos el enlace continúa funcionando. Utiliza el protocolo **PagP** (*Port Aggregation Protocol*) para la creación automática de EtherChannel. De esta forma, en caso de corte una sola línea abastece al medio, reduciendo la performance pero manteniendo el servicio.
Protección Spaning-Tree	Se trata de configurar la red de switch con enlaces en loop. Los loops están prohibidos en Ethernet pero mediante el protocolo **STP** (*Spanning-Tree Protocol*) se puede configurar la red en forma automática para detectar los loops e interrumpirlos hasta que una falla los habilite como necesarios. Las posibles configuraciones son: -El STP se puede habilitar para cada VLAN en particular. -A los port se les asigna una prioridad y un costo para que STP determine el mejor camino. -Se puede determinar el estado de la port (bloqueado, deshabilitado, forwarding, etc). Desde el estado de bloqueo al de forward se pasa por listening y learning. -*PortFast* es una función que habilita a pasar desde el bloqueo a forward sin pasar por los estados intermedios. -*UplinkFast* permite una rápida convergencia para cambios con enlaces redundantes. Otra variante es *BackboneFast*.
VLAN	La función **VLAN** (*Virtual LAN*) permite dividir la LAN en grupos virtuales para limitar el tráfico de multicast y broadcast. La configuración se realiza seleccionando: la port del switch, la dirección MAC, un grupo de direcciones IP, etc. -El protocolo **VTP** (*VLAN Trunk Protocol*) minimiza los riesgos de violaciones de seguridad y especificaciones en la generación de VLAN. -La función **VMPS** (*VLAN Management Policy Server*) permite asignar puertos de VLAN en forma dinámica. -Las funciones de **ISL** (*InterSwitch Link*) o **IEEE 802.1Q** permite la formación de enlaces punto-a-punto en la red de switch. -La función **InterVLAN** permite la conexión entre componentes de distintas VLAN. Esta función debe ser desarrollada por un router de capa 3. Se puede usar un módulo de router anexo al switch; en Cisco se denomina **RSM** (*Route Switch Module*).
ATM-LANE	Cuando el switch permite la conexión mediante troncales de tipo ATM, la configuración de las LAN se denomina **LANE** (*LAN-Emulation*). El LANE trabaja en el modelo cliente-servidor. Se debe configurar el ingreso de un LEC (*LANE Client*), el PVC, la función de multiprotocolo **MPOA**, etc.

Servicios Multicast	El servicio multicast se provee mediante el protocolos **IGMP** (*Internet Group Management Protocol*) y otros asociados. Un host puede ser incripto en el grupo de multicast y el switch debe inscribir dicha dirección MAC en la lista de direcciones adheridas. Se puede configura el grupo multicast, habilitar el protocolo IGMP (o **CGMP** propietario de Cisco) consultar estadísticas.
Supresión multi-broadcast	Esta función permite la supresión de tráfico multicast y broadcast cuando el mismo inunda la red. Este tráfico ciertas veces degrada la performance. Se puede configurar midiendo el ancho de banda (basado en hardware) o el número de paquetes (basado en software) en una período de tiempo (mayor a 1 seg). La medición se realiza por port del switch.
Multilayer switch	Esta técnica se conoce de diversas formas (Tag switching o MPLS, Netflow o MLS) e intenta reducir el tiempo de procesamiento mediante el análisis del primer paquete y la asignación de un tag o label en MPLS o la conmutación de ports del switch en MLS. En MLS el switch enruta (capa 3) el primer paquete y crea una MLS-cache para mantener los flujos bajo proceso (en capa 2). Es necesario rescribir las direcciones MAC. En la configuración se debe tener en presente el *accounting*, criptografía, NAT, CAR, etc. Se puede configurar la función de exportación de datos (estadísticas de tráfico por cada usuario, protocolo, port y tipo de servicio).
Filtro de protocolo	Esta función previene cierto tráfico de protocolo sobre un port. Por ejemplo, si una PC está configurada para IP y IPX, pero solo emite IP es eliminado del tráfico IPX. Cuando emita un paquete IPX será nuevamente colocado en el grupo de IPX.
Lista de IP permitidas	Esta función permite limitar el tráfico entrante al switch del tipo Telnet y SNMP. El tráfico ping y traceroute continúa trabajando normalmente.
Seguridad de port	Se trata de indicar las direcciones MAC que pueden ser conectadas a una Port. Si la dirección MAC de origen es distinta la conexión se inhibe y se genera una reporte SNMP.
SNMP/RMON	Es posible configurar la función de reporte Trap en el protocolo SNMP del switch y habilitar las funciones de grupos (estadística, historia, alarmas y eventos).
Chequeo de conectividad	Se trata de efectuar las operaciones *Ping* y *Traceroute*. Permiten detectar la presencia del componente conecta en el port y trazar (descripción paso-a-paso) la ruta que dispone hasta el elemento bajo estudio en una red remota.
Analizador de port	La función **SPAN** (*Swithed Port Analyzer*) realiza un espejado de tráfico desde una o más puertas hacia otra donde se coloca un analizador de red.
Reportes por puerta	Se trata de la función *Switch TopN Report*. Se puede coleccionar datos estadísticos de cada port. Los datos son: utilización de la puerta, número de Bytes y paquetes de entrada/salida, tráfico multicast y broadcast en la puerta, número de errores y de overflow del buffer.
Autentificación	Sobre el switch se pueden configurar mecanismos de autentificación para la entrada a las líneas de comando. Se trata de una autentificación local mediante password o mediante un server de acceso a la red del tipo **TACACS+** (*Terminal Access Controller Access Control System*). TACACS es una familia de protocolos de control de acceso basado en TCP o UDP (port 49). Utiliza el modelo client/server. Resume los procesos de autentificación, autorización y contabilidad (*accounting*). Como autentificación puede usar los protocolos para PPP (PAP, CHAP o EAP) o Kerberos. La autorización es la acción para determinar que acciones pueden ser desarrolladas, mientras que el accounting es la acción de memorizar que hace el usuario. Sobre el switch se puede configurar la clave de criptografía MD5, setear el número de login permitidos, setear el intervalo de timeout de respuesta del server.
Configuración de DNS	**DNS (*Domain Name System*).** Este sistema permite organizar la información de routing entre una denominación (seudónimo) simple de recordar y el número de dirección IP verdadero (se denomina resolución de nombre). El nombre completo tiene como máximo 63 caracteres. De ellos 3 caracteres indican el domino (edu-educación, com-comercial, gov-gubernamental, org-organización, mil-militar, etc) y 2 el país (ar-Argentina, it-Italia, etc). La tabla de dominios memorizada en el servidor se denomina *DNS Cache*. DNS opera sobre UDP por lo cual no existe una conexión propiamente dicha; solo sirve para resolver la relación entre dominio en formato de texto y la dirección IP asignada. Con posterioridad, la conexión es establecida sobre TCP hacia el servidor (por ejemplo de web).
Configuración redundantes	Pueden ser instalados módulos de supervisión redundantes (se realizan funciones de conmutación entre módulos, puesta en sincronismo, verificación de estado, etc). Puede trabajarse con software de sistemas imágenes.
Archivos de configuración	Pueden ser creados archivos con la configuración de un switch. Los mismos pueden ser usados en caso de falla absoluta del mismo o para descargarse en un swirtch similar nuevo.
Sincronización de tiempo	Mediante el protocolo **NTP** (*Network Time Protocol* de RFC-1305) se puede llevar la hora del UTC (*Coordinated Universal Time*) obtenida en general desde el sistema GPS (*Global Position System*). Se trata de un modelo cliente-servidor. Existen servidores públicos de NTP en Internet.

Tabla 02. Funciones configurables en los router.

	CONFIGURACIONES GENERALES
Routing	Se configura las distintas posibilidades de protocolos de routing: RIP, IGRP, OSPF, BGP, etc. Se pueden configurar rutas estáticas, direccionamiento secundario o filtrado de rutas.
Multicast	Se configura las funciones de multicast para grupos de usuarios. Se disponde de protocolos de gestión de grupos **IGMP** (*Internet Control Message Protocol*) y los de routing asociados (PIM, DVMRP o CMF).
Direcciones	Se configura las funciones **NAT/PAT** para la traslación automática de direcciones IP y ports de TCP entre la Internet y el sistema autónomo AS. Se configura la función de asignación de direcciones IP automática mediante **DHCP** (*Dynamic Host Configuration Protocol*).
Caching	Se refiere a la conexión de una memoria *Cache* al router de borde de la red para reducir el tráfico de paquetes web (http). Se configura el protocolo **WCCP** *(Web Cache Control Protocol)* para la conexión entre router y cache.
Protección hot-standby	**HSRP** (*Hot Standby Routing Protocol*). Este protocolo de *Cisco* entrega una protección hot standby automática entre dos routers. Cuando el router de trabajo falla el otro toma el control. Un router configurado con HSRP posee 4 estados posibles: activo, standby, *speaking* (recibe y emite mensajes *hello*) y *listening* (solo recibe mensajes *hello*). HSRP trabaja mediante el intercambio de 3 tipos de mensajes multicast: -*Hello*. Este mensaje se envía cada 3 seg para indicar información de estado y prioridad. El router con mayor prioridad es el que trabaja en un instante; los otros se encuentran en hot standby. -*Coup*. Este mensaje indica que un router pasa de la función standby a la función activo. -*Resign*. Este mensaje es emitido por el router activo cuando pasa al estado *Shutdown* o cuando un router de mayor prioridad ha enviado un mensaje *hello*.
Protección EtherChannel	De carácter similar al Switch.
	CALIDAD DE SERVICIO QoS
Control de congestión	Se trata de mecanismos de control de colas de espera en buffer. Se dispone de las variantes: -**FIFO** (*First In, First Out*). El primer mensaje en entrar es el primero en salir. Este es el mecanismo de QoS por *Default* y es válido solo en redes con mínima congestión. -**PQ** (*Priority Queuing*). Este mecanismo de control de congestión se basa en la prioridad de tráfico de varios niveles. Se configuran las prioridades y se monitorea la cola de espera. -**CQ** (*Custom Queuing*). Este mecanismo se basa en garantizar el ancho de banda mediante una cola de espera programada. Se reserva un espacio de buffer y una asignación temporal a cada tipo de servicio. -**WFQ** (*Weighted Fair Queuing*). Este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino y tipo de protocolo en IP, número de *Socket* -port de TCP/UDP-) y por el ToS en el protocolo IP.
Control de tráfico	Se trata de mecanismos para descarte de paquetes en caso de congestión en la red. -**WRED** (*Weighted Random Early Detection*). Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma random si la congestión aumenta (TCP se encarga del control de flujo reduciendo la velocidad de transferencia). -**GTS** (*Generic Traffic Shaping*). Provee un mecanismo para el control del flujo de tráfico en una interfaz en particular. Trabaja reduciendo el tráfico saliente limitando el ancho de banda de cada tráfico específico y enviándolo a una cola de espera.
Políticas de enrutamiento	El **PBR** (*Policy-Based Routing*) permite mejorar la QoS mediante la determinación de políticas. Se debe configurar un mapa de rutas para verificar la adaptación del paquete. Se basa en dirección IP, port TCP, protocolo, tamaño del paquete, etc.
CAR	(*Committed Access Rate*) permite generar una política de QoS basada en los bits de precedencia de IP. Se denomina señalización en banda.
Reservación de banda	La señalización fuera de banda se logra mediante el uso de un protocolo externo denominado **RSVP** (*Resource Reservation Protocol*). Sobre el mismo se configura su habilitación y la operación multicast.
Fagmentación-interleaving	Se trata de fragmentar un paquete extenso en pequeños y el intercalado de los mismos para reducir la ocupación prolongada por parte de un paquete. Trabaja con el protocolo **MLP** (*Multilink point-to-point Protocol*) sobre enlaces con PPP.
Compresión en tiempo-real	Comprime el encabezado de paquetes para la operación con **RTP** (*Real-Time Protocol*).

	SEGURIDAD
IPsec	Provee seguridad entre pares en tunel. Permite la autentificación de acceso, integridad de datos, privacidad, etc.
Firewall	El módulo de firewall se instala como un software sobre el router o en un servidor de acceso. Permite realizar las siguientes funciones: -Control de acceso. Crea un perímetro de defensa diseñado para proteger las reservas corporativas. Acepta, rechaza y controla el flujo de paquetes basado en identificadores de capa 3 o aplicaciones. El principio de funcionamiento es: "todas las conexiones son denegadas a menos que estén expresamente autorizadas". -*Logging*. Es el inicio de las conexiones entrantes y salientes. El uso de un sistema proxy y cache incrementa la velocidad de respuesta de estas operaciones. -Funciones de **NAT** (*Network Address Translator*) para direcciones públicas y privadas. -Autentificación. Involucra a 3 componentes: el servidor, el agente y el cliente. -Reportes. Ofrece un punto conveniente para monitorear (*Audit and log*) y generar alarmas.
AAA	(*Authentication, Authorization, Accounting*). Se configuran las opciones de autentificación (*login* y *password*), autorización (RADIUS, etc) y cuentas (*billing* y reportes).

2.2- PROTOCOLOS DE SOPORTE

2.2.1- STP (*Spanning-Tree Protocol*). STA es desarrollado originalmente en Digital DEC y luego fue incorporado a **IEEE 802.1d**. En las redes construidas mediante Switch-Ethernet se debe cuidar que no ocurran loop debido a que los caminos duplicados pueden generar paquetes duplicados. El uso de STA permite eliminar el problema de los loops y mantener las ventajas derivadas de la redundancia de enlaces (este párrafo puede leerse como generar pequeños anillos que permitan una reconfiguración en caso de corte de un enlace principal).

Este protocolo permite identificar los loop y mantener activa solo una puerta del switch. Por otro lado utiliza un algoritmo que permite identificar el mejor camino libre-de-loops en la red de switch. Para lograr este objetivo, se asigna a cada puerta un identificador consistente en la dirección MAC y una prioridad. La selección de la puerta se puede asignar en términos de prioridad (valor entre 0 y 63; por default es 32) y costo (0 a 65535).

El STP consiste en un intercambio de mensajes de configuración en forma periódica (entre 1 y 4 seg). Cuando se detecta un cambio en la configuración de la red (por falla o cambio de costo de la port) se recalcula la distancia (sumatoria de costos) para asignar una nueva puerta. Las decisiones se toman en el propio switch. En condiciones normales se selecciona un switch para que trabaje como *Root Switch* para determinar un topología de red estable (es el centro lógico de la topología en *Tree*). Por *default* el switch que posee la dirección MAC más baja es el seleccionado como root.

Los mensajes disponibles se denominan *Bridge-PDU* y son de dos tipos: *Configuration* y *Topology-change*. Los campos del mensaje de configuración incluyen 35 Bytes y el de cambio de topología solo los 4 Bytes iniciales. Por ejemplo, el mensaje de configuración contiene los siguientes campos de información.

3 Bytes	Indica el Identificador de Protocolo (2) y la Versión (1).
1 Byte	Identifica el Tipo de Mensaje (0 para configuración y 128 para cambio de topología).
1 Byte	Flag para indicar el cambio de configuración de la red.
12 Bytes	Se identifica la raíz (*Root*) mediante 8 Bytes y con 4 Bytes se identifica el costo de la ruta.
10 Bytes	Se identifica el switch mediante 8 Bytes y con 2 Byte se identifica la puerta del mismo.
4 Bytes	2 Bytes para identificar el tiempo de emisión del mensaje (*Age*) y 2 Byte para el tiempo máximo de vida.
2 Bytes	Indica el período de intercambio de mensajes de configuración *Hello*.
2 Bytes	Indica el tiempo de espera para emitir un mensaje en caso de detectar un cambio de configuración.

La port que utiliza la función STP se encuentra en algunos de los siguientes estados: bloqueado (no participa de la transmisión), listening (es un estado transitorio luego del bloqueo y hacia el forwarding), learning (es otro estado transitorio antes de pasar al forwarding), forwarding (transmite las tramas en forma efectiva) y dehabilitado (se trata del estado no-operacional). Si todas las port tienen la misma prioridad el forward lo realiza la port de menor número.

2.2.2- PagP (*Port Aggregation Protocol*). Es utilizado para la creación automática de enlaces del tipo EtherChannel. Este protocolo determina en forma automática los enlaces paralelos e informa a las puertas involucradas. De esta forma se paralelan los canales para evitar la duplicidad de tráfico del tipo multicast y broadcast. Configura también las distintas puertas para que sean interpretadas por el protocolo **STP**.

2.2.3- Protocolos para VLAN. El protocolo **VTP (*VLAN Trunk Protocol*)** trabaja en la capa 2 para mantener la consistencia cuando se adicionan, borran y redenominan las VLAN. Permite minimiza los riesgos de violaciones de seguridad y especificaciones. Se define un dominio (el grupo de swirtch donde se aplica las funciones de VTP) y un switch puede actuar de servidor o cliente de VTP.

La función **VMPS** (*VLAN Management Policy Server*) permite asignar puertos de VLAN en forma dinámica (conocido como *Dynamic Port VLAN Membership*). Esta función toma en cuenta la dirección MAC de origen cuando un equipo se conecta a la red. De esta forma una VLAN puede estar configurada para equipos en particular sin importar la posición física en la red. VMPS abre un socket sobre UDP para solicitar al server el mapeo en la VLAN.

Adicionalmente se dispone de la función **ISL** (*InterSwitch Link*) propietaria de Cisco o **IEEE 802.1Q** como standard industrial. Ambos permiten la formación de enlaces (trunk) de tipo punto-a-punto entre varias puertas de switch. Los trunk transportan información de múltiples VLAN para la extensión de las mismas a través de diversas redes. La negociación para los trunk se realiza mediante el protocolo **DTP** (*Dynamic Trunking Protocol*)

2.2.4- IGMP (*Internet Group Management Protocol*). Este protocolo standarizado en la RFC-1112 para la versión 1 y en RFC-2236 para la versión 2 se utiliza para la gestión de enlaces multicast. Las direcciones IP pueden ser individual (*unicast*) o grupal para algunos miembros o todos los de la red (*multicast* o *broadcast*). El grupo multicast puede ser permanente o transitorio (armado para un evento en especial).

El protocolo IGMP determina un servicio sin conexión con el mismo criterio de "best effort" de IP unicast. Se denomina **MBONE** (*Multicast Backbone*) a un set de routers y subredes interconectadas que soportan el servicio IP multicast. El protocolo permite la comunicación entre routers y host conectados en la red. Las operaciones de multicasting en las redes LAN son soportadas por protocolos standard y propietarios. Por ejemplo, en IEEE 802.1p se definen los protocolos para registración **GMRP** (*Group Multicast Registration Protocol*) y gestión de direcciones **GARP** (*Group Address Registration Protocol*).

Los protocolos que se utilizan para el routing en los servicios multicast son derivados de los utilizados para direcciones unicast. De esta forma se toman como origen el RIP y OSPF. Los algoritmos de routing disponibles son: algoritmo broadcasting en reversa RPB o multicast en reversa RPM; algoritmo *Spanning Trees* o el *Core-Based Trees*. Las variantes de protocolos de routing son las siguientes:

-PROTOCOLO DVMRP (*Distance Vector Multicast Routing Protocol*). Este protocolo está definido en RFC-1075. Es derivado del RIP y utiliza una variante del algoritmo **RPB** (*Reverse Path Broadcasting*). El RIP provee un solo tipo de métrica por lo que el OSPF (mantiene más de un tipo) tiene mejor performance. Sin embargo, DVMRP es más simple que MOSPF. Y se utilizó anticipadamente. DVMRP se encuentra sobre IGMP en el modelo de capas. La principal diferencia entre RIP y DVMRP es que, en tanto RIP calcula el próximo paso hacia el destino, en DVMRP se calcula la cantidad de pasos hacia el origen. DVMRP requiere de una periódica actualización para detectar nuevos receptores en el grupo y por ello tiene un problema de escala.

-PROTOCOLO MOSPF (*Multicast OSPF*). Se define en RFC-1584 como extensión del OSPF de la RFC-1583 y solo trabaja asociado al protocolo OSPF. El MOSPF provee el servicio de multicast pero no el servicio de tunelización del mismo (tampoco lo hace el DVMRP). En un protocolo de routing de tipo unicast la ruta se define en base a la dirección de destino, en tanto que en MOSPF se define en base al origen y los destinos. La definición de ruta se realiza en base al costo basado en la métrica de estado de enlace. Una vez definida la ruta se forma el árbol en la red y se descarta cada ruta individual. Se define una única ruta, no existe alternativas de igual-costo. MOSPF permite modificar la ruta basado en el ToS del datagrama IP. La optimización de ruta para un grupo no asegura la optimización en el uso de la red.

-PROTOCOLO PIM (*Protocol Independent Multicast*). Si bien es independiente del protocolo de routing de tipo unicast implementado, requiere del mismo para formar la tabla de rutas. Este protocolo mejora la deficiencia de DVMRP aplicando dos técnicas: modo-denso (protocolo diseñado para operar en un medio con miembros de distribuidos con alta densidad y ancho de banda elevado) o modo-distribuido (baja densidad de miembros -no significa pocos miembros- y ancho de banda reducido). El uso de una o de otra depende de la distribución de routers en la red.

2.2.5- MPS-MPLS (*Multilayer Switching-Multiprotocol Layer Switching*). Sobre este título se reportan varias tecnologías concurrentes. Se trata de optimizar la velocidad de conmutación en los switch y routers.

-***MPS-NETFLOW SWITCHING.*** Esta técnica de *Cisco* combina las acciones de router y switch para mejorar la performance a alta velocidad (por ejemplo en Gigabit Ethernet). El primer paquete de la secuencia es enrutado en forma normal en capa 3; la información obtenida sirve para crear un camino (*flow forwarding*) y los paquetes siguientes son procesados mediante un switch de nivel 2 (se trata de una operación orientada con-conexión). El camino se genera en base a las direcciones IP y las ports de TCP/UDP. La información está contenida en un *cache* que se crea a tal efecto.

Esta técnica de switch entre capas 2/3 se complementa en el *Core* de la red con *Tag Switching* o **MPLS**. Por otro lado, se utiliza este método para obtener información de performance de tráfico y proveer seguridad. Esta técnica utiliza los protocolos de routing normales y no requiere otros diseños especiales. Netflow entrega estadísticas de tráfico por cada usuario, protocolo, port y tipo de servicio. Esta estadísticas son útiles para análisis y diseño de la red y la facturación por departamentos en una empresa. La estadística de tráfico puede contener: la hora *Time-Stamp* del inicio y final, las

direcciones IP y port de origen y destino, número de interfaz de entrada y salida, número de paquetes y total de bytes de la transacción.

-MPLS-TAG.SWITCHING. Es un diseño de Cisco para el *Core* (*Backbone*) de una red IP cuando se trabaja a alta velocidad (por ejemplo, Gigabit Ethernet). Es un avance de la técnica **MPLS**. La arquitectura Tag Switch se encuentra en RFC-2105 del año 1997. Con posterioridad la denominación Tag se reemplazó por Label; Tag Switching se cambió por MPLS; el protocolo TDP por LDP. Luego que la tabla de rutas converge (usando protocolos de routing convencionales) los distintos router asignan una etiqueta *Tag* para cada ruta posible (dicho tag se encuentra como *header* de capa 2 o 3). El tag es corto y de longitud fija que es mejor manejado que el tabla de rutas (se puede asimilar al identificador de trayecto virtual VPI de ATM). Los tag generados localmente en el router se intercambia con los otros mediante un protocolo **TDP** (*Tag Distribution Protocol*). Este protocolo permite distribuir, requerir y actualizar la información de tag.

El tag switching consiste de dos componentes: el *forwarding* (responsable de la transferencia de paquetes) y el control. La información de tag se memoriza en una base de datos de información realizada a tal efecto y denominada **TIB** (*Tag Information Base*). Los paquetes que circulan en la red llevan el tag de identificación y no requieren de acciones de tabla de rutas. El tag puede ser una simple ruta unicast o multicast, o un identificador de flujo de tráfico (por ejemplo, para el caso de *Netflow* donde se identifica el flujo mediante direcciones IP, ports y políticas administrativas). Por otro lado, el tag switching puede trabajar con QoS mediante información de prioridades.