

Antologia

Licenciatura en Ingeniería de Sistemas Computacionales

Mike Zamora González

Universidad Tecnológica Costarricense



Diseño y Administración de Redes

Recopilación de Temas de Internet V3.0

Contenido

1	Fundamentos de Redes.....	7
1.1	Concepto de red.....	7
1.2	Tipos de redes	7
1.3	Parámetros que definen una red.....	8
1.4	Tipos de redes basadas en la distancia de cobertura	8
1.4.1	LAN: Local Area Network, Red de Area Loca	8
1.4.2	CAN: Campus Area Network, Red de Area Campus	8
1.4.3	MAN: Metropolitan Area Network, Red de Area Metropolitana	8
1.4.4	WAN: Wide Area Network, Red de Area Local	9
1.4.5	WLAN y WPAN.....	9
2	Arquitectura de una Red	10
2.1	El Modelo OSI.	10
2.2	Topologías de red.	14
2.3	Protocolos.	19
2.3.1	Protocolos de transporte.....	19
2.3.2	Protocolos de Red.	19
2.3.3	Protocolos de Aplicación.....	19
2.4	Modelos de comunicación.....	20
2.4.1	Control de acceso al medio.	20
2.4.2	Integración y compatibilidad de sistemas.....	21
2.5	Medios de transmisión.	24
2.5.1	Medios guiados.	24
2.5.2	Medios no guiados.....	25
2.5.3	Criterios generales para la instalación de cableado.....	26
3	Diseño de una red	27
3.1	Metas del diseño	27
3.1.1	Diseño estratégico de redes.	29
3.2	Administración de Redes.	30
4	Division en subredes.....	32
4.1	Dirección IP Clase A, B, C, D y E.....	32
4.2	Máscara de Red.....	33
4.2.1	Porción de Red:.....	34

4.2.2	Porción de Host:	35
4.2.3	Convertir Bits en Números Decimales	36
4.2.4	Calcular la Cantidad de Subredes y Hosts por Subred	38
4.3	Subneteo Manual de una Red Clase A	38
4.3.1	Adaptar la Máscara de Red por Defecto a Nuestras Subredes	38
4.3.2	Obtener Rango de Subredes	39
4.4	Subneteo Manual de una Red Clase B	40
4.4.1	Adaptar la Máscara de Red por Defecto a Nuestras Subredes	40
4.4.2	Obtener Cantidad de Hosts por Subred	41
4.4.3	Obtener Rango de Subredes	42
4.5	Subneteo Manual de una Red Clase C	43
4.5.1	Adaptar la Máscara de Red por Defecto a Nuestras Subredes	43
4.5.2	Obtener Cantidad de Hosts por Subred	44
4.5.3	Obtener Rango de Subredes	45
5	Fundamentos de IPv6	45
5.1	Conceptos	45
5.1.1	Protocolo de Internet versión 6 (Internet Protocol version 6, IPv6)	45
5.1.2	Espacio mayor de direccionamiento	46
5.1.3	Características de IPv6	46
5.1.4	Jerarquía de direcciones – Agregación de prefijos de red	46
5.1.5	Modos de configuración de IPv6	47
5.1.6	Renumeración	47
5.1.7	Multicasting	47
5.1.8	Encabezado eficiente	48
5.1.9	Etiqueta de flujo	48
5.1.10	Extensiones de encabezado	48
5.1.11	Movilidad	48
5.1.12	Seguridad	49
5.1.13	Mecanismos de Transición	49
5.2	Estructura del Protocolo IPv6	49
5.2.1	Encabezado	49
5.2.2	DATOS Cabecera TCP	52
5.3	Direccionamiento	53

5.3.1	Direcciones y direccionamiento en IPv6 (RFC2373)	53
5.3.2	Definición de dirección en IPv6.....	54
5.3.3	Diferencias con IPv4.....	54
5.3.4	Reservas de espacio de direccionamiento en IPv6.....	55
5.3.5	Direcciones especiales en IPv6	55
5.3.6	Representación de las direcciones IPv6	56
5.3.7	Direcciones unicast locales.....	57
5.3.8	Direcciones anycast (RFC2526)	58
5.3.9	Direcciones multicast (RFC2375)	59
5.3.10	Direcciones Requeridas para cualquier nodo.....	61
5.3.11	Direcciones unicast globales agregables (RFC2374).....	62
5.3.12	Formato para la representación en URL's (RFC2732)	65
5.3.13	Resumiendo	66
5.4	ICMPv6 (RFC2463).....	67
5.5	Neighbor Discovery (RFC2461)	69
5.6	Autoconfiguración en IPv6 (RFC2462).....	71
5.6.1	Autoconfiguración Stateless	72
5.6.2	Autoconfiguración Stateful – DHCPv6 (draft-ietf-dhcdhcpv6-15.txt).....	74
5.6.3	Renumeración	75
5.7	IPv6 sobre Ethernet (RFC2464).....	76
5.8	Multi-homing.....	77
5.9	IPsec	78
5.10	Movilidad.....	78
5.11	DNS (RFC1886).....	79
5.12	Protocolos de Routing.....	80
5.12.1	RIPng (RFC2080 y RFC2081)	80
5.12.2	OSPFv6 (RFC2740)	81
5.12.3	BGP4+ (RFC2283, RFC2545)	82
5.13	Estrategias de Transición (RFC1933)	83
5.13.1	Doble pila (IPv4 e IPv6)	83
5.13.2	Túneles IPv6 sobre IPv4.....	83
5.13.3	Transmisión de IPv6 sobre dominios IPv4 (RFC2529).....	84
5.13.4	Conexión de dominios IPv6 sobre redes IPv4.....	85

5.13.5	“Tunnel Server” y “Tunnel Broker”	85
5.13.6	Otros mecanismos de transición.....	85
5.14	Situación del estándar: RFC's y borradores.....	86
6	Administración De Redes.	87
6.1	Elementos Involucrados En La Administración De Red	89
6.2	Operaciones De La Administración De Red.....	89
6.2.1	Administración de fallas.....	89
6.2.2	Control de fallas.....	89
6.2.3	Administración de cambios.....	89
6.2.4	Administración del comportamiento.....	90
6.2.5	Servicios de contabilidad.....	90
6.2.6	Control de Inventarios.....	90
6.2.7	Seguridad.....	90
6.2.8	Llave privada.....	90
6.3	Funciones De Administración Definidas Por OSI.....	91
6.4	Protocolo De Administración De Red TCP/IP.....	92
6.5	Esquema De Administración.....	92
6.5.1	Administración de un aparato que no soporta SMMP:	93
6.6	Mensajes SNMP:	93
6.7	Tipos De Datos De SNMP.....	94
6.8	Base De Datos De Administración: MIB.....	94
6.8.1	Grupo de Sistemas.....	94
6.8.2	Grupo de Interfaces.....	95
6.8.3	Grupo de traducción de dirección.....	95
6.8.4	Grupo IP.....	95
6.8.5	Grupo TCP	95
6.8.6	Grupo de ICMP y UDP.....	95
6.8.7	Grupo EGP.....	95
6.8.8	Grupo de Transmisión.....	95
6.8.9	Grupo SNMP.....	95
6.8.10	Base de Información Administrativa MIB de SNMP	96
6.9	Aplicaciones SNMP	97
6.9.1	Transcend Network Supervisor de 3COM.....	97

6.9.2	SNMP Trap Watcher de BTT Software	98
6.9.3	SNMP Watcher de Dartware.....	99
6.9.4	NET-SNMP.....	99
6.9.5	Orion Network Performance Monitor de Solarwinds.....	100
6.9.6	LoriotPro.....	101
6.9.7	Multi Router Traffic Grapher (MRTG).....	101
6.10	Seguridad.....	103
6.11	Firma Digital.....	103
6.11.1	Operación de la firma digital.	104
6.12	Criptografía.	104
Bibliografía:.....		106

1 Fundamentos de Redes

1.1 Concepto de red

Una red (en general) es un conjunto de dispositivos (de red) interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación.

Dispositivos de red

- Estación de trabajo (Workstation)
- Un servidor (server)
- Impresora (printer)
- Concentrador (Hub)
- Conmutador de paquetes (Switch)
- Enrutador (router)
- Punto de acceso (access point)
- Consola de CDs (Jukebox)
- Modems satelitales
- Modems analógicos
- Estaciones terrenas vía satélite
- Conmutadores telefónicos
- etc, etc.

Una red debe cumplir con lo siguiente:

- ⇒ Un **medio** de comunicación donde transfiera información *Existen los medios inalámbricos e inalámbricos*
- ⇒ Un **recurso** para compartir *Discos, impresoras, archivos, scanners, CD-ROMs,....*
- ⇒ Un **lenguaje o reglas** para comunicarse *Existen los protocolos de red: Ethernet, TCP/IP, X.25, IPX,...*

1.2 Tipos de redes

Las redes pueden clasificarse con respecto a la información que es transferida de la siguiente manera:

- **Redes de DATOS** Compañías de beepers, compañías celulares de datos (SMS), proveedores de Internet, Voz paquetizada (VoIP).
- **Redes de VIDEO** Compañías de cableTV, Estaciones televisoras.
- **Redes de VOZ** Compañías telefónicas, compañías celulares.
- **Redes de AUDIO** Rockolas digitales, audio por Internet, Música por satélite.
- **Redes de MULTIMEDIOS** Compañías que explotan voz, datos, video simultáneamente.

También existen redes de microondas, redes vía satélite, redes de fibra óptica, redes públicas, redes privadas, redes eléctricas, redes ferroviarias, redes de carreteras, etc.

1.3 Parámetros que definen una red

- **Topología:** arreglo físico en el cual el dispositivo de red se conecta al medio
- **Medio físico:** cable físico (o frecuencia del espectro electromagnético) para interconectar los dispositivos a la red
- **Protocolo de acceso al medio:** Reglas que determinan como los dispositivos se identifican entre sí y como accesan al medio de comunicación para envíar y recibir la información

1.4 Tipos de redes basadas en la distancia de cobertura

Las redes de acuerdo a la cobertura geográfica pueden ser clasificadas en LANs, CANs, MANs, y WANs.

1.4.1 LAN: Local Area Network, Red de Area Loca

Una LAN conecta varios dispositivos de red en una area de corta distancia (decenas de metros) delimitadas únicamente por la distancia de propagación del medio de transmisión: coaxial (hasta 500 metros), par trenzado (hasta 90 metros) o fibra óptica (hasta 2 Km. en multimodo y hasta 300 Km. en monomodo), espectro disperso o infrarrojo (decenas de metros).

Una LAN podria estar delimitada también por el espacio en un edificio, un salón, una oficina, hogar...pero a su vez podría haber varias LANs en estos mismo espacios. En redes basadas en IP, se puede concebir una LAN como una subred, pero esto no es necesariamente cierto en la práctica.

Las LAN comúnmente utilizan las tecnologías Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface) para conectividad, así como otros protocolos tales como Appletalk, Banyan Vines, DECnet, IPX, etc.

1.4.2 CAN: Campus Area Network, Red de Area Campus

Una CAN es una colección de LANs dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en una área delimitada en kilometros.

Una CAN utiliza comúnmente tecnologías tales como FDDI y Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica y espectro disperso.

1.4.3 MAN: Metropolitan Area Network, Red de Area Metropolitana

Una MAN es una colección de LANs o CANs dispersas en una ciudad (decenas de kilometros). Una MAN utiliza tecnologías tales como ATM, Frame Relay, xDSL (Digital Subscriber Line), WDM (Wavelength Division Modulation), ISDN, E1/T1,

PPP, etc. para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas.

1.4.4 WAN: Wide Area Network, Red de Area Local

Una WAN es una colección de LANs dispersadas geográficamente cientos de kilómetros una de otra. Un dispositivo de red llamado enrutador es capaz de conectar LANs a una WAN.

Las WAN utilizan comúnmente tecnologías ATM (Asynchronous Transfer Mode), Frame Relay, X.25, E1/T1, GSM, TDMA, CDMA, xDSL, PPP, etc. para conectividad a través de medios de comunicación tales como fibra óptica, microondas, celular y vía satélite.

1.4.5 WLAN y WPAN

También existen las redes inalámbricas WLAN y WPAN, las primeras (wireless Local Area Network) están delimitadas por la distancia de propagación del medio y de la tecnología empleada, en interiores hasta 100 metros y en exteriores varios kilómetros.

Las WLAN utilizan tecnologías tales como IEEE 802.11a, 802.11b, 802.15, HiperLAN2, HomeRF, etc. para conectividad a través de espectro disperso (2.4 GHz, 5 GHz).

Las WPANs (Wireless Personal Area Network) están delimitadas en distancia aún más que las WLANs, desde los 30 metros hasta los 100 metros bajo condiciones óptimas en interiores.

Las WPAN utilizan tecnologías tales como IEEE 802.15, Bluetooth, HomeRF, 802.11b para conectividad a través de espectro disperso o con infrarrojo.

2 Arquitectura de una Red

2.1 El Modelo OSI.



Ilustración 1 - Modelo OSI

Cuando se produce un intercambio de datos entre equipos a través de un sistema de bus es preciso definir el sistema de transmisión y el método de acceso, así como informaciones relativas al establecimiento de los enlaces. Por este motivo, la International Standards Organization (ISO) especificó el modelo de referencia ISO/OSI, convertido en un estándar esencial a la hora de describir redes de comunicación y sus diferentes partes en las que se divide. Este modelo propone una serie de niveles o capas para intentar reducir la complejidad de comprensión de estos sistemas. El estándar describe siete capas, de tal modo que una se fundamenta en la anterior, aunque no es necesario emplear todas ellas para construir un sistema de comunicación ya que eso depende de su complejidad y aplicación. Esta separación estructurada permite que exista una independencia de cada capa, de tal modo que cada una puede ser modificada internamente sin afectar al resto, siendo responsable de extraer la información de control contenida en los datos recibidos y necesaria para esa capa, así como de enviar los datos a la siguiente capa. Dentro de cada capa la comunicación se lleva a cabo siguiendo reglas y convenciones predefinidas, que constituyen lo que generalmente se conoce por protocolo. Entre las capas adyacentes debe existir un interfaz que permite el intercambio de información, lo que se conoce como especificaciones de servicio. El conjunto total de capas y protocolos constituye la arquitectura de una red. Este modelo es válido tanto para grandes flujos de

información (intercambio de datos entre entidades bancarias) como aplicaciones muy sencillas (transmisión de estado de sensores todo/nada), por ello, no se establecieron restricciones de tiempo, ya que la prioridad principal es la exactitud de la datos recibidos. Esto supone una limitación para las aplicaciones industriales, pues en estos casos, además de la exactitud de los datos, resulta necesaria una caracterización temporal (condiciones de tiempo crítico), por lo que bajo el modelo OSI han nacido estándares que incluyen dichas restricciones de tiempo en la transmisión. También es necesario comentar que este modelo no es de obligado cumplimiento, sino que constituye un “manual de buenas prácticas” para que el sistema pueda formar parte de los “Sistemas Abiertos”. Estas capas del modelo OSI son las que deben ser implementadas en cada nodo de la red, donde la capa 1 constituye el medio físico de transmisión, y la capa 7 es la formada por la aplicación o interfaz de usuario. La siguiente tabla muestra una breve descripción de estas capas.

Capa	Nombre	Función	Características
7	Capa de Aplicación (Application Layer)	Funciones de usuario. Intercambio de variables. Servicios de comunicación específicos de usuario	Servicios de comunicación: Read/Write, Start/Stop
6	Capa de Presentación (Presentation Layer)	Representación de datos. Conversión del tipo de representación del sistema de comunicación en un formato adecuado al equipo. Diagnóstico	
5	Capa de sesión (Session Layer)	Sincronización. Requerimiento de respuestas. Establecimiento, disolución y vigilancia de una sesión.	Coordinación de la sesión.
4	Capa de Transporte (Transport Layer)	Establecimiento/disolución de enlace. Formación, repetición y clasificación de paquetes.	Transmisión asegurada de paquetes.
3	Capa de Red (Network Layer)	Direccionamiento de otras redes y control de flujo. Rutas de comunicación.	Comunicación entre dos.
2	Capa de Enlace de Datos (Data link Layer)	Método de acceso. Gestión de colisiones. Limitación de los bloques de datos, transmisión asegurada, detección y eliminación de errores.	CRC-Check. CSMA/CD, Token
1	Capa Física (Physical Layer)	Medio físico de transmisión. Test de errores a nivel de bit.	Cable coaxial/triaxial. Cable óptico. Cable bifilar. ITP

Nivel 1: Capa Física (Physical Layer). Este nivel procura la transmisión transparente de bits a través del soporte físico en el orden definido por el nivel de enlace (capa 2). Se definen las características eléctricas y mecánicas de la línea de transmisión (bus), así como conectores o medios de enlace hardware. También define los sistemas de modulación y demodulación de la señal transmitida/recibida, las señales de control que determinan la temporización y el orden de transmisión y realiza un diagnóstico de errores a nivel de bit. Entre otros estándares usados en este nivel, los más conocidos son el RS-232 y el RS-422. El cable de conexión no pertenece a este nivel ya que el modelo sólo se aplica a los nodos de la red y no a la red misma.

Nivel 2: Capa de enlace de datos (Data Link Layer). Este nivel tiene como función asegurar la transmisión de la cadena de bits entre dos sistemas. Este nivel es el encargado de recoger los datos del nivel de red (capa 3) para formar las tramas de envío (añadiendo datos de control), y viceversa. También impone los métodos de direccionamiento, detección y recuperación de errores, reenvío de tramas perdidas y regulación del tráfico de información en cuanto a velocidades de transmisión. En redes locales, el nivel de enlace procura también el acceso exclusivo al soporte de transmisión (acceso al medio). Para ello, dicho nivel se divide en dos subniveles, Medium Access Control (MAC) y Logic Link Control (LLC), que se designan también como niveles 2a y 2b respectivamente. Las normas más conocidas para los métodos de acceso aplicados en el subnivel MAC son IEEE 802.3 (Ethernet, CSMA/CD), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring). Para el subnivel LLC se aplica generalmente la norma IEEE 802.2, aunque debido a las características de tiempo real exigidas normalmente a sistemas de bus de campo, éstos utilizan métodos de acceso considerablemente modificados.

Nivel 3: Capa de red (Network Layer). Este nivel se encarga de la operatividad de la red, controlando la ruta de la comunicación de datos entre sistemas finales (nodos y caminos), entendiendo por sistemas finales el emisor y el receptor de una información cuyo recorrido puede llevar bajo circunstancias a través de diversos sistemas de tránsito. Por ello, el nivel de red debe seleccionar la ruta a seguir, lo que normalmente se denomina encaminamiento (Routing). Las estaciones, por medio de este nivel añaden una cabecera indicando la dirección de destino, asegurando que el encaminamiento de los paquetes de datos es apropiado para poder llegar hasta su destino. Este nivel es encargado de traducir nombres lógicos en direcciones físicas y controlar la congestión en la red. Conforme la red posee una topología más compleja, esta tarea resulta más complicada. En un enlace punto a punto no entra en juego este nivel.

Nivel 4: Capa de Transporte (Transport Layer). Este nivel entra en juego una vez que se ha producido el enlace entre nodos en la red. La comunicación es ya independiente de la red, siendo el nivel que enlaza lo que quiere transmitir el usuario con la información que hay que enviar. Este nivel tiene como misión ofrecer al usuario un enlace entre nodos fiable, entregando datos libres de error al nivel 5. Puede dividir la conexión para hacerla más rápida (varias conexiones al nivel de transporte). Los servicios ofrecidos incluyen el establecimiento del enlace de transporte, la transmisión de datos, así como la disolución del enlace. Para ello el usuario puede exigir, en general, una determinada calidad en el servicio (QoS, Quality of Service). Parámetros de calidad son, por ejemplo, la velocidad de transferencia y la tasa de errores residuales.

Nivel 5: Capa de Sesión (Session Layer). La tarea principal del nivel de sesión es sincronizar las relaciones de comunicación, es decir, permitir establecer una

sesión de comunicación entre dos capas de aplicación (nivel 7), una para cada nodo. El inicio de una sesión implica un conjunto de acciones de comunicación para establecer un proceso unitario (como transmitir un fichero, por ejemplo) que se distribuye en: control de comunicaciones uni ó bidireccional, administración del testigo, evitando que ambos lados traten de realizar la misma operación simultáneamente y establecimiento de puntos de chequeo en la información (puntos de sincronización). En caso de error sólo es necesario retransmitir de nuevo desde el último chequeo. También permite configurar el tipo de diálogo (full-duplex o semi-duplex), así como realizar ciertas verificaciones de seguridad. Esta capa no aparece en numerosos sistemas de comunicación.

Nivel 6: Capa de Presentación (Presentation Layer). Resuelve el problema de semántica y sintaxis de la información transmitida. Generalmente, al intercambiar datos, diferentes sistemas utilizan lenguajes distintos. El nivel de presentación traduce los diversos lenguajes de las estaciones de comunicación a un lenguaje unificado con una sintaxis abstracta para permitir un diálogo entre diferentes sistemas. Así, este nivel convierte los datos del nivel 7 a un lenguaje que es el acordado para la transmisión (aquí también podría incluirse la encriptación y compresión de datos), y modifica los datos recibido para que la aplicación reciba los datos conforme a su criterio. Para ello se utiliza en la mayor parte de los casos el Abstract Syntax Notation One (ASN.1) definido en ISO 8824 y las Basic Encoding Rules (BER) asociadas.

Nivel 7: Capa de Aplicación (Application Layer). El nivel de aplicación comprende los servicios específicos de enlace con las diferentes aplicaciones de comunicación. Como existen multitud de aplicaciones, es particularmente difícil establecer estándares unificados, puesto que las aplicaciones propiamente dichas no forman parte del modelo. Habitualmente incluye protocolos de uso general tales como la forma de iniciar y cerrar una sesión de comunicaciones. Existen numerosas propuestas de protocolos orientados a determinados tipos de aplicaciones. Para aplicaciones de automatización se tiene el Manufacturing Message Specification (MMS), que describe los servicios y protocolos del nivel de aplicación (MAP, Manufacturing Automation Protocol). Los sistemas de bus de campo modernos se orientan fuertemente en MMS a la hora de diseñar el nivel de aplicación.



Ilustración 2 - Modelo OSI para comunicación entre dos nodos.

Para lograr un entendimiento suficiente y seguro son imprescindibles los niveles 1, 2 y 4. El nivel 1 define las condiciones físicas, entre otras, los niveles de tensión y corriente. El nivel 2 define el mecanismo de acceso y el direccionamiento de la estación, para que en un determinado instante sólo pueda enviar datos una de las estaciones del bus. La seguridad y coherencia de los datos se garantiza gracias a la función del nivel 4, el de transporte. Este nivel también se ocupa de tareas de control de flujo de datos, de seccionamiento en bloques o paquetes y de los mecanismos de acuse o confirmación.

En resumen podemos decir que los niveles OSI 1 y 2 proporcionan el transporte de datos básico para una red simple. Los niveles 3 y 4 extienden estas funciones para una red compleja compuesta de muchas redes simples con diferentes propiedades. Los niveles 5 y 6 proporcionan un marco de trabajo para establecer y negociar las comunicaciones orientadas por el usuario y finalmente el nivel 7 proporciona los medios para comunicar la aplicación final con los procesos de envío y recepción. Se puede considerar que el flujo de los datos en un sistema de comunicación experimenta un tratamiento o “empaquetado” similar al de un objeto que se desea enviar por correo: a cada nivel del modelo OSI corresponde un tratamiento similar a las diversas fases de embalaje del objeto. La transmisión a través de la red corresponde entonces al envío del paquete, mientras que a la recepción, cada nivel del modelo OSI se encarga de desempaquetar la información agregada al embalaje, procediendo en sentido inverso, iniciando del envoltorio externo a los más internos. Cada nivel a la recepción se ocupa de desempaquetar lo que fue agregado a los datos originales al momento de la transmisión del nivel correspondiente.

2.2 Topologías de red.

Se llaman topologías de red a las diferentes estructuras de intercomunicación en que se pueden organizar las redes de transmisión de datos entre dispositivos. Cuando componentes de automatización autónomos tales como sensores, actuadores, autómatas programables, robots, etc., intercambian información, éstos

deben interconectarse físicamente con una estructura determinada. Cada topología de red lleva asociada una topología física y una topología lógica. La primera (topología física), es la que define la estructura física de la red, es decir, la manera en la que debe ser dispuesto el cable de interconexión entre los elementos de la red. La topología lógica es un conjunto de reglas normalmente asociado a una topología física, que define el modo en el que se gestiona la transmisión de los datos en la red. La utilización de una topología influye en el flujo de información (velocidad de transmisión, tiempos de llegada, etc.), en el control de la red, y en la forma en la que ésta se puede expandir y actualizar.

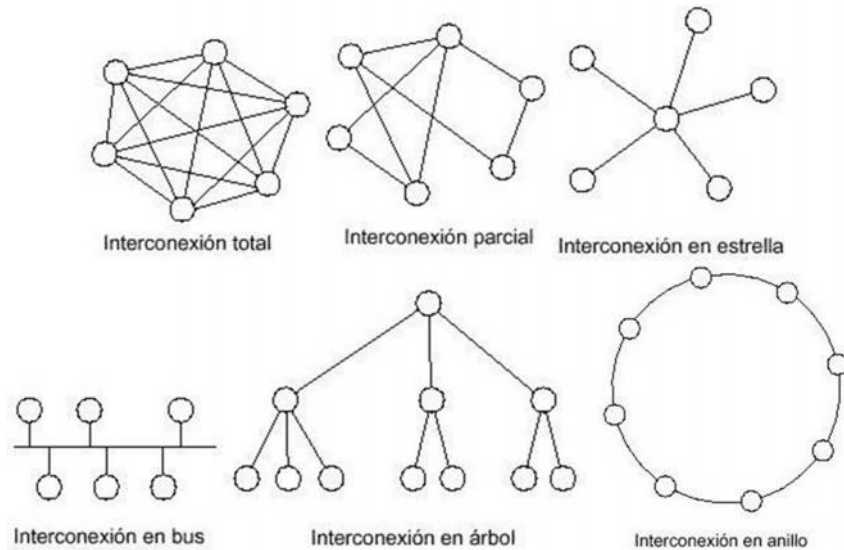


Ilustración 3 - Topologías de red.

- **Interconexión total y parcial.** Este tipo de interconexión proporciona múltiples enlaces físicos entre los nodos de la red, de tal modo que no existen varios canales de comunicación compartidos y múltiples caminos de interconexión entre dos nodos. La interconexión es total cuando todos los nodos están conectados de forma directa entre ellos, existiendo siempre un enlace punto a punto para su intercomunicación. La interconexión es parcial cuando no todos los nodos pueden conectarse mediante un enlace punto a punto con cualquier otro nodo de la red.
- **Interconexión en estrella.** Cada nodo se conecta a un nodo central encargado del control de acceso a la red por el resto de nodos (colisiones, errores, etc.). En esta topología adquiere una importancia decisiva el nodo central que se encarga de controlar toda la comunicación, pues cualquier perturbación en el mismo conduce, generalmente, al fallo de la red completa. Su implementación puede ser una decisión factible en el caso de que los nodos de la red no se encuentren muy distanciados del nodo central debido al coste que supone cablear cada nodo hasta el nodo central.
- **Interconexión en bus.** Todos los nodos se conectan a un único medio de transmisión utilizando los transceiver, encargados de controlar el acceso al bus. Los mensajes se envían por el bus y todos los nodos escuchan,

aceptando los datos sólo en el caso de que vayan dirigidos a él (reconocimiento de su propia dirección). Esta topología permite la adición y sustracción de nodos sin interferir en el resto, aunque un fallo en el medio de transmisión inutiliza por completo la red (rotura del cable, por ejemplo). Suelen ser necesarios terminadores de red para poder adaptar impedancias y evitar reflexiones de las ondas transmitidas y recibidas. Los nodos se deben conectar a la línea de bus principal mediante segmentos cortos pues ello influye directamente en la velocidad de transmisión y recepción de datos para ese nodo. Esta es una de las topologías más utilizadas habitualmente. Puede cubrir largas distancias empleando amplificadores y repetidores. Poseen un coste reducido, siendo las más sencillas de instalar. La respuesta es excelente con poco tráfico, siendo empleadas en redes pequeñas y con poco tráfico

- **Interconexión en árbol.** Esta topología puede interpretarse como el encadenamiento de diferentes estructuras en bus de diferente longitud y de características diferenciadas, constituyendo diferentes ramas de interconexión. En este caso adquieren gran importancia los elementos que permiten duplicar y enlazar las diferentes líneas, ya que actúan como nodos principales de manera análoga a como lo hace el nodo principal de la interconexión en estrella. Dado que existen varias estructuras de bus, cada una debe incorporar sus terminadores y elementos asociados, así como los elementos de enlace.
- **Interconexión en anillo.** Los nodos se conectan en serie alrededor del anillo. Sería equivalente a unir los extremos de una red en bus. Los mensajes se transmiten en una dirección (actualmente ya existen topologías en red con envío en ambos sentidos), pasando por todos los nodos necesarios hasta llegar a su destino. No existe un nodo principal y el control de la red queda distribuido entre todos los nodos. Cuando la red es ampliada o reducida, el funcionamiento queda interrumpido, y un fallo en la línea provoca la caída de la red. También se la conoce como red “testigo en anillo” o “Token ring”. Posee una relación coste – modularidad buena, en general, la instalación es complicada, aunque es fácil variar el número de estaciones. No influyen los fallos en las estaciones si no condicionan la capacidad del interfaz del anillo. Es muy sensible a fallos en los módulos de comunicaciones (interfaz) y en el medio de comunicación. El retardo grande para número de estaciones elevado.

Además de las topologías mencionadas, pueden conformarse diferentes topologías que mezclan varios tipos básicos de interconexión mediante la inclusión de elementos de enlace como repetidores, concentradores (hub), puentes (bridge), pasarelas (gateway), conmutadores (switch) y/o encaminadores (router). Estos elementos pueden incluir cierto nivel de computación en el manejo de la información para poder adaptar dos tipos de redes diferentes, o bien pueden consistir en meros retransmisores de la señal a otros segmentos de la red.

- **El repetidor (repeater):** copia la información que recibe de un lado en el otro y amplifica su nivel. El repetidor es transparente a todos los niveles de

las estaciones en comunicación, es decir, los niveles físicos de ambas redes deben ser idénticos. Por ello, los repetidores no se utilizan para acoplar subredes diferentes, sino para amplificar o prolongar una subred existente como por ejemplo una interconexión de bus.

- **Los puentes (bridge):** se utilizan para acoplar subredes que trabajan con el mismo protocolo en el nivel de enlace (Logical Link Control, LLC). Los soportes de transmisión y los métodos de acceso al bus (Medium Access Control, MAC) de las subredes a enlazar pueden ser diferentes. Los puentes se utilizan principalmente para unir redes locales que tienen diferente topología o cuando, en base a aplicaciones especiales, es necesario añadir determinadas estructuras a subredes. Ese tipo de puentes se utilizan en subredes que, si bien utilizan un soporte de transmisión diferente (cable bifilar, fibra óptica), tienen la misma estructura.
- **El encaminador (router, enrutador, encauzador):** sirve para enlazar redes OSI con niveles 1 y 2 diferentes. El encaminador determina además el camino óptimo (ruta de comunicación) de una información a través de una red existente (routing). Criterios para definir el camino óptimo pueden ser, por ejemplo, la longitud del recorrido o el retardo de transmisión mínimo. Para cumplir su tarea, el encaminador modifica las direcciones de origen y destino del nivel de la red de los paquetes entrantes antes de volver a transmitirlos. Como los encaminadores tienen que ejecutar tareas sensiblemente más complejas que los puentes, trabajan a menor velocidad.
- **Un conmutador (Switch):** se utiliza para conectar múltiples dispositivos de la misma red dentro de un edificio o campus. Por ejemplo, un switch puede conectar sus ordenadores, impresoras y servidores, creando una red de recursos compartidos. El switch actuará como un controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad. Existen dos tipos básicos de switches: gestionados y no gestionados. **Los switches no gestionados** funcionan de forma automática y no permiten realizar cambios. Los equipos de redes domésticas suelen utilizar switches no gestionados. **Los switches gestionados** le permiten acceder a ellos para programarlos. Esto proporciona una gran flexibilidad porque el switch puede monitorizarse y ajustarse local o remotamente, para proporcionarle el control de cómo se transmite el tráfico en su red y quién tiene acceso a su red.
- **Una pasarela (gateway, puerta de enlace):** se utiliza para acoplar redes con diferentes arquitecturas, es decir, permite interconectar dos subredes cualesquiera. En base al modelo de referencia OSI, una pasarela tiene como misión convertir los protocolos de comunicación de todos los niveles. Permite también acoplar una red ISO con una no conforme a esta norma. Los enlaces de red materializados mediante pasarela suponen complicaciones y ofrecen una velocidad más reducida.

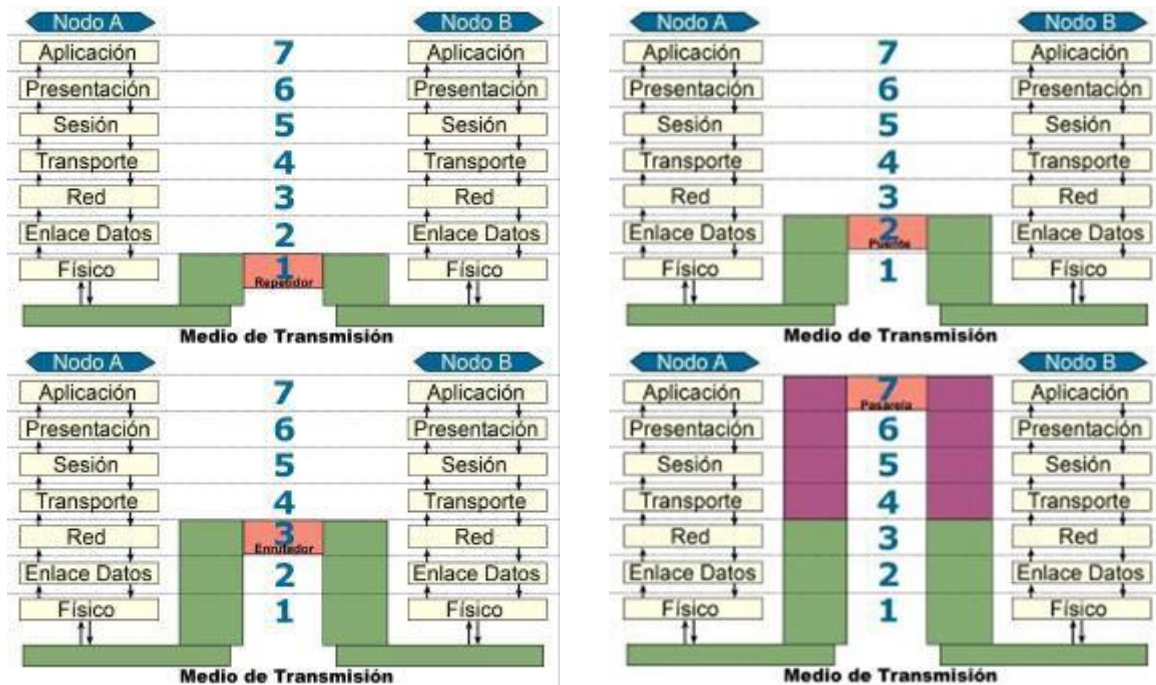


Ilustración 4 - Niveles OSI donde se emplazan los diferentes elementos de enlace entre nodos o estaciones: repetidor, puerta de enlace, enrutador y pasarela.

Por otro lado, para comunicar dos nodos, existen dos métodos básicos de intercambio de información:

- ✓ Conmutación de circuitos. Las estaciones intermedias que intervienen en la comunicación conectan sus circuitos de entrada y salida hasta establecer un canal físico entre ambos extremos. Durante la transmisión, el circuito físico sólo puede ser utilizado por las 2 estaciones que establecieron la conexión.
- ✓ Conmutación de paquetes. Orientado a la transmisión de datos no continuada. Los mensajes se dividen en paquetes que son multiplexados por los canales de comunicación de los que dispone un nodo. Cada nodo encamina el paquete por el enlace adecuado, aunque cada paquete puede seguir un camino distinto. Los enlaces pueden ser utilizados por paquetes de otras transmisiones. Con este sistema, la red de comunicación está ocupada por infinidad de paquetes, cada uno dirigido a un nodo diferente.

La elección de una topología de red suele estar determinada por ciertos factores como:

- Coste y/o Modularidad: Coste en medios de comunicación, sencillez de instalación y mantenimiento,
- Flexibilidad: Dificultad de incrementar o reducir el número de estaciones.
- Fiabilidad – Adaptación: Fallos en las estaciones o en el medio de comunicación, facilidad de mantener el servicio. Encaminamientos alternativos.

- Retardo – Caudal: Retardo mínimo introducido por la red. Factor determinante para comunicaciones de tiempo crítico.
- Tráfico de información que puede soportar.
- Aplicación a la que está destinado.
- Tecnología a emplear, dado que ciertos sistemas comerciales imponen su propia tecnología, que incorpora la topología por ellos diseñada, así como sus protocolos de comunicación.

2.3 Protocolos.

Los protocolos dentro del ámbito de red, son el conjunto de normas, reglas que se van a utilizar para el intercambio de los datos entre los equipos de una red. Es decir, que para que esto suceda es como darles un idioma para que se entiendan y puedan realizar la comunicación entre sí.

No hay un solo protocolo, existen más de ellos y pueden residir en el mismo equipo sin que colisionen entre sí. Los adaptadores de red son los encargados de recibir e identificar para llevarlos a su procesamiento en la computadora, existen varios tipos:

2.3.1 Protocolos de transporte.

- ⇒ ATP (Apple Talk Transición Protocol).
- ⇒ NETBios (Network Basic Input/Output System)
- ⇒ TCP (Transmission Control Protocol).

2.3.2 Protocolos de Red.

- ⇒ DDP (Delivery Datagram Protocol).
- ⇒ IP (Internet Protocol)
- ⇒ IPX (Internet Protocol Exchange).
- ⇒ NetBEUI (Network Basic Extended User Interface).

2.3.3 Protocolos de Aplicación.

- ⇒ AFP (Apple File Protocol).
- ⇒ FTP (File Transfer Protocol).
- ⇒ HTTP (HyperText Trasfer Protocol).

De todos ellos los más utilizados en la actualidad son: Apple Talk (sobre firewire) para comunicación entre equipos de esta misma marca, TCP/IP que se es el más conocido porque en la actualidad lo utilizamos para acceder a la Internet y se encuentra en casi todos los sistemas operativos existentes, IPX que es utilizado por los sistemas operativos de red de la marca Novell Netware. NetBIOS/NetBEUI creado por Microsoft e IBM actualmente utilizado en redes con sistema operativo Windows como protocolo nativo de este.

2.4 Modelos de comunicación.

Además de las diferentes técnicas de acceso y los sistemas de comunicación, resulta importante conocer los dos modelos básicos en los que se enmarca cualquier sistema de comunicación. Estos modelos son “fuente/destino” y “productor-consumidor”.

Con el modelo fuente/destino un nodo emite un mensaje a cada nodo destino, debiendo repetir ese mensaje para cada uno de los nodos si es que desea que el mensaje llegue a varios nodos pues la trama del mensaje enviado contiene una cabecera donde figura el nodo fuente y el nodo destino. De este modo, no es posible la llegada simultánea del mismo mensaje a todos los nodos, utilizando la red de comunicaciones durante un largo periodo de tiempo. Además, el tiempo de emisión a todos los nodos cambia según el número de nodos a los que se desea hacer llegar el mensaje. Este modelo es empleado por protocolos como Ethernet, Profibus, Interbus-S, Seriplex y Modbus.

El modelo productor/consumidor emplea un sistema por el que todos los nodos reciben los mensajes que se transmiten, siendo la tarea de cada nodo decidir si ese mensaje debe aceptarlo. De este modo, todos los nodos reciben el mensaje simultáneamente y no es necesario repetirlo para cada uno de los nodos a los que está dirigido, con el consiguiente ahorro en el tiempo de utilización del bus. Así, el tiempo de transmisión resulta constante independientemente del número de nodos a los que se desea hacer llegar el mensaje. En este caso, la trama del mensaje incluye un identificador de mensaje; este identificador permite que los nodos receptores conozcan si deben aceptarlo o no. Este tipo de emisión es apropiado cuando se realizan mensajes en emisión de difusión completa (broadcast) o semidifusión (multicast).

Actualmente, la mayoría de protocolos intentan emplear ambos tipos de mensajes para así optimizar el funcionamiento de la red dependiendo del tipo de mensajes a enviar o recibir. A continuación se muestra el formato de los mensajes para cada uno de los modelos.

A)	Fuente	Destino	Datos	CRC
B)	Identificador		Datos	CRC

Ilustración 5 - Formato de mensajes en los modelos: a) fuente/destino y b) productor/consumidor.

2.4.1 Control de acceso al medio.

El control de acceso al medio constituye la topología lógica de una red, y sirve para determinar qué nodo puede emplear la red en un instante determinado para enviar o recibir señales. Esta gestión se enmarca dentro de la segunda capa OSI. A menudo, se describe este proceso como MAC (Medium Access Control) o control de acceso al bus.

En una conexión punto a punto no se hace necesario el uso de técnicas de resolución de problemas ya que generalmente se dispone de un canal de recepción y otro de transmisión (full duplex), con lo que basta con enviar datos

cuando sea necesario dado que no habrá nadie más que emplee el canal. En cambio, para cualquier otro sistema de bus donde existen varios nodos compartiendo el mismo medio de transmisión, es necesario resolver los problemas de utilización que pueden existir. La situación ideal sería la de un sistema de control que resuelva rápidamente las interacciones o problemas en general que se pueden dar cuando varios nodos acceden simultáneamente al bus, y que sea poco sensible a los fallos de las estaciones, viéndose poco afectado por ampliaciones o reducciones de la red. Si existen tramas de control de la red, el método de acceso debe ser capaz de asumir esta cantidad de tráfico añadida, siendo aconsejable que disponga de tiempos de espera para organizar mejor el tráfico de la red. Estas técnicas generalmente son asíncronas. Existen dos tipos principales:

- Técnicas de repartición. A cada usuario se le asigna una fracción del la unidad total a repartir. Pertenecen a este tipo las técnicas de multiplexación por división de frecuencia (MDF), multiplexación por división de tiempo (MDT). Son eficientes si los usuarios demandan servicios con regularidad
- Técnicas de compartición. Se produce una asignación del medio en función de la demanda, son eficientes cuando el tráfico no es estable y la demanda se produce a ráfagas, como ocurre en las LAN. Las técnicas empleadas son: colisión (ó contienda), reserva y selección.
 - **Contienda:** Si el usuario necesita el canal de comunicación intenta tomarlo, produciéndose una contienda con los usuarios que tengan el mismo propósito. Se producirán colisiones y se debe incorporar algún algoritmo para resolver estas situaciones.
 - **Reserva:** El usuario conoce con adelanto cuando va a poder utilizar el medio. No se producirán colisiones en la transferencia de información, pero podrán existir en el proceso de reserva.
 - **Selección:** El usuario es avisado cuando llega su turno y toma el control del medio para transmitir. Los usuarios son seleccionados por algún tipo de turno y desconocen cuando van a serlo nuevamente.

2.4.2 Integración y compatibilidad de sistemas.

Actualmente la mayoría de aplicaciones industriales implican el uso de una gran cantidad de elementos de campo como sensores y actuadores. Dados los requerimientos actuales de la integración dentro de un entorno totalmente automatizado, estos elementos de campo no solo deben ser capaces de realizar complicadas funciones sino que también deben ser capaces de comunicarse y trabajar en conjunto con otros equipos, de acuerdo a las necesidades finales del usuario. Los equipos por tanto, en principio, deben tener la conformidad de un estándar de comunicación. Estos dispositivos tienen que satisfacer primeramente las pruebas de conformidad del estándar de comunicaciones que implementarán, pero muchas veces esto no es un requisito suficiente para poder trabajar en conjunto porque entre implementaciones que tienen la conformidad de un estándar puede que sea imposible el funcionamiento conjunto. Por consiguiente, deben también ofrecer otras propiedades como las llamadas interoperabilidad o cooperación entre dispositivos. Cuando tratamos temas relativos a la integración

de dispositivos de campo, es necesario en primer lugar poder distinguir claramente los siguientes conceptos: conformidad, interconectividad, interoperabilidad, cooperación e intercambiabilidad.

2.4.2.1 Conformidad.

En la época en que las redes eran privadas, un fabricante definía su protocolo de comunicación para todos sus equipos y eventualmente para todos los equipos compatibles con él. Hoy en día con el gran auge del concepto de sistema abierto y específicamente para dispositivos de campo, teniendo en cuenta el gran número de fabricantes, los servicios y protocolos deben ser estandarizados. ISO define el concepto de prueba de conformidad y también la manera de realizarla. La prueba de conformidad es una operación que nos permite decir si una implementación particular de un protocolo o un grupo de protocolos se ajustan a lo expresado en el estándar. Aunque si N equipos son declarados conformes, existe la posibilidad de que ellos no puedan cooperar en la misma aplicación. Las razones para la no cooperación, entre dispositivos que tienen la conformidad son simples, primeramente el estándar presenta opciones, algunas veces ambiguas, y selecciones diferentes pueden hacer que productos tengan la conformidad sin ser compatibles entre ellos. En segundo lugar las pruebas nunca son exhaustivas. En tercer lugar las consideraciones de tiempo y recursos no son tomadas en cuenta en las pruebas de conformidad. Estas razones, expuestas precedentemente, originan la necesidad de introducir la noción de interoperabilidad.

2.4.2.2 Interconectividad

La interconectividad está proporcionada por las capas que definen el protocolo de comunicación. Cada dispositivo en el sistema debe soportar el mismo protocolo en término de número de capas definidas por el mismo; pero cada dispositivo tiene su propia definición de los servicios o elementos de información soportados. Los dispositivos que tienen solamente interconectividad pueden intercambiar datos pero no tendrán conocimiento de qué es lo que éstos representan.

2.4.2.3 Interoperabilidad

La interoperabilidad de dispositivos que tienen la conformidad de un mismo estándar es una propiedad que expresa la capacidad de éstos de comunicarse para cooperación y para participar de un objetivo común. Las razones por las cuales muchas veces no existe la interoperabilidad pueden resumirse en las siguientes:

- Imprecisión de límites.
- Especificaciones estándares ambiguas o equivocadas.
- Implementaciones con prestaciones temporales diferentes.
- Pruebas de conformidad no exhaustivas.

La prueba de interoperabilidad es vista como un complemento a la prueba de conformidad y su primera aproximación se puede realizar reuniendo equipos reales que habían pasado las pruebas de conformidad en la misma plataforma y probar si tales equipos son capaces de comunicarse correctamente, y por

consiguiente, si ellos pueden interoperar. Esta es una operación costosa y difícil dado lo heterogéneo de los dispositivos y el número de equipos. Esta metodología permite solamente verificar aquellos productos que podrían trabajar juntos bajo un cierto número de hipótesis seleccionadas. Si el usuario final toma otro producto con otras configuraciones, está claro que la prueba anterior no puede garantizar la interoperabilidad en todos los casos. La interoperabilidad de las comunicaciones sin embargo no está definida de una manera estándar. Algunas confusiones acerca de la interoperabilidad han surgido del hecho de que esta propiedad es parcialmente obtenida de una prueba global. Se puede entonces introducir el concepto de cooperación entre dispositivos para distinguirlo de la interoperabilidad. La interoperabilidad está reservada a las capas de comunicación y a los perfiles de todas las partes estandarizadas. De esta manera podemos distinguir interoperabilidad de la cooperación entre dispositivos.

2.4.2.4 Cooperación entre dispositivos.

Podemos definir la cooperación entre dispositivos de campo como la propiedad que tienen las aplicaciones software o procesos de aplicación, de cada uno de los elementos que cooperan, para poder interactuar y satisfacer un objetivo determinado. Indudablemente esto presupone la interoperabilidad y por lo tanto la conformidad con un estándar común a todos estos dispositivos. Por lo tanto, podemos decir que los dispositivos cooperan cuando:

- Los servidores de procesos de aplicación interpretan correctamente los servicios requeridos realizados desde un cliente de procesos de aplicación.
- Clientes de procesos de aplicación interpretan correctamente los servicios de respuesta realizados por los servidores.
- Intercambios de datos realizados por los productores son interpretados por los consumidores.

Se dice que la interpretación de la información es correcta sí: la sintaxis es bien reconocida por todas las partes, la semántica es bien entendida y son respetadas las características de tiempo. Como ejemplo de elementos que no pueden cooperar, se puede citar el de dos o más dispositivos como uno que mide la presión y otro que la utiliza, que tienen definidas unidades de medición diferentes. En este caso la cooperación sólo es posible si uno de ellos es capaz de adaptarse a las características del otro con una operación de parametrización.

2.4.2.5 Intercambiabilidad

La intercambiabilidad puede definirse como la propiedad que presenta un dispositivo de ser reemplazado por otro, funcionalmente similar pero de fabricante diferente, sin tener que modificar el sistema. Cada equipo debe, obviamente, ser interoperable con los otros equipos del sistema global. Por ejemplo, si todas las características de los equipos A y B son similares entonces A y B son intercambiables. En el caso en que las características de A estén incluidas en las características de B, entonces A puede ser sustituido por B; pero B solamente es intercambiable con A si las características de este último son las utilizadas en la interoperabilidad del sistema y en las relaciones de cooperación.

2.5 Medios de transmisión.

Los medios de transmisión son los elementos por los que se transporta la información, haciendo que llegue con la menor cantidad de ruido y distorsión a todos los nodos (o estaciones) involucrados en el proceso de comunicación. A nivel de campo deben permitir mucha flexibilidad en cuanto a manejo físico del mismo y al incremento del número de nodos de manera simple. A continuación se presenta una breve descripción de los principales medios de transmisión utilizados en los entornos industriales.

De manera ineludible, asociado a los medios de transmisión se encuentran los conectores que permiten realizar la unión entre los nodos y elementos de la red y el medio de transmisión, debiendo ser “transparentes” al funcionamiento de la misma, sin entorpecer o atenuar el flujo de señales. Dependiendo del tipo de red a instalar, a menudo estos conectores suelen ser específicos, aunque existen conectores de uso general como los conectores DB9, DB15 y DB25 habitualmente empleados en transmisión de señales eléctricas.

En primer lugar, decir que existen dos clases principales de medios de transmisión, los medios guiados, y los medios no guiados. En el primer tipo existe un medio material por donde se transmite la información (cableado en general), y el segundo tipo utiliza el aire como medio de transmisión, es decir, suelen ser sistemas de transmisión inalámbricos. La elección de un tipo de red local conlleva la elección del medio de transmisión pues cada fabricante suele recomendar un tipo de medio de transmisión que mejor se adapta a la red, o bien aconseja varios medios de transmisión dependiendo de las distancias, velocidades de transmisión, ancho de banda, entorno de trabajo, etc.

2.5.1 Medios guiados.

La característica principal de un medio guiado es la existencia de un cable consistente en una envoltura de uno o más hilos conductores eléctricos u ópticos. Entre los medios de transmisión de señal eléctrica, uno de los parámetros a tener en cuenta es la impedancia característica, que debe mantenerse en todo el cable para asegurar una correcta transmisión, y la atenuación del cable, medida en dB (decibelios) por unidad de distancia. Respecto al cable óptico, se debe asegurar una buena transmisión del haz óptico, especialmente a través de los múltiples empalmes que se suelen realizar en cualquier instalación.

2.5.1.1 *Par trenzado.*

Es el medio de transmisión más antiguo. Está formado por dos hilos de cobre aislado entrelazados en forma helicoidal, uno para transmisión de datos y el otro referenciado a tierra. La utilización de la forma entrelazada tiene por objeto la reducción de la interferencia eléctrica con respecto a los pares de hilos cercanos, ya que como es sabido dos cables paralelos podemos asimilarlos a una antena. Existen los cables apantallados (STP, Shielded Twisted Pair) y no apantallados (UTP, Unshielded Twisted Pair); este último se clasifica en diferentes categorías (de la 2 a la 5) dependiendo de la calidad del mismo, actualmente ya existen cables de categorías 6 y 7, pues a veces es necesaria mayor calidad para soportar

mayor velocidad y ancho de banda. También existen numerosas variantes de cables dependiendo de la envoltura plástica para adaptarse a cualquier aplicación o emplazamiento (exteriores, temperaturas extremas, etc.) sin perjudicar la calidad de transmisión.

Existen cables con diferente número de pares en su interior, ya que dependiendo de la aplicación o tipo de red son necesarios más o menos pares. Su utilización tiene cabida tanto en aplicaciones digitales como analógicas. La aplicación más conocida es la transmisión telefónica, con cable STP de dos pares y conectores RJ45 y RJ11. Otra aplicación habitual es la de redes para transmisión de datos (ethernet, por ejemplo), con el uso de cuatro pares trenzados y conectores RJ45 y RJ11.

2.5.1.2 Cable coaxial.

El cable coaxial está formado por un núcleo de cobre rodeado de material aislante y un conductor exterior trenzado denominado comúnmente malla, se dispone en una estructura concéntrica. Cubriendo a todo el conjunto encontraremos externamente una cubierta protectora de material plástico. Existen dos tipos principales, de banda base y de banda ancha, aunque este último, a pesar de poseer mejores cualidades, es menos empleado dada su mayor complejidad de instalación y mayor coste. Este tipo de cable suele ser robusto ante interferencias, sus aplicaciones más conocidas son para señales de televisión y datos.

2.5.1.3 Fibra óptica.

Constituida por un núcleo muy fino de fibra de vidrio circular (existen diferentes materiales plásticos que dotan a la fibra óptica de diferentes propiedades y calidades), que al tener un elevado índice de refracción permite conducir la energía óptica en su interior. Este núcleo está envuelto por un recubrimiento opaco que aísla la fibra óptica de posibles interferencias. A diferencia del caso anterior, la transmisión no es digital sino analógica, por lo que se necesita disponer de amplificadores que refuercen la señal de forma periódica. Es el medio idóneo si se necesitan altas velocidades de transmisión, gran ancho de banda o cubrir largas distancias, pues la luz es más inmune a las interferencias electromagnéticas y posee tiempos de transición menores. Existen tres tipos básicos de fibra óptica, fibra monomodo, multimodo de índice gradual, y multimodo de índice discreto o escalonado, con diferentes grados de atenuación, velocidades de transmisión, y ancho de banda. Debido a la complejidad de la instalación y sus dispositivos asociados, resulta una opción muy cara, por lo que sólo se instala en lugares donde no sea posible otra alternativa.

2.5.2 Medios no guiados.

En emplazamientos donde resulta complicado trazar un tendido de cable, es conveniente utilizar un enlace inalámbrico. Actualmente, este tipo de enlaces está teniendo un gran auge debido a la aparición de sistemas de enlace como Wi-fi (IEEE 802.11b) y Bluetooth, que resuelven las comunicaciones entre dispositivos en distancias cercanas, pero donde se centran gran parte de las necesidades de los usuarios (por ejemplo, en una nave industrial). Sin embargo, los enlaces

mediante medios no guiados ya se vienen realizando con anterioridad mediante ondas de radio para distancias cercanas, y mediante enlaces de microondas, usados generalmente en enlaces punto a punto que deben cubrir largas distancias (se usan para comunicaciones terrestres y vía satélite).

2.5.3 Criterios generales para la instalación de cableado.

En entornos industriales, y especialmente a nivel de campo, donde existen numerosos dispositivos y por tanto, gran cantidad de conexiones y entramado de cables, es recomendable utilizar medios de transmisión de sencilla instalación, fácil manipulación, y mantenimiento sencillo para facilitar la reparación por personal no especializado. La selección del medio de transmisión dependerá de:

1. Las distancias y accesibilidad de los dispositivos; normalmente en el nivel de campo, dentro de las células de producción y entre ellas, se utiliza cable de par trenzado, ya que permite cubrir sin dificultad las distancias promedio de este tipo de entorno.
2. El coste del medio a utilizar, pues si las distancias son considerables, como en planta, lo mejor es utilizar un medio de transmisión poco costoso (el más utilizado es el cable de par trenzado apantallado o no apantallado).
3. La flexibilidad que presente la inserción de nuevos nodos; nuevamente en este caso el más adecuado es el cable de par trenzado.
4. La facilidad de permitir llevar los conductores de alimentación a los nodos remotos; pues en sistemas industriales, la mayoría de dispositivos inteligentes de campo necesitan fuentes de alimentación externa en corriente continua. Por lo tanto, el medio de transmisión también debe considerar este requerimiento.

3 Diseño de una red

Diseñar una red siempre ha sido difícil, pero hoy en día la tarea es cada vez más difícil debido a la gran variedad de opciones. A continuación se examinarán las principales metas del diseño de una red, cuales son las prioridades que se adaptan al desarrollo de la red, entre otras cosas. Un efectivo administrador de la red es también un cuidadoso planeador.

3.1 Metas del diseño

El diseñador de la red debe siempre preguntarse algunas preguntas básicas de la red antes de que empiece la fase del diseño. ¿Quién va a usar la red? ¿Qué tareas van a desempeñar los usuarios en la red? ¿Quién va a administrar la red? Igualmente importante ¿Quién va a pagar por ella? ¿Quién va a pagar la mantenerla? Cuando esas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más productivo. Estas prioridades se convertirán en las metas del diseño. Vamos a examinar algunas de esas metas clave.

- **Desempeño (performance):** Los tipos de datos procesados pueden determinar el grado de desempeño requerido. Si la función principal de la red es transacciones en tiempo real, entonces el desempeño asume una muy alta prioridad y desafortunadamente el costo de eleva súbitamente en este trueque desempeño/costo.
- **Volumen proyectado de tráfico:** Algunos equipos de interconexión como los puentes, concentradores pueden ocasionar cuellos de botella (bottlenecks) en las redes con tráfico pesado. Cuando se está diseñando una red se debe de incluir el número proyectado de usuarios, el tipo de trabajo que los usuarios harán, el tipo de aplicaciones que se correrán y el monto de comunicaciones remotas (www, ftp, telnet, VoIP, realaudio, etc). ¿Podrán los usuarios enviar ráfagas cortas de información o ellos podrán enviar grandes archivos? Esto es particularmente importante para determinar el monto de gráficas que se podrán transmitir sobre la red. Si bien un diseñador de red no puede predecir el futuro, éste debe de estar al tanto de las tendencias de la industria. Si un servidor de fax o email va a hacer instalado en la red, entonces el diseñador deberá de anticipar que estos nuevos elementos no afecten grandemente al volumen actual de tráfico de la red.
- **Expansión futura:** Las redes están siempre en continuo creciendo. Una meta del diseño deberá ser planear para el crecimiento de la red para que las necesidades compañía no saturen en un futuro inmediato. Los nodos deberán ser diseñados para que estos puedan ser enlazados al mundo exterior. ¿Cuántas estaciones de trabajo puede soportar el sistema operativo de red? ¿La póliza de precios del vendedor de equipos hace factible la expansión futura? ¿El ancho de banda del medio de comunicación empleado es suficiente para futuro crecimiento de la red? ¿El

equipo de comunicaciones tiene puertos disponibles para futuras conexiones?

- **Seguridad:** Muchas preguntas de diseño están relacionadas a la seguridad de la red. ¿Estarán encriptados los datos? ¿Qué nivel de seguridad en los *passwords* es deseable? ¿Son las demandas de seguridad lo suficientemente grandes para requerir cable de fibra óptica? ¿Qué tipos de sistema de respaldo son requeridos para asegurar que los datos perdidos siempre puedan ser recuperados? Si la red local tiene acceso a usuarios remotos, ¿Que tipo de seguridad será implementada para prevenir que *hackers* entren a nuestra red?
- **Redundancia:** Las redes robustas requieren redundancia, si algún elemento falla, la red deberá por sí misma deberá seguir operando. Un sistema tolerante a fallas debe estar diseñado en la red, de tal manera, si un servidor falla, un segundo servidor de respaldo entrará a operar inmediatamente. La redundancia también se aplica para los enlaces externos de la red. Los enlaces redundantes aseguran que la red siga funcionando en caso de que un equipo de comunicaciones falle o el medio de transmisión en cuestión. Es común que compañías tengan enlaces redundantes, si el enlace terrestre falla (por ejemplo, una línea privada), entra en operación el enlace vía satélite o vía microondas. Es lógico que la redundancia cueste, pero a veces es inevitable.
- **Compatibilidad: hardware & software** La compatibilidad entre los sistemas, tanto en *hardware* como en *software* es una pieza clave también en el diseño de una red. Los sistemas deben ser compatibles para que estos dentro de la red puedan funcionar y comunicarse entre sí, por lo que el diseñador de la red, deberá tener cuidado de seleccionar los protocolos mas estándares, sistemas operativos de red, aplicaciones (como un simple procesador de palabras). Así como de tener a la mano el *conversor* de un formato a otro.
- **Compatibilidad: organización & gente:** Ya una vez que la red esta diseñada para ser compatible con el hardware y software existente, sería un gran error si no se considera la organización y el personal de la compañía. A veces ocurre que se tienen sistemas de la más alta tecnología y no se tiene el personal adecuado para operarlos. O lo contrario, se tiene personal con amplios conocimientos y experiencia operando sistemas obsoletos. Para tener éxito, la red deberá trabajar dentro del marco de trabajo de las tecnologías y filosofías existentes.
- **Costo :** El costo que implica diseñar, operar y mantener una red, quizá es uno de los factores por los cuales las redes no tengan la seguridad, redundancia, proyección a futuro y personal adecuado. Seguido ocurre que las redes se adapten al escaso presupuesto y todos las metas del diseño anteriores no se puedan implementar. Los directivos, muchas veces no tienen idea del alto costo que tiene un equipo de comunicaciones, un sistema operativo para múltiple usuarios y muchas veces no piensan en el

mantenimiento. El costo involucrado siempre será un factor importante para el diseño de una red.

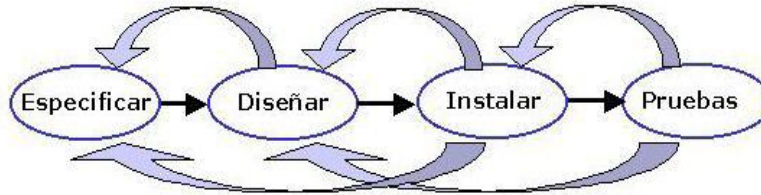


Ilustración 6 - pasos en el proceso de construcción e implementación de una red

- ❖ El paso de **Especificación de Requerimientos** es la etapa preliminar y es donde se especifican todos los requerimientos y variables que van a estar presentes en el diseño de una red.
- ❖ La Fase de **Diseño**, toma los elementos de la Especificación para diseñar la red en base a las necesidades de la organización. Cualquier punto no previsto se revisa y se lleva a la fase anterior de Especificación de Requerimientos.
- ❖ La fase de **Instalación** se toman "los planos" de la fase de diseño y se empiezan a instalar físicamente los dispositivos y elementos de la red. Cualquier imprevisto se regresa nuevamente a la fase de Diseño o en su caso a la fase de Especificación.
- ❖ La fase de **Pruebas** es la fase final del proceso y consiste en realizar toda clase de pruebas a la red ya instalada para comprobar o constatar que cumple con las Especificaciones de Requerimientos. Ya realizadas las pruebas con éxito la red está lista para su uso. Cualquier imprevisto, se regresa a las fases anteriores.

3.1.1 **Diseño estratégico de redes.**

Cuando hablamos de redes en algún lugar, estamos hablando de un trabajo arduo que abarca el diseño e instalación de un centro de cómputo que cuente con las características y requerimientos deseados, ya que este tipo de tecnologías e instalaciones requieren ciertos estándares para su correcto funcionamiento, por lo que describiremos algunas características:

1. En primer lugar debemos ver que el lugar o espacio donde se va a instalar la red cumpla con los requerimientos establecidos como pueden ser: libre de humedad, estática eléctrica, sin daños en techo y libre de polvo.
2. Se debe decidir la topología de red a utilizar (estrella, anillo, etc.).
3. El tipo de conectividad, es decir si por cable (Par trenzado, coaxial, etc.) o bien si será inalámbrico, cuantos cables se utilizarán para los puntos de acceso inalámbrico. Se deben revisar los cables y conexiones para que se asegure la continuidad del paso de la información a través de la red realizada.

4. La cantidad salidas necesarias de acuerdo a la cantidad de equipos que se conectarán a la red que se está diseñando, así como la planeación de la manera en que estarán ubicadas las computadoras, si hacia la pared, o bien por filas, en el caso de grandes instalaciones, el lugar donde estarán ubicados los puntos de enlace, puentes, repetidores y puntos de acceso inalámbrico para la red en los departamentos. Estos deben también estar de preferencia fuera de la vista de los usuarios; identificables y bien resguardados.
5. Designar el lugar del sitio donde se encontrarán los concentradores, ruteadores, servidores de datos y demás equipo necesario para el funcionamiento de la red.
6. De preferencia marcar en un plano, o diseñar un croquis de donde se localizarán cada uno de los puntos mencionados anteriormente.
7. Acondicionar el clima ambiental del lugar, los aparatos de red no deben estar expuestos a las altas temperaturas por lo que se recomienda para el lugar donde se encuentra el sitio principal de la red a una temperatura ambiente de 22 grados centígrados.
8. La instalación eléctrica requerida para el sitio principal y puntos de acceso a la red debe ser normalizada a 120 volts, contar con unidades de batería de respaldo para poder proteger el equipo de posibles descomposturas.

El diseño de la red es importante ya que gracias a esta obtendremos una red robusta, sin problemas de comunicación tanto interna como externa. Por lo que debemos decidir bien las características para la creación e implementación de una red.

Es importante que para las redes inalámbricas se ubiquen bien los puntos de acceso, que todos los accesorios que se van a utilizar en este tipo de red sean de una misma marca, para evitar incompatibilidades, por ejemplo si vamos a implementar una red inalámbrica de tipo “G” todos los accesorios deben ser para este tipo de conectividad y marca.

3.2 Administración de Redes.

Cuando se implementa una red dentro de una organización, debemos contar con el personal capacitado para la administración de esta, es decir contar con un Administrador de red (Net Administrador). El cual dentro de sus actividades debe realizar:

- ✓ Supervisar cableados y el buen funcionamiento de todos los aparatos involucrados en la red y conectividad.
- ✓ Supervisar el tráfico de la red, por medio de herramientas de software alternas o bien administrar por medio de un firewall si se cuenta con el para determinar accesos y bloqueos dentro de la red.
- ✓ Establecer puntos para servicio de impresión.
- ✓ Verificar que la red se encuentre libre de virus o intrusos.

- ✓ Realizar el mantenimiento a la red, como además del chequeo de virus, cableados, conexiones, hardware relacionado con la red.
- ✓ Realizar acciones correctivas en caso de fallas en la red.
- ✓ Tener un control de registro de las direcciones IP que utilizan los usuarios en la red.
- ✓ Realizar una bitácora de las actividades realizadas en la red.
- ✓ Documentar fallas y correcciones.
- ✓ Revisión de la continuidad eléctrica para evitar daños en el equipo de red.

El administrador de red es la persona responsable de la red por lo que debe tener un control estricto sobre las actividades dentro del sitio de red y en las actividades diarias de la organización, pues el fin es evitar fallas en la red y si surge alguna rápidamente realizar la acción correctiva.

4 Division en subredes

La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabajen a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio. El Subneteo permite una mejor administración, control del tráfico y seguridad al segmentar la red por función. También, mejora la performance de la red al reducir el tráfico de broadcast de nuestra red. Como desventaja, su implementación desperdicia muchas direcciones, sobre todo en los enlaces seriales.

4.1 Dirección IP Clase A, B, C, D y E

Las direcciones IP están compuestas por 32 bits divididos en 4 octetos de 8 bits cada uno. A su vez, un bit o una secuencia de bits determinan la Clase a la que pertenece esa dirección IP. Cada clase de una dirección de red determina una máscara por defecto, un rango IP, cantidad de redes y de hosts por red.

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

Ilustración 7 - Tabla de Clases

Cada Clase tiene una máscara de red por defecto, la Clase A 255.0.0.0, la Clase B 255.255.0.0 y la Clase C 255.255.255.0. Al direccionamiento que utiliza la máscara de red por defecto, se lo denomina “direccionamiento con clase” (classful addressing).

Clase de dirección IP:	Bits de mayor peso	Primer intervalo de dirección de octeto	Número de bits en la dirección de red
Clase A	0	0 - 127 *	8
Clase B	10	128 - 191	16
Clase C	110	192 - 223	24
Clase D	1110	224 - 239	28

Ilustración 8 - Tabla de Pesos según Clase

CLASE A	Red	Host		
Octeto	1	2	3	4
Bits	11111111	00000000	00000000	00000000
Mascara (defecto)	255	0	0	0

Dirección de Red: Primer octeto (8 bits)

Dirección de Host: Últimos 3 octetos (24 bits)

CLASE B	Red		Host	
Octeto	1	2	3	4
Bits	11111111	11111111	00000000	00000000
Mascara x defecto	255	255	0	0

Dirección de Red: Primeros 2 octetos (16 bits)

Dirección de Host: Últimos 2 octetos (16 bits)

CLASE C	Red			Host
Octeto	1	2	3	4
Bits	11111111	11111111	11111111	00000000
Mascara x defecto	255	255	255	0

Dirección de Red: Primeros 3 octetos (24 bits)

Dirección de Host: Último octeto (8 bits)

Ilustración 9 - Máscaras por Defecto

Siempre que se subnetea se hace a partir de una dirección de red Clase A, B, o C y está se adapta según los requerimientos de subredes y hosts por subred. Tengan en cuenta que no se puede subnetear una dirección de red sin Clase ya que ésta ya pasó por ese proceso, aclaro esto porque es un error muy común. Al direccionamiento que utiliza la máscara de red adaptada (subneteada), se lo denomina “direccionamiento sin clase” (classless addressing). En consecuencia, la Clase de una dirección IP es definida por su máscara de red y no por su dirección IP. Si una dirección tiene su máscara por defecto pertenece a una Clase A, B o C, de lo contrario no tiene Clase aunque por su IP pareciese la tuviese.

4.2 Máscara de Red

Otro aspecto del direccionamiento IP que es muy importante para saber como el direccionamiento IP opera es el uso de las máscaras de subred (subnet masks).

La subnet mask para una dirección IP en particular es utilizada por los enrutadores para resolver que parte de la dirección IP provee la dirección de red y que parte provee la dirección del host.

La gran pregunta es como el enrutador utiliza la máscara de subred para determinar que parte de una dirección IP se refiere a la dirección de red. Las direcciones IP y la máscara de red son vistas por el enrutador en formato binario. Los bits de la subred y los bits correspondientes de la dirección IP se les aplica un **AND** lógico. Cuando los dos bits correspondientes son 1s el resultado es 1, en caso contrario es 0.

A	B	A AND B
0	0	0
1	0	0
0	1	0
1	1	1

Ilustración 10 - Tabla de Verdad o AND lógico

Ejemplo 1:

Dirección IP: 180.20.5.9

Subnet mask: 255.255.0.0

Host address 180.20.5.9	10110100 00010100 00000101 00001001
Mascara subred 255.255.0.0	11111111 11111111 00000000 00000000 AND
Subred 180.20.0.0	10110100 00010100 00000000 00000000
Broadcast 180.20.255.255	10110100 00010100 11111111 11111111
Primer host 180.20.0.1	10110100 00010100 00000000 00000001
Ultimo host 180.20.255.254	10110100 00010100 11111111 11111110

La dirección de red resultante de 180.20.5.9 AND 255.255.0.0 es 180.20.0.0 (según las reglas del AND de la tabla de verdad)

10110100 00010100 00000101 00001001 (180.20.5.9)

11111111 11111111 00000000 00000000 (255.255.0.0)

10110100 00010100 00000000 00000000 (180.20.0.0)

La máscara de red se divide en 2 partes:

4.2.1 Porción de Red:

En el caso que la máscara sea por defecto, una dirección con Clase, la cantidad de bits "1" en la porción de red, indican la dirección de red, es decir, la parte de la dirección IP que va a ser común a todos los hosts de esa red. En el caso que sea una máscara adaptada, el tema es más complejo. La parte de la máscara de red cuyos octetos sean todos bits "1" indican la dirección de red y va a ser la parte de la dirección IP que va a ser común a todos los hosts de esa red, los bits "1" restantes son los que en la dirección IP se van a modificar para generar las diferentes subredes y van a ser común solo a los hosts que pertenecen a esa subred (asi explicado parece engorroso, así que más abajo les dejo ejemplos). En ambos caso, con Clase o sin, determina el prefijo que suelen ver después de una dirección IP (ej: /8, /16, /24, /18, etc.) ya que ese número es la suma de la cantidad de bits "1" de la porción de red.

4.2.2 Porción de Host:

La cantidad de bits "0" en la porción de host de la máscara, indican que parte de la dirección de red se usa para asignar direcciones de host, es decir, la parte de la dirección IP que va a variar según se vayan asignando direcciones a los hosts.

Ejemplos:

Si tenemos la dirección IP Clase C 192.168.1.0/24 y la pasamos a binario, los primeros 3 octetos, que coinciden con los bits "1" de la máscara de red (fondo rojo), es la dirección de red, que va a ser común a todos los hosts que sean asignados en el último octeto (fondo gris). Con este mismo criterio, si tenemos una dirección Clase B, los 2 primeros octetos son la dirección de red que va a ser común a todos los hosts que sean asignados en los últimos 2 octetos, y si tenemos una dirección Clase A, el 1 octeto es la dirección de red que va a ser común a todos los hosts que sean asignados en los últimos 3 octetos.

Porción de Red			Porción de Host			
192	.	168	.	1	.	0
11000000	.	10101000	.	00000001	.	00000000
255	.	255	.	255	.	0
11111111	.	11111111	.	11111111	.	00000000 = /24

Si en vez de tener una dirección con Clase tenemos una ya subneteada, por ejemplo la 132.18.0.0/22, la cosa es más compleja. En este caso los 2 primeros octetos de la dirección IP, ya que los 2 primeros octetos de la máscara de red tienen todos bits "1" (fondo rojo), es la dirección de red y va a ser común a todas las subredes y hosts. Como el 3º octeto está dividido en 2, una parte en la porción de red y otra en la de host, la parte de la dirección IP que corresponde a la porción de red (fondo negro), que tienen en la máscara de red los bits "1", se va a ir modificando según se vayan asignando las subredes y solo va a ser común a los host que son parte de esa subred. Los 2 bits "0" del 3º octeto en la porción de host (fondo gris) y todo el último octeto de la dirección IP, van a ser utilizados para asignar direcciones de host.

Porción de Red				Porción de Host			
132	.	18	.	0	.	0	
10000100	.	00010010	.	00000000	00	.	00000000
255		255	.	252	.	0	
11111111	.	11111111	.	11111100	00	.	00000000 = /22
				Subredes			

4.2.3 Convertir Bits en Números Decimales

Como sería casi imposible trabajar con direcciones de 32 bits, es necesario convertirlas en números decimales. En el proceso de conversión cada bit de un intervalo (8 bits) de una dirección IP, en caso de ser "1" tiene un valor de "2" elevado a la posición que ocupa ese bit en el octeto y luego se suman los resultados. Explicado parece medio engorroso pero con la tabla y los ejemplos se va a entender mejor.

Posición y Valor de los Bits								
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binario	1	0	0	0	0	0	0	0
Decimal	128	0	0	0	0	0	0	0
= 128								
Binario	0	1	0	0	0	0	0	0
Decimal	0	64	0	0	0	0	0	0
+ = 64								
Binario	0	0	1	0	0	0	0	0
Decimal	0	0	32	0	0	0	0	0
+ = 32								
Binario	0	0	0	1	0	0	0	0
Decimal	0	0	0	16	0	0	0	0
+ = 16								
Binario	0	0	0	0	1	0	0	0
Decimal	0	0	0	0	8	0	0	0
+ = 8								
Binario	0	0	0	0	0	1	0	0
Decimal	0	0	0	0	0	4	0	0
+ = 4								
Binario	0	0	0	0	0	0	1	0
Decimal	0	0	0	0	0	0	2	0
+ = 2								
Binario	0	0	0	0	0	0	0	1
Decimal	0	0	0	0	0	0	0	1
+ = 1								
= 255								

Ilustración 11 - Tabla de Conversion de binario a decimal y viceversa

$$\begin{array}{cccccccc}
 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 2^7 & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \\
 \hline
 128 & + & 64 & + & 32 & + & 16 & + & 8 & + & 4 & + & 2 & + & 1 & = & 255
 \end{array}$$

$$\begin{array}{cccccccc}
 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 2^7 & 2^6 & & & & & & \\
 \hline
 128 & + & 64 & & & & & & = & 192
 \end{array}$$

$$\begin{array}{cccccccc}
 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
 2^7 & & 2^5 & & 2^3 & 2^2 & & \\
 \hline
 128 & + & 32 & + & 8 & + & 4 & = & 172
 \end{array}$$

La combinación de 8 bits permite un total de 256 combinaciones posibles que cubre todo el rango de numeración decimal desde el 0 (00000000) hasta el 255 (11111111). Algunos ejemplos.

00000000 = 0	00010100 = 20	10100000 = 160
00000001 = 1	00011110 = 30	10110100 = 180
00000010 = 2	00101000 = 40	11010000 = 200
00000011 = 3	00110010 = 50	11011100 = 220
00000100 = 4	00111100 = 60	11110000 = 240
00000101 = 5	01000110 = 70	11111010 = 250
00000110 = 6	01010000 = 80	11111011 = 251
00000111 = 7	01011010 = 90	11111100 = 252
00001000 = 8	01100100 = 100	11111101 = 253
00001001 = 9	01111000 = 120	11111110 = 254
00001010 = 10	10001100 = 140	11111111 = 255

Ilustración 12 - Ejemplos de conversiones

4.2.4 Calcular la Cantidad de Subredes y Hosts por Subred

Cantidad de Subredes es igual a: 2^N , donde "N" es el número de bits "robados" a la porción de Host. Cantidad de Hosts x Subred es igual a: $2^M - 2$, donde "M" es el número de bits disponible en la porción de host y "-2" es debido a que toda subred debe tener su propia dirección de red y su propia dirección de broadcast.

Aclaración: Originalmente la fórmula para obtener la cantidad de subredes era $2^N - 2$, donde "N" es el número de bits "robados" a la porción de host y "-2" porque la primer subred (subnet zero) y la última subred (subnet broadcast) no eran utilizables ya que contenían la dirección de la red y broadcast respectivamente. Todos los tutoriales que andan dando vueltas en Internet utilizan esa fórmula. Actualmente para obtener la cantidad de subredes se utiliza y se enseña con la fórmula 2^N , que permite utilizar tanto la subred zero como la subnet broadcast para ser asignadas. Bueno, hasta acá la teoría básica. Una vez que comprendemos esto podemos empezar a subnetear.

4.3 Subneteo Manual de una Red Clase A

Dada la dirección IP Clase A 10.0.0.0/8 para una red, se nos pide que mediante subneteo obtengamos 7 subredes. Este es un ejemplo típico que se nos puede pedir, aunque remotamente nos topemos en la vida real. Lo vamos a realizar en 2 pasos:

4.3.1 Adaptar la Máscara de Red por Defecto a Nuestras Subredes

La máscara por defecto para la red 10.0.0.0 es:

Porción de Red		Porción de Host				
255	.	0	.	0	.	0
11111111	.	00000000	.	00000000	.	00000000

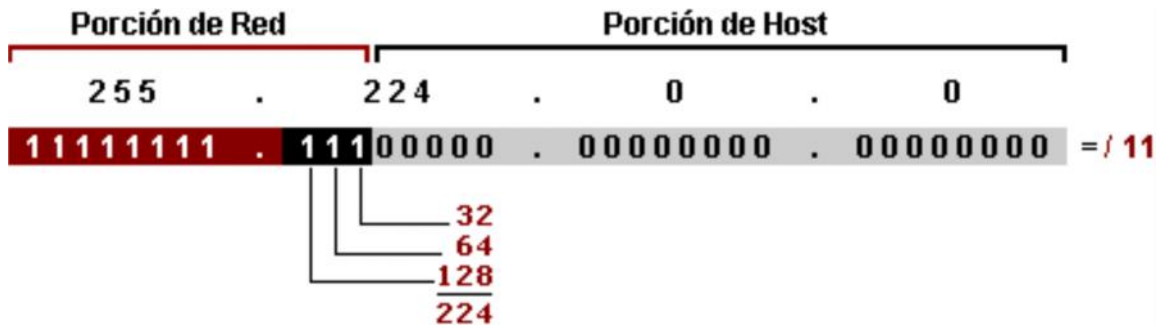
= / 8

Mediante la fórmula 2^N , donde N es la cantidad de bits que tenemos que robarle a la porción de host, adaptamos la máscara de red por defecto a la subred.

En este caso particular $2^N = 7$ (o mayor) ya que nos pidieron que hagamos 7 subredes.

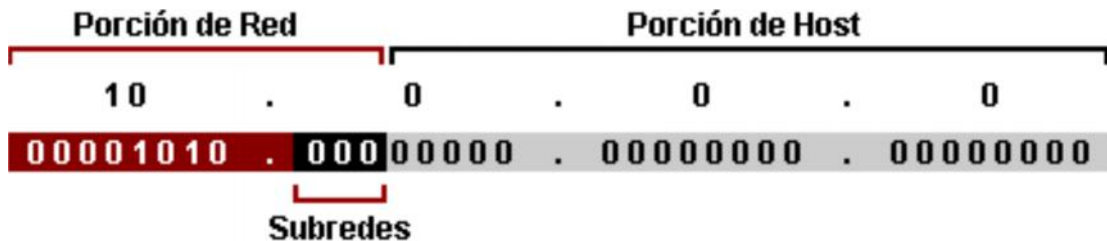
2^N	Redes	Máscara Binario	Máscara Decimal
2^1	2	11111111 . 10000000 . 00000000 . 00000000	255 . 128 . 0 . 0
2^2	4	11111111 . 11000000 . 00000000 . 00000000	255 . 192 . 0 . 0
2^3	8	11111111 . 11100000 . 00000000 . 00000000	255 . 224 . 0 . 0
2^4	16	11111111 . 11110000 . 00000000 . 00000000	255 . 240 . 0 . 0
2^5	32	11111111 . 11111000 . 00000000 . 00000000	255 . 248 . 0 . 0
2^6	64	11111111 . 11111100 . 00000000 . 00000000	255 . 252 . 0 . 0
2^7	128	11111111 . 11111110 . 00000000 . 00000000	255 . 254 . 0 . 0

Una vez hecho el cálculo nos da que debemos robar 3 bits a la porción de host para hacer 7 subredes o más y que el total de subredes útiles va a ser de 8, es decir que va a quedar 1 para uso futuro. Tomando la máscara Clase A por defecto, a la parte de red le agregamos los **3 bits** que le robamos a la porción de host reemplazándolos por "1" y así obtenemos 255.224.0.0 que es la máscara de subred que vamos a utilizar para todas nuestras subredes y hosts.



4.3.2 Obtener Rango de Subredes

Para obtener las subredes se trabaja únicamente con la dirección IP de la red, en este caso 10.0.0.0. Para esto vamos a modificar el mismo octeto de bits (el segundo) que modificamos anteriormente en la máscara de red pero esta vez en la dirección IP.

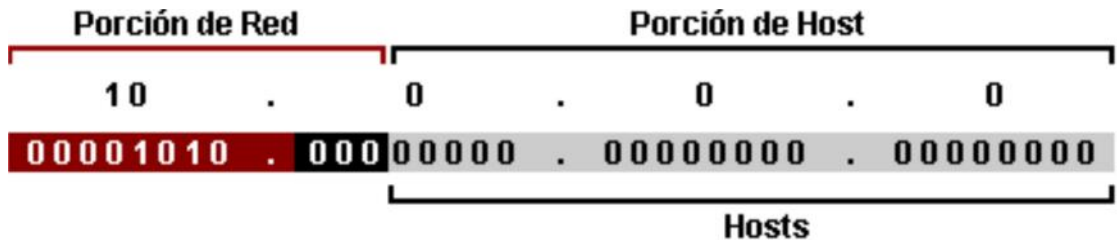


Para obtener el rango hay varias formas, la que me parece más sencilla a mí es la de restarle a 256 el número de la máscara de red adaptada. En este caso sería: $256 - 224 = 32$, entonces 32 va a ser el rango entre cada subred.

N° de Subred	Rango IP *		Hosts Asignables x Subred
	Desde	Hasta	
1	10.0.0.0	10.31.255.255	2.097.150
2	10.32.0.0	10.63.255.255	2.097.150
3	10.64.0.0	10.95.255.255	2.097.150
4	10.96.0.0	10.127.255.255	2.097.150
5	10.128.0.0	10.159.255.255	2.097.150
6	10.160.0.0	10.191.255.255	2.097.150
7	10.192.0.0	10.223.255.255	2.097.150
8	10.224.0.0	10.255.255.255	2.097.150

* La primera y la última dirección IP de cada Subred no se asignan ya que contienen la dirección de red y broadcast de la Subred.

Si queremos calcular cuántos hosts vamos a obtener por subred debemos aplicar la fórmula $2^M - 2$, donde **M** es el número de bits "0" disponible en la porción de host de la dirección IP de la red y **- 2** es debido a que toda subred debe tener su propia dirección de red y su propia dirección de broadcast.



En este caso particular sería:

$$2^{21} - 2 = 2.097.150 \text{ hosts utilizables por subred.}$$

4.4 Subneteo Manual de una Red Clase B

Dada la red Clase B 132.18.0.0/16 se nos pide que mediante subneteo obtengamos un mínimo de 50 subredes y 1000 hosts por subred. Lo vamos a realizar en 3 pasos:

4.4.1 Adaptar la Máscara de Red por Defecto a Nuestras Subredes

La máscara por defecto para la red 132.18.0.0 es:

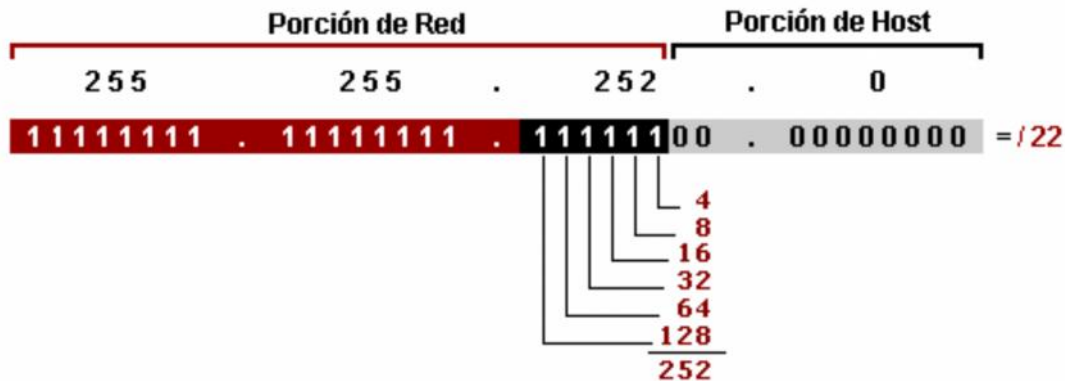


Usando la fórmula 2^N , donde **N** es la cantidad de bits que tenemos que robarle a la porción de host, adaptamos la máscara de red por defecto a la subred.

En este caso particular $2^N = 50$ (o mayor) ya que necesitamos hacer 50 subredes.

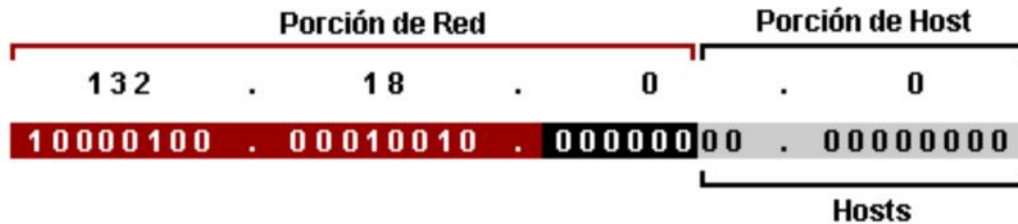
2^N	Redes	Máscara Binario	Máscara Decimal
2^1	2	11111111 . 11111111 . 10000000 . 00000000	255 . 255 . 128 . 0
2^2	4	11111111 . 11111111 . 11000000 . 00000000	255 . 255 . 192 . 0
2^3	8	11111111 . 11111111 . 11100000 . 00000000	255 . 255 . 224 . 0
2^4	16	11111111 . 11111111 . 11110000 . 00000000	255 . 255 . 240 . 0
2^5	32	11111111 . 11111111 . 11111000 . 00000000	255 . 255 . 248 . 0
2^6	64	11111111 . 11111111 . 11111100 . 00000000	255 . 255 . 252 . 0
2^7	128	11111111 . 11111111 . 11111110 . 00000000	255 . 255 . 254 . 0
2^8	256	11111111 . 11111111 . 11111111 . 00000000	255 . 255 . 255 . 0
2^9	512	11111111 . 11111111 . 11111111 . 10000000	255 . 255 . 255 . 128
2^{10}	1024	11111111 . 11111111 . 11111111 . 11000000	255 . 255 . 255 . 192

El cálculo nos da que debemos robar 6 bits a la porción de host para hacer 50 subredes o más y que el total de subredes útiles va a ser de 64, es decir que van a quedar 14 para uso futuro. Entonces a la máscara Clase B por defecto le agregamos los 6 bits robados reemplazándolos por "1" y obtenemos la máscara adaptada 255.255.252.0.



4.4.2 Obtener Cantidad de Hosts por Subred

Una vez que adaptamos la máscara de red a nuestras necesidades, ésta no se vuelve a tocar y va a ser la misma para todas las subredes y hosts que componen esta red. De acá en más solo trabajaremos con la dirección IP de la red. En este caso con la porción de host (fondo gris).



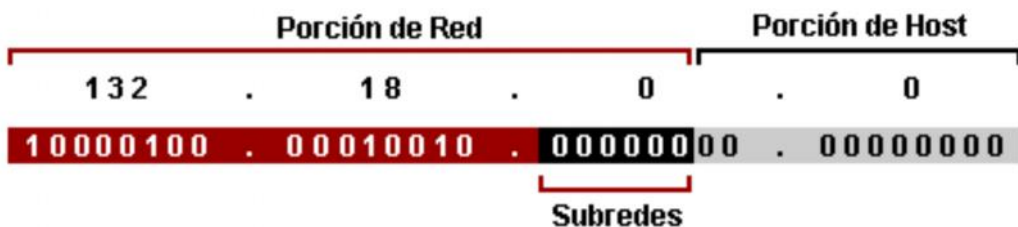
El ejercicio nos pedía, además de una cantidad de subredes que ya alcanzamos adaptando la máscara en el primer paso, una cantidad específica de 1000 hosts por subred. Para verificar que sea posible obtenerlos con la nueva máscara, no siempre se puede, utilizamos la fórmula $2^M - 2$, donde **M** es el número de bits "0" disponibles en la porción de host y **- 2** es debido a que la primer y última dirección IP de la subred no son utilizables por ser la dirección de la subred y broadcast respectivamente.

$$2^{10} - 2 = 1022 \text{ hosts por subred.}$$

Los 10 bits "0" de la porción de host (fondo gris) son los que más adelante modificaremos según vayamos asignando los hosts a las subredes.

4.4.3 Obtener Rango de Subredes

Para obtener las subredes se trabaja con la porción de red de la dirección IP de la red, más específicamente con la parte de la porción de red que modificamos en la máscara de red pero esta vez en la dirección IP. Recuerden que a la máscara de red con anterioridad se le agregaron 6 bits en el tercer octeto, entonces van a tener que modificar esos mismos bits pero en la dirección IP de la red (fondo negro).



Los 6 bits "0" de la porción de red (fondo negro) son los que más adelante modificaremos según vayamos asignando las subredes. Para obtener el rango hay varias formas, la que me parece más sencilla a mí es la de restarle a 256 el número de la máscara de subred adaptada. En este caso sería: **256-252=4**, entonces **4** va a ser el rango entre cada subred. En el gráfico solo puse las primeras 10 subredes y las últimas 5 porque iba a quedar muy largo, pero la dinámica es la misma.

N° de Subred	Rango IP *		Hosts Asignables x Subred
	Desde	Hasta	
1	132.18.0.0	132.18.3.255	1.022
2	132.18.4.0	132.18.7.255	1.022
3	132.18.8.0	132.18.11.255	1.022
4	132.18.12.0	132.18.15.255	1.022
5	132.18.16.0	132.18.19.255	1.022
6	132.18.20.0	132.18.23.255	1.022
7	132.18.24.0	132.18.27.255	1.022
8	132.18.28.0	132.18.31.255	1.022
9	132.18.32.0	132.18.35.255	1.022
10	132.18.36.0	132.18.39.255	1.022
...			
60	132.18.236.0	132.18.239.255	1.022
61	132.18.240.0	132.18.243.255	1.022
62	132.18.244.0	132.18.247.255	1.022
63	132.18.248.0	132.18.251.255	1.022
64	132.18.252.0	132.18.255.255	1.022

* La primera y la última dirección IP de cada Subred no se asignan ya que contienen la dirección de red y broadcast de la Subred.

4.5 Subneteo Manual de una Red Clase C

Nos dan la dirección de red Clase C 192.168.1.0 /24 para realizar mediante subneteo 4 subredes con un mínimo de 50 hosts por subred. Lo vamos a realizar en 3 pasos:

4.5.1 Adaptar la Máscara de Red por Defecto a Nuestras Subredes

La máscara por defecto para la red 192.168.1.0 es:

Porción de Red			Porción de Host	
255	.	255	.	0
11111111	.	11111111	.	00000000

= /24

Usando la fórmula 2^N , donde **N** es la cantidad de bits que tenemos que robarle a la porción de host, adaptamos la máscara de red por defecto a la subred.

Se nos solicitaron 4 subredes, es decir que el resultado de 2^N tiene que ser mayor o igual a 4.

2^N	Redes	Máscara Binario	Máscara Decimal
2^1	2	11111111 . 11111111 . 11111111 . 10000000	255 . 255 . 255 . 128
2^2	4	11111111 . 11111111 . 11111111 . 11000000	255 . 255 . 255 . 192
2^3	8	11111111 . 11111111 . 11111111 . 11100000	255 . 255 . 255 . 224
2^4	16	11111111 . 11111111 . 11111111 . 11110000	255 . 255 . 255 . 240
2^5	32	11111111 . 11111111 . 11111111 . 11111000	255 . 255 . 255 . 248
2^6	64	11111111 . 11111111 . 11111111 . 11111100	255 . 255 . 255 . 252

Como vemos en el gráfico, para hacer 4 subredes debemos robar 2 bits a la porción de host. Agregamos los 2 bits robados reemplazándolos por "1" a la máscara Clase C por defecto y obtenemos la máscara adaptada 255.255.255.192.



4.5.2 Obtener Cantidad de Hosts por Subred

Ya tenemos nuestra máscara de red adaptada que va a ser común a todas las subredes y hosts que componen la red. Ahora queda obtener los hosts. Para esto vamos a trabajar con la dirección IP de red, específicamente con la porción de host (fondo gris).



El ejercicio nos pedía un mínimo de 50 hosts por subred. Para esto utilizamos la fórmula $2^M - 2$, donde M es el número de bits "0" disponibles en la porción de host y $- 2$ porque la primer y última dirección IP de la subred no se utilizan por ser la dirección de la subred y broadcast respectivamente.

$$2^6 - 2 = 62 \text{ hosts por subred.}$$

Los 6 bits "0" de la porción de host (fondo gris) son los vamos a utilizar según vayamos asignando los hosts a las subredes.

4.5.3 Obtener Rango de Subredes

Para obtener el rango subredes utilizamos la porción de red de la dirección IP que fue modificada al adaptar la máscara de red. A la máscara de red se le agregaron 2 bits en el cuarto octeto, entonces van a tener que modificar esos mismos bits pero en la dirección IP (fondo negro).



Los 2 bits "0" de la porción de red (fondo negro) son los que más adelante modificaremos según vayamos asignando las subredes. Para obtener el rango la forma más sencilla es restarle a 256 el número de la máscara de subred adaptada. En este caso sería: $256-192=64$, entonces **64** va a ser el rango entre cada subred.

N° de Subred	Rango IP *		Hosts Asignables x Subred
	Desde	Hasta	
1	192.168.1.0	192.168.1.63	62
2	192.168.1.64	192.168.1.127	62
3	192.168.1.128	192.168.1.191	62
4	192.168.1.192	192.168.1.255	62

* La primera y la última dirección IP de cada Subred no se asignan ya que contienen la dirección de red y broadcast de la Subred.

5 Fundamentos de IPv6

5.1 Conceptos

5.1.1 Protocolo de Internet versión 6 (Internet Protocol version 6, IPv6)

Debido al crecimiento del Internet y la sofisticación de los dispositivos electrónicos, las soluciones propuestas con el fin de escalar el espacio de direccionamiento de Internet IPv4, no serán suficientes para cubrir la necesidad de las mismas en los próximos años. Como consecuencia de este escenario, el Grupo Especial sobre Ingeniería de Internet (Internet Engineering Task Force o IETF, por sus siglas en inglés) elaboró una serie de especificaciones para definir un protocolo IP de Siguierte Generación (IP Next Generation, IPng) que actualmente se conoce como Protocolo de Internet versión 6.

5.1.2 Espacio mayor de direccionamiento

El IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits para así soportar más niveles en la jerarquía de direccionamiento y un número mucho mayor de nodos direccionables. El diseño del protocolo agrega múltiples beneficios en seguridad, manejo de calidad de servicio, una mayor capacidad de transmisión y mejora la facilidad de administración, entre otras cosas.

Mientras que IPv4 soporta 4,294,967,296 (2^{32}) direcciones que es poco menos de 4.3 billones, IPv6 ofrece 3.4×10^{38} (2^{128}) direcciones, un número similar a $6.67126144781401e+23$ direcciones IP por cada metro cuadrado sobre la superficie de la Tierra. Adicionalmente, la dirección IPv6 se diseñó para ser subdividida en dominios de enrutamiento jerárquico que reflejan la topología del Internet actual.

5.1.3 Características de IPv6

- El esquema de direcciones de 128 bits provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos.
- Los múltiples niveles de jerarquía permiten juntar rutas, promoviendo un enrutamiento eficiente y escalable al Internet.
- El proceso de autoconfiguración permite que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso.
- La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de reenumerado.
- La difusión ARP es reemplazada por el uso de multicast en el link local.
- El encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
- Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.
- Las nuevas extensiones de encabezado reemplazan el campo Opciones de IPv4 y proveen mayor flexibilidad.
- IPv6 fue esbozado para manejar mecanismos de movilidad y seguridad de manera más eficiente que el protocolo IPv4.
- Se crearon varios mecanismos junto con el protocolo para tener una transición sin problemas de las redes IPv4 a las IPv6.

5.1.4 Jerarquía de direcciones – Agregación de prefijos de red

Un espacio mayor de direcciones de IPv6 permite mayores distribuciones de direcciones a las organizaciones y a los proveedores de servicios de Internet (ISPs). Al tener una gran disponibilidad de direcciones se posibilita el uso de un solo prefijo grande para toda la red de una organización y, por ende, el ISP puede sumar las rutas (agregar) de todos los prefijos de sus clientes en un solo prefijo y anunciarlo al Internet IPv6.

Cuando un usuario final cambia su proveedor de IPv6, el cual le proveía de direccionamiento IPv6, entonces también debe cambiar su prefijo de IPv6 para preservar su agregación global. Al mismo tiempo, el cambiar de proveedor implica una reenumeración de la red.

5.1.5 Modos de configuración de IPv6

Autoconfiguración. Definida en el RFC 2462 y también es conocida como *Configuración Automática de Dirección Sin Estado IPv6*. Esta funcionalidad permite que un ruteador IPv6 envíe, a través del enlace local, la información de red a las computadoras y que ellas puedan configurarse correctamente. La información enviada es el prefijo de IPv6 del enlace local y la ruta por defecto del mismo protocolo. Mediante este mecanismo cada computadora y servidor de IPv6 añade su dirección de capa de enlace (dirección MAC) en el formato EUI-64 al prefijo de IPv6 de unicast global único anunciado en la subred.

Configuración mediante servidor. Las computadoras que utilizan IPv6 pueden obtener sus parámetros y direcciones de configuración de un servidor de DHCP versión 6. Este modo es llamado *Configuración de Direcciones con Estado IPv6*.

5.1.6 Renumeración

El proceso de reenumeración de IPv6 fue diseñado para ser transparente entre los proveedores de IPv6 unicast y los usuarios finales. Esto se logra con el mecanismo de autoconfiguración que permite una reenumeración sencilla a las computadoras con sólo enviarles el nuevo prefijo IPv6 unicast para la red. Una desventaja de este mecanismo es la pérdida de las sesiones TCP y UDP que ocurren entre las computadoras y los servidores al momento exacto de la transición. Esto es algo que también ocurre actualmente con IPv4.

5.1.7 Multicasting

La difusión del Protocolo de Resolución de Dirección (Address Resolution Protocol, ARP) de IPv4 afecta la eficiencia de la red. Esta situación no ha sido incluida en IPv6, y en su lugar se utiliza el Multicasting el cual funciona de la siguiente manera:

- Se crea un grupo Multicast, formado por conjunto de interfases de red.
- Si se está interesado en que cierta computadora reciba los paquetes de difusión del grupo se agrega una interfaz de red, de esa forma se envía un paquete multicast al grupo X.
- Ese paquete sólo llegará a aquellas computadoras que tengan su interfaz incluida en el grupo multicast X. Con ello se permite tener niveles de eficiencia de red superiores a los presentados en IPv4, lo cual se verá traducido en la disminución de los ciclos de procesamiento de CPU de las computadoras en la red local al no procesar paquetes de difusión que no van dirigidos a ellos y de la misma manera se estará eliminando el problema de las tormentas de paquetes de difusión de IPv4.

5.1.8 Encabezado eficiente

El nuevo encabezado de IPv6 es más sencillo que el de IPv4. Del encabezado de IPv4 se removieron 6 campos: Longitud de encabezado, Identificación, Banderas, Desplazamiento por fragmentación, Suma de verificación de encabezado, Opciones y Relleno. Al pasar de un encabezado de IPv4 con longitud variable a IPv6 con menos campos y longitud fija se obtiene una reducción en los ciclos de CPU de los ruteadores al momento de enviar los paquetes de IPv6. Lo anterior conlleva un mejor desempeño de la red.

5.1.9 Etiqueta de flujo

Dentro del encabezado de IPv6 existe un nuevo campo llamado *Etiqueta de Flujo*, éste es usado por el nodo fuente para solicitar un manejo especial de secuencias específicas de paquetes. La etiqueta está dirigida al procesamiento de la estación destino, no para los ruteadores, y es de gran utilidad para aplicaciones como videoconferencias y voz sobre protocolo de Internet (VoIP). Asimismo agrupa todas aquellas que requieren un tratamiento especial de Calidad de Servicio (Quality of Service, QoS) en los ruteadores de la trayectoria.

5.1.10 Extensiones de encabezado

La utilización del campo *Opciones* en el encabezado de IPv4 presenta desventajas a la transmisión de los paquetes y a la eficiencia de la red. En lo que respecta a la variación del tamaño del encabezado es debido a que tiene campos opcionales. En el segundo caso todos los ruteadores que procesan el paquete deben computar el encabezado con su campo de longitud variable lo que introduce retardos y gasto de la capacidad del CPU en ciclos de procesamiento que son innecesarios.

Para resolver la situación anterior, IPv6 sustituye el campo *Opciones* al final del encabezado por las *Extensiones de Encabezado*, formando un encadenamiento de encabezados enlazados por un campo llamado *Siguiente Encabezado*. Se presenta un campo *Siguiente Encabezado* dentro de cada *Extensión de Encabezado* usado por IPv6. Este diseño con extensiones permite una mejor eficiencia en el procesamiento de los paquetes, ya que asegura que los ruteadores y nodos computan los encabezados dirigidos a ellos a lo largo de la trayectoria.

5.1.11 Movilidad

Debido a que la movilidad es una característica importante y deseable por las compañías proveedoras y los consumidores finales el *Protocolo de Internet Móvil* (*MobileIP*) esta capacidad está disponible tanto en IPv4 como en IPv6. Cabe destacar que en este último la movilidad se construyó dentro del protocolo en lugar de ser una nueva función agregada como en IPv4. Ello implica que cualquier nodo IPv6 puede usar un IP *Móvil* tanto como lo requiera. IPv6 *Móvil* utiliza dos Extensiones de Encabezado: un *Encabezado de Enrutamiento* para el registro y un *Encabezado de Destino* para entrega del datagrama entre los nodos móviles y sus nodos fijos correspondientes.

5.1.12 Seguridad

El protocolo *IPSec* estandarizado por el Grupo Especial sobre Ingeniería de Internet provee las funciones de:

- Limitar el acceso a sólo aquellos autorizados.
- Certifica la autenticación de la persona que envía los datos.
- Encripta los datos transmitidos a través de la red.
- Asegura la integridad de los datos.
- Invalida la repetición de sesiones, para evitar que no sean repetidas por usuarios maliciosos.

Los protocolos que respaldan el funcionamiento de *IPSec* son: la *Autenticación de Encabezado (Authentication Header, AH)* y la *Carga de Seguridad Encapsulada (Encapsulated Security Payload, ESP)*. Al estar incluidos en cada implementación de IPv6 se provee mayor seguridad ya que *IPSec* está presente en todos los nodos de la red.

5.1.13 Mecanismos de Transición

Actualmente no existe una fecha definida para dejar de utilizar IPv4 o comenzar a utilizar IPv6 completamente, por lo que al diseñar IPv6 se optó por incluir mecanismos que permitan una coexistencia de ambos esquemas de direccionamiento y que en el largo plazo permitan tener una transición sin complicaciones hacia IPv6. Estos esquemas son los siguientes:

- Nodos de Doble Pila sobre redes IPv4.
- Islas de Nodos de Sólo IPv6 sobre redes IPv4.
- Nodos de IPv4 que puedan comunicarse con redes IPv6.
- Nodos de IPv6 que puedan comunicarse con redes IPv4.

5.2 Estructura del Protocolo IPv6

5.2.1 Encabezado

Como se especifica en el [RFC 2460](#) *Especificación del Protocolo de Internet Versión 6*, el encabezado básico de IPv6 consta de 8 campos, 4 menos que el de IPv4, lo que da un total de 40 octetos.

Veamos, en primer lugar, la descripción de la cabecera de un paquete IPv4:

bits:	4	8	16	20	32
Versión	Cabecera	TOS	Longitud Total		
Identificación			Indicador	Desplazamiento de Fragmentación	
TTL	Protocolo		Checksum		
Dirección Fuente de 32 bits					
Dirección Destino de 32 bits					
Opciones					

Como vemos, la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de

la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso.

En la tabla anterior hemos usado abreviaturas, en aquellos casos en los que son comunes. En el resto, nuestra “particular” traducción de la nomenclatura original anglosajona, cuya “leyenda de equivalencias” indicamos a continuación:

- **Version** – Versión (4 bits)
- **Header** – Cabecera (4 bits)
- **TOS (Type Of Service)** – Tipo de Servicio (1 byte)
- **Total Length** – Longitud Total (2 bytes)
- **Identification** – Identificación (2 bytes)
- **Flag** – Indicador (4 bits)
- **Fragment Offset** – Desplazamiento de Fragmentación (12 bits – 1.5 bytes)
- **TTL (Time To Live)** – Tiempo de Vida (1 byte)
- **Protocol** – Protocolo (1 byte)
- **Checksum** – Código de Verificación (2 bytes)
- **32 bit Source Address** – Dirección Fuente de 32 bits (4 bytes)
- **32 bit Destination Address** – Dirección Destino de 32 bits (4 bytes)

En la tabla anterior, hemos marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que son modificados, según el siguiente esquema:



Hemos pasado de tener 12 campos, en IPv4, a tan solo 8 en IPv6.

El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.).

El caso del campo de “Desplazamiento de Fragmentación”, es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total “inutilidad” de

este campo. En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

- Longitud total → longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).

- Protocolo → siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los encaminadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).
- Tiempo de vida → límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

Los nuevos campos son:

- Clase de Tráfico (Traffic Class), también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).
- Etiqueta de Flujo (Flow Label), para permitir tráfico con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:

bits:	4	12	16	24	32
Versión	Clase de Tráfico	Etiqueta de Flujo			
Longitud de la Carga Util			Siguiente Cabecera	Límite de Saltos	
			Dirección		
			Fuente		
			De		
			128 bits		
			Dirección		
			Destino		
			De		
			128 bits		

El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.

La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, como ya hemos mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesamiento en routers y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin coadyuva, como hemos indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

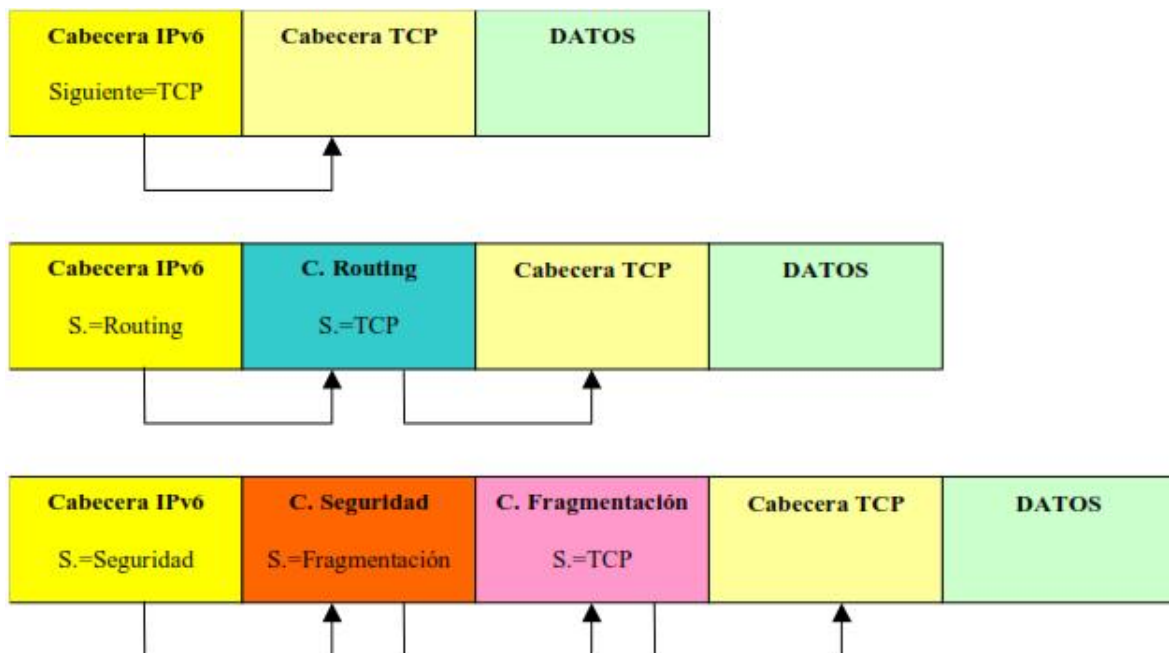
El valor del campo “siguiente cabecera”, indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso “salto a salto” (hop-by-hop). Así tenemos, por citar algunos ejemplos, cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier

caso, han de

ser procesadas en el orden riguroso en que aparecen en el paquete.

Sin entrar en más detalles, véanse a continuación los siguientes ejemplos

gráficos del uso del concepto de las “cabeceras de extensión” (definidas por el campo “siguiente cabecera”), mecanismo por el que cada cabecera es “encadenada” a la siguiente y anterior (si existen):



El MTU (Unidad Máxima de Transmisión), debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

5.2.2 DATOS Cabecera TCP

Dado que IPv6 no realiza verificación de errores de la cabecera, en tráfico UDP, se requiere el empleo del su propio mecanismo de checksum.

5.2.2.1 Extensiones de Encabezado

Son encabezados opcionales, enlazados uno después de otro, que van después del encabezado básico de IPv6. Un paquete IPv6 puede llevar uno o múltiples

extensiones de encabezados o inclusive no llevar ninguno. A continuación se definen las Extensiones de Encabezados:

- **Encabezado de Opciones Salto-por-Salto (protocolo 0).** Este campo es leído y procesado por cada nodo y enrutado a lo largo de la trayectoria de envío. Este es usado para paquetes Jumbograma y la Alerta de Ruteador.
- **Encabezado de Opciones de Destino (protocolo 60).** Lleva información opcional que está específicamente dirigida a la dirección de destino del paquete.
- **Encabezado de Enrutamiento (protocolo 43).** Puede ser usado por un nodo fuente IPv6 para forzar a que un paquete atravesase ruteadores específicos en su trayectoria al destino. Se puede especificar una lista de ruteadores intermediarios dentro del encabezado cuando se pone en 0 el campo de Tipo de Enrutamiento.
- **Encabezado de Fragmentación (protocolo 44).** En IPv6 se recomienda que el mecanismo PMTUD esté en todos los nodos. Si un nodo no soporta PMTUD y debe enviar un paquete más grande que el MTU se utiliza el Encabezado de Fragmentación. Cuando esa situación ocurre el nodo fragmenta el paquete y envía cada parte utilizando Encabezados de Fragmentación, los cuales son acumulados en el extremo receptor donde el nodo destino los reensambla para formar el paquete original.
- **Encabezado de Autenticación (protocolo 51).** Este se utiliza en IPSec para proveer autenticación, integridad de datos y protección ante una repetición, e incluye también protección a algunos campos del encabezado básico de IPv6. Este encabezado es conocido como *AH*.
- **Encabezado de Carga de Seguridad Encapsulada (protocolo 50).** Es usado en IPSec para proveer autenticación, integridad de datos, protección ante repetición y confidencialidad del paquete IPv6. Es conocido como *ESP*.

5.3 Direccionamiento

Los cambios introducidos por IPv6 no sólo son en cantidad de direcciones sino que incluyen nuevos tipos, representaciones y sintaxis.

5.3.1 Direcciones y direccionamiento en IPv6 (RFC2373)

Ya hemos dicho que IPv6 nos aporta, como principio fundamental, un espacio de 2128 direcciones, lo que equivale a 3,40E38 (340.282.366.920.938.463.463.374.607.431.768.211.456).

Hagamos una cuenta “rápida”, para hacernos a la idea de lo que esta cifra “impronunciable” implica. Calculemos el número de direcciones IP que podríamos tener por metro cuadrado de la superficie terrestre: ¡nada más y nada menos que 665.570.793.348.866.943.898.599!

Indudablemente, hay cabida para todos los dispositivos que podamos imaginar, no solo terrestres, sino interplanetarios. Aunque, por el momento, no podemos asegurar que tenga capacidad para los dispositivos “intergalácticos”.

5.3.2 Definición de dirección en IPv6

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Dichas direcciones se clasifican en tres tipos:

- ❖ Unicast: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.
- ❖ Anycast: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera “cae”.
- ❖ Multicast: Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

5.3.3 Diferencias con IPv4

Hay algunas diferencias importantes en el direccionamiento de IPv6 respecto de IPv4:

- No hay direcciones broadcast (su función es sustituida por direcciones multicast).
- Los campos de las direcciones reciben nombres específicos; denominamos “prefijo” a la parte de la dirección hasta el nombre indicado (incluyéndolo).
- Dicho prefijo nos permite conocer donde esta conectada una determinada dirección, es decir, su ruta de encaminado.
- Cualquier campo puede contener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.
- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.
- Todas las interfaces han de tener, al menos, una dirección unicast link-local (enlace local).
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast) o ámbito.
- Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.

- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace.

5.3.4 **Reservas de espacio de direccionamiento en IPv6**

A diferencia de las asignaciones de espacio de direccionamiento que se hicieron en IPv4, en IPv6, se ha reservado, que no “asignado”, algo más del 15%, tanto para permitir una fácil transición (caso del protocolo IPX), como para mecanismos requeridos por el propio protocolo.

Estado	Prefijo (en binario)	Fracción del Espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	011	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/512
Direcciones Unicast Locales de Enlace	1111 1110 10	1/1.024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1.024
Direcciones Multicast	1111 1111	1/256

De esta forma se permite la asignación directa de direcciones de agregación, direcciones locales, y direcciones multicast, con reservas para OSI NSAP e IPX. El 85% restantes queda reservado para uso futuro.

Podemos distinguir las direcciones multicast de las unicast por el valor del octeto de mayor orden de la dirección (FF, o 11111111 en binario, indica multi-cast). En cambio, en el caso de las anycast, no hay ninguna diferencia, sintácticamente hablando, y por tanto, son tomadas del espacio de direcciones unicast.

5.3.5 **Direcciones especiales en IPv6**

Se han definido también las direcciones para usos especiales como:

_ Dirección de auto-retorno o Loopback (::1) – No ha de ser asignada a una interfaz física; se trata de una interfaz “virtual”, pues se trata de paquetes que no

salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina).

_ Dirección no especificada (::) – Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección; por ejemplo, cuando se halla en el campo de dirección fuente, indica que se trata de un host que esta iniciándose, antes de que haya aprendido su propia dirección.

_ Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<dirección IPv4>) – Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

80 bits	16 bits	32 bits
0000 ... 0000	0000	dirección IPv4

_ Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:<dirección IPv4>) – permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan “direcciones IPv6 mapeadas desde IPv4”.

80 bits	16 bits	32 bits
0000 ... 0000	FFFF	Dirección IPv4

5.3.6 Representación de las direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

- a) x:x:x:x:x:x:x, donde “x” es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A

- b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplos:

Las direcciones:

1080:0:0:0:8:800:200C:417A (una dirección unicast).
FF01:0:0:0:0:0:0:101 (una dirección multicast).
0:0:0:0:0:0:0:1 (La dirección loopback).
0:0:0:0:0:0:0:0 (una dirección no especificada)

Pueden representarse como:

1080::8:800:200C:417A (una dirección unicast).
FF01::101 (una dirección multicast).
::1 (La dirección loopback).
:: (una dirección no especificada).

- c) Una forma alternativa y muy conveniente, cuando nos hallemos en un entorno mixto IPv4 e IPv6, es $x:x:x:x:x:d:d:d$, donde “x” representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y “d” representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPv4). Ejemplos:

$0:0:0:0:0:13.1.68.3$
 $0:0:0:0:FFFF:129.144.52.38$

Pueden representarse como:

$::13.1.68.3$
 $::FFFF:129.144.52.38$

La representación de los prefijos IPv6 se realiza del siguiente modo:

dirección-IPv6/longitud-del-prefijo

donde:

- dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas
- longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo.

Por ejemplo, las representaciones válidas del prefijo de 60 bits 12AB00000000CD3, son:

$12AB:0000:0000:CD30:0000:0000:0000:0000/60$
 $12AB::CD30:0:0:0:0/60$
 $12AB:0:0:CD30::/60$

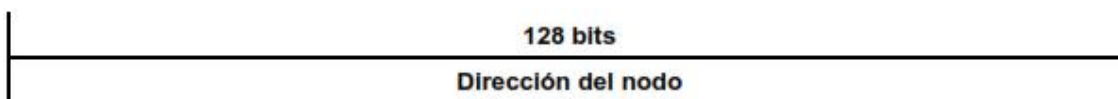
Por tanto, para escribir una dirección completa, indicando la subred, podríamos hacerlo como:

$12AB:0:0:CD30:123:4567:89AB:CDEF/60$

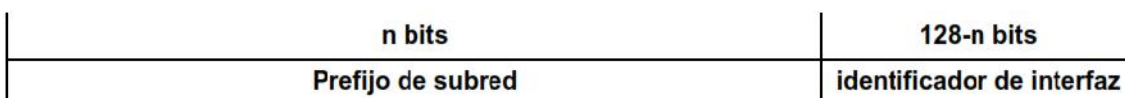
5.3.7 Direcciones unicast locales

Las direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Como hemos visto, hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura:



Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que esta conectado:



Dispositivos más sofisticados pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

El “identificador de interfaz” se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

Se han definido dos tipos de direcciones unicast de uso local: Enlace Local (Link-Local) y Sitio Local (Site-Local).

Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers. Por tanto, los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito esta limitado a la red local). Tienen el siguiente formato:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Se trata de direcciones FE80::<ID de interfaz>/10.

Las direcciones locales de sitio permiten direccionar dentro de un “sitio” local u organización, sin la necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los encaminadores no deben de retransmitir fuera del sitio ningún paquete cuya dirección fuente o destino sea “local de sitio” (su ámbito esta limitado a la red local o de la organización).

10 bits	38 bits	16 bits	64 bits
1111111011	0	ID de subred	Identificador de interfaz

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10.

5.3.8 **Direcciones anycast (RFC2526)**

Tal y como hemos indicado antes, las direcciones anycast tienen el mismo rango de direcciones que las unicast.

Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast.

Existe una dirección anycast, requerida para cada subred, que se denomina “dirección anycast del router de la subred” (subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

n bits	128-n bits
Prefijo de subred	00000000000000000000

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la “dirección anycast del router de la subred”, serán enviados a un router de la subred.

Una aplicación evidente de esta característica, además de la tolerancia a fallos, es la movilidad. Imaginemos nodos que necesitan comunicarse con un router entre el conjunto de los disponibles en su subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred.

La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones IPv6 usadas dentro de la subred.

Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit “universal/local” igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local). En este caso, las direcciones reservadas anycast de subred se construyen del siguiente modo:

64 bits	57 bits	7 bits
Prefijo de subred	1111110111 ... 111	ID anycast
Identificador de interfaz		

En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema:

n bits	121-n bits	7 bits
Prefijo de subred	1111111 ... 1111111	ID anycast
Identificador de interfaz		

5.3.9 Direcciones multicast (RFC2375)

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos multicast.

Las direcciones multicast tienen el siguiente formato:

8	4	4	112 bits
11111111	000T	ámbito	Identificador de Grupo

El bit “T” indica, si su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones.

Los bits “ámbito” tienen los siguientes significados:

0	Reservado
1	Ambito Local de Nodo
2	Ambito Local de Enlace
3	No asignado
4	No asignado
5	Ambito Local de Sitio
6	No asignado
7	No asignado
8	Ambito Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito Global
F	Reservado

El “Identificador de Grupo”, identifica, como cabe esperar, el grupo de multicast concreto al que nos referimos, bien sea permanente o temporal, dentro de un determinado ámbito.

Por ejemplo, si asignamos una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

- FF01::101 significa todos los NTS en el mismo nodo que el paquete origen
- FF02::101 significa todos los NTS en el mismo enlace que el paquete origen
- FF05::101 significa todos los NTS en el mismo sitio que el paquete origen
- FF0E::101 significa todos los NTS en Internet

Las direcciones multicast no-permanentes, sólo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal multicast local de sitio FF15::101, no tiene ninguna relación con un grupo usando la misma dirección en otro sitio, ni con otro grupo temporal que use el mismo identificador de grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupo.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminado.

Las principales direcciones multicast reservadas son las incluidas en el rango FF0x:0:0:0:0:0:0.

Algunos ejemplos útiles de direcciones multicast, según su ámbito, serían:

- FF01:0:0:0:0:0:1 – todos los nodos (ámbito local)
- FF02:0:0:0:0:0:1 – todos los nodos (ámbito de enlace)
- FF01:0:0:0:0:0:2 – todos los routers (ámbito local)
- FF02:0:0:0:0:0:2 – todos los routers (ámbito de enlace)
- FF05:0:0:0:0:0:2 – todos los routers (ámbito de sitio)

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada “Solicited-Node Address”, o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original.

Así, la dirección 4037::01:800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C.

Cada nodo debe de calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada.

5.3.10 Direcciones Requeridas para cualquier nodo

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

- Sus direcciones locales de enlace para cada interfaz
- Las direcciones unicast asignadas
- La dirección de loopback
- Las direcciones multicast de todos los nodos
- Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas
- Las direcciones multicast de todos los grupos a los que dicho host pertenece

Además, en el caso de los routers, tienen que reconocer también:

- La dirección anycast del router de la subnet, para las interfaces en las que esta configurado para actuar como router
- Todas las direcciones anycast con las que el router ha sido configurado
- Las direcciones multicast de todos los routers
- Las direcciones multicast de todos los grupos a los que el router pertenece

Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes:

- Dirección no especificada
- Dirección de loopback
- Prefijo de multicast (FF)
- Prefijos de uso local (local de enlace y local de sitio)

- Direcciones multicast predefinidas
- Prefijos compatibles IPv4

Se debe de asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).

5.3.11 Direcciones unicast globales agregables (RFC2374)

Dado que uno de los problemas que IPv6 resuelve es la mejor organización jerárquica del routing en las redes públicas (globales), es indispensable el concepto de direccionamiento “agregable”.

En la actualidad ya se emplea este tipo de direcciones, basadas en la agregación por parte de los proveedores del troncal Internet, y los mecanismos adoptados para IPv6, permiten su continuidad. Pero además, se incorpora un mecanismo de agregación basado en “intercambios”.

La combinación de ambos es la que permite un encaminamiento mucho más eficiente, dando dos opciones de conectividad a unas u otras entidades de agregación.

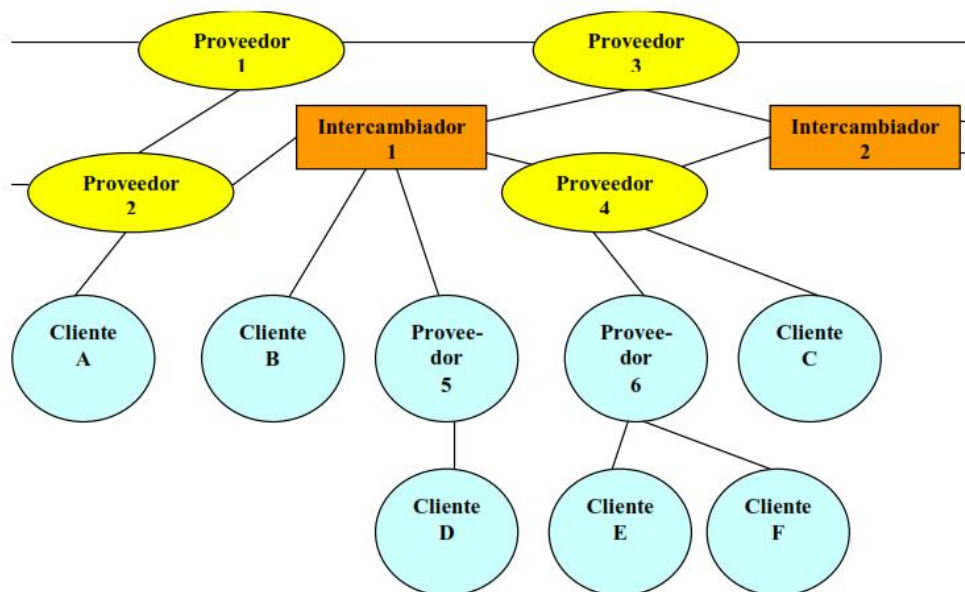
Se trata de una organización basada en tres niveles:

- ✓ Topología Pública: conjunto de proveedores e “intercambiadores” que proporcionan servicios públicos de tránsito Internet.
- ✓ Topología de Sitio: redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio “sitio”.
- ✓ Identificador de Interfaz: identifican interfaces de enlaces.

En la figura adjunta, el formato de direcciones agregables ha sido diseñado para soportar proveedores de larga distancia (identificados como Proveedor 1-4), intercambiadores (Intercambiador 1 y 2), proveedores de niveles inferiores (podrían ser ISP's, identificados como Proveedor 5 y 6), y Clientes (Cliente A-F).

A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones públicas IPv6. Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad directos, indirectamente a través del intercambiador, de uno o varios proveedores de larga distancia.

De esta forma, su direccionamiento es independiente de los proveedores de tráfico de larga distancia, y pueden, por tanto, cambiar de proveedor sin necesidad de reenumerar su organización. Este es uno de los objetivos de IPv6.



Además, una organización puede estar suscrita a múltiples proveedores (multi-homing o “multi-localización”), a través de un intercambiador, sin necesidad de tener prefijos de direcciones de cada uno de los proveedores.

5.3.11.1 Estructura de direcciones unicast globales agregables

El formato de las direcciones unicast globales agregables es el siguiente:

3	13	8	24	16	64 bits
FP	TLA ID	Res.	NLA ID	SLA ID	Interfaz ID
← Topología Pública →			← Topología de Sitio →		← Identificador de Interfaz →

Donde:

FP	Prefijo de Formato (001) - Format Prefix
TLA ID	Identificador de Agregación de Nivel Superior - Top-Level Aggregation Identifier
Res.	Reservado para uso futuro
NLA ID	Identificador de Agregación de Siguiente Nivel - Next-Level Aggregation Identifier
SLA ID	Identificador de Agregación de Nivel de Sitio - Site-Level Aggregation Identifier
Interfaz ID	Identificador de Interfaz

El campo Reservado permitirá, en el futuro, ampliaciones “organizadas” del protocolo, por ejemplo ampliar el número de bits de los campos TLA y NLA. Por el momento contiene ceros.

5.3.11.2 Identificador de Agregación de Nivel Superior

Se trata del nivel superior en la estructura jerárquica de enrutado.

Los routers situados en este nivel tienen, en la tabla de encaminado, una entrada para cada TLA ID activo, y probablemente entradas adicionales relativas al propio TLA ID donde están físicamente situados.

Podrían tener otras entradas, para su optimización, dependiendo de su topología, pero siempre pensando en que se minimice la tabla.

Esta estructura de direccionamiento permite 8,192 (2¹³) identificadores de

TLA. Se prevé su crecimiento haciendo que este campo crezca hacia la derecha en el espacio reservado para el futuro, o usando este mismo formato/estructura para prefijos de formato (FP) adicionales.

5.3.11.3 Identificador de Agregación de Siguiente Nivel

Es empleado por organizaciones a las que se ha asignado un TLA, para crear una estructura jerárquica de direccionamiento, acorde con su propia red, y para identificar los “sitios” u organizaciones que de ella dependen.

Pueden reservar los bits superiores para la diferenciación de la estructura de su red, en función a sus propias necesidades.

n	24-n bits	16	64 bits
NLA1	Site ID	SLA ID	Interfaz ID

Dado que cada organización que recibe un TLA dispone de 24 bits de espacio NLA, permite proporcionar servicio aproximadamente al número total de direcciones IPv4 soportadas actualmente.

Las organizaciones que reciben un TLA pueden soportar varios NLA en su propio espacio de direccionamiento (Site ID). Esto permite que sirvan tanto a clientes directos (suscriptores) como a otras organizaciones proveedoras de servicios públicos de tránsito. Y así sucesivamente, como se muestra en la siguiente figura:

n	24-n bits		16	64 bits
NLA1	Site ID		SLA ID	Interfaz ID
	m	24-n-m bits	16	64 bits
	NLA2	Site ID	SLA ID	Interfaz ID
		o	24-n-m-o bits	16
		NLA3	Site ID	SLA ID
				Interfaz ID

El diseño del espacio NLA de cada organización es libre para cada TLA asignado, y así sucesivamente con los niveles inferiores. Sin embargo, se recomienda seguir los procedimientos del RFC2050.

En cualquier caso es fundamental apreciar el balance entre eficacia de encaminado agregable y flexibilidad.

Las estructuras más jerárquicas permiten una mejor agregación, y por tanto reducen las tablas de encaminado.

Por el contrario, asignaciones más planas del espacio NLA proporcionan mejor flexibilidad en la conexión (crecimientos no previstos en un determinado espacio), resultando en tablas de encaminado mayores, y por tanto menos eficaces.

5.3.11.4 Identificador de Agregación de Nivel de Sitio

El SLA es usado por organizaciones “finales” para crear su propia estructura jerárquica de direcciones e identificar sus subredes. Es equivalente al concepto de subred en IPv4, con la muy apreciable diferencia de que cada corporación tiene un mayor número de subredes (16 bits proporcionan capacidad para 65.535).

Del mismo modo que en el caso del NLA, se puede escoger entre una estructura “plana”, o crear varios niveles, según la figura adjunta:

n	16-n bits		64 bits
SLA1	Subred		Interfaz ID
	m	16-n-m bits	64 bits
SLA2	Subred		Interfaz ID

Una gran compañía podría necesitar varios identificadores SLA. Como es lógico, cada caso dependerá de cómo están conectadas sus diversas delegaciones.

5.3.12 Formato para la representación en URL's (RFC2732)

Cuando navegamos, continuamente aludimos a URL, en muchas ocasiones sin conocer el significado preciso de esta abreviatura.

La especificación original (RFC2396), que data del año 1.988, nos dice que Uniform Resource Locator (Localizador de Recurso Uniforme), es un medio simple y extensible para identificar un recurso a través de su localización en la red.

Una vez aclarado esto, y de la misma forma que en ocasiones usamos direcciones en formato IPv4 para escribir un URL, se han descrito unas normas para realizar la representación literal de direcciones IPv6 cuando se usan herramientas de navegación WWW.

El motivo por el que ha sido preciso realizar esta definición es bien simple. Con la anterior especificación no estaba permitido emplear el carácter “:” en una dirección, sino como separador de “puerto”. Por tanto, si se desea facilitar operaciones tipo “cortar y pegar” (cut and paste), para trasladar direcciones entre diferentes aplicaciones, de forma rápida, era preciso buscar una solución que evitase la edición manual de las direcciones IPv6.

La solución es bien sencilla: el empleo de los corchetes (“[”, “]”) para encerrar la dirección IPv6, dentro de la estructura habitual del URL.

Veamos algunos ejemplos; las direcciones siguientes:

- FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- 1080:0:0:0:8:800:200C:4171
- 3ffe:2a00:100:7031::1
- 1080::8:800:200C:417A
- ::192.9.5.5

- `::FFFF:129.144.52.38`
- `2010:836B:4179::836B:4179`

Serían representadas como:

- `http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html`
- `http://[1080:0:0:0:8:800:200C:417A]/index.html`
- `http://[3ffe:2a00:100:7031::1]`
- `http://[1080::8:800:200C:417A]/foo`
- `http://[::192.9.5.5]/ipng`
- `http://[::FFFF:129.144.52.38]:80/index.html`
- `http://[2010:836B:4179::836B:4179]`

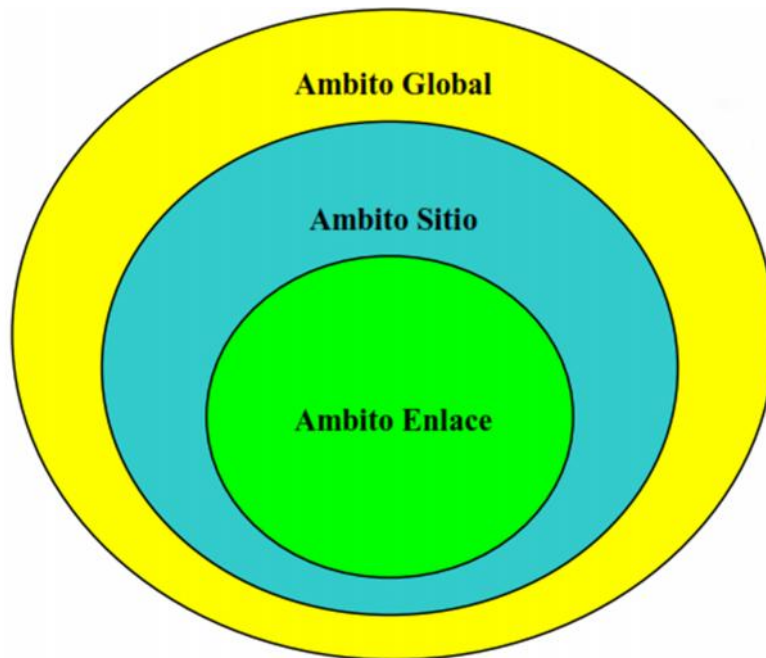
Hemos añadido alguna “complicación”, para que el propio lector descubra el uso del separador de puertos.

5.3.13 **Resumiendo**

Puede parecerle, al lector, un esquema muy complejo, pero en realidad es muy simple y sobre todo, muy eficiente.

Los resultados de este esquema son:

- a. Las direcciones siguen siendo asignadas por el proveedor, pero al cambiar de proveedor, sólo cambia el prefijo, y la red se “renumera” automáticamente (routers, sitios y nodos finales – dispositivos – servidores).



- b. Las interfaces pueden tener múltiples direcciones.
- c. Las direcciones tienen ámbito (Global, Sitio, Enlace).
- d. Las direcciones, al estar compuestas por un prefijo y un identificador de interfaz, nos permiten separar “quién es” de “donde esta conectado”:
- e. Además, las direcciones tienen un período de vida (de validez).

El RFC2450 propone las reglas para la administración de los TLA's y NLA's. Además, en <http://www.arin.net/regserv/ipv6/IPv6.txt>, podemos encontrar más

información al respecto de las normas para registros IPv6, del mismo modo que en <http://www.ripe.net/ripenncc/about/regional/maps/ipv6policy-draft090699.html>, o en <http://www.apnic.net/drafts/ipv6/ipv6-policy-280599.html>. En todos los casos, la máxima autoridad competente es IANA (Internet Assigned Numbers Authority).

5.4 ICMPv6 (RFC2463)

El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), descrito originalmente en el documento RFC792 para IPv4, ha sido actualizado para permitir su uso bajo IPv6.

El protocolo resultante de dicha modificación es ICMPv6, y se le ha asignado un valor, para el campo de “siguiente cabecera”, igual a 58. ICMPv6 es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6.

ICMPv6 es empleado por IPv6 para reportar errores que se encuentran durante el procesamiento de los paquetes, así como para la realización de otras funciones relativas a la capa “Internet”, como diagnósticos (“ping”).

El formato genérico de los mensajes ICMPv6 es el siguiente:

bits	8	16	32
Tipo	Código	Checksum	
Cuerpo del Mensaje			

El campo “tipo” indica el tipo de mensaje, y su valor determina el formato del resto de la cabecera.

El campo “código” depende del tipo de mensaje, y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.

El checksum o código de redundancia nos permite detectar errores en el mensaje ICMPv6.

Los mensajes ICMPv6 se agrupan en dos tipos o clases: mensaje de error y mensajes informativos. Los mensajes de error tienen cero en el bit de mayor peso del campo “tipo”, por lo que sus valores se sitúan entre 0 y 127.

Los valores de los mensajes informativos oscilan entre 128 y 255.

Los mensajes definidos por la especificación básica son los siguientes:

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	Descripción	
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Se está trabajando en nuevos tipos de mensajes, siendo el más interesante de ellos el definido en un borrador de IETF (draft-ietf-ipngwg-icmp-name-lookups05.txt), que permitirá solicitar a un nodo información completa como su "nombre de dominio completamente cualificado" (Fully-Qualified-Domain-Name).

Por razones de seguridad, las cabeceras ICMPv6 pueden ser autenticadas y encriptadas, usando la cabecera correspondiente. El uso de este mecanismo permite, además, la prevención de ataques ICMP, como el conocido "Negación de Servicio" (DoS o Denial of Service Attack).

5.5 Neighbor Discovery (RFC2461)

En IPv6, el protocolo equivalente, en cierto modo, a ARP en IPv4, es el que denominamos “descubrimiento del vecindario”. Sin embargo, incorpora también la funcionalidad de otros protocolos IPv4, como “ICMP Router Discovery” y “ICMP Redirect”.

Tal como indica esta “traducción”, consiste en el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad (“reachability”) acerca de las rutas a los “vecinos” activos.

El protocolo ND (abreviatura común de “Neighbor Discovery”), también se emplea para mantener limpios los “caches” donde se almacena la información relativa al contexto de la red a la que está conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Cuando un router, o una ruta hacia él, falla, el host buscará alternativas funcionales.

ND emplea los mensajes de ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios.

El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.

Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies.

ND define cinco tipos de paquetes ICMPv6:

- Solicitud de Router (Router Solicitation) – generado por una interfaz cuando es activada, para pedir a los routers que se “anuncien” inmediatamente. Tipo en paquete ICMPv6 = 133.
- Anunciación de Router (Router Advertisement) – generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una “solicitud de router”, a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida, configuración de direcciones, límite de salto sugerido, etc. Es fundamental para permitir la reenumeración. Tipo en paquete ICMPv6 = 134.
- Solicitud de Vecino (Neighbor Solicitation) – generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas. Tipo en paquete ICMPv6 = 135.
- Anunciación de Vecino (Neighbor Advertisement) – generado por los nodos como respuesta a la “solicitud de vecino”, o bien para indicar cambios de direcciones en la capa de enlace. Tipo en paquete ICMPv6 = 136.

- Redirección (Redirect) – generado por los routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, en parte a “ICMP redirect”. Tipo en paquete ICMPv6 = 137.

El protocolo ND, frente a los mecanismos existentes en IPv4, reporta numerosas ventajas:

- El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de encaminado.
- La anunciación de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- La anunciación de router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
- La anunciación de router permite la autoconfiguración de direcciones
- Los routers pueden anunciar a los host del mismo enlace el MTU (tamaño máximo de la Unidad de transmisión).
- Se extienden los multicast de resolución de direcciones entre 2 ciones, reduciendo de forma importante las interrupciones relativas a la resolución de direcciones en nodos distintos al objetivo, y evitando las interrupciones en nodos sin IPv6.
- Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
- Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación de router. Sin embargo, los
- Routers pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que los host consideren que los destinos están fuera del enlace; de esta forma, enviarán el tráfico a los routers, quién a su vez lo redireccionará según corresponda.
- A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto está en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace (enlaces sin multidifusión y media compartida).
- La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
- A diferencia de ARP, en ND se puede detectar fallos de la mitad del enlace, es decir, con conectividad en un solo sentido, evitando el tráfico hacia ellos.
- A diferencia de IPv4, no son precisos campos de preferencia (para definir la “estabilidad” de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.

- El uso de direcciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una reenumeración para usar nuevos prefijos globales.
- El límite de saltos es siempre igual a 255, lo que evita que haya envíos accidentales o intencionados desde nodos fuera del enlace, dado que los routers decrementan automáticamente este campo en cada salto.
- Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

En este RFC se describe, además, el “modelo conceptual” de las estructuras de datos y su manipulación, que un dispositivo (host o router) requeriría para cumplir los protocolos IPv6. Se trata, pues, de un documento clave para la correcta interpretación de IPv6, cuando se trata de aplicarlo a su uso por parte de desarrolladores.

En resumen, ND reemplaza, con grandes mejoras e importantes ventajas, a ARP.

5.6 Autoconfiguración en IPv6 (RFC2462)

La autoconfiguración es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que nos permite afirmar que IPv6 es “Plug & Play”.

El proceso incluye la creación de una dirección de enlace local, verificación de que no esta duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra información).

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (stateful o configuración predeterminada), o de forma automática (stateless descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración “stateless” (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un “identificador de interfaz”, que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia de router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace. En la autoconfiguración “stateful” (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host. Ambos tipos de autoconfiguración (stateless y stateful), se complementan.

Un host puede usar autoconfiguración sin intervención (stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración “sin intervención” se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan sólo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente.

Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuánto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección es “preferred” (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es “deprecated” (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado.

Mientras esta en estado “desaprobado”, su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión TCP), debe usar una dirección “preferida”, siempre que sea posible.

Una dirección “desaprobada” debería ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y a las que les es muy difícil cambiar a otra dirección sin interrupción del servicio.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.

La autoconfiguración está diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los routers también tienen que “aprobar” el algoritmo de detección de direcciones duplicadas.

5.6.1 Autoconfiguración Stateless

El procedimiento de autoconfiguración stateless (sin intervención o descubrimiento automático), ha sido diseñado con las siguientes premisas:

- Evitar la configuración manual de dispositivos antes de su conexión a la red. Se requiere, en consecuencia, un mecanismo que permita a los hosts obtener o crear direcciones únicas para cada una de sus interfaces, asumiendo que cada interfaz puede proporcionar un identificador único para sí misma (identificador de interfaz). En el caso más simple, el identificador de interfaz consiste en la dirección de la capa de enlace, de dicha interfaz.

El identificador de interfaz puede ser combinado con un prefijo, para formar la dirección.

- Las pequeñas redes o sitios, con máquinas conectadas a un único enlace, no deberían requerir la presencia de un servidor “stateful” o router, como requisito para comunicarse. Para obtener, en este caso, características “plug & play”, empleamos las direcciones de enlace local, dado que tienen un prefijo perfectamente conocido que identifica el único enlace compartido, al que se conectan todos los nodos. Cada dispositivo forma su dirección de enlace local anteponiendo el prefijo de enlace local a su identificador de interfaz.
- En el caso de redes o sitios grandes, con múltiples subredes y routers, tampoco se requiere la presencia de un servidor de configuración de direcciones “stateful”, ya que los hosts han de determinar, para generar sus direcciones globales o de enlace local, los prefijos que identifican las subredes a las que se conectan. Los routers generan mensajes periódicos de anunciación, que incluyen opciones como listas de prefijos activos en los enlaces.
- La configuración de direcciones debe de facilitar la reenumeración de los dispositivos de un sitio, por ejemplo, cuando se desea cambiar de proveedor de servicios. La reenumeración se logra al permitir que una misma interfaz pueda tener varias direcciones, que recibe “en préstamo”. El tiempo del “préstamo” es el mecanismo por el que se renuevan las direcciones, al expirar los plazos para las viejas, sin que se conceda una prórroga. Al poder disponer de varias direcciones simultáneamente, permite que la transición no sea “disruptora”, permitiendo que ambas, la vieja y la nueva dirección den continuidad a la comunicación durante el período de transición.
- Sólo es posible utilizar este mecanismo en enlaces capaces de funciones multicast, y comienza, por tanto, cuando es iniciada o activada una interfaz que permite multicast.
- Los administradores de sistemas necesitan la habilidad de especificar que mecanismo (stateless, stateful, o ambos), deben ser usados. Los mensajes de anunciación de los routers incluyen indicadores para esta función.

Los pasos básicos para la autoconfiguración, una vez la interfaz ha sido activada, serían:

- a) Se genera la dirección “tentativa” de enlace local, como se ha descrito antes.
- b) Verificar que dicha dirección “tentativa” puede ser asignada (no esta duplicada en el mismo enlace).
- c) Si esta duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).
- d) Si no esta duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección “tentativa” a la interfaz en cuestión.

- e) Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.
- f) Si no hay routers, se invoca el procedimiento de autoconfiguración “stateful”.
- g) Si hay routers, estos contestarán indicando fundamentalmente, como obtener las direcciones si se ha de utilizar el mecanismo “stateful”, u otra información, como tiempos de vida, etc.

Hay algunos detractores de este mecanismo, ya que implica que cualquier nodo puede ser identificado en una determinada red si se conoce su identificador IEEE (dirección MAC). Por ello, para permitir que la dirección no sea estática, se esta trabajando en el documento draft-ietf-ipngwg-addrconf-privacy-01.txt.

5.6.2 Autoconfiguración Stateful – DHCPv6 (draft-ietf-dhcdhcpv6-15.txt)

DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, superior al facilitados por el mecanismo de configuración “stateless”.

Como ya hemos indicado, ambos mecanismos pueden usarse de forma concurrente para reducir el coste de propiedad y administración de la red.

Para lograr este objetivo, se centraliza la gestión de los recursos de la red, tales como direcciones IP, información de encaminado, información de instalación de Sistemas Operativos, información de servicios de directorios, sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en ficheros de configuración locales en cada nodo.

Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de “extensiones” que incorporan esta nueva información. Al respecto es fundamental el documento dhc-v6exts-12.txt.

Los objetivos de DHCPv6 son:

- DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.
- DHCP es compatible, lógicamente, con el mecanismo de autoconfiguración “stateless”.
- DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.
- DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de relés DHCP.
- DHCP coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.
- Los clientes DHCP pueden operar en enlaces donde no hay routers IPv6.

- Los clientes DHCP proporcionan la habilidad de reenumerar la red.
- Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.
- DHCP incorpora los mecanismos apropiados de control de tiempo y retransmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en el soporte inherente del formato de direccionamiento y autoconfiguración IPv6; son las siguientes:

- La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección IP fuente para localizar un servidor o relé en su mismo enlace.
- Los indicadores de compatibilidad BOOTP y broadcast han desaparecido.
- El multicast y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por si mismos su rango por la dirección multicast, para la función requerida.
- La autoconfiguración stateful ha de coexistir e integrarse con la stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida de IPv6, para facilitar la reenumeración automática de direcciones y su gestión.
- Se soportan múltiples direcciones por cada interfaz.
- Algunas opciones DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios (RFC2165).

De esta forma, se soportan las siguientes funciones nuevas:

- Configuración de actualizaciones dinámicas de DNS.
- Desaprobación de direcciones, para reenumeración dinámica.
- Relés preconfigurados con direcciones de servidores, o mediante multicast.
- Autenticación.
- Los clientes pueden pedir múltiples direcciones IP.
- Las direcciones pueden ser reclamadas mediante el mensaje de “iniciar reconfiguración”.
- Integración entre autoconfiguración de direcciones “stateless” y “stateful”
- Permitir relés para localizar servidores fuera del enlace.

5.6.3 **Renumeración**

En los párrafos anteriores ya hemos descrito el mecanismo básico de reenumeración, basado en el “préstamo” o alquiler de direcciones, en las fases de “preferida” y “desaprobada”, y en el tiempo de vida de las mismas.

En cualquier caso, podemos describir el mecanismo de forma sencilla, como consistente en disminuir el tiempo de vida del prefijo en los paquetes de anunciación del router, de forma que las direcciones pasen a ser desaprobadas, frente a las nuevas, que pasan a ser preferidas.

Sin embargo, este mecanismo está básicamente diseñado para los host.

En el caso de los routers, se trabaja en un nuevo documento “draft-ietf-ipngwrouter-renum-10.txt”, que permitirá mecanismos similares y más adecuados.

5.7 IPv6 sobre Ethernet (RFC2464)

Aunque ya han sido definidos protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM, PPP, ...), como ejemplo mucho más habitual y básico, centraremos este apartado en Ethernet (CSMA/CD y tecnologías full-duplex basadas en ISO/IEC8802-3). Mas adelante, en este mismo documento, citaremos los protocolos adecuados para cada una de las otras tecnologías.

Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet. La cabecera Ethernet contiene las direcciones fuente y destino Ethernet, y el código de tipo Ethernet con el valor hexadecimal 86DD.

El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

48 bits	48 bits	16 bits	
Dirección Ethernet Destino	Dirección Ethernet Fuente	1000011011011101 (86DD)	Cabecera y datos IPv6

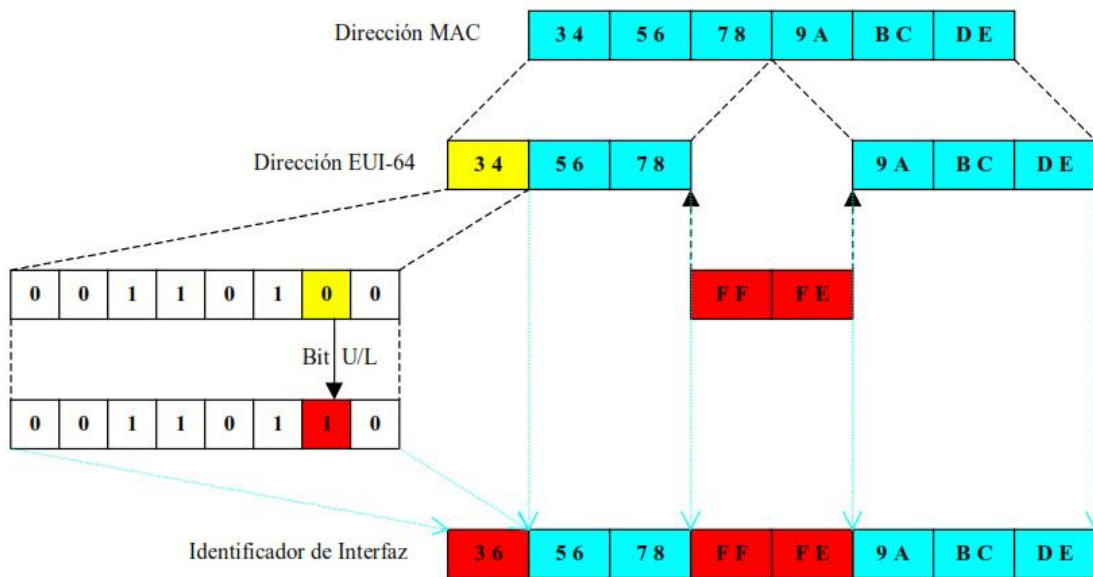
El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).

Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC de 48 bits (IEEE802). Tomamos los 3 primeros bytes (los de mayor orden), y les agregamos “FFFE” (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según lo define IEEE.

El identificador de interfaz se obtiene, a continuación, partiendo del EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor valor del primer byte del EUI-64 (el 2º bit por la derecha, el 2º bit de menor peso). Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.

Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz, pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L.

Véase el esquema siguiente:



Para mapear direcciones unicast IPv6 sobre Ethernet, se utilizan los mecanismos ND para solicitud de vecinos.

Para mapear direcciones multicast IPv6 sobre Ethernet, se emplean los 4 últimos bytes de la dirección IPv6, a los que se antepone “3333”.

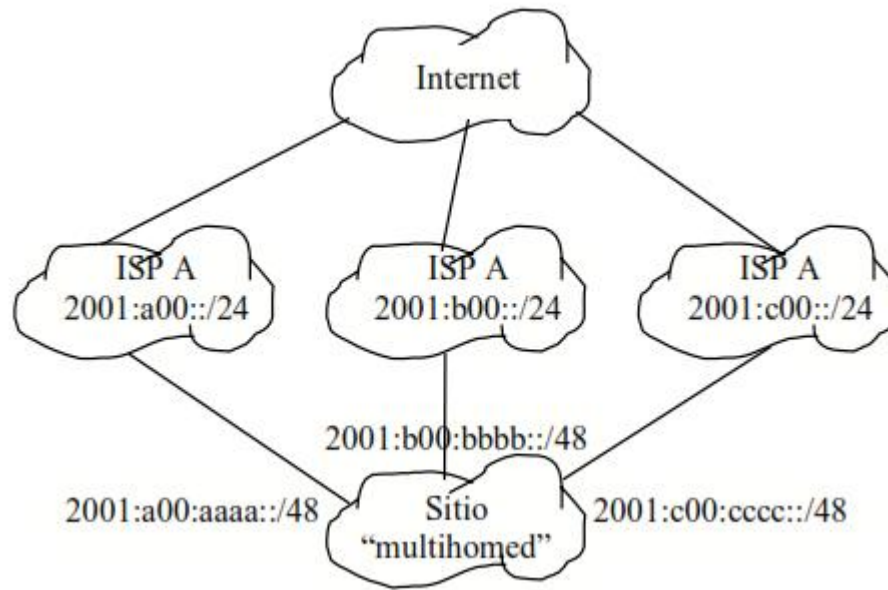
5.8 Multi-homing

Como venimos viendo, el mecanismo de asignación de direcciones IPv6 es totalmente jerárquico.

El multi-homing (“múltiples hogares”) es el mecanismo por el cual un determinado sitio o red puede estar conectado a otros por múltiples caminos, por razones de seguridad, redundancia, ancho de banda, balanceo de carga, etc.

Dado que un determinado sitio utiliza el prefijo de su ISP, o proveedor de nivel superior, un sitio puede ser “multi-homed” simplemente teniendo varios prefijos. Frecuentemente, cada prefijo estará asociado a diferentes conexiones físicas, aunque no necesariamente, dado que se puede tratar de una sola conexión física y diversos túneles o conexiones virtuales.

La problemática se plantea por la dificultad de que un host decida, en una red “multi-homed”, que dirección fuente utilizar.



Algunos de los documentos sobre los que se está trabajando en este campo son:

- Default Address Selections for IPv6 (draft-ietf-ipngwg-default-addr-select00.txt).
- IPv6 Multi-homing with Route Aggregation (draft-ietf-ipngwg-ipv6multihomewith-aggr-00.txt).
- Multi-homed Routing Domain Issues for IPv6 (draft-ietf-ipngwg-multi-isp00.txt).

5.9 IPsec

Una de las grandes ventajas de IPv6 es, sin duda, la total integración de los mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo.

Se trata por tanto de algo obligatorio, y no adicional ni “añadido” como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación – “Authentication Header”) y ESP (encriptación – “Encapsulation Security Payload”), que permiten, básicamente, emplear las mismas extensiones de protocolo empleadas en IPv4, y que de hecho, al haber sido desarrolladas con posterioridad al inicio de los trabajos de IPv6, ya lo contemplan.

Dado que los mecanismos asociados ya han sido descritos, simplemente citamos las normas básicas que son aplicables: RFC2401 al RFC2412 y RFC2451.

5.10 Movilidad

La posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad, es otra de las motivaciones básicas de IPv6. Como no, ya se han iniciado trabajos al respecto en IPv4, pero las complicaciones para usar la movilidad en este caso son enormes.

El documento base de estos trabajos es draft-ietf-mobileip-ipv6-12.txt. La idea básica permite identificar a un nodo móvil por su dirección de partida (“home address”), independientemente de su punto de conexión a Internet en cada momento dado. Por supuesto, cuando no está en su punto de origen o de partida, también está asociado con la información que permite identificar su posición o dirección actual (“care-of-address”). Los paquetes enviados a un nodo móvil (a su dirección de origen), son transparentemente encaminados a su “dirección actual”.

El protocolo también permite que los nodos IPv6 almacenen la información de vinculación entre la dirección de partida y la posición actual, a modo de caché, y por tanto sean capaces de enviar los paquetes destinados al nodo móvil, directamente a su “dirección actual”.

Para ello, el protocolo define nuevas opciones de destino, una de las cuales ha de ser soportada incluso en paquetes recibidos por todos los nodos (aunque no sean móviles).

Además, hay que prever, dada la estructura habitual de las redes inalámbricas (ejemplo muy habitual, la telefonía celular), que un nodo móvil puede estar conectado simultáneamente a varias redes (varias células que se solapan), y debe de ser alcanzable por cualquiera de ellas.

Los trabajos iniciales están documentados en el RFC2002 (soporte de movilidad en IP) y sucesivos. Además, se han publicado ya las especificaciones para túneles inversos en redes IP móviles (RFC2344), en cuya actualización se está trabajando (draft-ietf-mobileip-rfc2344-bis-01.txt).

Se trabaja también en apartados como los requisitos de autenticación, autorización y facturación (draft-ietf-mobileip-aaa-reqs-03.txt), comúnmente denominadas AAA (Authentication, Authorization and Accounting), las extensiones de autenticación (draft-ietf-mobileip-challenge-09.txt), las claves de registro AAA (draft-ietf-mobileip-aaa-key-01.txt), la optimización de rutas (draft-ietf-mobileipoptim-09.txt), claves de registro para la optimización de rutas (draft-ietf-mobileipregkey-01.txt), registros regionales (draft-ietf-mobileip-reg-tunnel-02.txt), entre otros.

5.11 DNS (RFC1886)

El mecanismo fundamental por el cual nos referimos a direcciones IP para a localización de un host, es el uso de literales (URL), como ya hemos anticipado en apartados anteriores.

Sin embargo, para que este mecanismo funcione, a más bajo nivel existe un protocolo denominado “Sistema de Nombres de Dominio” (Domain Name System o DNS).

Este mecanismo, definido para IPv4 (RFC1034 y RFC1035), fue actualizado por el RFC1886, básicamente incluyendo un nuevo tipo de registro para almacenar las direcciones IPv6, un nuevo dominio para soportar las “localizaciones” (lookups) basadas en IPv6, y definiciones actualizadas de tipos de consultas existentes que devuelven direcciones Internet como parte de procesos de secciones adicionales.

Las extensiones han sido diseñadas para ser compatibles con las aplicaciones existentes y, en particular, con las implementaciones del propio DNS.

El problema del sistema de DNS existente es fácilmente comprensible: Al hacer una consulta, las aplicaciones asumen que se les devolverá una dirección de 32 bits (IPv4). Para resolverlo, hay que definir las siguientes extensiones, antes indicadas:

- Un nuevo tipo de registro de recurso para mapear un nombre de dominio con una dirección IPv6: Es el registro AAAA (con un valor de tipo 28, decimal).
- Un nuevo dominio para soportar búsquedas basadas en direcciones. Este dominio es IP6.INT. Su representación se realiza en orden inverso de la dirección, separando los nibbles (hexadecimal) por puntos (“.”), seguidos de “IP6.INT”. Así, la búsqueda inversa de la dirección 4321:0:1:2:3:4:567:89ab, sería “b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.1.2.3.4.IP6.INT”
- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6. Ello incluye TODAS las consultas, lógicamente (NS, MX, MB, ...).

Además, para soportar la agregación de direcciones IPv6, la reenumeración y el multi-homing, se trabaja en un nuevo documento (draft-ietf-ipngwg-dnslookups-07.txt), que incluye un nuevo tipo de registro de recurso (A6) para almacenar las direcciones IPv6 de forma que se agilice la reenumeración de la red. Se prevé que este documento sustituya al RFC1886.

Otros documentos relevantes son: RFC2181 (clarificaciones a las especificaciones DNS), RFC2535 (extensiones de seguridad para DNS), RFC2672 (redirección de árboles DNS), RFC2673 (etiqueta binarias en DNS).

5.12 Protocolos de Routing

Básicamente se adoptan los mismo protocolos de encaminado que los existentes en las redes IPv4: RIP, OSPF y BGP. Pero además se está trabajando en IDRP (ISO Inter-Domain Routing Protocol) e IS-IS (Intermediate System to Intermediate System).

5.12.1 RIPng (RFC2080 y RFC2081)

La especificación del Protocolo de Información de Rutas (RIP – “Routing Information Protocol”) para IPv6, recoge los cambios mínimos e indispensables al RFC1058 y RFC1723 para su adecuado funcionamiento.

RIPng es un protocolo pensado para pequeñas redes, y por tanto se incluye en el grupo de protocolos de pasarela interior (IGP – “Interior Gateway Protocol”), y emplea un algoritmo denominado “Vector-Distancia”. Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática.

RIPng sólo puede ser implementado en routers, donde requerirá como información fundamental, la métrica o número de saltos (entre 1 y 15), que un paquete ha de

emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por lo general atravesando un nuevo router.

Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo.

Estos parámetros han de ser configurados por el administrador de la red.

El router incorporará, en la tabla de encaminado, una entrada para cada destino accesible (alcanzable) por el sistema. Cada entrada tendrá como mínimo, los siguiente parámetros:

- El prefijo IPv6 del destino.
- La métrica (número de saltos entre este router y el destino).
- La dirección IPv6 del siguiente router, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.

Además se podrán crear rutas internas (saltos entre interfaces del propio router), o rutas estáticas (definidas manualmente).

RIPng es un protocolo basado en UDP. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng).

El inconveniente de RIPng, al igual que en IPv4, siguen siendo, además de su orientación a pequeñas redes (diámetro de 15 saltos como máximo), en que su métrica es fija, es decir, no puede variar en función de circunstancias de tiempo real (retardos, fiabilidad, carga, etc.).

5.12.2 OSPFv6 (RFC2740)

El protocolo de encaminado “Abrir Primero el Camino más Corto” (OSPF –“Open Shortest Path First”), es también un protocolo IGP (para redes autónomas), basado en una tecnología de “estado de enlaces” (“link-state”).

Se trata de un protocolo de encaminado dinámico, que detecta rápidamente cambios de la topología (como un fallo en un router o interfaz) y calcula la siguiente ruta disponible (sin bucles), después de un corto período de convergencia con muy poco tráfico de routing.

Cada router mantiene una base de datos que describe la topología del sistema autónomo (de la red), y es lo que denominamos base de datos de “estado de enlaces”. Todos los routers del sistema tienen una base de datos idéntica, indicando el estado de cada interfaz, y de cada “vecino alcanzable”.

Los routers distribuyen sus “estados locales” a través del sistema autónomo (la red) por medio de desbordamientos (“flooding”).

Todos los routers utilizan el mismo algoritmo, en paralelo, y construyen un árbol de las rutas más cortas, como si fueran la raíz del sistema. Este árbol de “rutas más cortas” proporciona la ruta a cada destino del sistema autónomo.

Si hubiera varias rutas de igual coste a un determinado destino, el tráfico es distribuido equilibradamente entre todas. El coste de una ruta se describe por una métrica simple, sin dimensión.

Se pueden crear áreas o agrupaciones de redes, cuya topología no es retransmitida al resto del sistema, evitando tráfico de routing innecesario.

OSPF permite el uso de máscaras diferentes para la misma red (“variable length subnetting”), lo que permite el encaminado a las mejores rutas (las más largas o más específicas).

Todos los intercambios de protocolo OSPF son autenticados, y por tanto sólo pueden participar los routers verificados (“trusted”).

OSPFv6 mantiene los mecanismos fundamentales de la versión para IPv4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección.

OSPFv6 se ejecuta basado en cada enlace, en lugar de en cada subred.

Además, ha sido necesario eliminar la autenticación del protocolo OSPFv6, dado que IPv6 incorpora estas características (AH y ESP).

A pesar de la mayor longitud de las direcciones, se ha logrado que los paquetes OSPFv6 sean tan compactos como los correspondientes para IPv4, eliminando incluso algunas limitaciones y flexibilizando la manipulación de opciones.

5.12.3 BGP4+ (RFC2283, RFC2545)

El Protocolo de Pasarelas de Frontera (BGP – “Border Gateway Protocol”) es un protocolo de encaminado para la interconexión de sistemas autónomos, es decir, para el enrutado entre diferentes dominios.

Frecuentemente se emplea para grandes corporaciones y para la conexión entres proveedores de servicios (como ISP’s).

Su principal función es, por tanto, el intercambio de información de disponibilidad o alcance entre varios sistemas BGP, incluyendo información de los sistemas autónomos que contienen, permitiendo así construir las rutas más adecuadas y evitar bucles de tráfico.

BGP4 incorpora mecanismos para soportar enrutado entre dominios sin clases (“classless interdomain routing”), es decir, el uso de prefijos, agregación de rutas, y todos los mecanismos en los que se basa IPv6.

BGP se basa en que un dispositivo sólo informa a los otros dispositivos que se conectan a él, acerca de las rutas que el mismo emplea. Es decir, es una estrategia de “salto a salto”. La implicación es la simplicidad de Internet, pero la desventaja es que este mecanismo impide políticas complejas, que precisan de técnicas como el enrutado de fuente (“source routing”).

BGP usa TCP como protocolo de transporte, a través del puerto 179.

BGP4+ añade a BGP (RFC1771), extensiones multiprotocolo, tanto para IPv6 como para otros protocolos, como por ejemplo IPX.

5.13 Estrategias de Transición (RFC1933)

La clave para la transición es la compatibilidad con la base instalada de dispositivos IPv4. Esta afirmación define un conjunto de mecanismos que los hosts y routers IPv6 pueden implementar para ser compatibles con host y routers IPv4.

Estos mecanismos permitirán usar infraestructuras IPv4 para IPv6 y viceversa, dado que se prevé que su uso será prolongado, e incluso indefinido en muchas ocasiones.

5.13.1 Doble pila (IPv4 e IPv6)

El camino más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas separadas.

Los dispositivos con ambos protocolos también se denominan “nodos IPv6/IPv4”.

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6).

El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión).

El DNS podrá devolver la dirección IPv4, la dirección IPv6, o ambas.

Como ya hemos explicado en el apartado de direcciones especiales IPv6, se pueden emplear la dirección IPv4 (32 bits), anteponiéndole 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 “mapeada desde IPv4”.

5.13.2 Túneles IPv6 sobre IPv4

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

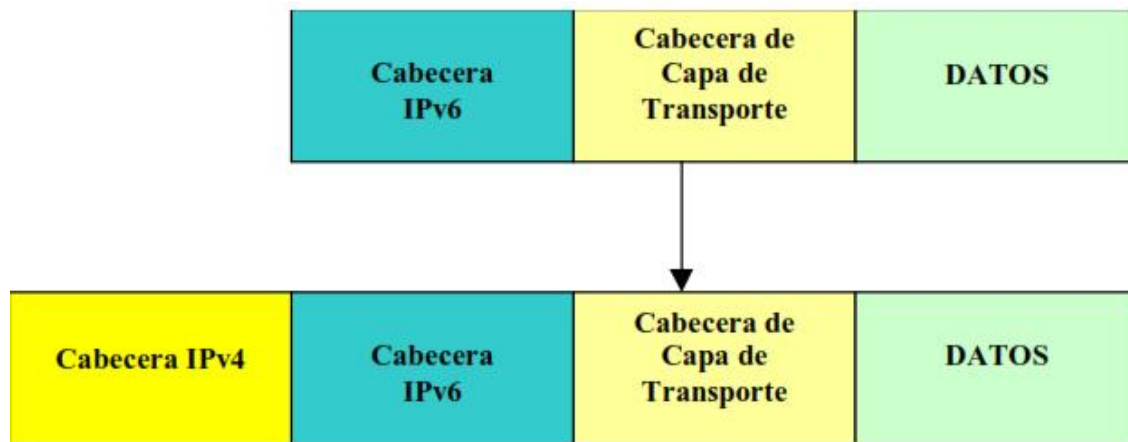
Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete/es IPv6 en IPv4.

Estos túneles pueden ser utilizados de formas diferentes:

- Router a router. Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
- Host a router. Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.
- Host a host. Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
- Router a host. Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel. En los dos primeros casos (router a router y host a router), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina “túnel configurado”, describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

En los otros dos casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina “túnel automático”.



El “desencapsulado”, en el extremo final del túnel, realiza la función opuesta, lógicamente.

5.13.3 Transmisión de IPv6 sobre dominios IPv4 (RFC2529)

Este mecanismo permite a hosts IPv6 aislados, sin conexión directa a routers IPv6, ser totalmente funcionales como dispositivos IPv6.

Para ello se emplean dominios IPv4 que soportan multicast como su enlace local virtual. Es decir, usamos multicast IPv4 como su “ethernet virtual”.

De esta forma, estos hosts IPv6 no requieren direcciones IPv4 compatibles, ni túneles configurados.

Los extremos finales del túnel se determinan mediante ND. Es imprescindible que la subred IPv4 soporte multicast.

Este mecanismo se denomina comúnmente “6 over 4”.

5.13.4 Conexión de dominios IPv6 sobre redes IPv4

El documento draft-ietf-ngtrans-6to4-04.txt nos indica un mecanismo comúnmente denominado “6 to 4”, para asignar un prefijo de dirección IPv6 a cualquier sitio que tenga al menos una dirección IPv4 pública.

De esta forma, dominios o hosts IPv6 aislados, conectados a infraestructuras IPv4 (sin soporte de IPv6), pueden comunicar con otros dominios o hosts IPv6 con una configuración manual mínima.

Este mecanismo funciona aún cuando la dirección IPv4 global (pública) es única y se accede a la red mediante mecanismos NAT (Network Address Translation), que es el caso más común en las redes actuales para el acceso a Internet a través de ISP's.

5.13.5 “Tunnel Server” y “Tunnel Broker”

El documento draft-ietf-ngtrans-broker-02.txt sienta las bases para aplicaciones que permiten utilizar, de forma libre y gratuita, nuestras direcciones IPv4 actuales, sobre las infraestructuras IPv4, para acceder a redes y sitios IPv6.

Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres DNS permanentes.

La diferencia con el mecanismo “6to4” es que el “Tunnel Broker” no requiere la configuración de un router.

Se trata de ISP's IPv6 “virtuales”, proporcionando conectividad IPv6 a usuarios que ya tienen conectividad IPv4.

El “tunnel broker” es el lugar donde el usuario se conecta para registrar y activar “su túnel”. El “broker” gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario.

El “tunnel server” es un router con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo órdenes del “broker” crea, modifica o borra los servicios asociados a un determinado túnel/usuario.

El mecanismo para su configuración es tan sencillo como indicar, en un formulario Web, datos relativos al S.O., la dirección IPv4, un “apodo” para la máquina, y el país donde esta conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

Se pueden hallar ejemplos de estos sistemas en <http://www.freenet6.net> y <http://carmen.cselt.it/ipv6/download.html>.

5.13.6 Otros mecanismos de transición

Estas técnicas pueden ser utilizadas incluso de forma combinada.

Se está trabajando en varios mecanismos alternativos y modificaciones a los aquí expuestos, a través de los borradores draft-ietf-ngtrans-mech-06.txt, draft-ietf-ngtrans-translator-03.txt, draft-ietf-ngtrans-socks-gateway-04.txt, draft-ietf-ngtrans-dstm-01.txt, draft-ietf-ngtrans-tcpudp-relay-00.txt, draft-ietf-ngtrans-hometun-00.txt y draft-ietf-ngtrans-ipv4survey-00.txt.

Un documento introductorio completo a todos los mecanismos es draft-ietfngtrans-introduction-to-ipv6-transition-03.txt.

5.14 Situación del estándar: RFC's y borradores

Los RFC's existentes son los siguientes:

	Documento	Título
Especificaciones Básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2461	Descubrimiento del Vecindario para IPv6 (ND)
	RFC2462	Autoconfiguración de Direcciones "stateless" IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
	RFC1951	Descubrimiento del MTU de la ruta para IPv6
	RFC1809	Uso del campo "Etiqueta de Flujo" en IPv6
Direccionamiento	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1697	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
	RFC2450	Propuesta de normas de asignación de TLA y NLA
Routing	RFC2080	RIP para IPv6
	RFC2081	Aplicabilidad de RIPv6 para IPv6
	RFC2283	Extensiones Multiprotocolo para BGP-4
	RFC2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
	RFC2740	OSPF para IPv6
DNS	RFC1886	Extensiones DNS para soportar IPv6
IPv6 sobre ...	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2467	Transmisión de paquetes IPv6 sobre redes FDDI
	RFC2470	Transmisión de paquetes IPv6 sobre redes Token Ring
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
	RFC2492	IPv6 sobre redes ATM
Seguridad	RFC2401	Arquitectura de Seguridad para IP
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)
	RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
Multicast	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
	RFC2776	Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)
Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
	RFC2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transición	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunnelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
	RFC2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
	RFC2766	Protocolo de Traslación - Traslación de Dirección de Red
	RFC2767	Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)
API	RFC2292/bis	Advanced Sockets API para IPv6
	RFC2553/bis	Basic Socket API para IPv6
MIB	RFC2452	Base de Información de Gestión para IPv6: TCP
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
	RFC2466	Base de Información de Gestión para IPv6: ICMPv6
Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre Jumbogramas IPv6
	RFC2426	Extensiones FTP para IPv6 y NAT
	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas
	RFC2474	Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2663	Consideraciones y Terminología de IP NAT
	RFC2732	Formato para la representación literal de direcciones IPv6 en URL's
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2775	Transparencia de Internet

Pero además, se esta trabajando en los siguientes documentos (drafts):

	Documento	Título
Especificaciones Básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2461	Descubrimiento del Vecindario para IPv6 (ND)
	RFC2462	Autoconfiguración de Direcciones "stateless" IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
	RFC1981	Descubrimiento del MTU de la ruta para IPv6
Direccionamiento	RFC1808	Uso del campo "Etiqueta de Flujo" en IPv6
	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
Routing	RFC2450	Propuesta de normas de asignación de TLA y NLA
	RFC2050	RIP para IPv6
	RFC2081	Aplicabilidad de RIPv6 para IPv6
	RFC2283	Extensiones Multiprotocolo para BGP-4
	RFC2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
DNS	RFC2740	OSPF para IPv6
	RFC1886	Extensiones DNS para soportar IPv6
IPv6 sobre ...	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2467	Transmisión de paquetes IPv6 sobre redes FDDI
	RFC2470	Transmisión de paquetes IPv6 sobre redes Token Ring
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
Seguridad	RFC2492	IPv6 sobre redes ATM
	RFC2401	Arquitectura de Seguridad para IP
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)
Multicast	RFC2406	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
Anycast	RFC2776	Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)
	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
	RFC2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transición	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explicitos
	RFC2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
	RFC2766	Protocolo de Traslación - Traslación de Dirección de Red
	RFC2767	Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)
API	RFC2292/bis	Advanced Sockets API para IPv6
	RFC2553/bis	Basic Socket API para IPv6
MIB	RFC2452	Base de Información de Gestión para IPv6: TCP
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
	RFC2466	Base de Información de Gestión para IPv6: ICMPv6
Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre Jumbogramas IPv6
	RFC2426	Extensiones FTP para IPv6 y NAT
	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas
	RFC2474	Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2663	Consideraciones y Terminología de IP NAT
	RFC2732	Formato para la representación literal de direcciones IPv6 en URL's
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2775	Transparencia de Internet

6 Administración De Redes.

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red mas segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

- Mezclas de diversas señales, como voz, datos, imagen y gráficas.
- Interconexión de varios tipos de redes, como WAN, LAN y MAN.
- El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo y microondas.
- Diversos protocolos de comunicación, incluyendo TCP/IP, SPX/IPX, SNA, OSI.
- El empleo de muchos sistemas operativos, como DOS, Netware, Windows NT, UNIS, OS/2.
- Diversas arquitecturas de red, incluyendo Ethernet 10 base T, Fast Ethernet, Token Ring, FDDI, 100vg-Any Lan y Fiber channel.
- Varios métodos de compresión, códigos de línea, etc...

El *sistema de administración de red* opera bajo los siguientes pasos básicos:

1. Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
2. Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
3. Transportación de la información del equipo monitoreado al centro de control.
4. Almacenamiento de los datos coleccionados en el centro de control.
5. Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
6. Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con

varias Arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.

6.1 Elementos Involucrados En La Administración De Red

- a) **Objetos:** son los elementos de más bajo nivel y constituyen los aparatos administrados.
- b) **Agentes:** un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. El agente genera el grado de administración apropiado para ese nivel y transmite información al administrador central de la red acerca de:
 - Notificación de problemas.
 - Datos de diagnóstico.
 - Identificador del nodo.
 - Características del nodo.
- c) **Administrador del sistema:** Es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

6.2 Operaciones De La Administración De Red.

Las operaciones principales de un sistema de administración de red son las siguientes:

6.2.1 Administración de fallas.

La administración de fallas maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

- a) Detección de fallas.
- b) Diagnóstico del problema.
- c) Darle la vuelta al problema y recuperación.
- d) Resolución.
- e) Seguimiento y control.

6.2.2 Control de fallas.

Esta operación tiene que ver con la configuración de la red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

6.2.3 Administración de cambios.

La administración de cambios comprende la planeación, la programación de eventos e instalación.

6.2.4 Administración del comportamiento.

Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye: El número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

6.2.5 Servicios de contabilidad.

Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

- Tiempo de conexión y terminación.
- Número de mensajes transmitidos y recibidos.
- Nombre del punto de acceso al servicio.
- Razón por la que terminó la conexión.

6.2.6 Control de Inventarios.

Se debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.

6.2.7 Seguridad.

La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

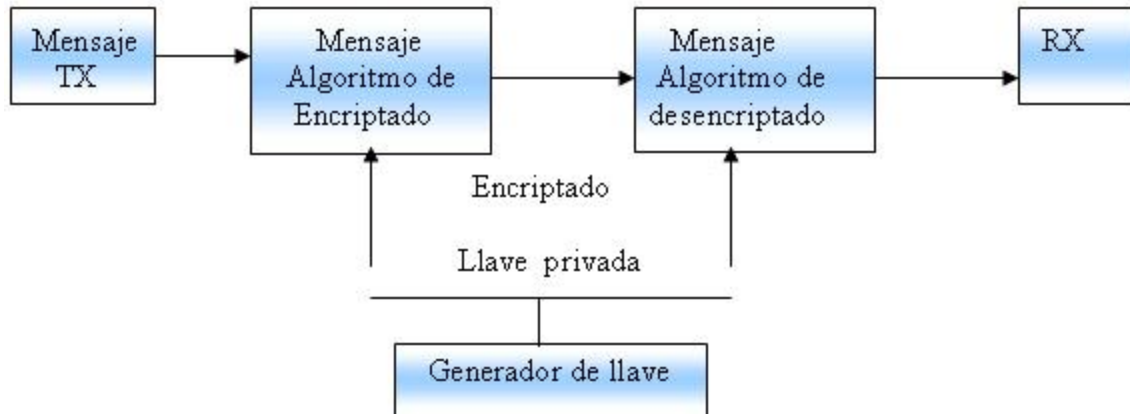
- Identificación y autenticación del usuario, una clave de acceso y un password.
- Autorización de acceso a los recursos, es decir, solo personal autorizado.
- Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración rendimiento, seguridad e inventarios.

6.2.8 Llave privada.

En éste método los datos del transmisor se transforman por medio e un algoritmo público de criptografía con una llave binaria numérica privada solo conocida por el transmisor y por el receptor. El algoritmo más conocido de este tipo es el DES (Data Encryption Standard).

El algoritmo opera así:



6.3 Funciones De Administración Definidas Por OSI.

OSI define las cinco funciones de administración básicas siguientes:

- Configuración
- Fallas
- Contabilidad
- Comportamiento
- Seguridad.

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.

La función de fallas incluye la detección, el aislamiento y la corrección de fallas en la red.

La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red.

La función de comportamiento mantiene el comportamiento de la red en niveles aceptables.

La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

El modelo OSI incluye cinco componentes claves en la administración de red:

CMIS: Common Management Information Services. Éste es el servicio para la colección y transmisión de información de administración de red a las entidades de red que lo soliciten.

CMIP: Common Management Information Protocol. Es el protocolo de OSI que soporta a CMIS, y proporciona el servicio de petición/respuesta que hace posible el intercambio de información de administración de red entre aplicaciones.

SMIS: Specific Management Information Services. Define los servicios específicos de administración de red que se va a instalar, como configuración, fallas, contabilidad, comportamiento y seguridad.

MIB: Management Information Base. Define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información en el MIB incluye: número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, etc...

Servicios de Directorio: Define las funciones necesarias para administrar la información nombrada, como la asociación entre nombres lógicos y direcciones físicas.

Management Information Base (MIB) es un esquema o un modelo que contiene la orden jerárquica de todos los objetos manejados. Cada objeto manejado en un MIB tiene un identificador único. El identificador incluye el tipo (tal como contador, secuencia, galga, o dirección), el nivel de acceso (tal como read/write), restricciones del tamaño, y la información de la gama del objeto.

Define las variables necesitadas por el protocolo del SNMP para supervisar y para controlar componentes en una red. Los encargados traen o almacenan en estas variables. MIB-ii refiere a una base de datos extendida de la gerencia del SNMP que contenga las variables no compartidas por CMOT y el SNMP. Los formatos del MIB de CMIP y del SNMP diferencian en estructura y complejidad.

6.4 Protocolo De Administración De Red TCP/IP.

El sistema de administración de red de TCP/IP se basa en el protocolo SNMP (Simple Network Management Protocol), que ha llegado a ser un estándar de ipso en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado por múltiples fabricantes de puentes, repetidores, ruteadores, servidores y otros componentes de red.

Para facilitar la transición de SNMP a CMOT (Common Management Information Services and Protocol Over TCP/IP), los dos protocolos emplean la misma base de administración de objetos MIB (Management information Base).

Para hacer mas eficiente la administración de la red, la comunidad de TCP/IP divide las actividades en dos partes:

- a) Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
- b) Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas.

6.5 Esquema De Administración.

Como se observa, el agente y la MIB residen dentro del aparato que es monitoreado y controlado. La estación administradora contiene software que opera los protocolos usados para intercambiar datos con los agentes, y software de aplicación de administración de red que provee la interfaz de usuario para a fin de habilitar a un operador para saber el estado de la red , analizar los datos recopilados e invocar funciones de administración.



El administrador de red controla un elemento de red pidiendo al agente del elemento que actualice los parámetros de configuración y que le de un informe sobre el estado de la MIB. El agente intercambia mensajes con el administrador de la red con el protocolo SNMP. Cualquier elemento que participe en la red puede ser administrado, incluidos host, ruteadores, concentradores, puentes, multiplexores, módems, switches de datos, etc... Cuando el aparato controlado no soporta SNMP, se usa un agente Proxy. El agente Proxy actúa como un intermediario entre la aplicación de administración de red y el aparato no soporta SNMP.

6.5.1 Administración de un aparato que no soporta SMMP:



6.6 Mensajes SNMP:

El administrador de red de la estación de control y los agentes instalados en los aparatos manejados se comunican enviando mensajes SNMP. Sólo hay 5 mensajes:

Get request: Contiene una lista de variables que el administrador desea leer de una MIB; es decir, el administrador pregunta a un agente sobre el estado de un objeto.

Get Next request: Este comando provee un modo de leer secuencialmente una MIB.

Set request: El administrador usa este comando para ordenar un cambio en el valor de una o más variables.

Get response: El agente envía este mensaje como réplica a un mensaje de Get request, Get next request o Set request.

Trap: El agente usa este mensaje para informar que ha ocurrido un hecho significativo:

- falla de un enlace local.
- otra vez funciona el enlace.
- mensaje recibido con autenticación incorrecta.

Un mensaje SNMP debe estar totalmente contenido en un datagrama IP, el cuál por omisión, es de 576 bytes, por lo que su tamaño puede llegar a ser de hasta 484 bytes.

6.7 Tipos De Datos De SNMP.

SNMP maneja los siguientes tipos de datos:

Enteros: Para expresar, por ejemplo, el MTU (Maximum Transfer Unit).

Dirección IP: Se expresa como cuatro bytes. Recuérdese que cada elemento de red se configura con al menos una dirección IP.

Dirección física: Se expresa como una cadena de octetos de longitud adecuada; por ejemplo, para una red Ethernet o Token Ring, la dirección física es de 6 octetos.

Contador: Es un entero no negativo de 32 bits, se usa para medir, por ejemplo, el número de mensajes recibidos.

Tabla: es una secuencia de listas.

Cadena de Octetos: Puede tener un valor de 0 a 255 y se usa para identificar una comunidad.

6.8 Base De Datos De Administración: MIB.

La MIB define los objetos de la red operados por el protocolo de administración de red, y las operaciones que pueden aplicarse a cada objeto. Una variable u objeto MIB se define especificando la sintaxis, el acceso, el estado y la descripción de la misma. La MIB no incluye información de administración para aplicaciones como Telnet, FTP o SMTP, debido que es difícil para las compañías fabricantes instrumentar aplicaciones de este tipo para el MIB.

- a) **Sintaxis:** Especifica el tipo de datos de la variable, entero, cadena dirección IP, etc...
- b) **Acceso:** Especifica el nivel de permiso como: Leer, leer y escribir, escribir, no accesible.
- c) **Estado:** Define si la variable es obligatoria u opcional.
- d) **Descripción:** Describe textualmente a la variable.

La **MBI-1** define solo 126 objetos de administración, divididos en los siguientes grupos:

6.8.1 Grupo de Sistemas.

Se usa para registrar información del sistema el cual corre la familia de protocolos, por ejemplo:

- Compañía fabricante del sistema.
- Revisión del Software.
- Tiempo que el sistema ha estado operando.

6.8.2 Grupo de Interfaces.

Registra la información genérica acerca de cada interface de red, como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados, MTU del aparato, etc...

6.8.3 Grupo de traducción de dirección.

Comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar, como la tabla ARP, que relaciona direcciones IP con direcciones físicas de la red LAN.

6.8.4 Grupo IP.

Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc... También contiene información de variables de control que permite aplicaciones remotas puedan ajustar el TTL (Time To Live) de omisión de IP y manipular las tablas de ruteo de IP.

6.8.5 Grupo TCP

Este grupo incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activas como dirección IP, puerto o estado actual.

6.8.6 Grupo de ICMP y UDP.

Mismo que el grupo IP y TCP.

6.8.7 Grupo EGP.

En este grupo se requieren sistemas(ruteadores) que soporten EGP.

La **MIB-2** pretende extender los datos de administración de red empleados en redes Ethernet y Wan usando ruteadores a una orientación enfocada a múltiples medios de administración en redes Lan y Wan. Además agrega dos grupos más:

6.8.8 Grupo de Transmisión.

Grupo que soporta múltiples tipos de medios de comunicación, como cable coaxial, cable UTP, cable de fibra óptica y sistemas TI/EI.

6.8.9 Grupo SNMP.

Incluye estadísticas sobre tráfico de red SNMP.

Cabe señalar que un elemento de red, solo necesita soportar los grupos que tienen sentido para él.

6.8.10 Base de Información Administrativa MIB de SNMP

Una Base de Información Administrativa MIB es una colección de información que está organizada jerárquicamente. Las MIB son accedidas utilizando un protocolo de administración de red como SNMP. Ellas son compresiones de objetos administrados y están identificadas por identificadores de objetos.

Un objeto administrado (a menudo llamado un objeto MIB, un objeto, o un MIB) es una de cualquier cantidad de características de un dispositivo administrado. Los objetos administrados son compresiones de una o más instancias de objeto, que son esencialmente variables.

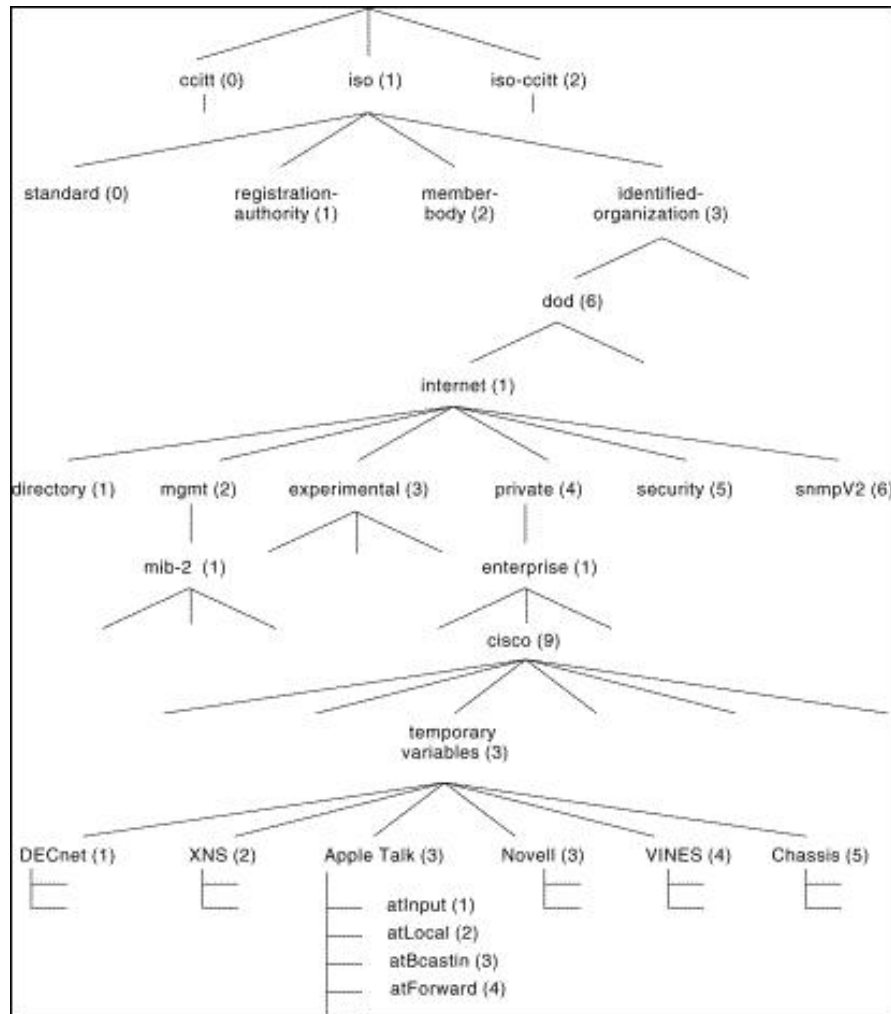
Existen dos tipos de objetos administrados: escalares y tabulares. Los objetos escalares definen sólo una instancia de objeto. Los objetos tabulares definen múltiples instancias relacionadas con objetos que están agrupadas en las tablas MIB.

Un ejemplo de objeto administrado es atInput, el cual es un objeto escalar que contiene una sola instancia de objeto, el valor entero que indica el número total de paquetes AppleTalk de entrada en la interfaz de un enrutador

Un identificador de objeto (o ID de objeto) identifica de forma única un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser graficada como un árbol con una raíz sin nombre, cuyos niveles están asignados por diferentes organizaciones. La Fig. 3 ilustra en árbol MIB. Las identificaciones de objeto MIB de más alto nivel pertenecen a organizaciones de estándares, mientras que las identificaciones de objetos de más bajo nivel son asignadas por organizaciones asociadas.

Los vendedores pueden definir ramas privadas que incluyen objetos administrados por sus propios productos. Los MIB que no han sido estandarizados típicamente están localizados en la rama experimental.

El objeto administrado atInput puede ser identificado de forma única, ya sea por el nombre del objeto –iso.identified-organization.dod.internet.private.enterprise.cisco.temporary.variables.AppleTalk.atInput– o por el descriptor de objeto equivalente, 1.3.6.1.4.1.9.3.3.1.



Árbol MIB que ilustra las diferentes jerarquías asignadas por distintas organizaciones

6.9 Aplicaciones SNMP

6.9.1 *Transcend Network Supervisor de 3COM*

Este software fácil de usar soporta las tareas de administración crítica hasta 1.500 usuarios. Las operaciones automáticas y predeterminaciones inteligentes simplifican las tareas de administración como descubrimiento, mapeo, monitoreo de congestión, visión de eventos, y reporte. Soporta datos concurrenciosos y redes de voz, con mapeo y monitoreo de sistemas de telefonía interconectada 3Com® NBX®. Este producto está disponible para todos los administradores de red sin importar su nivel de experiencia.

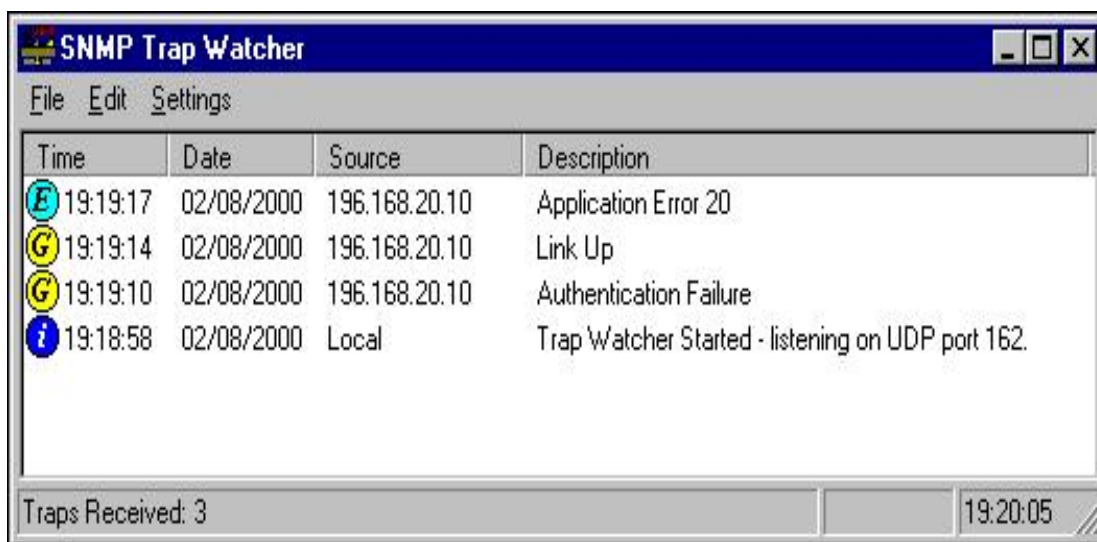
- Disponible gratis en línea e incluido con la mayoría de los dispositivos 3Com® SuperStack®.
- Descubre automáticamente y mapea hasta 1.500 dispositivos con IP habilitado
- Monitorea y reporta el estado de los dispositivos y enlaces claves

- Recomienda optimizaciones
- Mapea conexiones puerto a puerto
- Pasa eventos y alarmas via e-mail, beeper, o mensajes SMS
- El motor de eventos inteligente usa técnicas de correlación para eliminar reporte de eventos desordenado
- Interfaz de usuario intuitiva
- Formato de reporte definido por el usuario
- Visualización gráfica de los dispositivos y conexiones
- Umbrales y alertas fáciles de colocar
- Descarga con un solo botón de nuevas actualizaciones de software

6.9.2 ***SNMP Trap Watcher de BTT Software***

SNMP Trap Watcher está diseñado para ser utilizado para recibir trampas SNMP de equipos de red, incluyendo enrutadores, switches, y estaciones de trabajo. Las trampas son enviadas cuando errores o eventos específicos ocurren en la red. Las trampas normalmente sólo son enviadas a estaciones finales que están enviando peticiones SNMP al dispositivo en cuestión, usando aplicaciones como SNMP Manager o HP OpenView. Sin embargo, algunos dispositivos pueden ser configurados para enviar trampas a las direcciones de estaciones administrativas específicas.

Las trampas SNMP son enviadas por el puerto UDP 162, y SNMP Trap Watcher permite filtrar las trampas por cadena o por tipo (Empresa Específica o Genérico). Usando la 'ventana de decodificación', y seleccionando una trampa específica de la lista, una decodificación de la trampa puede ser visualizada. Esta opción es más útil para depurar el equipo de red que está en etapas tempranas de desarrollo.



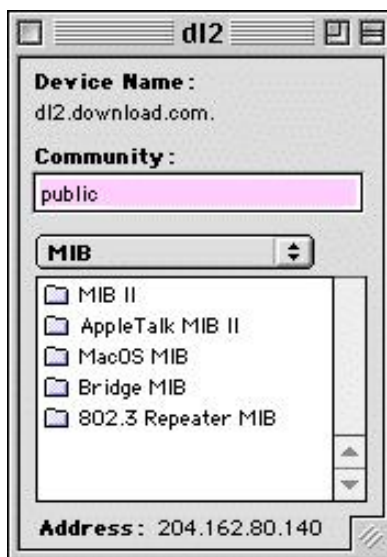
13– Ventana Principal de SNMP Trap Watcher

En circunstancias normales, las trampas SNMP sólo serían de interés para Administradores de Red y Administradores de Sistema.

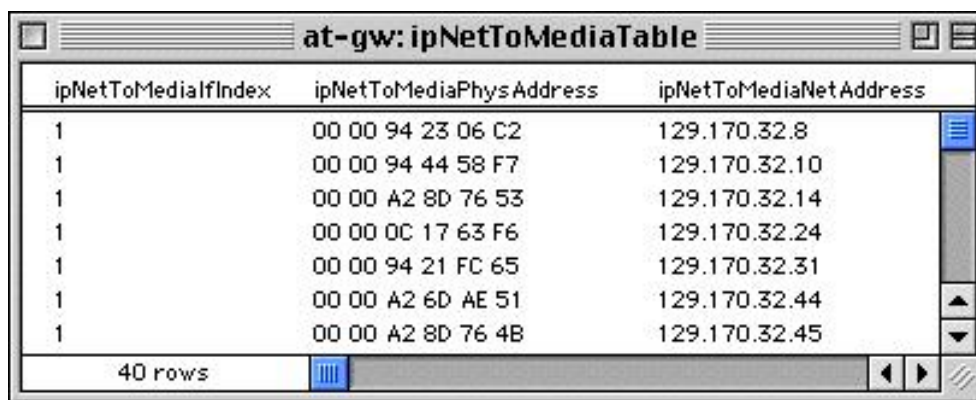
6.9.3 SNMP Watcher de Dartware

SNMP Watcher es una herramienta para recuperar información usando SNMP. SNMP Watcher puede ser usado para monitorear y controlar los componentes de la red. SNMP Watcher puede ser usado para comprobar componentes de red para información sobre su configuración, actividad y errores.

SNMP Watcher visualiza información SNMP para AppleTalk y dispositivos IP. Puede descargar y visualizar información de varios dispositivos simultáneamente. Puede reportar la rata de cambio de varios contadores MIB en una tabla simple para resolución de problemas.



14 Ventana de SNMP Watcher



ipNetToMediaIndex	ipNetToMediaPhysAddress	ipNetToMediaNetAddress
1	00 00 94 23 06 C2	129.170.32.8
1	00 00 94 44 58 F7	129.170.32.10
1	00 00 A2 8D 76 53	129.170.32.14
1	00 00 0C 17 63 F6	129.170.32.24
1	00 00 94 21 FC 65	129.170.32.31
1	00 00 A2 6D AE 51	129.170.32.44
1	00 00 A2 8D 76 4B	129.170.32.45

15 Ventana de SNMP Watcher

6.9.4 NET-SNMP

Net-SNMP es un suite de aplicaciones usados para implementar SNMPv1, SNMPv2 y SNMPv3 usando IPv4 e IPv6. El suite incluye:

- Aplicaciones de línea de comando para:

- Recuperar información de un dispositivo con capacidades SNMP, ya sea una petición (snmpget, snmpgetnext), o múltiples peticiones (snmpwalk, snmptable, snmpdelta)
- Manipular información de configuración en un dispositivo con capacidades SNMP (snmpset)
- Recuperar una colección fija de información desde un dispositivo con capacidades SNMP (snmpdf, snmpnetstat, snmpstatus)
- Convertir entre formas numéricas y textuales de identificadores de objetos MIB y visualizar contenido y estructura (snmptranslate)
- Navegador MIB gráfico (tkmib), usando Tk/perl.
- Aplicación daemon para recibir notificaciones SNMP (snmptrapd). Las notificaciones elegidas pueden ser reportadas (a syslog, NT Event Log, o a un archivo de sólo texto), reenviadas a otro sistema administrador SNMP, o pasadas a una aplicación externa.
- Un agente extensible para responder a las peticiones de información administrativa (snmpd). Éste incluye soporte construido para un amplio rango de módulos de información MIB, y puede ser extendido usando módulos dinámicamente cargados, scripts externos y comandos, y los protocolos SNMP Multiplexing (SMUX) y Agent Extensibility.
- Una biblioteca para desarrollar nuevas aplicaciones SNMP, con C y perl APIs.
- Net-SNMP está disponible para muchos sistemas Unix y similares, y también para Microsoft Windows. La funcionalidad dependiendo del sistema.

6.9.5 Orion Network Performance Monitor de Solarwinds

Orion Network Performance Monitor es un aplicación de administración de desempeño de fácil comprensión basada en la administración de fallas, disponibilidad y ancho de banda de la red que permite a los usuarios ver las estadísticas en tiempo real y la disponibilidad de su red directamente desde el navegador de red. La aplicación Orion Network Performance Monitor monitoreará y recogerá datos de enrutadores, switches, servidores, y cualquier otro dispositivo con SNMP disponible. Adicionalmente, Orion monitorea carga de la CPU, utilización de memoria, y espacio de disco disponible. Orion NMP es una aplicación de disponibilidad administrada altamente escalable, capaz de monitorear desde 10 hasta más de 10.000 nodos.

El motor de alerta de Orion permite configurar alertas para cientos de situaciones e incluye la habilidad de definir las dependencias de los dispositivos. Mientras, el motor de reportes de Orion permite sacar datos que se necesiten desde la base de datos de Orion y visualizarlos en la red o directamente en el escritor de reportajes.



16 Ventanas de Orion Network Performance Monitor

6.9.6 LoriotPro

LoriotPro es una solución de software de monitoreo flexible y escalable que permite control de costos al monitorear y medir la utilización a través de las redes, Sistemas de Información y infraestructuras inteligentes.

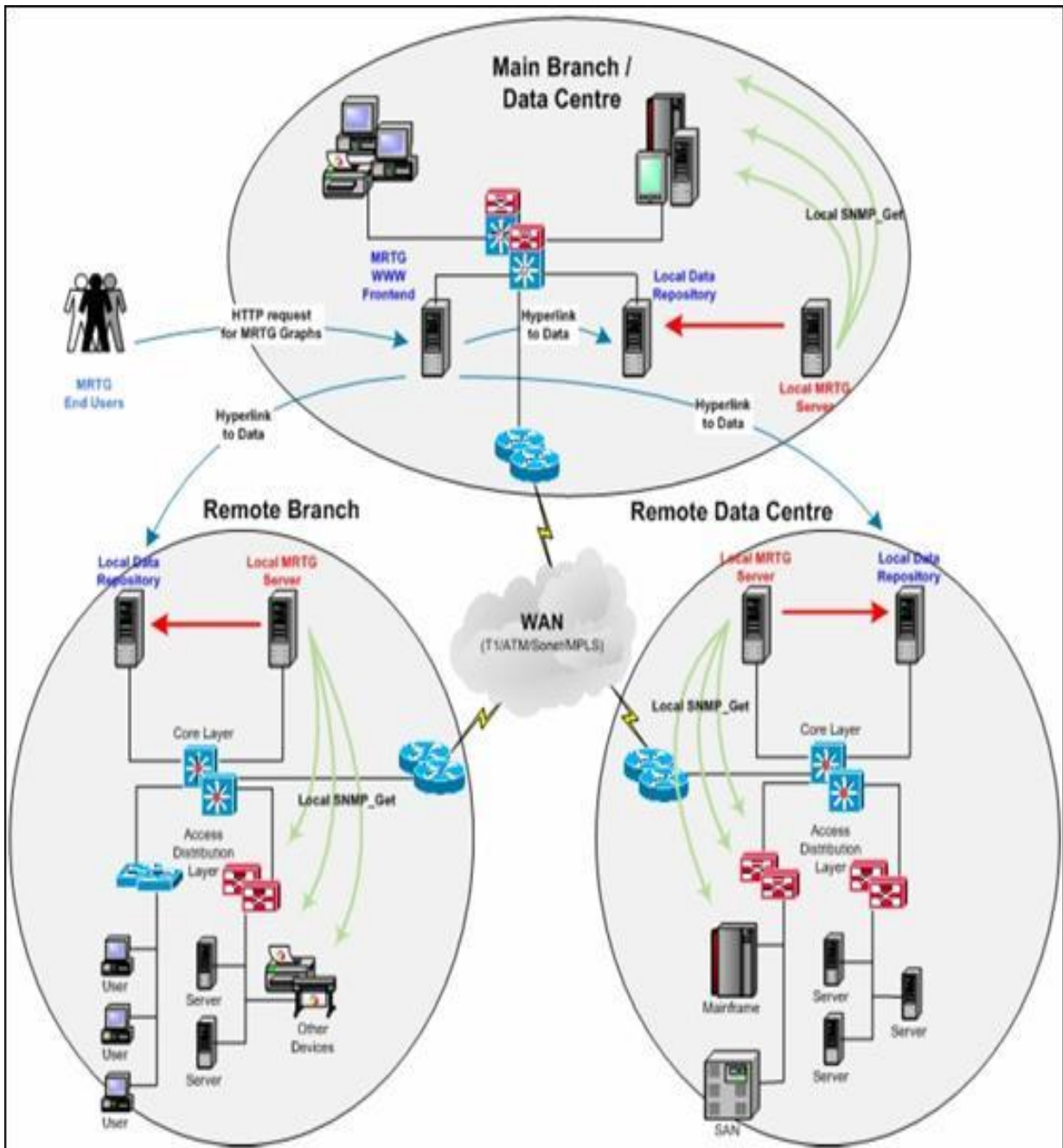
Las características principales de LoriotPro son:

- Monitoreo de disponibilidad de dispositivos y aplicaciones
- Mapas de enrutamiento IP y vistas personalizadas
- Directorio jerárquico de los recursos de la red
- Manejo de desempeño, tendencias.
- Administración de fallas, eventos, trampas, y reporte en el sistema (Syslog)
- Herramientas avanzadas de SNMP y MIB (navegador, caminador, compilador)
- Consola remota de red con control de los derechos del usuario
- Plataforma abierta con tecnología SDK y Plug-in

6.9.7 Multi Router Traffic Grapher (MRTG)

MRTG es una aplicación de administración de red que puede monitorear cualquier host de red remoto que tenga el soporte del protocolo SNMP activado. MRTG, como una aplicación basada en SNMP, lleva a cabo peticiones SNMP contra sus hosts objetivos en una base regular.

Originalmente MRTG fue diseñado para adquirir información del ancho de banda relacionada a las interfaces de la red en un host de red. Hoy en día MRTG puede interrogar a un host acerca de identificadores objetos SNMP y construir el gráfico de variación. Más aun, las nuevas versiones de MRTG son capaces de extender más allá las capacidades de SNMP y recoger información numérica desde cualquier host que recoja y guarde este tipo de información.



17 Departamento distribuido en red de MRTG

MRTG adquiere la información SNMP llevando a cabo las siguientes tareas:

- Interroga el host remoto y obtiene el valor del identificador objeto SNMP específico.
- Actualiza el gráfico de variación con los nuevos valores y borra el gráfico antiguo. Los gráficos son imágenes en formato PNG. La nueva variación del gráfico es guardada en un lugar que puede ser local o remoto en un servidor dedicado a almacenamiento MRTG

Almacena el nuevo valor en el archivo de reporte. El archivo de reporte puede estar localizado en el host local o remotamente en un servidor de almacenamiento MRTG

6.10 Seguridad.

En redes de computadoras, como en otros sistemas, su propósito es de reducir riesgos a un nivel aceptable, con medidas apropiadas. La seguridad comprende los tópicos siguientes:

- a) *Identificación*: (ID) es la habilidad de saber quién es el usuario que solicita hacer uso del servicio.
- b) *Autenticación*: Es la habilidad de probar que alguien es quien dice ser; prueba de identidad. Por ejemplo un *password* secreto que solo el usuario debe conocer.
- c) *Control de Acceso*: una vez que se sabe y se puede probar que un usuario es quien es, es sistema decide lo que le permite hacer.
- d) *Confidencialidad*: Es la protección de la información para que no pueda ser vista ni entendida por personal no autorizado.
- e) *Integridad*: Es la cualidad que asegura que el mensaje es seguro, que no ha sido alterado. La integridad provee la detección del uso no autorizado de la información y de la red.
- f) *No repudiación*: La no repudiación es la prevención de la negación de que un mensaje ha sido enviado o recibido y asegura que el enviador del mensaje no pueda negar que lo envió o que el receptor niegue haberlo recibido. La propiedad de no repudiación de un sistema de seguridad de redes de cómputo se basa en el uso de firmas digitales.

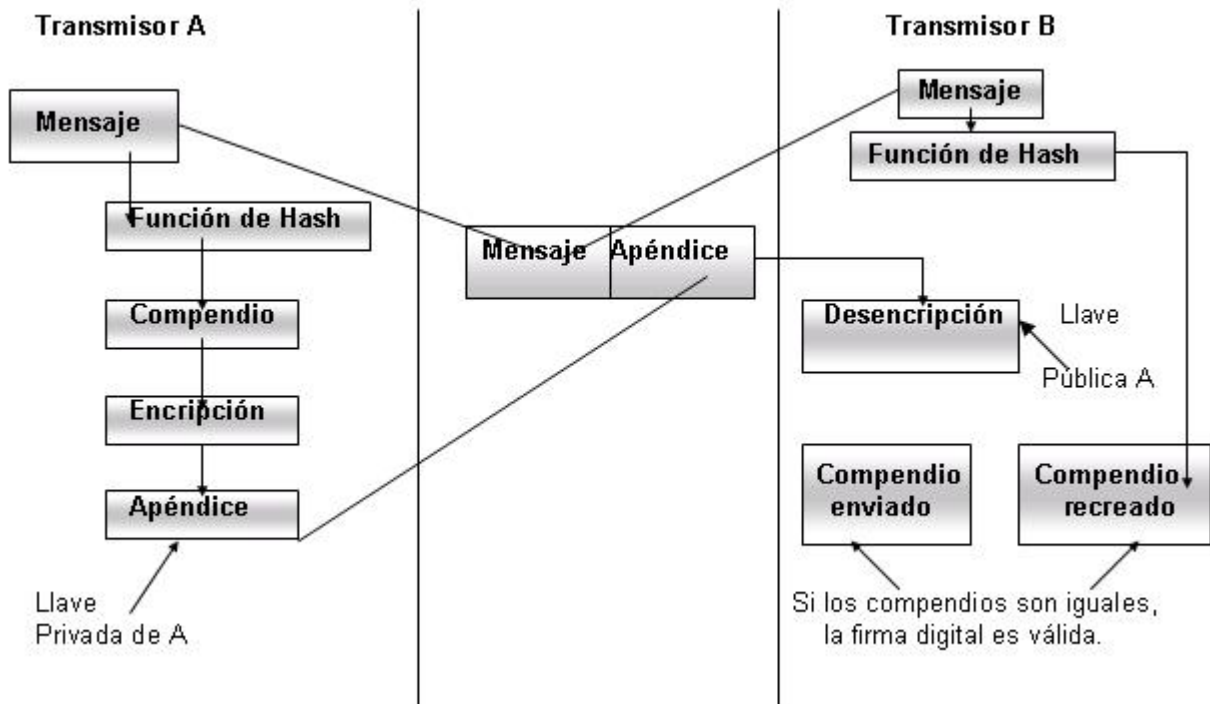
6.11 Firma Digital.

Es un método para verificar el origen y el contenido de un documento electrónico. Se basa en la idea que si el texto de un documento se procesa con un algoritmo de encriptación, luego cualquier cambio en el documento original causará un cambio en la salida del proceso de encriptación, el cual será fácilmente detectado. El mecanismo de encriptación se llama algoritmo Hash, y la salida del proceso se denomina compendio. La creación del compendio del mensaje cuya llave solo es conocida para el enviador se llama firma digital.

La función del Hash se basa en el algoritmo de encriptación de DES. Si se desea mantener secreto el mensaje original, puede encriptarse con una llave privada.

Generalmente no se usa una llave pública porque este método es más lento que el método de encriptación DES.

6.11.1 Operación de la firma digital.



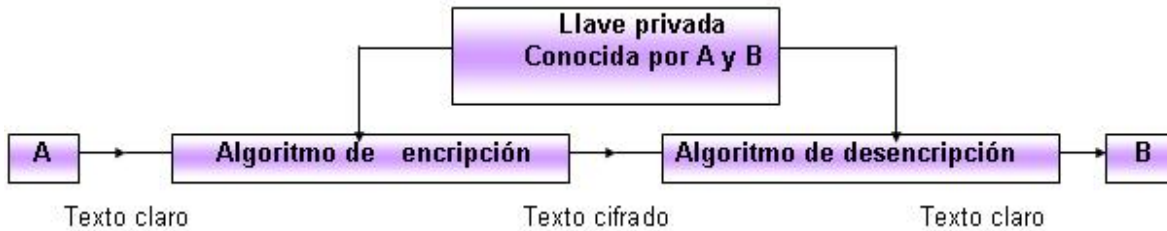
6.12 Criptografía.

Es la técnica que hace ininteligible la información cuando es transmitida, convirtiéndola en un texto cifrado. En el receptor se restaura el texto cifrado a la información original o texto claro con el proceso de criptografía inverso.

El proceso de encriptación se usa un algoritmo que transforma los datos a un texto cifrado empleando una o mas llaves de encriptación durante el proceso de transformación. El texto cifrado es inentendible para cualquier receptor sin el uso del algoritmo de encriptación y de la llave correcta para desencriptar la información.

Hay dos métodos de encriptación:

- Simétrica o de llave privada: conocida por el transmisor y por el receptor para encriptar y desencriptar el mensaje.
- Asimétrica : usa una llave pública para la encriptación del mensaje y una llave privada para la desencriptación del mensaje. Como se verá más adelante, las llaves privada y pública están relacionadas matemáticamente.
- Encriptación con método de llave privada.*



El emisor A genera Información a un texto claro, el cual es sometido a un proceso de encriptación usando un algoritmo de encriptación usando un algoritmo de encriptación y una llave privada para generar el texto cifrado que se transmite.

El contenido del texto cifrado depende ahora de dos elementos: el algoritmo de criptografía y la llave de encriptación, la cual es secreta y solo conocida por A y B.

La Administración de red es la forma de aprovechar al máximo los recursos tanto físicos como internos de la red, manteniéndola operativa y segura para los usuarios. En una administración de red interactúan varios factores que trabajan conjuntamente para proporcionarnos información sobre la situación en que se encuentra nuestra red, y darle posible solución.

Bibliografia:

- Manual de Subneteo, Profesora Martha Beatriz Chavez Teran, UNITEC, 2012.
- Monografia Manual de Subneteo, Zikra, 2009.
- Redes de Comunicación: Topologia y enlaces, Universidad de Valencia, 2010.
- Monografia Tutorial de Subneteo, Gastoncracia, www.GarciaGaston.com.ar, 2009.
- Monografia Planeacion y Administracion de redes, Ing. Ma. Eugenia Macias Rios, 2011.
- Diseño de Redes Locales, Universidad de Oviedo, JA Sirgo y Rafael C. González, 2011.
- Monografia Administracion de Redes, Patricia Cleopatra Victoria Aguilar, 2012