UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

"PLANIFICACION E IMPLEMENTACIÓN DE IPv6
EN UNA RED DE CAMPUS"

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

Eric Gustavo Coronel Castillo

PROMOCIÓN
1996 - II

LIMA – PERÚ
2008

PLANIFICACIÓN E IMPLEMENTACIÓN DE IPv6 EN UNA RED DE CAMPUS

DEDICATORIA

A mi Madre, por su paciencia y apoyo incondicional en todo momento.
A mis hermanos, por su complicidad en esta empresa.
A Olga, sin su comprensión y paciencia no hubiera sido posible lograr esta meta.
A María Fernanda; mí hija, el motor de mi existencia.

S U M A R I O

El presente trabajo aborda primeramente y en forma breve la situación actual de Internet, donde se resalta las implicancias de la escasez de direcciones IP y la necesidad de migrar a un nuevo protocolo que nos permita solucionar este problema, y a la vez mejorar el desempeño logrado por el protocolo IPv4.

Luego se hace una descripción de la arquitectura del protocolo IPv6, aquí se explica las ventajas y dificultades de implementar IPv6.

Seguidamente se describe la red de campus, para identificar los requerimientos hardware y software para la implementación del protocolo IPv6.

Finalmente planteamos el plan de numeración y los pasos a seguir para la implementación de IPv6 con Dual Stack.

I N D I C E

P R Ó L O G O

La crisis del protocolo IPv4 obliga a migrar a un nuevo protocolo denominado IPv6, esta migración no se puede dar de manera inmediata, sino que debe ser gradual, por lo tanto debemos tener un proceso de transición durante el cual en las redes informáticas deben convivir ambos protocolos.

El siguiente trabajo tiene por objetivo presentar una alternativa de solución de como llevar la implementación del protocolo IPv6 en una red de campus.

En el Capitulo I se expone las razones por las que debemos migrar a un nuevo protocolo para la Internet, estos están respaldados por datos estadísticos que nos permiten confirmar la imperiosa necesidad de hacer esta migración. También se presenta las múltiples ventajas que tendríamos con este nuevo protocolo, no sólo en la cantidad de direcciones, sino también en otros aspectos que beneficiaran el desarrollo de las Tecnologías de Información y Comunicación (TIC).

En el Capitulo II se realiza un desarrollo detallado de la arquitectura del protocolo IPv6, pasando por sus cimientos, la estructura de su cabecera, y sus tipos de direccionamiento.

En el Capitulo III se analiza la red de campus, de que manera se va a organizar para hacer una mejor administración; por ejemplo como se van a distribuir los nodos y cuales van hacer las VLAN's que se estarían creando para controlar el trafico en la red.

En el Capitulo IV se analiza el plan de numeración, tanto en IPv4 como en IPv6, y esto es debido a que se esta planteando utilizar "Dual Stack" como solución para poder mantener IPv4 e IPv6 en un proceso de transición.

En el Capitulo V se muestra como realizar su implementación en los switch's, routers y hosts; cuales serían los comandos a utilizar en cada uno de los casos.

Finalmente, concluimos el trabajo presentando las conclusiones a las que se llega luego del análisis y planificación del despliegue del protocolo IPv6.

C A P Í T U L O I
INTRODUCCIÓN

La Internet ha permitido un rápido desarrollo de las Tecnologías de Información y Comunicación, que a su vez, han revolucionado la forma en que las personas trabajan, interactúan y viven diariamente. Estas tecnologías han transformado la economía mundial y anuncian una nueva y dinámica "sociedad de la información".

Hoy en día es imposible o muy difícil realizar nuestras tareas cotidianas y de investigación sin el acceso a Internet, por lo tanto, puedo concluir que la Internet es actualmente imprescindible en nuestras vidas.

Partiendo de esta necesidad, con las limitaciones en cuanto de direcciones físicas de IPv4, entre otras cosas, es mi deber contribuir a la difusión y uso de IPv6 en el ámbito académico y comercial.

1.1. Los motivos de IPv6

La Internet Assigned Numbers Authority (IANA) es responsable de la coordinación global del sistema de direccionamiento del protocolo de Internet, así como también del Autonomous System Numbers utilizado para encaminamiento el tráfico de Internet.

Actualmente hay dos tipos de Protocolo de Internet (IP) en uso: IP versión 4 (IPv4) e IP versión 6 (IPv6). IPv4 fue desplegado el 1 de enero de 1983, y sigue siendo el más utilizado. Las direcciones IPv4 son números de 32-bit expresado como 4 octetos en notación decimal (por ejemplo, 192.0.2.53). El despliegue del nuevo protocolo IPv6 comenzó en 1999. Las direcciones IPv6 son de 128 bits y los números son convencionalmente expresado utilizando cadenas hexadecimales (por ejemplo, 2001:0db8:582:ae33::29).

Tanto las direcciones IPv4 y IPv6 son asignadas generalmente en una forma jerárquica. Las direcciones IP son asignadas por proveedores de servicios de Internet (ISPs). Los ISP obtienen las asignaciones de direcciones IP desde un Registro Local de Internet (LIR) ó un Registro Nacional de Internet (NIR) ó de su Registro Regional de Internet (RIR).

Tabla 1 . 1[1]

Registros Regionales.

Registro	Area
AfriNIC	Africa
APNIC	Asia / Pacifico
ARIN	Norte América
LACNIC	América Latina y algunas islas del Caribe
RIPE NCC	Europa, Medio Oriente, y Asia Central

El rol del IANA es de asignar direcciones IP del grupo de direcciones no asignadas a los RIR de acuerdo a sus necesidades. Cuando un RIR requiere más direcciones IP para la asignación dentro de su región, la IANA hace una asignación adicional para la RIR. La IANA no hará asignaciones directamente a proveedores de servicios de Internet o de los usuarios finales, excepto en circunstancias específicas, tales como asignaciones de direcciones multicast ó de otro tipo de protocolo específico.

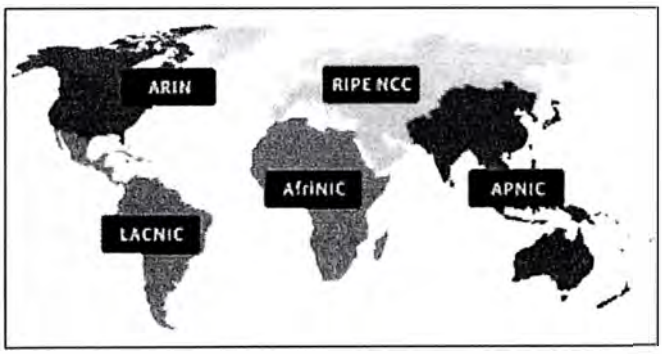


Figura 1 . 1 Registros Regionales[1].

El motivo básico por el que surge, en el seno del Internet Engineering Task Force (IETF), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o "Siguiente Generación del Protocolo Internet"), fue la evidencia de la falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2^{32} (4.294.967.296). En cambio, IPv6 nos ofrece un espacio de 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456). Sin embargo, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora.

Los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de

[1] IANA. Disponible en: http://www.iana.org/numbers [Consulta: 17 mayo 2008]

campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Podemos recordar algunas "famosas frases" que nos ayudarán a entender hasta que punto, los propios "precursores" de la revolución tecnológica que estamos viviendo, no llegaron a prever:

> *"Pienso que el mercado mundial de ordenadores puede ser de cinco unidades", Thomas Watson, Presidente de IBM en 1.943*[2]
>
> *"640 Kbps. de memoria han de ser suficientes para cualquier usuario", Bill Gates, Presidente de Microsoft, 1.981*[2]
>
> *"32 bits proporcionan un espacio de direccionamiento suficiente para Internet", Dr. Vinton Cerf, padre de Internet, 1.977*[2]

No es que estuvieran equivocados, sino que las TIC han evolucionado de un modo mucho más explosivo de lo esperado.

Desde ese momento, y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico. Entre los "parches" más conocidos, podemos citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

El inconveniente más importante de estas ampliaciones de IPv4, es que utilizar cualquiera de ellos es muy fácil, pero no tanto cuando pretendemos usar al mismo tiempo dos "añadidos", y muy poco práctico el uso simultáneo de tres o más.

1.2. ¿Por qué IPv6?

El reducido espacio de IPv4, a pesar de disponer de cuatro mil millones de direcciones (4.294.967.296), junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, nos esta llevando a límites no sospechados en aquel momento.

Además, uno de los problemas de IPv4 permanecería: la gran dimensión de las tablas de encaminado (routing) en la troncal de Internet, que la hace ineficaz, y perjudica enormemente los tiempos de respuesta.

La falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable, por el momento, en Norte América. Sin embargo, en zonas

---

[2] 6SOS. Tutorial de IPv6 Versión 4.0 05-01-2004. Disponible en: http://www.6sos.net/documentos/6SOS_Tutorial_IPv6_v4_0.pdf [Consulta: 17 mayo 2008]

geográficas como Asia (en Japón la situación esta llegando a ser crítica), y Europa, el problema se agrava.

Como ejemplos, podemos citar el caso de China que ha pedido direcciones para conectar 60.000 escuelas, tan sólo ha obtenido una clase B (65.535 direcciones), o el de muchos países Europeos, Asiáticos y Africanos, que solo tienen una clase C (255 direcciones) para todo el país.

Tanto en Japón como en Europa el problema es creciente, dado al importante desarrollo de las redes de telefonía celular, inalámbricas, módems de cable, xDSL, etc., que requieren direcciones IP fijas para aprovechar al máximo sus posibilidades e incrementar el número de aplicaciones en las que pueden ser empleados.

La razón de utilización de las direcciones IP por parte de los usuarios, esta pasando en pocos meses de 10:1 a 1:1, y la tendencia se invertirá. En pocos meses, podemos ver dispositivos "siempre conectados", con lo que fácilmente un usuario podría tener, en un futuro no muy lejano, hasta 50 o 100 IP's (1:50 o 1:100).

Algunos Proveedores de Servicios Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los PSI's se ven obligados a delegar tan sólo reducidos números de direcciones IP públicas para sus grandes clientes corporativos.

La solución, temporalmente, es el uso de mecanismos NAT. Desafortunadamente, de seguir con IPv4, esta tendencia no sería "temporal", sino "invariablemente permanente". Ello implica la imposibilidad práctica de muchas aplicaciones, que quedan relegadas a su uso en Intranets, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT:

- RTP y RTCP ("Real-time Transport Protocol" y "Real Time Control Protocol") usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación).
- La autenticación Kerberos necesita la dirección fuente, que es modificada por NAT en la cabecera IP.
- IPsec pierde integridad, debido a que NAT cambia la dirección en la cabecera IP.
- Multicast, aunque es posible, técnicamente, su configuración es tan complicada con NAT, que en la práctica no se emplea.

Además de NAT, fue necesario mejorar la arquitectura de direccionamiento y pasar del direccionamiento IP-Classful al direccionamiento IP-Classless, estas mejoras incluyen la posibilidad de implementar VLSM y CIDR (Subneting de Subneting y Agregación de rutas - Superneting) orientadas a hacer mas eficiente la distribución de direcciones IP y disminuir el tamaño de las tablas de ruteo..

1.3. El crecimiento de Internet

Los siguientes cuadros estadísticos avalan lo expuesto.

Tabla 1 . 2

Estadísticas Mundiales del Internet a Septiembre del 2007[3]

ESTADISTICAS MUNDIALES DEL INTERNET Y DE POBLACION						
Regiones	**Población (2007 Est.)**	**% Población Mundial**	**Usuarios**	**% Población (Penetración)**	**% Uso Mundial**	**Crecimiento (2000-2007)**
África	933,448,292	14.2 %	43,995,700	4.7 %	3.5 %	874.6 %
Asia	3,712,527,624	56.5 %	459,476,825	12.4 %	36.9 %	302.0 %
Europa	809,624,686	12.3 %	337,878,613	41.7 %	27.2 %	221.5 %
Oriente Medio	193,452,727	2.9 %	33,510,500	17.3 %	2.7 %	920.2 %
Norte América	334,538,018	5.1 %	234,788,864	70.2 %	18.9 %	117.2 %
Latinoamérica / Caribe	556,606,627	8.5 %	115,759,709	20.8 %	9.3 %	540.7 %
Oceanía / Australia	34,468,443	0.5 %	19,039,390	55.2 %	1.5 %	149.9 %
TOTAL MUNDIAL	**6,574,666,417**	**100.0 %**	**1,244,449,601**	**18.9 %**	**100.0 %**	**244.7 %**

Tabla 1 . 3

Los 10 Países Lideres en Internet a Septiembre del 2007

Con Mayor Número de Usuarios[3]

#	País o Región	Usuarios	Población (2007 Est.)	% Población (Penetración)	Fecha dato mas reciente	(%) de Usuarios
1	Estados Unidos	212,708,864	301,967,681	70.4 %	Nielsen//NR Agos./07	17.1 %
2	China	162,000,000	1,317,431,495	12.3 %	CNNIC - Junio/07	13.0 %
3	Japón	87,540,000	128,646,345	68.0 %	ITU - Agos./07	7.0 %
4	India	60,000,000	1,129,667,528	5.3 %	ITU - Sept./07	4.8 %
5	Alemania	52,182,474	82,509,367	63.2 %	Nielsen//NR Agos./07	4.2 %
6	Brasil	42,600,000	186,771,161	22.8 %	ITU - Agos./07	3.4 %
7	Reino Unido	38,512,837	60,363,602	63.8 %	Nielsen//NR Agos./07	3.1 %
8	Corea del Sur	34,120,000	51,300,989	66.5 %	MIC - Dic./06	2.7 %
9	Francia	34,007,264	61,350,009	55.4 %	Nielsen//NR Agos./07	2.7 %
10	Italia	32,190,658	59,546,696	54.1 %	Nielsen//NR Jul./07	2.6 %
Los 10 Países Lideres		**755,862,097**	**3,379,554,873**	**22.4 %**	**IWS - Sept.30/07**	**60.7 %**
Resto del Mundo		**488,587,504**	**3,195,111,544**	**15.3 %**	**IWS - Sept.30/07**	**39.3 %**
Total Mundial Usuarios		**1,244,449,601**	**6,574,666,417**	**18.9 %**	**IWS - Sept.30/07**	**100.0 %**

[3] Éxito Exportador. Disponible en: http://www.exitoexportador.com/stats.htm. [Consulta: 17 mayo 2008]

Tabla 1 . 4

Los 10 Países de Internet con la Mas Alta Tasa de Penetración[3]

#	País ó Región	Población (2007 Est.)	Usuarios	Penetración (% Población)	Fuente
1	Países Bajos	16,447,682	14,544,400	88.4 %	ITU - Agos/07
2	Noruega	4,657,321	4,074,100	87.5 %	ITU - Agos/07
3	Islandia	299,076	258,000	86.3 %	ITU - Sept/06
4	Suecia	9,107,795	6,981,200	76.7 %	ITU - Agos./07
5	Nueva Zelandia	4,274,588	3,200,000	74.9 %	ITU - Sept./05
6	Portugal	10,539,564	7,782,760	73.8 %	IWS - Sept./07
7	Luxemburgo	463,273	339,000	73.2 %	ITU - Agos./07
8	Australia	20,984,595	15,300,000	72.9 %	ITU - Agos./07
9	Estados Unidos	301,967,681	212,708,864	70.4 %	Nielsen//NR Ago./07
10	Falkland Islands	1,900	2,736	69.4 %	CIA - Dic./02
10 Países Lideres		**368,744,311**	**265,190,224**	**71.9 %**	**IWS - Sept.30/07**
Resto del Mundo		**6,205,922,106**	**979,259,377**	**15.8 %**	**IWS - Sept.30/07**
Total Mundial Usuarios		**6,574,666,417**	**1,244,449,601**	**18.9 %**	**IWS - Sept.30/07**

Pero lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto encaminables (enrutables): Videoconferencia, Voz sobre IP, seguridad, e incluso juegos.

En 1.997, el mercado de dispositivos con aplicaciones capaces de conectarse a Internet (sin incluir terminales ni ordenadores, tan sólo WebTV, agendas electrónicas, teléfonos con acceso a Internet, y consolas de juegos), era de 3.000.000. En el año 1.998, este se duplica hasta llegar a los 6.000.000, y las previsiones de crecimiento para el 2.002, según IDC, fueron de 56.000.000.

Sólo contabilizando el crecimiento de la nueva generación de telefonía móvil (UMTS), para el año 2.004 se estimaron cifras del orden de los 1.000.000.000 de usuarios, la misma cifra que para la telefonía fija y que para el número de usuarios "fijos" de Internet.

El mismo Foro UMTS/GSM estimo las necesidades de direcciones IP para los dispositivos de la red (no para los dispositivos de los usuarios), para el año 2.005, en 3,2 millones, y de 6,3 para el 2.010. Según el mismo informe, en el 2.005, se proyectó un requerimiento total de 20.000.000.000 de direcciones IP para los dispositivos de los usuarios.

Además debemos considerar los innumerables dispositivos que vamos creando; los ya existentes, los cuales son mejorados mediante su conexión a la red, por ejemplo:

Teléfonos, pues la siguiente generación, sin duda, pasara por tecnologías IP (VoIP).

- Televisión y Radio, también basados en tecnologías IP.
- Sistemas de seguridad, televigilancia y control.
- Frigoríficos que evalúan nuestros hábitos de consumo y nos dan la opción de a) imprimir la lista de la compra, b) hacer el pedido en el supermercado para que nos sea entregado automáticamente, c) hacer el pedido para que pasemos a recogerlo decidiendo "in situ" el resto de la compra, d) navegar por un supermercado virtual y permitirnos llenar el carro según nuestros hábitos añadiendo nuestros caprichos ocasionales.

  Despertadores, que conocen nuestros tiempos de desplazamiento habituales a nuestro lugar de trabajo, y con motivo de un accidente o gran nevada, de los que son informados mediante los servicios de la red, calculan el tiempo adicional que necesitamos y nos levantan con la anticipación precisa, ¡aún a riesgo de que los destrocemos al arrojarlos contra la pared!
- Walkman MP3, que conectados a la red, nos permiten recuperar y almacenar creaciones musicales.

Nuevas tecnologías emergentes, como Bluetooth, WAP, redes inalámbricas, redes domésticas, etc., hacen más patente esta necesidad de crecimiento, al menos, en los que al número de direcciones se refiere.

Por ejemplo, la última tendencia es la de permitir a cualquier dispositivo serie, ser conectado a una LAN o WAN, y por que no a Internet. Este tipo de "convertidores", denominados "Universal Device Server", o Servidor de Dispositivos Universal, permite que aplicaciones impensables por las limitaciones de los cableados serie, se realicen remotamente a través de redes, o incluso que un sistema de alarmas, que antes requería un módem dedicado para la conexión con la central de recepción de alarmas, pueda ahora enviar un e-mail, ¡con todo lujo de detalles!.

Podríamos hablar, en general, de casi cualquier dispositivo tanto doméstico como industrial, integrado en la gran red, pero también en dispositivos de control médico, marcapasos, etc.

1.4. Características principales de IPv6

Si resumimos las características fundamentales de IPv6 obtenemos la siguiente relación:

- Mayor espacio de direcciones.
- "Plug & Play": Autoconfiguración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS) y Clase de Servicio (CoS).

- Multicast: Envío de UN mismo paquete a un grupo de receptores.
- Anycast: Envío de UN paquete a UN receptor dentro de UN grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los encaminadores (routers), alineados a 64 bits (preparados para su procesado óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del encaminador (router).
- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Encaminado (enrutado) más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Renumeración y "multi-homing", que facilita el cambio de proveedor de servicios.
- Características de movilidad.

Pero hay que insistir, de nuevo, en que estas son las características básicas, y que la propia estructura del protocolo permite que este crezca, o dicho de otro modo, sea escalado, según las nuevas necesidades y aplicaciones o servicios lo vayan precisando. Precisamente, la escalabilidad es la baza más importante de IPv6 frente a IPv4.

1.5. Proyección de IPv6

El camino de IPv4 a IPv6 no es una cuestión de transición ni de migración, sino de evolución, de integración, pero se trata de una evolución disruptora, rompedora, y al mismo tiempo necesaria. IPv6 nos permitirá un crecimiento escalable y simple, principales handicaps actuales de IPv4. Preparemos y mejoremos nuestras redes, las de nuestros clientes, las nuevas implantaciones, con dispositivos, sistemas operativos y aplicaciones que estén realmente listos o en camino de cumplir las especificaciones de IPv6, sin por ello dejar de ser válidos en IPv4.

C A P Í T U L O I I
ARQUITECTURA TCP/IPv6

Hablar de IPv6, es hablar de una evolución del protocolo IP, ya que los creadores de IPv4 a principios de los años 70s, no predijeron en ningún momento el gran éxito que este protocolo iba a tener en muy poco tiempo, en una diversidad de campos, no solo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

2.1. Los cimientos de IPv6

Los criterios que se han seguido a lo largo del desarrollo de IPv6 han sido fundamentales para obtener un protocolo sencillo y al mismo tiempo extremadamente consistente y escalable.

Destacamos la especial aptitud para ser soportado por plataformas existentes, y una evolución que permite su uso concurrente con IPv4: No es necesario realizar un cambio "instantáneo en una fecha X", sino que el cambio es transparente.

Estos criterios se han alcanzado en gran medida por la ortogonalidad[1] y simplificación de la cabecera de longitud fija, lo que redunda en la eficacia, tanto en pequeños encaminadores como en los más grandes, con soportes de ancho de banda muy superiores a los 100 Gbytes con los dispositivos actuales.

Los equipos actuales, a pesar de sus tremendas capacidades de procesamiento de paquetes, no serían capaces de acometer la misma tarea, ni de ofrecer soluciones a todas las necesidades emergentes, con la estructura de la cabecera IPv4, sin contar la imposibilidad de gestionar las tablas de encaminado de los troncales, si siguen creciendo al ritmo actual.

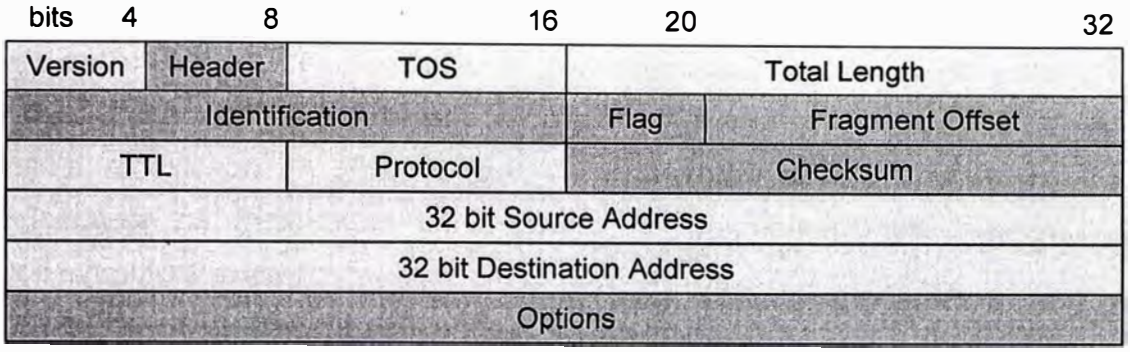
[1] Ortogonalidad: Independencia entre campos.

2.2. Especificaciones básicas de IPv6

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

Tabla 2 . 1

Cabecera del Paquete IPv4

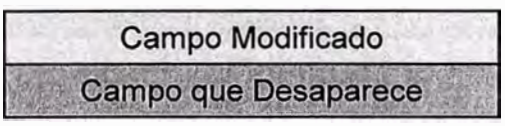


En la Tabla 2.1 tenemos la estructura de la cabecera IPv4. Podemos ver que la longitud mínima de la cabecera IPv4 es de 20 bytes, cada fila de la tabla representa 4 bytes. A ello hay que añadir las opciones, que dependen de cada caso.

A continuación tenemos la descripción de cada campo:

- 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)
- Options: Opciones

En la Tabla 2.1 se ha marcado, mediante el color de fondo, los campos que desaparecen 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 hace innecesario este campo. En IPv6 los encaminadores no fragmentan los paquetes, la 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 tráficos 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, presenta la cabecera mostrada en la Tabla 2.2.

Tabla 2 . 2

Cabecera del Paquete IPv6

bits 4	12	16	24	32
Versión	Clase de Trafico	Etiqueta de Flujo		
Longitud de Carga Útil		Siguiente Cabecera	Limite de Saltos	
Dirección Fuente de 128 bits				
Dirección Destino de 128 bits				

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

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

La longitud fija de la cabecera, implica una mayor facilidad para su proceso en routers y conmutadores, incluso mediante hardware, lo que implica mayores prestaciones.

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 destinos 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.

En la Figura 2.1 se ilustra 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).

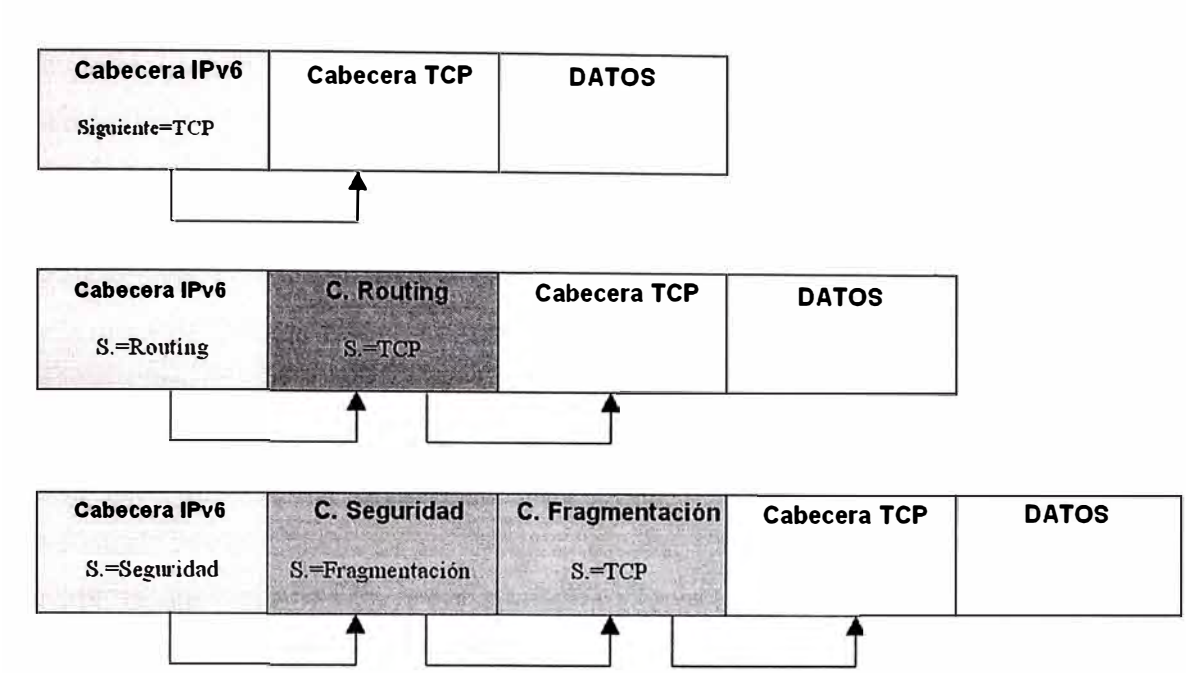


Figura 2 . 1 Ejemplos de Uso del Campo "Siguiente Cabecera"

La Unidad Máxima de Transmisión (MTU), 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.

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

2.3. Direcciones y direccionamiento en IPv6

Ya hemos dicho que IPv6 nos aporta, como principio fundamental, un espacio de 2^{128} direcciones, lo que equivale a 3,40E38 (340.282.366.920.938.463.463.374.607.431.768.211.456).

Calculemos el número de direcciones IP que podríamos tener por metro cuadrado de la superficie terrestre: la cantidad obtenida es 665.570.793.348.866.943.898.599.

La que significa que hay direcciones para todos los dispositivos que podamos imaginar, no solo terrestres, sino interplanetarios.

2.3.1. 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).

2.3.2. 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.

2.3.3. 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.

Tabla 2 . 3

Tabla de Asignamiento.

Estado	Prefijo (Binario)	Fracción de 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	
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.

2.3.4. 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

2.3.5. Representación de las direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

a) x: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:x:d: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:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

Pueden representarse como:

::13.1.68.3

::FFFF:129.144.52.38

d) 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

2.3.6. 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:

128 bits
Dirección del nodo

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

n bits	128 – n bits
Prefijo de subred	Identificador de la Interfaz

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: Local de Enlace (Link-Local) y Local de Sitio (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
1111111010	0	ID de la subred	Identificador de Interfaz

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

2.3.7. Direcciones anycast

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	0000000000000000000

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	

2.4. Direcciones multicast

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 bits	4 bits	4 bits	112 bits
11111111	000T	ámbito	00000000000000000000

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

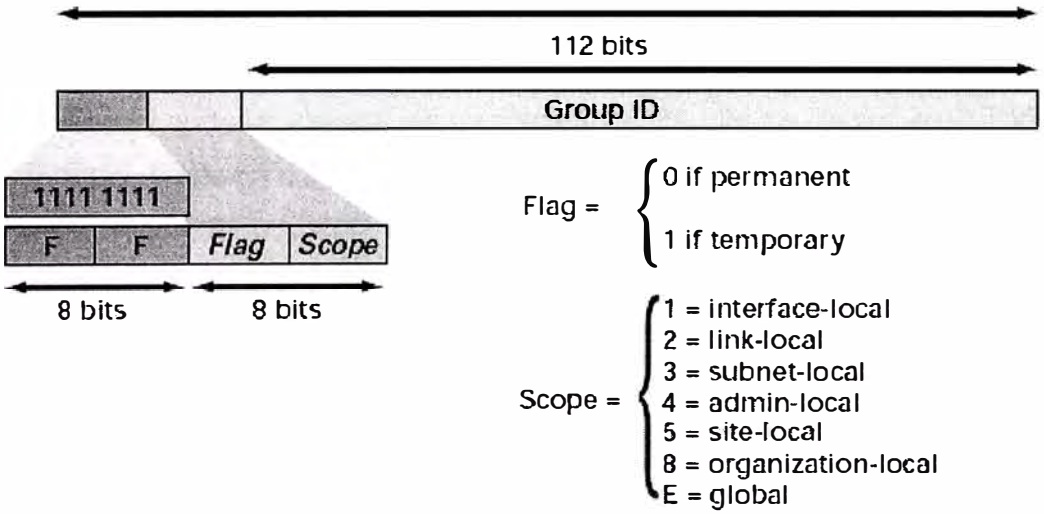


Figura 2 . 2 Formato del Direccionamiento Multicast

La Figura 2.2 muestra el formato del direccionamiento multicast; 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:0:0:0:0:0:0:0.

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

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

2.5. 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).

2.6. Direcciones IPv6 globales unicast y anycast

Las direcciones unicast y anycast comparten el mismo formato. El espacio de direcciones unicast contiene las direcciones anycast. Esas direcciones aparecen como direcciones unicast para los dispositivos que no son configurados como anycast.

Cuando una dirección unicast es asignado a mas de una interfaz, se convierte en una dirección anycast, los nodos al cual la dirección es asignado debe ser explícitamente configurado para ser usado y reconocido como dirección anycast.

Un paquete que es enviado a una dirección anycast enruta al dispositivo o interfaz que comparte la dirección. Un enviante crea un paquete con la anycast como dirección destino y reenvía a su ruteador más cercano. El origen puede usar direcciones anycast para controlar la ruta a través del cual fluye el tráfico.

Un ejemplo del uso de anycast en Border Gateway Protocol (BGP) en redes "multihomed" es cuando un cliente tiene múltiples ISPs con múltiples conexiones a cualquier otro. El cliente puede configurar una dirección anycast diferente para cada ISP. Cada ruteador para el ISP dado tiene la misma dirección anycast configurada. El dispositivo origen puede elegir que ISP para el envió de paquetes. Sin embargo los ruteadores a lo largo de la ruta determinan el ruteador más próximo para alcanzar ese ISP usando la dirección anycast IPv6.

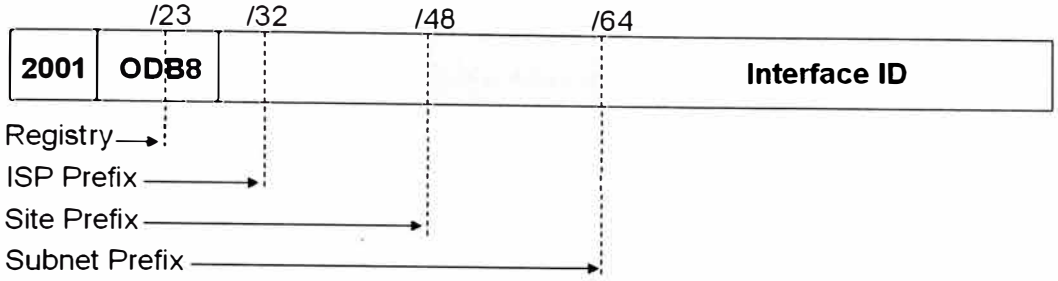


Figura 2 . 3 Formato de Direccionamiento Global Unicast y Anycast

Otro uso para una anycast es cuando una LAN esta conectada a múltiples ruteadores. Esos ruteadores pueden tener la misma dirección IPv6 anycast tal que el dispositivo distante necesita identificar solo la dirección anycast. Los dispositivos intermediarios pueden elegir la mejor ruta para alcanzar el punto de entrada más cercano a esa subred.

Las direcciones unicast globales IPv6 son equivalentes de las direcciones unicast globales IPv4. La estructura de la dirección habilita prefijos de enrutamiento a ser agregados, limitando así el número de entradas de la tabla de ruteo en la tabla de ruteo global. Las direcciones unicast globales usadas sobre los enlaces son agregadas en las salidas a las organizaciones superiores y eventualmente hacia los ISP´s.

Las direcciones unicast globales son definidas por un prefijo de enrutamiento global, un ID de subred, y un ID de interfaz. El espacio de direcciones Unicast IPv6 abarca el rango de direcciones IPv6 entero, con la excepción de FF00::/8 (1111 1111), el cual es usado para direcciones multicast. Las direcciones unicast actuales asignadas por el Internet Assigned Numbers Authority (IANA) usa el rango de direcciones que inician con el valor binario 001 (2000::/3), el cual es un octavo del espacio de direcciones IPv6 y es el bloque mas grande de los bloques de direcciones asignadas.

Las direcciones con un prefijo de 2000::/3 (001) hasta E000::/3 (111), con la excepción de las direcciones multicast FF00::/8 (1111 1111), se requirió para tener identificadores de interfaz de 64 bits en el formato de identificador universal extendido (EUI)-64.

Las direcciones unicast globales típicamente consisten de un prefijo de enrutamiento global de 48 bits y 16 bits de ID de subnet. En el ahora obsoleto RFC 2374, el formato de direcciones unicast globales agregables, el prefijo de enrutamiento global incluido los otros dos campos estructurados jerarquicamente denominados Top Level Aggregator y Next Level Aggregator. Debido a que esos campos se basaron en política, el IETF decidió removerlos de los RFCs. Sin embargo algunas redes IPv6 existentes desplegadas al principio podrían aún estar usando redes basadas en la vieja arquitectura. Un campo de subred de 16 bits denominada ID de subnet podría ser usado por organizaciones individuales para crear su propio direccionamiento jerárquico local e

identificar sus subredes. Este campo permite a una organización usar hasta 65535 subredes individuales. (RFC 2374 a sido reemplazado por el RFC 3587).

La Figura 2.3 muestra el formato de direccionamiento Global Unicast y Anycast.

CAPÍTULO III

LA RED DE CAMPUS, REQUERIMIENTOS HARDWARE/SOFTWARE

3.1. La red de campus

El campus Universitario, posee una extensión próxima a un kilómetro de longitud, en esta residen todas las facultades incluyendo las oficinas administrativas. Debido a la extensión del campus se contemplo la necesidad de un backbone enlazando nodos distribuidos estratégicamente para dar cobertura de acceso a la red a las zonas donde hay presencia humana comprometida con los objetivos de la organización. La Figura 3.1 muestra el campus dividido en sectores, cada sector por lo general comprende una facultad, el cuadro 3.1 muestra la relación de sectores y las facultades respectivas.

Tabla 3 . 1

Lista de facultades y sectores.

SECTOR	FACULTAD/DEPENDENCIA
A	Ingeniería mecánica (FIM)
B	Pabellón Central (Oficinas Administrativas)
C	Ingeniería Química Manufacturera (FIQM)
D	Ingeniería Petrolera (FIP), Ingeniería Ambiental (FIA)
E	Teatro
F	Ingeniería Geológica Metalúrgica y Minera (FIGMM)
G	Ingeniería Civil (FIC)
H	Arquitectura Urbanismo y Arte (FAUA)
I	Ingeniería Geológica Metalúrgica y Minera (FIGMM)
J	Ingeniería Civil (FIC)
K	Hidráulica
M	Ingeniería Económica Estadística y Ciencias Sociales (FIECS)
N	Centro de Computo
Q	Ingeniería Eléctrica y Electrónica (FIEE)
R	Ciencias (FC)
S	Ingeniería Industrial y de Sistemas (FIIS)
T	Centro de Investigaciones Sísmicas y Mitigación de Desastres (CISMID)
U	Centro de Tecnología de Información y Comunicación (CETIC)

3.2. El backbone

El backbone de la red esta compuesto por enlaces que salen del nodo principal ubicados en el pabellón central (B), hacia los nodos secundarios que se encuentran en la facultad de ingeniería civil, centro de computo, facultad de ingeniería electrónica en los sectores G, N y Q respectivamente; cada enlace esta compuesto por 12 pares de fibra óptica, 6 pares de fibra multimodo 62.5/125 y 6 pares de fibra monomodo 10/125. La presencia de fibre óptica multinodo es debido a la antigua infraestructura de red con que contaba el campus (Backbone ATM, ethernet de 10 Mbps a nivel de acceso). La cantidad de pares de fibra óptica en exceso se hace necesario para cubrir posibles ampliaciones o deterioro de algunos de los pares.

Los pares de fibra óptica monomodo fueron conectorizados en la actualización del equipo electrónico de comunicaciones, la actualización realizada llevo al backbone a gigabitethernet y en el nivel de acceso a ethernet 10/100.

La fibra óptica ha sido instalada a través de ducterias subterráneas, las líneas en verde en la Figura 3.1 muestran el trayecto de estas ducterias, saliendo del nodo principal B, hacia cada uno de los nodos secundarios G, N y Q. Aunque la figura 3.1 muestra como si se tratara de un bus, en realidad desde el nodo B salen conexiones punto a punto hacia cada uno de los otros nodos. La tecnología usada actualmente para el transporte de datos a alta velocidad en el backbone es Gibabit ethernet operando a 1000 Mbps, completamente compatible con ethernet 10/100, tecnología usada para el acceso de los usuarios finales.

La Figura 3.2 muestra un diagrama lógico de interconexión de los diferentes nodos que componen la red de campus universitario. Muestra los enlaces entre los diferentes nodos secundarios con el nodo principal, existe una conexión punto a punto en cada caso, a partir de cada uno de los nodos secundarios y también del primario se extienden las conexiones hacia los nodos de acceso para la conexión de los dispositivos de usuarios finales.

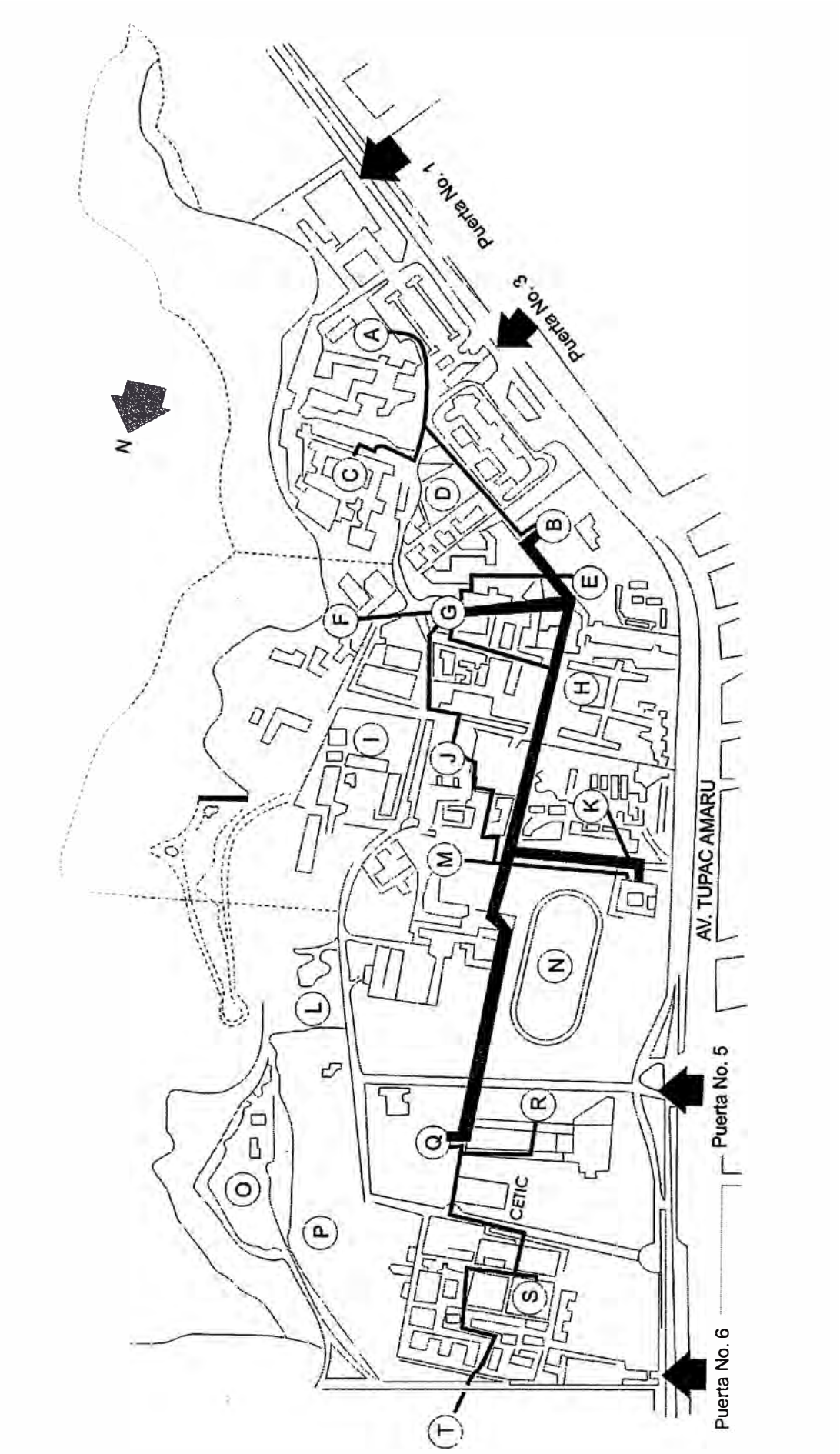


Figura 3 . 1 El Campus Universitario Dividido en Sectores

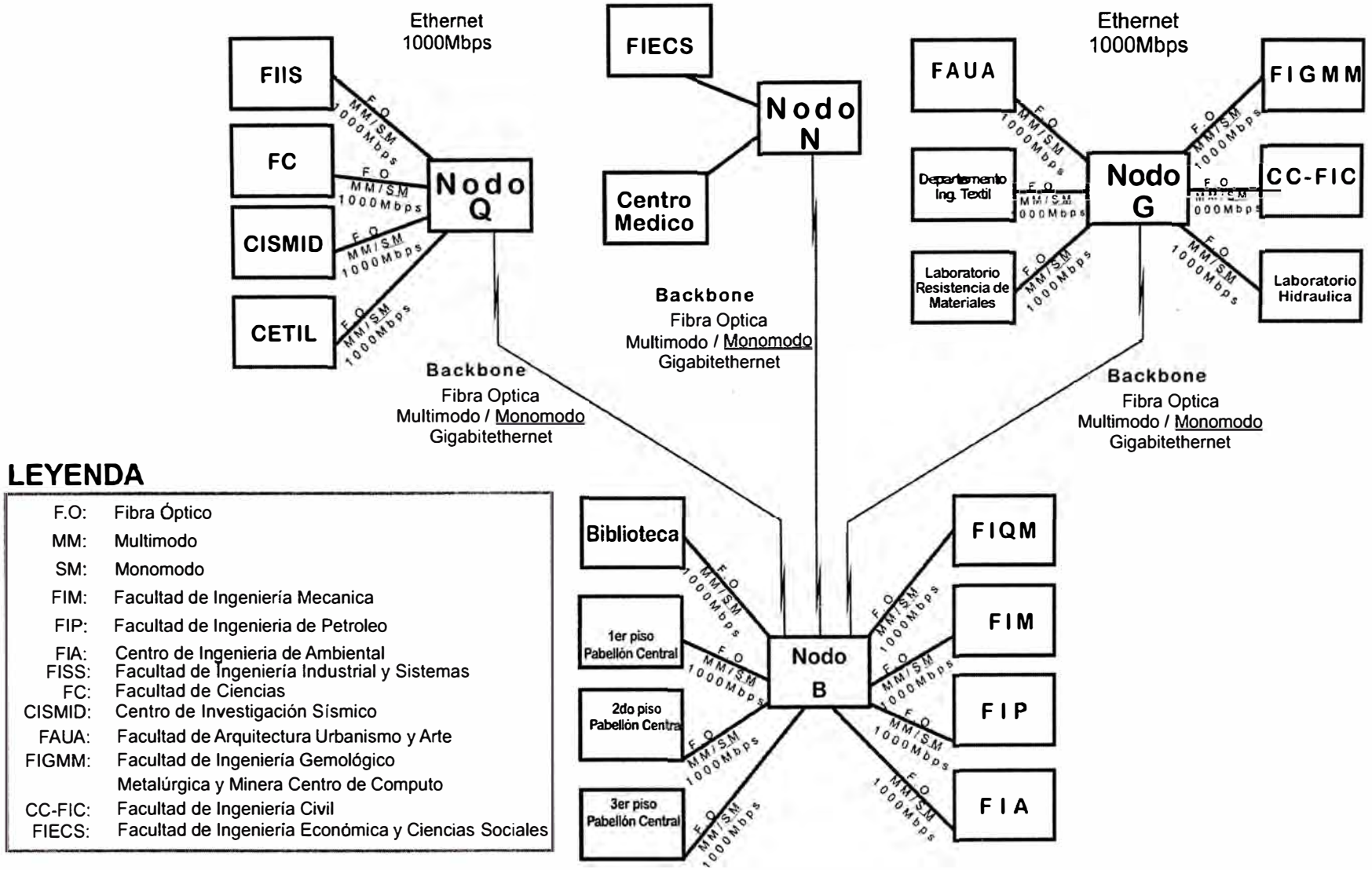


Figura 3 . 2 Vista lógica de interconexión de los diferentes Nodos.

La Figura 3.3 muestra los nodos secundarios conectándose al principal, y al backbone usado para la interconexión. El medio fisico utilizado es Fibra Óptica Monomodo para dar soporte a equipos Gigabitethernet.

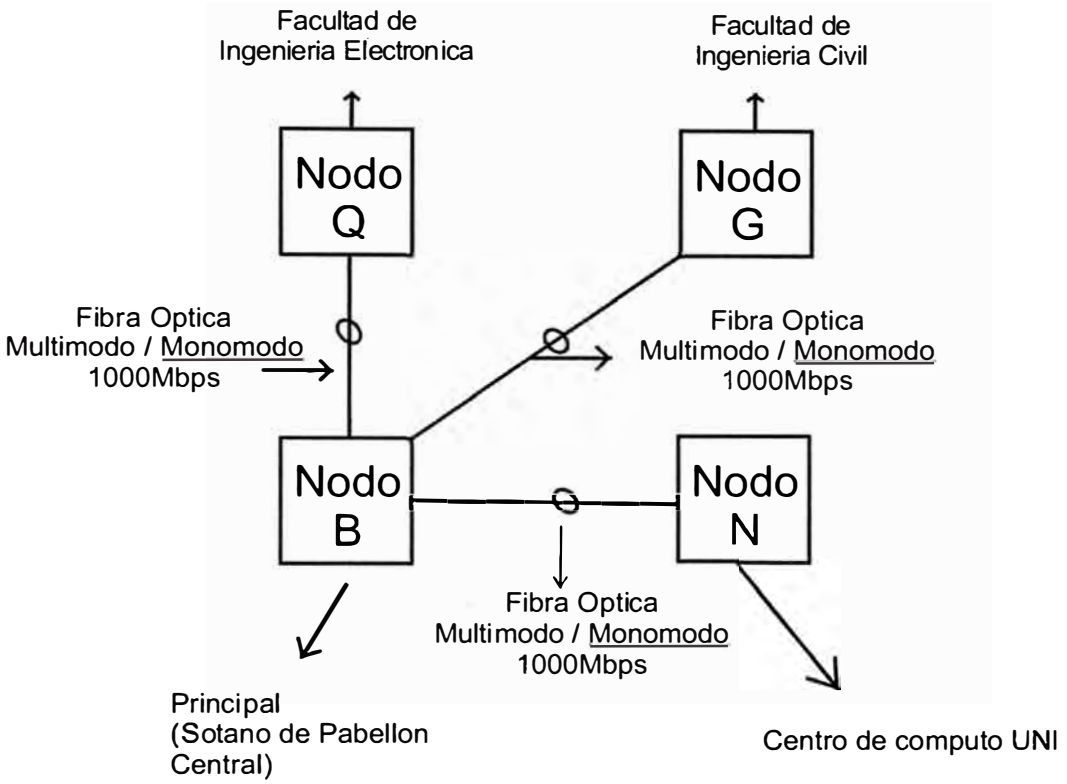


Figura 3 . 3 Interconexión de los nodos secundarios al nodo principal

3.3. Los enlaces de distribución

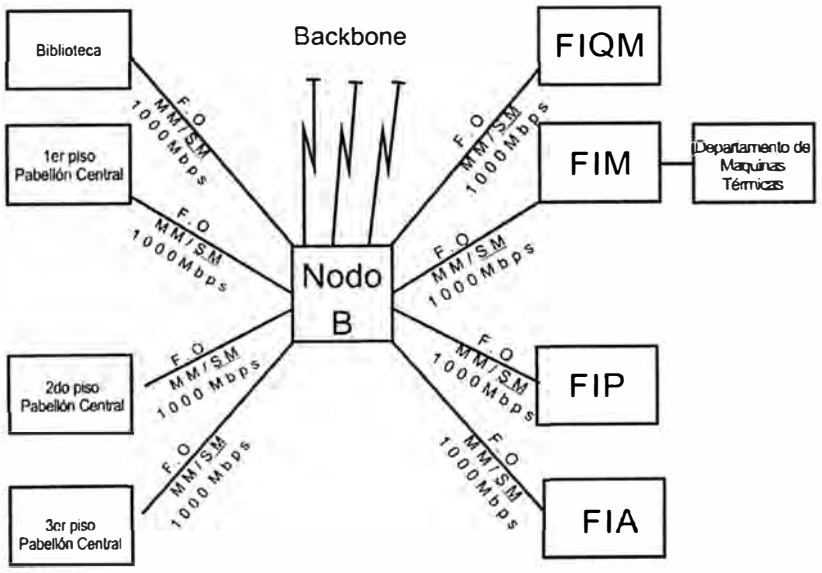
A partir de cada uno de los nodos primario y secundarios se extienden enlaces hacia los diferentes sectores de las diferentes facultades, las longitudes que deben cubrir cada uno de estos enlaces superan los 100 metros, no siendo factible el uso de cable par trenzado, siendo por tanto necesario la instalación de fibra óptica entre los nodos secundarios y los puntos de acceso, además la norma de cableado estructurado establece que toda conexión entre edificios debe hacerse usando fibra óptica, una de las razones para el uso de fibra óptica es evitar el problema de las diferencias de los potenciales a tierra de cada edificio, al no usarse señal eléctrica se produce un aislamiento perfecto.

Los enlaces interconectan SWITCH'S 10/100/1000, en los nodos secundarios se encuentran los SWITCH´s (conmutadores) 10/100/1000 y en los puntos de acceso están los SWITCH'S 10/100, para poder transmitir las señales de los switch´s a través de la fibra óptica se requiere una conversión del tipo de señal de eléctrico a óptico y viceversa, para eso se usan puertos Bgic.

3.3.1. El nodo B

El nodo principal (B) conecta a los nodos de acceso ubicados en las facultades de Ingeniería Química Manufacturera, Ingeniería Mecánica, Ingeniería de petróleo, Ingeniería ambiental, Biblioteca, pabellón central pisos 1, 2 y 3. Cada uno de los enlaces es de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo, actualmente conectorizado mediante Fibra Óptica Monomodo. Ver Figura 3.4.

En cada uno de los nodos de acceso reside en un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, SWITCH de 24 puertos que incorpora puertos Gbic con salida a fibra óptica, un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS). Desde estos puntos se distribuye las conexiones de usuario final en el área de trabajo mediante un cableado horizontal utilizando cable par trenzado.



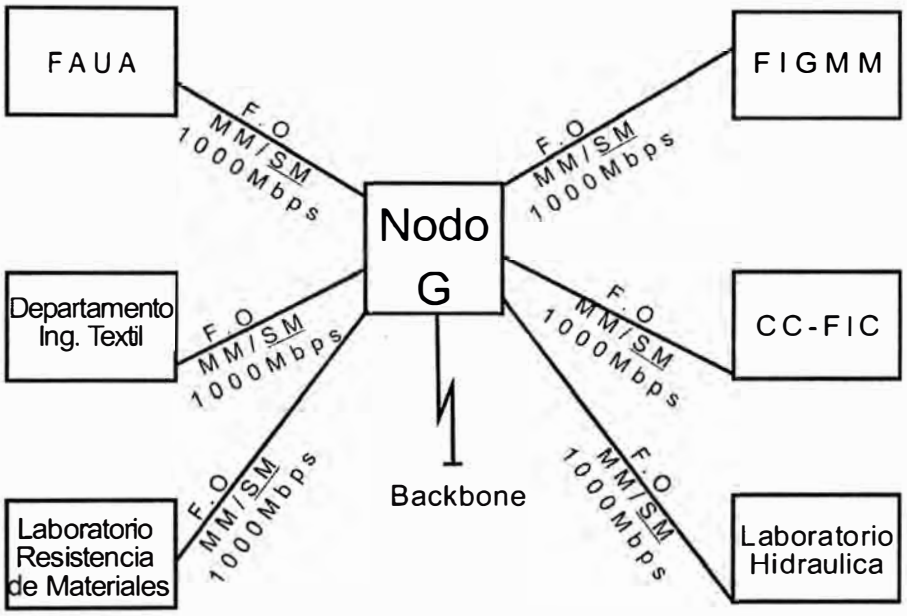
F.O: Fibra Optica
MM: Multimodo
SM : Monomodo
FIM: Facultad de Ingeniería Mecánica
FIP: Facultad de Ingeniería de Petroleo
FIA: Facultad de Ingeniería de Ambiental

Figura 3 . 4 El nodo primario B y los puntos de acceso.

3.3.2. El nodo G

El nodo G conecta a las facultad de Arquitectura Urbanismo y Arte, facultad de Ingeniería Geológica y Minera, departamento de Ingeniería textil, laboratorio de resistencia de materiales, laboratorio de hidráulica, Centro de computo de la facultad de Ingeniería civil. Ver figura 3.5.

Cada uno de los enlaces son de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo. Actualmente conectorizado mediante Fibra Óptica Monomodo.



FAUA: Facultad de Arquitectura Urbanismo y Arte
FIGMM: Facultad de Ingeniería Gemológica Metalúrgica y Minera
CC-FIC: Facultad cd Computo Facultad de Ingeniaría Civil

Figura 3 . 5 El nodo secundario G y los puntos de acceso.

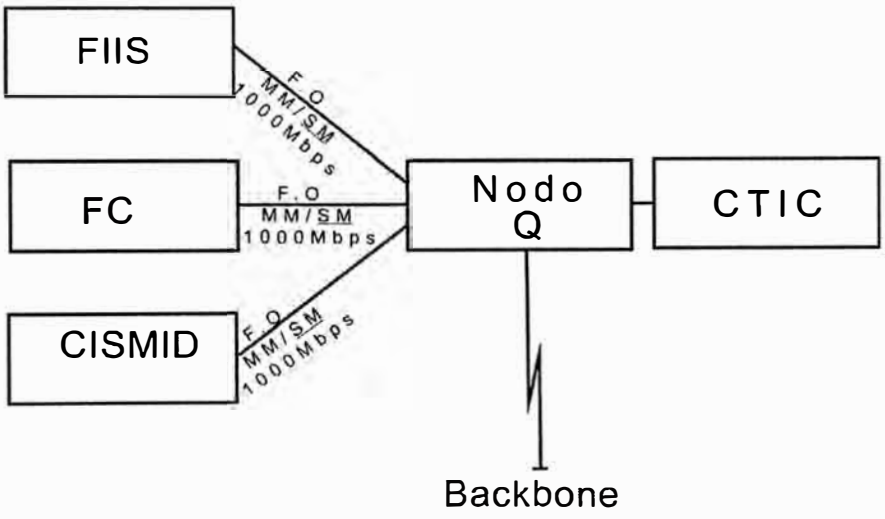
En cada uno de los nodos de acceso reside un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, SWITCH de 24 puertos que incorpora puertos puertos Gbic con salida a fibra óptica, un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS).

3.3.3. El nodo Q

El nodo Q ubicado en la facultad de ingeniería eléctrica y electrónica, conecta a las facultades de ingeniería industrial y de sistemas ubicado en el sector S, facultad de ciencias ubicada en el sector R y el CISMID ubicado en el sector T. Ver figura 3.6.

Cada uno de los enlaces son de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo. Actualmente conectorizado mediante Fibra Óptica Monomodo.

En cada uno de los nodos de acceso reside un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, SWITCH de 24 puertos que incorpora puertos Gbic con salida a fibra óptica, un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS).



F.O: Fibra Optica
MM: Multimodo
SM : Monomodo
FIIS: Facultad de Ingeniería Industrial y Sistemas
FC : Facultad de Ciencias
CISMID

Figura 3 . 6 El nodo secundario Q y los puntos de acceso.

3.3.4. El nodo N

El nodo N ubicado en el centro de computo de la universidad conecta a los puntos de acceso ubicados en la Facultad de Ingeniería Económica Estadística y de Ciencias Sociales ubicada en el sector M, el centro medico, laboratorio de hidráulica ubicada en el sector K y el laboratorio de topografía ubicado en el sector J. Ver figura 3.7.

Cada uno de los enlaces son de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo. Actualmente conectorizado mediante Fibra Óptica Monomodo.

En cada uno de los nodos de acceso reside un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, SWITCH de 24 puertos que incorpora puertos Gbic con salida a fibra óptica, un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS).

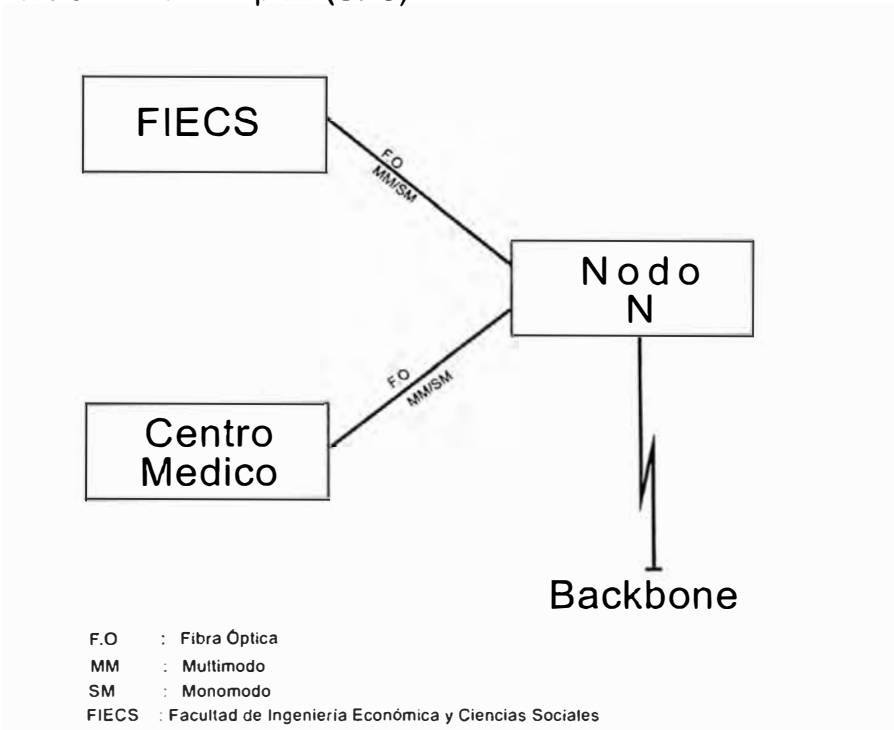


Figura 3 . 7 El nodo secundario N y los puntos de acceso.

3.3.5. Estructura de cada nodo

El nodo principal cuenta con un chasis Catalyst 6506, conteniendo puertos Gigabit y puertos 10/100.

Los nodos secundarios cuentan con un chasis Catalyst 4510R, conteniendo puertos Gigabits y puertos 10/100. La Figura 3.8 muestra una representación esquemática de cada uno de los nodos.

El switch Catalyst 6506 del nodo principal interconecta a los nodos secundarios. La Figura 3.8 muestra gráficamente una representación de la forma como se interconectan los nodos, para ser más preciso debemos añadir que las conexiones se realizan a través del panel de conexiones de fibra óptica en cada uno de los nodos.

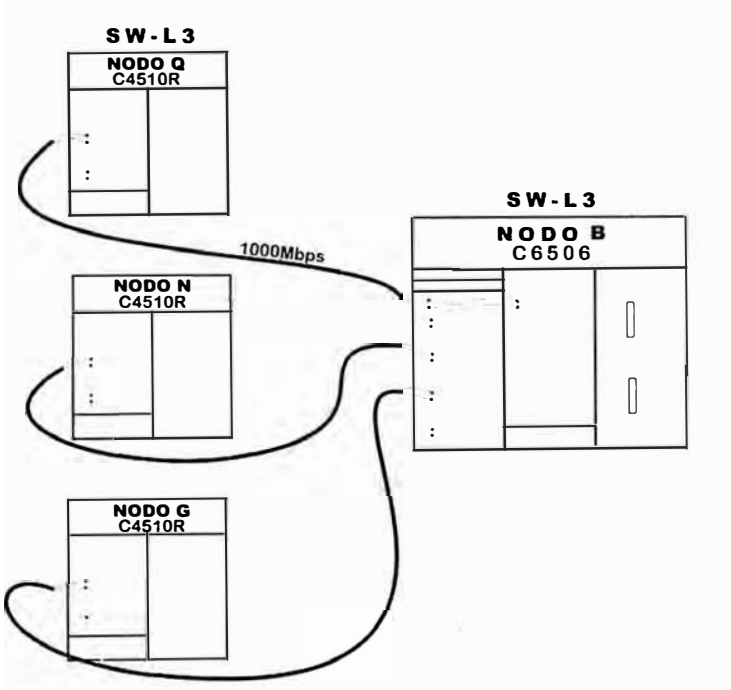


Figura 3 . 8 Composición de cada nodo y su interconexión.

De cada uno de los switchs C4510R, se conectan los switch C3750C y C2950, convirtiéndose de este modo en los dispositivos de acceso a la red para los usuarios finales. De esta manera, los usuarios finales, desde sus PC´s acceden a los recursos de la red, que están en su mismo dominio. La Figura 3.9 muestra una vista aproximada de la interconexión entre los equipos del nodo principal y nodos secundarios, la Figura 3.10 los componentes de cada nodo y su interconexión.

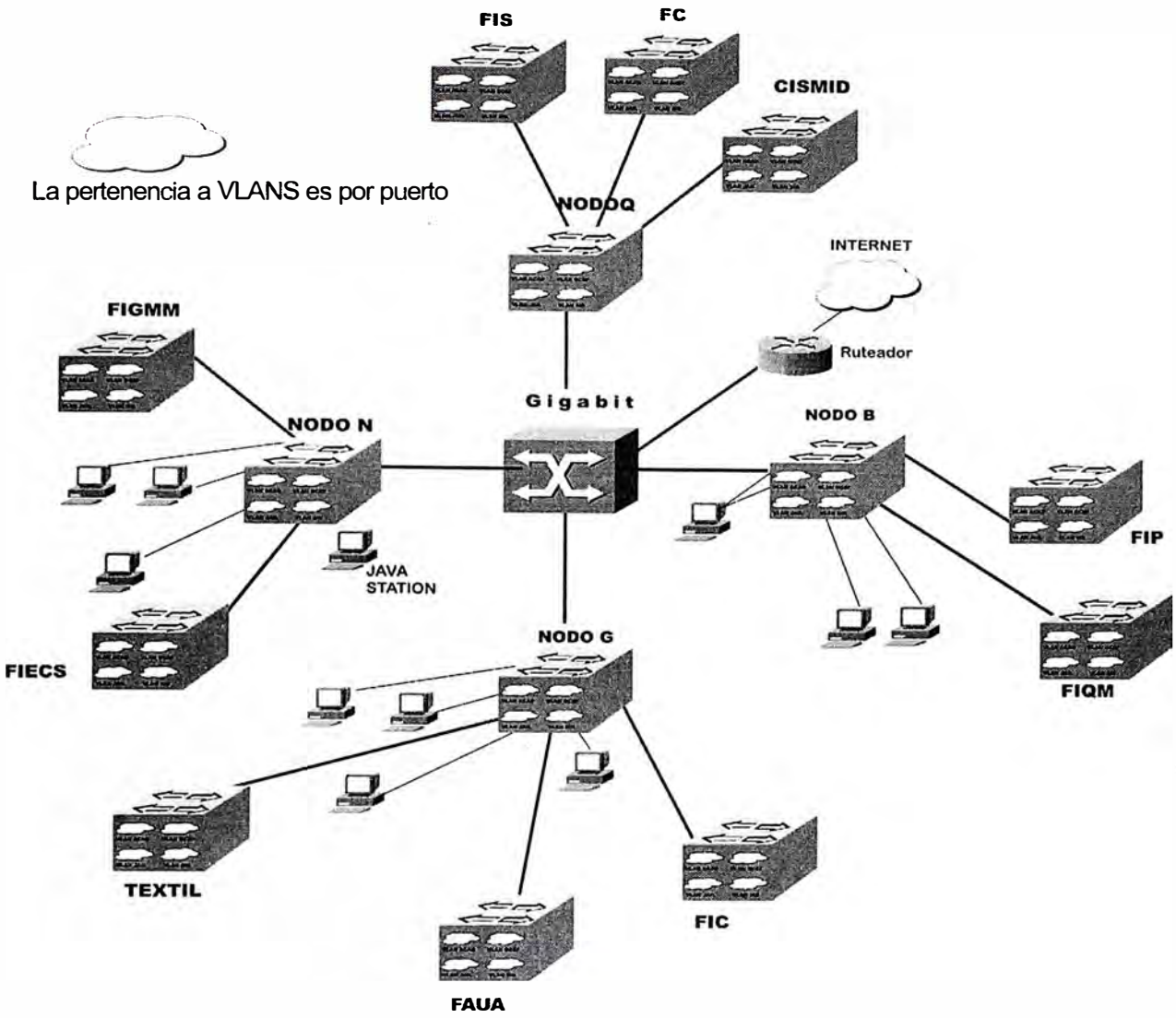


Figura 3 . 9 Diagrama lógico de Interconexión y VLAN's.

El backbone (nodo principal B y nodos secundarios G, N y Q) están compuestos por:

- 1 SWITCH C6506, en el nodo principal
- 3 SWITCH C4510, uno en cada nodo secundario

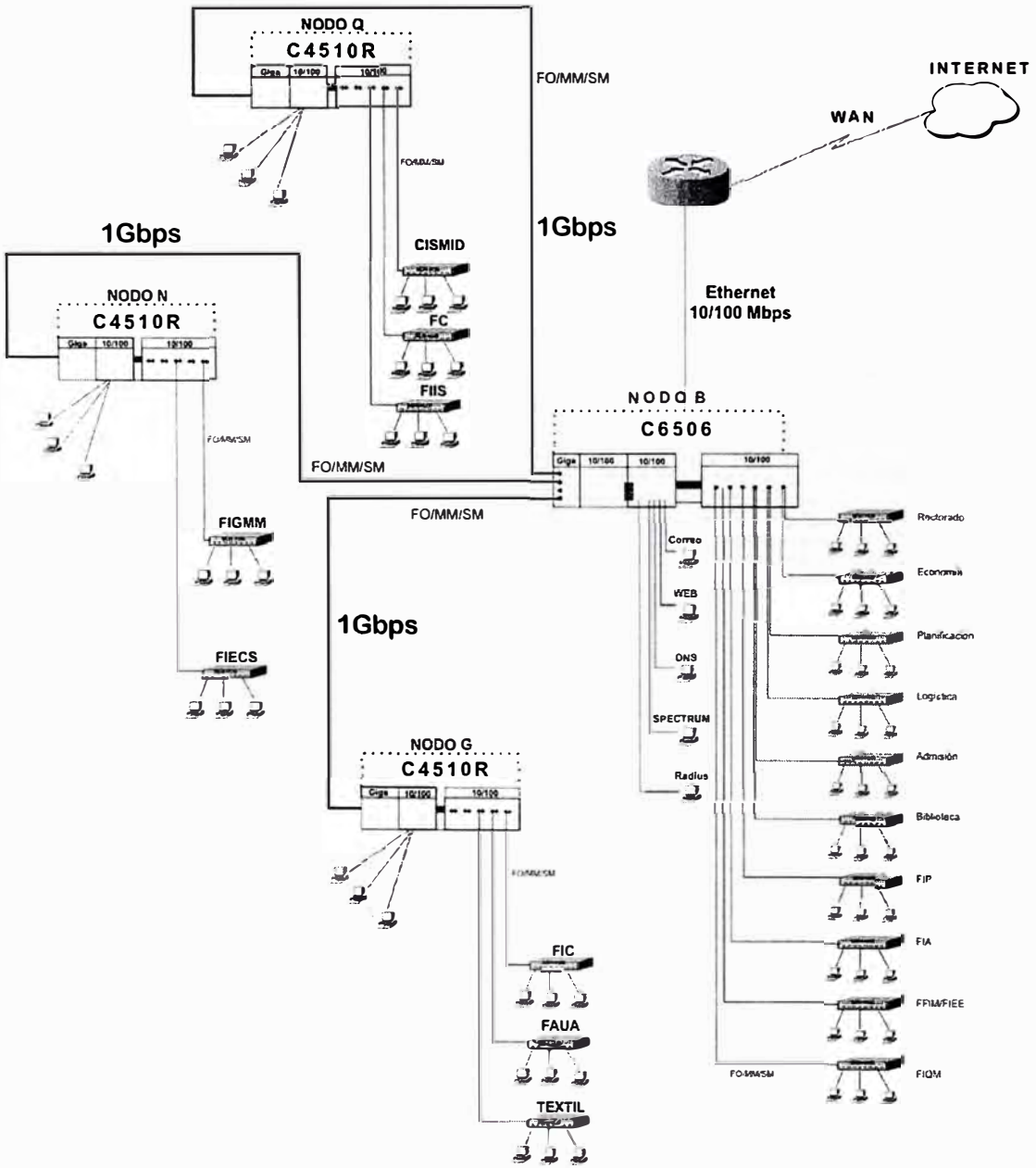


Figura 3 . 10 Representación de los componentes de cada nodo y su interconexión.

C6506: Cisco Catalyst 6506
C4510R: Cisco Catalyst 4500
FC: Facultad de Ciencias (Sector R)
FIIS: Facultad de Ing. Industrial Y sistemas (Sector S)
CISMID: Centro de Investigacion Sismicas y mitigacion de desastres. (Sectot T)
FO-MM/SM: Enlace de fibra OpticaMultimodo (MM) monomodo(SM)

3.4. Características de los equipos de comunicación

3.4.1. Descripción de los switch empleados en el caso de estudio

En la Figura 3.11 se muestra las características de los switchs empleados en el presente estudio.

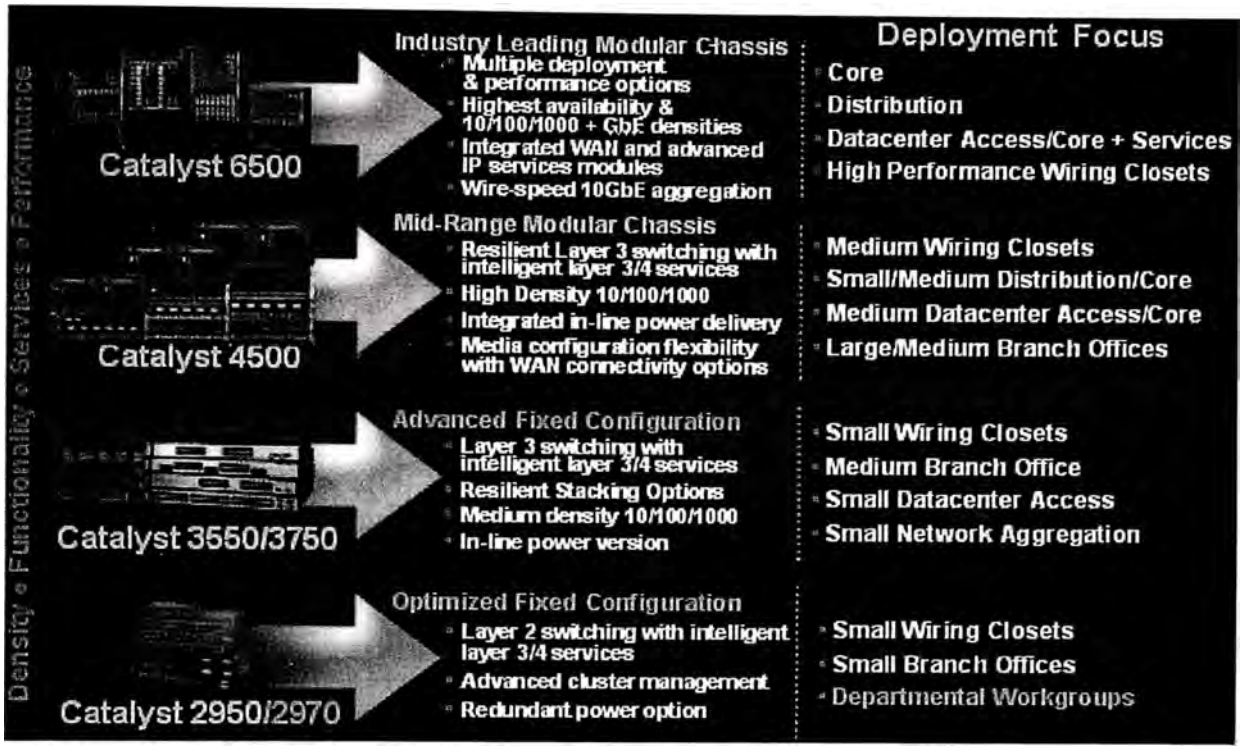


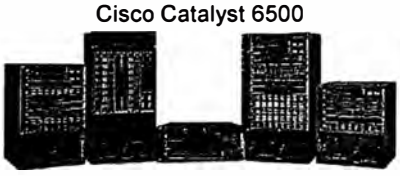
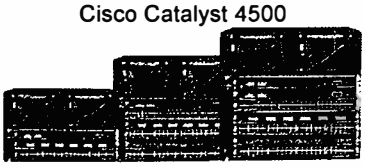
Figura 3 . 11 Switchs empleados en el caso de estudio.

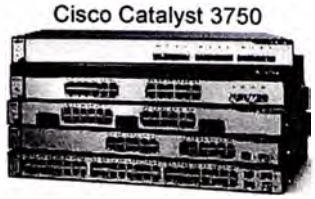
3.4.2. Tabla de resumen de características de los switchs

La Tabla 4.16 muestra aspectos fundamentales de los switchs usados en la red.

Tabla 4 . 1

Aspectos fundamentales de cada tipo de switch usado en la red.

SWITCH	MODELO DE SWITCH	CARACTERÍSTICAS
Cisco Catalyst 6500 	Catalyst 6506	Series switch fabric modules (SFM), including the Switch Fabric Module 2 (WS-X6500-SFM2), in combination with the Supervisor Engine 2, deliver an increase in available system bandwidth from the existing 32 Gbps to 256 Gbps. Architecture that allows 30 million packets per second (Mpps) of Cisco Express Forwarding-based central forwarding performance on Supervisor Engine 2 and up to 210 Mpps of distributed forwarding performance. 32 Gbps to 256 Gbps
Cisco Catalyst 4500 	Catalyst 4510R	96-Gbps capacity backplane Provides enough capacity to forward wire-rate, nonblocking 72 Mpps and supports up to 8 interface modules Nonblocking high density application

SWITCH	MODELO DE SWITCH	CARACTERÍSTICAS
Cisco Catalyst 3750 	WS-C3750G-24TS-E	24 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports 32-Gbps, high-speed stacking bus Innovative stacking technology 1.5-rack unit (RU) stackable, multilayer switch Enterprise-class intelligent services delivered to the network edge IP Services Image installed Full dynamic IP routing
Cisco Catalyst 2900 	Catalyst 2950SX-24	8.8-Gbps maximum forwarding bandwidth 6.6-Mpps wire-speed forwarding rate 24 10/100 ports with 2 fixed 1000BASE-SX uplinks 1 RU standalone, fixed-configuration, managed 10/100 switch SI Software

La Tabla 3.2 muestra características del switch Cisco serie C6500.

Tabla 3 . 2

Características del switch Cisco serie C6500

	Part Number	Description	Deployment	Minimum Software		
				Catalyst OS	Hybrid	Cisco IOS Software
Chassis	WS-C6504-E	4-slot E-Series chassis (1271W/ power supply)	Wiring closet branch, Internet edge, small collapsed core/ distribution, and server connectivity	8.4(2)	12.2(17d) SXB7	12.2(18) SXE1
	WS-C6506-E	6-slot E-Series chassis (1300W/ power supply for data only and 6000W for PoE)	Wiring closet branch, Internet edge, small collapsed core/ distribution, and server connectivity	• 5.4(2) • 8.4(1) for 6000 W power supply	12.2(14) SX2	12.2(14) SX
	WS-C6509-E	9-slot E-Series chassis (1300W/ power supply for data only and 6000W for PoE)	High-performance core, distribution, data center, collapsed core/distribution, and server connectivity	• 5.4(2) • 8.4(1) for 6000 W power supply	12.2(14) SX2	12.2(14) SX
Catalyst Supervisor Engines	WS-SUP32-GE-3B	Supervisor Engine 32 with eight GE SFP uplinks	Wiring closet branch or collapsed core/distribution and server connectivity	8.4(1)	12.2(17d) SXB7	12.2(18) SXF
	WS-SUP32-10GE-3B	Supervisor Engine 32 with two 10 GE Xenpak	Wiring closet or collapsed core/distribution and server connectivity	8.4(4)	12.2(17d) SXB7	12.2(18) SXF
	WS-SUP720-3B	Supervisor Engine 720 with two GE SFP uplinks, integrated 720-Gbps switch fabric	High-performance core, distribution, or data center	8.3(7)	12.2(17d) SXB1	12.2(17d) SXB1
Gigabit Ethernet (GE)	WS-X6408A-GBIC	8-port GE GBIC line card	Low-density GE fiber connectivity	5.3(1a) CSX	12.2(14) SX2	12.2(14) SX
	WS-X6724-SFP	24-port GE SFP line card (requires Supervisor Engine 720)	High-performance and medium-density GE fiber connectivity	8.1(2)	12.2(14) SX2	12.2(17a) SX
	WS-X6748-SFP	48-port GE SFP line card (requires Supervisor Engine 720)	High-performance and high-density GE fiber connectivity	8.3(2)	12.2(14) SX2	12.2(17d) SXB
10/100/1000 Ethernet	WS-X6148A-GE-45AF	48-port 10/100/1000 RJ-45 with PoE 802.3af, TDR, and Jumbo Frame support	Wiring closet requiring PoE	8.4(1)	12.2(17d) SXB7	12.2(18) SXF*
	WS-X6148A-GE-TX	48-port 10/100/1000 RJ-45 with TDR and Jumbo Frame support (upgradable to PoE)	Wiring closet, low-density server aggregation	8.4(1)	12.2(17d) SXB7	12.2(18) SXF*
	WS-X6748-GE-TX	48-port 10/100/1000 RJ-45 high-performance GE-TX (requires Cisco Supervisor Engine 720)	High-performance data center access and server connectivity	8.1(2)	12.2(14) SX2	12.2(17a) SX
10/100 Ethernet	WS-X6148A-45AF	48-port 10/100 RJ-45 with PoE 802.3af and TDR support	Wiring closet requiring PoE	8.4(1)	12.2(17d) SXB7	12.2(18) SXF*
	WS-X6196-21AF	96-port 10/100 RJ-21 with PoE 802.3af	High-density wiring closet requiring PoE	8.4(1)	12.2(17d) SXB7	12.2(18) SXF*
10 Gigabit Ethernet	WS-X6704-10GE	4-port high-performance 10 GE line card	High-performance and high-density 10 GE connectivity	8.1(2)	12.2(17a) SX1	12.2(17a) SX
Service Modules	WS-X6[illegible]-SLB-S-K9	High-performance server load balancing module with integrated SSL fare-ionality	Data center	—	—	12.2(18) SXE with CSM5.1.1.3
	WS-SVC-FWM-1-K9	High-performance firewall module with integrated virtual-secure fare-ionality	Branch, Internet edge, data center distribution	7.5(1)	12.2(17d) SXB7	12.2(18) SXE1
Bundles	WS-C6506E-S32-GE	Includes Supervisor Engine 32 with eight GE SFP uplinks and 6-slot chassis at a US$15000 discount	Wiring closet branch, Internet edge, small collapsed core/ distribution, and server connectivity	8.4(4)	12.2(17d) SXB7	12.2(18) SXF

Desde la Tabla 3.3 a la Tabla 3.6 se muestran características del switch Cisco serie C4500.

Tabla 3 . 3

Supervisor Engines	Feature Description
Entry-Level, Layer 2: Catalyst 4500 Supervisor II-Plus	• Scalable to 64 Gbps, 48 Mpps forwarding • Redundant capable 2xGE uplinks • 266 MHz CPU • Active VLAN Support (up to 2k) • Baseline security and QoS features: - IP Security filtering: 16k entries - Per port/VLAN Rate-limiting: 512 policies
High-End, Layer 2: Catalyst 4500 Supervisor II-Plus-10GE	• Scalable to 108 Gbps, 81 Mpps forwarding • Redundant capable 2x10GE and 4x1GE uplinks • 667 MHz CPU • Same Supervisor II-Plus features, but more: - Active VLAN Support (up to 4k) - Multicast and Broadcast Suppression
Entry-Level Layer 3: Catalyst 4500 Supervisor IV	• Scalable to 64 Gbps, 48 Mpps forwarding • Redundant capable 2xGE uplinks • 333 MHz CPU • Active VLAN Support (up to 4k) • Enhanced security and QoS Features: - IP Security filtering: 32k entries - Per port/VLAN Rate-limiting: 1024 policies - NetFlow support for traffic monitoring

Tabla 3 . 4

	96-Port 10/100 Data Only	144-Port 10/100 Data Only	High Density 10/100 244-388 Port Data Only
Single Supervisor Engine	• WS-C4503 • 2xWS-X4148-RJ • 2xPWR-C45-1000AC • WS-X4013+-TS	• WS-C4506 • 3xWS-X4148-RJ • 2xPWR-C45-1000AC • WS-X4515	• WS-C4510R • 5-7xWS-X4148-RJ • 2xPWR-C45-1400AC • WS-X4516-10GE
Redundant Supervisor Engines	• WS-C4507R • 2xWS-X4148-RJ • 2xPWR-C45-1000AC • 2xWS-X4013+	• WS-C4507R • 3xWS-X4148-RJ • 2xPWR-C45-1000AC • 2xWS-X4515	• WS-C4510R • 5-7xWS-X4148-RJ • 2xPWR-C45-1400AC • 2xWS-X4516-10GE
Benefits	Resiliency and longevity for a small premium over a high-end stackable.	Use WS-X4013+10GE when additional bandwidth is required in a L2 network.	Simplicity: All 388 ports receive feature consistency using the Supervisor Engine.

Tabla 3 . 5

	802.3af Class-2 Devices (7 Watts)	802.3af Class 0 and 3 Devices (15.4 Watts)
1300 Watt AC (PWR-C45-1300ACV) Requires a 15A Circuit at Minimum	102	46
2800 Watt AC (PWR-C45-2800ACV) Requires a 20A Circuit at Minimum	178	80
4200 Watt AC (PWR-C45-4200ACV) Requires 15A Circuit at Minimum	• 384 PDs @ 200V • 241 PDs @ 100V	• 222 PDs @ 200V • 109 PDs @ 100V

Tabla 3 . 6

Catalyst 4500 802.3af Linecards	Description
WS-X4548-GB-RJ45V	Catalyst 4500 PoE 802.3af 10/100/1000, 48-Ports (RJ45)
WS-X4524-GB-RJ45V	Catalyst 4500 PoE 802.3af 10/100/1000 24-Ports (RJ45)
WS-X4506-GB-T	Catalyst 4500 6-Port 10/100/1000 PoE or SFP (optional)
WS-X4248-RJ45V or WS-X4248-RJ21V	Catalyst 4500 PoE 802.3af 10/100, 48-Ports (RJ-45 or RJ-21)
WS-X4224-RJ45V	Catalyst 4500 10/100 PoE 802.3af 24-Ports (RJ45)

En la Tabla 3.7 se muestran características del switch Cisco serie C3750.

Tabla 3 . 7

Características del switch Cisco serie C3750.

Feature	Description
Cisco Catalyst 3750E-24TD	24 Ethernet 10/100/1000 ports and 2 X2 10 Gigabit Ethernet uplinks
Cisco Catalyst 3750E-24PD	24 Ethernet 10/100/1000 ports with PoE and 2 X2 10 Gigabit Ethernet uplinks
Cisco Catalyst 3750E-48TD	48 Ethernet 10/100/1000 ports and 2 X2 10 Gigabit Ethernet uplinks
Cisco Catalyst 3750E-48PD	48 Ethernet 10/100/1000 ports with PoE and 2 X2 10 Gigabit Ethernet uplinks
Cisco Catalyst 3750E-48PD-F	48 Ethernet 10/100/1000 ports with 15.4 watts PoE on all 48 ports and 2 X2 10 Gigabit Ethernet uplinks

CAPÍTULO IV
PLAN DE NUMERACIÓN DE IPv6

4.1. Análisis de requerimientos de direcciones IP

Luego de realizar una evaluación de las necesidades de acceso a la red por cada nodo se ha elaborado la Tabla 4.1 que resume estas necesidades.

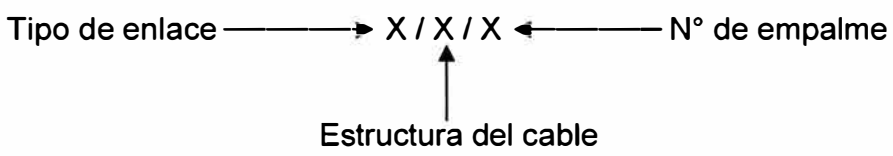
Tabla 4 . 1

Tabla de Enlaces

	Enlace	12MM/6SM	6MM/6SM	INT 4MM	Empalmes		Descripción
		A	B	C	N°	ROTULADO	
1	B1-N	794			24	B1-N / A / 01.....24	CETEL-Centro de Computo
2	B1-Q	1005			24	B1-Q / A / 01...24	CETEL-FIEE
3	B1-G5	410			24	B1-G5 / A / 01...24	CETEL-FIC
4	B1-A			69	8	B1-A / C / 01...8	CETEL-1° Piso Pabellón Central
5	B1-B			76	8	B1-B / C / 01...8	CETEL-2° Piso Pabellón Central
6	B1-C			57	8	B1-C / C / 01...8	CETEL-3° Piso Pabellón Central
7	B1-Biblioteca			75	8	B1-BB / C / 01...8	CETEL-Biblioteca Central(BB)
8	B1-Cabina			70	8	B1-Cab / C / 01...8	CETEL-Cabina (CAB)
9	B1-A2		231		12	B1-A2 / B / 01 ... 12	CETEL-FIM
10	A2-A1		198		12	A2-A1 / B / 01 ... 12	FIM - Postgrado FIM
11	B1-A3		373		12	B1-A3 / B / 01 ... 12	CETEL-Electrónica
12	B1-B2		395		12	B1-B2 / B / 01 ... 12	CETEL-Teatro
13	B1-C1		222		12	B1-C1 / B / 01 ... 12	CETEL-FIQT
14	B1-D1		222		12	B1-D1 / B / 01 ... 12	CETEL-FIA
15	B1-D2		245		12	B1-D2 / B / 01 ... 12	CETEL-FIP
16	N-K		172		12	N-K / B / 01 ... 12	Centro de Computo-LNH
17	N-M2		350		12	N-M2 / B / 01 ... 12	Centro de Computo-FIECS
18	N-M1		346		12	N-M1 / B / 01 ... 12	Centro de Computo-Centro Medico
19	N-J2		294		12	N-J2 / B / 01 ... 12	Centro de Computo-Topografía
20	Q-R		522		12	Q-R / B / 01 ... 12	FIEE-FC

	Enlace	12MM/6SM	6MM/6SM	INT 4MM	Empalmes		Descripción
		A	B	C	N°	ROTULADO	
21	Q-S		289		12	Q-S / B / 01 ... 12	FIEE-FIIS
22	Q-T1		709		12	Q-T1 / B / 01 ... 12	FIEE-CISMID
23	G5-E		253		12	G5-E / B / 01 ... 12	FCI-IECOS
24	G5-F		368		12	G5-F / B / 01 ... 12	FIC-FAUA
25	G5-G2		151		12	G5-G2 / B / 01 ... 12	FIC-Centro Computo FIC
26	G5-H		163		12	G5-H / B / 01 ... 12	FCI-Textil
27	G5-I4		504		12	G5-I4 / B / 01 ... 12	FIC-FIGMM
28	G5-J1		178		12	G5-J1 / B / 01 ... 12	FIC-Infraestructuras
29	I4-EXING		230		12	I4-EX / B / 01 ... 12	FIGMM-ExIngemet (EX)

Para el codificado del rotulado de empalmes se ha considerado el siguiente formato:



4.2. Diagrama arquitectónico de la red

Diagrama de la Topología en Fibra Óptica de la Red Lan, que consta de los siguientes Nodos de Núcleo, Distribución y Acceso.

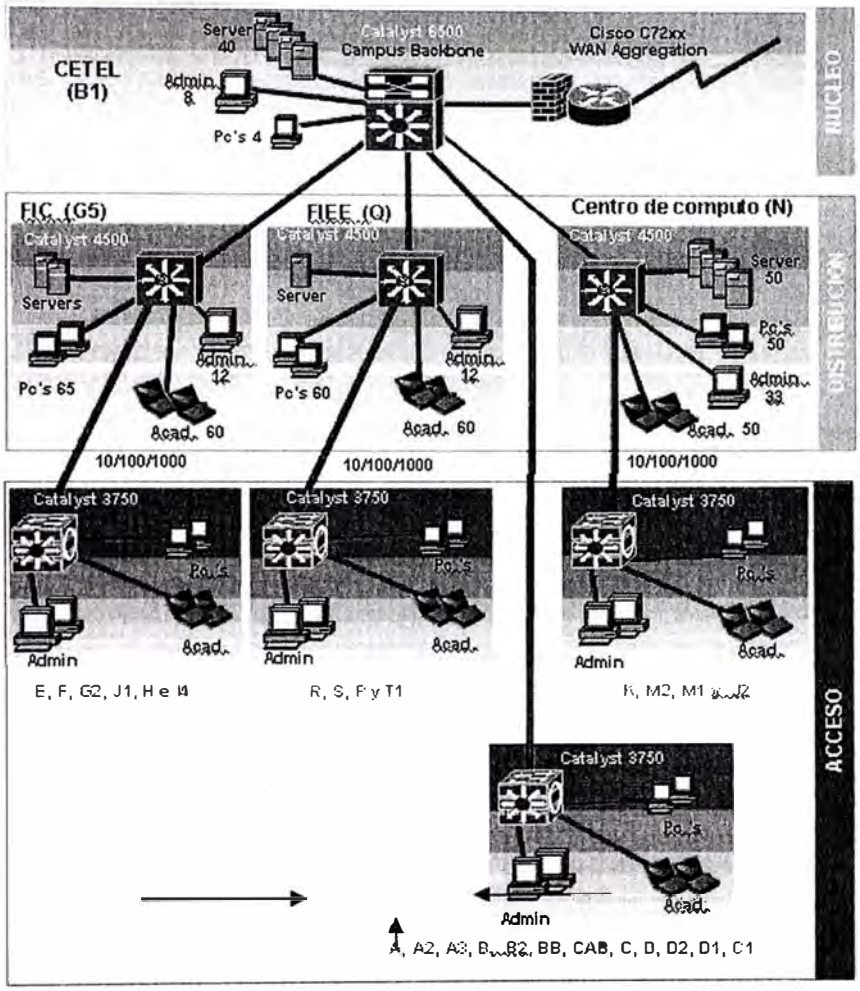


Figura 4 . 1 Diagrama Arquitectónico de la Red

4.3. Diagrama de enlaces de fibra óptica

Diagrama de la Topología en Fibra Óptica de la Red Lan, con empalmes y sus características:

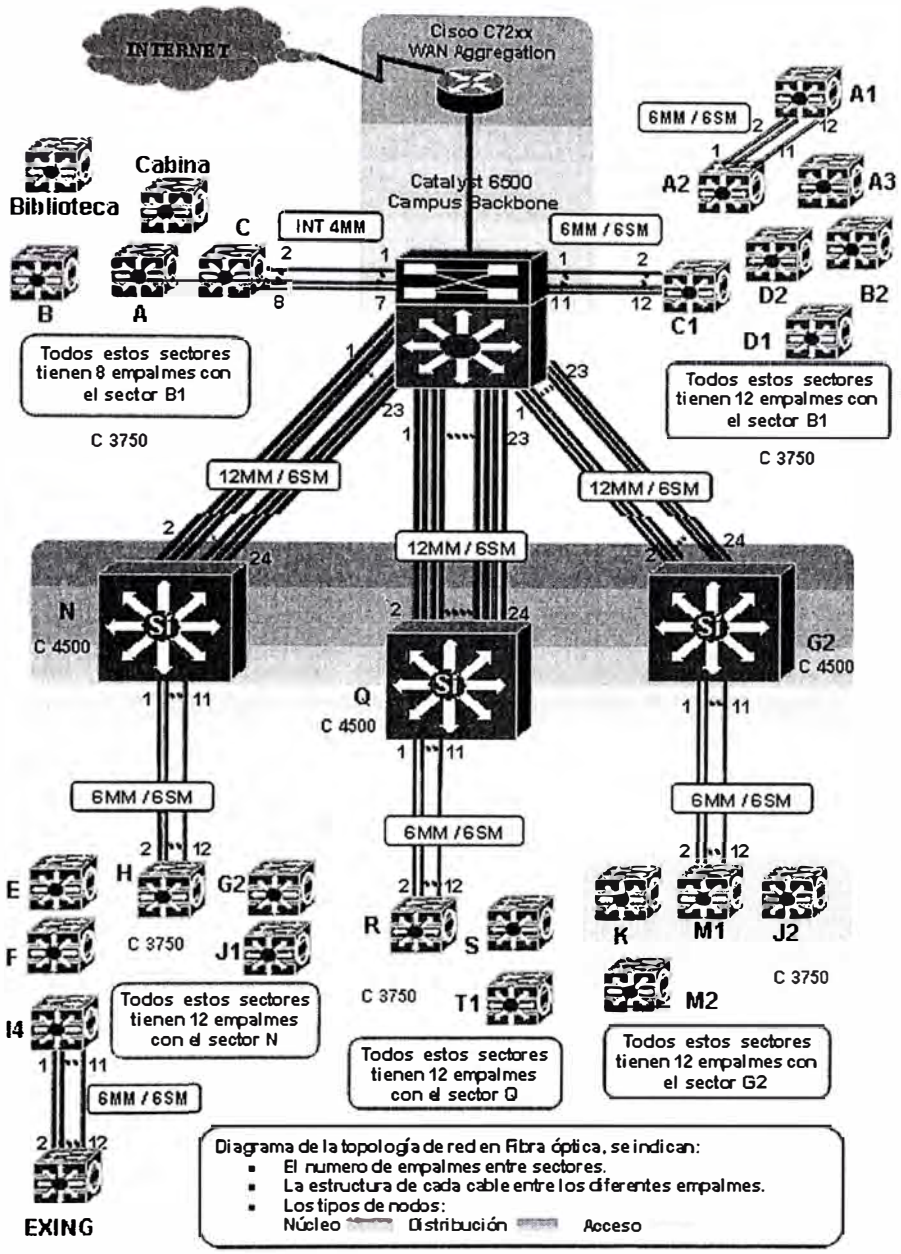


Figura 4 . 2 Diagrama de Enlaces de Fibra Óptica

4.4. Sistema de numeración de cableado estructurado

Sistema de numeración de Cableado Estructurado para cada una de los nodos.

Tabla 4 . 2

Rotulado de los Puntos de Conexión a la Red

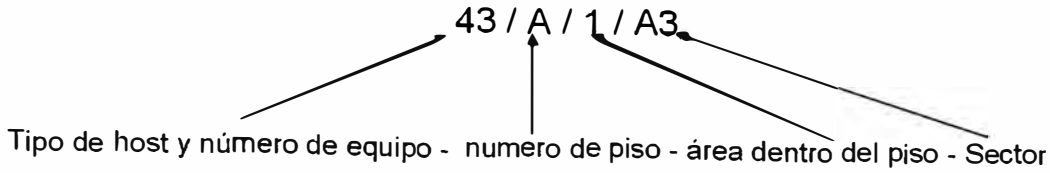
Enlace	Hosts Intranet (I)		Hosts Administrativos (Ad)		Hosts Servidores (S)		Hosts Académicos (Ac)		Descripción
B1	4	01/A/1/B1 .... 04/A/1/B1	8	201/A/1/B1 .... 208/A/1/B1	40	401/A/1/B1 .... 440/A/1/B1	-	----------	NOC de la Red
N	50	01/A//1/N 50/A/1/N	33	201/A/1/B1 .... 233/A//1/B1	50	401/A/1/N 450/A/1/N	6	601/A/1/N 601/A/1/N	Centro de Computo
Q	60	01/A/1/Q 50/A/1/Q	12	201/A/1/Q 212/A/1/Q	1	401/A/1/Q	60	601/A/1/Q 660/A/1/Q	FIEE
G5	65	01/A/1/G5 .... 50/A/1/G5	12	201/A/1/G5 .... 212/A/1/G5	2	401/A/1/G5 .... 402/A/1/G5	60	601/A/1/G5 .... 660/A/1/G5	FIC
A	12	01/A/1/A 12/A/1/A	34	201/A/1/A 234/A/1/A	-	----------	2	601/A/1/A 602/A/1/A	1° Piso Pabellón Central
B	33	01/B/1/B 33/B/1/B	45	201/B/1/B 245/B/1/B	-	----------	2	601/B/1/B 602/B/1/B	2° Piso Pabellón Central
C	34	01/C/1/C 33/C/1/C	43	201/C/1/C 243/C/1/C	-	----------	2	601/C/1/C 602/C/1/C	3° Piso Pabellón Central
Biblioteca (BB)	4	01/A/1/BB 04/A/1/BB	8	201/A/1/BB 204/A/1/BB	-	----------	120	601/A/1/BB 720/A/1/BB	Biblioteca Central
Cabina (cab)	80	01/B/1/CAB 80/B/1/CAB	-	----------	-	----------	-	----------	Cabina
A2	56	01/B/1/a2 .... 56/B/1/a2	12	201/A/1/A2 .... 212/A/1/A2	-	----------	60	601/A/1/A2 .... 660/A/1/A2	FIM
A1	34	01/B/1/A1 .... 34/B/1/A1	12	201/A/1/A1 .... 212/A/1/A1	-	----------	60	601/A/1/A1 .... 660/A/1/A1	Postgrado FIM
A3	43	01/B/1/A3 .... 43/B/1/A3	12	201/A/1/A3 .... 212/A/1/A3	-	----------	60	601/A/1/A3 .... 660/A/1/A3	Electrónica
B2	12	01/B/1/CAB 80/B/1/CAB	12	201/A/1/B2 .... 212/A/1/B2	-	----------	-	----------	Teatro
C1	67	01/B/1/CAB 80/B/1/CAB	12	201/A/1/C 212/A/1/C	-	----------	60	601/A/1/C 660/A/1/C	FIQT
D1	78	01/B/1/CAB 80/B/1/CAB	12	201/A/1/D1 .... 212/A/1/D1	-	----------	60	601/A/1/D1 .... 660/A/1/D1	FIA
D2	76	01/B/1/CAB 80/B/1/CAB	12	201/A/1/D2 .... 212/A/1/D2	-	----------	60	601/A/1/ D2 .... 660/A/1/D2	FIP

Enlace	Hosts Intranet (I)		Hosts Administrativos (Ad)		Hosts Servidores (S)		Hosts Académicos (Ac)		Descripción
K	20	01/B/1/CAB 80/B/1/CAB	12	201/A/1/K 212/A/1/K	-	———	30	601/A/1/K 630/A/1/K	LNH
M2	23	01/B/1/CAB 80/B/1/CAB	12	201/A/1/M2 .... 212/A/1/M2	-	———	60	601/A/1/M2 .... 660/A/1/M2	FIECS
M1	22	01/B/1/CAB 80/B/1/CAB	30	201/A/1/M1 .... 230/A/1/M1	-	----------	-	----------	Centro Medico
J2	12	01/B/1/CAB 80/B/1/CAB	0	----------	-	----------	30	601/A/1/J2 .... 630/A/1/J2	Topografia
R	78	01/B/1/CAB 80/B/1/CAB	12	201/A/1/R 212/A/1/R	-	----------	60	601/A/1/R 660/A/1/R	FC
S	130	01/B/1/CAB 80/B/1/CAB	12	201/A/1/S 212/A/1/S	-	----------	80	601/A/1/S 660/A/1/S	FIIS
T1	45	01/B/1/CAB 80/B/1/CAB	12	201/A/1/T1 .... 212/A/1/T1	-	———	60	601/A/1/T1 .... 660/A/1/T1	CISMID
E	34	01/B/1/CAB 80/B/1/CAB	12	201/A/1/E 212/A/1/E	-	----------	60	601/A/1/E 660/A/1/E	IECOS
F	45	01/B/1/CAB 80/B/1/CAB	12	201/A/1/F 212/A/1/F	-	----------	60	601/A/1/F 660/A/1/F	FAUA
G2	40	01/B/1/CAB 80/B/1/CAB	12	201/A/1/G2 .... 212/A/1/G2	-	----------	60	601/A/1/G2 .... 660/A/1/G2	Centro ComputoFIC
H	24	01/B/1/CAB 80/B/1/CAB	12	201/A/1/H 212/A/1/H	-	----------	60	601/A/1/H 660/A/1/H	Textiles
I4	44	01/B/1/CAB 80/B/1/CAB	12	201/A/1/I4 .... 212/A/1/I4	-	----------	60	601/A/1/I4 .... 660/A/1/I4	FIGMM
J1	50	01/B/1/CAB 50/B/1/CAB	12	201/A/1/J1 .... 212/A/1/J1	-	----------	20	601/A/1/J1 .... 620/A/1/J1	Infraestructuras
EXING (EX)	14	01/B/1/CAB 80/B/1/CAB	12	201/A/1/EX 212/A/1/EX	-	----------	40	601/A/1/EX 640/A/1/EX	ExIngemet

Para la codificación de cada uno de los nodos se ha considerado, el tipo de host y número de equipo, numero de piso, área dentro del piso y sector.

Tipo de host y número de equipo	Número de piso	Área dentro del piso	Sector
Hosts Intranet = 0 ~200	A = 1° piso		B1 = CETEL
Hosts Administrativos = 201 ~ 400	B = 2° piso		A3 = ELECTRONICA
Hosts Servidores = 401 ~ 600	C = 3° piso		S = FIIS
Hosts Académicos = 601 ~ 800	D = 4° piso		(VER TABLA)

Por ejemplo:



Para la identificación de una roseta como la identificada, se tiene:

- El equipo número 43 de la Intranet.
- En el primer piso.
- Del sector A3 ("electrónica").

4.5. Sistema de numeración de la red

La migración será realizada teniendo en cuenta la doble pila IPv4 e IPv6, siendo necesario por tanto un esquema de direccionamiento IPv4 y un esquema de direccionamiento IPv6.

4.5.1. Clasificación funcional de la red

Sistema de numeración de Red para las diferentes áreas de red lógica como se define a continuación:

Tabla 4 . 3

Estaciones por cada grupo funcional.

Red	Número de host necesarios	Total de ip's de los host por sumatoria de subredes	Número total de ip's por opción de redondeo	Dirección de red	Descripción
Net C (Red se servidores)	4 Subredes con 93 host	4 subredes con 136 ip's			
Net A (Red Intranet)	30 Subredes con 1289 host	30 subredes con 2064 ip's			
Net D (Red Académica)	26 Subredes con 1292 host	26 subredes con 1460 ip's			
Net B (Red Administrativa)	28 Subredes con 453 host	28 subredes con 656 ip's			
Red de equipos de comunicación	31 switch y 4 host de gestión				

La Tabla 4.3 muestra el número de direcciones IP por cada grupo funcional, en este caso como se tiene cierta cantidad de direcciones sin emplear se pueden asignar en forma proporcional a cada sector o área para un futuro crecimiento.

4.5.2. Esquema de direccionamiento IPv4

La red a usarse será: 172.23.0.0/16

Tabla 4 . 4

Distribución global de IP's según grupos funcionales.

Red		Subnets (4096 IP's)	Subnets (2048 IP's)	Subnets (1024 IP's)	Descripción
	0	172.23.16.0/20			No empleada
	1	172.23.16.0./20			Net A (Red Intranet)
	2		172.23.32.0/21	172.23.40.0/22	Net D (Red Académica)
				172.23.40.0/22	Net B (Red Administrativa)
					No empleada
	3	172.23.48.0./20			No empleada
	4	172.23.64.0./20			No empleada
	.....				No empleada
	.....				No empleada
	15	172.23.240.0./20			No empleada

La Tabla 4.4 muestra la distribución global de IP's por cada grupo funcional.

4.5.3. Red de servidores (net C)

Utiliza direcciones IP públicas: 200.106.56.0/24

Tabla 4 . 5

Distribución de IP's para el grupo funcional Servidores.

Red	Subnets (64 IP's)	Subnets (8 IP's)	Descripción
200.106.56.0/24	299.106.56.0/26		CETEL
	200.106.56.64/26		Sector N
		200.106.56.128/29	FIEE
		200.106.56.136/29	FIC
		200.106.56.144/29	Disponible
		.....	.....
		200.106.56.184/29	Disponible
	200.106.56.192/26		Disponible

La Tabla 4.5 muestra la distribución de IP's para el grupo funcional Servidores.

4.5.4. Red intranet (net A)

Tabla 4 . 6

Distribución de IP's para el grupo funcional Intranet.

Red	Subnets (256 IP's)	Subnets (128 y 64 ip's)	Subnets (32, 16 y 8 IP's)	Sector	Nª de host	Redondeo	
172.23.16.0/20	172.23.16.0/24			S	130	256	256
		172.23.17.0/25		Cabina	80	128	256
		172.23.17.128/25		D1	78	128	
		172.23.18.0/25		R	78	128	256
		172.23.18.128/25		D2	76	128	
		172.23.19.0/25		C1	67	128	256
		172.23.19.128/25		G5	65	128	
		172.23.20.0/26		N	60	64	256
		172.23.20.64/26		A2	56	64	
		172.23.20.128/26		Q	50	64	
		172.23.20.192/26		J1	50	64	
		172.23.21.0/26		T1	45	64	256
		172.23.21.64/26		F	45	64	
		172.23.21.128/26		I4	44	64	
		172.23.21.192/26		A3	43	64	
		172.23.22.0/26		G2	40	64	256
		172.23.22.64/26		C	34	64	
		172.23.22.128/26		E	34	64	
		172.23.22.192/26		A1	34	64	
			172.23.23.0/26	B	33	64	256
			172.23.23.64/27	H	24	32	
			172.23.23.96/27	M2	23	32	
			172.23.23.128/27	M1	22	32	
			172.23.23.160/27	K	20	32	
			172.23.23.192/28	EXING	14	16	
			172.23.23.208/28	A	12	16	
			172.23.23.224/28	B2	12	16	
			172.23.23.240/28	J2	12	16	
			172.23.24.0/29	CETEL	4	8	256
			172.23.24.8/29	Biblioteca	4	8	
		No empleada		----------		16	
		No empleada		----------		32	
		No empleada		----------		64	
		No empleada		----------		128	
	La subredes desde 172.23.25.0 /24 hasta la subred 172.23.31.0/24 no se emplean						

La Tabla 4.6 muestra la distribución de IP's para el grupo funcional Intranet.

4.5.5. Red académica (net D)

La red a usarse será: 172.23.32.0/21.

Tabla 4 . 7

Distribución de IP's para el grupo funcional Académica.

Red	Subnets (256 IP's)	Subnets (128 y 64 ip's)	Subnets (32, 8 y 4 IP's)	Sector	Nº de host	Redondeo	
172.23.32.0/21		172.23.32.0/25		Biblioteca	120	128	128
		172.23.32.128/25		S	80	128	128
		172.23.33.0/26		Q	60	64	128
		172.23.33.64/26		G5	60	64	
		172.23.33.128/26		A2	60	64	128
		172.23.33.192/26		A1	60	64	
		172.23.34.0/26		A3	60	64	128
		172.23.34.64/26		C1	60	64	
		172.23.34.128/26		D1	60	64	128
		172.23.34.192/26		D2	60	64	
		172.23.35.0/26		M2	60	64	128
		172.23.35.64/26		R	60	64	
		172.23.35.128/26		T1	60	64	128
		172.23.35.192/26		E	60	64	
		172.23.36.0/26		F	60	64	128
		172.23.36.64/26		G2	60	64	
		172.23.36.128/26		H	60	64	128
		172.23.36.192/26		I4	60	64	
		172.23.37.0/26		EXING	40	64	128
		172.23.37.64/27		K	30	32	
		172.23.37.96/27		J2	30	32	
		172.23.38.0/27		J1	20	32	128
		No empleada		----------		32	
		No empleada		----------		32	
		172.23.38.96/29		N	6	8	
		No empleada		----------		8	
		172.23.38.112/30		A	2	4	
		172.23.38.116/30		B	2	4	
		172.23.38.120/30		C	2	4	
		No empleada		----------		4	
		No empleada					
		No empleada					

La Tabla 4.7 muestra la distribución de IP's para el grupo funcional Académica.

4.5.6. Red administrativa (net B)

La red a usarse será: 172.23.40.0/22.

Tabla 4 . 8

Distribución de IP's para el grupo funcional Administrativa.

Red	Subnets (256 IP's)	Subnets (64 y 32 ip's)	Subnets (16 IP's)	Sector	Nº de host	Redondeo	
172.23.40.0/22		172.23.40.0/26		B	45	64	64
		172.23.40.64/26		C	43	64	64
		172.23.40.128/26		A	34	64	64
		172.23.40.192/26		N	33	64	64
			172.23.41.0/27	M1	30	32	64
			172.23.41.32/28	C1	12	16	
			172.23.41.48/28	G5	12	16	
			172.23.41.64/28	Q	12	16	64
			172.23.41.80/28	A1	12	16	
			172.23.41.96/28	A2	12	16	
			172.23.41.112/28	A3	12	16	
			172.23.41.128/28	T1	12	16	64
			172.23.41.144/28	F	12	16	
			172.23.41.160/28	I4	12	16	
			172.23.41.176/28	J1	12	16	
			172.23.41.192/28	G2	12	16	64
			172.23.41.208/28	H	12	16	
			172.23.41.224/28	E	12	16	
			172.23.41.240/28	K	12	16	
			172.23.42.0/28	B2	12	16	64
			172.23.42.16/28	D1	12	16	
			172.23.42.32/28	D2	12	16	
			172.23.42.48/28	S	12	16	
			172.23.42.64/28	M2	12	16	64
			172.23.42.80/28	R	12	16	
			172.23.42.96/28	EXING	12	16	
			172.23.42.112/28	CETEL	8	16	
			172.23.42.128/28	BIBLIOTECA	8	16	64
		No empleada		----------		16	
		No empleada		----------		16	
		No empleada		----------		16	
		No empleada					

La Tabla 4.8 muestra la distribución de IP's para el grupo funcional Administrativa.

4.5.7. Distribución del sistema de numeración para los equipos de comunicación y 4 host de gestión

Considérese la subred: 172.23.240.0/24

Tabla 4 . 9

Distribución de IP's para los equipos de comunicación.

Ubicación	Código del switch	Dirección asignada	Descripción
B1	B1/C/SW1	172.23.240.2	CETEL
N	N/D/SW1	172.23.240.3	Centro de Computo
Q	Q/D/SW1	172.23.240.4	FIEE
G5	G5/D/SW1	172.23.240.5	FIC
A	A/A/SW1	172.23.240.6	1° Piso Pabellón Central
B	B/A/SW1	172.23.240.7	2° Piso Pabellón Central
C	C/A/SW1	172.23.240.8	3° Piso Pabellón Central
Biblioteca	BB/A/SW1	172.23.240.9	Biblioteca Central
Cabina	CAB/A/SW1	172.23.240.10	Cabina
A2	A2/A/SW1	172.23.240.11	FIM
A1	A1/A/SW1	172.23.240.12	Postgrado FIM
A3	A3/A/SW1	172.23.240.13	Electrónica
B2	B2/A/SW1	172.23.240.14	Teatro
C1	C1/A/SW1	172.23.240.15	FIQT
D1	D1/A/SW1	172.23.240.16	FIA
D2	D2/A/SW1	172.23.240.18	FIP
K	K/A/SW1	172.23.240.19	LNH
M2	M2/A/SW1	172.23.240.20	FIECS
M1	M1/A/SW1	172.23.240.21	Centro Medico
J2	J2/A/SW1	172.23.240.22	Topografía
R	R/A/SW1	172.23.240.23	FC
S	S/A/SW1	172.23.240.24	FIIS
T1	T1/A/SW1	172.23.240.25	CISMID
E	E/A/SW1	172.23.240.26	IECOS
F	F/A/SW1	172.23.240.27	FAUA
G2	G2/A/SW1	172.23.240.28	Centro Computo FIC
H	H/A/SW1	172.23.240.29	Textiles
I4	I4/A/SW1	172.23.240.30	FIGMM
J1	J1/A/SW1	172.23.240.31	Infraestructuras
EXING	EX/A/SW1	172.23.240.32	ExIngemet
HOST DE GESTION			

La Tabla 4.9 muestra la distribución de identificación de cada uno de los equipos de comunicación, su ubicación y la dirección IP asignada.

4.6. Distribución de hosts por ubicación, equipos y pertenencia funcional

4.6.1. IP's por grupo funcional

Tabla de Equipos de Comunicación asociadas a la densidad de hosts por área, o sector, la numeración respectiva y la cantidad de ellos por cada nodo, ya sea de Núcleo, Distribución y Acceso. Cada Switch tiene 24 Puertos10/100/1000 BaseTx y 2 Puertos de enlace o Trunking ya sea en fibra o UTP. Tabla a ser llenada durante el proceso de asignación de IP's.

Tabla 4 . 10

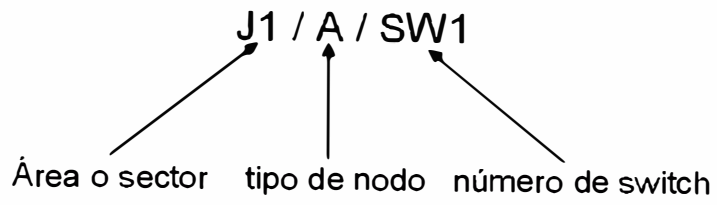
Tabla Resumen: Ubicación, Equipo y Grupo Funcional.

Ubicación	N° de equipos		Equipo/Puertos	Dirección de Red				Descripción
				Intranet	Académicos	Servidores	Administrativos	Codificación
B1	4	1	C6509					B1/C/SW1
		3	C2950SX-24					B1/A/SW2.....4
N	7	1	C4510R					N/D/SW1
		6	C2950SX-24					N/A/SW2.....SW7
Q	7	1	C4510R					Q/D/SW1
		6	C2950SX-24					Q/A/SW2.....SW7.
G5	7	1	C4510R					G5/D/SW1
		6	C2950SX-24					G5/A/SW2.....SW7
A	2	1	C3750G-24TS-E					A/A/SW1
		1	C2950SX-24					A/A/SW2
B	4	1	C3750G-24TS-E					B/A/SW1
		3	C2950SX-24					B/A/SW2....SW4
C	4	1	C3750G-24TS-E					C/A/SW1
		3	C2950SX-24					C/A/SW2....SW4
Biblioteca (BB)	6	1	C3750G-24TS-E					BB/A/SW1
		5	C2950SX-24					BB/A/SW2....SW4
Cabina (CAB)	4	1	C3750G-24TS-E					CAB/A/SW1
		3	C2950SX-24					CAB/A/SW2....SW4
A2	6	1	C3750G-24TS-E					A2/A/SW1
		5	C2950SX-24					A2/A/SW2....SW6
A1	5	1	C3750G-24TS-E					A1/A/SW1
		4	C2950SX-24					A1/A/SW2....SW5
A3	5	1	C3750G-24TS-E					A3/A/SW1
		4	C2950SX-24					A3/A/SW2....SW5
B2	2	1	C3750G-24TS-E					B2/A/SW1
C1	6	1	C3750G-24TS-E					C1/A/SW1
		5	C2950SX-24					C1/A/SW2....SW6
D1	7	1	C3750G-24TS-E					D1/A/SW1
		6	C2950SX-24					D1/A/SW2....SW7
D2	7	1	C3750G-24TS-E					C/A/SW1

Ubicación	N° de equipos		Equipo/Puertos	Dirección de Red				Descripción
				Intranet	Académicos	Servidores	Administrativos	Codificación
		6	C2950SX-24					C/A/SW2....SW7
K	3	1	C3750G-24TS-E					C/A/SW1
		2	C2950SX-24					C/A/SW2....SW3
M2	4	1	C3750G-24TS-E					C/A/SW1
		3	C2950SX-24					C/A/SW2....SW4
M1	4	1	C3750G-24TS-E					C/A/SW1
		3	C2950SX-24					C/A/SW2....SW4
J2	2	1	C3750G-24TS-E					J2/A/SW1
		1	C2950SX-24					C/A/SW2
R	7	1	C3750G-24TS-E					R/A/SW1
		6	C2950SX-24					R/A/SW2....SW7
S	10	1	C3750G-24TS-E					S/A/SW1
		9	C2950SX-24					S/A/SW2....SW9
T1	5	1	C3750G-24TS-E					T1/A/SW1
		4	C2950SX-24					T1/A/SW2....SW5
E	5	1	C3750G-24TS-E					E/A/SW1
		4	C2950SX-24					E/A/SW2....SW5
F	5	1	C3750G-24TS-E					F/A/SW1
		4	C2950SX-24					F/A/SW2....SW5
G2	5	1	C3750G-24TS-E					G2/A/SW1
		4	C2950SX-24					G2/A/SW2....SW5
H	4	1	C3750G-24TS-E					H/A/SW1
		3	C2950SX-24					H/A/SW2....SW4
I4	5	1	C3750G-24TS-E					I4/A/SW1
		4	C2950SX-24					I4/A/SW2....SW5
J1	4	1	C3750G-24TS-E					J1/A/SW1
		3	C2950SX-24					J1/A/SW2....SW4
EXING (EX)	3	1	C3750G-24TS-E					EX/A/SW1
		2	C2950SX-24					EX/A/SW2....SW3

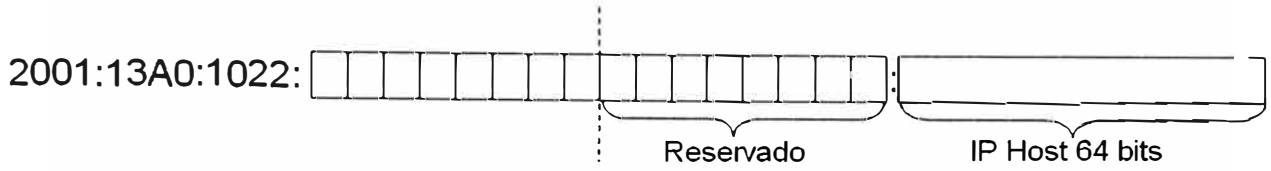
La Tabla 4.10 muestra el resumen sobre la ubicación, equipo y grupo funcional, se ha considerado abreviar los nodos como sigue: A = ACCESO, D = DISTRIBUCION y C = CORE (NUCLEO).

Para la codificación y rotulado de cada switch se ha considerado, el área o sector, el tipo de nodo, y el número de switch. Por ejemplo:



4.6.2. Esquema de direccionamiento en IPv6

El prefijo de red a usar será: 2001:13A0:1022:



Se designará un prefijo por cada subred considerada en la correspondiente subred IPv4.

a) Red de servidores (net C)

Tabla 4 . 11

Distribución Global de IP's versión 6 según grupo funcional Servidores.

Subnet	Sector	N° de host
2001:13A0:1022:0000::/56	CETEL	8
2001:13A0:1022:0100::/56	Sector N	8
2001:13A0:1022:0200::/56	FIEE	8
2001:13A0:1022:0300::/56	FIC	8

La Tabla 4.11 muestra la distribución global de direcciones IP's versión 6 según el grupo funcional Servidores.

b) Red intranet (net A)

Tabla 4 . 12

Distribución de IP's versión 6 para el grupo funcional Intranet

Subnet	Sector	N° de host
2001:13A0:1022:0400::/56	S	130
2001:13A0:1022:0500::/56	Cabina	80
2001:13A0:1022:0600::/56	D1	78
2001:13A0:1022:0700::/56	R	78
2001:13A0:1022:0800::/56	D2	76
2001:13A0:1022:0900::/56	C1	67
2001:13A0:1022:0A00::/56	G5	65
2001:13A0:1022:0B00::/56	N	60
2001:13A0:1022:0C00::/56	A2	56
2001:13A0:1022:0D00::/56	Q	50
2001:13A0:1022:0E00::/56	J1	50

Subnet	Sector	N° de host
2001:13A0:1022:0F00::/56	T1	45
2001:13A0:1022:1000::/56	F	45
2001:13A0:1022:1100::/56	I4	44
2001:13A0:1022:1200::/56	A3	43
2001:13A0:1022:1300::/56	G2	40
2001:13A0:1022:1400::/56	C	34
2001:13A0:1022:1500::/56	E	34
2001:13A0:1022:1600::/56	A1	34
2001:13A0:1022:1700::/56	B	33
2001:13A0:1022:1800::/56	H	24
2001:13A0:1022:1900::/56	M2	23
2001:13A0:1022:1A00::/56	M1	22
2001:13A0:1022:1B00::/56	K	20
2001:13A0:1022:1C00::/56	EXING	14
2001:13A0:1022:1D00::/56	A	12
2001:13A0:1022:1E00::/56	B2	12
2001:13A0:1022:1F00::/56	J2	12
2001:13A0:1022:2000::/56	CETEL	4
2001:13A0:1022:2100::/56	Biblioteca	4

La Tabla 4.12 muestra la distribución de direcciones IP's versión 6 según el grupo funcional Intranet.

c) Red académica (net D)

Tabla 4 . 13

Distribuciones de IP's versión 6 para el grupo funcional Académica.

Subnet	Sector	N° de host
2001:13A0:1022:2200::/56	Biblioteca	120
2001:13A0:1022:2300::/56	S	80
2001:13A0:1022:2400::/56	Q	60
2001:13A0:1022:2500::/56	G5	60
2001:13A0:1022:2600::/56	A2	60
2001:13A0:1022:2700::/56	A1	60
2001:13A0:1022:2800::/56	A3	60
2001:13A0:1022:2900::/56	C1	60
2001:13A0:1022:2A00::/56	D1	60
2001:13A0:1022:2B00::/56	D2	60
2001:13A0:1022:2C00::/56	M2	60
2001:13A0:1022:2D00::/56	R	60
2001:13A0:1022:2E00::/56	T1	60

2001:13A0:1022:2F00::/56	E	60
2001:13A0:1022:3000::/56	F	60
2001:13A0:1022:3100::/56	G2	60
2001:13A0:1022:3200::/56	H	60
2001:13A0:1022:3300::/56	I4	60
2001:13A0:1022:3400::/56	EXING	40
2001:13A0:1022:3500::/56	K	30
2001:13A0:1022:3600::/56	J2	30
2001:13A0:1022:3700::/56	J1	20
2001:13A0:1022:3800::/56	N	6
2001:13A0:1022:3900::/56	A	2
2001:13A0:1022:3A00::/56	B	2
2001:13A0:1022:3B00::/56	C	2

La Tabla 4.13 muestra la distribución de direcciones IP's versión 6 según el grupo funcional Académica.

d) Red administrativa (net B)

Tabla 4 . 14

Distribución de IP's para el grupo funcional Administrativa.

Subnet	Sector	N° de host
2001:13A0:1022:3C00::/56	B	45
2001:13A0:1022:3D00::/56	C	43
2001:13A0:1022:3E00::/56	A	34
2001:13A0:1022:3F00::/56	N	33
2001:13A0:1022:4000::/56	M1	30
2001:13A0:1022:4100::/56	C1	12
2001:13A0:1022:4200::/56	G5	12
2001:13A0:1022:4300::/56	Q	12
2001:13A0:1022:4400::/56	A1	12
2001:13A0:1022:4500::/56	A2	12
2001:13A0:1022:4600::/56	A3	12
2001:13A0:1022:4700::/56	T1	12
2001:13A0:1022:4800::/56	F	12
2001:13A0:1022:4900::/56	I4	12
2001:13A0:1022:4A00::/56	J1	12
2001:13A0:1022:4B00::/56	G2	12
2001:13A0:1022:4C00::/56	H	12
2001:13A0:1022:4D00::/56	E	12
2001:13A0:1022:4E00::/56	K	12
2001:13A0:1022:4F00::/56	B2	12
2001:13A0:1022:5000::/56	D1	12

2001:13A0:1022:5100::/56	D2	12
2001:13A0:1022:5200::/56	S	12
2001:13A0:1022:5300::/56	M2	12
2001:13A0:1022:5400::/56	R	12
2001:13A0:1022:5500::/56	EXING	12
2001:13A0:1022:5600::/56	CETEL	8
2001:13A0:1022:6600::/56	BIBLIOTECA	8

La Tabla 4.14 muestra la distribución de direcciones IP's versión 6 según el grupo funcional Administrativa.

e) Distribución del sistema de numeración para los equipos de comunicación y host de gestión

Tabla 4 . 15

Distribución de IP's versión 6 para los equipos de comunicación.

Prefijo de Net	Ubicación	Código del switch	Descripción
2001:13A0:1022:6700::/56	B1	B1/C/SW1	Cetel
	N	N/D/SW1	Centro de Computo
	Q	Q/D/SW1	FIEE
	G5	G5/D/SW1	FIC
	A	A/A/SW1	1° Piso Pabellón Central
	B	B/A/SW1	2° Piso Pabellón Central
	C	C/A/SW1	3° Piso Pabellón Central
	Biblioteca	BB/A/SW1	Biblioteca Central
	Cabina	CAB/A/SW1	Cabina
	A2	A2/A/SW1	FIM
	A1	A1/A/SW1	Postgrado FIM
	A3	A3/A/SW1	Electrónica
	B2	B2/A/SW1	Teatro
	C1	C1/A/SW1	FIQT
	D1	D1/A/SW1	FIA
	D2	D2/A/SW1	FIP
	K	K/A/SW1	LNH
	M2	M2/A/SW1	FIECS
	M1	M1/A/SW1	Centro Medico
	J2	J2/A/SW1	Topografía
	R	R/A/SW1	FC
	S	S/A/SW1	FIIS
	T1	T1/A/SW1	CISMID
	E	E/A/SW1	IECOS
	F	F/A/SW1	FAUA

Prefijo de Net	Ubicación	Código del switch	Descripción
	G2	G2/A/SW1	Centro Computo FIC
	H	H/A/SW1	Textiles
	I4	I4/A/SW1	FIGMM
	J1	J1/A/SW1	Infraestructuras
	EXING	EX/A/SW1	ExIngemet

La Tabla 4.15 muestra la distribución de direcciones IP's versión 6 de los equipos de comunicación.

C A P Í T U L O V
IMPLEMENTACIÓN EN LOS SWITCH'S Y ROUTER

5.1. Estrategias de despliegue de IPv6

El continuo crecimiento de la Internet global requiere que su arquitectura completa evolucione para incluir las nuevas tecnologías que soporten el creciente número de usuarios, aplicaciones, dispositivos, y servicios.

IPv6 se diseño para satisfacer esos requerimientos y permitir un retorno al entorno global donde las reglas de direccionamiento de la red sean nuevamente transparentes a las aplicaciones.

El espacio de direcciones IP actuales es incapaz de satisfacer el incremento potencial en el número de usuarios o las necesidades de la expansión geográficas de Internet, y mucho menos los requerimientos de aplicaciones emergentes tales como Asistentes Digitales Personales habilitados para la Internet (PDAs), Redes de Área del Hogar (HANs), automóviles conectados a la Internet, servicios de telefonía integrada, juegos distribuidos.

IPv6 cuadruplica el número de bits de las direcciones de red de 32 bits (en IPv4) a 128 bits, el cual provee direcciones IP únicas globales más que suficiente para cada dispositivo de red sobre el planeta. El uso de direcciones IPv6 únicas globales simplifica los mecanismos usados para la alcanzabilidad y la seguridad de extremo a extremo para los dispositivos de red, funcionalidades que son cruciales para las aplicaciones y servicios que están conduciendo la demanda de direcciones.

El tiempo de vida de IPv4 ha sido extendido usando técnicas tales como reuso de direcciones con traducción y distribuciones de uso temporal. Aunque esas técnicas aparentan el incremento del espacio de direcciones y satisfacen la configuración cliente/servidor tradicional, ellos fallan para satisfacer los requerimientos de las nuevas aplicacones. La necesidad de entornos que sean permanentemente (tales como Internet residencial a través de banda ancha, cable model, o ethernet para el hogar) contactables excluye esa conversión de direcciones IP, pooling, y tecnicas de distribución temporal, y el "plug and play" requerido por los dispositivos consumidores de Internet incrementa mas el requerimiento de direcciones. La flexibilidad del espacio de direcciones IPv6 provee el soporte para direcciones privadas pero debe reducir el uso de "traducciones de

direcciones de red" (NAT) debido a que las direcciones globales son ampliamente disponibles. IPv6 reintroduce la seguridad y calidad de servicio de extremo a extremo (QoS) que no siempre están disponibles en una red basada en NAT.

Los organismos de estandarización para los servicios de datos inalámbricos están preparándose para el futuro, e IPv6 provee los requerimientos de direccionamiento de extremo a extremo para esos nuevos entornos como teléfonos móviles y puertas de acceso para voz sobre IP residenciales. IPv6 provee esos servicios, tales como autoconfiguración integrada, QoS, seguridad, e IP móvil de ruta directa, también requerido por esos entornos.

IPv6 provee los siguientes beneficios:

- Un espacio de direcciones más grande para la escalabilidad y alcanzabilidad global.
- Cabecera simplificada para el rendimiento y eficiencia de ruteo.
- Políticas y jerarquías amplias para la flexibilidad de la arquitectura de red.
- Soporte eficiente para el ruteo y agregación de rutas.
- Autoconfiguración sin servidor, renumeración mas fácil, multihoming, y soporte "plug and play" mejorado.
- Seguridad con soporte obligatorio de "IP Security" (IPSec) para todos los dispositivos IPv6.
- Soporte mejorado para IP móvil y dispositivos de computación móvil.
- Soporte multicast mejorado con direcciones incrementadas y mecanismos eficientes.

Estamos en las etapas iniciales del despliegue de IPv6, con las pocas aplicaciones IPv6 en el mercado y los primeros productos ruteadores necesitando realizar negociaciones entre los servicios IPv6 disponibles. El foco inicial de esos productos es la migración y técnicas de transición requeridos para el despliegue mas que satisfacer los requerimientos para altos niveles de trafico.

Aunque el éxito de IPv6 dependerá finalmente de la disponibilidad de aplicaciones que corren sobre IPv6, una parte clave del diseño IPv6 esta en su habilidad para integrarse y coexistir con las redes IPv4.

Se espera que los host IPv4/IPv6 necesitaran coexistir por un tiempo sustancial durante la fase de migración de IPv4 a IPv6, y el desarrollo de estrategias de transición, herramientas y mecanismos han sido parte del diseño básico de IPv6 desde el principio.

Cisco ha sido parte de esta actividad, participando en el desarrollo de técnicas de transición y estrategias de despliegue para sus productos que satisfacen un rango de clientes y requerimiento de red, si usted es un proveedor de servicios o cliente empresarial y si está planificando una prueba de despliegue o un despliegue en vivo en un entorno controlado. Su elección de una estrategia ó estrategias de despliegue dependerá de su entorno de red actual y factores tales como la cantidad de tráfico IPv6 y la disponibilidad de aplicaciones IPv6 en sus sistemas finales, y la preparación para el despliegue.

5.2. Planificando la estrategia de despliegue de IPv6

5.2.1. Introducción

Cisco favorece una estrategia de transición de IPv4 a IPv6 que empieza desde el borde de la red y se mueve hacia el núcleo. Esta estrategia permite controlar el costo de despliegue y centrarse en las necesidades de las aplicaciones, más que completar una actualización de red total hacia una red IPv6 nativa. Los productos ruteadores IPv6 de Cisco ofrecen las características para una estrategia de integración como esta. Las diferentes estrategias de despliegue permiten que la primera fase de la transición a IPv6 se de ya, aunque como una prueba controlada de las capacidades de IPv6 o como una fase inicial de implementaciones de redes IPv6 mayores.

Los escenarios contemplados para este proceso son:

Proveedor de Servicios

Empresarial

Nuestro escenario es el empresarial por que se trata de una red de campus.

5.2.2. Escenario empresarial

Como administrador u operador de red de una Red Empresarial (RE), se podría desear evaluar y probar IPv6 ahora debido a que se planea introducir aplicaciones IPv6 dentro de un futuro cercano. No se debe esperar que un gran número de aplicaciones IPv6 estén disponibles inicialmente, algunos de los ofrecimientos de IP móvil están siendo introducidos en el mercado ejecutándose y escalando mejor usando las características de "direct-path" que llegaran a estar disponibles en una infraestructura IPv6, mas que en aquellas disponibles con IPv4.

Se puede probar y evaluar IPv6 como el direccionamiento extremo a extremo, autoconfiguración integrada, QoS, y seguridad requerida por los nuevos entornos para teléfonos móviles, o se puede expandir el espacio de direcciones disponibles para algunos nuevos dispositivos tales como los sistemas de telefonía basado en IP.

Se puede retornar a un entorno donde las reglas de direccionamiento de la red sean mas transparentes a las aplicaciones, y reintroducir seguridad de extremo a extremo y calidad de servicio que nos están ahora disponibles a través de redes IPv4 que usan NAT, y otras técnicas de conversión de direcciones, pooling, y asignación temporal.

Dos formas claves de evaluar y probar productos y servicios IPv6 son las siguientes:

- Configurar un dominio IPv6 y conectarse a una red IPv6 remota existente tal como el 6bone.
- Configurar dos o más dominios IPv6 e interconectar estos a traves de una infraestructura IPv4 existente.

Las técnicas de transición IPv6 actuales soportados en el software IOS de Cisco permite la evaluación y prueba de los productos y aplicaciones IPv6 en los entornos descritos en una forma aislada e independiente tal que no halla una interrupción en las actividad actual del negocio.

5.3. Identificando requerimientos

Como operador o administrador de red de una red empresarial, deberia iniciar la elección de los servicios y aplicaciones IPv6 que debería ser ofrecido a través de IPv6, y decidir donde desea proveer esos servicios.

Las actividades entonces consistentes en la creación de un dominio IPv6 y la configuración de un DNS que soporte ambos registros IPv4 e IPv6, y si hubiese la necesidad de intercomunicación entre hosts IPv6 puro y host IPv4 puro, operando uno de los mecanismos de traducción protocolar tales como NAT-PT en el ruteador o un TCP-UDP relay.

Debería luego identificar el ruteador o ruteadores en la red que necesiten ser dual-stack. Ellos serán parte del dominio IPv6, usando protocolos de ruteo para comunicarse con las aplicaciones IPv6, y cada protocolo IPv4 o IPv6 para comunicarse fuera del dominio. El protocolo elegido dependerá si su red se conecta directamente a un proveedor de servicio IPv6, o usando una de las estrategias disponibles para transportar el trafico IPv6 a través de la infraestructura IPv4 disponible a una red o dominio IPv6. En ambos casos, solicitar las direcciones IPv6 del proveedor de servicio relevante.

5.4. Selección de la estrategia de despliegue

Las estrategias claves usadas en el despliegue IPv6 en el borde de la red involucra transportar tráfico a través de la red IPv4, permitiendo a dominios IPv6 aislados comunicarse con cada otro antes de la transición completa a un backbone IPv6 nativo. Es también posible correr IPv4 e IPv6 a través de la red, desde todo el borde hacia el núcleo, o traducir entre IPv4 e IPv6 para permitir a los hosts comunicación en un protocolo para comunicarse transparentemente con hosts corriendo el otro protocolo. Todas las técnicas

permiten que las redes se actualicen y desplieguen incrementalmente con una minima interrupción de los servicios IPv4.

Las cuatro estrategias claves para el despliegue IPv6 son como sigue:

- **Despliegue IPv6 sobre tuneles IPv4:** Estos túneles encapsulan el tráfico IPv6 en paquetes IPv4, y son principalmente para la comunicación entre sites IPv6 aislados o conexiones a redes IPv6 remotas sobre un backbone IPv4. Las técnicas incluyen el uso de túneles configurados manualmente, túneles de encapsulación de ruteo genérico (GRE), mecanismos de túneles semiautomáticos tales como el servicio mediador de túnel, y mecanismos de túnel completamente automáticos tales como IPv4-compatible y 6to4.
- **Despliegue IPv6 sobre enlaces de datos dedicados:** Esta técnica habilita a dominios IPv6 aislados a comunicarse mediante el uso de la misma infraestructura capa 2 similar a IPv4, pero con IPv6 usando independientemente Frame Relay o ATM PVC´s, enlaces ópticos independientes, o Multiplexión por división de onda densa (dWDM).
- **Despliegue IPv6 sobre backbone´s MPLS:** Esta técnica permite a los dominios IPv6 aislados comunicarse con otros, pero sobre un backbone MPLS IPv4. Múltiples técnicas están disponibles en diferentes puntos en la red, pero cada una requiere pequeños cambios para infraestructura backbone o reconfiguración de los ruteadores del núcleo debido a que el reenvío esta basado en etiquetas más que en la cabecera IP misma.
- **Desplegando IPv6 usando backbones dual-stack:** Esta técnica permite que aplicaciones IPv4 e IPv6 coexistan en una capa backbone de enrutamiento IP dual. Todos los ruteadores en la red requieren ser actualizados para ser dual stack, la comunicación IPv4 usa la pila de protocolos IPv4 y la comunicación IPv6 usa la pila de protocolos IPv6.

Adicionalmente a las estrategias para el despliegue de IPv6 en un entorno IPv4, también se necesita mecanismos de traducción de protocolo (por ejemplo, un dispositivo NAT-PT que utiliza únicamente a navegadores con IPv6 para conectarse a servidores WEB con únicamente IPv4) o dual stack servers (por ejemplo, un servidor de correo que maneja solamente IPv4 y clientes de correo con únicamente IPv6) para permitir la comunicación entre aplicaciones usando IPv4 y aplicaciones usando IPv6.

Estos mecanismos llegan a crecer en importancia a la par como el despliegue de IPv6 se mueva desde las pruebas a las fase real de uso, y más relevante cuando los desarrolladores de aplicaciones decidan que continuar con el soporte a IPv4 no es económico.

Eventualmente, conforme IPv6 llega a ser el protocolo elegido, esos mecanismos permitirán a los sistemas IPv4 heredados ser parte de la red IPv6. Los mecanismos de traducción entre los protocolos IPv4 e IPv6 en los sistemas finales, o en un servidor dedicado, o en un ruteador en la red IPv6, y, junto con los hosts dual-stack, provee un completo conjunto de herramientas para el despliegue incremental de IPv6 sin interrupción del trafico IPv4.

La estrategia de despliegue recomendada para un campus es usar backbones dual-stack.

5.5. Desplegando IPv6 usando backbones IPv6 dual stack

Usar backbones dual-stack es una estrategia básica para enrutar IPv4 e IPv6. Todos los ruteadores en la red requieren ser actualizados a dual-stack. Las comunicaciones IPv4 usa la pila de protocolo IPv4 (que reenvían paquetes IPv4 basados en rutas aprendidas por protocolos de ruteo específicos IPv4), y las comunicaciones IPv6 usan la pila de protocolo IPv6 con rutas IPv6 aprendidos a través de protocolos de ruteo IPv6 específicos.

Los requerimientos claves son que cada site tenga un prefijo IPv6 unicast global y entradas apropiadas en un DNS que relacione los nombres de host y las direcciones IP tanto para IPv4 e IPv6. Las aplicaciones eligen usar entre IPv4 o IPv6 sobre la base de la respuesta del DNS, las aplicaciones seleccionaran la dirección correcta basada en el tipo de tráfico IP y requerimientos particulares de comunicación.

En la actualidad, el ruteo dual-stack es una estrategia de despliegue valida para infraestructuras con mixtura de IPv4 e IPv6 (tal como un campus), requiriendo ser configurados ambos protocolos. Y debe ser configurado con suficiente memoria para las tablas de ruteo IPv4 e IPv6.

También, Cisco no recomienda una actualización completa de toda la red a dual-stack, hasta que haya una mejor paridad entre características y niveles de tráfico. Si bien IPV6 en el software IOS de Cisco soporta completamente dual-stack, la implementación actual de IPv6 requiere mejoras en varios servicios (por ejemplo, IPv6 multicast) antes de que cualquier red pueda ser actualizada a dual-stack.

5.6. Mecanismo de traducción de protocolos

Todas las estrategias de integración proveen IPv6 de extremo a extremo. La intercomunicación entre IPv4 e IPv6 requiere algunos niveles de traducción entre los protocolos IPv4 e Ipv6 en el host o ruteador, o hosts dual-stack, con un acuerdo del nivel de aplicación de cual protocolo usar.

Una variedad de mecanismo de traducción de protocolos está bajo consideración del IETF NGTrans Working Group, como los siguientes:

- Traducción Network Address Translation-Protocol (NAT-PT)

- TCP-UDP Relay
- Mecanismo de transición Dual Stack (DSTM)
- SOCKS-Based Gateway

Esos mecanismos de traducción protocolar llegan a ser más relevantes conforme IPv6 llega a ser mas frecuente, e incluso cuando IPv6 llegue a ser el protocolo de elección para permitir a los sistemas IPv4 heredados ser parte de las redes IPv6.

Los mecanismos tienden a caer en dos categorías, los que no requieren cambios en los hosts IPv4 o IPv6, y los que si requieren cambios. Un ejemplo del primero es el mecanismo TCP-UDP relay que se ejecuta sobre un servidor dedicado y configura conexiones separadas en el nivel de transporte en hosts IPv4 e IPv6, y entonces simplifica la transferencia de información entre los dos. Un ejemplo de este último es el mecanismo BIS que requiere capas protocolares extras a ser añadidos a la pila de protocolos IPv4.

Los mecanismos de traducción que permiten la comunicación entre hosts que usan únicamente IPv6 e IPv4, tal como NAT-PT o BIS, usa un algoritmo denominado Stateless IP/ICMP Translator (SIIT). Este mecanismo traduce, sobre una base de paquete por paquete, las cabeceras en el paquete IP entre IPv4 e IPv6, y traduce las direcciones en las cabeceras entre IPv4 y cada dirección Ipv4-traducida o direcciones IPv6 IPv4 mapeadas. El mecanismo asume que cada host IPv6 tiene una dirección Ipv4 temporalmente asignada a este. SIIT es soportado en IPv6 por los IOS Cisco como parte de la implementación NAT-PT.

5.6.1. NAT-PT

El mecanismo de traducción NAT-PT en la capa de red entre IPv4 e IPv6. Un Application Level Gateway (ALG) traduce entre las solicitudes y respuestas DNS IPv4 e IPv6.

El uso más grande es donde los nuevos hosts corren IPv6 únicamente o la red no implementa el acceso dual-stack de IPv6 para el IOS Cisco. Este tiene los mismos beneficios de NAT para IPv4, y podría ser más fácil introducir IPv6 inicialmente debido a esta familiaridad y experiencia. Sin embargo NAT-PT también hereda las mismas limitaciones que NAT para IPv4, y hace dificultoso el re-ruteo rápido (ALGs no son tan rápidos como los ruteadores IP). También, los servidores dedicados tienen un único punto de falla en la red. Aunque permiten seguridad en la capa de aplicación, NAT-PT impide la seguridad de red de extremo a extremo, y hace extremadamente más dificultoso la unión de redes con direcciones IP privadas.

Cisco planea soportar NAT-PT en la fase II de IPv6 para el IOS Cisco.

5.6.2. TCP-UDP Relay

El mecanismo TCP-UDP Relay es similar a NAT-PT en que requieren servidor dedicado y DNS, pero traduce en la capa de transporte más que en la capa de red, con el DNS nuevamente proporcionando la relación entre las direcciones IPv4 e IPv6.

Cuando el servidor TCP relay recibe una solicitud, establece una conexión separada en el nivel de transporte con los hosts origen y el destino IPv4 e IPv6, y luego simplifica la transferencia de datos de una conexión a otra. UDP relay trabaja en forma similar.

El mayor uso de este mecanismo es para redes IPv6 nativas que quieren accede a hosts con IPv4 solamente, tales como servidores IPv4, pero sin el gasto de actualizar cada lado a IPv6 o IPv4. El mecanismo Relay soporta trafico bidireccional (multicast no es soportado), pero como con NAT-PT, permite seguridad en el nivel de aplicación pero impide seguridad de red extremo a extremo. El re-ruteo rápido es dificultoso, y los servidores dedicados llegan a ser un único punto de falla en la red.

5.6.3. BIS

El mecanismo BIS es para la comunicación entre aplicaciones IPv4 sobre con IPv4 únicamente e IPv6 únicamente.

Tres capas extras – extensión del resolver de nombres, mapeador de direcciones, y traductor – son añadidos a la pila de protocolos IPv4 entre las capas de aplicación y red. Si una aplicación necesita comunicarse con un hosts de IPv6 únicamente, la capa extra mapea una dirección IPv6 a la dirección IPv4 del host. El mecanismo de traducción es definido como parte de SIIT.

Este mecanismo es para la implementación de sistemas finales únicamente. Una extensión al mecanismo BIS permite a hosts dual-stack usar la técnica.

5.6.4. DSTM

El mecanismo de traducción DSTM es para hosts dual-stack en un dominio IPv6 que no tiene aun una dirección IPv4 asignado al lado IPv4, pero requiere comunicarse con sistemas o permitir ejecutar aplicaciones IPv4 en la parte superior de su pila de protocolos IPv6. El mecanismo requiere un servidor dedicado que dinámicamente provee direcciones IPv4 globales temporales para la duración de la comunicación (usando DHCP), y usa túneles dinámicos para transportar el tráfico IPv4 en paquetes IPv6 a través del dominio IPv6.

DSTM llega a ser mucho más relevante conforme IPv6 llega a difundirse más y las direcciones IPv4 llegan a ser mas escasos tal que ellos necesitan ser compartidos entre hosts, y donde los requerimientos son transportar trafico IPv4 sobre IPv6 o comunicar hosts IPv6 en un dominio IPv6 y pequeños sistemas IPv4 heredados.

5.6.5. Gateway basado en SOCKS IPv6/IPv4

El mecanismo de Gateway basados en SOCKS IPv6/IPv4 es para la comunicación entre host con IPv4 únicamente e IPv6 únicamente. Esto consiste en funcionalidad adicional en ambos sistemas finales (cliente) y ruteador dual-stack (Gateway) para permitir un entorno de comunicación que transmita dos conexiones terminadas IPv4 e IPv6 en la capa de aplicación.

Este mecanismo se basa en el protocolo SOCKSv5, y hereda todas las características de ese protocolo.

Existen comandos SOCKSV5 sin cambios, y el protocolo mantiene la seguridad de extremo a extremo entre el cliente y el gateway, y el gateway y el destino.

El mecanismo usa una característica denominada delegación de resolución de nombre DNS para determinar las direcciones IPv6, delegando la resolución de nombre al Gateway, así no se requiere cambios en el DNS existente.

5.7. Tareas pre-despliegue

Antes de desplegar IPv6, necesita registrar una dirección IPv6 (Proveedor de Servicio de Internet) o solicitar un prefijo IPv6 de su Proveedor de Servicios de Internet (enterprise), configurar su DNS, decida una política para la administración de la red, y seleccione los protocolos de ruteo requerido.

El registro de dirección IP es dependiente de si Ud. Es un proveedor o Enterprise, si Ud esta registrando para un entorno de producción o quiere ganar experiencia de IPv6 a través de la comunidad 6bone, y la estrategia de despliegue seleccionada. Su DNS debe ser configurado con un componente servidor para soportar IPv6, y con una Resolver Library que maneje ambos tipos de registros de recursos IPv4 e IPv6. En los inicios de la administración de red los ruteadores dual-stack usa TFTP, ping, Telnet, y traceroute, con soporte completo para MIBs IPv6. El soporte de los protocolos de ruteo iniciales se centra RIP, IS-IS y BGP multiprotocolo para IPv6, con soporte para OSPFv3 y el protocolo de ruteo de puerta interior mejorada versión 6 (EIGRPv6) planificado para IPv6 para el IOS Cisco.

Las tareas de pre-despliegue que necesita realizar antes de iniciar su despliegue de prueba, son:

- Requerimientos de direcciones IPv6
- Requerimientos de servidor de nombres de dominio
- Gestión de red
- Protocolos de ruteo

5.8. Implementación de dual stack (IPv4/IPv6) en el ruteador y switch capa 3

La red actualmente contempla la existencia de 4 vlan's: red académica, red intranet, red administrativa, red de equipos de comunicaciones. La configuración de vlan's a utilizarse será el de vlan's locales (también denominadas vlan´s geográficas).

Esto significa que cada switch capa 3 que contenga definición y asignación de puertos a vlan's llevara a cabo el enrutamiento entre vlan's.

En cada switch de sector deberá ser definido cada una de las cuatro vlan's, asignándose los puertos según el grupo al cual pertenezca.

Cada vlan definida localmente se corresponde con una subred, según las definiciones en las Tablas del Capitulo 4.

En cada switch capa 3 deberá asignarse una dirección IPv4 e IPv6 a cada interface vlan, para que se lleve a cabo la función de ruteo respectiva.

Cada host perteneciente a una vlan, tendrá como puerta de enlace la dirección ip asignada a cada interfase vlan respectiva, en cada switch. Esto significa que cada host tendrá dos puertas de enlace, una para la pila IPv4 y la otra para IPv6.

La relación entre las vlan´s y las redes lógicas es implícita, para los hosts, todos los hosts conectados a los puertos asignados a una misma vlan deben tener el mismo prefijo de red.

Un switch capa 3 que tenga habilitado el ruteo, luego que se asigne una dirección IPv6 a su interfaz vlan anunciará el prefijo de red correspondiente.

Los host solicitarán y recibirán el prefijo de red IPv6 desde las interfaces vlan de los switch capa 3, autoconfigurándose con el prefijo y el EUI-64. Para esto cada PC deberá tener activo la pila IPv6.

Luego deberá configurarse el protocolo de ruteo ripng (rip para IPv6), para posibilitar la comunicación entre los host pertenecientes a otros switch´s, asegurando de este modo la comunicación entre todos los hosts.

5.9. Configuración

A continuación se muestran los entornos en los cuales se llevarán a cabo las configuraciones IPv6.

5.9.1. Configuración de los switch's

Para configurar IPv6 en los switch´s se utilizaran los siguientes comandos.

a) Para seleccionar la interfaz a configurar use el comando:

   hostname(config)# interface interface_name

b) Para asignar la dirección link-local utilizar el comando:

   hostname(config-if)# ipv6 address autoconfig

   Otra forma de generar la direccion link-local es:

hostname(config-if)# ipv6 enable

c) Asigne la dirección IPv6 usando el siguiente comando:

hostname(config-if)# ipv6 address ipv6-address [eui-64]

d) Para configurar una ruta por defecto y ruta estática, use los comandos:

hostname(config)# ipv6 route interface_name ::/0 next_hop_ipv6_addr

hostname(config)# ipv6 route if_name destination
next_hop_ipv6_addr [admin_distance]

e) Para verificar la configuración IPv6 use los siguientes commandos:

hostname# show ipv6 interface [if_name]

hostname# show ipv6 interface

ipv6interface is down, line protocol is down

IPv6 is enabled, link-local address is fe80::20d:88ff:feee:6a82 [TENTATIVE]

No global unicast address is configured

Joined group address(es):

ff02::1

ff02::1:ffee:6a82

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds

f) Para visualizar la table de ruteo IPv6, ejecute el siguiente commando:

hostname# show ipv6 route

hostname# show ipv6 route

IPv6 Routing Table - 7 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 – OSPF ext 2

L fe80::/10 [0/0]

via ::, inside

L fec0::a:0:0:a0a:a70/128 [0/0]

via ::, inside

C fec0:0:0:a::/64 [0/0]

via ::, inside

L ff00::/8 [0/0]

via ::, inside

5.9.2. Configurando RIP para IPv6

a) Para ingresar al modo configuración global ejecute el comando:

hostname # configure terminal

b) Para activar el proceso rip ejecute el commando:

hostname (config)# ipv6 router rip cisco

c) Para determinar el maximo numero de rutas redundantes a usar ejecute:

hostname (config-router)# maximum-paths 1

d) Para propagar

hostname (config-if)# exit

hostname (config)# interface Ethernet 0/0

hostname (config-if)# ipv6 rip cisco default-information originate

5.10. Instalación de IPv6 en los host's

a) Para activar la pila IPv6 en los hosts con windows XP, abrir una ventana de consola y ejecute ipv6 install. La Figura 5.1. muestra el resultado de la ejecución.

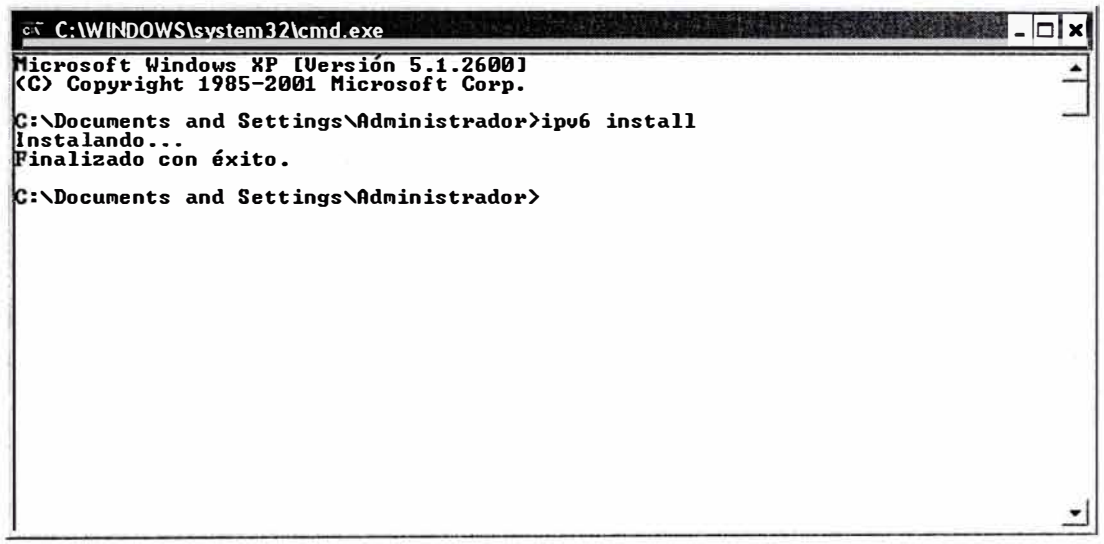


Figura 5 . 1 Activación de la Pila IPv6 en Windows XP

b) Para visualizar las pilas IPv4 e IPv6 ejecute el comando ipconfig. La Figura 5.2 muestra el resultado de la ejecución del comando.

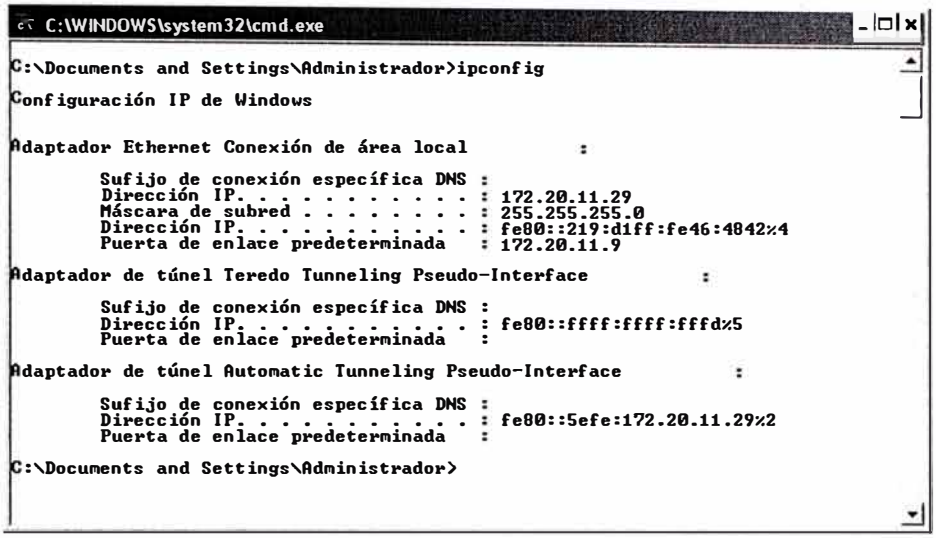


Figura 5 . 2 Pila de IPv4 e IPv6

5.11. Implementación del servidor DNS IPv6:

Instalación de la ultima versión más estable de Bind, configuración para su operación dual-stack.

```
% tar -xzf bind-9.2.1.tar.gz
% cd bind-9.2.1
```

Para el soporte de DNSSEC, deberá compilar con soporte de encriptación

```
% ./configure -enable-ipv6 -with-openssl
```

Finalmente instalamos

```
% make && make install
```

Configurando DNSSEC

Ejemplo del archivo de configuración named.conf

/etc/named.conf

```
options {
directory "/var/named";
// a caching only nameserver config
zone "." IN {
type hint;
file "named.ca";
};

// this defines the loopback name lookup
zone "localhost" IN {
type master;
file "master/localhost.zone";
```

```
allow-update { none; };
};

// this defines the loopback reverse name lookup
zone "0.0.127.in-addr.arpa" IN {
type master;
file "master/localhost.rev";
allow-update { none; };
};

// This defines the secv6 domain name lookup
// Secure (signed) zone file is
// secv6.your.domain.signed
// Regular zone file is secv6.your.domain
zone "secv6.your.domain" IN {
type master;
file "master/secv6.your.domain.signed";
// file "master/secv6.your.domain";
};

// this defines the secv6 domain reverse
// name lookup (AAAA)
zone "secv6.int" IN {
type master;
file "master/secv6.int";
};

// this defines the secv6 domain reverse
// name lookup (A6)
zone "secv6.arpa" IN {
type master;
file "master/secv6.rev";
};

// secret key truncated to fit
key "key" {
```

```
algorithm hmac-md5;
secret "HxbmAnSO0quVxcxBDjmAmjrmhgDUVFcFNcfmHC";
};
```

Ejemplo de configuración de los registros de entrada de un dominio

/var/named/master/secv6.your.domain

```
$TTL 86400
$ORIGIN secv6.your.domain.
@ IN SOA secv6.your.domain. hostmaster.your.domain. (
2002011442 ; Serial number (yyyymmdd-num)
3H ; Refresh
15M ; Retry
1W ; Expire
1D ) ; Minimum
IN MX 10 noah.your.domain.
IN NS ns.secv6.your.domain.
$ORIGIN secv6.your.domain.
ns 1D IN AAAA fec0::1:250:b7ff:fe14:35d0
1D IN A6 0 fec0::1:250:b7ff:fe14:35d0
secv6.your.domain. 1D IN AAAA fec0::1:250:b7ff:fe14:35d0 1D IN A6 0
fec0::1:250:b7ff:fe14:35d0
pc2 1D IN AAAA fec0::1:250:b7ff:fe14:35d0  1D IN A6 0
fec0::1:250:b7ff:fe14:35d0
pc3 1D IN A6 0 fec0::1:250:b9ff:fe00:131  1D IN AAAA
fec0::1:250:b9ff:fe00:131
pc6 1D IN A6 0 fec0::1:250:b7ff:fe14:3617  1D IN AAAA
fec0::1:250:b7ff:fe14:3617
pc4 1D IN A6 0 fec0::1:250:b7ff:fe14:35c4  1D IN AAAA
fec0::1:250:b7ff:fe14:35c4
pc5 1D IN A6 0 fec0::1:250:b7ff:fe14:361b  1D IN AAAA
fec0::1:250:b7ff:fe14:361b
pc7 1D IN A6 0 fec0::1:250:b7ff:fe14:365a  1D IN AAAA
fec0::1:250:b7ff:fe14:365a
pc1 1D IN A6 0 fec0::1:250:b9ff:fe00:12e  1D IN AAAA
fec0::1:250:b9ff:fe00:12e
pc1 1D IN A6 0 fec0:0:0:1::1 1D IN AAAA fec0:0:0:1::1
$INCLUDE "/var/named/master/Ksecv6.your.domain.+003+27034.key"
```

CONCLUSIONES

a) Los creadores de IPv4 no consideraron la demanda que podía llegar a tener este protocolo, situación que ha llevado en este momento al agotamiento inminente de direcciones IPv4 razón por la cual se planteo un incremento en la capacidad de direccionamiento en el nuevo protocolo IPv6.
b) Las soluciones transitorias planteadas para postergar el agotamiento de direcciones IPv4, ya cumplieron su función. Soluciones como NAT impiden una identificación global de los hosts, siendo un factor limitante para el despliegue de muchos servicios y el desarrollo de otros que requieren identificadores globales.
c) Dada la investigación realizada, queda claro la importancia y necesidad de implementar IPv6, ya que las mejoras que ofrece son realmente significativas, independientemente de la necesidad de espacio para las direcciones que requiere el mundo actual.
d) Una de las ventajas que ofrece IPv6 es la capacidad que tiene para dar soporte a IP's del protocolo IPv4, lo cual es de suma importancia, ya que resulta impensable la posibilidad de eliminar de un día para otro un protocolo tan utilizado como lo es IPv4. Para ser reemplazado IPv4 es necesario que la nueva arquitectura soporte ambos protocolos para lograr una migración gradual.
e) El protocolo IPv6 está pensado de una forma muy ambiciosa y con mucha visión de futuro. Es necesario dar soporte a las aplicaciones que en la actualidad se ejecutan en el protocolo IPv4.
f) Uno de los puntos que se consideraron para el desarrollo de este protocolo fue la capacidad de brindar soporte a dispositivos móviles. Generalmente los dispositivos móviles tienen una limitada capacidad de transmisión de datos; pero por la forma en que se enrutan los paquetes IP se reduce de forma considerable el trafico en la red utilizando un menor ancho de banda.
g) IPv4 e IPv6 cuentan con una serie de especificaciones que los hacen diferentes, a pesar que la versión 6 está basada en la versión 4. Los espacios en las direcciones son mucho mayores en IPv6, la configuración resulta ser mucho más sencilla y amigable para los usuarios. IPv6 no maneja broadcast por seguridad, lo cual puede

ser una desventaja para los administradores de red que en ocasiones lo utilizan para hacer pruebas de conectividad.

h) La Tabla 6.1 muestra una comparación entre los protocolos IPv4 e IPv6.

Tabla 6 . 1

Comparativo entre Protocolos

Tema	IPv4	IPv6	Ventajas IPv6
Espacio de direcciones	2^4 direcciones	2^{128} direcciones	Prácticamente espacio ilimitado.
Configuración	Manual o DHCP	Universal Plud And Play (UPnP) con ó sin DHCP.	Menor gasto de operaciones y reducción de errores.
Broadcast/Multicast	Usa Ambos	No se usa broadcast; existen diferentes formas de Multicast.	Mejor eficiencia en el ancho de banda.
Soprte Anycast	No	Completo	Soporta nuevas aplicaciones móviles.
Configuración de la Red	Gran parte manual.	Facilita la renumeración de los hosts y routers	Fácil migración y menor necesidad de operaciones.
Soporte de calidad de servicio (QoS)	Tipos de servicio usando diferentes servicios	Clases de flujo y etiquetas de flujo	Mayor control de QoS.
Seguridad	Usa IPSec para la seguridad de paquetes	IPSec se usa como llave tecnológica para la protección de datos y el control de paquetes.	Red unificada para la seguridad con lo cual se genera un ambiente computacional de mayor seguridad.
Movilidad	Difícil de implementar.	Optimización de enrutamiento y movilidad jerárquica.	Mejor eficiencia y escalabilidad.

Las pruebas comparativas son contundentes, IPv6 supera enormemente a IPv4.

i) Una buena alternativa para la migración a IPv6 en la red de campus es usar **Dual Stack**, y utilizar VLAN locales para una mejor administración de la red. Se recomienda utilizar switch que tengan la capacidad de hacer conmutación y ruteo.

j) En esta fase inicial de implementación se propone identificar los hosts de la red de campus, asi como los switch´s y ruteadores con direcciones IPv6 además de las IPv4, esto no debería ocasionar la interrupción de los servicios brindados por IPv4, sino además ser accesibles mediante direcciones IPv6, esta transparencia se logra implementando el servicio DNS para IPv6, e identificando a todos los host´s por nombres.

BIBLIOGRAFIA

a) Fuentes Bibliográficas

1. Sam Brown - Brian Browne - Neal Chen - Paul Fong - Robbie Harrell - Eric Knipp - Bart Saylors - Rob Webber - Edgar Parenti, "Configuring IPv6 for Cisco IOS", Syngress Publishing - 2002.

2. Cisco, "The ABCs of IP Version 6", Cisco IOS Learning Service - 2002.

3. Joseph Davies, "Understanding IPv6", Microsoft Press - 2002.

4. Desmeules, Regis, "Cisco Self-Study: Implementing Cisco IPv6 Networks (IPV6)", Cisco Press - 2003.

b) Otras Fuentes

5. http://www.iana.org/numbers [Consulta: 17 mayo 2008]

6. http://www.6sos.net/documentos/6SOS_Tutorial_IPv6_v4_0.pdf [Consulta: 17 mayo 2008]

7. http://www.exitoexportador.com/stats.htm [Consulta: 17 mayo 2008]

8. http://www.aseta.org/seminarios/ciberseguridad/DDiazIPv6-UIT.pdf [Consulta: 18 mayo 2008]

9. http://blogfiee.blogspot.com/2008/07/videoclases-protocolo-ipv6.html [Consulta: 20 mayo 2008]

10. http://www.cisco.com/en/US/docs/ios/solutions_docs/ipv6/IPv6dswp.pdf [Consulta: 15 junio 2008]