

8 JUNE 2011  
**THE FUTURE**  
IS FOREVER



# Desplegando la Red IPv6

Jesús Martínez Alfonso  
Dariene Gandarias Jorge  
Oscar G. Acosta

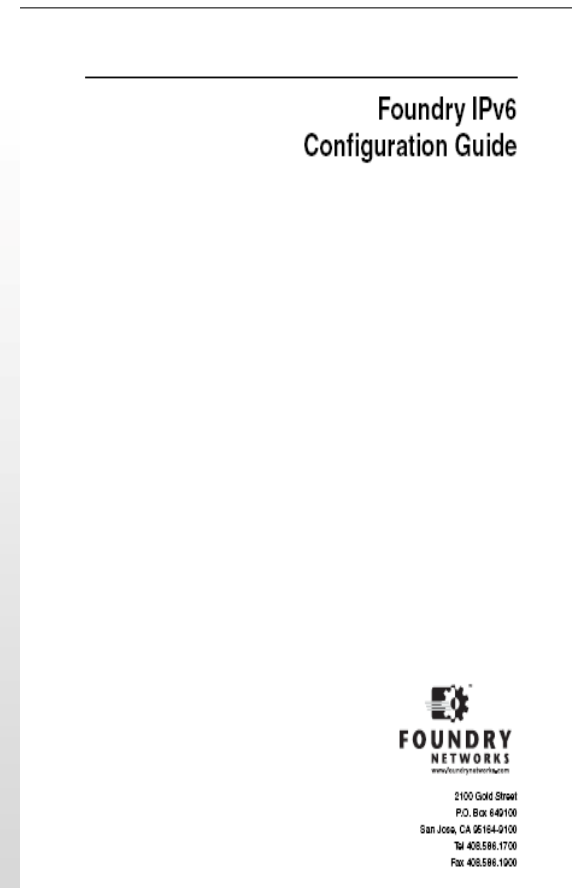
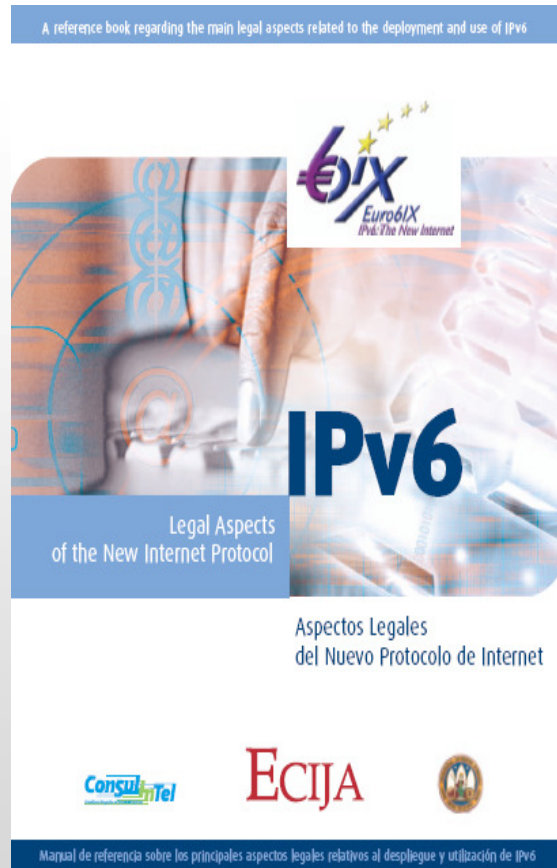
Junio 2011



# OBJETIVOS

- Presentar el por qué es necesario desplegar IPv6.
- Mostrar el estado actual del desarrollo e implementación del protocolo IPv6 en la Región.
- Explicar el proceso de transición a IPv6 en una red privada.
- Mostrar el camino a seguir para desplegar IPv6.
- Permitir identificar especialistas interesados en trabajar en la introducción del protocolo IPv6.
- Permitir identificar posibles proyectos a acometer, basados en IPv6.
- Apoyar e impulsar la divulgación, investigación y formación profesional sobre IPv6 en la redes.

# LIBROS RECOMENDADOS



# SUMARIO

## Parte 1. Introducción a IPv6 (1:30 horas – Dariene y Jesús)

- ¿Por qué IPv6? Limitaciones de IPv4
- Orígenes
- Características y ventajas
- Políticas de asignación y uso de direcciones IPv6
- Estado del despliegue en el mundo y en la región: principales actores
- Preparando la introducción de IPv6 en una red

## Parte 2. Arquitectura del direccionamiento en IPv6 (1:30 horas – Jesús)

- Plan de direccionamiento IPv6
- Esquema de numeración para subredes

# SUMARIO

## Parte 3. Mecanismos de transición (1:30 horas – Jesús y Dariene)

- Dual Stack
- Túneles
- Traductores

## Parte 4. Configuración de IPv6 (30 Min– Jesús)

- Mapa de tareas de configuración
- Servicios IPv6
- Configurando la PC

# SUMARIO

## Parte 5. Seguridad en IPv6 (1 hora – Oscar)

- Introducción
- IPsec
- Nuevas amenazas con IPv6
- Amenazas en la transición
- Estado del arte de los ataques sobre IPv6

## Parte 6. Caso de Estudio (30 min – Dariene)

- IPv6 en la red TRANSNET

# SUMARIO



Parte 1. Introducción a IPv6

Parte 2. Arquitectura del direccionamiento en IPv6

Parte 3. Mecanismos de transición

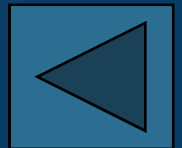
Parte 4. Configuración de IPv6

Parte 5. Seguridad en IPv6

Parte 6. Caso de Estudio

# Parte 1. Introducción a IPv6

- ¿Por qué IPv6? Limitaciones de IPv4
- Orígenes
- Características y ventajas
- Políticas de asignación y uso de direcciones IPv6
- Estado del despliegue en el mundo y en la región: principales actores
- Preparando la introducción de IPv6 en una red





## ¿Por qué IPv6? Limitaciones de IPv4

- La versión 4 del protocolo IP ha funcionado con éxito durante décadas gracias a su gran poder de adaptación a las distintas tecnologías subyacentes.
- Pero a pesar de la gran flexibilidad de IPv4, ha surgido la necesidad de su reemplazo.
- La principal razón para el uso de IPv6 es el agotamiento del espacio de direcciones IPv4.
- Cuando IPv4 surgió las direcciones tenían un total de 32 bits y se agrupaban en clases.

	1	8	16	24	32	
Clase A	0	Net ID	Host ID			
Clase B	1	0	Net ID	Host ID		
Clase C	1	1	0	Net ID	Host ID	
Clase D	1	1	1	0	MULTICAST	
Clase E	1	1	1	1	0	RESERVADO

## ¿Por qué IPv6? Limitaciones de IPv4

- Los métodos de asignación de las direcciones tenían que ver con el tamaño de la red y en consecuencia con la clase de la misma.
- Esto traía como consecuencia que un gran número de direcciones asignadas no fueran utilizadas y que ocurriera un rápido agotamiento de las direcciones clase B, que por su tamaño intermedio resultaban las más adecuadas para la mayoría de las organizaciones.
- Una primera solución fue asignar no solo clases B, sino bloques de direcciones clase C adyacentes.
- Esto generó un gran aumento en las entradas de los enrutadores y por ende un aumento en la memoria necesaria en los mismos para las tablas de enrutamiento.

## ¿Por qué IPv6? Limitaciones de IPv4

- La siguiente solución a este problema fue el surgimiento del CIDR (Classless InterDomain Routing, RFC 1519) que, en esencia, eliminó el concepto de clases e introdujo el concepto de máscara. Ejemplos:

Prefijo	Máscara de subred	Cantidad de bits disponibles	Cantidad de direcciones IP
/30	255.255.255.252	2	$2^2=4$
/27	255.255.255.224	5	$2^5=32$
/23	255.255.254.0	9	$2^9=512$

- Ejemplo: 192.168.34.220 /30

- 11000000 10101000 10000010 11011100 ----- (Red)
- 11000000 10101000 10000010 11011101 ----- (Asignar)
- 11000000 10101000 10000010 11011110 ----- (Asignar)
- 11000000 10101000 10000010 11011111 ----- (Broadcast)

## ¿Por qué IPv6? Limitaciones de IPv4

- A modo de aclaración:

- Las RFC (Request for Comments) son notas sobre Internet que comenzaron a publicarse en 1969. Cada una es un documento cuyo contenido es una propuesta oficial relacionada con un protocolo de Internet. Cada RFC tiene un título y un número asignado, que no puede repetirse ni eliminarse aunque el documento quede obsoleto.
- Es el IETF (Internet Engineering Task Force ) el encargado de regular estas propuestas estándares conocidos como RFCs. Esta organización internacional fue creada en Estados Unidos en 1986. Su objetivo es velar porque la arquitectura de Internet y los protocolos que la conforman funcionen correctamente.

## ¿Por qué IPv6? Limitaciones de IPv4

- Luego se publicó la RFC 1597 (la RFC 1918 la dejó obsoleta posteriormente), que define tres bloques de direcciones privadas, con el objetivo de utilizarlas cuando no sea imprescindible el uso de direcciones públicas y así poder hacer un uso más racional del espacio de direcciones IP. Los bloques son los siguientes:
  - 10.0.0.0 /8
  - 172.16.0.0 /12
  - 192.168.0.0 /16

## ¿Por qué IPv6? Limitaciones de IPv4

- Más adelante se introdujo el mecanismo NAT (Network Address Translator) que permite brindar conectividad a una red con unas pocas direcciones públicas (ver RFC 1631 y otras asociadas).
- El NAT resuelve algunos problemas pero introduce otros como son:
  - Dificulta el uso de IPsec y de las VPN ya que los dispositivos NAT modifican el encabezado de los paquetes.
  - En algunos casos dificulta la comunicación, sobretodo cuando se usan algunos servicios como por ejemplo VoIP.
  - La administración remota de redes que se encuentran detrás de un NAT, es más complicada.
  - Imposibilita el uso de el modelo punto a punto, impidiendo el uso de algunos servicios como son los P2P (Peer to Peer). En una red P2P no existen clientes ni servidores fijos. Los nodos actúan simultáneamente como ambas cosas.
  - Disminuye la visibilidad de los dispositivos móviles desde fuera de la red y el mantenimiento ininterrumpido de las comunicaciones en condiciones de movilidad.

## ¿Por qué IPv6? Limitaciones de IPv4

- Sin embargo, a pesar de todos estos esfuerzos, en la actualidad las direcciones IPv4 están casi totalmente agotadas.
- Para comprender lo que se explicará más adelante es necesario conocer:
  - La IANA (Internet Assigned Numbers Authority) es la encargada, junto con la ICANN (Internet Corporation for Assigned Names and Numbers), de la asignación de los bloques de direcciones IP, de los nombres de dominios, entre otras tareas.
  - Los RIR (Regional Internet Registry) son los encargados de la signación y registro de bloques de direcciones IP y de ASNs (Autonomous System Number) dentro de una región en particular.

## ¿Por qué IPv6? Limitaciones de IPv4

- Existen cinco RIRs:

- APNIC (Asian Pacific Network Information Centre)
- RIPE-NIC (Réseaux IP Européens Network Coordination Centre)
- ARIN (American Registry for Internet Numbers)
- LACNIC (Latin American and Caribbean Internet Address Registry)
- AfriNIC (African Network Information Centre)



- La IANA delega los recursos de Internet a los RIRs.
- Los RIRs, siguiendo las políticas regionales establecidas, delegan estos recursos a ISPs (Internet Service Providers) y a organizaciones.



## ¿Por qué IPv6? Limitaciones de IPv4

- En agosto del 2010 el espacio de direcciones IPv4, administrado por la IANA, estaba casi en su totalidad asignado.

IPv4 Address Space Consumption										Current					
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255
Allocated to RIR					IANA Free Pool					Other Uses					
Allocated to RIR in 2010															

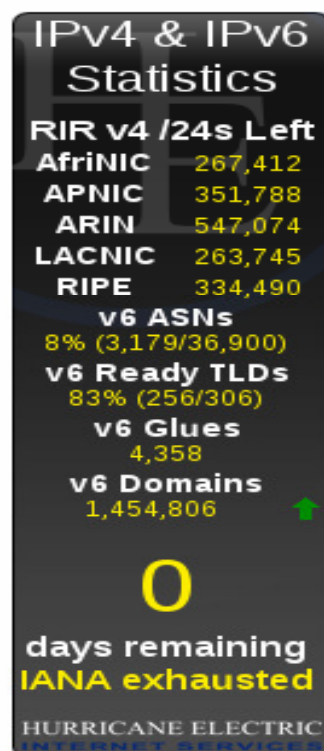
## ¿Por qué IPv6? Limitaciones de IPv4

- En febrero del 2011 se anunció que el stock central de direcciones IPv4 administrado por la IANA quedó finalmente agotado, al entregar los últimos bloques disponibles de direcciones IPv4 a los cinco RIRs existentes.

# ¿Por qué IPv6? Limitaciones de IPv4

Escrito el 10/02/2011 a las 19:45

## Se terminó el stock central de direcciones IPv4



El momento tantas veces anunciado finalmente llegó: ya no hay mas bloques IPv4 libres en poder de la [IANA](#). Nos encontramos en una etapa nueva en Internet, en la cual uno de los recursos fundamentales, que constituye la base de la red, se ha agotado. La solución prevista, la adopción de IPv6, se hace más necesaria que nunca. Qué podemos esperar hacia el futuro?

El día 3 de Febrero de 2011 se hizo público el anuncio del agotamiento del stock de direcciones IPv4 en poder de la IANA (ver: "<http://lacnic.net/sp/anuncios/2011-agotamiento-ipv4.html>"). El día 31 de Enero se habían otorgado dos bloques /8 a [APNIC](#) (el registro regional de Asia y Pacífico), quedando sólo 5 bloques disponibles en manos de [IANA](#). Ante esa situación, entró en vigencia la política global que indicaba que se debían repartir esos 5 bloques restantes entre los 5 registros regionales de Internet ([ARIN](#), [APNIC](#), [LACNIC](#), [RIPE-NCC](#) y [AfrinIC](#)), quedando la IANA finalmente sin bloques libres.

La situación al día de hoy es que los registros regionales (RIRs) cuentan con un espacio de direcciones que les permitirá subsistir por algún tiempo, que variará en función de la demanda de cada región. Se estima que el primer RIR que agotará su espacio de direcciones es APNIC, previéndose que ocurra alrededor del último trimestre de 2011. Por otra parte, en nuestra región, las previsiones de LACNIC estiman que mitad de 2013 sería una fecha probable para el agotamiento de las direcciones.

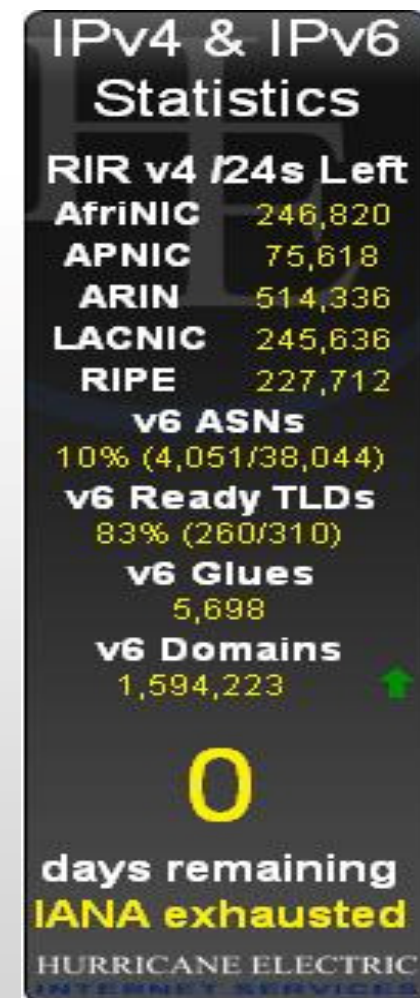
Ante ese escenario, es importante tener en cuenta que la única solución para continuar con una Internet como la que conocemos, en constante evolución, es adoptar el protocolo IPv6, la nueva versión del protocolo IP, desarrollado en los años '90. No adoptar las medidas necesarias hoy en día puede tener consecuencias negativas en el desarrollo de Internet y en la continuidad de las actividades de cada organización. Es necesario que todos los sectores se involucren en una transición ordenada hacia la nueva versión del protocolo IP.

## ¿Por qué IPv6? Limitaciones de IPv4

- Se puede asegurar que en un futuro bastante cercano a los RIRs también se les agotarán las direcciones IPv4.
- El 15 de abril de 2011 APNIC anunció que ha distribuido el último espacio de sus reservas de direcciones IPv4. Esto significa que ahora estará distribuyendo direcciones IPv4 a sus miembros de su último bloque /8.
- Se estima que RIPE NCC agote sus direcciones IPv4 a finales de 2011.
- LACNIC estima que para el 15 de mayo de 2014 ocurra el agotamiento de sus direcciones IPv4. El 31 de marzo de 2011 quedaban 75 270 656 direcciones IPv4 disponibles.

## ¿Por qué IPv6? Limitaciones de IPv4

- Existen en muchos sitios de Internet figuras parecidas a esta que se actualizan constantemente.
- Aquí se brindan estadísticas sobre la cantidad de direcciones IPv4 disponibles aún en los RIRs.
- Además muestran otros aspectos relacionados con IPv6 como son la cantidad de ASNs, dominios y otros.



## ¿Por qué IPv6? Limitaciones de IPv4

- La siguiente tabla muestra la utilización y disponibilidad, hasta el 31 de marzo de 2011, de los bloques de direcciones IP /8 que posee LACNIC.

Block	Direcciones totales	Direcciones utilizadas	Porcentaje	Direcciones disponibles	Porcentaje
177	16777216	4194304	25.00%	12582912	75.00%
179	16777216	0	0.00%	16777216	100.00%
181	16777216	1884160	11.23%	14893056	88.77%
186	16777216	13773824	82.10%	3003392	17.90%
187	16777216	16777216	100.00%	0	0.00%
189	16777216	16777216	100.00%	0	0.00%
190	16777216	15464448	92.18%	1312768	7.82%
191	16777216	0	0.00%	16777216	100.00%
200	16777216	16415232	97.84%	361984	2.16%
201	16777216	16062464	95.74%	714752	4.26%

## ¿Por qué IPv6? Limitaciones de IPv4

- En la actualidad 32 bits no son suficiente, teniendo en cuenta las perspectiva futuras, ya que estos 32 bits no pueden adaptarse al crecimiento proyectado por Internet.
- Gran variedad de servicios brindados sobre una plataforma IP (redes NGN) que implican que las redes de telefonía fija, de telefonía móvil, de datos y otras, dejen de ser redes independientes y converjan en una única red soportada sobre IP
- Existe una gran variedad de terminales como PDAs, teléfonos celulares, computadoras y otros dispositivos que acceden a los diferentes servicios.



## ¿Por qué IPv6? Limitaciones de IPv4

- La “Internet de las cosas”, en donde disímiles dispositivos necesitarán de una dirección IP para lograr la conectividad a las redes, demanda una gran cantidad de direcciones IP.
- El desarrollo de una gran cantidad de tecnologías de banda ancha trae como consecuencia un gran aumento en el uso actual y en las proyecciones futuras del protocolo IP. Ejemplos:
  - Tecnologías DSL (Digital Subscriber Line)
  - PLC (Power Line Communication)
  - WiMAX (Worldwide Interoperability for Microwave Access)
  - FTTH (Fiber To The Home)



## ¿Por qué IPv6? Limitaciones de IPv4

- Otro motivo es la necesidad de un soporte nativo para nuevas aplicaciones como el audio y el video que requieren de transmisión en tiempo real y necesitan ciertas garantías en los retardos y el ancho de banda. Ejemplos:
  - VoIP
  - Videoconferencia
  - Telepresencia
- Es decir, es necesario proporcionar calidad de servicio.
- Para resolver esta limitante de Pv4, el IETF tuvo que desarrollar un nuevos protocolos como el RSVP (Resource reServation Protocol) que asigna recursos a los enrutadores para poder garantizar calidad de servicio en las aplicaciones IPv4 que lo requieran.

## ¿Por qué IPv6? Limitaciones de IPv4



- Además, en la actualidad hay una tendencia al aumento de la movilidad en los usuarios para la cual IPv4 no está preparada de manera nativa.
- Para garantizarla debe utilizar la tecnología IP Móvil que implica el uso de direcciones privadas y del NAT debido a la poca cantidad de direcciones IPv4 disponibles en la actualidad.

## Orígenes



- IPv6 fue desarrollado por el IETF.
- La estandarización del protocolo IPv6 comenzó en 1991.
- A partir del año 1995 se comenzaron a publicar las primeras RFCs relacionadas con IPv6.
- En 1996 se creó la red 6Bone que no fue más que una plataforma mundial de prueba para IPv6.
- El Forum IPv6 (<http://www.ipv6forum.com>) fue fundado en febrero de 1999.
- Luego, se fueron creando, en muchos países del mundo, TF IPv6.
- En el 2004 fue anunciado por la ICANN que los DNS principales de Internet habían sido modificados para soportar tanto IPv4 como IPv6.

# CARACTERÍSTICAS Y VENTAJAS

- IPv6 conserva muchas de las características de la versión anterior.
- Introduce algunos cambios bastante significativos como:
  - Tamaño de las direcciones IP
  - Notación y tipos de direcciones IP
  - Encabezado flexible
  - Calidad de servicio a nivel de red (QoS)
  - Autoconfiguración
  - Soporte nativo de multicast
  - Soporte nativo para la movilidad
  - Mejoras en la seguridad

# CARACTERÍSTICAS Y VENTAJAS

## Tamaño de las direcciones IP

- IPv6 cuadriplica el valor del tamaño de estas direcciones de IPv4.
- Usa un total de 128 bits en lugar de 32 bits, garantizando que las direcciones no se agoten hasta un futuro bastante lejano. Con ello se pueden formar  $2^{128}$  ( $3,4 \times 10^{38}$ ) direcciones IP.

### IPv4

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

### IPv6

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

- Mantiene el mecanismo CIDR con una organización flexible y jerárquica.

# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

- La nueva versión del protocolo IP introduce cambios en la notación y en los tipos de direcciones.
- La notación decimal por puntos usada para IPv4 resulta muy extensa e incómoda luego del aumento a 128 bits en las direcciones de red.
- Para hacer esta notación más práctica y compacta se usa la notación hexadecimal con dos puntos.

Decimal	Binario	Hexadecimal
0	0	0
1	1	1
2	10	2
3	11	3
4	100	4
5	101	5
6	110	6
7	111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

- Son usados 32 dígitos hexadecimales ya que cada uno representa 4 bits, quedando 8 grupos separados por dos puntos que representan cada uno 16 bits.
  - Ej: **2001:0db8:0000:0000:0000:0000:0000:0000**
- Se pueden eliminar los ceros innecesarios para escribir la dirección de forma más compacta.
  - Ej: **2001:db8:0:0:0:0:0:0**
- Además se utiliza la técnica de la compresión cero, mediante la cual una cadena de ceros repetidos se reemplaza por un par de dos puntos.
  - Ej: **2001:db8::**
- En la RFC 5952 se explican detalladamente las reglas para escribir direcciones IPv6 .

# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

- Los prefijos IPv6 son asignados de la siguiente manera según la RFC 3177.

Prefijo	Asignar a	Cantidad de direcciones
/32	LIR (Generalmente el ISP)	$2^{96}$
/48	Organización	$2^{80}$
/64	Subred	$2^{64}$
/128	Host	1

- Se recomienda utilizar prefijos que sean múltiplos de 4, para mayor facilidad a la hora de realizar el direccionamiento dentro de la organización y dentro de la subred.



# CARACTERÍSTICAS Y VENTAJAS

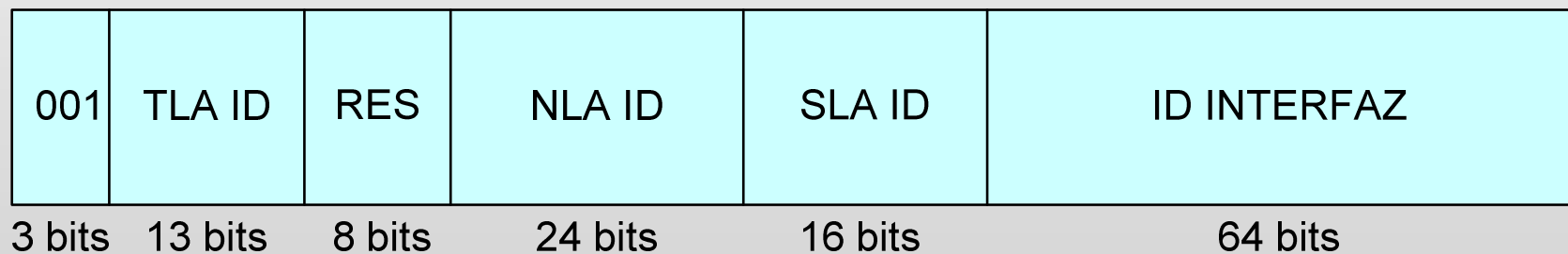
## Notación y tipos de direcciones IP

- En la nueva versión del protocolo IP existen tres tipos de direcciones:
  - **Unicast**: Identifica una interfaz única y es equivalente a la dirección IPv4 actual.
  - **Anycast**: Identifica un conjunto de interfaces. Un paquete enviado a una dirección anycast es entregado sólo a una de dichas interfaces (generalmente a la más cercana según la distancia medida por el protocolo de enrutamiento).
  - **Multicast**: Identifica también a un conjunto de interfaces con la diferencia de que un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección.
- La RFC 2373 define y explica, de manera general, los tipos de direcciones IPv6 existentes.

# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

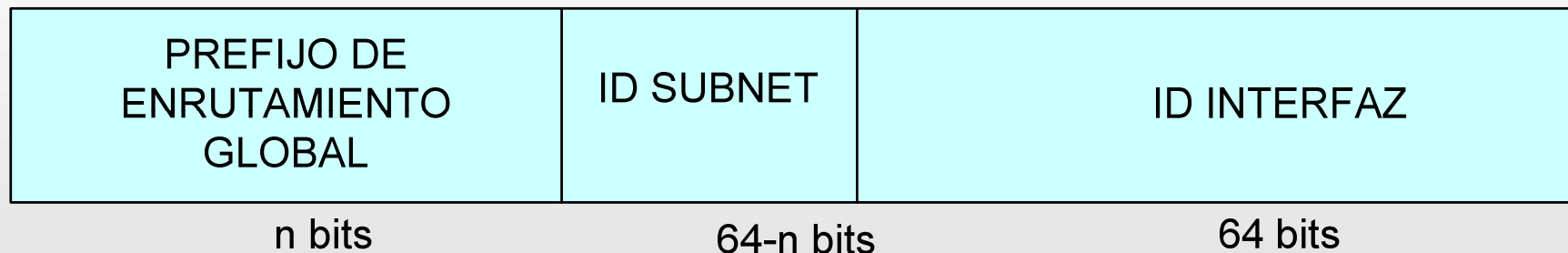
- Las direcciones Unicast poseen dos ámbitos: el global y el de enlace local.
- Las de ámbito global se pueden encaminar globalmente. Su ámbito es la red Internet IPv6 y son equivalentes a las direcciones IPv4 reales.
- La estructura, que inicialmente, tuvo este tipo de direcciones se definió en la RFC 2374 pero ya está obsoleta.



# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

- En la actualidad la nueva estructura para las direcciones unicast de ámbito global está definida es la RFC 3587, que fue la RFC que dejó obsoleta a la RFC 2374.

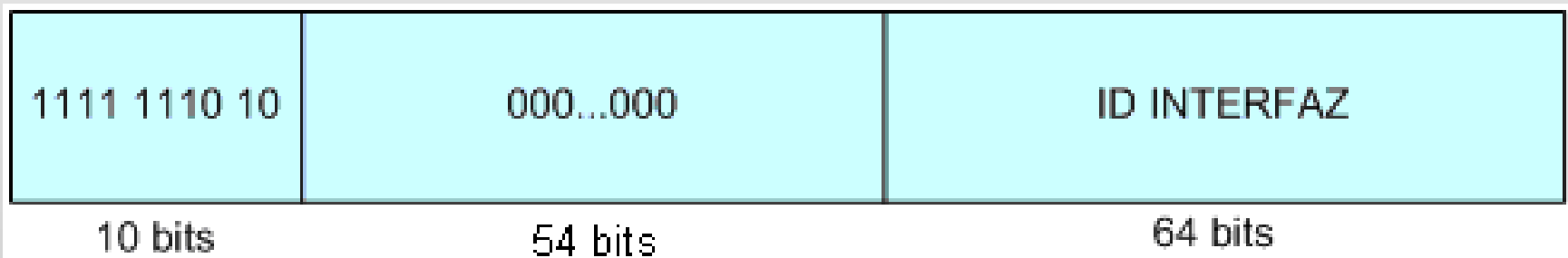


- El prefijo de enrutamiento global está diseñado para ser estructurado jerárquicamente por los RIR e ISPs.
- El campo de subred está diseñado para ser estructurado jerárquicamente por los administradores del sitio.

# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

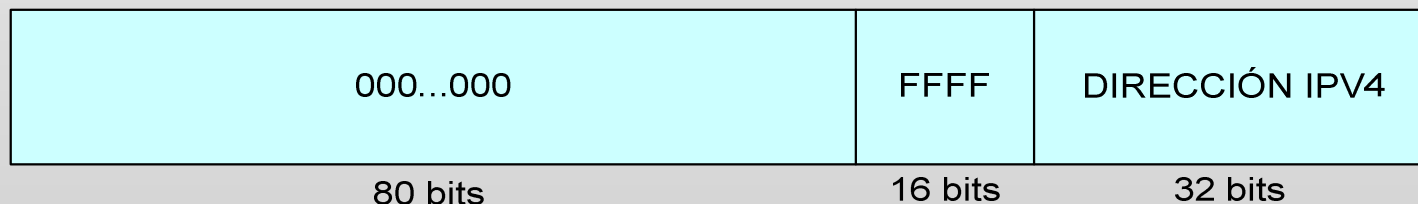
- Las de ámbito de enlace local son utilizadas para comunicarse dentro de un dominio de capa 2 por lo que su ámbito lo constituye la red de enlace.
- Los enrutadores no pueden encaminar paquetes hacia o desde estas direcciones.
- Los hosts IPv6 generan este tipo de direcciones automáticamente en sus interfaces.
- También pueden ser configuradas manualmente.



# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

- Dentro de las direcciones unicast se encuentran además, las llamadas direcciones de uso especial, las cuales no llevan ámbito.
  - Dirección no especificada: los 128 bits están en cero. Esta dirección es utilizada como dirección origen por los dispositivos que no tienen dirección IPv6.
  - Dirección de loopback: usada por los nodos para realizar lazos internos. Posee los primeros 127 bits en cero y el último en 1. Es la dirección análoga a 127.0.0.0 en IPv4.
  - Dirección IPv4 insertada: está encaminada a soportar la coexistencia de ambas versiones.



# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

**Anycast:** Identifica un conjunto de interfaces. Un paquete enviado a una dirección anycast es entregado sólo a una de dichas interfaces (generalmente a la más cercana según la distancia medida por el protocolo de enrutamiento).

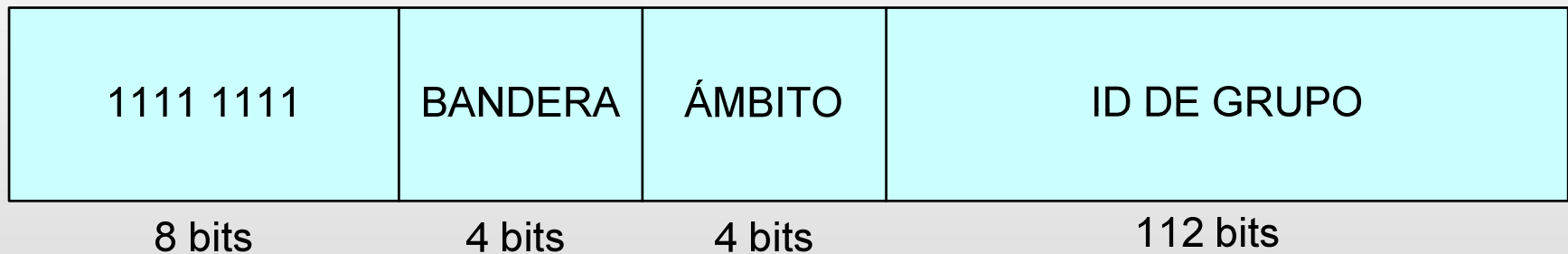
- Las direcciones Anycast no pueden diferenciarse estructuralmente en el formato de las direcciones unicast.
- Para que los nodos entiendan que una dirección es anycast deben ser configurados para ello.
- Este tipo de direcciones es utilizado frecuentemente para replicar importantes recursos de la red y proporcionar redundancia.

# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP

**Multicast:** Identifica también a un conjunto de interfaces con la diferencia de que un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección.

- Las direcciones Multicast reemplazan a las direcciones broadcast usadas para el control.



- La Bandera tiene asignado cuatro bits de los cuales solo tres menos significativos están en uso.
- El ámbito le proporciona a los enrutadores la información necesaria para mantener el tráfico dentro del dominio apropiado.

# CARACTERÍSTICAS Y VENTAJAS

## Notación y tipos de direcciones IP RESUMEN

- Unicast {
  - Global - (2000::/3)
  - Enlace local - (FE80/10)
  - No especificada - (::)
  - Loopback - (::1)
  - IPv4 insertada – (::FFFF:w.x.y.z/96)
  - Otras}
- Anycast { • Mismo formato que las Unicast }
- Multicast { • FF00/8 }

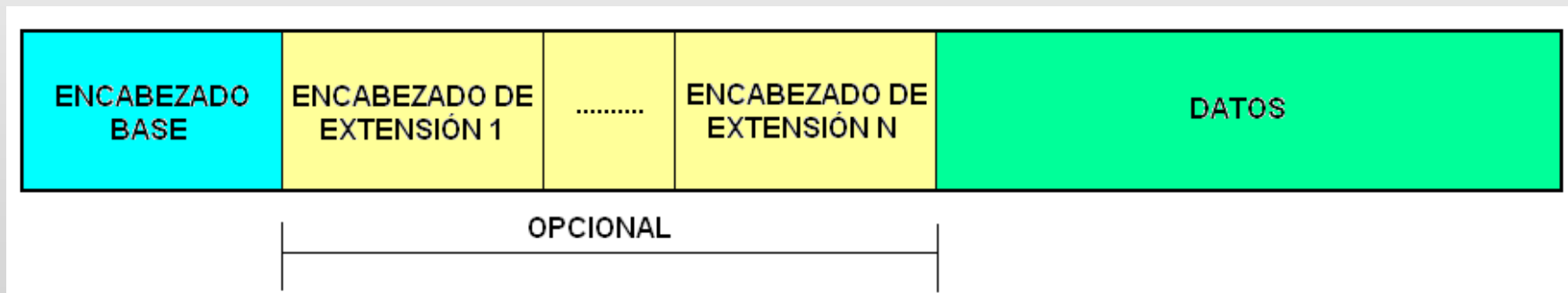




# CARACTERÍSTICAS Y VENTAJAS

## Encabezado flexible

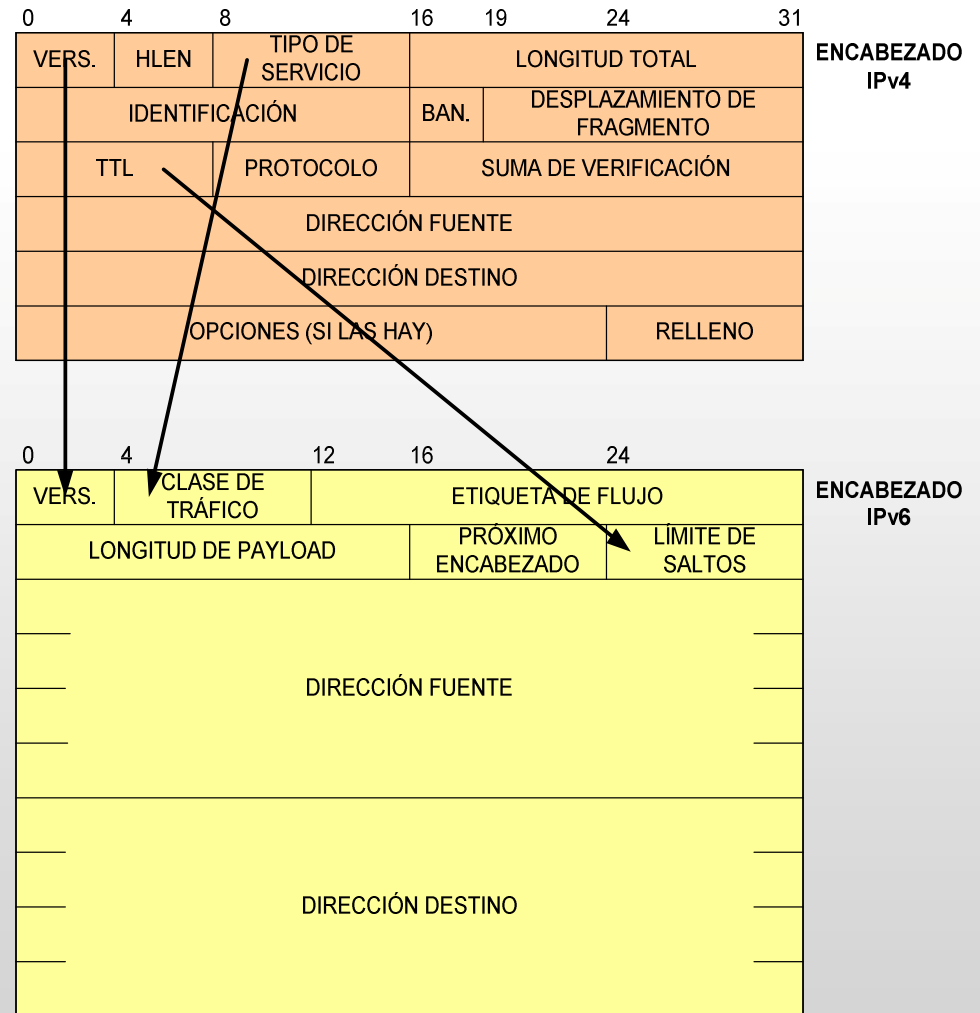
- Utiliza un formato de encabezado flexible.
- IPv6 posee un encabezado base de tamaño fijo (40 octetos), a diferencia de IPv4 en donde el tamaño depende de las opciones utilizadas (20-60 octetos).
- Además, utiliza un conjunto de encabezados opcionales (también llamados encabezados de extensión).



# CARACTERÍSTICAS Y VENTAJAS

## Encabezado flexible

- El encabezado base contiene menos información que el encabezado del datagrama IPv4.
- Las opciones y algunos de los campos fijos que aparecen en el encabezado de un datagrama IPv4 se han cambiado por encabezados de extensión en IPv6.



# CARACTERÍSTICAS Y VENTAJAS

## Encabezado flexible

- Los encabezados opcionales se usan en cada datagrama según sean necesarios, similar a como ocurre con las opciones de IPv4.
- Esto resulta muy eficiente porque no será imprescindible transmitir campos fijos del encabezado que no en todos los casos son usados.

# CARACTERÍSTICAS Y VENTAJAS

## Encabezado flexible

- Existen siete encabezados de extensión estándares para IPv6.
- Estos encabezados son procesados en el mismo orden en que están en el datagrama por ello existe un orden recomendado para su utilización.

Nº	Nombre del encabezado	PRÓXIMO ENCABEZADO
1	Opciones de salto a salto	0
2	Opciones de destino (para los pasos intermedios)	60
3	De enrutamiento	43
4	De fragmentación	44
5	De autenticación	51
6	De encriptación	50
7	Opciones de destino (para el destino final)	60

# CARACTERÍSTICAS Y VENTAJAS

## Calidad de servicio a nivel de red

- Gracias a los campos CLASE de TRÁFICO y ETIQUETA DE FLUJO del encabezado base de IPv6, este protocolo es capaz de brindar calidad de servicio a nivel de red.
- El campo CLASE DE TRÁFICO se utiliza para establecer prioridades entre los paquetes.
- El campo ETIQUETA DE FLUJO identifica paquetes IPv6 con el mismo origen y con el mismo destino. Está antes de las direcciones para que los routers lo puedan analizar y realicen el enrutado por flujos.
- Los flujos no son más que conjuntos de paquetes con características comunes.
- Los paquetes correspondientes a los flujos reciben todos el mismo tratamiento.

# CARACTERÍSTICAS Y VENTAJAS

## Autoconfiguración

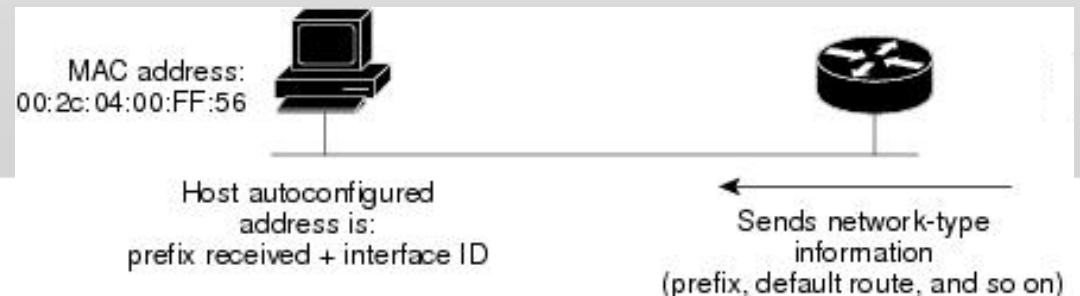
- IPv6 es capaz de realizar la autoconfiguración. Por ello se dice que es plug and play.
- Esto resulta extremadamente importante en el despliegue ya que facilita su implantación.
- Excepto para las direcciones de enlace, la autoconfiguración está definida solo para los hosts. Los routers deben usar configuración manual.
- Existen dos métodos fundamentales para la autoconfiguración:
  - Sin estado (Stateless) (RFC 4862)
  - Con estado (Stateful) (RFC 3315)

# CARACTERÍSTICAS Y VENTAJAS

## Autoconfiguración

### ■ Stateless:

- No se requiere ninguna configuración manual del host ni se precisa de servidores adicionales.
- El host genera su propia dirección al combinar su identificador de interfaz con los prefijos anunciados por los routers, ya sean direcciones de enlace local o globales.
- Los prefijos son anunciados por el router periódicamente y además en respuesta a solicitudes realizadas por los hosts.
- En ausencia del router, el host solo puede generar la dirección de enlace local. Esta es suficiente para lograr la comunicación entre dispositivos conectados al mismo enlace.



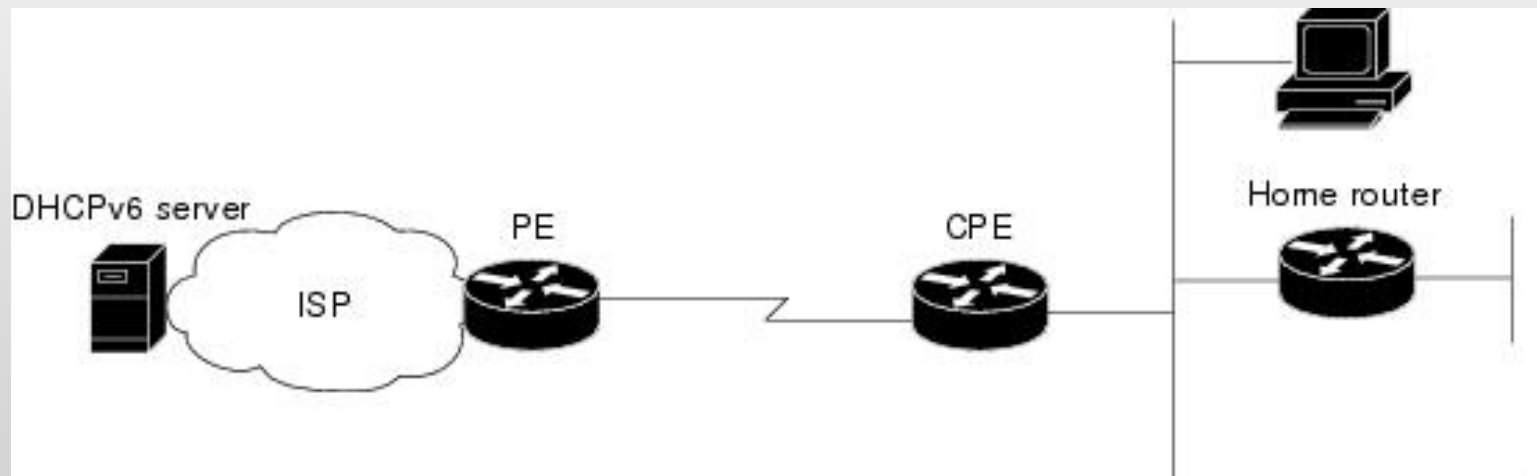


# CARACTERÍSTICAS Y VENTAJAS

## Autoconfiguración

### ■ Stateful:

- El host obtiene la dirección desde un servidor a través del protocolo DHCPv6.
- Estos servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host de manera similar a como funciona en IPv4.



# CARACTERÍSTICAS Y VENTAJAS

## **Soporte nativo de multicast**

- Soporta de manera intrínseca las transmisiones multicast.
- En la caso de IPv4, se encuentra implementado mediante parches usando el protocolo IGMP (Internet Group Management Protocol).

# CARACTERÍSTICAS Y VENTAJAS

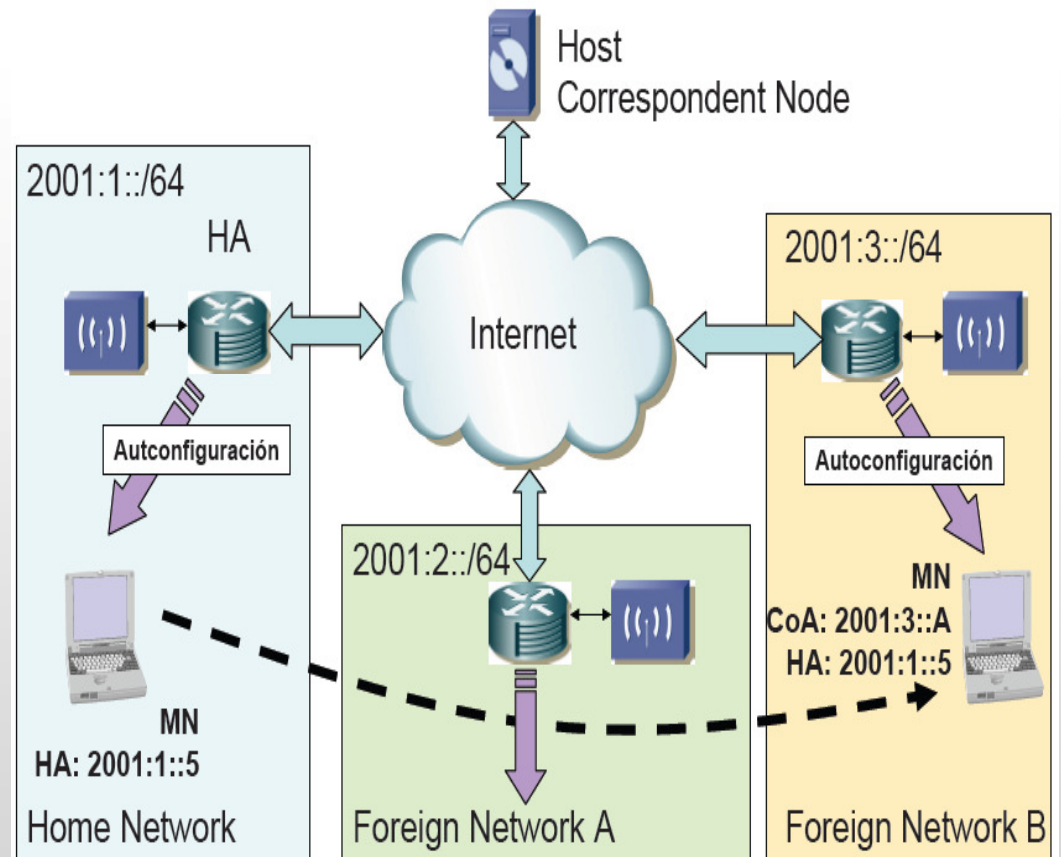
## Soporte nativo para la movilidad

- IPv6 proporciona movilidad ya que garantiza que se pueda alcanzar un host aunque este se esté moviendo por Internet. La diferencia con IPv4 es que lo hace de manera nativa y que utiliza mecanismos más eficientes y robustos. La RFC 3775 aborda el soporte para la movilidad en IPv6.

# CARACTERÍSTICAS Y VENTAJAS

## Soporte nativo para la movilidad

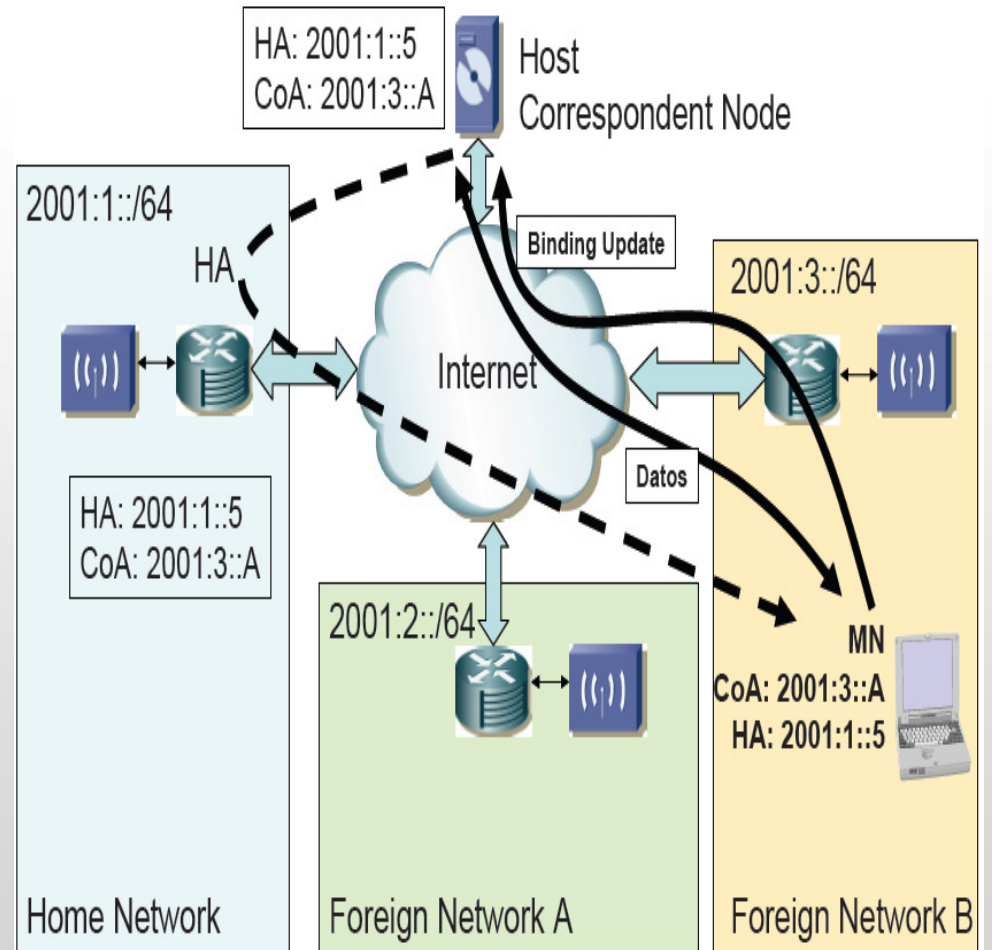
- Mientras el nodo se encuentra en su red (Home Network) tiene asignada una dirección IP conocida como Home Address y los paquetes serán encaminados hacia esa dirección utilizando los mecanismos tradicionales de ruteo.
- Gracias a los mecanismos de autoconfiguración, cuando el nodo se desplaza hacia otra red adquiere una nueva dirección conocida como Care of Address que contiene el prefijo de esta nueva red.



# CARACTERÍSTICAS Y VENTAJAS

## Soporte nativo para la movilidad

- Seguidamente debe informar su nueva dirección al Home Agent (ubicado en la Home Network) para que establezca una asociación entre la Home Address y la Care of Address. Este proceso es conocido como Binding.
- A partir de este momento, el Home Agent redireccionará todos los paquetes dirigidos al host móvil hacia su nueva dirección.
- De esta manera se logra que el movimiento del host sea transparente para las aplicaciones de niveles superiores.



# CARACTERÍSTICAS Y VENTAJAS

## Soporte nativo para la movilidad

- El nodo con el que se comunica el nodo móvil se conoce como nodo correspondiente. Si este nodo posee habilitada la capacidad de movilidad, entonces se puede utilizar un ruteo optimizado y no hay necesidad del Binding.
- En este caso el nodo móvil envía su Care of Address al nodo correspondiente por lo que no hay necesidad del Home Agent.

# CARACTERÍSTICAS Y VENTAJAS



## Mejoras en la seguridad

- Incorporación de la autenticación y la encriptación en la capa IP mediante el uso de las cabeceras de extensión.
- Soporta IPsec (IP security) de manera nativa. IPSec no es más que un conjunto de protocolos que se encargan de ofrecer seguridad a las redes IP a nivel de red. Es capaz de brindar:
  - Cifrado de los datos transmitidos para lograr privacidad.
  - Chequeo de la integridad de los mensajes para asegurar que no han sido cambiados en el camino.
  - Protección contra algunos tipos de ataque.
  - Posibilidad de que los dispositivos negocien los algoritmos de seguridad y las llaves requeridas.
- En IPv6 las redes son más seguras y robustas extremo a extremo que las que ofrece IPv4 con el uso del NAT. No hay necesidad de usar el NAT.

# POLÍTICAS SOBRE DIRECCIONES IPV6

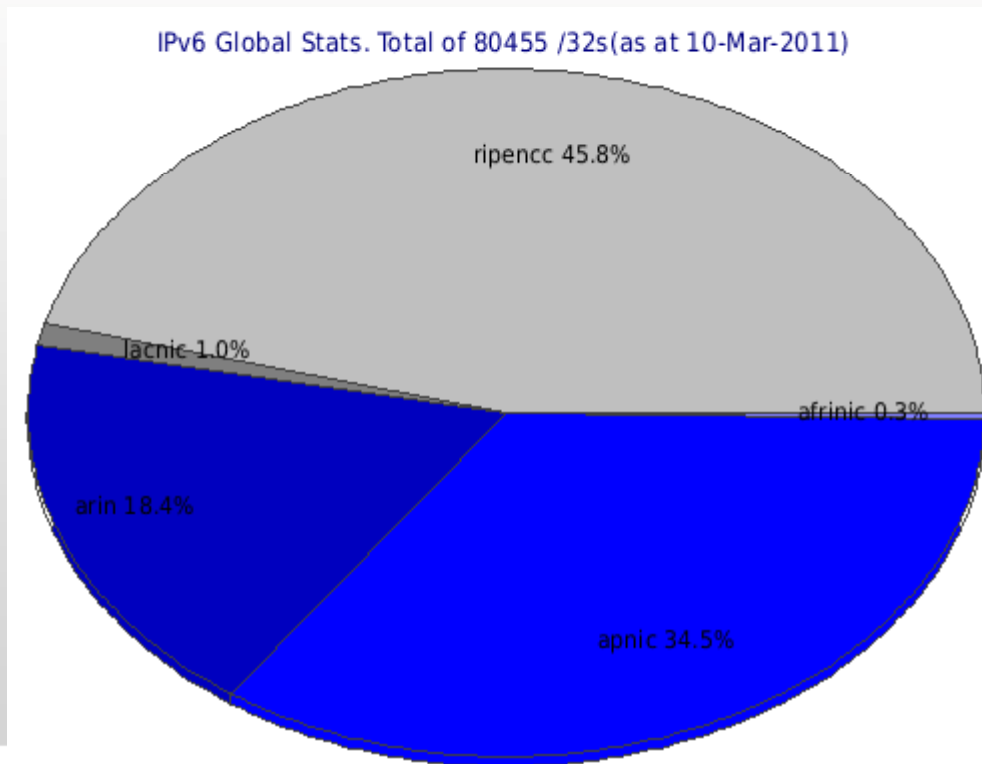


- El espacio global de direcciones unicast que IANA puede adjudicar a los RIRs es 2000::/3.
- Específicamente a LACNIC se le han asignado 2 bloques:
  - 2001:1200::/23
  - 2800:0000::/12
- LACNIC posee algunas políticas para la asignación y uso posterior de los bloques de direcciones que se asigna a los ISP:
  - El tamaño mínimo de adjudicación de un ISP es /32.
  - Los ISP deberán asignar a sus entidades correspondientes /48, excepto para suscriptores muy grandes.
  - Algunas entidades recibirán asignaciones de /64 cuando se conoce que una y solo una subred es necesaria.
  - Otras recibirán /128 cuando se conoce que uno y solo un dispositivo se está conectando.



## DESPLIEGE DE IPV6

- Actualmente existen más de 100 países que ha adoptado la nueva versión del protocolo IP.
- Los cinco RIRs existentes han asignado en total 80455 bloques IPv6 con máscara /32 hasta marzo del 2011.

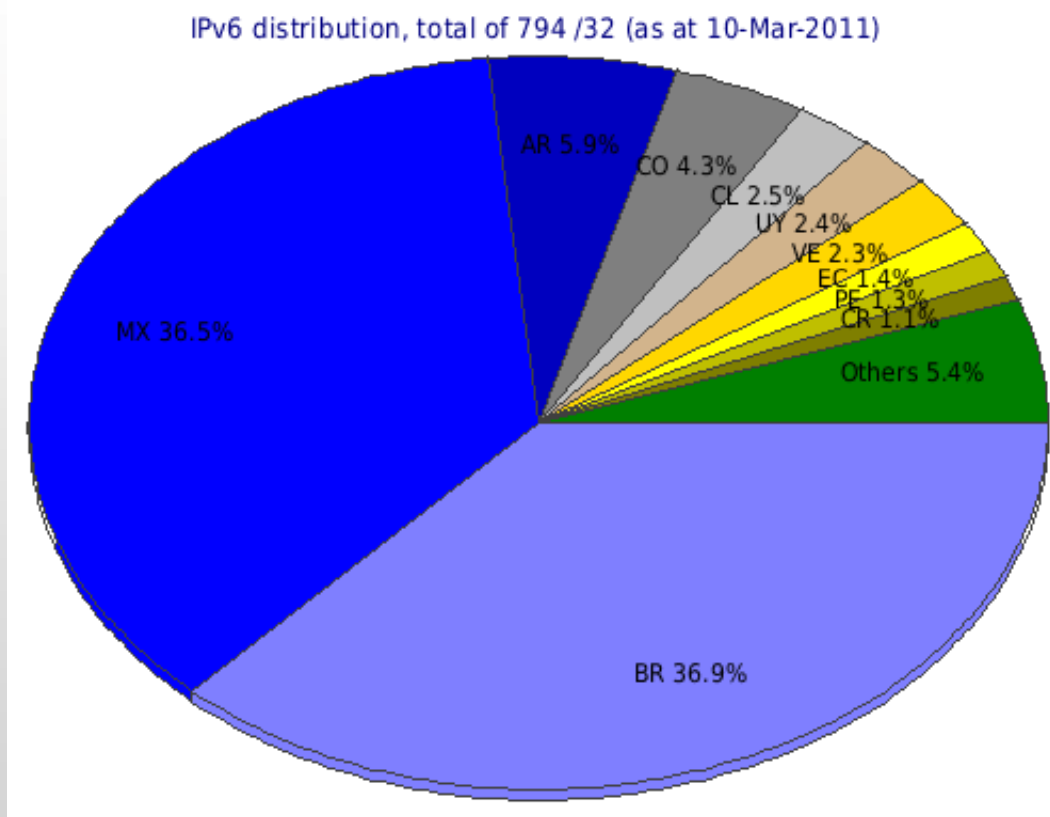


## DESPLIEGE DE IPV6

- En la actualidad existen numerosos productos comerciales y redes nativas IPv6 para uso académico y de investigación alrededor de todo el mundo, así como múltiples proyectos internacionales de interoperabilidad basados en este protocolo.

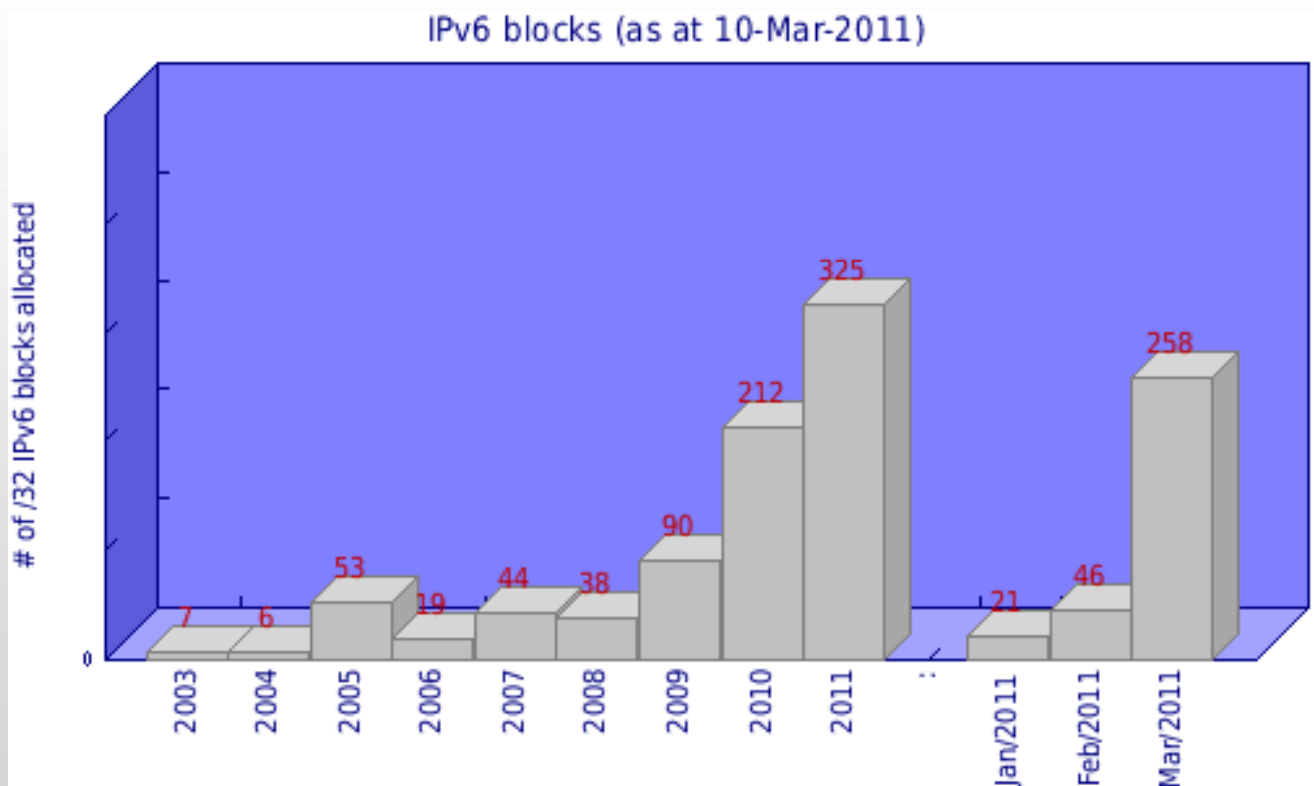
## DESPLIEGE DE IPV6

- En el caso de LACNIC hasta marzo de 2011 han sido asignados 794 bloques de direcciones IPv6 con /32 a lo países latinoamericanos.



## DESPLIEGE DE IPV6

- Este gráfico muestra el número de bloques de direcciones IPv6 con /32 asignadas por LACNIC en la región.



## DESPLIEGE DE IPV6

- En la región de Latinoamérica, los países con mayor actividad relacionada con el despliegue de IPv6 son Brasil, México, Argentina, aunque existen otros países que también han realizado trabajos relacionados con el tema.
- Un ejemplo de ello lo constituye la UNAM (Universidad Nacional Autónoma de México) que cuenta con IPv6 nativo en algunos segmentos de red desde el mes de junio de 1999.
- Actualmente se trabaja en implementar ambas versiones del IP en forma nativa desde el backbone hasta el nivel de acceso en gran parte de RedUNAM, y se busca ya tener una conexión IPv6 nativa por algún ISP mexicano.
- RedUNAM ofrece servicios de IPv6 para algunas facultades y escuelas de la propia UNAM y de otras universidades que se han conectado por medio de túneles IPv6 sobre IPv4.

## DESPLIEGE DE IPV6

- En Cuba comenzaron las actividades relacionadas con IPv6 desde el 2003 cuando se constituyó el Grupo de Trabajo.
- En el 2004 se crea y se publica el portal IPv6 de Cuba y se da a conocer la existencia del Grupo de Trabajo en una reunión de LACNIC.
- En la actualidad en el portal IPv6 se puede obtener una gran cantidad de información actualizada.
- En septiembre de 2010 se crea por el MIC el Grupo de Recursos de Internet que tiene entre sus objetivos trazar la estrategia sobre la Introducción del IPv6 en Cuba.

## DESPLIEGE DE IPV6

- LACNIC ha entregado un total de 5 bloques de direcciones IPv6 a Cuba hasta la actualidad.

Entidad	Bloque IPv6	Fecha de asignación
CITMATEL	2001:1340::/32	6 de abril de 2005
ETECSA DATOS	2001:1358::/32	29 de junio de 2005
ETECSA NAP	2001:13c8::/32	18 de agosto de 2005
SITRANS	2800:230::/32	4 de junio de 2008
INFOMED	2800:360::/32	29 de mayo de 2009

- De estos cinco bloques, actualmente solo visibles desde Internet los tres primeros.

## DESPLIEGE DE IPV6

- Alrededor de todo el mundo se están realizando múltiples esfuerzos para fomentar la adopción del protocolo IPv6.
- En ejemplo evidente es el día Mundial de IPv6 que es hoy 8 de Junio del 2011.
- La ISOC (Internet Society) es la encargada de llevar a cabo la coordinación y comunicación necesaria para las actividades que se realizarán este día.
- Esta organización se encarga de brindar orientación relacionada con los estándares, educación y políticas de Internet. Su misión es asegurar el desarrollo, evolución y uso de Internet para el beneficio de todas las personas del mundo.



## DESPLIEGE DE IPV6



- Este día se realizarán múltiples pruebas en todo el mundo con el objetivo de acelerar la adopción generalizada de IPv6 por parte de los proveedores de servicios de red, fabricantes, vendedores, compañías web y otros.
- Las pruebas consistirán, en su mayoría, en la publicación de sitios web soportados sobre IPV6. De esta manera, se permitirá que los hosts que tengan habilitado IPv6, puedan navegar por Internet de igual manera a como lo hacen utilizando IPv4.
- Varios grandes proveedores de contenidos se han comprometido a ofrecer todos sus servicios, tanto sobre IPv4 como sobre IPv6 durante todo este día.
- Entre los que se han comprometido a participar en ese experimento se encuentran Facebook, Google, Yahoo, Cisco, Juniper y otros.

## PREPARACIÓN PARA LA INTRODUCCIÓN DE IPV6

- Para la adecuada introducción de IPv6 es importante conocer la metodología descrita en la Resolución 156 / 2008 del MIC.
- Esta metodología consta de tres etapas para la introducción de IPv6 en el país.
- En este momento se encuentra en revisión.

# PREPARACIÓN PARA LA INTRODUCCIÓN DE IPV6

- A la hora de introducir IPv6 en una red se deben seguir los siguientes pasos generales:
  - Realizar un inventario del equipamiento de la red
  - Solicitar un bloque de direcciones IPv6
  - Elaborar un plan de direccionamiento
  - Configurar el equipamiento necesario para la transición
  - Implementar los servicios básicos
  - Implementar otros servicios
  - Implementar los mecanismos de seguridad
  - Anunciar el bloque de direcciones IPv6

## PREPARACIÓN PARA LA INTRODUCCIÓN DE IPV6

- Es muy importante realizar un inventario del equipamiento de red para detectar si existe algún equipo que no sea compatible con IPv6 y pueda ser upgradeado o si es necesario adquirir nuevo equipamiento (inversiones).
- De ser necesario adquirir nuevo equipamiento se debe tener en cuenta la Resolución 140 / 2008 del MIC que establece que todo el equipamiento importado a partir de enero de 2009 debe ser compatible con IPv6.

## PREPARACIÓN PARA LA INTRODUCCIÓN DE IPV6

- Para obtener algún bloque de direcciones IP (tanto IPv4 como IPv6) así como un ASN directamente de LACNIC es importante registrarse por la metodología descrita en la Resolución 138 / 2008 del MIC.
- En esta resolución se explica que primero se debe enviar una carta de solicitud a la DRN .
- Luego de aprobada por la DRN (Dirección de Regulaciones y Normas) dicha solicitud debe descargarse del sitio de LACNIC el formulario correspondiente y enviarse por correo a LACNIC.
- Una vez aprobada la solicitud del recurso por LACNIC, será necesario firmar un contrato y hacer un pago referente al registro de dicho recurso.
- Sin embargo, como parte de las acciones que LACNIC lleva a cabo para que el nuevo protocolo pueda ser desplegado en la región, los bloques IPv6 no tienen costo alguno para todos aquellos que ya posean bloques IPv4 asignados por el RIR.

## PREPARACIÓN PARA LA INTRODUCCIÓN DE IPV6

- Los sistemas críticos de Internet deben ser los primeros en implementarse. Estos son: DNS, correo y Web.
- Con esto se logrará la visibilidad de los portales web en ambos protocolos (IPv4 e IPv6) y se permitirá la navegación tanto para IPv4 como para IPv6.
- Los mecanismos de seguridad deben ser implementados de la misma forma que se hace para IPv4. Ejemplo: se deben agregar todas las ACLs necesarias para proteger la red.

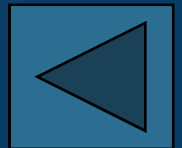
## PREPARACIÓN PARA LA INTRODUCCIÓN DE IPV6



- Por último debe realizarse el anuncio del bloque de direcciones IPv6 para que sea visible desde Internet.
- El anuncio de un bloque de direcciones IPv6, se puede hacer por medio de un ASN propio de la red, si este se tiene o entregándole el bloque IPv6 al NAP de ETECSA.
- Este anuncio, de cualquier manera, debe ser realizado por el NAP, ya sea por ASN o por direcciones IPv6 propias de la red solicitante.
- El anuncio deben solicitarlo los ISP a los cuales les fue entregado un bloque /32 por LACNIC.
- Las organizaciones a los cuales les fueron entregados los bloques /48 por parte de los ISP no deben encargarse de esta solicitud, pues forman parte del bloque /32 entregado al ISP por LACNIC.

# Parte 2. Arquitectura del direccionamiento en IPv6

- Plan de direccionamiento IPv6
- Esquema de numeración de subredes





# PLAN DE DIRECCIONAMIENTO

- Repasando algunos conceptos:

- **Red:** se refiere a una colección de subredes en la cual todos los equipos que la integran pueden intercambiar datos entre sí.
- **Subred:** es el conjunto de dispositivos o equipos que comparten un medio físico de transmisión y utilizan técnicas de comunicación comunes.
- **Protocolos de Comunicación:** definen las reglas para la transmisión y recepción de la información entre los nodos de la red, de modo que para que dos nodos se puedan comunicar entre si es necesario que ambos empleen la misma configuración de protocolos.
  1. Protocolos de los niveles físicos y de enlace: niveles 1 y 2 del modelo OSI (definen las funciones asociadas con el uso del medio de transmisión: envío de los datos a nivel de bits y trama, y el modo de acceso de los nodos al medio.
  2. Protocolos de los niveles de red y transporte: niveles 3 y 4 del modelo OSI (se encargan básicamente del encaminamiento de la información y de garantizar una comunicación extremo a extremo libre de errores. Ejemplos: IP, TCP y UDP.

# PLAN DE DIRECCIONAMIENTO

## The five-layer TCP/IP model

### 5. Application layer

DHCP \* DNS \* FTP \* Gopher \* HTTP \* IMAP4 \* IRC \* NNTP \* XMPP \* POP3 \*  
SIP \* SMTP \* SNMP \* SSH \* TELNET \* RPC \* RTP \* RTCP \* RTSP \* TLS/SSL \*  
SDP \* SOAP \* BGP \* PPTP \* L2TP \* GTP \* STUN \* NTP \* ...

### 4. Transport layer

TCP \* UDP \* DCCP \* SCTP \* RSVP \* ...

### 3. Network(Internet) Layer

IP (IPv4 \* IPv6) \* IGMP \* ICMP \* OSPF \* ISIS \* IPsec \* ARP \* RARP \* RIP \* ...

### 2. Data link layer

802.11 \* ATM \* DTM \* Token Ring \* Ethernet \* FDDI \* Frame Relay \* GPRS \*  
EVDO \* HSPA \* HDLC \* PPP \* ...

### 1. Physical layer

Ethernet physical layer \* ISDN \* Modems \* PLC \* SONET/SDH \* G.709 \*  
Optical Fiber \* WiFi \* WiMAX \* Coaxial Cable \* Twisted Pair \* ...

# PLAN DE DIRECCIONAMIENTO

## ■ Direccionamiento y encaminamiento:

- Algunos protocolos definen otra dirección (dirección lógica) independiente de la topología de la red. Esta nueva dirección, cuyo **plan de direccionamiento** es fijado por el diseñador de la red, permite la interconexión entre múltiples redes, con distintas topologías entre sí, y por tanto con distintos formatos de direcciones físicas. Este es el caso de TCP/IP, donde, para que un nodo pueda comunicarse con otro usando este juego de protocolos es necesario que ambos tengan direcciones IP.
- Esta dirección IP de los nodos es una dirección lógica que es independiente de la tarjeta y de la topología de la red, y que es única dentro de cada red global. Por tanto, para hacer posible la comunicación con el protocolo TCP/IP, cada nodo deberá tener asignada una dirección única IP de acuerdo a un plan de direccionamiento IP de la red, previamente diseñado, de forma que en ningún caso la red global tenga direcciones duplicadas entre nodos.

## PLAN DE DIRECCIONAMIENTO

- Es importante además, revisar algunos conceptos sobre los sistemas numéricos.
- Existen muchos sistemas numéricos. Los más comunes son:

Sistema	Base	Dígitos
2	Binario	0,1
8	Octal	0,1,2,3,4,5,6,7
10	Decimal	0,1,2,3,4,5,6,7,8,9
16	Hexadecimal	0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

# PLAN DE DIRECCIONAMIENTO

- Para representar un número se pueden utilizar dos notaciones:

- Notación posicional

$$(a_{n-1}a_{n-2} \dots a_1a_0)_r$$

- Ejemplo:  $(387)_{10}$   $r = 10$  ,  $n = 3$

- Notación polinomial

$$\sum_{i=0}^{n-1} a_i r^i = a_{n-1} r^{n-1} + a_{n-2} r^{n-2} + \dots + a_1 r^1 + a_0 r^0$$

- Ejemplo:  $(387)_{10} = 3 \cdot 10^2 + 8 \cdot 10^1 + 7 \cdot 10^0$

## PLAN DE DIRECCIONAMIENTO

- Para algunas conversiones entre sistemas numéricos se usa la notación polinomial.
- Ejemplo: Hexadecimal  $\longrightarrow$  Decimal , Binario  $\longrightarrow$  Decimal

$$(B2A)_{16} = (11*16^2 + 2*16^1 + 10*16^0)_{10}$$

$$(B2A)_{16} = (11*256 + 2*16 + 10)_{10}$$

$$(B2A)_{16} = (2858)_{10}$$

$$(11011)_2 = (1*2^4 + 1*2^3 + 0*2^2 + 1*2^1 + 1*2^0)_{10}$$

$$(11011)_2 = (16 + 8 + 0 + 2 + 1)_{10}$$

$$(11011)_2 = (27)_{10}$$

## PLAN DE DIRECCIONAMIENTO

- Para convertir del sistema decimal a otro cualquiera, debemos realizar divisiones sucesivas por la base del sistema al cual se quiere convertir.
- Luego se toman los residuos, empezando de atrás hacia adelante.

Ejemplo 1: convertir  $(25)_{10}$  a base 2      Ejemplo 2: convertir  $(25)_{10}$  a base 16

$$\begin{array}{ll} 25:2 = 12 & r = 1 \\ 12:2 = 6 & r = 0 \\ 6:2 = 3 & r = 0 \\ 3:2 = 1 & r = 1 \\ 1:2 = 0 & r = 1 \end{array} \quad \uparrow$$

Por tanto,  $(25)_{10} = (11001)_2$

$$\begin{array}{ll} 25:16 = 1 & r = 9 \\ 1:16 = 0 & r = 1 \end{array} \quad \uparrow$$

Por tanto,  $(25)_{10} = (19)_{16}$

## PLAN DE DIRECCIONAMIENTO

- Para convertir de Binario a Hexadecimal se agrupan los dígitos de 4 en cuatro.

Ejemplo:  $(101\ 1101\ 1110)_2$  a base 16

$\underbrace{101}_5\ \underbrace{1101}_D\ \underbrace{1110}_E$

Por tanto,  $(101\ 1101\ 1110)_2 = (5ED)_{16}$



## PLAN DE DIRECCIONAMIENTO

- Para convertir de Hexadecimal a Binario se toma cada dígito y se convierte en 4 dígitos.

Ejemplo:  $(3F45)_{16}$  a base 2

$\begin{array}{cccc} \underbrace{3} & \underbrace{F} & \underbrace{4} & \underbrace{5} \\ 0011 & 1111 & 0100 & 0101 \end{array}$

Por tanto,  $(3F45)_{16} = (0011 \ 1111 \ 0100 \ 0101)_2$

## PLAN DE DIRECCIONAMIENTO

- La asignación y utilización de las direcciones IPv6 se debe realizar en correspondencia con la estructura de Red IPv4 que hoy existe, teniendo en cuenta posibles alternativas de crecimiento (tanto en infraestructura como en servicios).
- Además se debe tomar como marco de referencia las recomendaciones del Registro Regional (LACNIC) expresadas en las políticas aprobadas para la Región (<http://www.lacnic.net/sp/politicas>) y otras especificaciones de carácter público como las RFC 2373, 2450, 3177, 3587, 4029 y otras.
- A diferencia del protocolo IPv4, el direccionamiento en IPv6 está orientado a las subredes.

# PLAN DE DIRECCIONAMIENTO

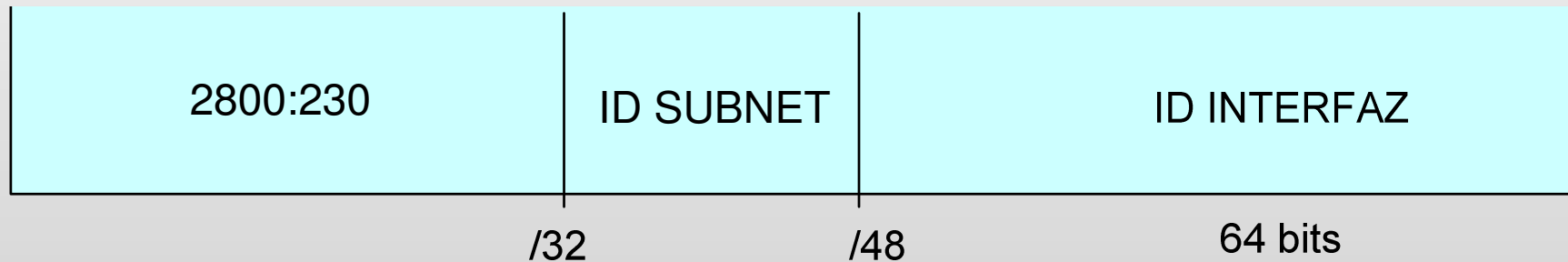
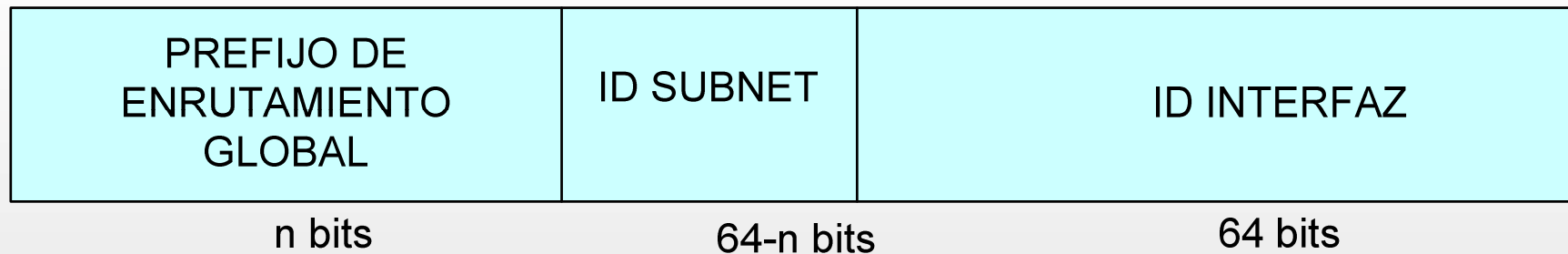
- “Un buen plan de direccionamiento es lo mas complejo y requiere muy buen conocimiento de la red. Además, también de los equipos, de los usuarios, de detalles del software, etc” J. Palet
- Se propone la formulación de un plan de direccionamiento para direcciones IPv6 que sea:
  - amigable: de fácil implementación y entendimiento, permitiendo una plataforma sencilla para los administradores sucesores.
  - confiable: sin incongruencias y ajustado a las políticas globales y regionales de asignación, intentando garantizar equidad.
  - flexible: que disponga de un sistema de asignación tolerante evitando la sobrecarga asociada a su gestión.
  - perdurable: no ponga en riesgo la estructura del bloque de direcciones IPv6, subsistiendo por una suma de años

# PLAN DE DIRECCIONAMIENTO

- Los objetivos que se persiguen con un plan de direccionamiento son:
  - Fomentar el cuidado del espacio de direcciones IPv6 y promover su buen uso, a pesar de su amplia definición.
  - Construir una formula estándar, coherente y sencilla que sirva para la delegación de direcciones a entidades o dependencias relacionados de la red que pudieran aparecer en el tiempo.
  - Definir políticas que deberán cumplir los nodos a los cuales les sea asignado un espacio de direcciones IPv6.
  - Proponer modelos de asignación de direcciones IPv6 para entidades que reciban bloques de direcciones IPv6 (opcional).

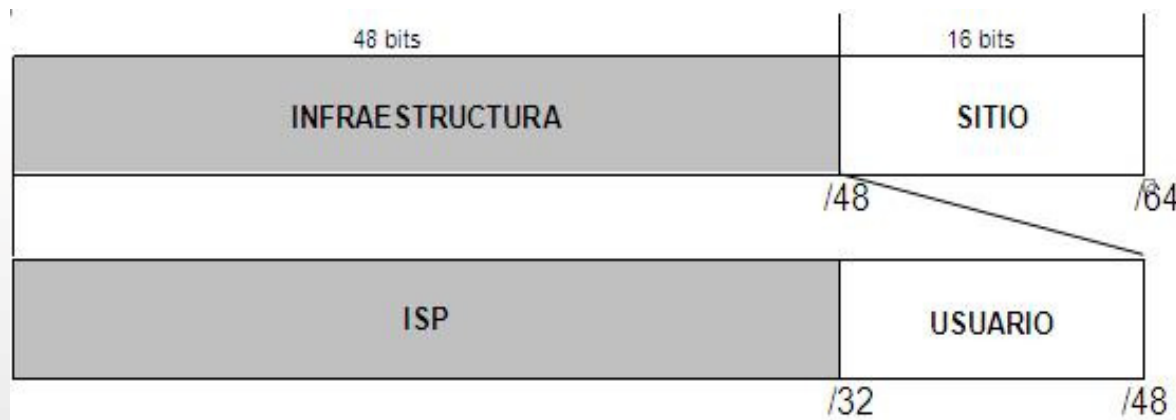
## PLAN DE DIRECCIONAMIENTO

- Para comprender mejor lo que se explicará a continuación repasemos el formato de direcciones unicast globales.



# PLAN DE DIRECCIONAMIENTO

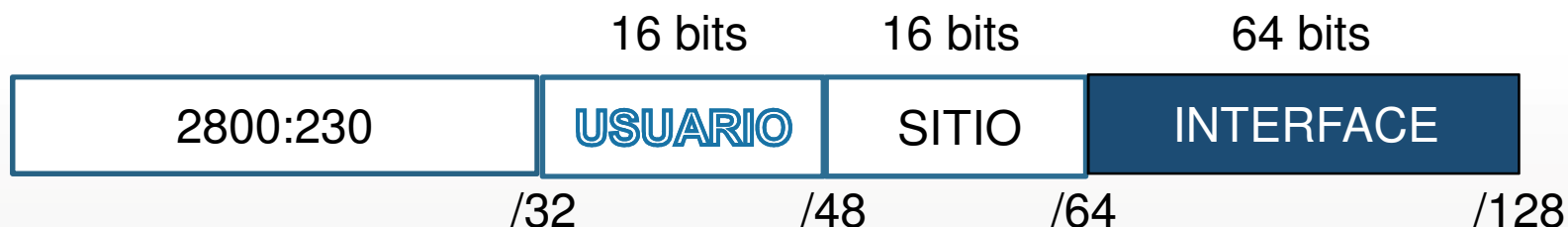
- Estructura de la dirección IPv6:



- Ejemplo: 2800:230::/32
- La política de asignación de LACNIC define asignar bloques de direcciones ::/32 a registros locales o ISP y estos a su vez asignaran como mínimo a los usuarios finales /48, destinándose a los sitios 16 bits, pudiendo asignar  $2^{16} = 65,536$  direcciones de subred o lo que es lo mismo 65,536 /64 direcciones LAN.

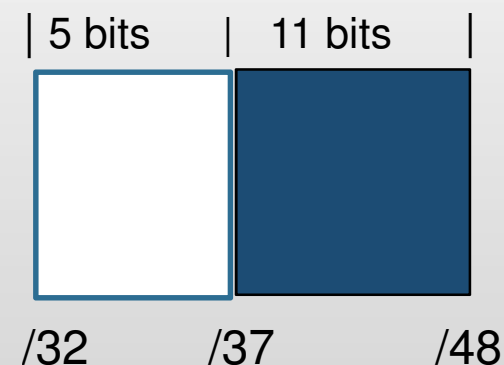
# PLAN DE DIRECCIONAMIENTO

- Ejemplo de asignación a ISP o a LIR



- Para asignaciones a ISP, en correspondencia con las Políticas aprobadas por LACNIC, las asignaciones son de un /32, por lo que los ISP pueden direccionar solo 16 bit en el campo USUARIO.

**En el caso en que se necesite asignar direcciones por un Proveedor que tiene 1600 redes y piense en un crecimiento de 500 redes más en los próximos 3 años, entonces pudiera ser :**



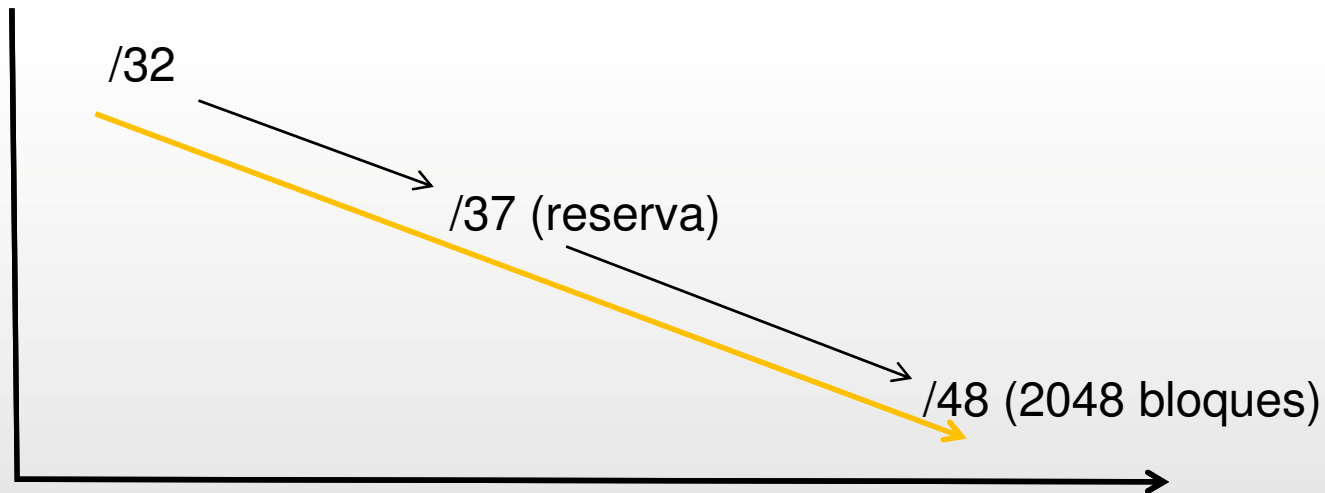
Donde:

R (5 bit): campo de 5 bit utilizado para reserva de crecimiento futuro.

M (11 bit): este campo de 11 bit será utilizado para el direccionamiento de las subasignaciones de bloques ::/48

# PLAN DE DIRECCIONAMIENTO

Niveles de asignación



- Estos usuarios finales a su vez podrán direccionar 16 bits, lo que equivale a disponer cada uno de 65, 536 /64
- En total la red podrá disponer de 134, 217 728 /64 u equipos conectados a la red desde el punto de vista del direccionamiento.



# PLAN DE DIRECCIONAMIENTO

- Conociendo la estructura de USUARIOS FINALES el direccionamiento para las Redes sería:

R	NLA1 (11 bits)	HexaDec	Prefijo nodo
00000	00000000000	0x0000	2800:230:0000::/48 nodo 1
00000	00000000001	0x0001	2800:230:0001::/48 reservado nodo 1
00000	00000000010	0x0002	2800:230:0002::/48 nodo 2
00000	00000000011	0x0003	2800:230:0003::/48 reservado nodo 2
00000	00000000100	0x0004	2800:230:0004::/48 nodo 3
00000	00000000101	0x0005	2800:230:0005::/48 reservado nodo 3
00000	00000000110	0x0006	2800:230:0006::/48 nodo 4
00000	00000000111	0x0007	2800:230:0007::/48 reservado nodo 4
...			
00000	01111111110	0x03FE	2800:230:03FE::/48 nodo 511
00000	01111111111	0x03FF	2800:230:03FF::/48 reservado nodo 511
00000	10000000000	0x0400	2800:230:0400::/48 nodo X

Dec.	Bin.	Hexa.
0	0	0
1	1	1
2	10	2
3	11	3
4	100	4
5	101	5
6	110	6
7	111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

# PLAN DE DIRECCIONAMIENTO

- Expresado de en formato binario sería:

0010 1000 0000 0000:0000 0010 0011 0000:xxxx xxxx xxxx xxxx /48

0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0000::/48	2800:230::/48	nodo 1
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0001::/48	2800:230:1::/48	R. nodo 1
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0010::/48	2800:230:2::/48	nodo 2
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0011::/48	2800:230:3::/48	R. nodo 2
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0100::/48	2800:230:4::/48	nodo 3
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0101::/48	2800:230:5::/48	R. nodo 3
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0110::/48	2800:230:6::/48	nodo 4
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0111::/48	2800:230:7::/48	R. nodo 4
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 1000::/48	2800:230:8::/48	nodo 5
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 1001::/48	2800:230:9::/48	R. nodo 5
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 1010::/48	2800:230:a::/48	...
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 1011::/48	2800:230:b::/48	...
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 1100::/48	2800:230:c::/48	...
0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 1101::/48	2800:230:d::/48	...
0010 1000 0000 0000:0000 0010 0011 0000:0000 0 000 0000 1110::/48	2800:230:e::/48	...
0010 1000 0000 0000:0000 0010 0011 0000:0000 0 000 0000 1111::/48	2800:230:f::/48	...

.....

Dec.	Bin.	Hexa.
0	0	0
1	1	1
2	10	2
3	11	3
4	100	4
5	101	5
6	110	6
7	111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

# PLAN DE DIRECCIONAMIENTO

- Ejemplo: el direccionamiento para el NODO1 sería:

## BLOQUE 1

0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0000/48 NODO 1  
2800:230:0000/48 ó 2800:230::/48

## BLOQUE 2

0010 1000 0000 0000:0000 0010 0011 0000:0000 0000 0000 0001/48 R. NODO 1  
2800:230:0001/48 ó 2800:230:01::/48

16 bits

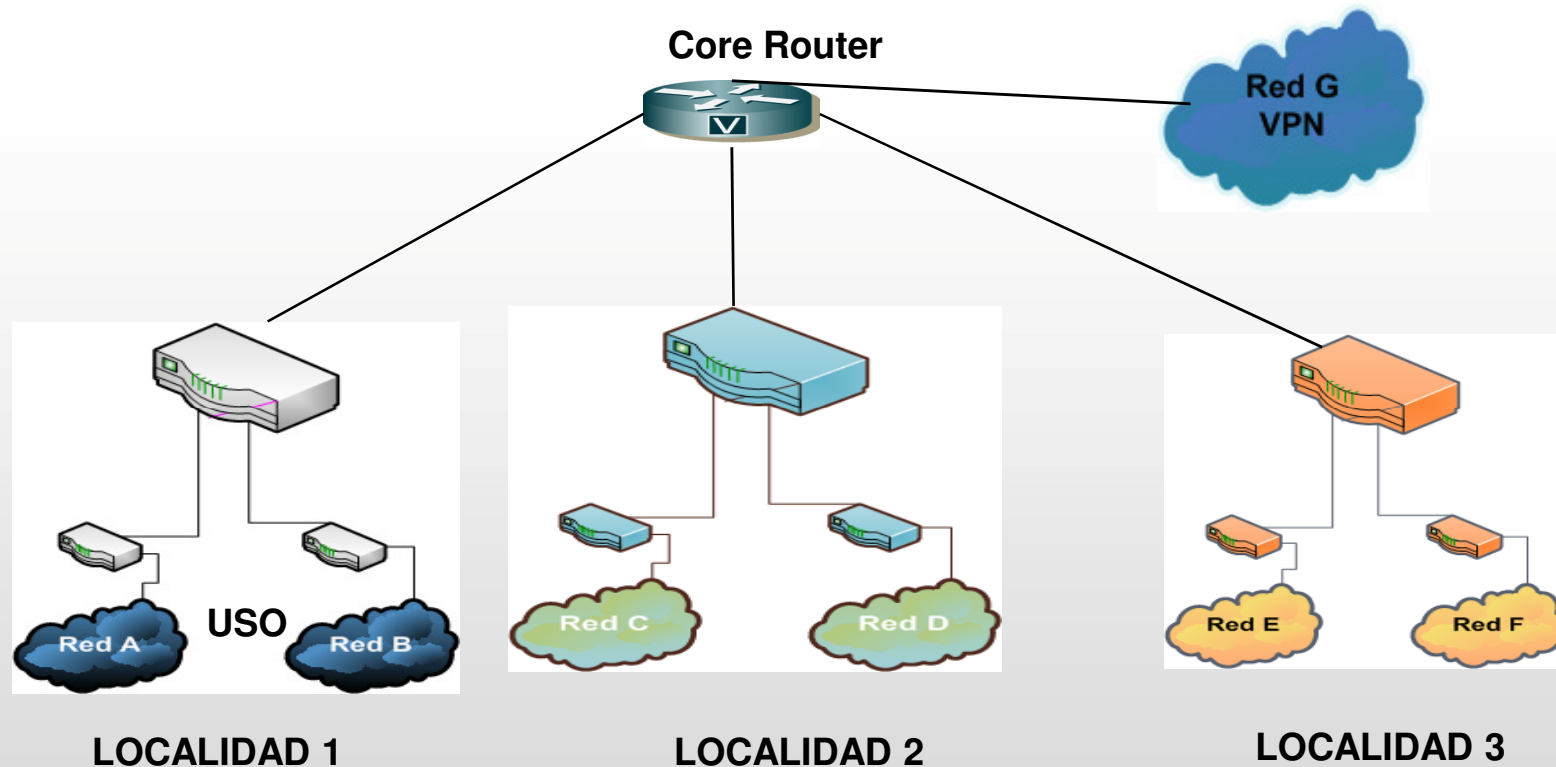
16 bits

2800:230:0000 0000 0000 0000:0000 0000 0000 0000::/64	2800:230::/64	subred 1
2800:230:0000 0000 0000 0000:0000 0000 0000 0001::/64	2800:230:0:1::/64	subred 2
2800:230:0000 0000 0000 0000:0000 0000 0000 0010::/64	2800:230:0:2::/64	subred 3
2800:230:0000 0000 0000 0000:0000 0000 0000 0011::/64	2800:230:0:3::/64	subred 4
2800:230:0000 0000 0000 0000:0000 0000 0000 0100::/64	2800:230:0:4::/64	subred 5
2800:230:0000 0000 0000 0000:0000 0000 0000 0101::/64	2800:230:0:5::/64	subred 6
2800:230:0000 0000 0000 0000:0000 0000 0000 0110::/64	2800:230:0:6::/64	subred 7
2800:230:0000 0000 0000 0000:0000 0000 0000 0111::/64	2800:230:0:7::/64	subred 8
2800:230:0000 0000 0000 0000:0000 0000 0000 1000::/64	2800:230:0:8::/64	subred 9
2800:230:0000 0000 0000 0000:0000 0000 0000 1001::/64	2800:230:0:9::/64	subred 10
2800:230:0000 0000 0000 0000:0000 0000 0000 1010::/64	2800:230:0:a::/64	subred 11
2800:230:0000 0000 0000 0000:0000 0000 0000 1011::/64	2800:230:0:b::/64	subred 12

Dec.	Bin.	Hexa.
0	0	0
1	1	1
2	10	2
3	11	3
4	100	4
5	101	5
6	110	6
7	111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

# PLAN DE DIRECCIONAMIENTO

EJEMPLO DE UNA ORGANIZACIÓN QUE RECIBE UN BLOQUE  $::/48$  DEL ISP



Definir cual subred será:

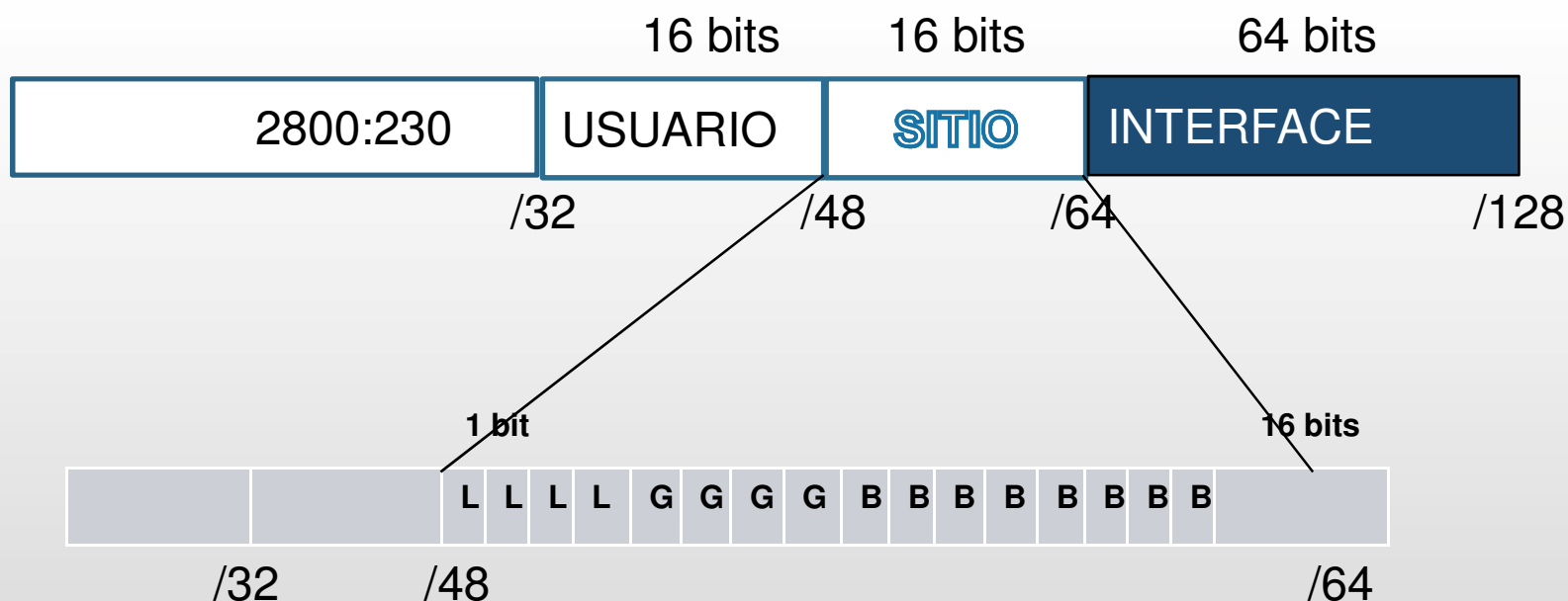
1. primaria
2. secundaria



Optimizar las tablas de rutas

## PLAN DE DIRECCIONAMIENTO

- Veamos cual pudiera ser la distribución del espacio de direcciones de esa organización :



Podemos estar direccionando hasta 16 bits, donde:

L.- pudiera definir una localidad ( $2^4$  bits)

G.- definir un tipo ( $2^4$  bits)

B.- definir cualquier otro tipo de asignación ( $2^8$  bits)

# PLAN DE DIRECCIONAMIENTO

Ejemplo No1.-

RED PRIMARIA: Localidad

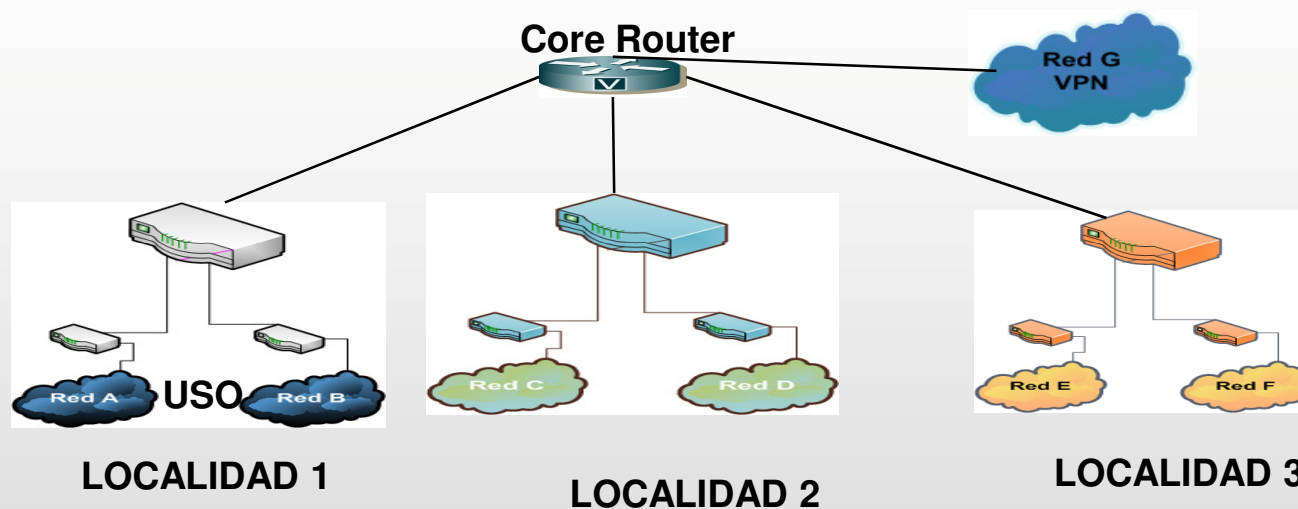
No. de Localidades: 3 grupos

Backbone: 1 grupo

Otras Redes (VPN): 1 grupo

Futuras Localidades: 2 grupos

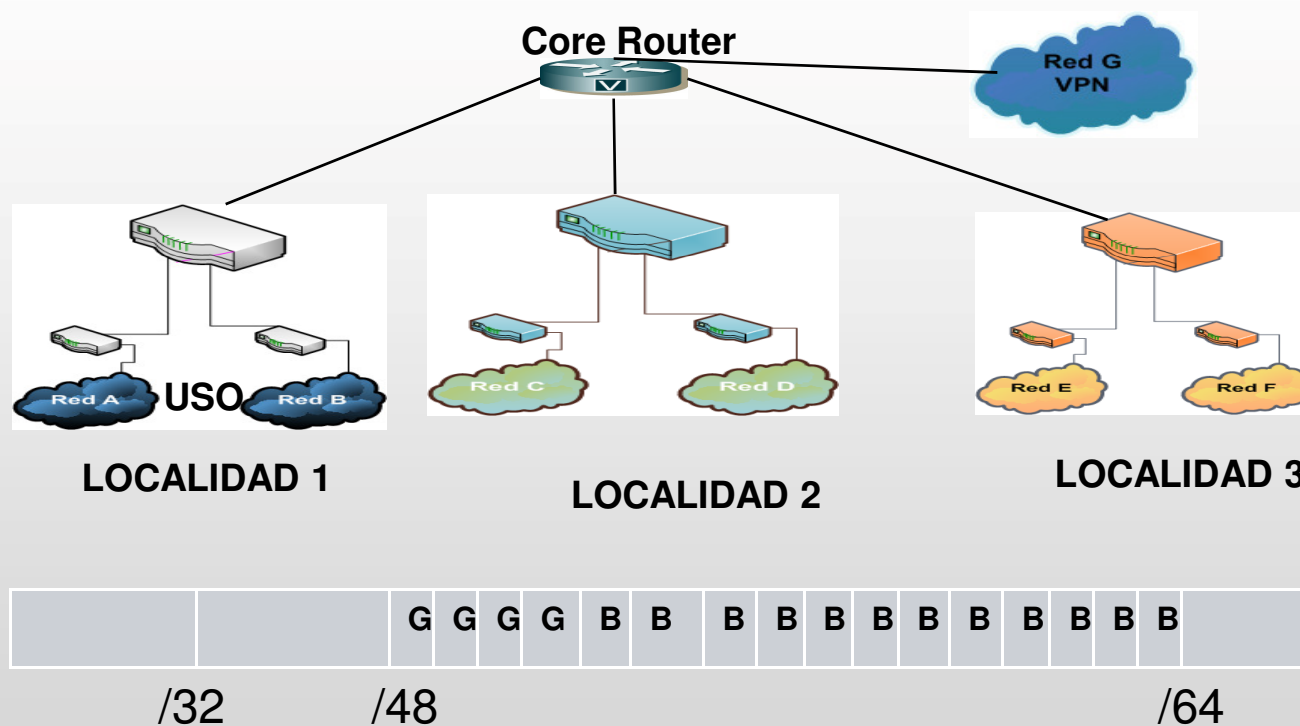
TOTAL: 7 grupos (subredes)



# PLAN DE DIRECCIONAMIENTO

## Ejemplo No2.- RED PRIMARIA: Uso

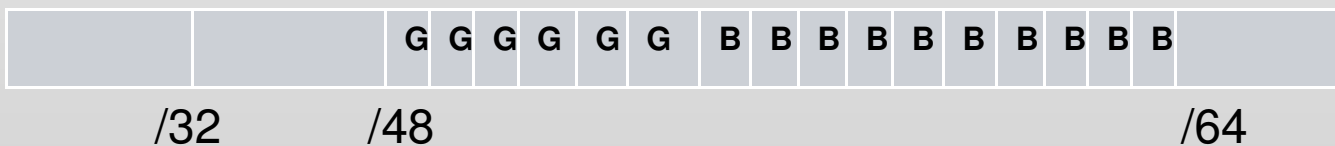
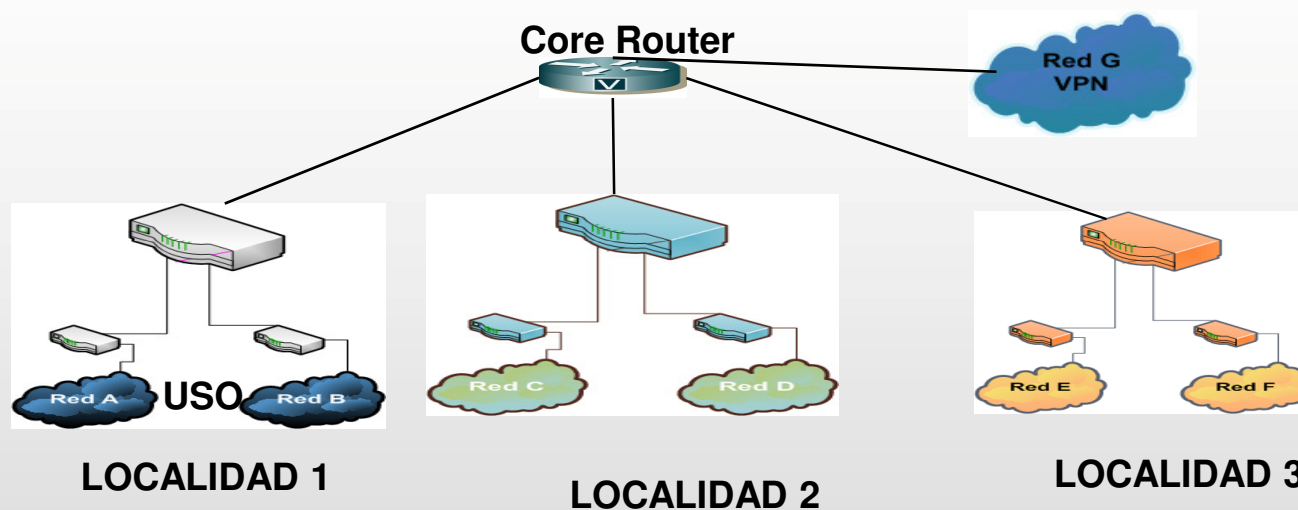
**No. por uso: 5 grupos**  
**Backbone: 1 grupo**  
**Futuros usos: 4 grupos**  
**TOTAL: 10 grupos (subredes)**



# PLAN DE DIRECCIONAMIENTO

Ejemplo No3.-  
RED PRIMARIA: Localidad

No. por LOCALIDAD: 16  
No. por USO: 15  
Backbone: 1 grupo  
TOTAL: 32 grupos (subredes)





# PLAN DE DIRECCIONAMIENTO

**Ejemplo No3.-**  
**RED PRIMARIA: PROVINCIA**

**PROVINCIA: 16**  
**MUNICIPIO: 168**  
**INFRAESTRUCTURA: 1**

1 bit

16 bits

	P	P	P	P	P	M	M	M	M	M	B	B	B	B	B	B	
--	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	--

No.	PROVINCIAS	CANT. MCPIO
1	PINAR DEL RÍO	11
2	ARTEMISA	11
3	MAYABEQUE	11
4	LA HABANA	15
5	MATANZAS	13
6	CIENFUEGOS	8
7	VILLA CLARA	13
8	SANCTI SPIRITUS	8
9	CIEGO DE AVILA	10
10	CAMAGUEY	13
11	LAS TUNAS	8
12	GRANMA	13
13	HOLGUIN	14
14	S. DE CUBA	9
15	GUANTANAMO	10
16	MCPIO ESPECIAL	1

# PLAN DE DIRECCIONAMIENTO



- Entonces podemos resumir que el **PLAN DE DIRECCIONAMIENTO** se debe plasmar en un documento de trabajo:

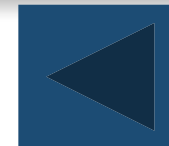


- En este documento se deben escribir los Objetivos.
- Las Políticas que se seguirán para las asignaciones.
- El modelo teórico que se utilizará.

- El desglose de las asignaciones.
- Recomendaciones de trabajo.
- Bibliografía utilizada

- En un documento excel, se llevará por la persona designada los bloques que se asignaran para garantizar que no se asigne un bloque dos veces.

# ESQUEMA DE NUMERACIÓN PARA SUBREDES

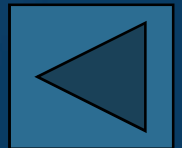


- **Política para la creación del esquema de numeración de las subredes.**
- Para la creación del esquema de numeración para las subredes del USUARIO1, comenzamos asignando a las subredes IPv4 ya configuradas subredes equivalentes en IPv6.

Prefijo de subred IPv4	Prefijo de subred IPv6 equivalente
172.16.0.0/24	2800:230::/64
192.168.100.0/24	2800:230:0:1::/64
10.10.0.0/24	2800:230:0:2::/64
191.207.15.0/24	2800:230:0:3::/64

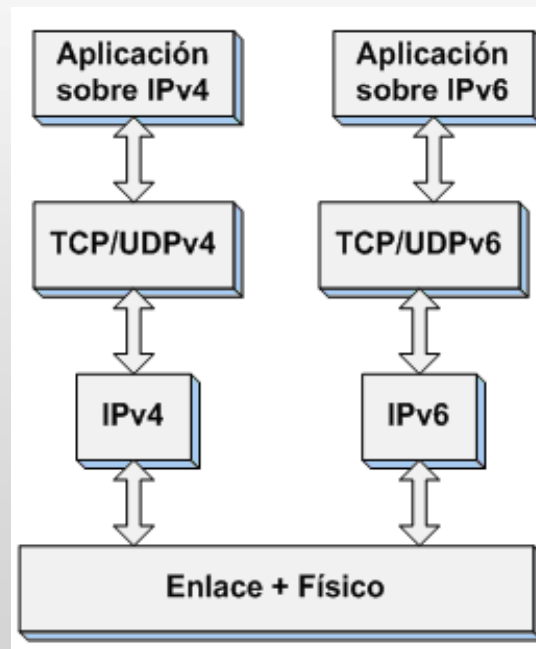
# Parte 3. Mecanismos de transición

- Dual stack
- Túneles
- Traductores



## DUAL STACK

- Es el método más simple para la introducción de IPv6.
- Significa mantener dos pilas de protocolos que trabajen paralelamente: una sobre IPv4 y la otra sobre IPv6.
- El dispositivo puede trabajar con ambas versiones y tener acceso tanto a los recursos IPv4 como IPv6.



## DUAL STACK

- Gracias a la doble pila, los hosts que la poseen pueden comunicarse con hosts IPv4 nativos y con hosts IPv6 nativos.
- Lo mismo sucede con los routers, que al poseer una doble pila, pueden encaminar paquetes tanto a hosts IPv4 como a hosts IPv6.
- Los nodos doble pila contienen tanto direcciones IPv4 como IPv6.
- Las direcciones IPv4 generalmente son obtenidas a través de un servidor DHCP.
- Las direcciones IPv6 pueden ser configuradas manualmente en las tablas del dispositivo o pueden ser obtenidas a través mecanismos de autoconfiguración propios de IPv6.

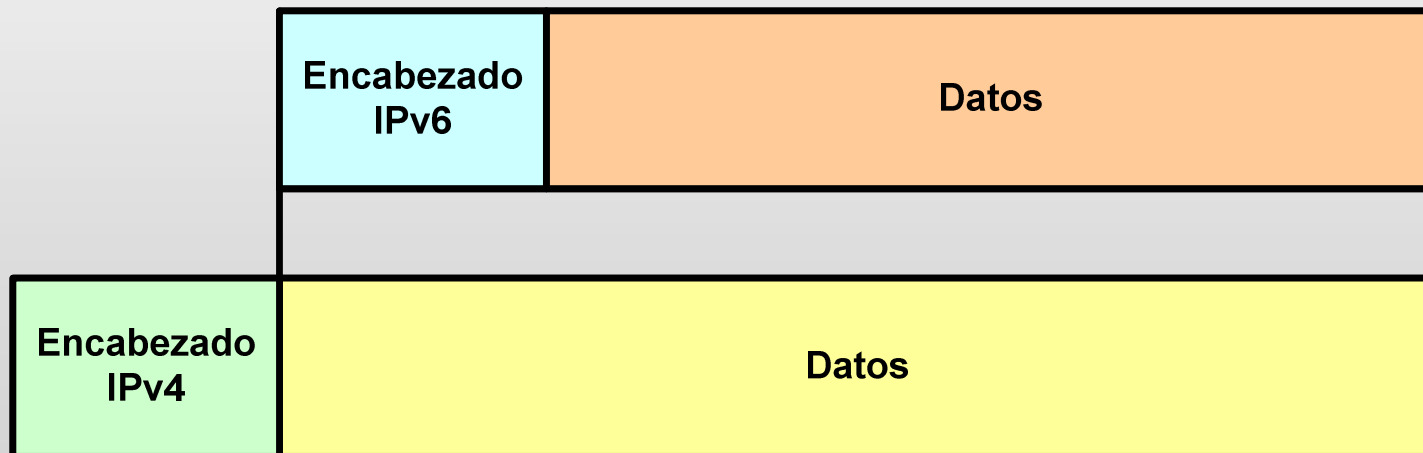
## DUAL STACK



- Este mecanismo no necesita de herramientas especiales para su implementación.
- El único paso necesario para hacer que un nodo sea doble pila es activar IPv6 en su sistema operativo.
- La tendencia actual de los fabricantes de sistemas operativos es activar IPv6 por defecto.
- Se dice que el backbone de cualquier red se convierte en doble pila cuando todos sus enrutadores son capaces de manejar ambos protocolos.
- Es necesario incluir los mecanismos de seguridad al igual que se hace para IPv4. Ejemplo: las reglas en los firewalls (adicionar las ACLs correspondientes para solo permitir el tráfico IPv6 deseado, al igual que ocurre con IPv4).

# TÚNELES

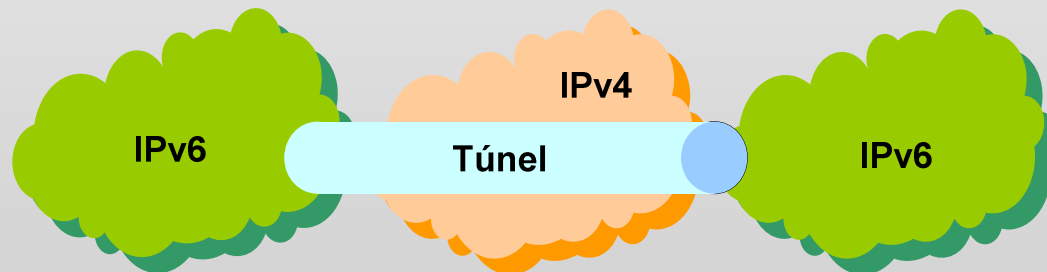
- Son utilizados para enlazar nodos compatibles a través de una red incompatible haciendo uso de la encapsulación.
- Actúan como enlaces punto a punto entre estos nodos.
- Este mecanismo de transición es, en muchas ocasiones, usado en conjunto con la doble pila.
- Permiten que hosts IPv6 se comuniquen a través de un backbone IPv4 encapsulando los datagramas IPv6 en datagramas IPv4.





# TÚNELES

- Se requiere de dos puntos extremos (generalmente enrutadores) con una doble pila que se encarguen de encapsular y desencapsular los paquetes.
- La encapsulación es ejecutada por un router de borde que debe enviar la información a través de un enlace IPv4 existente.
- En el otro extremo del túnel debe existir otro router de borde que se encarga del proceso inverso es decir, de desencapsular el paquete enviado.
- De esta manera, el uso de IPv6 es transparente para el backbone IPv4 ya que no hay ninguna necesidad de cambiar sus protocolos de enrutamiento ni sus enrutadores.



# TÚNELES

- Existen dos tipos de túneles:
  - Túneles automáticos: no requieren configuración de ningún tipo.
  - Túneles configurados: requieren de configuración manual y son usados cuando dos sitios intercambian tráfico de manera regular o cuando solo unos pocos sitios necesitan conectarse y la configuración manual no resulta un problema.
- Las tecnologías existentes más importantes son:
  - 6to4
  - 6over4
  - ISATAP
  - Teredo
  - Broker

# Túneles

## 6to4

- Los túneles 6to4 están definidos en la RFC 3056.
- Su objetivo es conectar dominios IPv6 a través de dominios IPv4.
- El dominio IPv6 que usa este mecanismo es llamado dominio 6to4.
- Define un modo específico de usar las direcciones IPv4 para construir las direcciones IPv6 que usará el dominio 6to4.

# Túneles

## 6to4

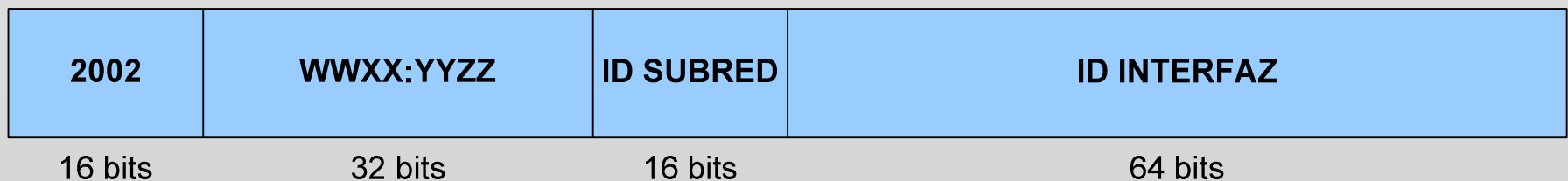
- 2002::/16 es el espacio de direcciones reservado para 6to4.
- WWXX:YYZZ es la representación hexadecimal de la dirección pública IPv4 del router de borde.

- Ejemplo: 190.54.20.87

10111110 00110110 00010100 01010111

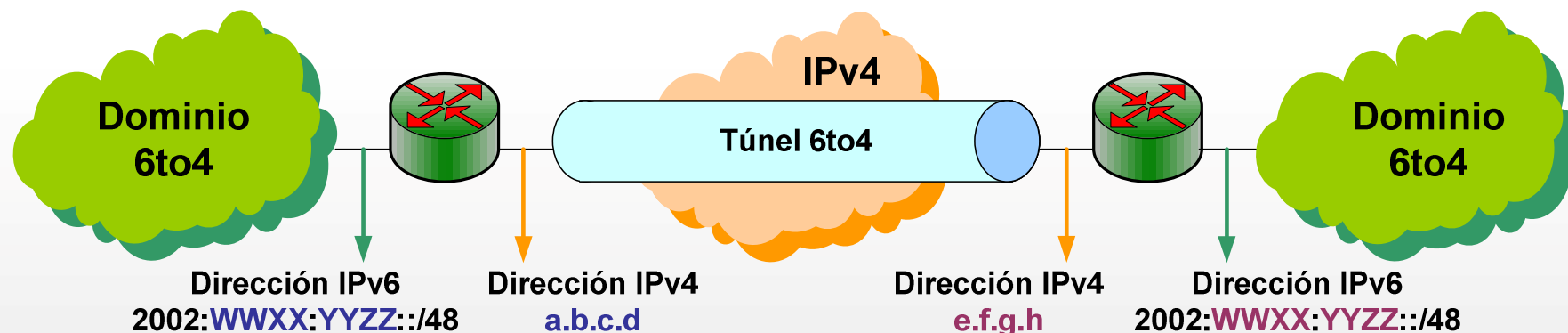
BE36:1457

- El campo ID SUBRED posee 16 bits destinados a identificar la subred.
- El campo ID INTERFAZ posee 64 bits destinados a identificar la interfaz de red.



# Túneles

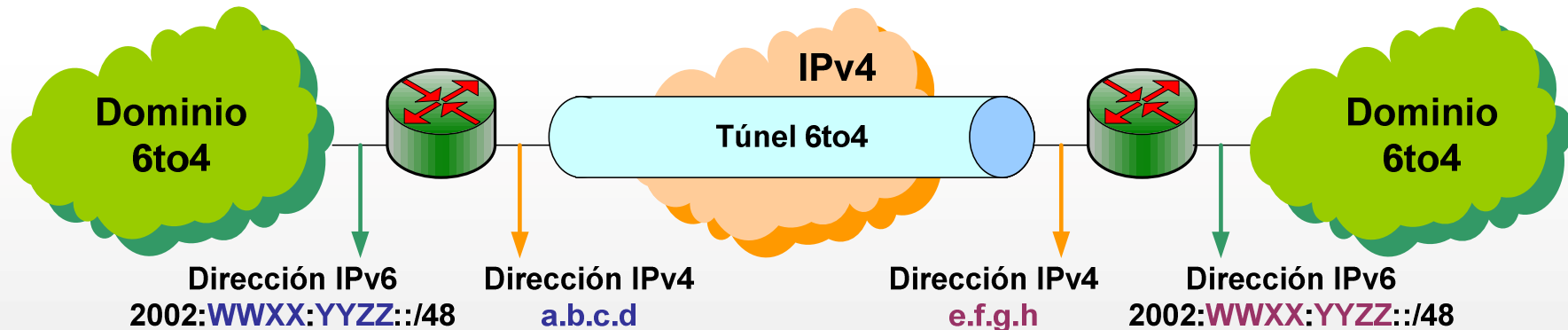
## 6to4



- Como se puede apreciar, permite asignar direcciones IPv6 y alcanzar hosts localizados en la Internet IPv6 sin necesidad de obtener un prefijo de dirección IPv6 global de un ISP.
- Con la utilización de este mecanismo, el tráfico IPv6 es enviado a través de redes IPv4 comunicando redes aisladas que utilizan 6to4.
- Si un dominio 6to4 quiere comunicarse con otro dominio 6to4 no se necesita de ninguna configuración adicional.

# Túneles

## 6to4



- Los paquetes IPv6 que llegan al router de borde son encapsulados en paquetes IPv4 y enviados a través de la red IPv4 para luego ser desencapsulados en el router de borde perteneciente al extremo final del túnel.
- Los dominios 6to4 pueden comunicarse gracias a que los paquetes IPv6 enviados poseen la dirección IPv4 del destino del túnel en la dirección de destino de los mismos.

# Túneles

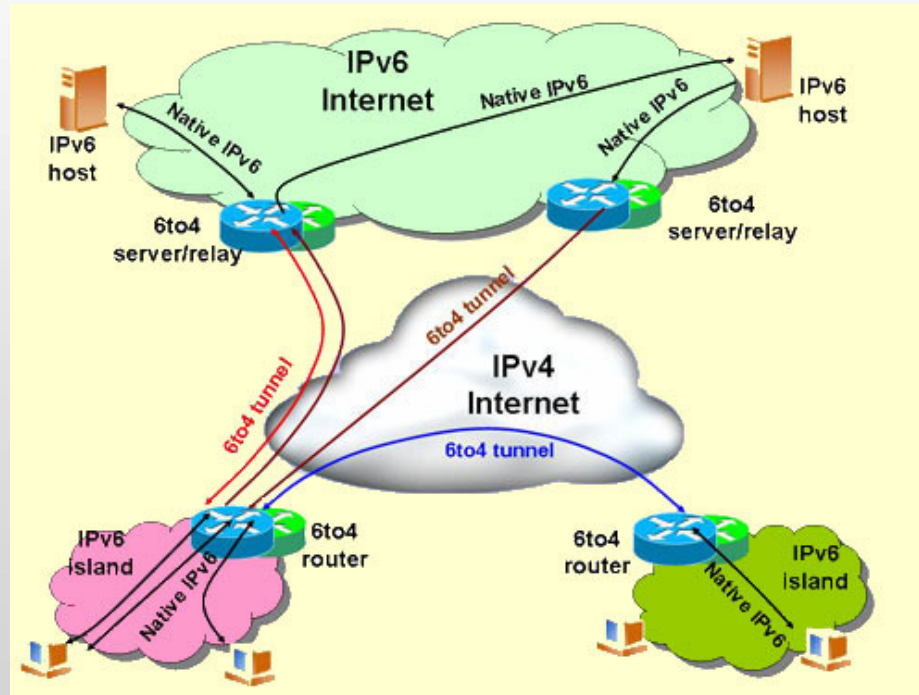
## 6to4

- Al implementar este tipo de túnel, los dominios IPv6 pueden comunicarse sin necesidad de implementar ningún protocolo de enrutamiento ya que de esto se encarga la red IPv4.
- Cuando un dominio 6to4 desea comunicarse con un dominio IPv6 no 6to4 se debe usar un relay 6to4.

# Túneles

## 6to4

- Un relay 6to4 no es más que un router con una interfaz conectada al dominio 6to4 y otra conectada a la red IPv6.
- En este caso es necesario que el relay 6to4 anuncie el prefijo 2002::/16 a la red IPv6 y deberá anunciar rutas a hacia los prefijos de las redes IPv6 en la red 6to4.





# Túneles

## ISATAP

- Este tipo de túnel se encuentra descrito en la RFC 4214.
- Constituye una alternativa a 6over4 ya que no hace uso de direcciones multicast.
- Al igual que 6over4, crea un identificador de interfaz basándose en la dirección IPv4.
- Soporta tanto la configuración automática como la manual.
- Requieren que los nodos IPv6 a interconectar posean un soporte doble pila.
- Es un método diseñado para ser usado en intranets, que no es capaz de atravesar los NAT.

# Túneles

## ISATAP

- Los identificadores de interfaces se crean a partir de las direcciones IPv4.
- Se utiliza el prefijo 0000:5EFE que, al combinarse con la dirección IPv4, conforma el identificador de interfaz de 64 bits requerido.
- Luego se agrega el prefijo FE80::/64 para crear las direcciones de enlace local.
- En el caso de necesitarse direcciones IPv6 globales es necesario recibir la asignación de un prefijo global por parte de algún ISP.
- Los prefijos asignados a redes ISATAP por los ISP deben pertenecer a un espacio definido con este propósito para diferenciarlas de redes IPv6 nativas.

# Túneles

## ISATAP

- La comunicación entre nodos IPv6 pertenecientes a una misma red se realiza únicamente mediante las interfaces ISATAP que tengan configuradas.
- Cuando la comunicación es hacia redes IPv6 externas se deben utilizar routers ISATAP que se encarguen de desencapsular el paquete IPv6 proveniente del túnel ISATAP y lo encaminan utilizando las técnicas de enrutamiento propias de IPv6.

# Túneles

## Teredo

- La descripción de este tipo de túnel se puede encontrar en la RFC 4380.
- Está diseñado para atravesar los NATs por lo que también es conocido como NAT Traversal.
- Su objetivo es permitirle a los hosts que se encuentran detrás de los NATs acceder a redes IPv6 utilizando un túnel UDP.
- Para el funcionamiento de Teredo se usa un servidor Teredo y un router relay Teredo. Aunque estos son dos elementos lógicos diferentes se pueden implementar en un mismo nodo.

# Túneles

## Teredo

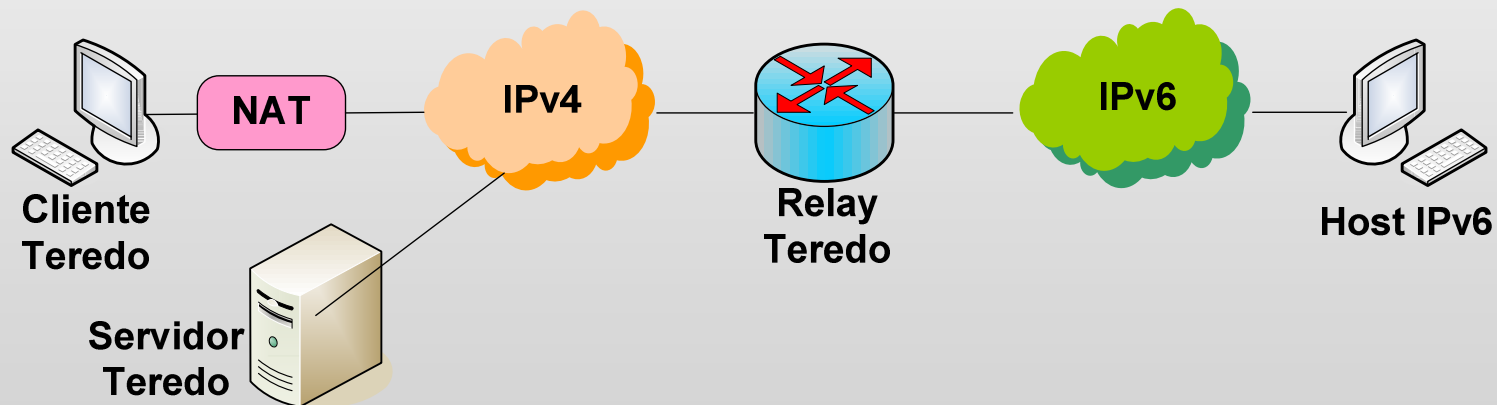
- Las direcciones usadas por este mecanismo deben usar el prefijo global IPv6 asignado para este servicio (2001:0000::/32).
- Los próximos 32 bits están constituidos por la dirección IPv4 del servidor Teredo.
- Seguidamente existen 16 bits asignados para las banderas que sirven para indicar el tipo de NAT usado.
- Los últimos 16 y 32 bits están destinados respectivamente al puerto UDP y a la dirección IPv4 asociados al cliente expresada en hexadecimal.

<b>2001:0000</b>	<b>Dirección IPv4 Servidor Teredo</b>	<b>Banderas</b>	<b>Puerto UDP Cliente</b>	<b>Dirección IPv4 Cliente</b>
32 bits	32 bits	16 bits	16 bits	32 bits

# Túneles

## Teredo

- El cliente Teredo ubicado en la red IPv4 interactúa con el servidor Teredo para obtener una dirección IPv6 Teredo que contiene la dirección IPv4 y el puerto a utilizar para la comunicación.
- Seguidamente los paquetes IPv6 enviados por el cliente Teredo son mapeados a través del NAT y encaminados a través del relay Teredo para ser entregados a un host IPv6 perteneciente a una red IPv6.



# Túneles

## Teredo

- Los datos enviados nunca pasan por el servidor Teredo. Con ello se garantiza la privacidad de los datos y se minimiza la carga del servidor Teredo.
- Debido a la gran variedad de implementaciones que existen de los NATs no puede garantizarse que este método funcione.
- Su uso no es muy aconsejable y solo debe implementarse como último recurso.

# Túneles

## Broker

- Este método se encuentra descrito en la RFC 3053.
- Son útiles para los escenarios en donde un usuario aislado con conexión IPv4 desea incorporarse a la red IPv6 y la configuración de túneles manuales le resulta poco práctica.
- Es un túnel configurado en el que se usan tareas programadas en lugar de la configuración manual.
- La configuración en este tipo de túnel es generalmente sencilla en los clientes, no siendo así en los servidores.
- Las direcciones IPv6 asignadas en ambos lados del túnel deben pertenecer al espacio de direcciones IPv6 globales asignado para el uso de este servicio.



# Túneles

## Broker

- Pueden considerarse como ISP virtuales capaces de proveer conectividad IPv6 a los usuarios conectados a la Internet IPv4.
- La idea de este mecanismo es que los servidores destinados para brindar este servicio, administren automáticamente las peticiones para la realización del túnel provenientes de los usuarios.
- El cliente del túnel Broker puede ser un host o un router doble pila conectado a la Internet IPv4.

# Túneles

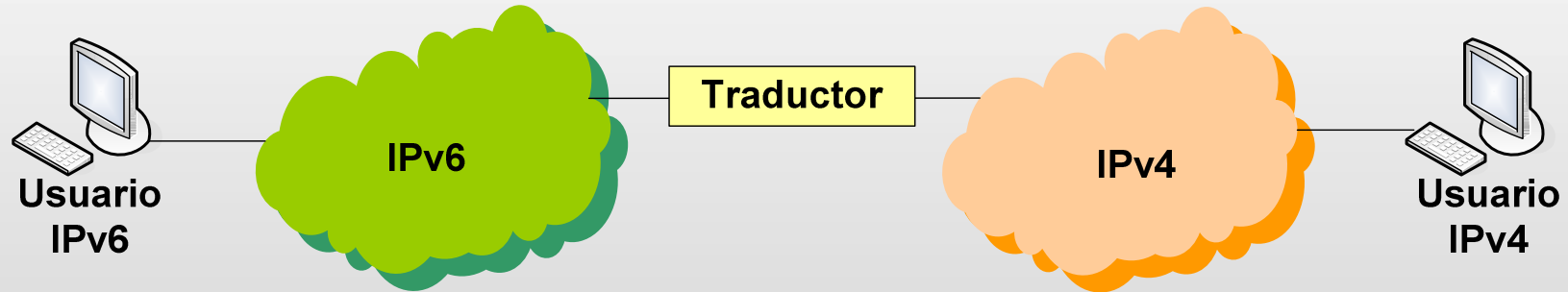
## Broker



- Este mecanismo consta de dos elementos:
  - El túnel Broker (TB): es a donde se conectan los usuarios para registrarse y activar un túnel. Además es quien se ocupa de la creación modificación y eliminación de los túneles.
  - El túnel server (TS): es un router doble pila conectado Internet y conserva estadísticas del uso de cada túnel activo.

# TRADUCTORES

- Realizan la conversión directa entre los protocolos IPv4 e IPv6 de manera bidireccional.
- Permiten la comunicación entre hosts que solo son IPv4 y hosts que solo son IPv6.



# TRADUCTORES

- Se basa en los campos comunes de las cabeceras de ambas versiones para realizar la traducción de datagramas IPv6 a IPv4 y viceversa.
- Puede ser implementado en otras capas, además de la de red, como la de transporte o la de aplicación.
- Pueden ser de dos tipos:
  - Stateless: es capaz de procesar las traducciones de manera individual es decir, sin hacer referencia alguna a paquetes traducidos previamente.
  - Stateful: es necesario tener en cuenta las traducciones previas.

# TRADUCTORES

- Las tecnologías existentes más importantes son:
  - SIIT
  - NAT-PT y NAPT-PT
  - BIS y BIA
  - TRT
  - NAT64

# TRADUCTORES

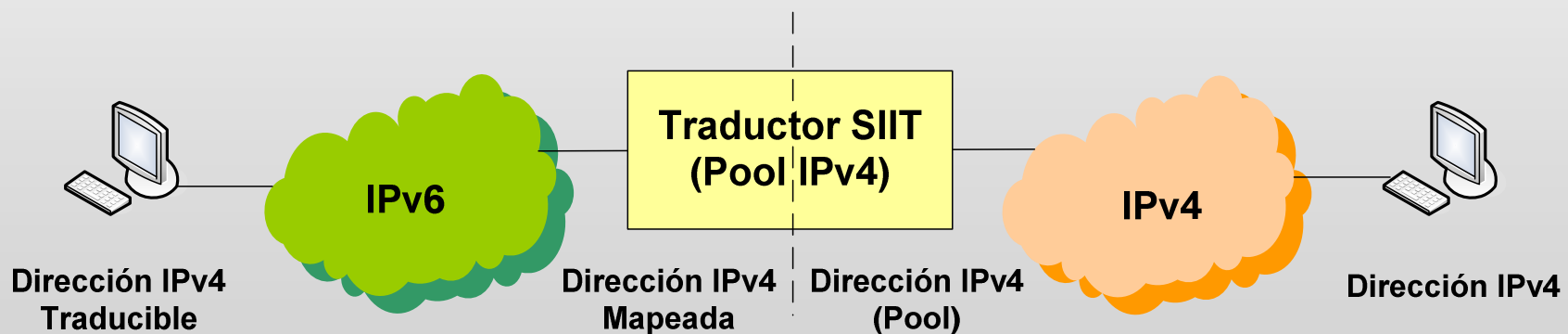
## SIIT

- Está descrito en la RFC 2765.
- Plantea la traducción entre las cabeceras IPv4 e IPv6, así como entre los protocolos ICMPv4 e ICMPv6.
- Esta traducción se realiza de forma independiente para los protocolos IP e ICMP y no se registra el control de estado de los enlaces realizados.
- Está diseñado para escenarios donde los nodos no tienen asignadas direcciones IPv4 de modo permanente.
- En este mecanismo se utiliza un pool de direcciones IPv4 de manera dinámica y asume la existencia de un método para la generación de las direcciones IPv4-traducibles.

# TRADUCTORES

## SIIT

- Cuando la comunicación es en el sentido host IPv6 - host IPv4 se usa una dirección IPv4 traducible como dirección local, obtenida temporalmente del pool IPv4, y luego el nodo IPv6 envía el paquete a la dirección IPv4-mapeada del traductor.
- Si el sentido de la comunicación es host IPv4 - host IPv6, los paquetes del nodo IPv4 llegan al traductor y salen con la dirección destino de la dirección IPv4-traducida.



# TRADUCTORES

## SIIT

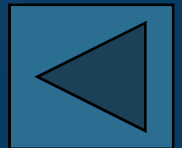


- El mecanismo SIIT posee un grupo de limitaciones importantes:
  - No se traducen las opciones de IPv4 ni la mayoría de los encabezados extensión de IPv6.
  - Las implementaciones de IPsec son limitadas.
  - Los dominios multicast de IPv4 no pueden ser ampliados a IPv6.



# Parte 4. Configuración de IPv6

- Mapas de tareas de configuración
- DNS en IPv6
- Configurando la PC



## MAPA DE TAREAS DE CONFIGURACIÓN

- El Mapa de Tarea es la descripción detallada de todas las tareas a realizar para lograr una buena configuración del IPv6 en la Red.
- Las tareas se desarrollan en el orden indicado en el mapa de tareas.

# MAPA DE TAREAS DE CONFIGURACIÓN

- Veamos un ejemplo: QUEREMOS INICIAR LA CONFIGURACIÓN DE LOS SERVICIOS IPv6 EN NUESTRA RED

TAREA	DESCRIPCIÓN	OBTENER INSTRUCCIONES PARA
1. Antes de comenzar la configuración de IPv6, compruebe que haya cumplido todos los requisitos previos.	Antes de configurar un router habilitado para IPv6, debe completar las tareas de planificación e instalación del SO con interfaces habilitadas para IPv6.	Realizar la planificación de una red IPv6, inventarios de Medios Técnicos, etc. (Plan de Direccionamiento y Configuración de interfaces de equipos IPv6).
2. Configurar un router y otros elementos de la Red.	Defina el prefijo de sitio de la red. Identificar elementos y servicios críticos.	Verificar el IOS del router. Configurar un router para IPv6 Configurar elementos identificados y servicios.
3. Configurar los switch de red.	Si en la configuración de red hay conmutadores, es ahora cuando los debe configurar para IPv6.	Consulte la documentación del fabricante de conmutadores.
4. Configurar el servicio DNS de redes para IPv6.	Configure el servicio de nombres principal (DNS, NIS o LDAP) para reconocer las direcciones IPv6 después de configurar para IPv6 el router.	Agregar direcciones IPv6 a DNS

# MAPA DE TAREAS DE CONFIGURACIÓN



## ■ Continuación del ejemplo:

TAREA	DESCRIPCIÓN	OBTENER INSTRUCCIONES PARA
5. Modificar las direcciones de las interfaces habilitadas para IPv6 en hosts y servidores.	Después de configurar el router para IPv6, realice las modificaciones pertinentes en los hosts y servidores habilitados para IPv6.	Modificar la configuración de una interfaz de IPv6 para hosts y servidores
6. Configurar interfaces de túnel en el router.	Configure en el router un túnel manual o una interfaz de túnel. La red IPv6 local necesita túneles para comunicarse con otras redes IPv6 aisladas.	Configurar un túnel Configurar manualmente túneles para tráfico IPv6 a través de redes IPv4.
7. Configurar reglas de seguridad en cada uno de los componentes	Establecer los mecanismos de seguridad que permitan el correcto funcionamiento de la Red	Agregar reglas de seguridad en cada componente y reglas globales de seguridad
8. Realizar pruebas de funcionalidad.	Realizar la pruebas necesarias que verifiquen el correcto funcionamiento de la Red.	Comprobar que cada una de las partes este en correcto funcionamiento

## DNS EN IPV6

- La RFC 1886 explica los cambios que deben hacerse en el servidor DNS para que soporte IPv6 (ver también RFC3596).
- En esencia, debe agregarse un registro AAAA.
- **Extensiones del DNS para soportar IPv6 – Nombres a Números**
  - El tipo de registro AAAA
    - Específico para IPv6
    - Perteneciente a la clase IN
    - Almacena una sola dirección IPv6
  - Formato de los datos AAAA
    - Registros de 128bit en Hexadecimal
    - Ordenados con el byte de mayor significancia a la izquierda
  - Consultas AAAA
    - Retornan todos los registros AAAA asociados para un nombre de dominio en la sección de “respuesta”
    - No genera ningún otro tipo de consulta

## DNS EN IPV6

- La RFC 1886 explica los cambios que deben hacerse en el servidor DNS para que soporte IPv6 (ver también RFC3596).
- En esencia, debe agregarse un registro AAAA.
- **Extensiones del DNS para soportar IPv6 – Nombres a Números**
  - El tipo de registro AAAA
    - Específico para IPv6
    - Perteneciente a la clase IN
    - Almacena una sola dirección IPv6
  - Formato de los datos AAAA
    - Registros de 128bit en Hexadecimal
    - Ordenados con el byte de mayor significancia a la izquierda
  - Consultas AAAA
    - Retornan todos los registros AAAA asociados para un nombre de dominio en la sección de “respuesta”
    - No genera ningún otro tipo de consulta

## Configurando la PC

- La forma de instalar IPv6 en una PC varía según sea su sistema operativo.

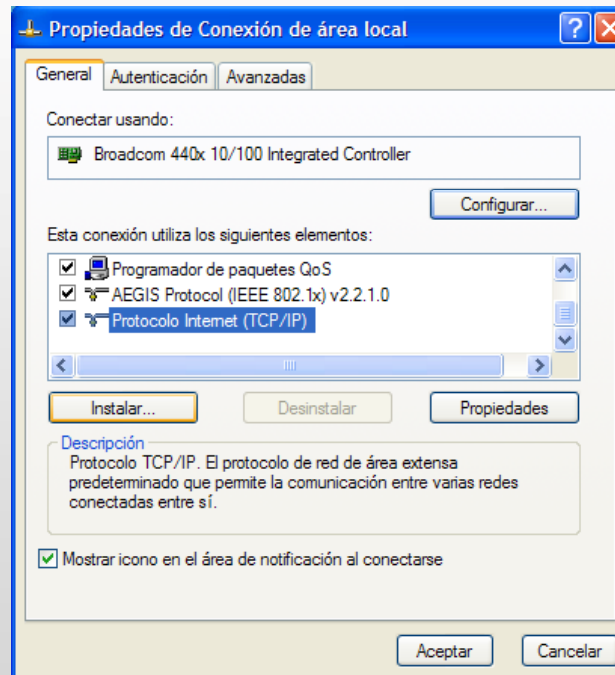
Windows XP SP1 y posteriores, Windows Server 2003

Windows Vistas, Windows Server 2008, Windows 7

- Ejemplo: En el caso de XP o 2003 se puede realizar la instalación/desinstalación utilizando la consola mediante los comandos:
  - `ipv6 install`
  - `ip uninstall`
- Para verificar la instalación se utilizan los comandos:
  - `ipconfig`
  - `ipv6 if`

# Configurando la PC

- También se puede instalar/desinstalar desde “Conexiones de red”:
  - Se selecciona “Propiedades” en la tarjeta de red en la cual se quiere instalar IPv6 y se oprime el botón “Instalar”.
  - Luego se selecciona “Protocolo”, se selecciona “Agregar” y finalmente se selecciona IPv6.



- Windows 7 ya lo trae activado por defecto.



## Configurando la PC



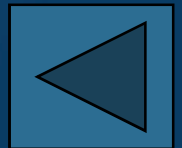
- En XP o 2003 se pueden utilizar, además, el grupo de comandos “netsh interface ipv6”.
- Ejemplos:
  - netsh interface ipv6 add address (Agrega una dirección IPv6 a la interfaz)
  - netsh interface ipv6 show address (Muestra las direcciones IPv6)
  - netsh interface ipv6 show interface (Muestra los parámetros de las interfaces)
- Se utilizan los comandos “ping6” y “tracert6”, aunque se pueden utilizar “ping” y “tracert” si el DNS devuelve registros AAAA.

## Configurando la PC

- Características soportadas en las últimas versiones de Windows:
  - Autoconfiguración
  - Tunel 6in4
  - Tunel 6to4
  - Relay 6to4
  - Tuneles Teredo
  - Tuneles ISATAP
  - IPsec (llaves manuales)

# Parte 6. Caso de estudio

- Proyecto Piloto “Uso de IPv6 en la Red Transnet”
- Tarea Técnica “Uso de IPv6 en la Red Transnet”
- Pruebas realizadas para verificar la disponibilidad en el uso del protocolo IPv6



# PROYECTO PILOTO



## Contenido

- Para realizar la transición a IPv6 de una red se debe primero confeccionar el Proyecto Piloto (Instrucción No 5/2007 del MIC). El contenido del Proyecto Piloto debe contener los siguientes aspectos:
  - Título
  - Resumen
  - Objetivos
  - Medidas de control y seguridad
  - Supervisión
  - Asesoría
  - Capacitación
  - Entre otros.
- Del Proyecto Piloto se deriva la Tarea Técnica

# TAREAS TÉCNICA

## Contenido

- La Tareas Técnica debe contener los siguientes aspectos:
  - Título
  - Resumen
  - Introducción. Detalles del estado actual de la red
  - Diferentes etapas para la transición, sus objetivos, las tareas a ejecutar en cada una de ellas y quien es el responsable de la ejecución de las mismas.
  - Conclusiones

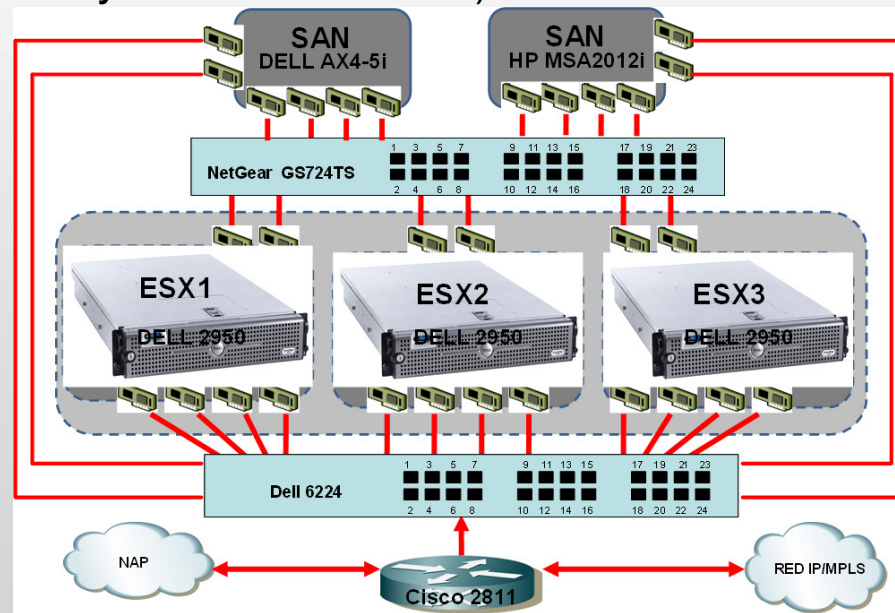
# TAREAS TÉCNICA

## **Introducción. Detalles del estado actual de la red TRANSNET**

- La Red TRANSNET del MITRANS posee recursos IP recibido directamente de LACNIC:
- Las direcciones IPv4 fueron anunciadas por el NAP desde julio 2008 y desde esa fecha TRANSNET gestiona su tráfico nacional e internacional y establece su política de ruteo.
- El nodo de la red TRANSNET, conocido como el Hosting, se encuentra ubicado en el MIC, específicamente en InfoCom.
- La administración del Hosting se realiza de manera remota mediante un enlace de 2 Mb entre el Hosting y la empresa SITRANS.
- El Hosting utiliza la plataforma de virtualización VMware ESX que posee un sistema operativo autónomo que permite la administración de los dispositivos virtuales creados y de los servicios instalados.

# TAREAS TÉCNICA

- La red cuenta con el siguiente equipamiento:
  - 1 Router Cisco 2811
  - 2 Switch L3 (1 Dell 6224 y 1 NETGEAR GS724T)
  - 3 Servidores Dell Power Edge 2950
  - 2 SAN (1 Dell AX4-5i y 1 HP MSA2012i)



## TAREAS TÉCNICA

- Los usuarios de la red pueden acceder a los servicios de dos maneras diferentes: mediante líneas dedicadas o mediante líneas conmutadas. En ambos casos, todos los clientes de la red pertenecen a la VPN TRANSNET.
- Las líneas dedicadas contratadas existentes ascienden a más de 180 y varían en cuanto a su velocidad desde 64 kbps hasta 2 Mbps. Existen líneas dedicadas con rango de direcciones IP público y otras con rango privado.
- Los usuarios con acceso conmutado (alrededor de 1800) utilizan la plataforma PAP que es administrada por ETECSA.



# TAREAS TÉCNICA

## ETAPAS

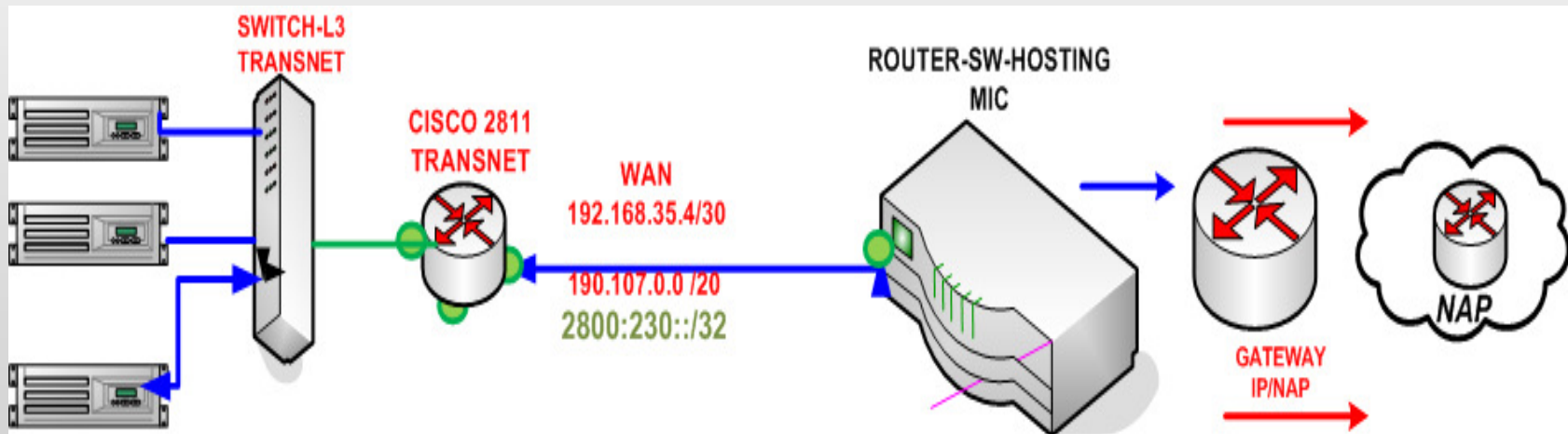
- Para lograr la adecuada transición a IPv6 en la red TRANSNET se ha elaborado una guía que consta de tres etapas. Las principales tareas a ejecutar son:
- Etapa 1. Configurar IPv6 en la subred TRANSNET en SITRANS.  
Ejecutor: TRANSNET .
  - Los administradores deben adquirir conocimientos teóricos y prácticos básicos de IPv6.
  - Se deben identificar todos activos de red y sistemas operativos de la red SITRANS que serán configurados con doble pila.
  - Dividir el bloque IPv6 asignado a SITRANS en /64 y asignar bloques /64 a cada grupo lógico existente.

## TAREAS TÉCNICA

- Configurar interfaces con doble pila en el switch Dell L3 6224.
- Realizar pruebas que consisten en activar la doble pila en servidores de pruebas Windows y FreeBSD dentro de una subred en SITRANS y configurar servicios de DNS y Web para ver si responden tanto a IPv4 como a IPv6.
- Configurar el DNS para que responda a encuestas desde hosts IPv6.
- Configurar el servidor Firewall PFSense con IPV6.
- Probar con IPv6 otros servicios que se utilizan en IPv4. Por ejemplo: Correo.
- Extender IPv6 a la Red Local de Transnet.
- Verificar el funcionamiento de IPv6 con la ayuda de comandos.

## TAREAS TÉCNICA

- Etapa 2. Configuración de IPv6 en el Hosting y configuración del segmento perteneciente al backbone de ETECSA para transmitir tráfico IPv6 nacional e internacional al router 2811 de TRANSNET. Ejecutor: TRANSNET y ETECSA.
  - Activación de la doble pila en el router Cisco 2811 en sus 3 interfaces.
  - Configurar la doble pila en los servicios del Hosting.
  - Activación de los bloques IPv6 en las asignaciones realizadas.

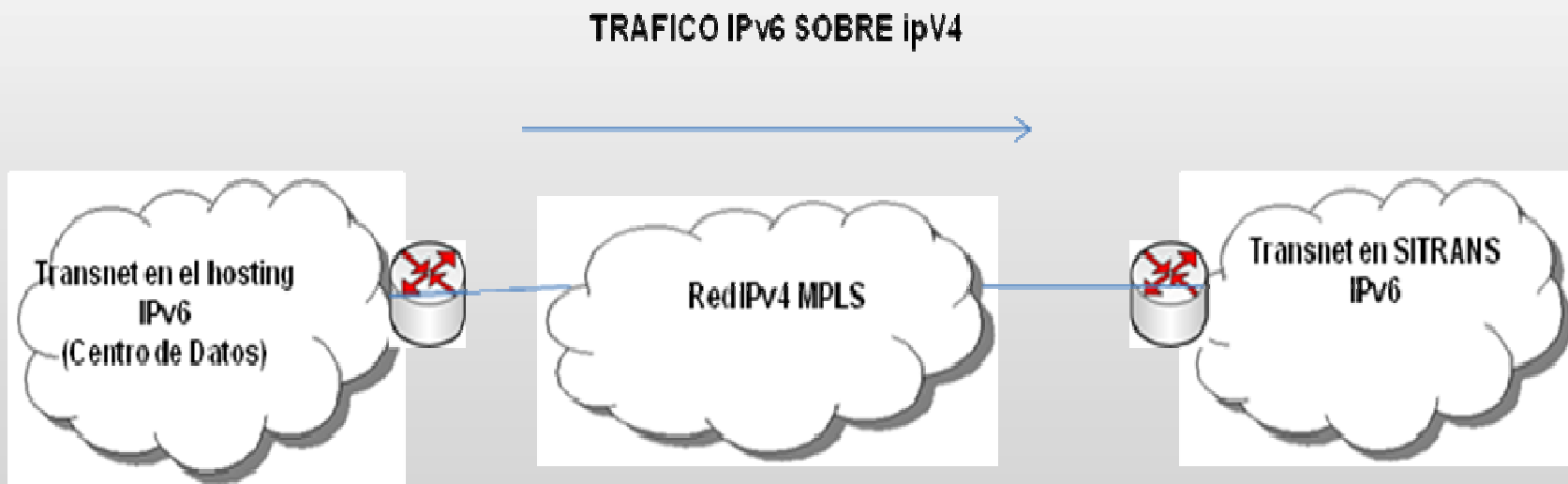


## TAREAS TÉCNICA

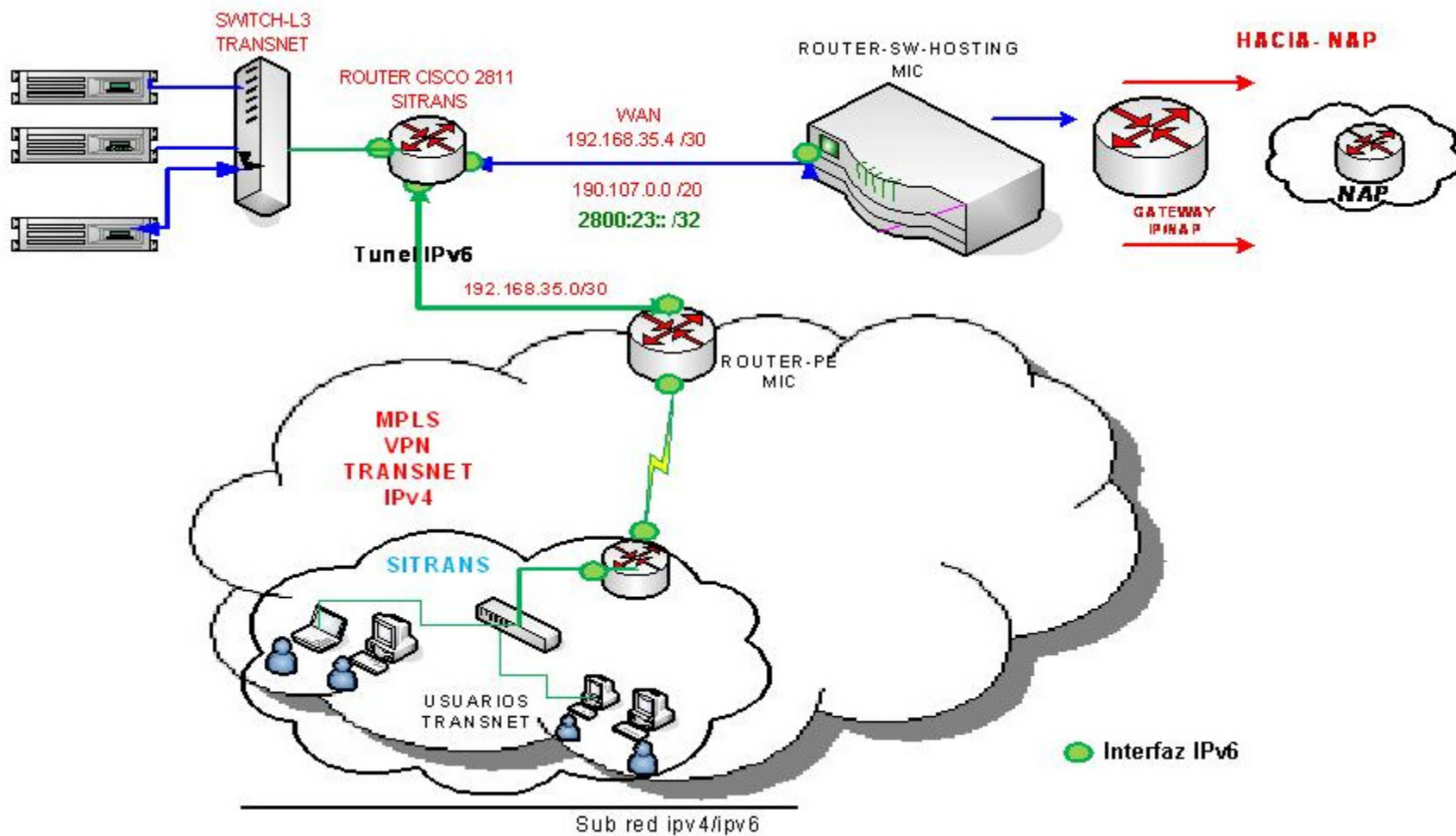
- Actualizar el IOS en los router que sean necesarios.
- Asignar direcciones IPv6 de ETECSA y configurarlas en los routers y switches que intervienen en la tarea.
- Activar el anuncio del nuevo bloque IPv6 de TRANSNET tanto en el Router-SW-Hosting como con el Gateway del NAP.
- Comprobar el tráfico IPv6 usando por ejemplo ICMPv6.

## TAREAS TÉCNICA

- Etapa 3. Configuración de un túnel para tráfico IPv6 sobre la red IPv4 entre TRANSNET y SITRANS. Ejecutor: TRANSNET.
  - Identificar las interfaces de cada extremo en las que se configurará el túnel.
  - Definir cuál es el tipo de túnel que se utilizará.
  - Realizar las configuraciones necesarias en ambos extremos.



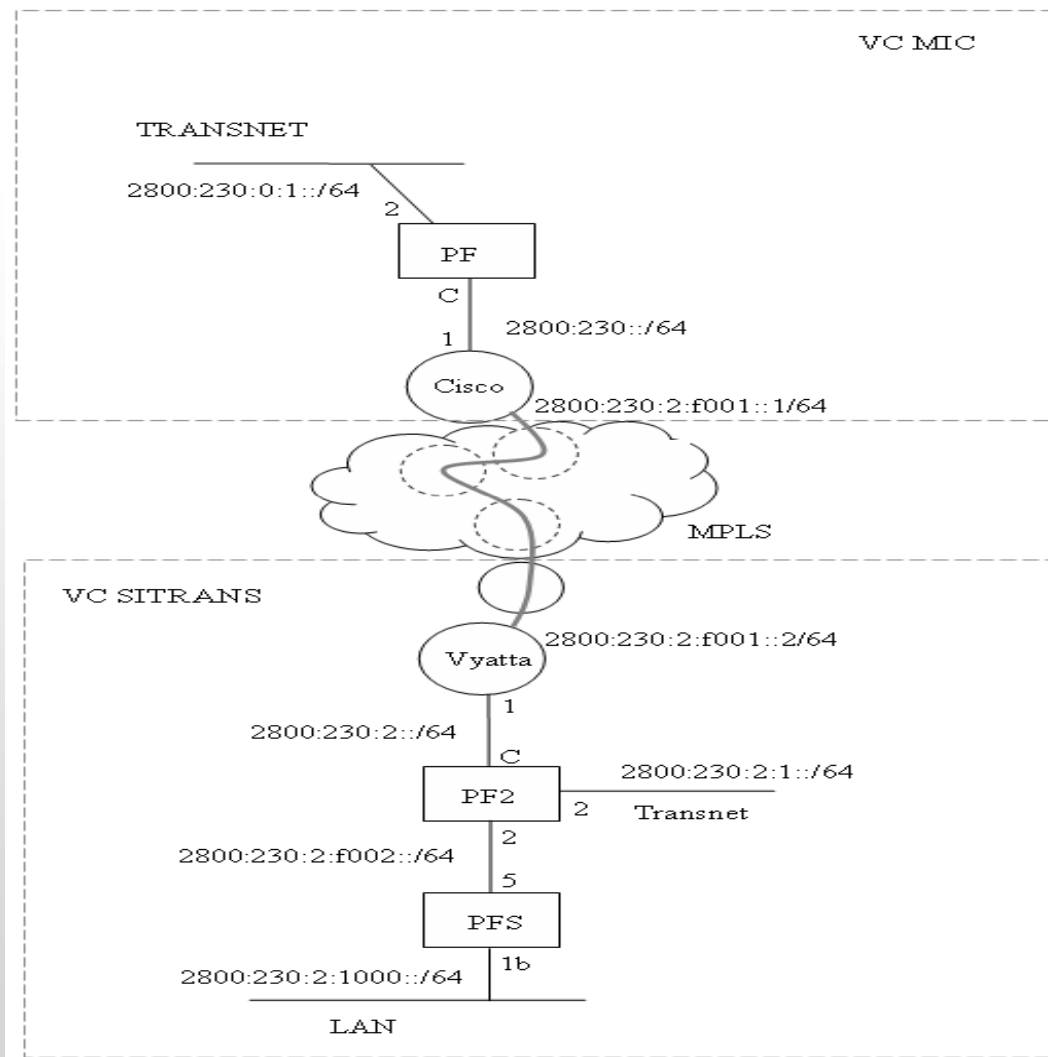
# TAREAS TÉCNICA



## PRUEBAS REALIZADAS

- Con el objetivo de comprobar el funcionamiento de IPv6 se realizaron un conjunto de pruebas en la Empresa SITRANS, donde radica la administración de TRANSNET.
  1. Se realizaron pruebas internas dentro del Data Center de SITRANS.
  2. Se comprobó el funcionamiento del túnel entre SITRANS y TRANSNET.
- Los bloque de direcciones IPv6 asignados a TRANSNET y a SITRANS son los siguientes:
  - 2800:230:0::/48 (TRANSNET)
  - 2800:230:2::/48 (SITRANS)

# PRUEBAS REALIZADAS





## PRUEBAS REALIZADAS

- Para poder realizar las pruebas primeramente se habilitaron algunos servicios como el DNS y el correo tanto en el Data Center de SITRANS como en el de TRANSNET.
- Después se instaló IPv6 en las máquinas de algunos usuarios y se utilizaron herramientas como “ping” y “tracert” para verificar el correcto funcionamiento del protocolo y los servicios.

# PRUEBAS REALIZADAS

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\jemar.SITRANS>
C:\Documents and Settings\jemar.SITRANS>ping www.ipv6.transnet.cu

Pinging www.ipv6.transnet.cu [2800:230:2:1::13] with 32 bytes of data:

Reply from 2800:230:2:1::13: time=1ms
Reply from 2800:230:2:1::13: time=2ms
Reply from 2800:230:2:1::13: time=2ms
Reply from 2800:230:2:1::13: time=1ms

Ping statistics for 2800:230:2:1::13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

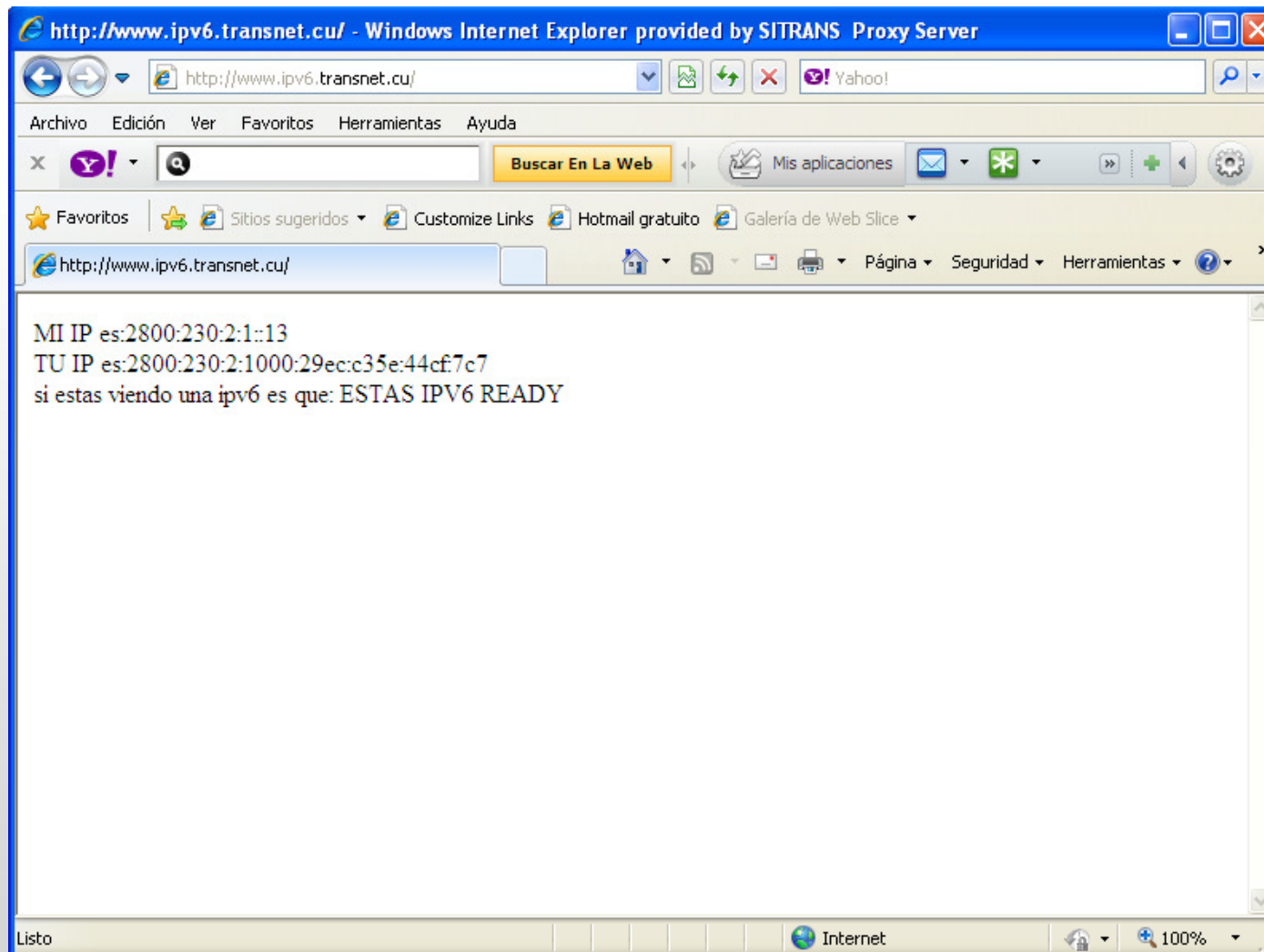
C:\Documents and Settings\jemar.SITRANS>tracert www.ipv6.transnet.cu

Tracing route to www.ipv6.transnet.cu [2800:230:2:1::13]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    2800:230:2:1000::1b
  2     1 ms     1 ms     <1 ms    2800:230:2:f002::2
  3     2 ms     1 ms     1 ms    2800:230:2:1::13

Trace complete.
```

# PRUEBAS REALIZADAS



# PRUEBAS REALIZADAS

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\jemar.SITRANS>ping correoweb.transnet.cu

Pinging webmail.transnet.cu [2800:230:0:1::31] with 32 bytes of data:

Reply from 2800:230:0:1::31: time=34ms
Reply from 2800:230:0:1::31: time=37ms
Reply from 2800:230:0:1::31: time=35ms
Reply from 2800:230:0:1::31: time=36ms

Ping statistics for 2800:230:0:1::31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 37ms, Average = 35ms

C:\Documents and Settings\jemar.SITRANS>tracert correoweb.transnet.cu

Tracing route to webmail.transnet.cu [2800:230:0:1::31]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    2800:230:2:1000::1b
  2     1 ms    <1 ms    <1 ms    2800:230:2:f002::2
  3     2 ms    *        3 ms    2800:230:2::1
  4    44 ms    40 ms    39 ms    2800:230:2:f001::1
  5    40 ms    41 ms    36 ms    2800:230::c
  6    39 ms    40 ms    43 ms    2800:230:0:1::31

Trace complete.
```

# PRUEBAS REALIZADAS



Correo :: Bienvenidos a Horde - Windows Internet Explorer provided by SITRANS Proxy Server

http://correoweb.transnet.cu/imp/login.php

Archivo Edición Ver Favoritos Herramientas Ayuda

Y! Buscar En La Web Mis aplicaciones

Favoritos Sitios sugeridos Customize Links Hotmail gratuito Galería de Web Slice

Correo :: Bienvenidos a Horde

**Bienvenidos a TransMail**

Usuario

Contraseña

Modo Tradicional

[Cambiar a conexión segura](#)

**U.d está usando IPv6. Su dirección es: '2800:230:2:1000:29ec:c35e:44cf:7c7'. La dirección de este servidor es: '2800:230:0:1::31'**

Internet 100%

## BIBLIOGRAFÍA

- Afifi, H. y Toutain, L. “Methods for IPv4-IPv6 Transition”.
- Agilent Technologies, “IPv6 Transition Test Challenges”. 2002.
- ALCATEL. “To Move to IPv6”. 2002.
- Colectivo de Autores. “IPv6 para todos”. 2009. ISBN: 978-987-25392-1-4.
- Davies, J. “Understanding IPv6”. Microsoft Press. 2008. ISBN: 978-0735612457.
- Durand, A. “Deploying IPv6”. 2001.
- Mackay, M. y Edwards, C. “IPv6 Transitioning Management - Laying the Foundation for Managed IPv4/IPv6 Interoperation”. Lancaster University.
- Palet, J. “Tutorial de IPv6”. Consulintel. IPv6 Forum.
- Raicu, I. y Zeadally, S. “Evaluating IPv4 to IPv6 Transition Mechanisms”. 2003.
- van Beijnum, I. “Running IPv6”. Apress. 2006. ISBN : 1-59059-527-0.

# BIBLIOGRAFÍA

- Sitios consultados:
  - [portalipv6.lacnic.net](http://portalipv6.lacnic.net)
  - [www.cu.ipv6tf.org](http://www.cu.ipv6tf.org)
  - [www.sixxs.net](http://www.sixxs.net)
- RFC Consultadas:
  - 1933, 2473, 2529, 2765, 2766, 2767, 2893, 3053, 3056, 3142, 3338, 4214, 4380.
- Otras (en la carpeta)

**MUCHAS GRACIAS**  
**¿PREGUNTAS?**