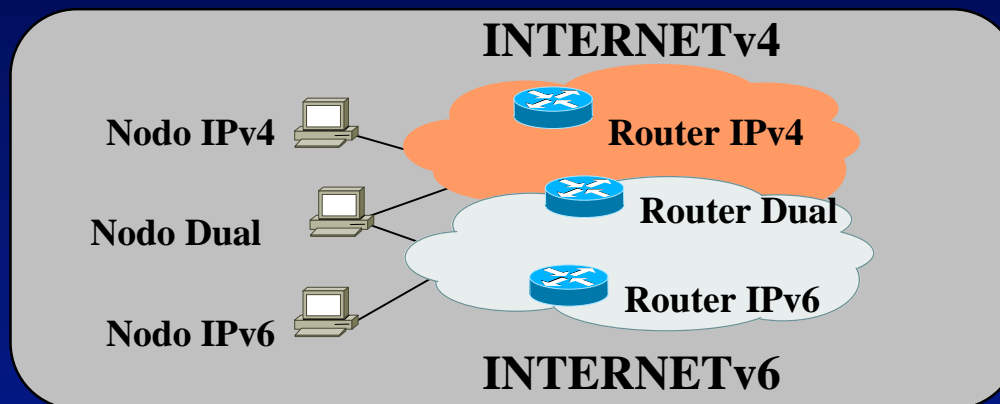


IPv6: Mecanismos de Transición IPv4 - IPv6.

Carlos Ralli Ucendo (ralli@tid.es)

Introducción

- Características de Migración IPv4-IPv6:
 - IPv4 e IPv6 incompatibles a nivel de paquete:
 - Los nodos finales actuales de Internet no generan ni reconocen IPv6.
 - Los routers IP actuales de Internet descartan los paquetes IPv6.
 - La principal dificultad es migrar la red Internet:
 - Durante la etapa de transición, a nivel lógico, habrá Internet IPv4 e IPv6.



- Mecanismos de Transición IPv4-IPv6: Permiten la integración y/o interacción de sistemas IPv4 e IPv6.

Clasificación

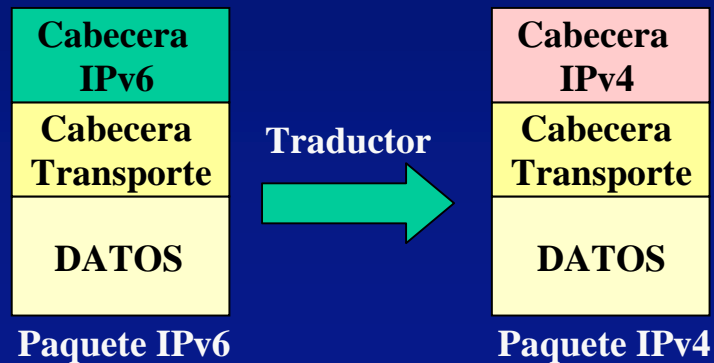
- Mecanismos de Tipo Túnel: Se basan en encapsular, están enfocados a unir dos islas IPvX a través de un océano IPvY.

- Túneles Manuales.
- Túneles Automáticos.
- Túneles 6to4.
- 6over4.



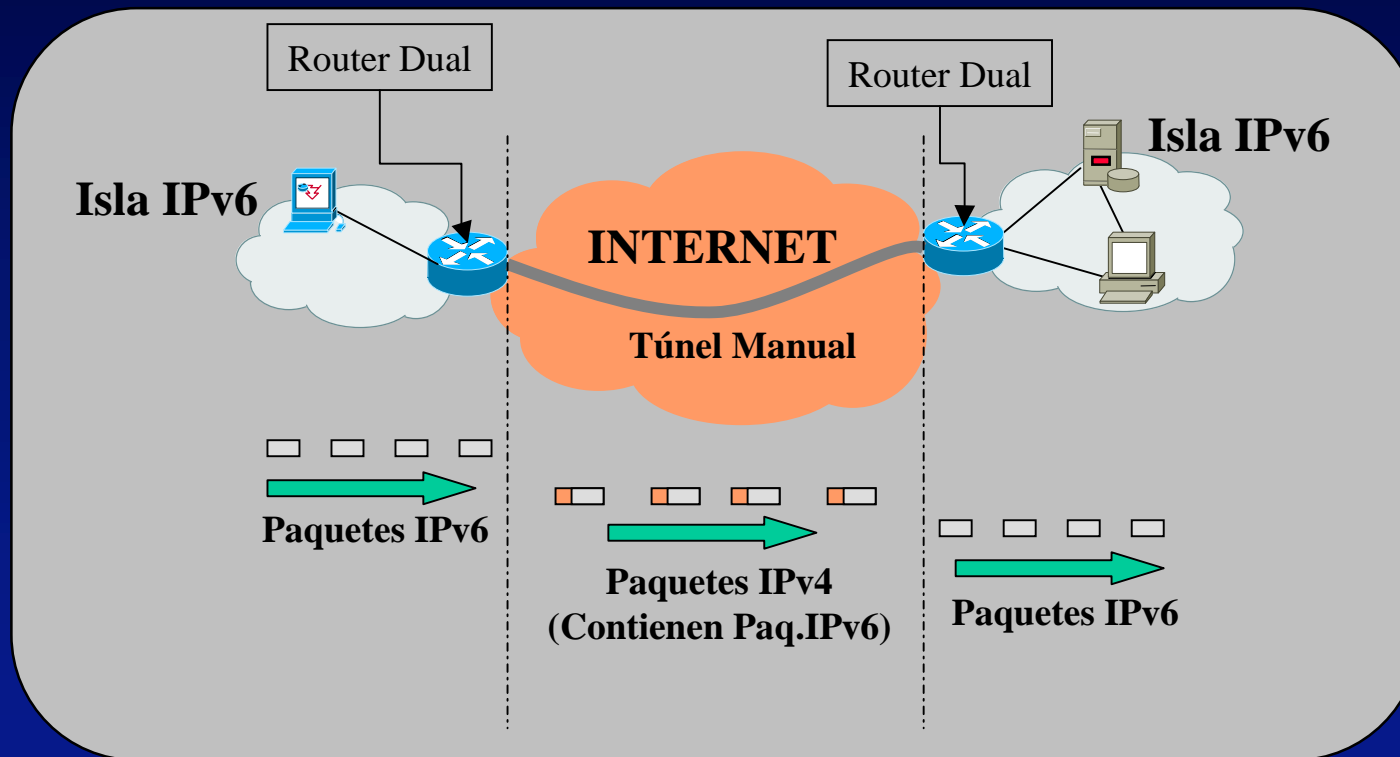
- Mecanismos de Traducción: Se basan en traducir, en un elemento de red, los paquetes de un formato a otro.

- NAT-PT.
- SOCKSv5.
- BIS (Bump in the Stack).



Túneles Manuales (I)

- Definido en: RFC 2893.
- Características Principales:
 - **Funcionalidad:** interconectar islas IPv6 a través de un océano IPv4.
 - Cada extremo es un nodo dual y en ellos se configura las direcciones IPv4 e IPv6 tanto local como remotas.

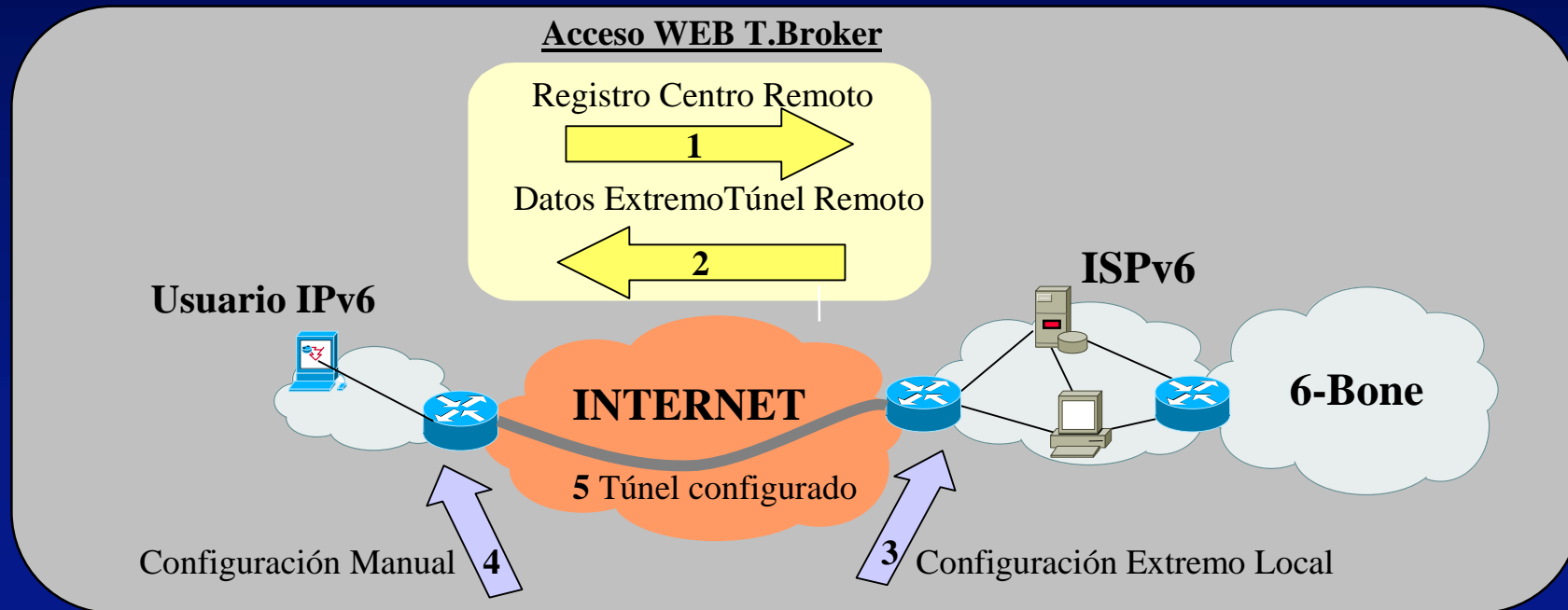


Túneles Manuales (II)

- Ventajas de este Sistema:
 - Método muy utilizado en el acceso al 6-Bone.
 - Disponible en multitud de plataformas (Cisco, Telebit, Linux, Solaris, Windows NT, etc).
 - Es un método totalmente transparente respecto al nivel IPv6 y superiores, con lo cual no afecta a las aplicaciones.
 - No consume excesivos recursos, la MTU se reduce en 20 bytes (cab. IPv4 típica).
 - Aplicación Principal: Conexión con ISP IPv6 remoto a través de Internet.
- Inconvenientes:
 - No son dinámicos, sino que se establecen manualmente o de forma semi-automática.
 - Si se unen N islas y la topología no considera un nodo central o intercambiador, el número de túneles a establecer en cada sitio asciende a $N-1$. En el caso de pensar en la conexión entre sí de miles de islas IPv6 distribuídas por la Internet actual, este método carece de sentido.
- Herramienta de Gestión Establecimiento Túneles Manuales: Tunnel-Broker.

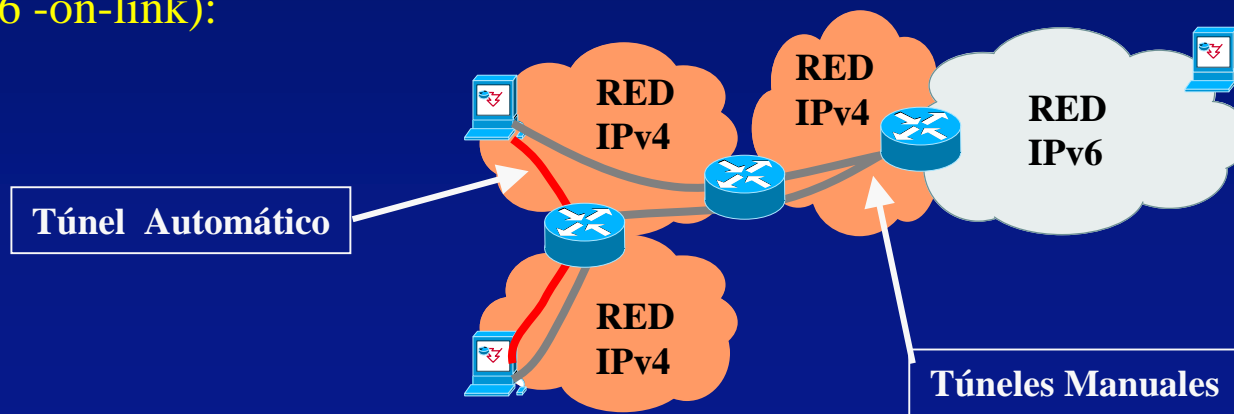
Túneles Manuales (III)

- Herramienta Tunnel Broker: definido en: “Draft-ietf-ngtrans-broker”.
 - Sistema de Alta de Túneles con interfaz WEB.
 - ISPv6 proporcionan acceso al 6-Bone y son accesibles por Internet.
 - Datos o Script Configuración → Usuario.
 - Datos Usuario y Configuración Local → Administrador Sistema.
 - Opcionalmente: Detección tiempos de inactividad y liberar de recursos.
 - Implementaciones: Ultima BT, Windows NT4.0.



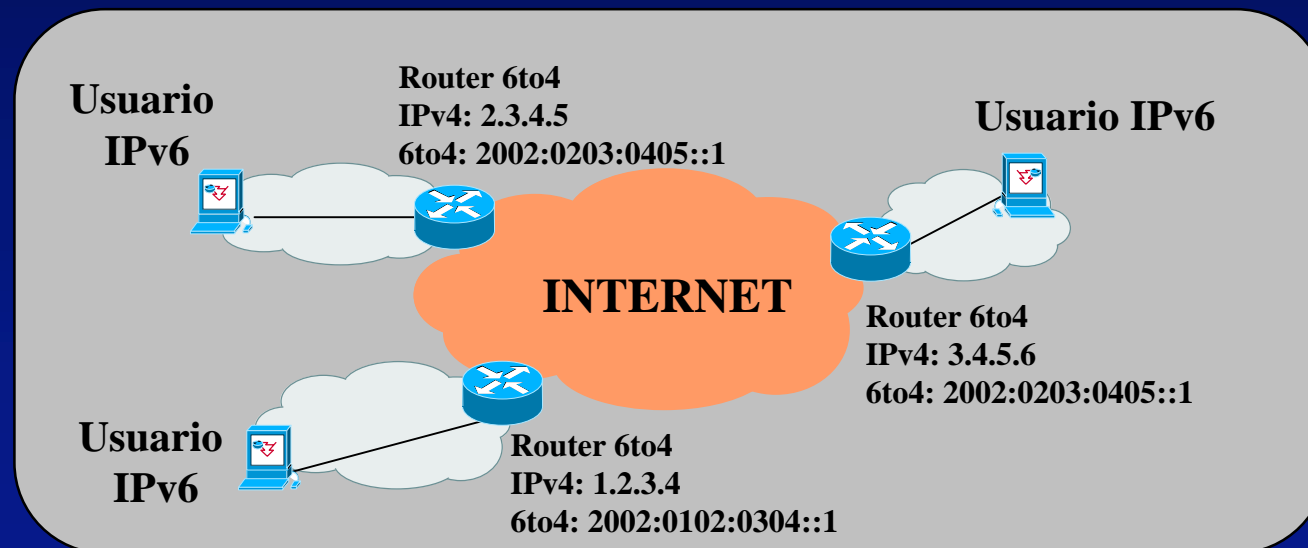
Túneles Automáticos

- Definido en: RFC 2893.
- Características Principales:
 - Permite a nodos duales comunicarse a través de una infraestructura IPv4.
 - Direcciones IPv6 “IPv4-Compatible”: Prefijo 0::/96 + Dirección IPv4.
 - Se define una interfaz virtual para la dirección “IPv4 Compatible”.
 - Los paquetes destinados a direcciones “IPv4 Compatible” se envían por el túnel automático. Reglas:
 - Dirección origen IPv6: Dirección “IPv4 Compatible” local.
 - Dirección Destino IPv4: Extraída de la dirección “IPv4 Compatible” remota.
 - Uso Túneles Automáticos y Túneles Manuales: Hosts IPv6 aislados (sin routers IPv6 -on-link):



Túneles 6to4 (I)

- Definido en: “Draft-ietf-ngtrans-6to4-06.txt”.
- Características Principales:
 - Su principal aplicación es unir islas IPv6 dispersas en un océano IPv4.
 - A cada isla IPv6 se le asigna un prefijo IPv6: 2002::



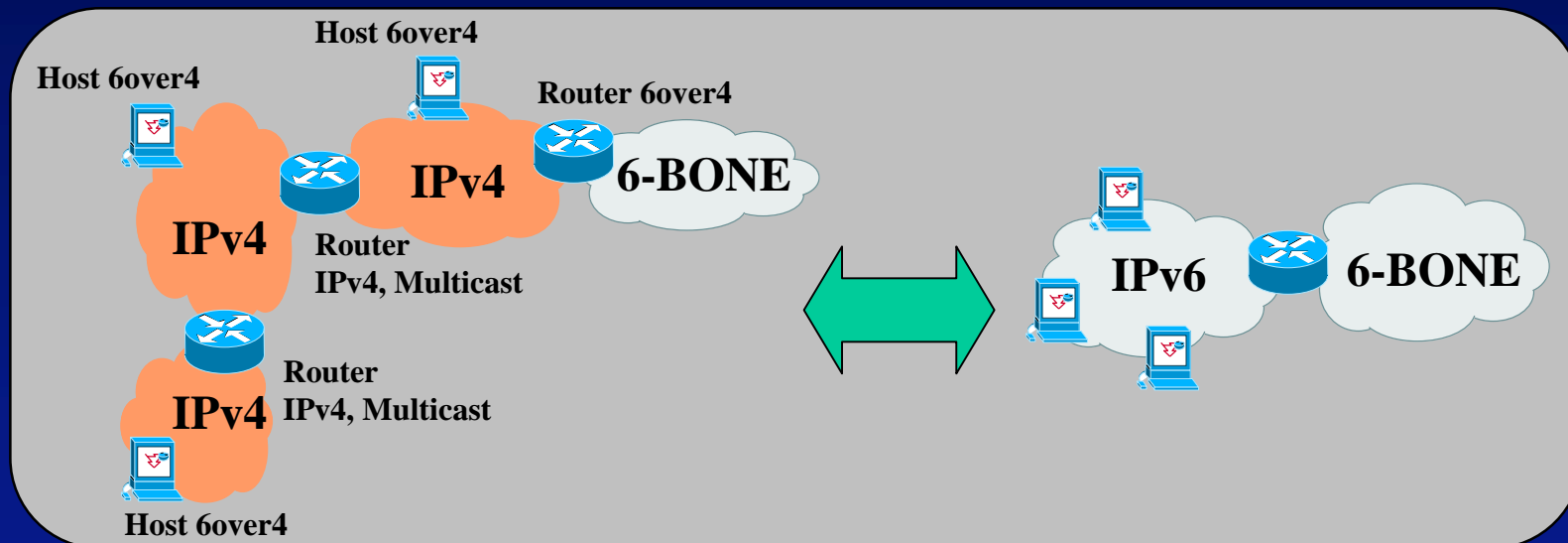
Túneles 6to4 (II)

- Ventajas:
 - Al igual que los túneles manuales, son transparentes a nivel IPv6 y, por tanto, no afectan a las aplicaciones.
 - Se trata de túneles establecidos dinámicamente y sin configuración previa.
 - Dadas N islas IPv6, sólo se establecen los túneles necesarios para las conexiones activas en cada momento.

- Inconvenientes:
 - Para organizaciones que se conecten a un ISP IPv6 remoto, no es necesario más que un túnel (o quizá dos por redundancia con otro ISP IPv6), por lo que puede ser suficiente emplear el mecanismo de Túneles Manuales, que se haya más extendido.

6over4 (I)

- Definido en: RFC 2529.
- Características Principales:
 - **Nodos IPv6 dispersos en subredes IPv4** → Se forma una “LAN virtual” IPv6.
 - **Tráfico IPv6 entre nodos encapsulado en IPv4. Direcciones IPv4 Multicast.**
 - **Los procesos de Neighbor/Router Discovery se hacen empleando Multicast.**
 - **Router 6over4 con acceso 6-BONE** → Todos los nodos acceden al 6-BONE .



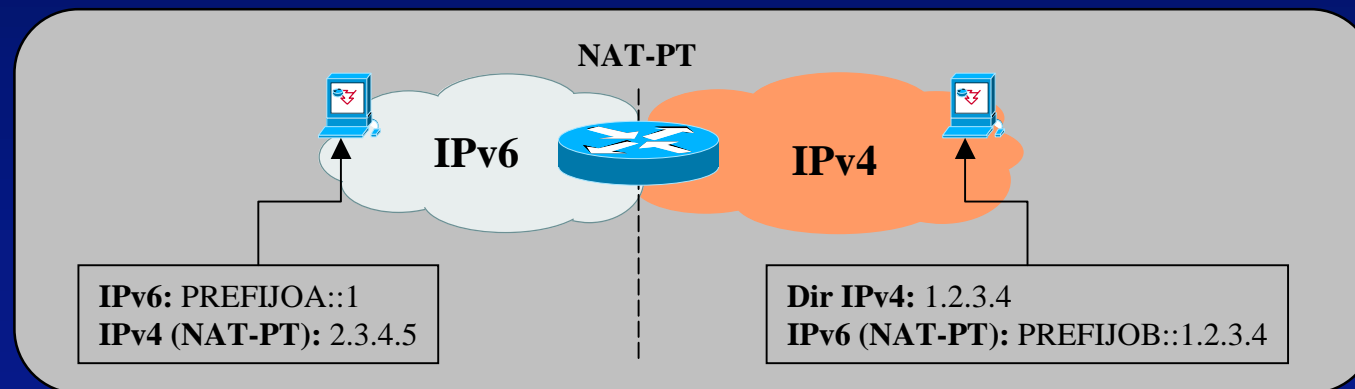
6over4 (II)

- Ventajas:
 - Al igual que los túneles anteriores, son transparentes a nivel IPv6 y, por tanto, no afectan a las aplicaciones.
 - Se trata de túneles establecidos dinámicamente y sin configuración previa.
 - Permite probar IPv6 en algunos nodos de una red IPv4 corporativa sin instalar el stack IPv6 en los routers internos.
 - Instalando en un solo router el stack IPv6 y conectándolo al 6-Bone se proporciona acceso a dicha red a todos al resto de nodos IPv6.

- Inconvenientes:
 - Se trata de un mecanismo adecuado para redes finales únicamente.
 - Todavía no está ampliamente implementado (Windows NT).

NAT-PT (I)

- Definido en: RFC 2766
- Características Principales:
 - NAT Tradicional: Traduce direcciones (conexión de redes con dir. IPv4 privado).
 - NAT-PT: Traducción de direcciones y protocolo.
 - Traducción basada en el algoritmo SIIT (RFC 2765).
 - No es transparente a nivel de aplicación → Precisa algunas extensiones:
 - DNS-ALG: Transforma peticiones DNS “A” a peticiones “AAAA”.
 - FTP-ALG: Las conexiones con FTP son problemáticas pues abren dos conexiones TCP intercambiando direcciones IP a nivel de aplicación.

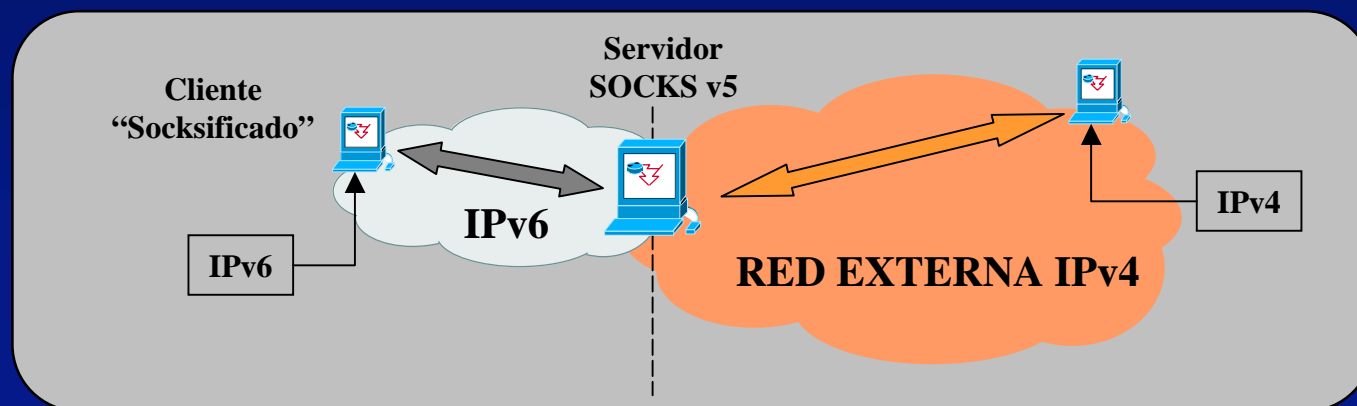


NAT-PT (II)

- Ventajas:
 - Muchas redes corporativas poseen experiencia en la gestión/administración de NATs.
 - Implementado en la mayor parte de los routers (Cisco, Telebit, Linux) y en algunas plataformas habituales en nodos finales (Windows 2000).
 - Si la comunicación extremo-a-extremo es heterogénea (IPvX-IPvY) NAT-PT resulta adecuado (teniendo en cuenta siempre la carga de tráfico prevista).
- Inconvenientes:
 - Los NATs poseen un alto coste de gestión y administración.
 - El proceso de traducción es más costoso en recursos que el de entunelar.
 - Si la comunicación extremo-a-extremo es homogénea (IPvX-IPvX) siempre es preferible emplear túneles a dos sistemas de traducción consecutivos.
 - Si en un protocolo de aplicación intercambian direcciones IP (DNS, FTP, etc.), es necesario una extensión o módulo que incluya un algoritmo para su tratamiento específico (DNS-ALG, FTP-ALG).

SOCKSv5 (I)

- Definido en: RFC 1928, “draft-ietf-ngtrans-socks-gateway-05”.
- Características Principales:
 - Uso tradicional SOCKSv5: conectividad IP directa a Internet en redes con firewall a determinados hosts.
 - Servidor SOCKSv5 dual ➡ Traductor de Protocolos (Algoritmo SIIT).
 - Traducción IPv4-IPv6 y viceversa. Conexiones SIEMPRE iniciadas por cliente.
 - Dos componentes: Servidor SOCKSv5 + Librería SOCKSv5 (cliente).
 - Implementaciones:
 - NEC (www.socks.nec.com)
 - Fujitsu (<ftp://ftp.kame.net/pub/kame/misc>)



SOCKSv5 (II)

- Funcionamiento Detallado: (Red IPv4 = Red Interna).
 - Una aplicación en el nodo cliente inicia una conexión TCP o UDP con un nodo externo empleando el nombre completo (FQDN).
 - La librería SOCKSv5 en el cliente intercepta la resolución del nombre (“gethostbyname”) e inicia una conexión TCP al puerto 1080 del servidor SOCKSv5.
 - El servidor SOCKSv5 devuelve al cliente una dirección IPv4 remota falsa (“fake IPv4 address”).
 - El servidor SOCKSv5 inicia la conexión TCP o UDP con el nodo remoto y hace de proxy entre el cliente y el nodo externo. Si el nodo externo es IPv6, aplica además el algoritmo de traducción SIIT (RFC 2765).
 - En el cliente, los paquetes con la “fake IPv4 address” como origen o destino son interceptados y tratados por la librerías SOCKSv5 que los recibe o envía respectivamente al servidor SOCKSv5.

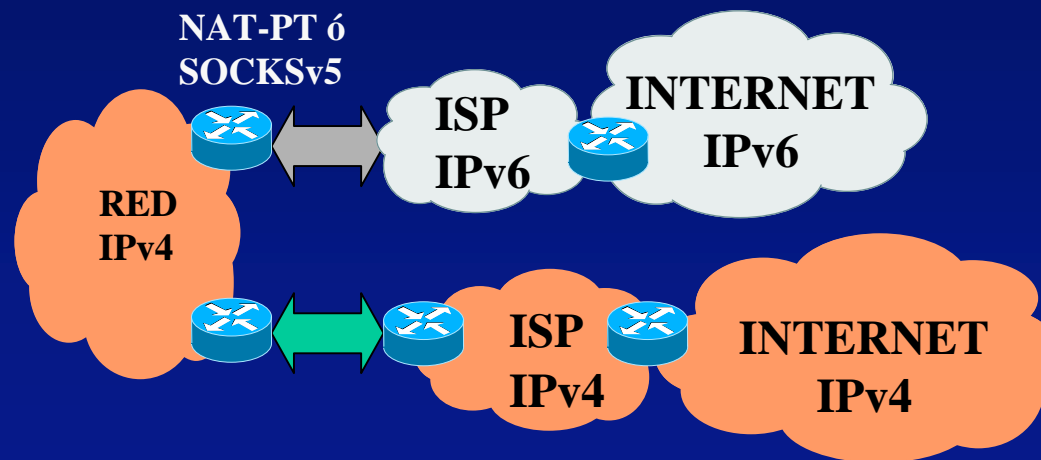
SOCKSv5 (III)

- Ventajas:
 - Sistema apto actualmente para corporaciones que deseen dar acceso a determinados nodos internos a servicios IPv6 sin probar exhaustivamente el protocolo.
 - Provee sistemas de autenticación adecuados para evitar usos indeseados.

- Inconvenientes:
 - Instalación de las librerías SOCKSv5 en todos los clientes a los que se desee dar acceso.
 - El proceso de traducción es costoso en cuanto a consumo de recursos en el servidor, por lo que un factor limitante es la carga de tráfico prevista.
 - Las conexiones sólo pueden ser iniciadas por los nodos internos, con lo cual no es posible ofrecer servicios al exterior mediante este método.
 - Como todos los mecanismos de traducción debe incorporar algoritmos específicos para aquellos protocolos de aplicación que intercambien direcciones IP (FTP).

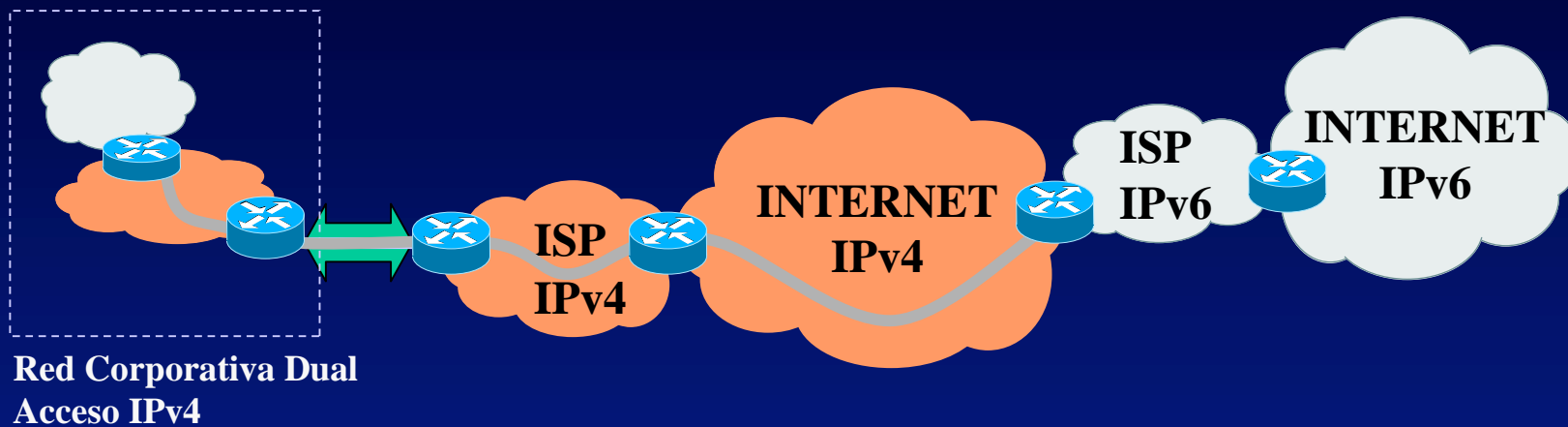
Estrategias Migración (I)

- Características de Migración IPv4-IPv6:
 - En general, Redes Finales primero y, según aumente el tráfico IPv6: ISP y Backbones principales.
 - Recomendaciones para redes finales:
 - Servidores “Doble stack”: para atender peticiones IPv4 e IPv6.
 - Clientes “Doble stack”: conectividad con servidores IPv4 e IPv6.
- Estrategias de Migración de Redes Finales (clientes y servidores):
 - **Mediante Mecanismos de Traducción:**



Estrategias Migración (II)

- Mediante Mecanismos de tipo Túnel:
 - Primera Fase: conexión IPv4 al ISP y entunelar el tráfico IPv6 en IPv4, hasta que el ISP ofrezca conexión con IPv6 Nativo.



- Segunda Fase: Conexión IPv6 al ISP y túnel IPv4 sobre IPv6 para conectar Internetv4 (caso complementario).

Estrategias Migración (III)

- Estrategias de Migración para ISPs:
 - Conexión nativa a Backbones IPv4 e IPv6, si no emplear túneles.
 - Modos de Acceso:
 - ISP IPv4 Tradicionales: Acceso IPv4 y tratar de ofrecer acceso a Internetv6 mediante un traductor.
 - Nuevos ISP IPv6: Acceso IPv6 y mediante túnel a través de Internet. Ofrecer conectividad a Internetv4 mediante traductores.

- Estrategias de Migración de Backbones:
 - Mantener configuración actual y migrar cuando tráfico entunelado > tráfico IPv4.
 - Debido a los problemas del número de rutas existente, recomendar y colaborar con los ISP y otros Backbones para evitar una migración “forzosa”.