

# Servicios de comunicaciones móviles basados en IPv6 (MIPv6), Beneficios y Retos



LACNIC X

5º Foro Latinoamericano de IPv6 -  
FLIP-6

25 de Mayo de 2007

César Olvera, Miguel A. Díaz  
CONSULINTEL

[cesar.olvera@consulintel.es](mailto:cesar.olvera@consulintel.es)  
[miguelangel.diaz@consulintel.es](mailto:miguelangel.diaz@consulintel.es)



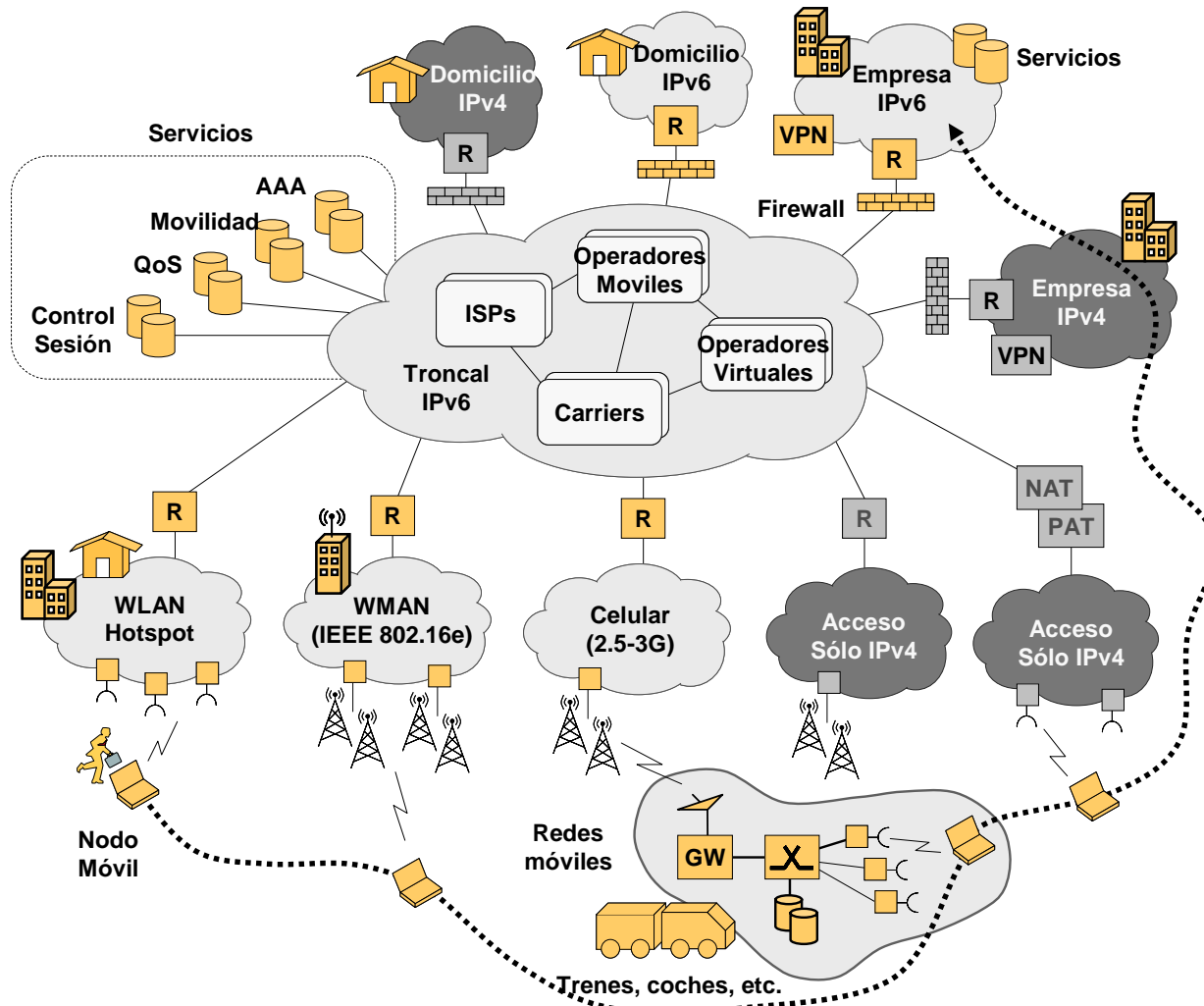


# Objetivo

- El modelo de conectividad a Internet está evolucionando rápidamente
  - Aparición de nuevos dispositivos portátiles
  - Más extensa cobertura de las redes de acceso
  - Hacia un enfoque basado en la movilidad de los usuarios
- Los operadores ven una fuente importante de ingresos en un servicio de movilidad basado en IPv6 (MIPv6)
  - Que permita a sus usuarios ser siempre alcanzables con independencia de la red en la que se encuentren
- Sin embargo, aunque MIPv6 está estandarizado desde hace tiempo, aún quedan algunos flecos que es necesario resolver para permitir el despliegue a gran escala del servicio de movilidad



# Servicios de comunicaciones móviles

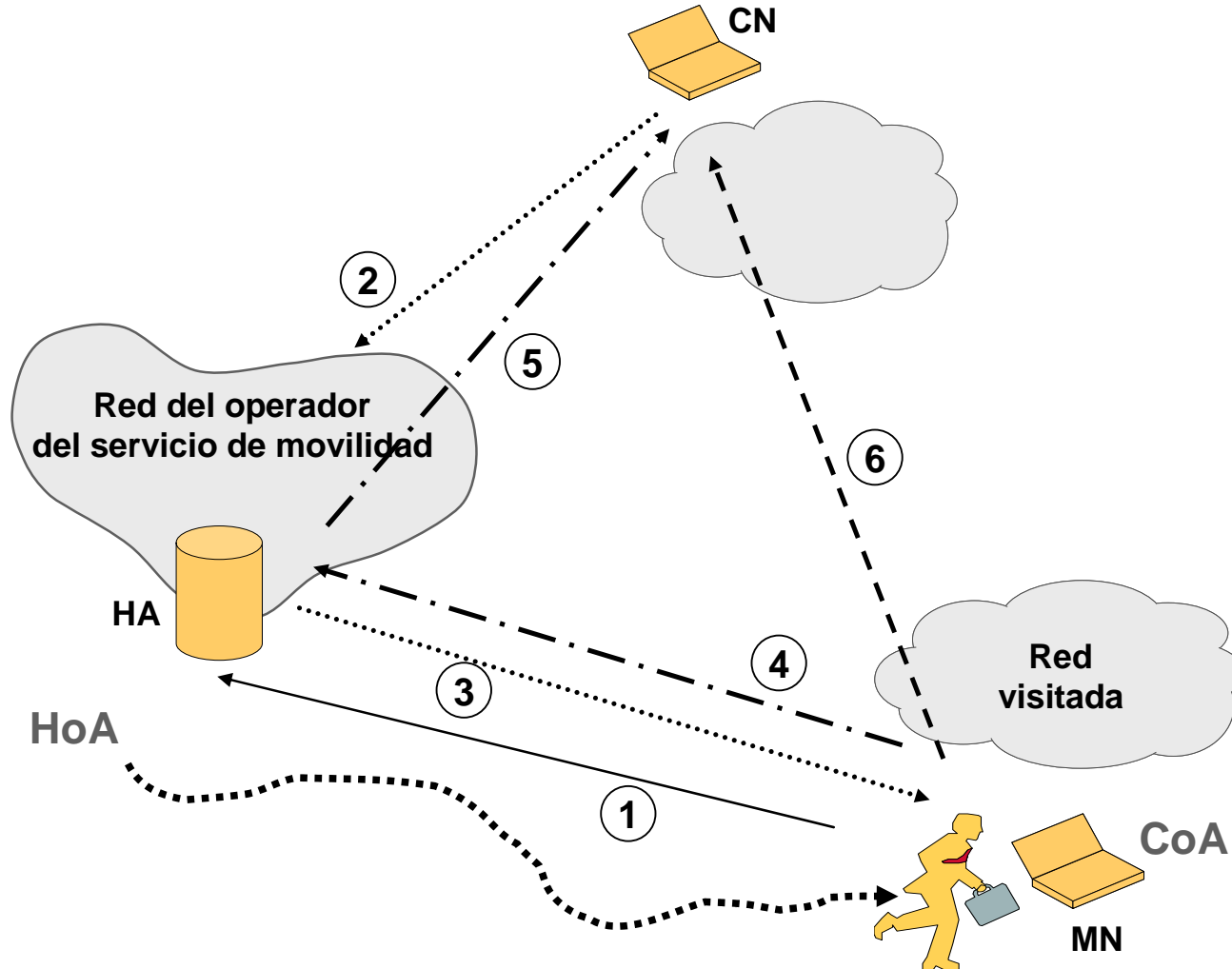


# Componentes de MIPv6

- Home Agent (HA)
  - Agente que se despliega en la red del operador que despliega el servicio de movilidad
  - Es el encargado de tener registrada la “verdadera posición” del nodo móvil
- Mobile Node (MN)
  - Dispositivo del usuario
  - Cuando se encuentra en la red de su operador tiene una dirección IPv6 denominada Home Address (HoA)
  - Cuando se desplaza y se encuentra en una red visitada adquiere una dirección IPv6 diferente, denominada Care-of Address (CoA)
- Correspondent Node (CN)
  - Nodo que pretende contactar con el MN
  - En principio, si no sabe cual es su posición real trata de contactar usando la HoA del MN



# Funcionamiento básico de MIPv6





# MIPv6

- Mecanismo básico esta estandarizado por IETF
  - RFC3775 “Mobility Support in IPv6”
  - Proporciona la definición de los agentes involucrados en el soporte de movilidad, su funcionamiento y sus interacciones
  - Funciona de una manera efectiva y eficiente si pensamos en un despliegue
    - ❑ Experimental o a baja escala
    - ❑ Donde participen muy pocos usuarios
    - ❑ Donde la configuración de los agentes implicados es predominantemente manual
- Sin embargo si pensamos en movilidad como servicio de producción en un operador, el marco de estandarización actual no es suficiente
  - Para que sea posible el despliegue de MIPv6 a gran escala en un operador, con centenas o millares de usuarios, es necesario aún cierto trabajo
    - ❑ Configuración dinámica de los nodos que intervienen en el servicio de movilidad
    - ❑ Funcionamiento de MIPv6 en las redes visitadas
  - Como el que se está realizando en el proyecto **IST ENABLE**
    - ❑ Análisis de los principales problemas y las soluciones propuestas por el proyecto



# IST ENABLE

- <http://www.ist-enable.eu/>
- Proyecto IST co-financiado por la UE
- Objetivo principal: conseguir el despliegue a gran escala del servicio de movilidad de una manera eficiente y sobre entornos IPv6, teniendo también en cuenta la transición desde IPv4
- El proyecto aborda entre otros, los temas aún abiertos y para los que no existe una solución estandarizada, contribuyendo para ello con diversos organismos de estandarización como IETF, 3GPP, etc.
  - Diseño de una arquitectura de referencias que permita la integración de los agentes involucrados en un servicio de movilidad real a gran escala
  - Mejora de MIPv6 para habilitar una movilidad transparente en grandes redes de producción con múltiples dominios administrativos, tipos de acceso heterogéneos y un número elevado de usuarios
  - Enriquecimiento de MIPv6 básica con un conjunto de características avanzadas como QoS, Fast Handover, etc.
  - Análisis de los objetivos y diseño de los principios que permitan la evolución de MIPv6 a largo plazo
  - La investigación y desarrollos que se está llevando a cabo el proyecto permitirá el despliegue robusto del servicio de movilidad sobre IPv6 con un uso intensivo de la red con aplicaciones como multimedia (vídeo y audio), servicios de localización, emergencia, etc. Y además que soporte posibles evoluciones futuras



# MIPv6 en redes grandes

- Principales problemas y las soluciones consideradas
  1. Inicialización y configuración dinámica de los nodos que intervienen en el servicio de movilidad
    - Bootstrapping
  2. Funcionamiento de MIPv6 en las redes visitadas
    - Atravesar los Firewalls
    - Funcionamiento en redes sólo-IPv4



# 1. Inicializando el servicio de movilidad

- Cuando un usuario inicia el servicio de movilidad
  - Está en disponibilidad de ser alcanzado siempre a través de la misma dirección IP (su HoA)
  - Incluso aunque se desplace y se encuentre en otras redes diferentes a las de su operador
- Sin embargo para que esto pueda llevarse a cabo es necesario realizar una serie de pasos para la configuración automática y de forma dinámica del servicio de movilidad
  - Autenticación y autorización del usuario
  - Asignación del HA
  - Intercambio del material criptográfico



# Autenticación y autorización del usuario

- Cuando un proveedor ofrece el servicio de movilidad
  - Primero debe afrontar la identificación del usuario (autenticación)
  - Posteriormente comprobar si dicho usuario tiene derecho a disfrutar del servicio de movilidad (autorización)
  - Y en su caso computar el tiempo que ha estado disfrutando del servicio para su posterior facturación
  - Estos son requisitos básicos no cubiertos por el marco de estandarización actual de MIPv6, y que el operador precisa para el despliegue de cualquiera de sus servicios comerciales
- Este tipo de funciones se realizan habitualmente por medio de una infraestructura de AAA (Authentication, Authorization and Accounting), basada en los protocolos RADIUS o Diameter



# Asignación del HA

- Para el servicio de movilidad el proveedor debe ser capaz de proporcionar diversos datos relacionados con la red del proveedor
  - Debe proporcionar la Home Network (HN), es decir, el prefijo de la red a la que el MN del usuario pertenece de forma permanente mientras éste se encuentra desplazándose por otras redes
  - Además el MN debe ser configurado con la dirección IPv6 que tendrá dentro de la HN, es decir la Home Address (HoA)
    - Para ello el proveedor podrá proporcionársela al MN mediante algún mecanismo no estandarizado aún, o alternatively y gracias a las características de auto configuración de IPv6, este podría ser capaz de crear su propia HoA una vez sabido el prefijo de la HN a la que pertenece
- Por otra parte, con el despliegue a gran escala de este tipo de servicios, es posible que existan varios HAs con el fin, no solo de conseguir una redundancia del servicio ante eventuales averías de alguno de estos nodos, sino también para poder distribuir de una manera eficiente la carga de procesamiento de paquetes para atender a todos los usuarios demandantes del servicio
  - El estándar de MIPv6 define un método básico para descubrir un HA una vez conocida la HN, el cual se basa en el uso de direcciones IPv6 de tipo anycast
  - Sin embargo este método no permite un reparto equitativo de la carga de procesamiento entre los diversos HAs existentes
  - Por lo que es mucho más recomendable la definición de un mecanismo que sea capaz de asignar un determinado HA al MN de un usuario cuando este solicita el inicio del servicio
  - Además dicho mecanismo debería ser capaz de reasignar al MN un nuevo HA en el caso de detectar que el que se le ha asignado inicialmente está sobrecargado o incluso se ha averiado



# Intercambio del material criptográfico

- El uso ESP de IPsec es uno de los métodos definidos en MIPv6 para la protección de los paquetes de señalización entre el MN y HA
  - Con este mecanismo se garantiza la autenticación mutua de los nodos y además se proporcionan herramientas para la encriptación de los paquetes intercambiados entre los nodos que utilizan el servicio de movilidad
  - Así pues con la protección de la señalización con IPsec además de confidencialidad se consigue garantizar que dichos paquetes no han sido modificados en el camino hasta llegar a nodo destino
  - Pero para que IPsec funcione apropiadamente es necesario definir en ambos nodos (MN y HA) el material criptográfico adecuado que permita establecer las Security Associations (SAs) que IPsec maneja durante su funcionamiento
- De nuevo el estándar de MIPv6 no define ningún método en concreto para el intercambio del material criptográfico entre los nodos que permita el establecimiento de las SAs
  - Una alternativa habitual es la configuración manual de las claves utilizadas en el establecimiento de las SAs
    - ❑ Obviamente esta solución no es viable en el caso del despliegue de un servicio a gran escala en un operador
  - También se puede emplear el protocolo IKE como herramienta para la automatización del intercambio de claves y establecimiento de SAs
    - ❑ Sin embargo es un protocolo demasiado complejo y difícil de depurar como para ser usado en un entorno con millares de usuarios.
  - Finalmente, el uso de IKEv2 parece más recomendable puesto que es un protocolo más simple, con posibilidades reales de ser implementado en dispositivos portátiles que se caracterizan por la escasez de recursos hardware (capacidad de procesamiento, memoria, etc.), aunque de nuevo no hay ninguna estandarización o recomendación de cómo integrar este protocolo en el servicio de movilidad



# Bootstrapping

- Los tres pasos anteriores son esenciales para que un MN pueda iniciar el servicio de movilidad
  - Lo deseable es poder realizarlos de la manera más rápida posible con el fin de que el usuario no tenga que realizar largas esperas durante el inicio del servicio
  - La mejor solución para ello es agrupar todos esos pasos en un procedimiento único mediante el cual el usuario
    - se autentica frente al operador
    - se le informa de diversos parámetros de red (HN, HoA) necesarios para el inicio de la movilidad
    - se le asigna un HA y se establece el material criptográfico para el establecimiento de las SAs que permitan cifrar la señalización MIPv6
- A este procedimiento único se le conoce con el término de MIPv6 Bootstrapping
- ENABLE ha estado trabajando para identificar los diferentes escenarios en los que se puede realizar el Bootstrapping, los agentes que intervienen y el modo en el que interactúan
  - RFC4640 "Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)"



## 2. Problemas de MIPv6 en las redes visitadas

- Existen dos obstáculos principales para que MIPv6 pueda funcionar en las redes visitadas
  - Presencia de Firewalls que filtren los paquetes de tipo MIPv6
  - Falta de soporte IPv6 en la red visitada por el usuario.



# Atravesando los Firewalls (I)

- En MIPv6 existen dos tipos de tráfico
  - Tráfico de señalización que se encarga de iniciar y mantener el servicio de movilidad activo entre los agentes (HA-MN y CN-MN)
  - Tráfico de datos que transporta los datos de aplicación de la comunicación entre el CN y el MN
- El tráfico MIPv6 utiliza cabeceras de extensión IPv6 específicamente diseñadas para el servicio de MIPv6
  - Lo cual puede representar un problema cuando existen Firewalls instalados en cualquiera de las redes en las que se encuentran los nodos que intervienen en la movilidad (MN, HA y CN)
- Puede ser que los Firewalls no soporten MIPv6
  - No entienden ni las cabeceras de extensión MIPv6 ni el tráfico que llevan
  - Por tanto, dicho tráfico será directamente bloqueado e impedirá el funcionamiento del servicio de movilidad
- Los problemas derivados de la presencia de Firewalls sin soporte MIPv6 son básicamente tres. En los cuales el Firewall:
  - No entiende los mensajes de señalización MIPv6 (BU, BA, CoTI, HoTI) y por tanto se descartan
    - Como consecuencia no se puede iniciar el servicio de movilidad
  - No permite el paso de paquetes IPsec puesto que no es capaz de saber cual es su contenido
    - Como consecuencia los paquetes de señalización MIPv6 entre el MN y el HA no llegan a su destino y no se puede iniciar el servicio de movilidad
  - No entiende los mensajes con cabeceras MIPv6 por lo que el tráfico de datos es descartado
    - Como consecuencia no es posible la comunicación entre el CN y el MN



# Atravesando los Firewalls (II)

- En función de si existen uno o varios Firewalls y de la red en la que se encuentren (red del HA, red visitada por el MN o red del CN) se pueden presentar alguno o todos de tales problemas
- En ENABLE se han analizado y evaluado diversas tecnologías como posibles soluciones para este problema
  - Universal Plug and Play, STUN/TURN/ICE, Application Layer Gateways, Middlebox Communication, Simple Middlebox Control, NSIS y NAT/FW NSLP y Policy Based Networks
- NSIS apunta ser el protocolo más prometedor que ayudaría a solventar este problema
- La gran ventaja de NSIS frente al resto de tecnologías
  - Define una arquitectura y un protocolo de señalización que permite a los nodos que manejan tráfico MIPv6 informar a todos los Firewalls que se deben atravesar hasta alcanzar el destino, del tipo de tráfico que están enviando y de sus características, con el fin de que los Firewalls se configuren de forma apropiada para que ese tráfico sea cursado



# Funcionamiento en redes IPv4 (I)

- MIPv6 es un protocolo diseñado para funcionar sobre redes IPv6
  - Sin embargo aunque un operador decida realizar el despliegue de IPv6 y MIPv6 en su red para proporcionar servicios a sus usuarios, no es una garantía de que el servicio sea operativo en cualquier escenario en el que se encuentre el usuario en sus desplazamientos
  - Es muy probable que durante un período de tiempo, existan otros operadores en los que no se realice el despliegue de IPv6 y por tanto sus redes sean solo IPv4
- Esto supone un problema cuando un usuario del servicio de movilidad debido a su desplazamiento se encuentra en este tipo de redes
  - Al tener solo conectividad IPv4 el MN no será capaz de contactar con el proveedor del servicio de movilidad, es decir, con el HA
- Un despliegue real del servicio MIPv6 tiene que considerar esta problemática y solucionarla
  - A pesar de que IPv6 hace tiempo que ha dejado de ser un protocolo experimental y empieza a estar desplegado en las redes de los operadores más importantes, es seguro que durante un período de tiempo indeterminado habrá otros operadores que no desplieguen este protocolo en sus redes



## Funcionamiento en redes IPv4 (II)

- En ENABLE se vislumbran dos aproximaciones distintas para dar solución a la problemática de que el MN esté conectado en una red IPv4 y quiera contactar con el HA en una red IPv6
  - Utilizar el mecanismo de transición **IPv6 Softwires** para que el MN sea capaz de obtener conectividad IPv6 (a pesar de que esté conectado en una red IPv4) y posteriormente utilizar MIPv6 de forma normal como si estuviera conectado a una red IPv6 nativa
  - Utilizar las **extensiones del protocolo MIPv6 (DSMIPv6)** que están siendo definidas en el IETF con el fin de que el MN pueda encapsular los paquetes MIPv6 dentro de paquetes IPv4 para hacerlos llegar al HA



# Conclusiones

- El modelo basado en la movilidad de los usuarios MIPv6 se irá implantando en los próximos años debido a un diseño robusto y eficiente, que lo diferencia de su antecesor MIPv4
- Sin embargo aún existen algunos flecos en la estandarización de MIPv6 que necesitan ser abordados para ofrecer soluciones que permitan el despliegue a gran escala de MIPv6
- A medida que proyectos como ENABLE avancen en sus objetivos y una vez que se finalice el diseño de una arquitectura de referencia que solvete los problemas tratados en las secciones anteriores, los usuarios estarán en disposición de entrar en un nuevo mundo de servicios móviles



# Referencias

- Proyecto IST ENABLE (Enabling efficient and operacional mobility in large heterogeneous IP networks), <http://www.ist-enable.eu/>
- RFC3775 "Mobility Support in IPv6", Junio 2004
- RFC3776 "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", Junio 2004
- RFC4225 "Mobile IP Version 6 Route Optimization Security Design Background", Diciembre 2005
- RFC4283 "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", Noviembre 2005
- RFC4285 "Authentication Protocol for Mobile IPv6", Enero 2006
- RFC2865 "Remote Authentication Dial In User Service (RADIUS)", Junio 2000
- RFC3588 "Diameter Base Protocol", Septiembre 2003
- RFC2462 "IPv6 Stateless Address Autoconfiguration", Diciembre 1998
- RFC2526 "Reserved IPv6 Subnet Anycast Addresses", Marzo 1999
- RFC2406 "IP Encapsulating Security Payload (ESP)", Noviembre 1998
- RFC2409 "The Internet Key Exchange (IKE)", Noviembre 1998
- RFC4306 "Internet Key Exchange (IKEv2) Protocol", Diciembre 2005
- RFC4640 "Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)", Septiembre 2006
- "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", draft-ietf-nsis-nslp-natfw, Trabajo en curso
- "Softwires Hub & Spoke Deployment Framework with L2TPv2", draft-ietf-softwire-hs-framework-l2tpv2, Trabajo en curso
- "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mip6-nemo-v4traversal, Trabajo en curso



# Preguntas

