Foro Seguridad RedIRIS, abril 2013

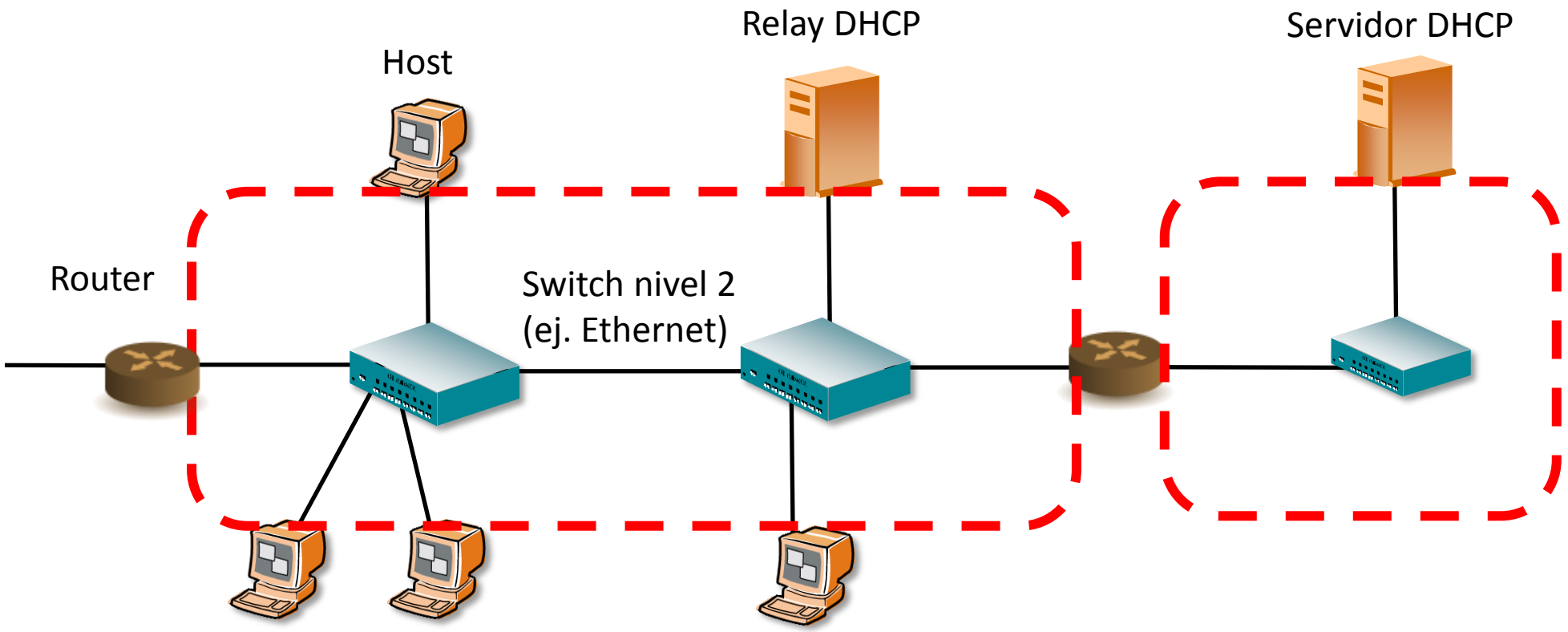
SEcure Neighbor Discovery (SEND)

Alberto García Martínez

U. Carlos III de Madrid

El enlace

- **Link, según definición de RFC 4903**

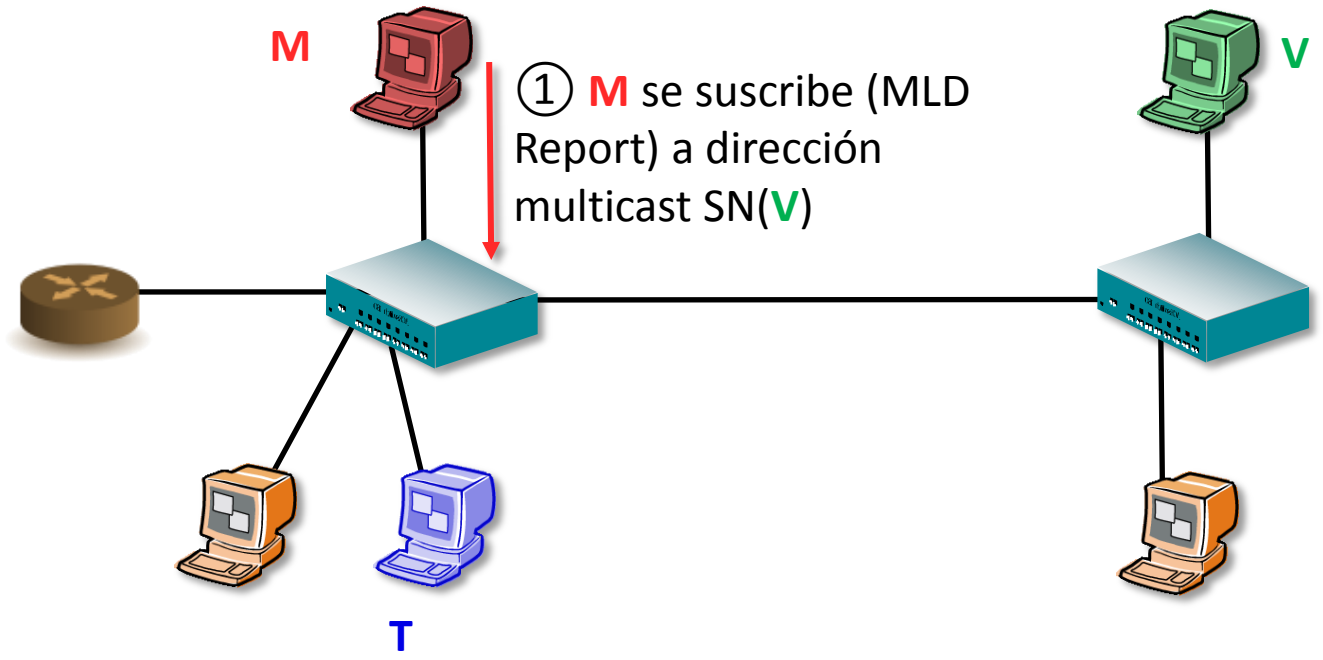


Repaso de algunos mecanismos básicos relacionados con IPv6

- **IP identifica a interlocutor por la dirección fuente de un paquete recibido**
  - **Utilizado por protocolos de nivel superior como TCP y UDP**
- **Neighbor Discovery**
  - **Mensajes Router Solicitation (RSol)/Router Advertisement (RAdv)**
    - **Routers mandan RAdv, que informa de**
      - Identificación de routers en el enlace
      - Prefijos para configuración de direcciones y determinación de prefijos *on-link*
  - **Mensajes Neighbor Solicitation (NSol)/Neighbor Advertisement (NAdv)**
    - **Muy parecido a ARP**
    - **Funciones**
      - Resolución de dirección (IP a MAC)
      - Detección de direcciones duplicadas
      - Neighbor Unreachability Detection
  - **Mensaje Redirect**
- **Niveles inferiores: Ethernet aprende MAC a partir de la dirección fuente de las tramas recibidas (‘*transparent bridging*’, ‘*backward learning*’)**

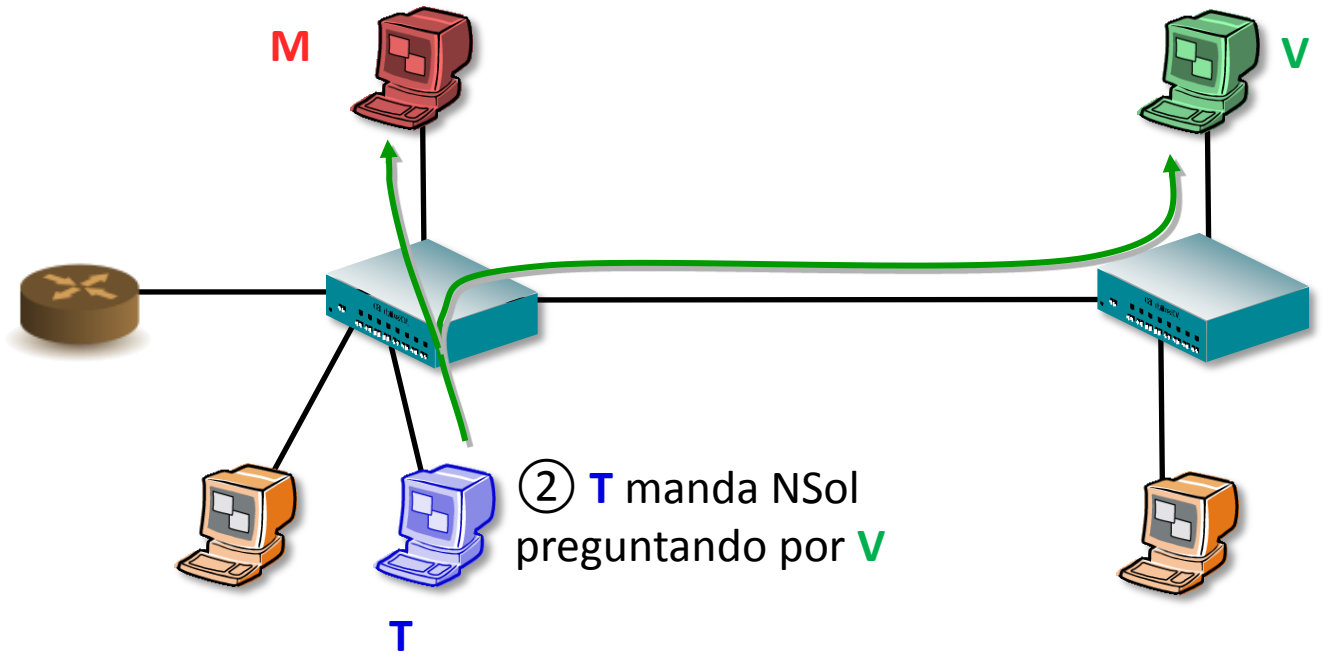
Ejemplo de ataque en un enlace

- Nodo M desea suplantar a nodo V sólo en comunicación T ↔ V



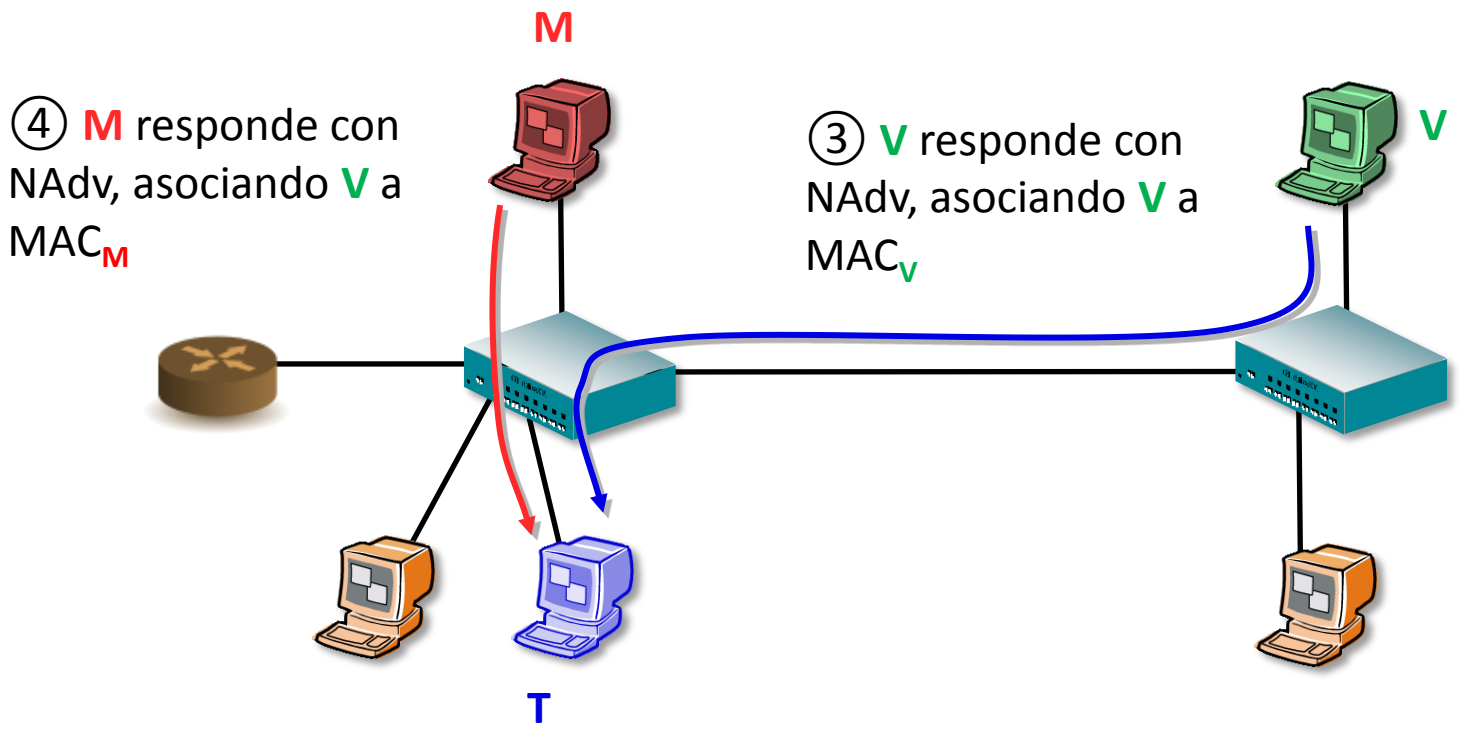
Ejemplo de ataque en un enlace

- Nodo M desea suplantar a nodo V sólo en comunicación T ↔ V



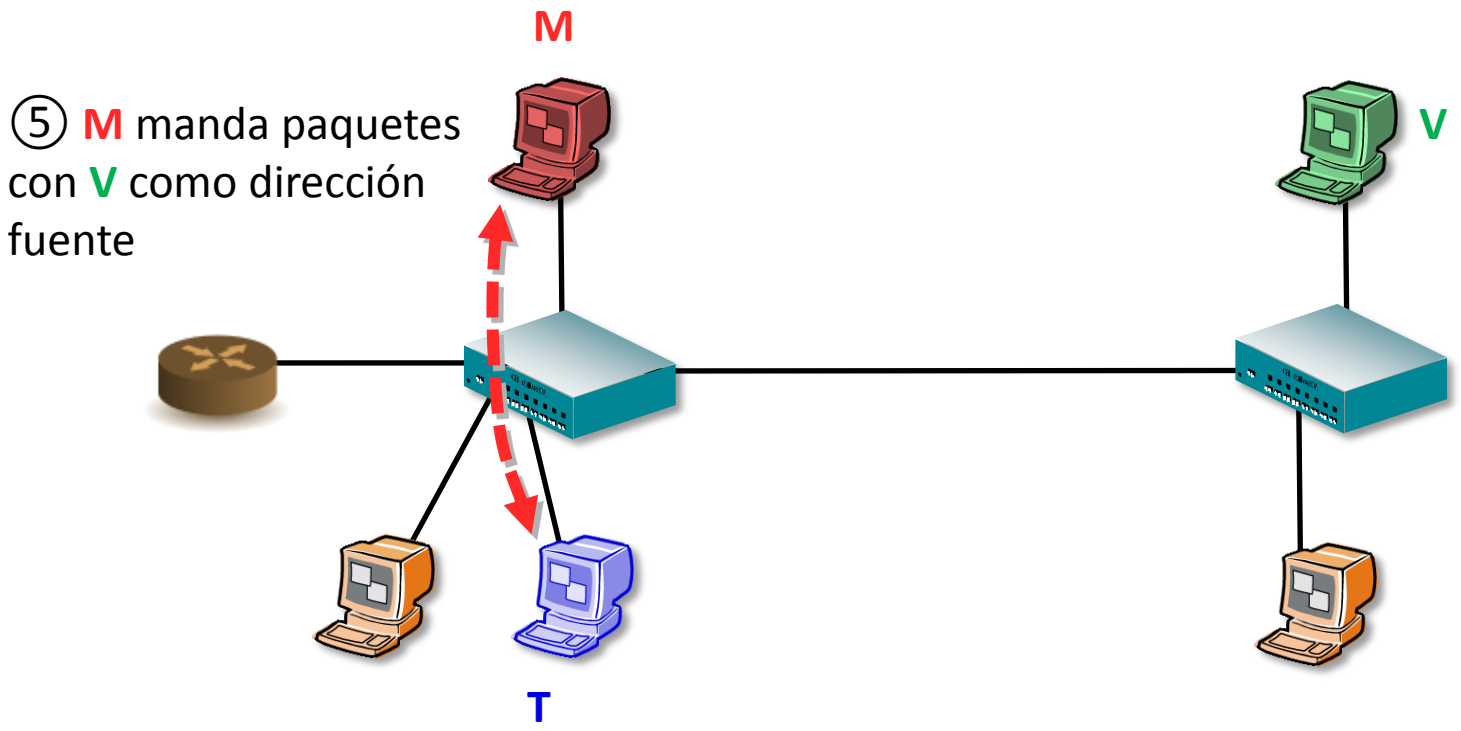
Ejemplo de ataque en un enlace

- **Nodo M desea suplantar a nodo V sólo en comunicación T ↔ V**



Ejemplo de ataque en un enlace

- **Nodo M desea suplantar a nodo V sólo en comunicación T ↔ V**



Amenazas en el enlace

- Atacante manda paquetes con dirección fuente que no le corresponde (*IP spoofing*)
- Atacante utiliza NSol/NAdv para hacer que otros nodos asocien 'de forma ilegítima' pares <IP, MAC>
- Atacante utiliza NSol/NAdv para impedir que otro nodo configure su dirección IPv6
- Atacante utiliza RAdv para identificarse como router en el enlace
  - Equipos en la red mandan al atacante paquetes dirigidos fuera del enlace
- Atacante genera paquetes con MAC fuente que no le corresponde para influir en aprendizaje de los switches Ethernet
  - Switches le mandan tráfico para esa MAC

Espacio de soluciones

- IPsec?
- Soluciones manuales:
  - Configurar filtros en los switches (Port Access List),
  - Indicar qué equipos son routers, filtrar tráfico en los switches de acuerdo a esto (RA Guard – Cisco, Juniper…)
- Definir soluciones 'automáticas' que cubren distintas partes del problema
  - SEcure Neighbor Discovery (SEND, RFC 3971)
    - ✓ Definido para proteger intercambio de Neighbor Discovery
  - Source Address Validation Implementation (SAVI)

Criterios de diseño para SEND

- Proteger sólo intercambio de información ND
  - ¡NO protege tráfico de datos!
- Proteger identidades a nivel IP
  - Sólo nodo con IP legítima puede propagar información ND asociada a esa IP
    - ✓ Sólo nodo con IP legitima puede asociar MAC a esa IP, responder a DAD para esa IP, etc.
  - Solo router legítimamente autorizado puede identificarse como tal
    - ✓ Propagar prefijos, etc.
- Mínimos mensajes adicionales (respecto a ND)
- Robusto frente a repetición de mensajes
- Asume que los hosts y routers cambiarán el software (tendrán que ser 'SEND-capable')
- Mínima configuración en hosts
  - No quiero configurar una clave pública por cada host vecino
  - Ni siquiera tener que emitir un certificado por cada host!
- No busca confidencialidad

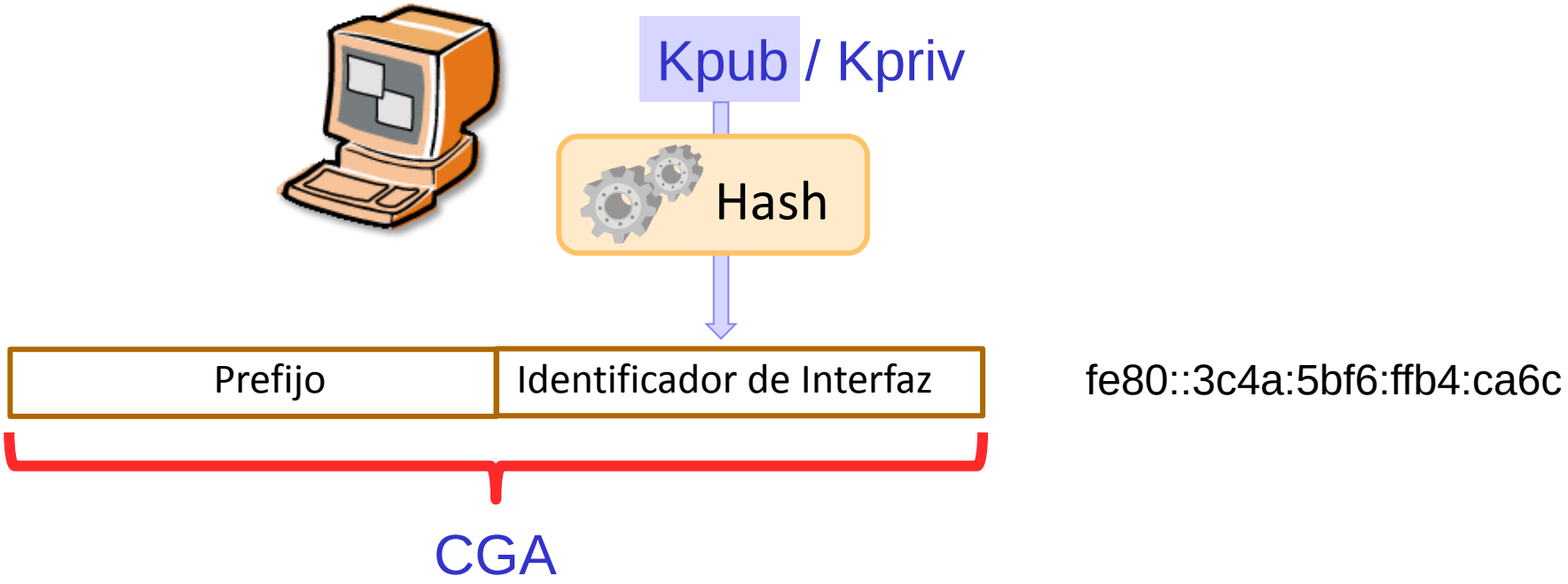
Diseño

- ¿Como hacer que ‘Sólo nodo con IP legítima puede propagar información ND asociada a esa IP’?
  - Nodos tienen dirección IPv6 que sólo ellos pueden probar que les corresponde: CGA
  - Dirección asociada a un par clave pública/clave privada con la que pueden firmar mensajes ND

CGA

Cryptographically Generated Addresses, RFC 3972

- **Dirección IPv6 que se genera de la siguiente forma**
  - **Generar par clave privada/pública**
  - **Identificador de interfaz de la dirección IPv6 se obtiene a partir de hash de la clave pública (y de alguna cosa más: prefijo de la dirección…)**
  - **Prefijo es el asignado al enlace**



CGA

- En CGA, están fuertemente ligados clave pública y dirección IPv6!
- Mensajes ND en SEND incorporan una opción en la que viaja la clave pública del emisor
  - Receptor puede comprobar si el hash de la clave pública se corresponde con la dirección IPv6 fuente del paquete recibido
- La comprobación NO requiere configuración!
- Una CGA puede ser link-local, global, etc.

Firma de información de ND

Mensaje NAdv

Dirección fuente = CGA_H; Direccion destino = … (multicast, unicast)

Información ND: MAC de H

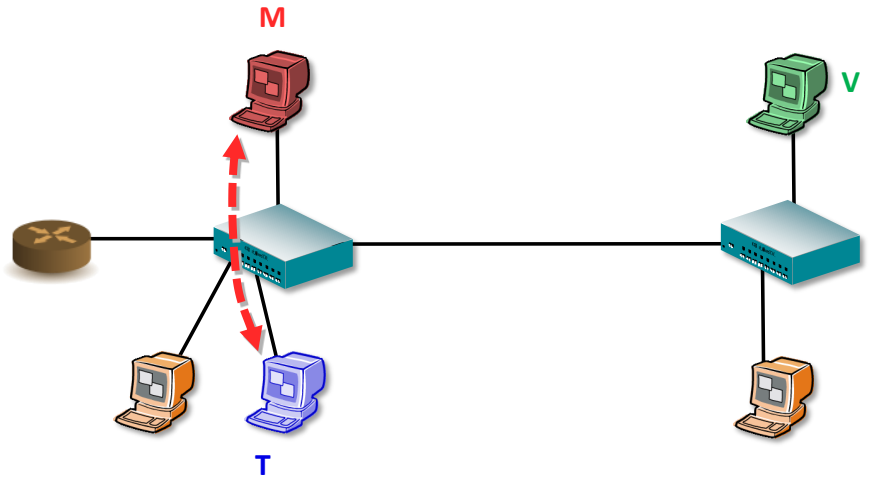
Opciones SEND añadidas a mensaje ND:

Clave pública asociada a CGA_H

Firma con clave privada de H de la información

- **Emisor firma los mensajes ND que genera con la clave privada asociada a la CGA**
  - **Firma incluida como opción en mensaje ND**
- **Nodo receptor VALIDA mensaje**
  - **Utiliza clave pública del emisor incluida en mensaje para validar su IPv6**
    - ✓ **Si no hay correspondencia entre hash(clave pública) y dirección fuente del mensaje ND, el mensaje se descarta**
  - **Con clave pública de la CGA, valida firma del mensaje ND**
  - **Como las direcciones IPv6 incluidas en NAdv como Target tienen que ser iguales que la dirección fuente del mensaje, implícitamente valida los datos contenidos en NAdv**

¿Cómo romper SEND?



- **Para poder suplantar a una dirección IPv6 en SEND, atacante puede**
  - a) **generar par clave pública/privada tal que hash sea igual que el de la dirección suplantada**
    - ✓ **Complejidad: del orden de 2^61 pruebas**
  - b) **obtener la clave privada a partir de la clave pública**
    - ✓ **Todavía más difícil!**

Autorización de función de routers

- Es el administrador el que indica qué equipo puede actuar como router
  - Aquí SÍ que hace falta algo de configuración
- Administrador firma certificado X509.3 'esta clave pública es de un router'
  - Hosts validan mensajes RAdv con la clave pública de este certificado
  - El certificado también puede restringir el rango de prefijos permitidos para anuncios RAdv
- Mensajes nuevos para transportar certificados desde el host al router
  - Certification Path Solicitation (CPA), generado por el host hacia ff02::2
  - Certification Path Advertisement (CPS), respuesta de un router a un host
- Hosts tienen configurado 'trust anchor' que valida alguna rama superior del certificado

CPA
Certificate 2: Issuer: mi_red.net
Validity: Jan 1, 2013 through Dec 31, 2013
Subject: router1.link1.mi_red.net

CPA
Certificate 2: Issuer: mi_red.net
Validity: Jan 1, 2013 through Dec 31, 2013
Subject: router13.link2.mi_red.net

Trust anchor
Certificate 1: Issuer: mi_red.net
Validity: Jan 1, 2013 through Dec 31, 2013
Subject: mi_red.net

Limitaciones

- Sólo protege ND
  - No protege frente a IP spoofing de paquetes distintos de ND
  - No protege frente a MAC spoofing
- Incluso en ND, sólo protege a nivel IP
  - Un nodo que utilice su IP puede generar NSol con IP ←→ MAC_{falsa}
- En general, requiere configuración de trust anchor en los hosts
  - Dificultad si se cambia de organización
  - Sería fácil si hubiera cadena de certificación desde autoridad conocida (como RPKI)
- Coste computacional de firmar y validar
  - (Aunque sólo para mensajes ND, ¡no se firman mensajes de datos!)
- No bien resuelta coexistencia equipos SEND/no-SEND en el mismo enlace
- Problema 'huevo o gallina' en la verificación de la validez de los certificados de los routers
  - No se pueden chequear revocaciones hasta que se obtenga comunicación con el exterior
  - Para obtener comunicación con el exterior, hay que aceptar el certificado de un router

Implementaciones

- **Routers: Cisco, Juniper**
- **Hosts, básicamente pruebas de concepto**
  - **Linux:**
    - ✓ **amnesiak.org/ndprotector/**
    - ✓ **https://code.google.com/p/ipv6-send-cga/**
    - ✓ **http://sourceforge.net/projects/easy-send/ (JAVA)**
  - **Windows: Windows Secure Neighbor Discovery (WinSEND)**

¿y comparado con IPv4?

- Problema parecido en resolución de direcciones mediante ARP
- Pero… algo más grave en IPv6 porque
  - El router se determina mediante RAdv (en IPv4 mediante DHCP o por configuración manual)
  - DAD permite impedir que un equipo configure direcciones
- Solución de SEND no trasladable a IPv4: depende de CGA, que requiere muchos bits en la dirección, no disponibles en IPv4

¿Preguntas ???????