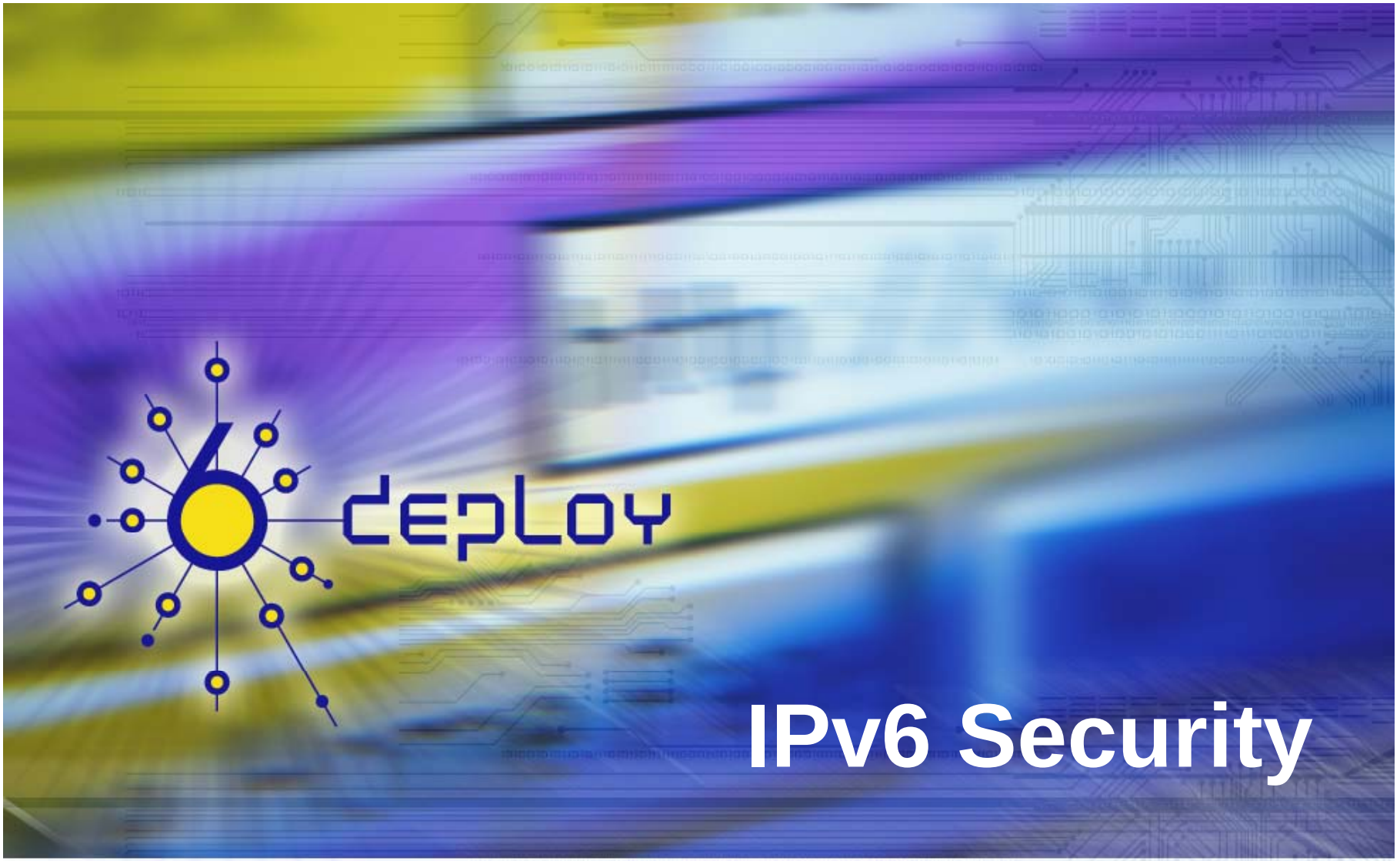


IPv6 Security

Athanassios Liakopoulos (*aliako@grnet.gr*)

EFIPSANS IPv6 Training, Budapest, Hungary

Copy …Rights

IPv6 Deployment and Support

- *This slide set is the ownership of the 6DEPLOY project via its partners*
- *The Powerpoint version of this material may be reused and modified only with written authorization*
- *Using part of this material must mention 6DEPLOY courtesy*
- *PDF files are available from www.6diss.org*
- *Looking for a contact ?*
  - ***Mail to : martin.potts@martel-consulting.ch***
  - ***Or: bernard.tuy@renater.fr***

Contributors

IPv6 Deployment and Support

- János Mohácsi, NIIF/HUNGARNET - Hungary
- Octavio Medina, Octavio Medina, Laurent Toutain, ENST
- Bernard Tuy, Jérôme Durand, Emmanuel Goiffon, Renater
- Peter Kirstein, Steve Hailes, Piers O'Hanlon, UCL
- Wolfgang Fritsche, IABG
- Jim Bound, Hewlett Packard
- Patrick Grostete, Archrock
- Mohsen Souissi, AFNIC
- Alain Durand, Sun Microsystems
- Bill Manning, ISI
- Alain Baudot, France Telecom R&D
- … and many others

Table of Contents

IPv6 Deployment and Support

What's the big problem?

IPv6 Deployment and Support

- We have firewalls and intrusion detection systems, so we're safe from outside attack
- VPNs, RADIUS, SSH, etc. allow secure remote access
- PKI may be used to determine node identity
- S/MIME or PGP protects electronic messages
- SSL/TLS protects web access
- Virus scanning is effective
- Security patches can be applied centrally
- IPv6 has complete built-in security
- *… and it's always sunny outside, pink bunnies play happily in streets, all are kind to old ladies …*

Why is there a problem?

IPv6 Deployment and Support

- Hostile environment
- Diverse motivations for attackers
- Lack of security consciousness
- Lots of potential points of attack
- Security policies are often considered as unacceptable
- No regulatory framework
- Legal aspects unclear

Why is there a problem?

IPv6 Deployment and Support

- If you believe that encryption (or firewalls or intrusion detection systems) are the answer to all your security problems, then you probably asked the wrong question
- Security is about securing a *system*
- Security is a ***process,*** not a product
- Concentration on technology is deeply naïve
- If you do major changes, such as enabling IPv6 in a network, you must ensure you haven't introduced new security holes

Security Threats

IPv6 Deployment and Support

- Network
  - passive tap, active tap, denial of service (DoS), faking, replay, traffic analysis, etc
- Other
  - physical attack, trojan horses, viruses, worms, logic bombs, passwords, loopholes, collusion, accidental access, tempest, social engineering, etc

Security Services

IPv6 Deployment and Support

- **Authentication**
  - verify that received data or user is appropriate
- **Integrity**
  - ensure that received data is not altered
- **Confidentiality**
  - ensure that unintended parties cannot determine what was sent
  - ensure that datagram is not intercepted and playedback at some later time
- **Non-repudiation**

Cost Effective Security

IPv6 Deployment and Support

- Does *absolute* security exist?
- Security means effort & cost
- Compromise on the level of security but …
  - … evaluate risks
  - … evaluate cost of losses
- Estimating cost effective security is complex task as you don't know …
  - … motivations of attacker
  - … value of information or goodwill

New Environment – Problems

- Wireless communications today are widely used

New Environment – Problems

- Infrastructure doesn’t protect data
- Applications can’t be trusted to secure data
- New forms of viruses?
- Security in mobile devices not standardised (in many operating systems)
- Devices easy to lose (or steal) or break
- Radio is a broadcast medium
- Most mobile devices come with security disabled
- Data loss is painful; the more so the more one relies on it

So what's to be done?

IPv6 Deployment and Support

- Play Luddite?
- Wireless nodes will always be resource scarce compared to equivalent wired nodes
- Actually, there is (going to be) a LOT of heterogeneity in this space
  - Low mobility high b/w devices (e.g. 802.11)
  - High mobility low b/w devices (e.g. cell phones to RFID tags)
  - IPv4/IPv6 heterogeneous protocol suites
- The UIs will not be getting significantly better
- There's battery lifetime to consider (new DoS attacks)
- Much of it is going to look very different from now ...

What is new with IPv6?

IPv6 Deployment and Support

- **Security was considered from the beginning in IPv6 protocols design**
  - When new services were considered, their security was part of IPv6 thinking
    - Threats to mobile access and mobile IP, protocols for authentication and network access, making intrusion harder
- **Some of the key improvements:**
  - IPsec is mandated to be supported in host-to-host communications
  - Cryptographically Generated Addresses (CGA)
  - SEcure Neighbor discovery (SEND)

Threats to be encountered in IPv6

IPv6 Deployment and Support

- Scanning Gateways and Hosts
- Scanning for Multicast Addresses
- Unauthorised Access Control
- Firewalls
- Protocol Weaknesses
- Distributed Denial of Service
- Transition Mechanisms
- Worms/Viruses
  - There are already worms that use IPv6 (e.g. Rbot.DUD)

Scanning Gateways and Hosts (Reconnaissance)

IPv6 Deployment and Support

- **Subnet size is much larger**
  - A default /64 subnet has 2^{64} addresses, aka approximately $18x10^{18}$ addresses
  - It requires about 500.000 years to scan a typical (/64) subnet at a rate of 1million addresses per second!
  - *nmap* does support IPv6 network scanning
- **IPv6 scanning methods are likely to change**
  - DNS based, multicasting, common numbering, etc

Scanning Gateways and Hosts (Reconnaissance)

- **DNS based methods**
  - DNS has more significant role in IPv6 networks as IPv6 addresses are difficult to remember
  - Public servers will still need to be DNS reachable giving attackers some public hosts to attack, as it is done in IPv4
- **Scanning techniques**
  - Administrators may adopt easy to remember addresses
    - e.g. ::1,::2,::53, or simply the IPv4 last octet/address
  - Limit the possible combinations of EUI-64 Interface ID
    - Fixed part "*ff:fe*", Ethernet card vendors numbering
  - Parallelised scanning?

Scanning Gateways and Hosts (Reconnaissance)

IPv6 Deployment and Support

- **Privacy extensions make reconnaissance less effective**
  - IPv6 address change over time -> Limit the amount of time a given IPv6 address can be targeted
  - By enabling privacy extensions, it become difficult to track hosts for management purposes / accountability (side-effect)
- **Recommendations**
  - Protect public DNS servers
  - Avoid DNS zone transfers, crawlers, etc
  - Avoid easy to guess addresses

Scanning Multicast Addresses

- **IPv6 supports new multicast addresses**
  - Local multicast ensures that a compromised host can easily find all the other hosts in a subnet
  - Multicast enables an attacker to identify key resources on a network, e.g. all DHCP servers (*FF05::5*), all NTP servers, etc
    - All node (*FF02::1*), all router (*FF05::2*) multicast addresses are also supported in IPv4, e.g. *2240.0.{1,2}*
  - These addresses must be filtered at the border in order to make them unreachable from the outside
    - IPv6 specs forbids the generation of ICMPv6 packets in response to messages to global multicast addresses that contain requests

Auto-configuration / Neighbour Discovery

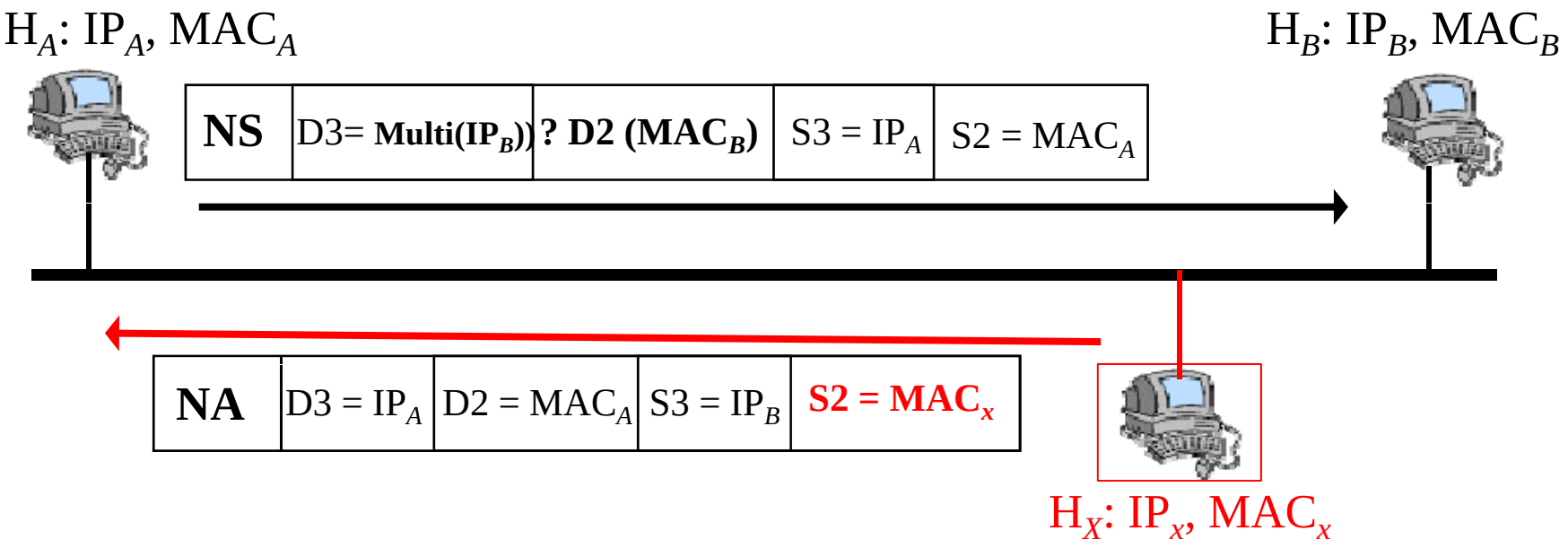
IPv6 Deployment and Support

- **Neighbour Discovery**
  - Suffers similar problems as ARP cache poisoning
- **SEcure Neighbor Discovery (SEND) [RFC3971]**
  - Applicable in environments where physical security is not assumed, e.g. wireless
  - Based on CGA
    - Linux implementation: DoCoMo's Open Source SEND Project
  - Certify routers with a trust anrchor, verify ownership of addresses, avoid replay attacks, etc
- **DHCPv6 with authentication is also possible**
- **ND with IPsec is also possible**

ND Attacks (1/3)

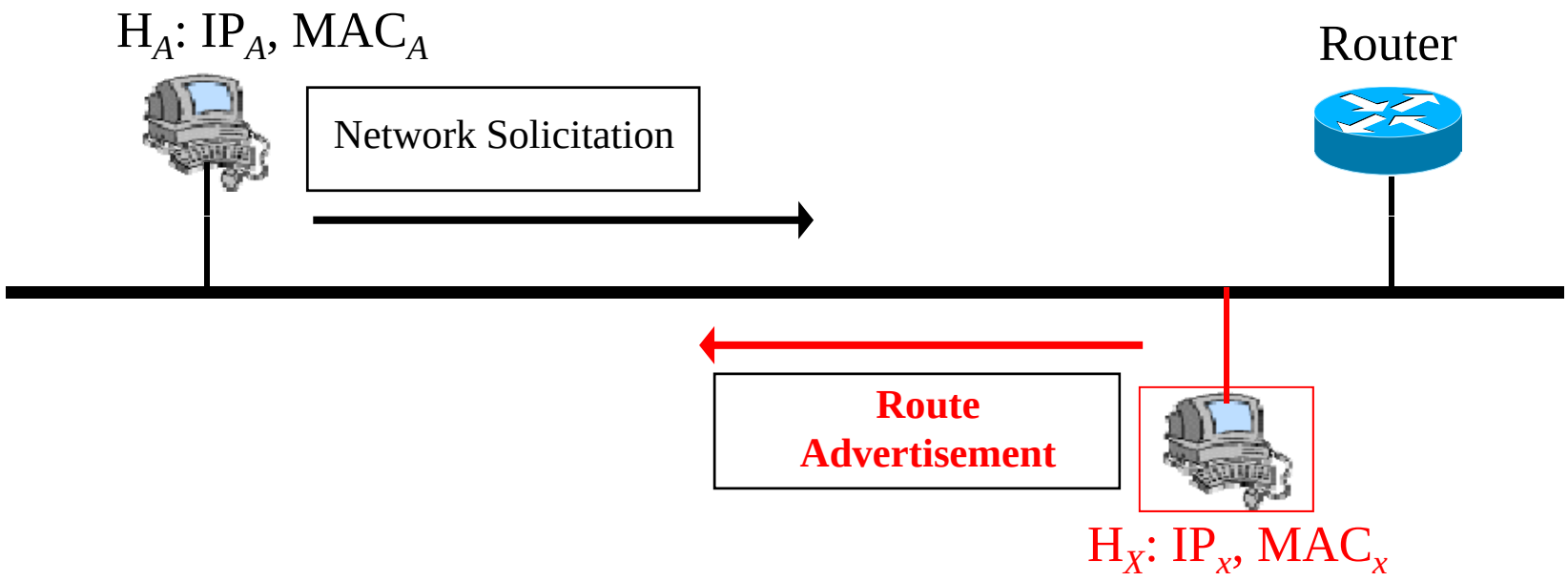
IPv6 Deployment and Support

- **Attacker sends fake NA messages**
  - Attack node claims to be any system in the LAN
  - Sink or divert traffic



ND Attacks (2/2)

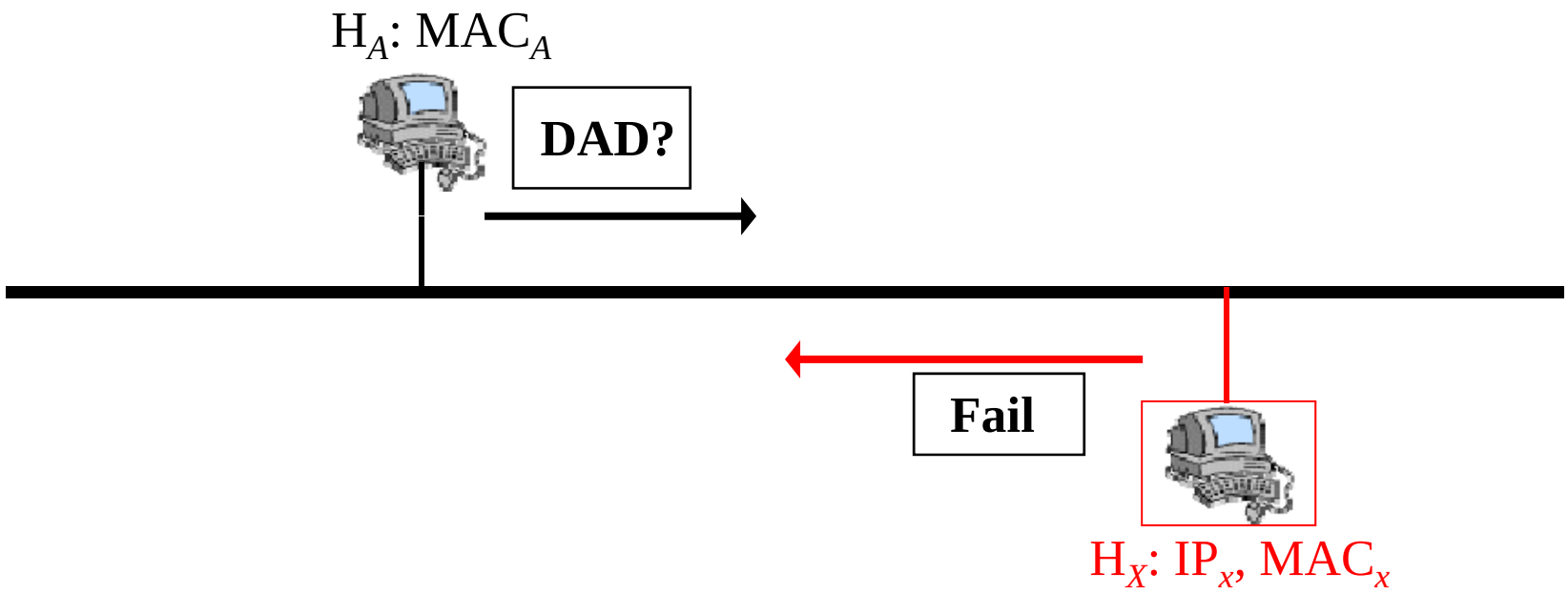
- **Attack node sends fake RA**
  - Attack node claims to be the router
  - Sink or divert traffic



ND Attacks (3/3)

IPv6 Deployment and Support

- **Attack node sends fake DAD replies**
  - Attack node claims to have any IPv6 address checked via DAD
  - Prevent new nodes to set an IPv6 address



Security of IPv6 addresses

IPv6 Deployment and Support

- **Privacy Extensions for Stateless Address auto-configuration [RFC 3041]**
  - Prevents device/user tracking
  - Makes accountability harder
- **Host-ID could be token to access networks**

Security of IPv6 addresses

IPv6 Deployment and Support

- **Cryptographically Generated Addresses (CGA) IPv6 addresses [RFC3972]**
  - Addresses for which the interface identifier is generated by computing a cryptographic one-way hash function from a public key and auxiliary parameters
  - Providing a binding of IP addresses to public keys without requiring a full key management infrastructure, e.g. certification authority
  - Used for SEcuring Neighbor Discovery (SEND)
  - Extended for other uses [RFC4581]
    - Secure Mobile IPv6 Binding information
    - IETF CSI Working Group

Cryptographically Generated Addresses (CGA)

- **Basic procedures**
  - Generate a CGA from the cryptographic hash of a public key and auxiliary parameters,
  - Verify the association between the public key and the CGA
  - Sign a message sent from the CGA, and verify the signature
- **CGA parameters**
  - Included in the ND messages
  - Data structure
    - **Modifier**, chosen arbitrarily (16 octets)
    - **Address prefix,** valid on the respective link (8 octets)
    - **Collision count** (1 octet)
    - **Public key** (Variable length)
    - **Optional extension fields** (Variable length)

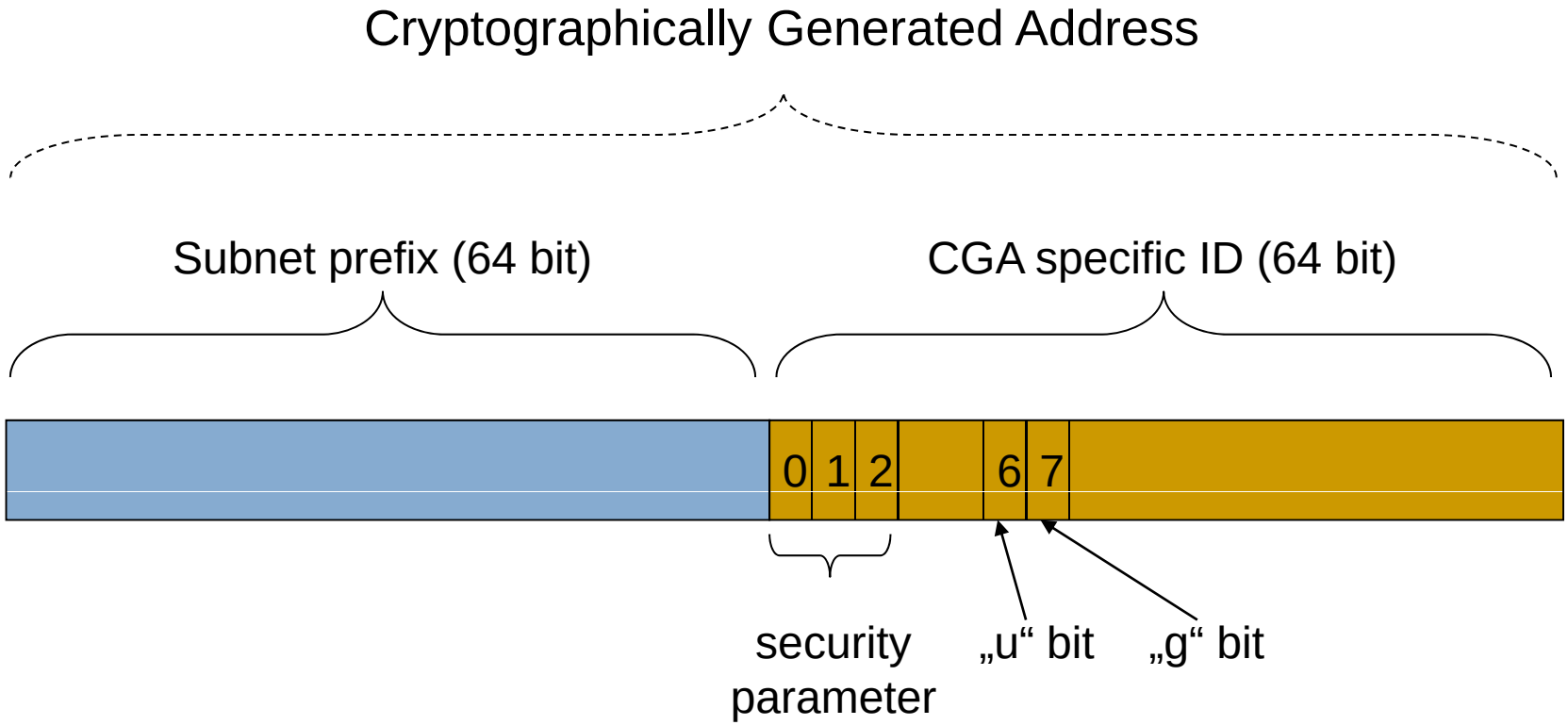
CGA: Generation of public / private key pair

IPv6 Deployment and Support

1. Choose an arbitrary value for the 16 octet modifier
2. Select an appropriate value for the security parameter (0: « low resistance » to brute-force to 7: « high resistance to brute-force »
3. Hash (SHA-1) concatenation of modifier, address prefix (set to zero), collision count (set to zero) and public key
4. If first 16 times security parameter bits are not zero, increase modifier by 1 and repeat hash computation (back to 4)
5. Hash (SHA-1) concatenation of final modifier, real address prefix, collision count (set to zero) and public key
6. The identifier are the first 64 bits of the result with overriding the first 3 bits by the security parameter and setting u and g bit
7. If duplicate address detection fails, increase collision counter and go back to 6

CGA - structure

IPv6 Deployment and Support



Unauthorised Access Control

- **Policy implementation in IPv6 with Layer 3 and Layer 4 is still done in firewalls**
- **Some design considerations!**
  - Filter site-scoped multicast addresses at site boundaries
  - Filter *IPv4-mapped* IPv6 addresses on the wire

Action	Src	Dst	Src port	Dst port
permit	a:b:c:d::e	x:y:z:w::v	any	ssh
deny	any	any		

Unauthorised Access Control

- **Non-routable + bogon (unallocated) address filtering slightly different**
  - in IPv4 easier deny non-routable + bogons
  - in IPv6 simpler to permit legitimate (almost)

Action	Src	Dst	Src port	Dst port
deny	2001:db8::/32	host/net		
permit	2001::/16	host/net	any	service
permit	2002::/16	host/net	any	service
permit	2003::/16	host/net	any	service
deny	3ffe::/16	host/net	any	service
deny	any	any		

Layer3 / Layer4 Spoofing

IPv6 Deployment and Support

- **Layer 3 spoofing is similar in IPv6**
  - Source address filtering is the basic mechanism to avoid spoofing
  - IPv6 address are globally aggregated making spoof mitigation at aggregation points easy to deploy
  - Host part of the IPv6 address can not be protected
    - IPv6 <– >MAC address (user) mapping is needed for accountability
  - Automatic tunnellig mechanims may be expoited
- **Layer 4 spoofing is identical in IPv6**

Amplification (DDoS) Attacks

- **There are no *broadcast addresses* in IPv6**
  - This would stop any type of amplification attacks that send ICMP packets to the broadcast address
  - Global multicast addresses for special groups of devices, e.g. link-local addresses, etc.
- **IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to global multicast addresses**
  - Many popular operating systems follow the specification
  - Still uncertain on the danger of ICMP packets with global multicast source addresses

Mitigation of IPv6 Amplification

- **Be sure that your host implementations follow the ICMPv6 specifications [RFC 4443]**
- **Implement ingress filtering**
  - Defeats Denial of Service Attacks which employ IP Source address spoofing [RFC 2827]
  - Prohibit attackers from using forged source addresses, which do not reside within a range of legitimately advertised prefixes.
- **Implement ingress filtering of IPv6 packets with IPv6 multicast source address**

Mixed IPv4/IPv6 environments

- **Some security issues with transition mechanisms**
  - Tunnels often interconnect networks over areas supporting the “wrong” version of protocol
  - Tunnel traffic often not anticipated by the security policies. It may pass through firewall systems due to their inability to check two protocols in the same time
- **Do not operate completely automated tunnels**
  - Avoid “translation” mechanisms between IPv4 and IPv6, use dual stack instead
  - Only authorised systems should be allowed as tunnel end-points

IPv6 transition mechanisms

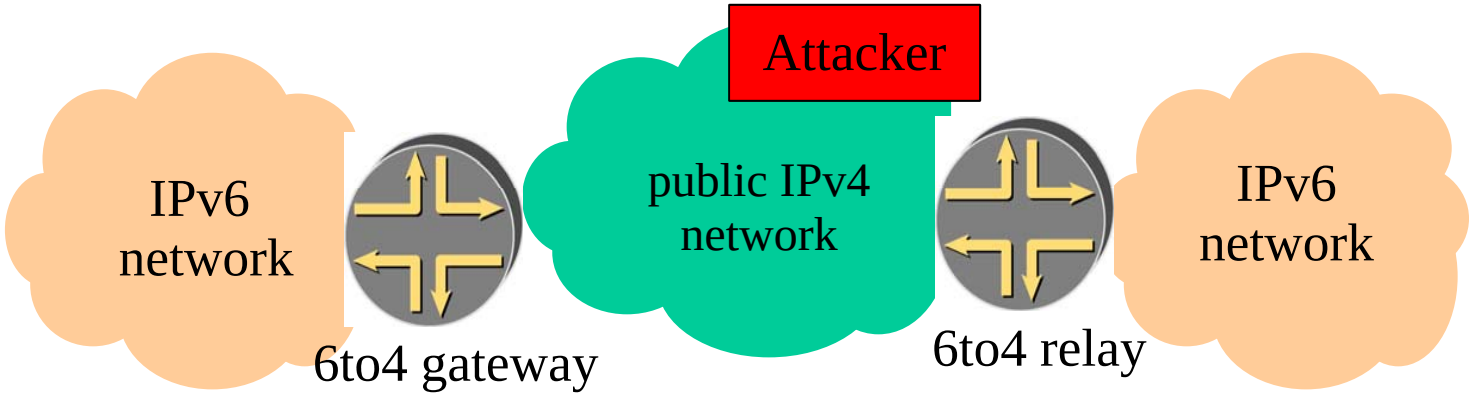
IPv6 Deployment and Support

- **~15 methods possible in combination**
- **Dual stack:**
  - Enable the same security for both protocols
- **Tunnels:**
  - *ip tunnels* : punching the firewall (protocol 41)
  - *gre tunnels* : probable more acceptable since used several times before IPv6

L3 – L4 Spoofing in IPv4 with 6to4

IPv6 Deployment and Support

- **Via 6to4 tunnelling, spoofed traffic can be injected from IPv4 into IPv6**
  - IPv4 Src: Spoofed IPv4 Address
  - IPv4 Dst: 6to4 Relay Anycast (192.88.99.1)
  - IPv6 Src: 2002:: Spoofed Source
  - IPv6 Dst: Valid Destination



Other threats (1/2)

- **IPv6 Routing Attack**
  - Use traditional authentication mechanisms for BGP and IS-IS.
  - Use IPsec to secure protocols such as OSPFv3 and RIPng
- **Viruses and Worms**
- **Sniffing**
  - Without IPsec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- **TCP ICMP attacks**
  - Slight differences with ICMPv6
  - http://tools.ietf.org/html/draft-gont-tcpm-icmp-attacks-05

Other threats (2/2)

- **Application Layer Attacks**
  - Even with IPsec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPsec will do nothing to prevent
- **Man-in-the-Middle Attacks (MITM)**
  - Without IPsec, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4
- **Flooding**
  - Flooding attacks are identical between IPv4 and IPv6

Vulnerability Testing & Assessment

IPv6 Deployment and Support

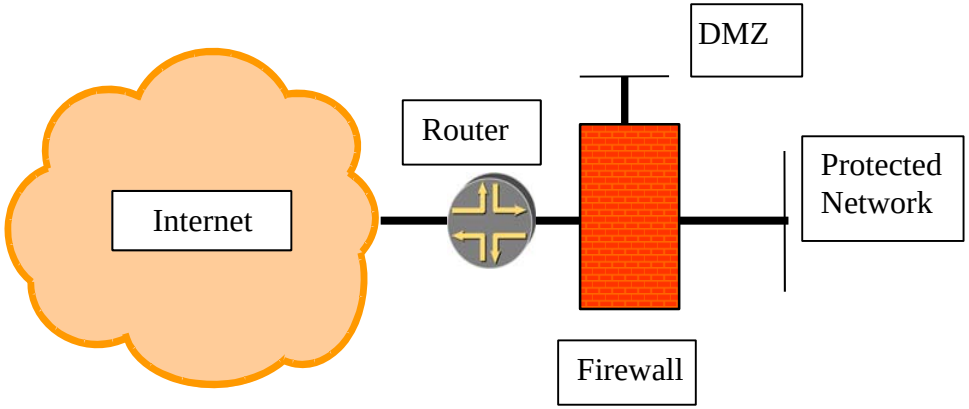
- **Testing tools**
  - *Ettercap, nmap, LSOF, Snoop, DIG, Etherape, Wireshark, Fping, Ntop, SendIP, TCPDump, WinDump, IP6Sic, NetCat6, Ngrep, THC Amap*, etc
- **Assessment tools**
  - *SAINT, nessus, ndpmon*, etc

IPv6 Architecture & Firewalls

IPv6 Deployment and Support

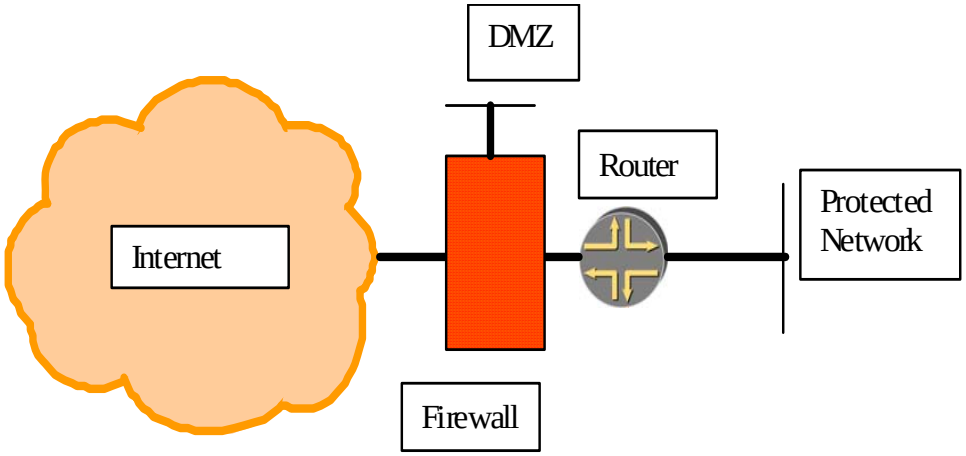
- **Requirements**
  - Same level of security with IPv6 possible as with IPv4 (security and privacy)
    - No need to enable NAT (for improving security of the IP infrastructure)
    - Even better security is possible in IPv6 infrastructure using (e2e) IPsec
  - Weaknesses of the packet filtering cannot be hidden by NAT
  - IPv6 does not require ***end-to-end connectivity***, but provides ***end-to-end addressability***
  - Not breaking IPv4 security
  - Support for IPv4/IPv6 transition and coexistence
  - Support for IPv6 header chaining
- **There are some IPv6-capable firewalls**
  - Cisco ACL/PIX, *iptables*, *ipfw*, Juniper NetScreen, etc

IPv6 Firewall Setup (method 1)



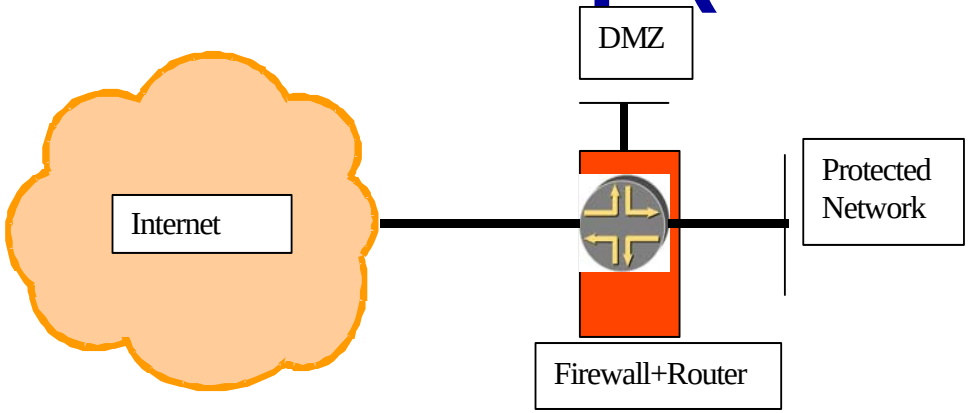
- **“Internet ↔ router↔ firewall ↔ net” architecture**
- **Requirements:**
  - Firewall must support/recognise ND/NA filtering
  - Firewall must support RS/RA if SLAAC is used
  - Firewall must support MLD messages if multicast is required

IPv6 Firewall Setup (method 2)



- **“Internet ↔ firewall ↔ router ↔ net” architecture**
- **Requirements**
  - Firewall must support ND/NA
  - Firewall should support filtering dynamic routing protocol
  - Firewall should have large variety of interface types

IPv6 Firewall Setup (method 3)



- **“Internet ↔ firewall/router(edge device) ↔ net” architecture**
- **Requirements**
  - Can be powerful - one point for routing and security policy – very common in SOHO (DSL/cable) routers
  - Must support what usually router & firewall do

Firewall setup (1/2)

IPv6 Deployment and Support

- No blind ICMPv6 filtering possible

	Echo request/reply	**Debug**
	No route to destination	**Debug – better error indication**
	TTL exceeded	**Error report**
	Parameter problem	**Error report**
IPv6 specific	**NS/NA**	**Required for normal operation – except static ND entry**
required	**RS/RA**	**For Stateless Address Autoconfigration**
	Packet too big	**Path MTU discovery**
	MLD	**Requirements in for multicast in architecture 1**

Firewall setup (2/2)

- No blind IP options (→ extension Header) filtering possible:

Hop-by-hop header	What to do with jumbograms or router alert option? – probably log and discard – what about multicast join messages?
Routing header	Source routing – in IPv4 it is considered harmful, but required for IPv6 mobility – log and discard if you don't support MIPv6, otherwise enable only Type 2 routing header for Home Agent of MIPv6
ESP header	Process according to the security policy
AH header	Process according to the security policy
Fragment header	All but last fragments should be bigger than 1280 octets

Overview of IPv6 Firewalls

IPv6 Deployment and Support

	IPFilter 4.1	PF 3.6	IP6fw	Iptables	Cisco ACL	Cisco PIX 7.0	Juniper firewall	Juniper NetScreen	Windows XP SP2
Portability	Excellent	Good	Average	Weak	Weak	Weak	Weak	Weak	Weak
ICMPv6 support	Good	Good	Good	Good	Good	Good	Good	Good	Good
Neighbor Dissovery	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Good	Excellent	Weak
RS /RA support	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Excellent	Excellent	Good
Extension header support	Good	Good	Good	Excellent	Good	Good	Good	Good	Weak
Fragmantation support	Weak	Complete block	Weak	Good	Weak	Average	Weak	Average	Weak
Stateful firewall	Yes	Yes	No	Csak USAGI	Reflexive firewall	Yes	ASP necessary	Yes	No
FTP proxy	No	Next version	No	No	since 12.3 (11)T	?	No	No	No
Other	QOS support	QoS support, checking packet vailidity	Predefined rules in *BSD	EUI64 check,	Time based ACL		No TCP flag support today, HW based	IPSec VPN, routing support	Graphical and central configuration

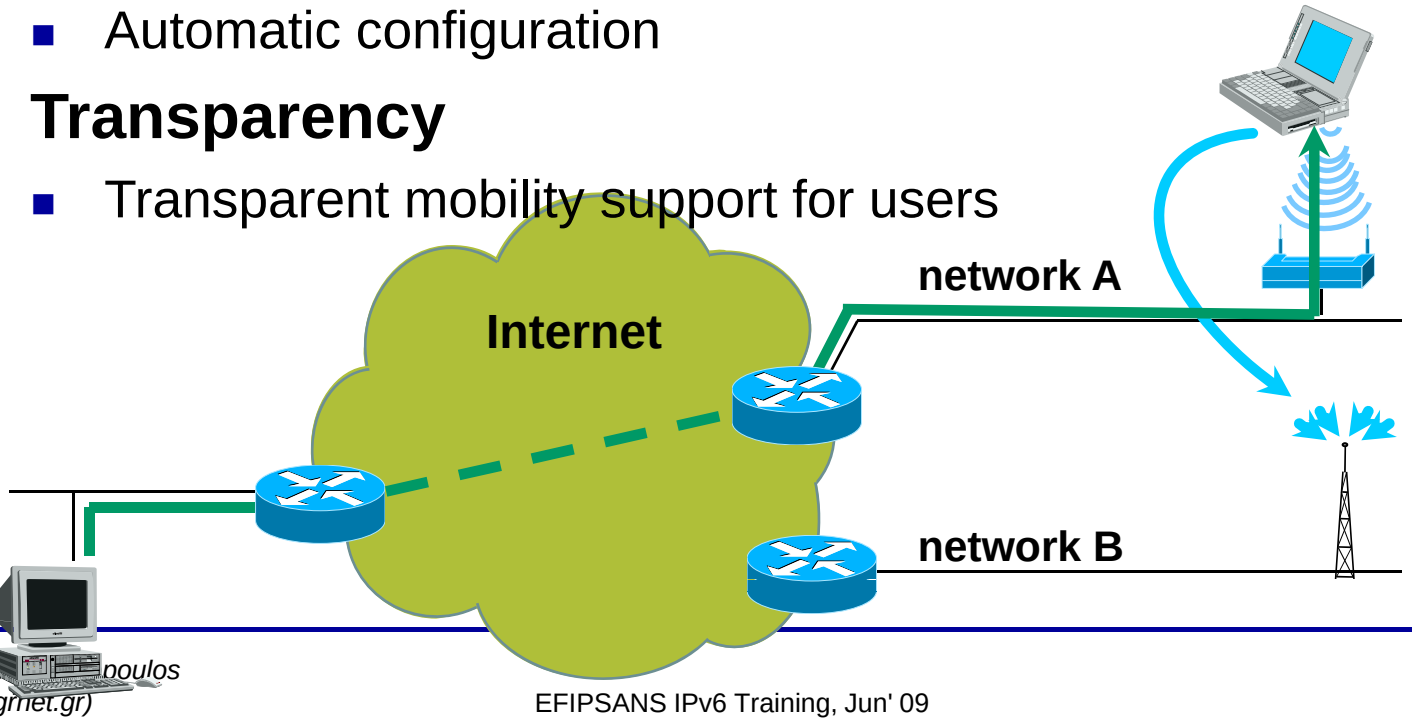
Firewall L4 issues

IPv6 Deployment and Support

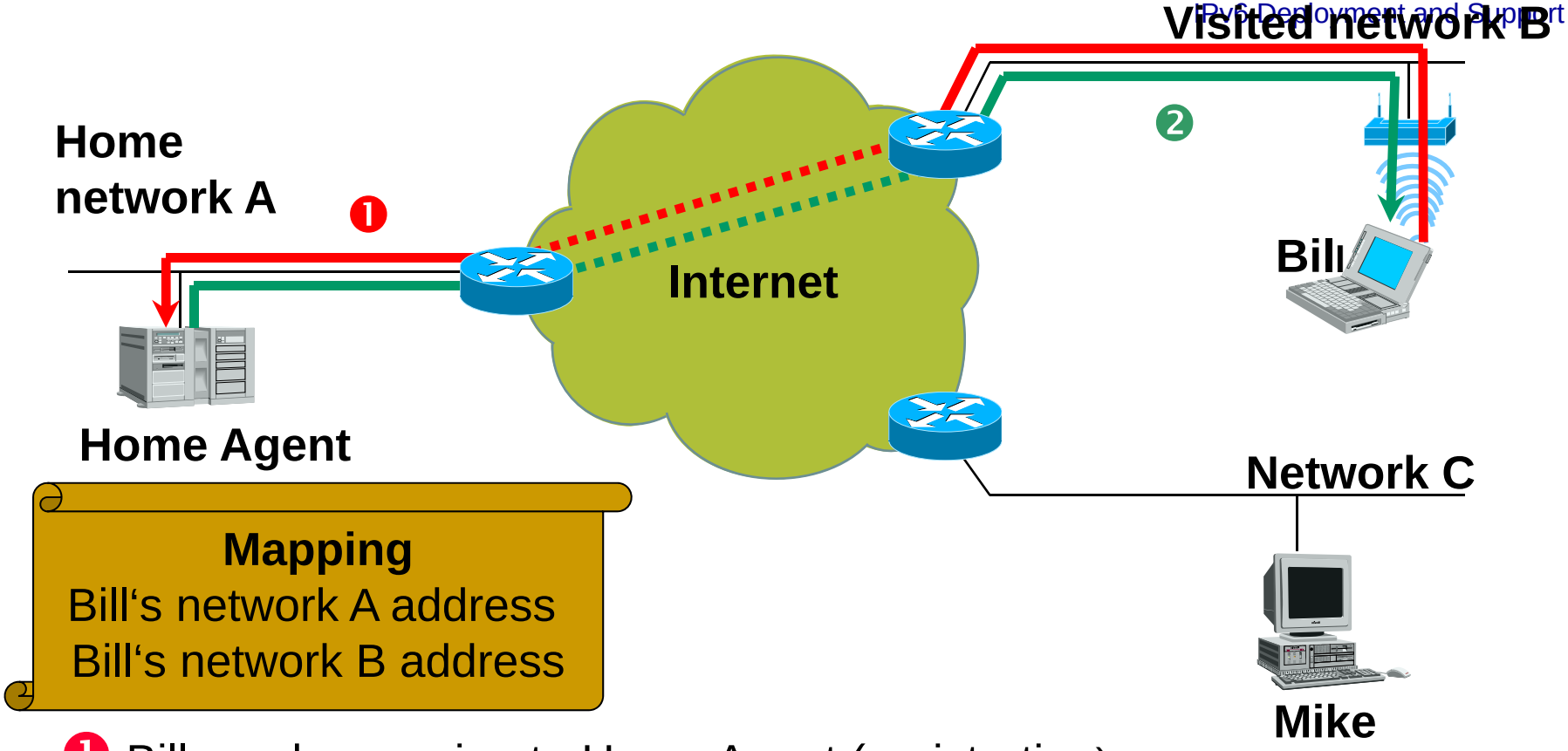
- FTP
  - Complex: PORT, LPRT, EPRT, PSV, EPSV, LPSV (RFC 1639, RFC 2428)
  - Virtually no support in IPv6 firewalls
- HTTP seems to be the next generation file transfer protocol with WEBDAV and DELTA
- Other non trivially proxy-able protocol:
  - No support (e.g.: H.323)

Mobile IP (MIP)

- **Mobility**
  - Growing number of mobile Internet users
  - Mobility support in the Internet required
- **Addressing**
  - Reachability of user under one fixed IP address
  - Automatic configuration
- **Transparency**
  - Transparent mobility support for users

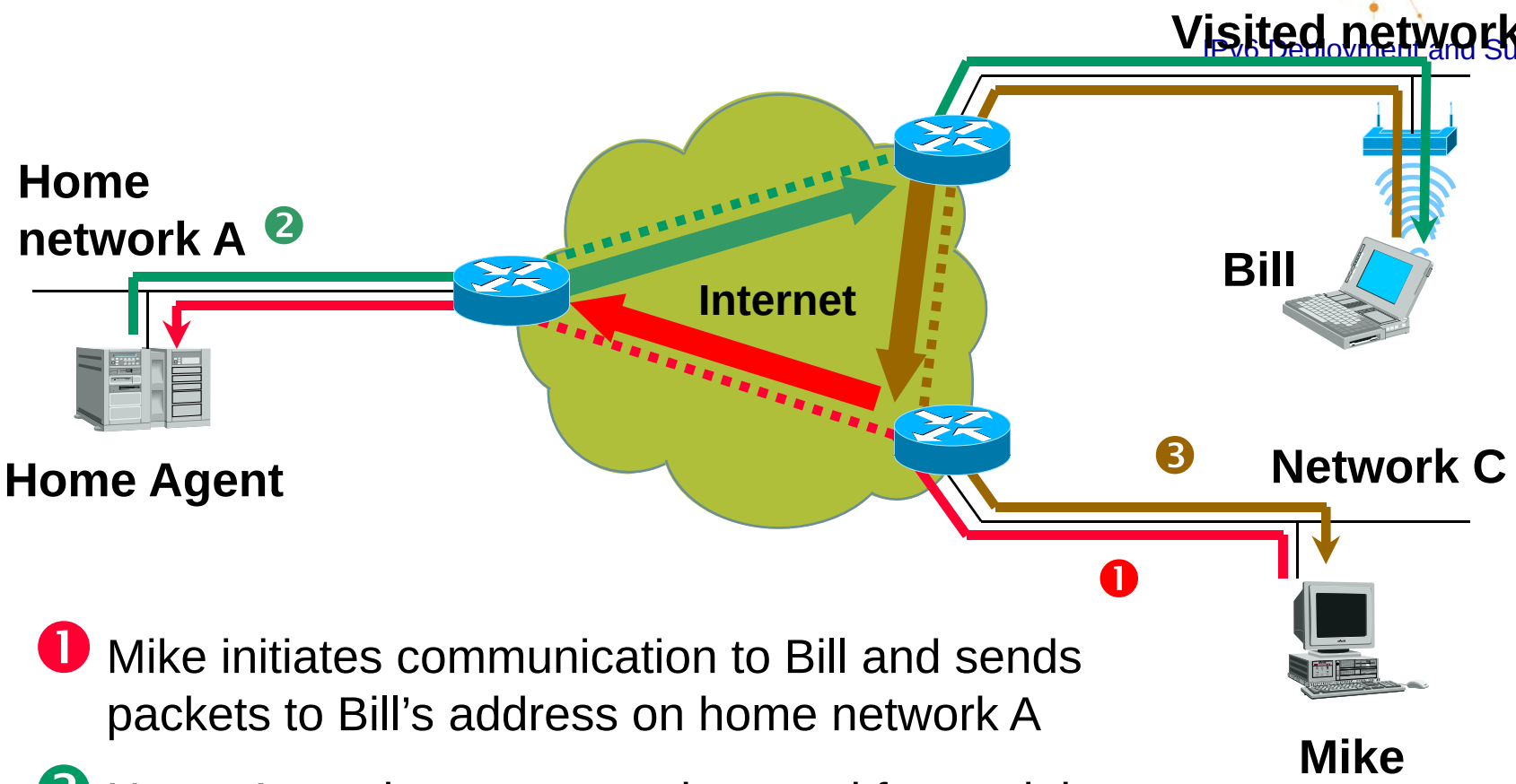


MIPv6 – Home Registration



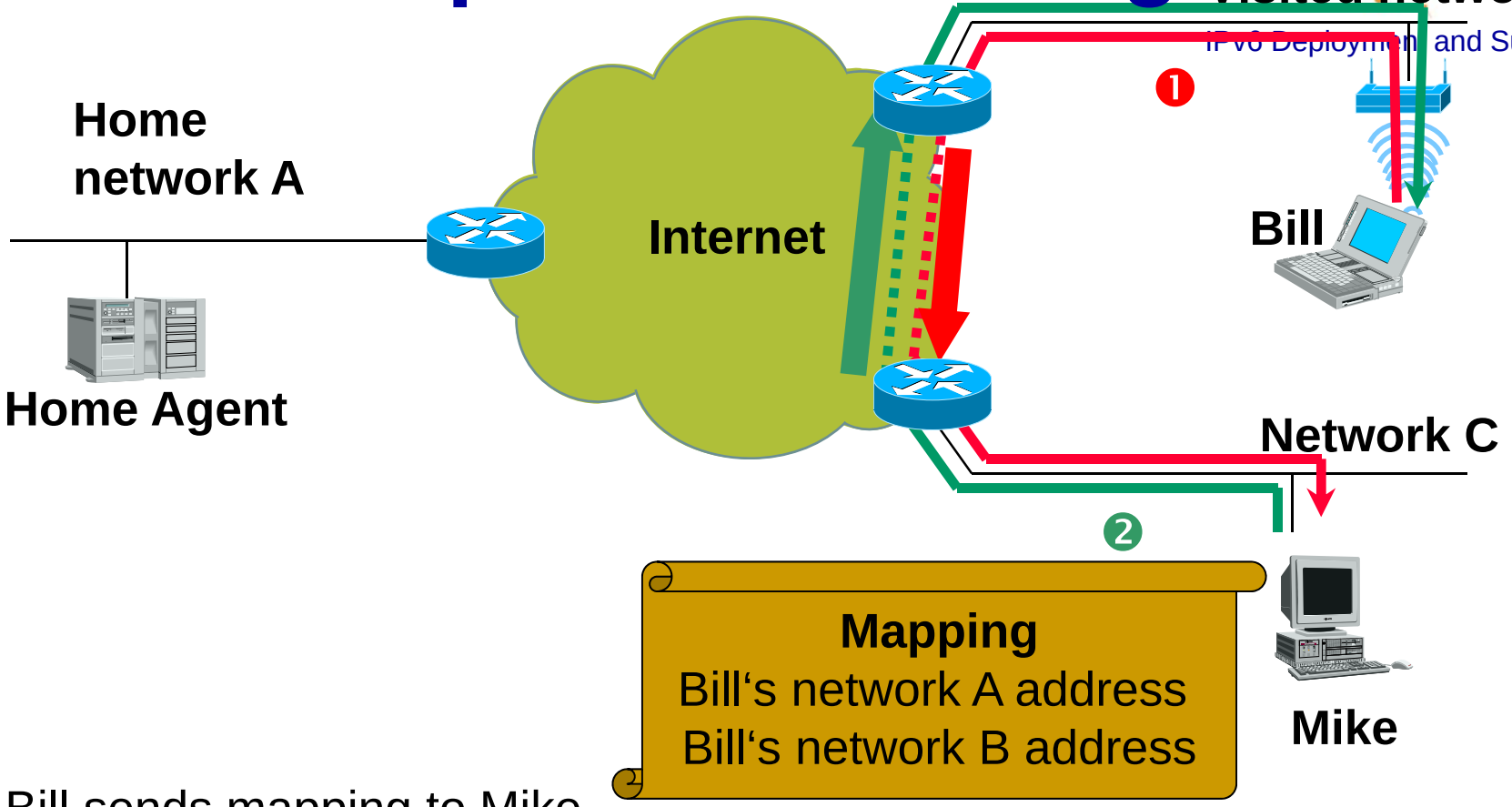
1. Bill sends mapping to Home Agent (registration)
2. Home Agent confirms receipt of mapping and start to receive packets for Bill (proxy)

MIPv6 – Triangle Routing



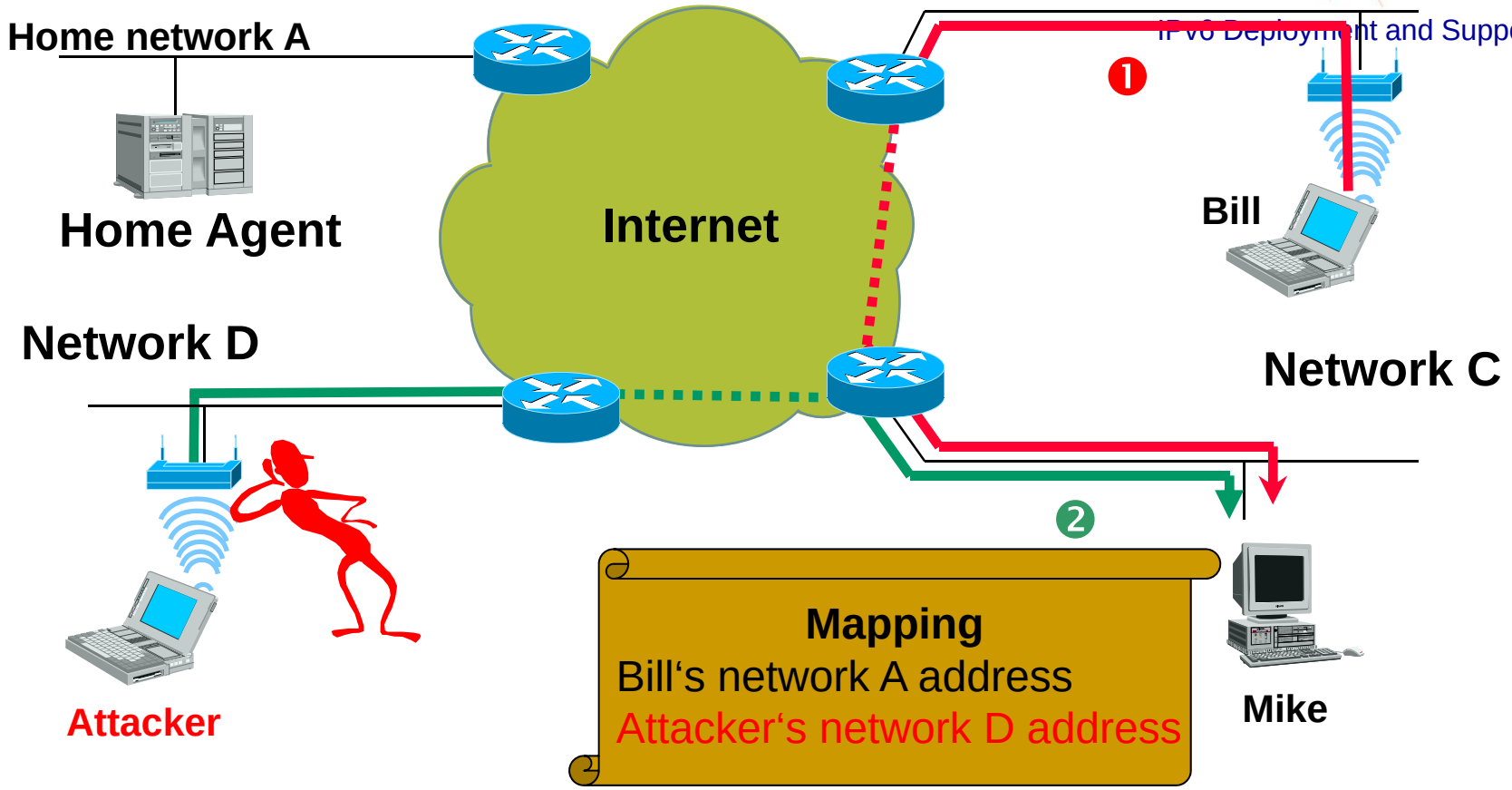
1. Mike initiates communication to Bill and sends packets to Bill's address on home network A
2. Home Agent intercepts packets and forward them to Bill's address on visited network B
3. Bill replies directly to Mike

MIPv6 – Optimise Routing



1. Bill sends mapping to Mike
2. Mike sends following packets directly to Bill’s address on visited network B

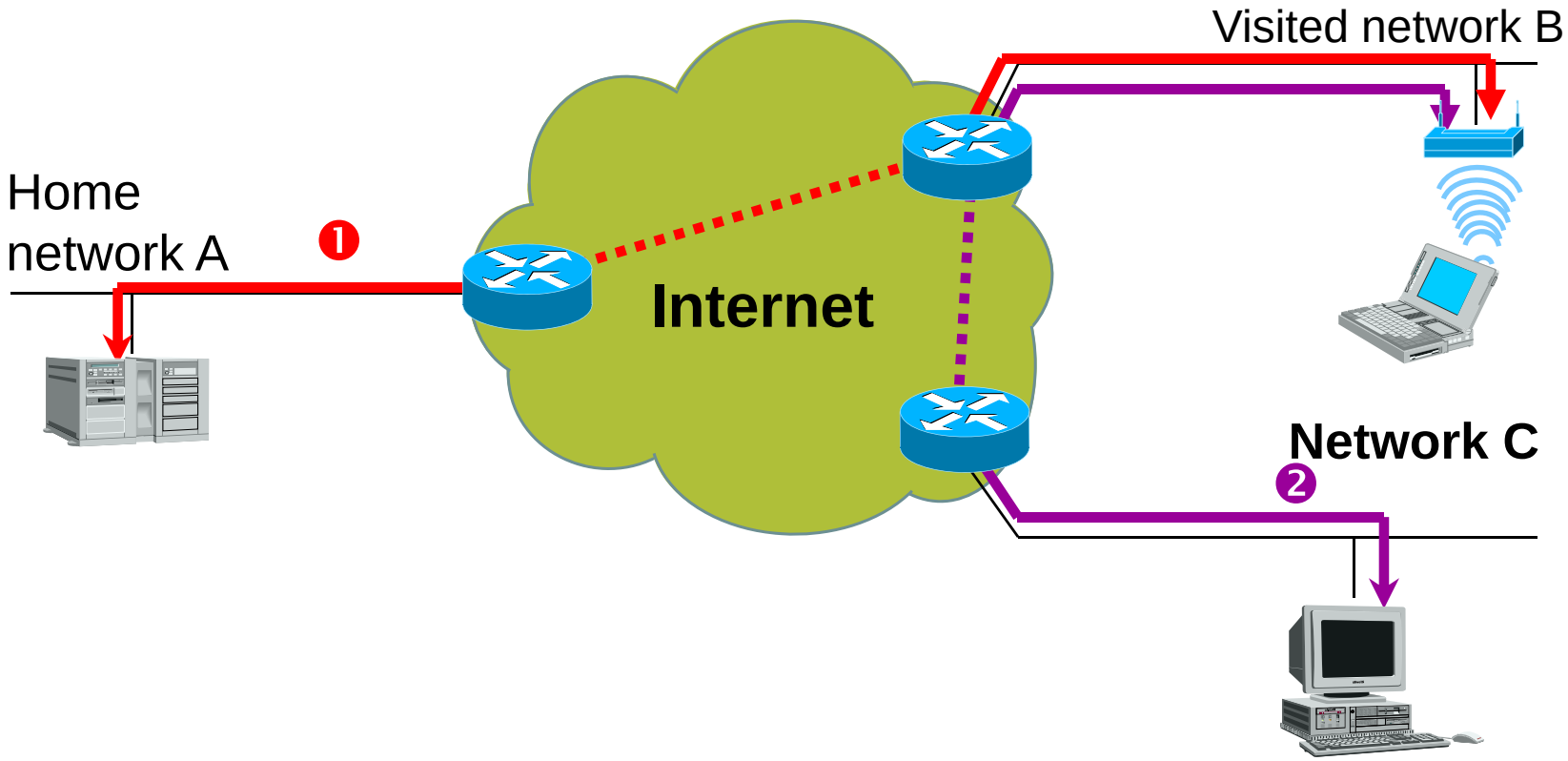
MIPv6 – Attack Scenario



❶ Bill sends mapping to Mike

❷ Attacker re-directs traffic sent from Mike to Bill towards himself

MIPv6 – Trust Relationship

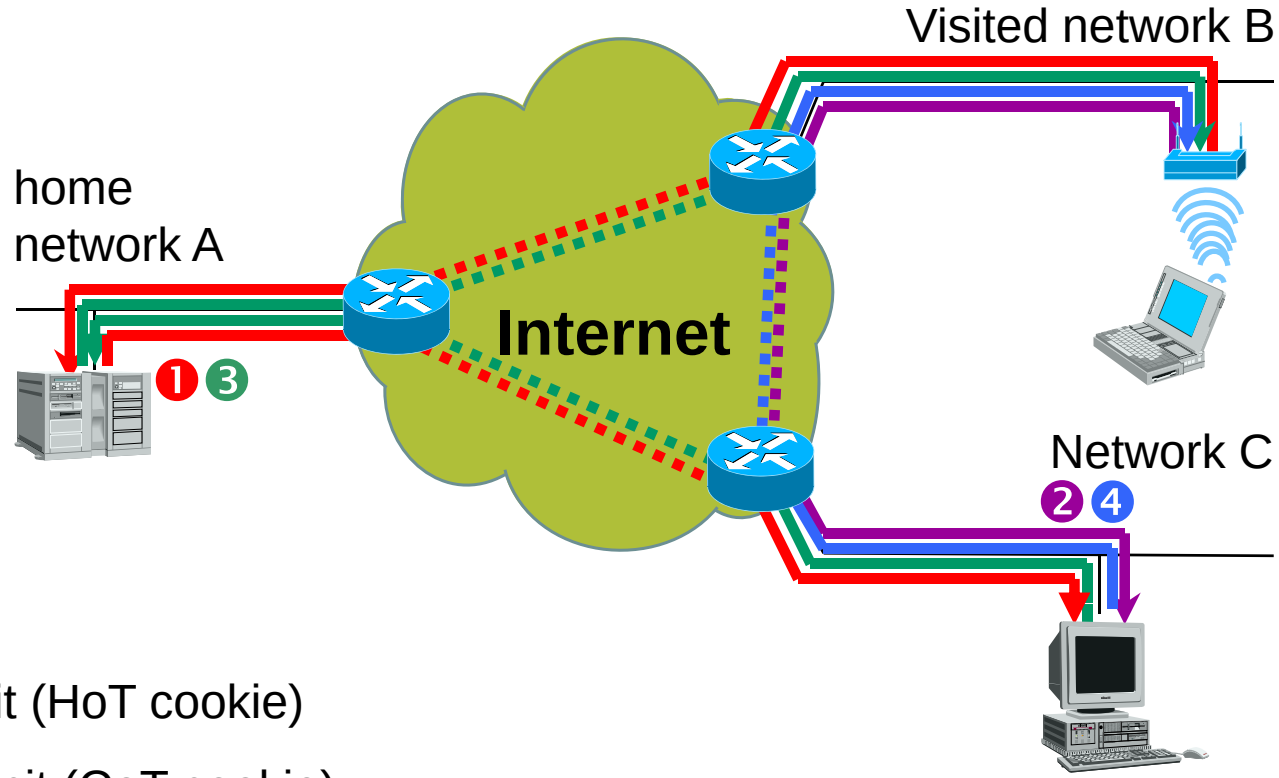


❶ Trust relationship between MN and HA --> IPSec can be used

❷ No trust relationship between MN and CN --> ???

MIPv6 - Return Routability

IPv6 Deployment and Support



1. Home Test Init (HoT cookie)
2. Care-of Test Init (CoT cookie)
3. Home Test (HoT cookie, home keygen token, home nonce index)
4. Care-of Test (CoT cookie, care-of keygen token, care-of nonce index)

Mobile IPv6: Remaining security issues

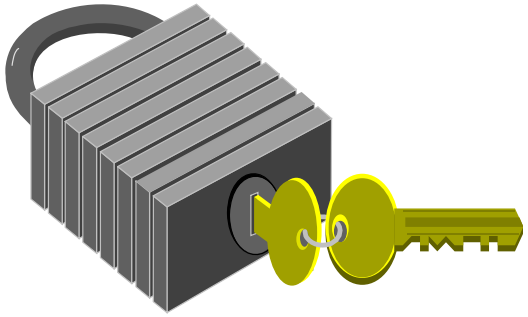
- Attacker on the path between HA and CN plus between MN and CN will be able to receive all Return Routability packets
- This attacker could still send Binding information on behalf of the MN
- Cryptographically Generate Addresses can help
- This still requires Return Routability itself to proof reachability of MN's addresses

Security: VPNs

IPv6 Deployment and Support

- Layer 2 solutions
  - MPLS
- IPSecurity
  - IPsec - Suite of protocols
- Other solutions
  - OpenVPN, Tinc, yavipin, etc

Security: IPSec



- **General IP Security mechanisms**
  - From the IETF IPsec Working Group
    - http://tools.ietf.org/wg/ipsec/
    - IP Security Architecture: RFC 4301
    - IPsec-related Technologies: IKE, SKIP, ISAKMP, etc
- **Applies to both IPv4 and IPv6:**
  - Mandatory support -not use- for IPv6,
  - Optional support for IPv4
- **Applicable to use over LANs, across public & private WANs, & for the Internet**

IPsec Protocol Overview

IPv6 Deployment and Support

- **IPsec is a security framework**
  - Provides suit of security protocols
  - Secures a pair of communicating entities
- **Security Associations**
  - To agree on the security algorithms and parameters between the sender and the receiver
  - SA Transport: Use IPsec end-to-end, securing the packet payload
    - Promoted by IPv6
  - SA Tunnel**:** Use IPsec between gateways or a host and a gateway

Security Association

IPv6 Deployment and Support

- **IPsec Services**
  - Authentication
    - AH (Authentication Header - RFC 4302)
  - Confidentiality
    - ESP (Encapsulating Security Payload - RFC 4303)
  - Replay protection, Integrity
  - Key management
    - IKEv2 (Internet Key Exchange - RFC4306)
- **Implementations**
  - Linux-kernel (USAGI), Cisco IOS-12.4(4)T, BSD&OSX(Kame)

Summary

IPv6 Deployment and Support

- **Security improvements with IPv6**
  - IPv6 has potential to be a foundation of a more secure Internet
- **Elements of the IPv6 security infrastructure are mature enough to be deployed in production environment.**
- **Other elements are in prototype state**
  - e.g. CGA, SEND … but even these are ready for experimental deployment


deploy
Questions?