IPv6 Security

Copy …Rights

- *This slide set is the ownership of the 6DISS 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 6DISS 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

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

Table of Contents

- Introduction to Security Problems
- The Security Threats
- Mobile Computing and Access Control
- Cryptographically Generated Addresses
- Protocol for Authentication and Network Access
- Securing the Infrastructure with IPSEC
- Specific IPv6-related threats and their solution

Introduction

- Security – isn’t it all solved?
- Conventional threats
- Wireless systems now
- A vision of the future
- Protection now
- Protection in the future

So what’s the big problem?

- We have firewalls and Intrusion Detection Systems – so we’re safe from outside attack
- VPNs, RADIUS, SSH, etc. allow secure remote access
- PKI can be used to determine identity
- S/MIME or PGP protects mail
- SSL/TLS protects web access
- Virus scanning is effective
- Security patches can be applied centrally – SMS
- 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?

- Lots of money + intellectual property (=money)
- Hostile environment (motivations for attack vary)
- Lack of security consciousness
- Lots of potential points of attack
- Policies are often seen as unacceptable
- No regulatory framework
- Legal aspects unclear

A warning….

- 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
- Over-concentration on technology is deeply naïve
- However if you do major changes, like IPv4-IPv6, you must ensure you have introduced new holes

Network Threats

- Passive tap
- Active tap
- Denial of service
- Faking/replay
- Traffic analysis

Other Threats

- Physical attack
- Trojan Horses, viruses, worms, logic bombs
- Passwords
- Loopholes
- Collusion
- Accidental access
- Tempest
- Social Engineering

Cost effective protection

- Absolute security?
    - GIVE UP ON THE IDEA OF CERTAINTY
        - – IT'S FICTIONAL
- Security = delay = cost to an attacker.
- But security costs implementer too.
- So compromise on level of security
    - Evaluate risks
    - Evaluate cost of losses
    - Don't spend more than this
    - Hard --
        - don't know motivation of attacker
        - don't know value of information or goodwill

Wireless systems

- Oh and then it all gets decidedly worse. And the culprits?

© 2003 CNET Networks, Inc.

- Toys!
- aka ‘empowering the workforce’

New problems

- Infrastructure doesn’t protect data
- Applications can’t be trusted to secure data
- New forms of virus?
- Security in mobile devices not standardised (many OS)
- 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?

- Play Luddite?   - Too late
- 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 (802.11)
  - High mobility low b/w devices (cell phones to RFID tags)
  - IPv4/IPv6 heterogeneous protocol suites
- The UIs will not be getting significantly better (au contraire)
- 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?

- Security was considered from the beginning in IPv6
  - One can rely on certain features existing
- When new services were considered, their security was part of IPv6 thinking
- Some of the areas where the thinking is obvious are:
  - Threats to Mobile access and Mobile IP
  - Cryptographically generated addresses
  - Protocol for Authentication and Network Access
  - IPsec
  - Making intrusion harder

Security Issues

- •Same as ever – robustness
  - – Authentication, Confidentiality, Integrity
  - – Non-repudiation
  - – Access control (authorisation)
  - – Accounting/billing
- •But
  - – Focus is on ‘certainty’ – and it’s not clear we can have that
  - – Resource poverty – processing power/bandwidth
  - – Actuators can kill people
  - – Lawful interception

Security issues

- Encryption, signatures etc. affected by resources
- VPNs and PKI work OK in principle (to the same extent as wired systems)
- So does application level security
- Malicious code – no ubiquitous approach

Traditional approach to securing systems

- If we want to secure a system, then we need to follow a number of principles:
  - Prevention is *never* 100% effective – so:
    - Need defence in depth – several different mechanisms
    - Mechanisms for detecting and responding to attacks, preferably in real time, are essential:
    - Start by securing the weakest link
    - Compartmentalise – don’t put all of your data in one basket
    - Mediocre security now is better than great security never
    - Take your users with you

Mechanisms for detecting and responding to attacks

- Detect – get to know you’re being attacked.
- Localise – determine what’s being attacked.
- Identify – determine who the attacker is.
- Assess – why are they doing this?
- Respond or Prevent – depends on all of above.
- Recover – Have a plan better than ‘go find a new job’
- Keep Audit Trail – so that you can assess the damage

What changes in this?

- Ambient computing = invisible computing
  - But heterogeneity in infrastructure, network protocols, etc.
- Issues of scale mean that human intervention is largely impracticable. One needs:
  - Autonomic mechanisms, new models of trust
  - To abandon the simple certainties of conventional security
  - Mechanisms to make intrusion more difficult to do and easier to detect
  - New techniques to deal with mobility

Threats due to Mobility

- Mobility in the system means changing physical connectivity and logical context. It needs:
  - Different types of policies; ones that can capture context.
  - Those policies implemented in a context dependent way
  - A flexible architecture to allow for composition of appropriate components
  - Some assurance about how this will perform
- There are big privacy issues

Conclusions

- Security at present just about works
  - But it is a bolt on – it has been a painful process to get here

Vision of future

- systems of huge scale,
- with huge heterogeneity,
- and a bigger impact on our lives than ever before

- Need R&D urgently to
  - think what security means in these environments
  - build security in to these systems from day 1
- Need public debate about impacts on society

Threats to be Countered in IPV6

- Scanning gateways and Hosts for weakness
- Scanning for multicast addresses
- Exposing weaknesses with NATs
- Unauthorised access
- Weaknesses in Firewalls
- Performance attacks with fragmented headers
- Protocol Weaknesses
- Distributed Denial of Service

Threats

Scanning and addresses

Scanning in IPv6

- Subnet Size is much larger
  - Default subnets in IPv6 have 2^64 addresses (approx. 18x10^18). Exhaustive scan on every address on a subnet is no longer reasonable (if 1 000 000 address per second then > 500 000 year to scan)
  - NMAP doesn't even support for IPv6 network scanning

Scanning in IPv6 /2

- IPv6 Scanning methods are likely to change
  - Public servers will still need to be DNS reachable giving attacker some hosts to attack – this is not new!
  - Administrators may adopt easy to remember addresses (::1,::2,::53, or simply IPv4 last octet)
  - EUI-64 address has “fixed part”
  - Ethernet card vendors guess
  - New techniques to harvest addresses – e.g. from DNS zones, logs
    - Deny DNS zone transfer
  - By compromising routers at key transit points in a network, an attacker can learn new addresses to scan
- Other possible network hiding: DNS splitting

Scanning in IPv6 / 3

- New attack vectors “All node/router …. addresses”
- New Multicast Addresses - IPv6 supports new multicast addresses that can enable an attacker to identify key resources on a network and attack them
- For example, all nodes (FF02::1), all routers (FF05::2) and all DHCP servers (FF05::5)
- These addresses must be filtered at the border in order to make them unreachable from the outside – this is the default if no IPv6 multicasting enabled.

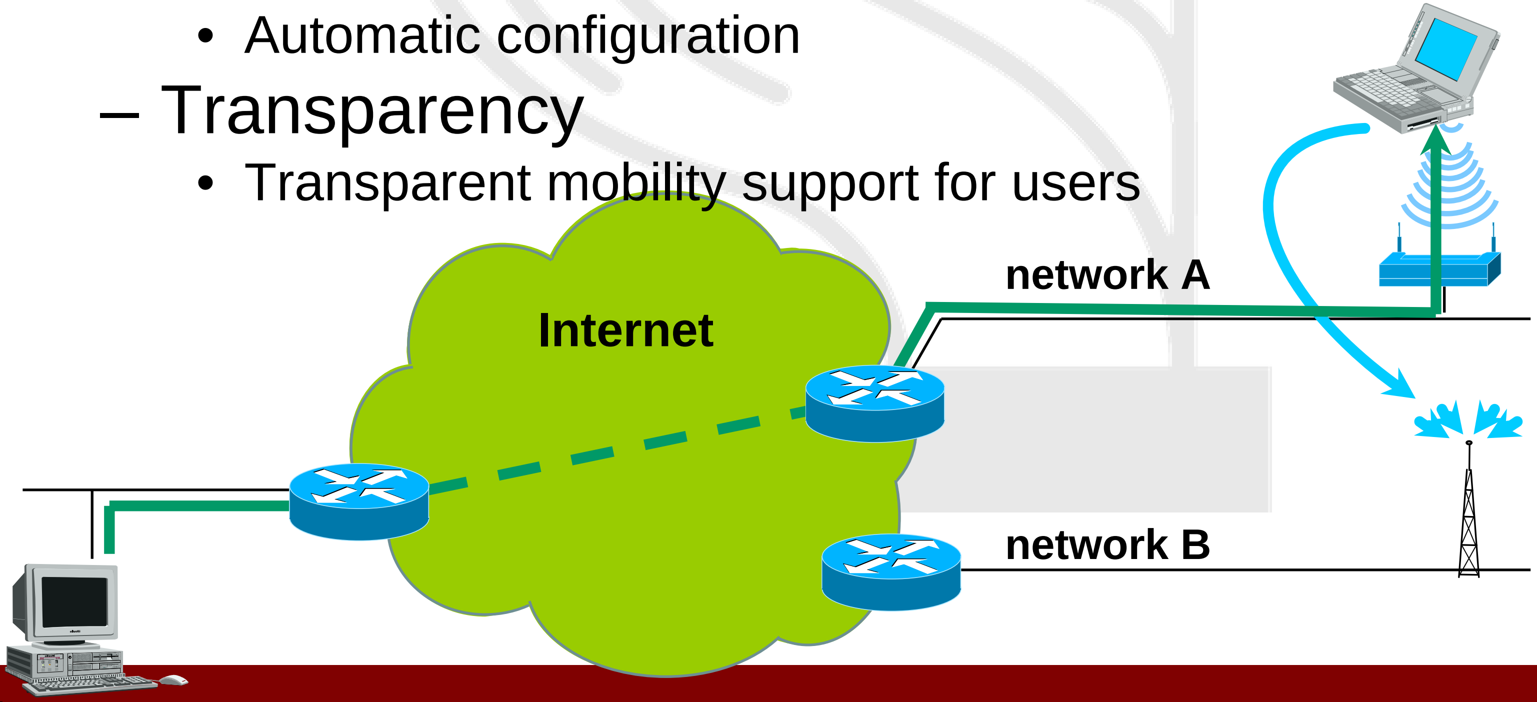
Security of IPv6 addresses

- Private addresses as defined RFC 3041
  - – prevents device/user tracking from
  - – makes accountability harder
- New privacy extended IPv6 addresses generated CGA (crytographically generated addresses)
  - – maintains privacy
  - – accountability possible by link administrators
- New feature: Host ID could be a token to access to a network. – additional security possible

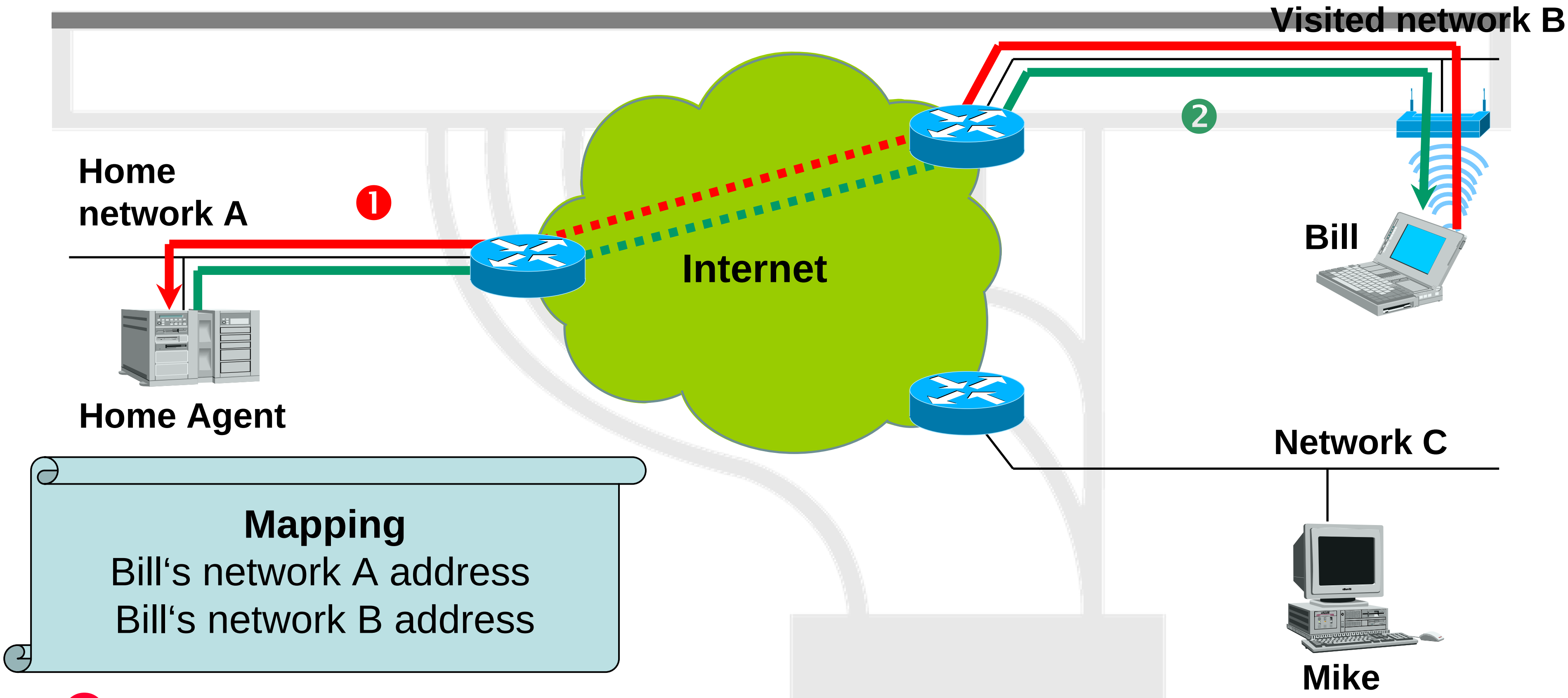
Mobile IP Security

Mobile IP (MIP)- Intention

- 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

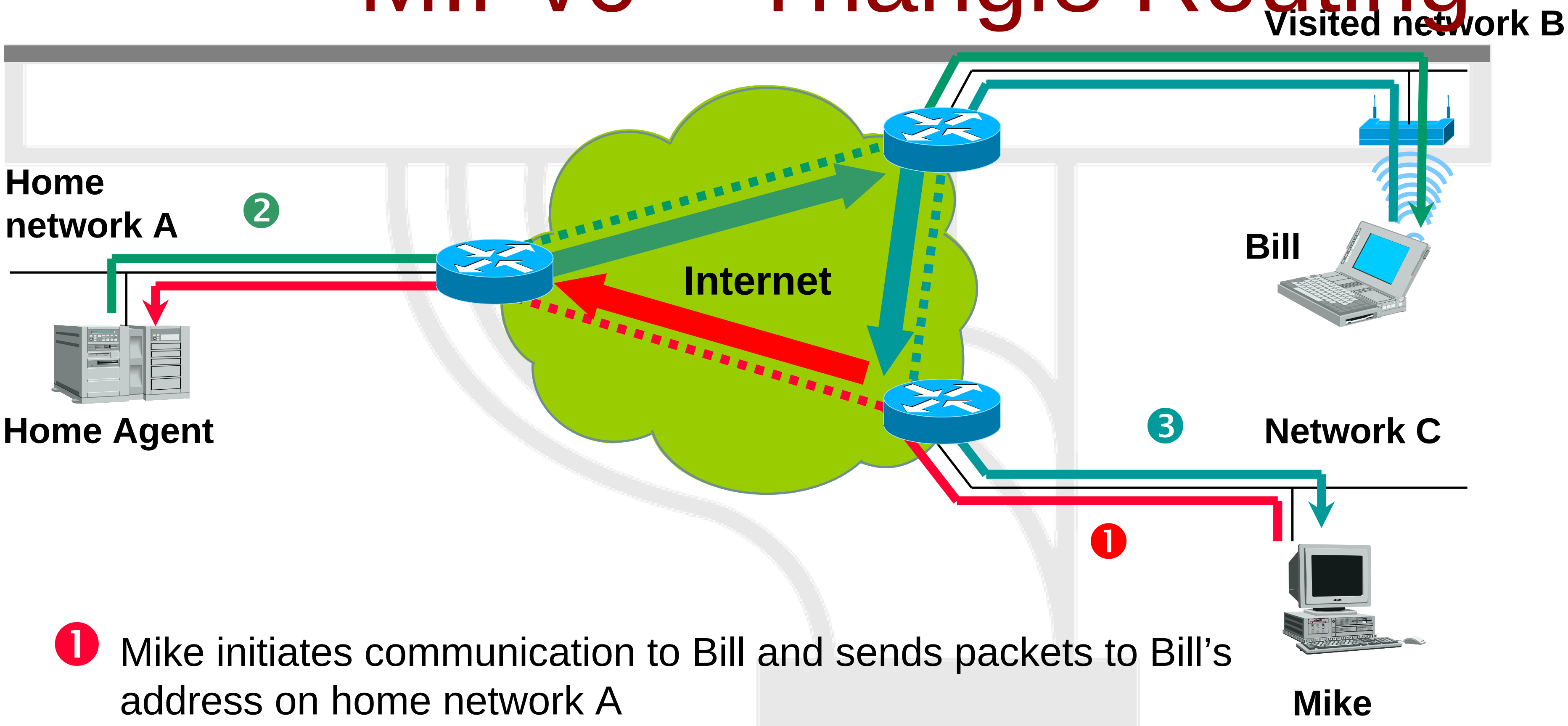


Mapping
Bill‘s network A address
Bill‘s network B address

❶ Bill sends mapping to Home Agent (registration)

❷ Home Agent confirms receipt of mapping and start to receive packets for Bill (proxy)

MIPv6 – Triangle Routing

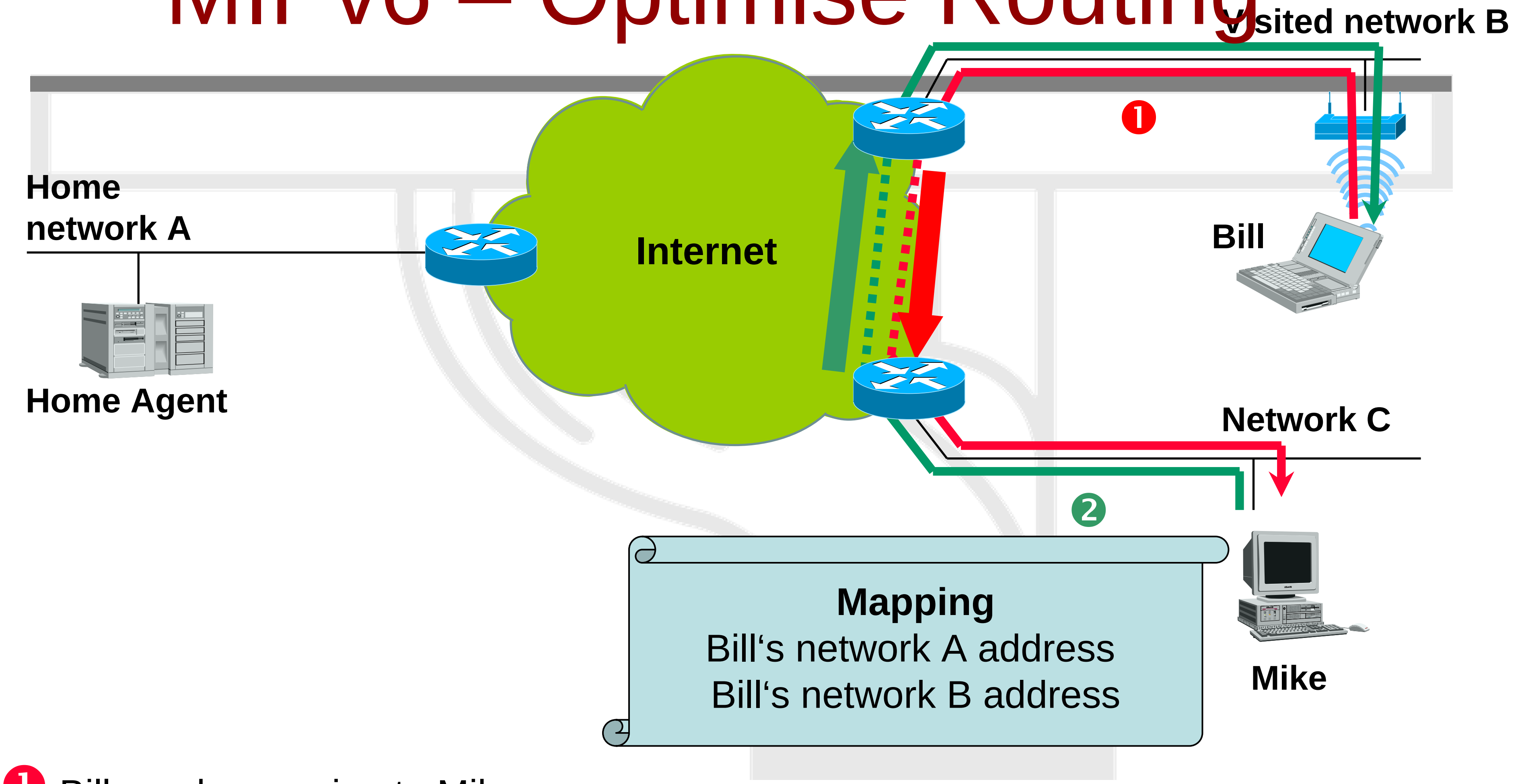


1 Mike initiates communication to Bill and sends packets to Bill's address on home network A

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

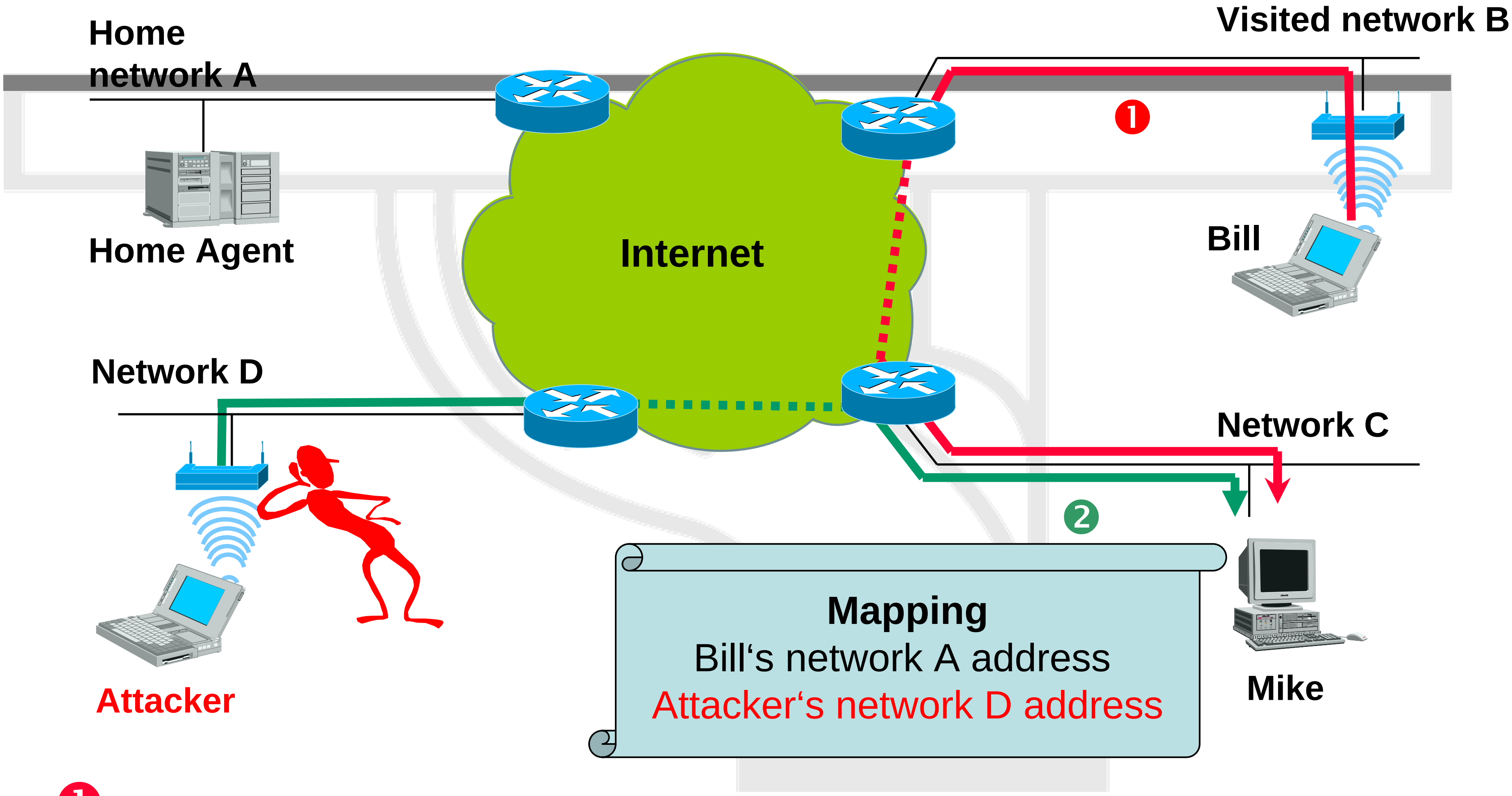


Mapping
Bill‘s network A address
Bill‘s network B address

❶ Bill sends mapping to Mike

❷ Mike sends following packets directly to Bill’s address on visited network B

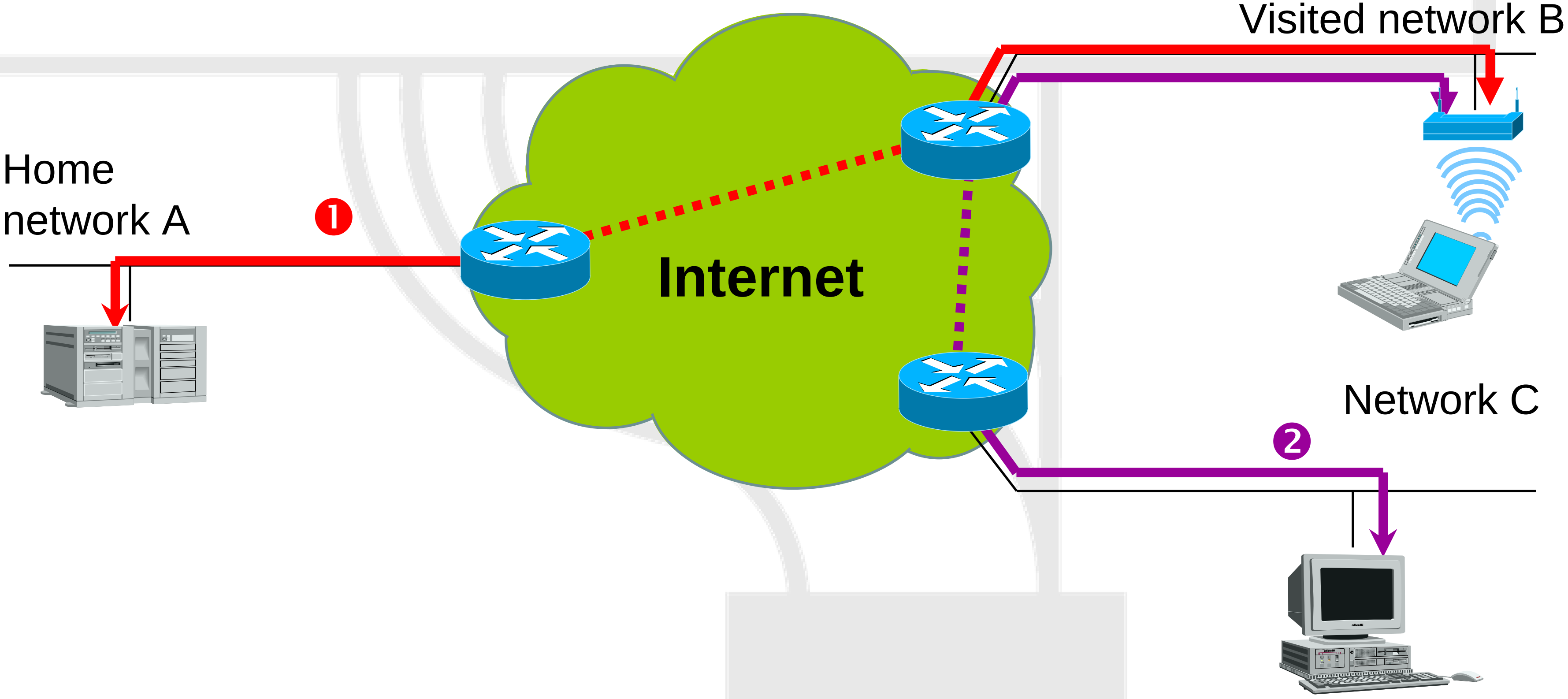
MIPv6 – Attack Scenario



❶ Bill sends mapping to Mike

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

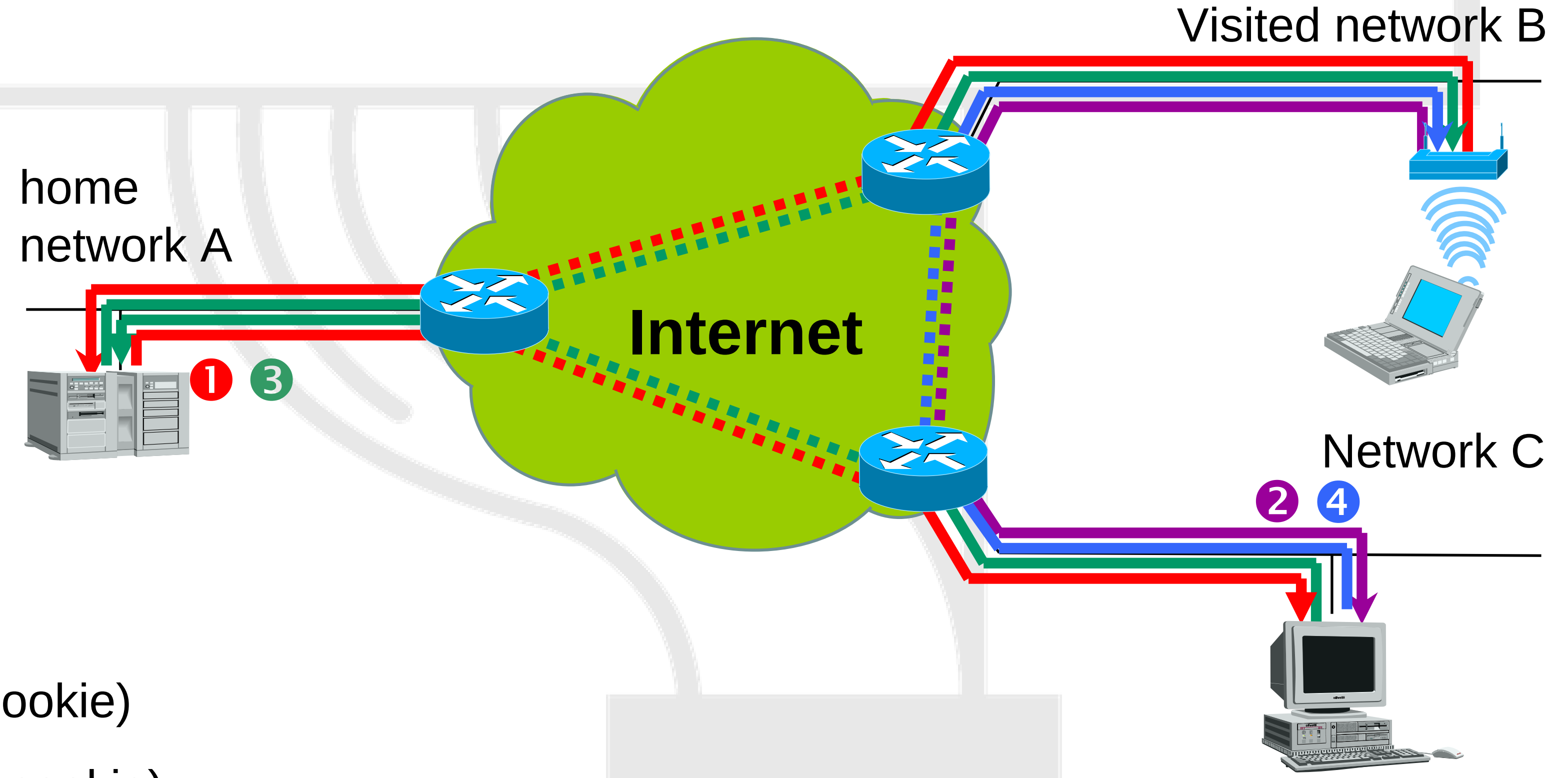
MIPv6 – Trust Relationship



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

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

MIPv6 - Return routability



lome Test Init (HoT cookie)

Care-of Test Init (CoT cookie)

lome Test (HoT cookie, home keygen token, home nonce index)

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 here (see next slides)

This still requires Return Routability itself to proof reachability of MN's addresses

Cryptographically Generated Addresses (CGA) Overview

- – IPv6 addresses, which carry hashed information about public key in the identifier part
- – Benefits
  - Provide similar to certificates a binding of IP address to public keys without requiring a key management infrastructure
  - Help to secure IPv6 Neighbor Discovery (resolve chicken-egg problem of IPsec)
  - Could help to further secure Mobile IPv6 Binding infomtion

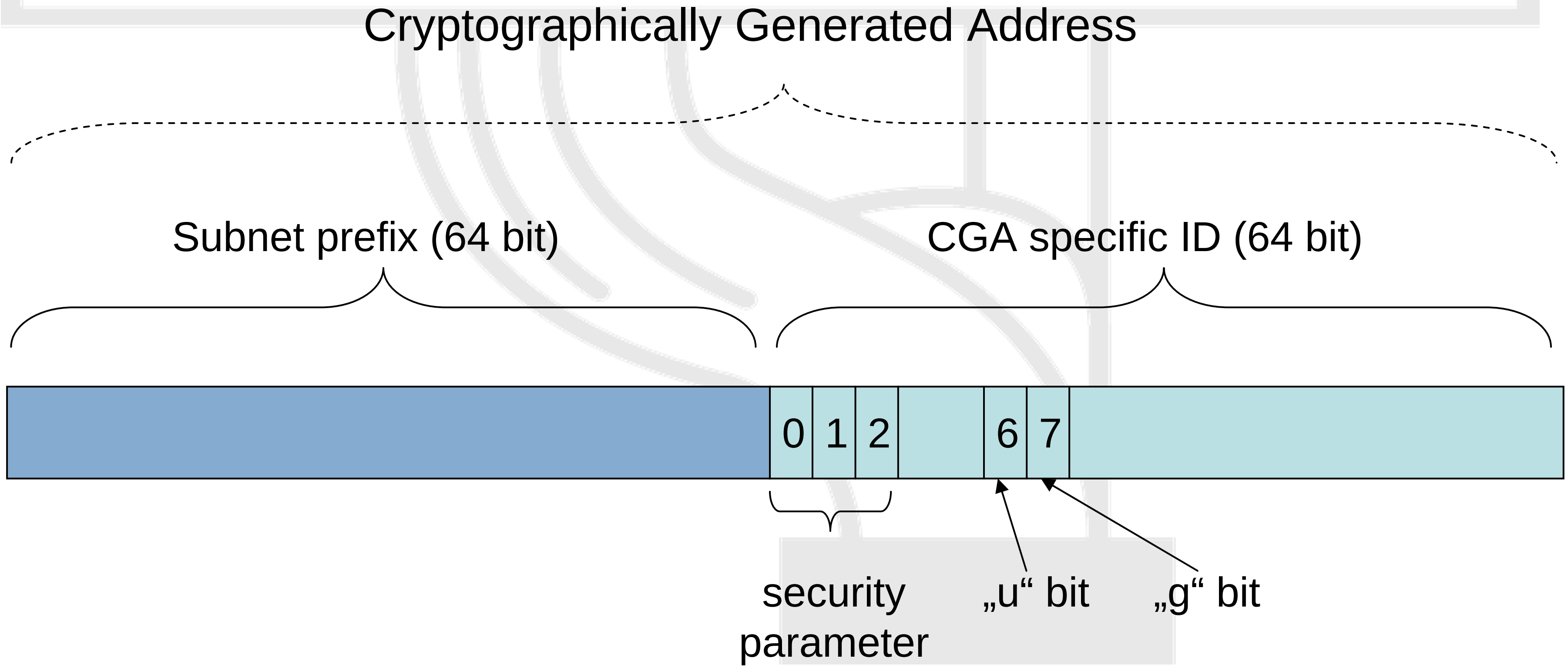
CGA - parameters

- – Modifier
  - • 16 octets long, Chosen arbitrarily
- – Address prefix
  - • 8 octet long, Prefix valid on the respective link
- – Collision count, 1 octet long
- – Public key, Variable length

CGA – generation of Pub/Priv Key Pair

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



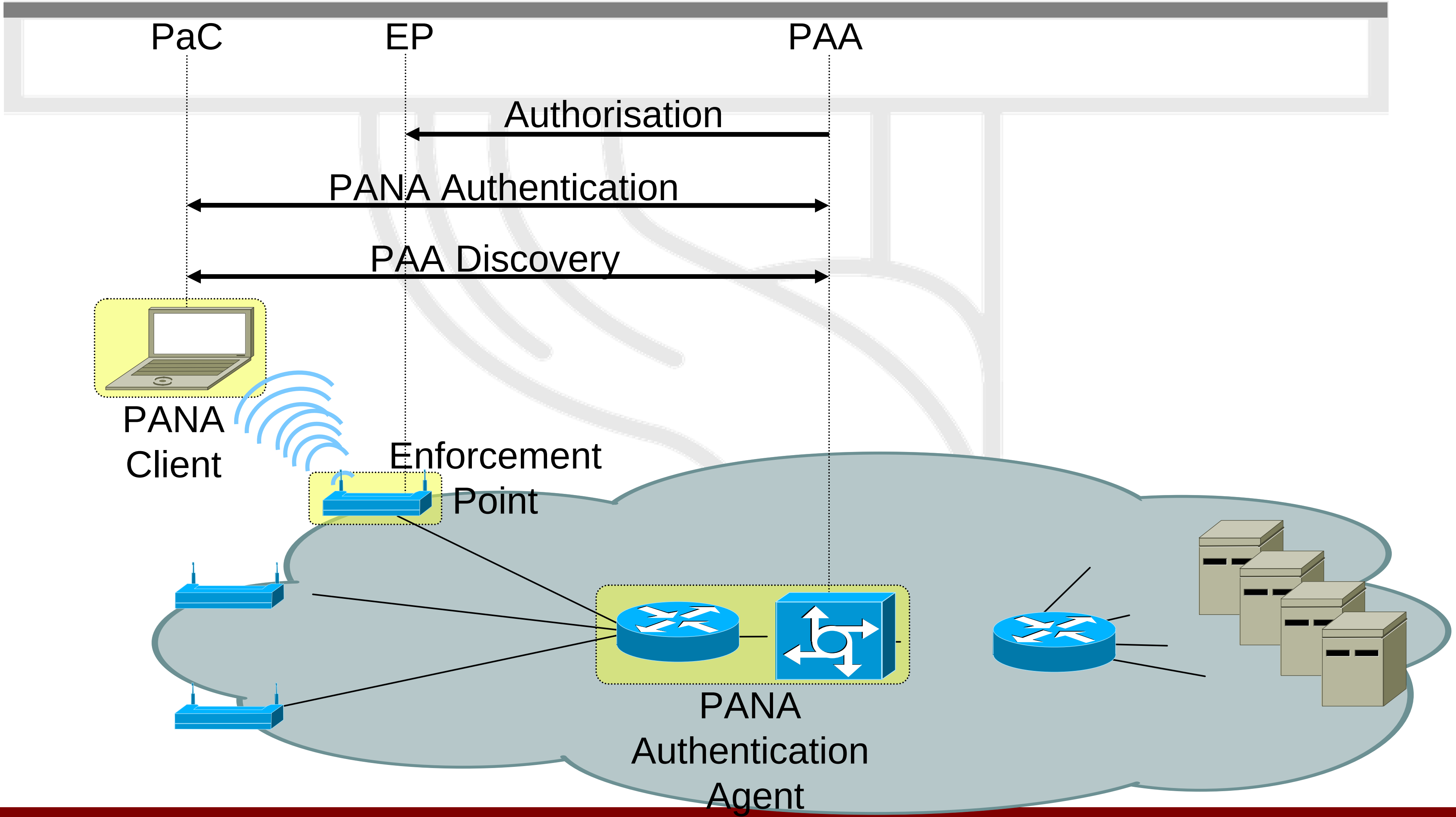
Protocol for Authentication and Network Access

PANA

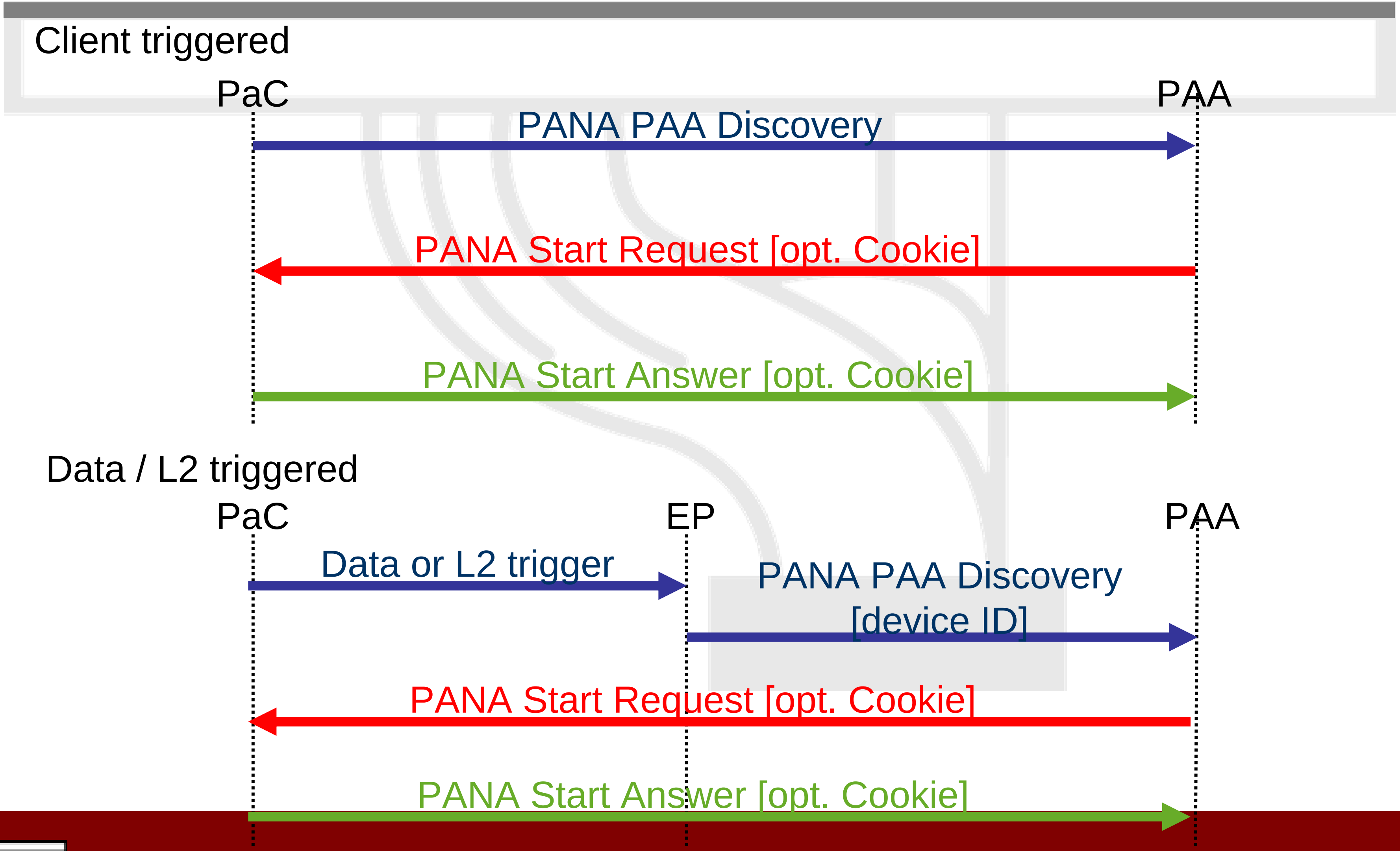
PANA - overview

- Intention
  - Enable network access authentication
  - Provide a link layer agnostic solution
- Protocol aspects
  - PANA is an own protocol
  - Runs on top of UDP / IP
  - Carries EAP authentication messages (EAP MD5, EAP PEAP, EAP LEAP, EAP- TLS, EAP TTLS, …)
  - Additional information in Attribute Value Pairs (Cookie, Protection-Capability, Device-ID, EP-Device-ID, EAP, MAC Session ID, …)
  - Supports separation of ISP and NAP authentication

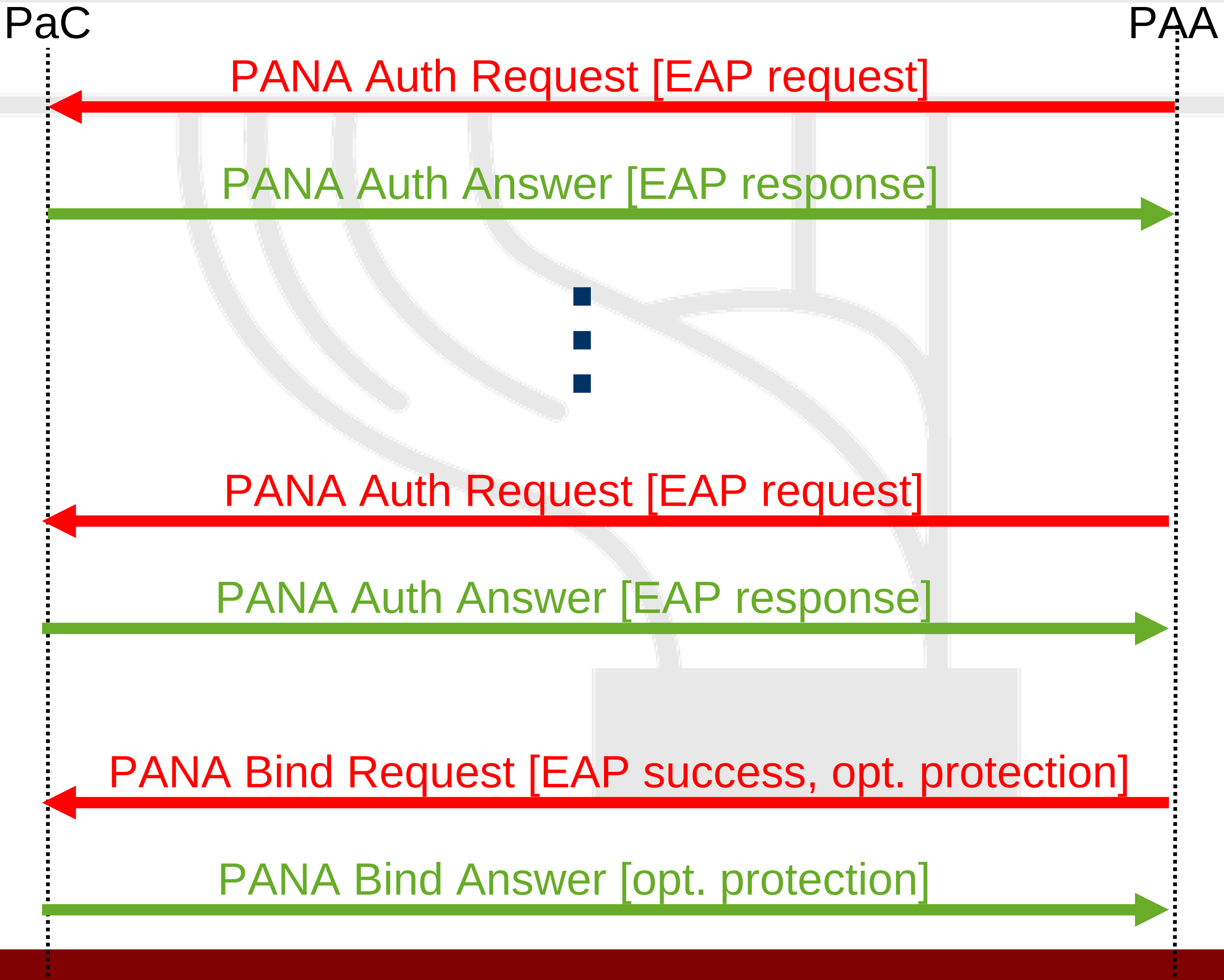
PANA - architecture



PANA - PAA discovery phase

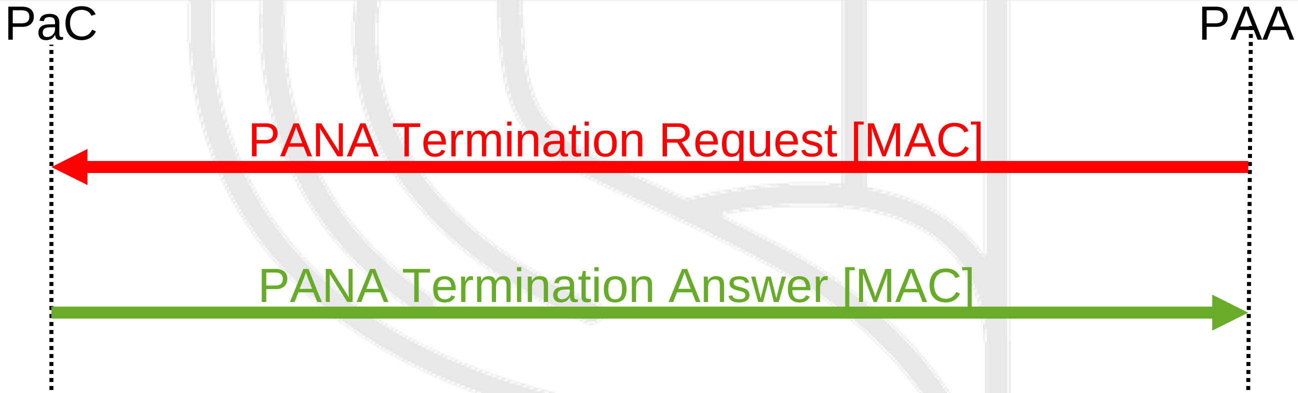

Client triggered
PaC
PAA
PANA PAA Discovery
PANA Start Request [opt. Cookie]
PANA Start Answer [opt. Cookie]
Data / L2 triggered
PaC
EP
PAA
Data or L2 trigger
PANA PAA Discovery
[device ID]
PANA Start Request [opt. Cookie]
PANA Start Answer [opt. Cookie]

PANA - authentication phase

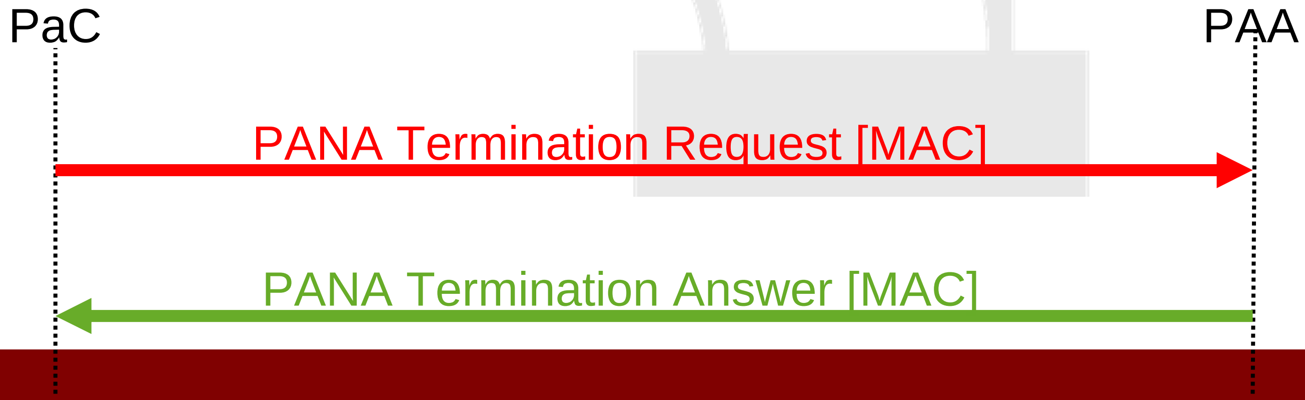

PaC
PAA
PANA Auth Request [EAP request]
PANA Auth Answer [EAP response]
PANA Auth Request [EAP request]
PANA Auth Answer [EAP response]
PANA Bind Request [EAP success, opt. protection]
PANA Bind Answer [opt. protection]

PANA - termination phase

PAA triggered



Client triggered



PANA – open issues

- Separation between EP and PAA
  - Requires communication between both
  - Not in scope of the PANA specification
  - COPS, SNMP, Diameter could be candidates here

Mobility support

- If client roams between different PAAs a re-use of existing PANA session would be nice
- Communication between involved PAAs required
- Not in scope of the PANA specification
- Context Transfer Protocol potential candidate

Specific IPv6 related problems

Threats

Unauthorized Access and Firewalls

Unauthorised Access control in IPv6

- Policy implementation in IPv6 with Layer 3 and Layer 4 is still done in firewalls
- Some design considerations! – see next slides
  - Filter site-scoped multicast addresses at site boundaries
  - Filter IPv4 mapped IPv6 addresses on the wire
  - Multiple address per interfaces

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 in IPv6

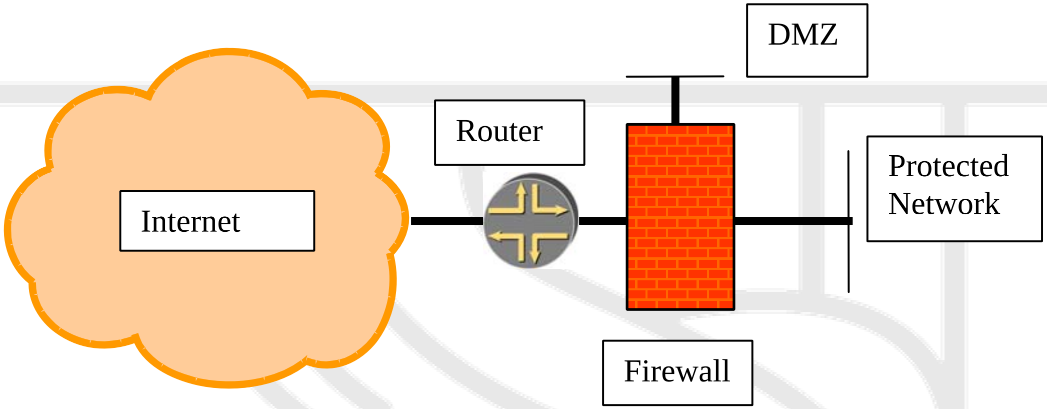
- non-routable + bogon address filtering slightly different
  - – in IPv4 easier deny non-routable + bogon
  - – in IPv6 easier to permit legitimate (almost)

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
permit	3ffe::/16	host/net	any	service
deny	any	any		

IPv6 Firewalls

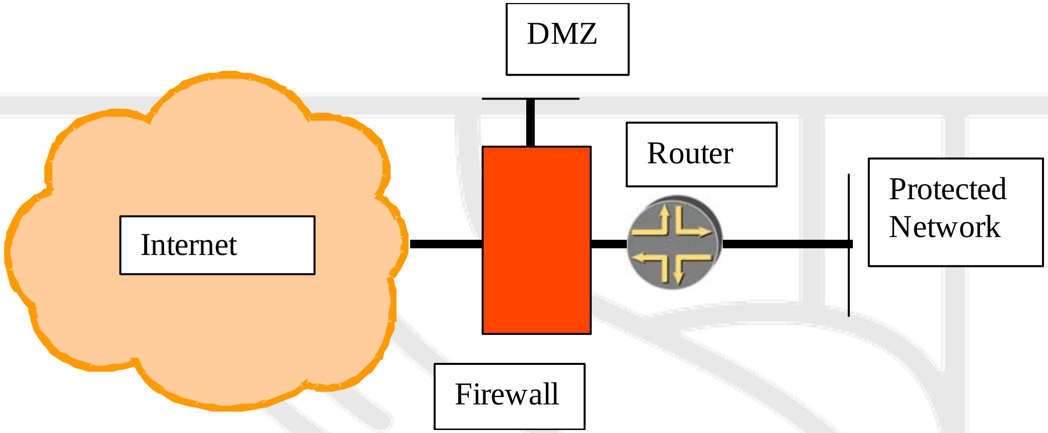
- IPv6 architecture and firewall - requirements
  - No need to NAT – same level of security with IPv6 possible as with IPv4 (security and privacy) – even better: e2e security with IPSec
  - Weaknesses of the packet filtering cannot be made hidden by NAT
  - “IPv6 does not require end-to-end connectivity, but provides end-to-end addressability”
  - Support for IPv6 header chaining
  - Support for IPv4/IPv6 transition and coexistence
  - Not breaking IPv4 security

IPv6 firewall setup - method1



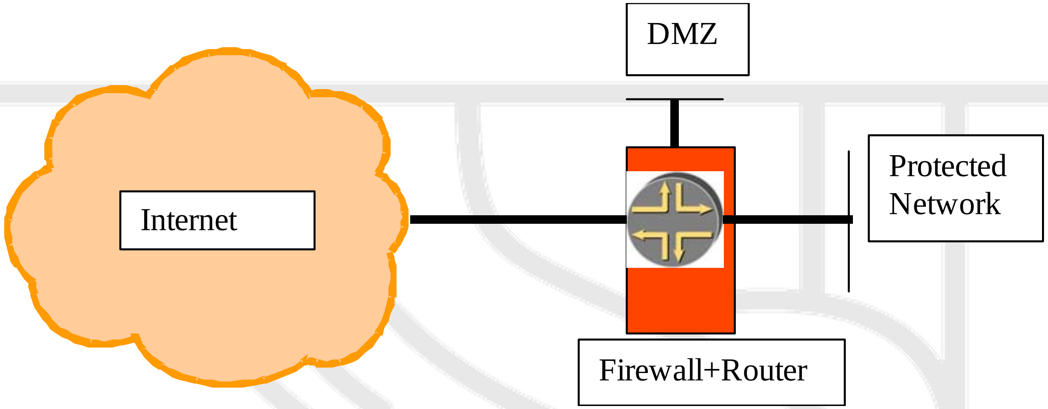
- Internet ↔router↔firewall↔net architecture
- Requirements:
  - Firewall must support/recognise ND/NA filtering
  - Firewall must support RS/RA if SLAAC is used
  - Firewall must support MLD messages if multicast is required

IPv6 firewall setup - method2



- 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 - method3



- 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 AND firewall do

Firewall setup

- 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
NS/NA	Required for normal operation – except static ND entry
RS/RA	For Stateless Address Autoconfigration
Packet too big	Path MTU discovery
MLD	Requirements in for multicast in architecture 1

IPv6 specific

required

Firewall setup 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

Interoperability of filtered applications

- FTP:
  - Very 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)

Overview of IPv6 firewalls

	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

Threats

Fragmentation and header handling

Header Manipulation and Fragmentation Best Practices

- Deny IPv6 fragments destined to an internetworking device - Used as a DOS vector to attack the infrastructure
- Ensure adequate IPv6 fragmentation filtering capabilities. For example, drop all packets with the routing header if you don't have MIPv6
- Potentially drop all fragments with less than 1280 octets (except the last fragment)
- All fragment should be delivered in 60 seconds otherwise drop

Threats

L3-L4 spoofing

L3- L4 Spoofing in IPv6

- While L4 spoofing remains the same, IPv6 address are globally aggregated making spoof mitigation at aggregation points easy to deploy
- Can be done easier since IPv6 address is hierarchical
- However host part of the address is not protected
  - You need IPv6 <– >MAC address (user) mapping for accountability!

Threats

IPv4 ARP and DHCP attacks - Subverting host initialization

Autoconfiguration/Neighbour Discovery

- Neigbor Discovery ~ security ~ Address Resolution Protocol
  - No attack tools – arp cache poisioning
  - No prevention tools – dhcp snooping
- Better solution with SEND
  - based on CGA: token1=hash(modifier, prefix, publickey, collision-count)
  - RFC3972 available!
- DHCPv6 with authentication is possible
- ND with IPSec also possible

Threats

Broadcast amplification

Amplification (DDoS) Attacks

- There are no broadcast addresses in IPv6
  - This would stop any type of amplification/"Smurf" attacks that send ICMP packets to the broadcast address
  - Global multicast addresses fro special groups of devices, e.g. link-local addresses, site-local addresses, all site-local routers, etc.
- IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to global multicast addresses (exception Packet too big message – it is questionable practice).
  - 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 implementation follow the RFC 2463
- Implement RFC 2827 ingress filtering
- Implement ingress filtering of IPv6 packets with IPv6 multicast source address

Other threats

- 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
- 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

Specific IPv6 related threats

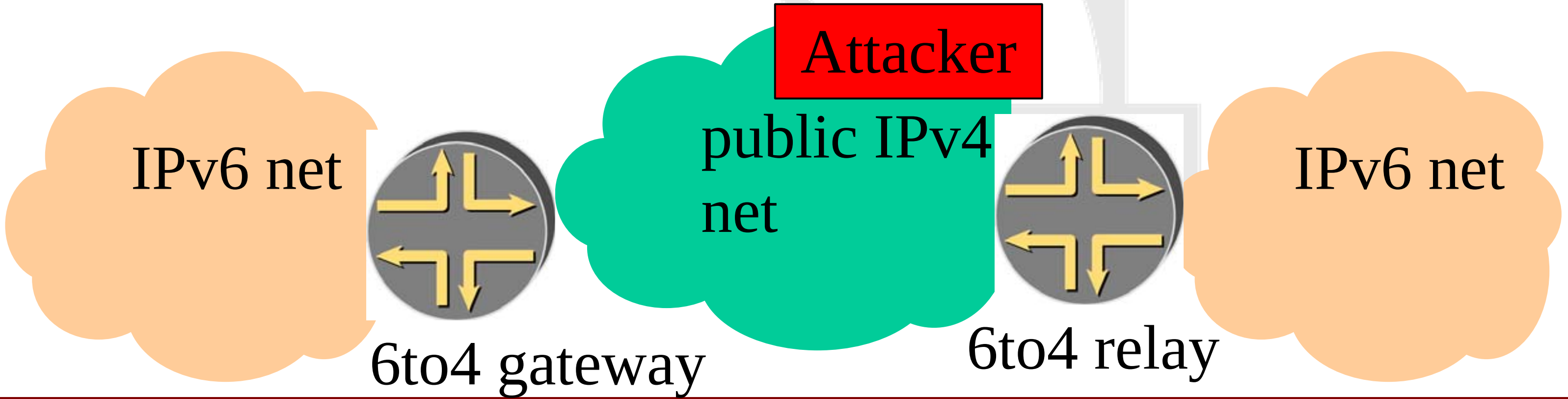
Transition Mechanisms

IPv6 transition mechanisms

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

L3 – L4 Spoofing in IPv4 with 6to4

- For example, via 6to4 tunneling 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



Mixed IPv4/IPv6 environments

- There are security issues with the transition mechanisms
  - Tunnels are extensively used to interconnect networks over areas supporting the “wrong” version of protocol
  - Tunnel traffic many times has not been anticipated by the security policies. It may pass through firewall systems due to their inability 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 authorized systems should be allowed as tunnel end-points
  - Automatic tunnels can be secured by IPSec

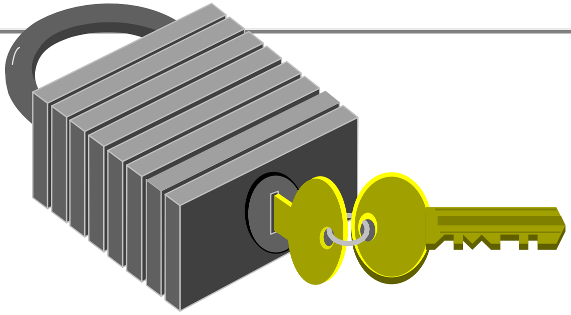
IPv6 security infrastructure

- IPSec
- AAA
  - – Radius only -> Diameter?
  - – TACACS+ - no plan

IPv6 Security infrastructure

IPSec

IPSec



- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management - requires a PKI infrastructure (IKE) – new simplified and unified IKEv2 will be available soon.
- applicable to use over LANs, across public & private WANs, & for the Internet
- IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.
- IPSec is mandated in IPv6 – you can rely on for e2e security
  - But some like 3G may not use it after all!

Security: IPsec

- Work made by the IETF IPsec wg
- Applies to both IPv4 and IPv6 and its implementation is:
  - Mandatory for IPv6
  - Optional for IPv4

- IPsec Architecture: RFC 2401

- IPsec services
  - Authentication
  - Integrity
  - Confidentiality
  - Replay protection

- IPsec modes: Transport Mode & Tunnel Mode

- IPsec protocols: AH (RFC 2402) & ESP (RFC 2406)

IPsec Architecture (RFC 2401)

- Security Policies: Which traffic is treated?
- Security Associations: How is traffic processed?
- Security Protocols: Which protocols (extension headers) are used?
- Key Management: Internet Key Exchange (IKE)
- Algorithms: Authentication and Encryption

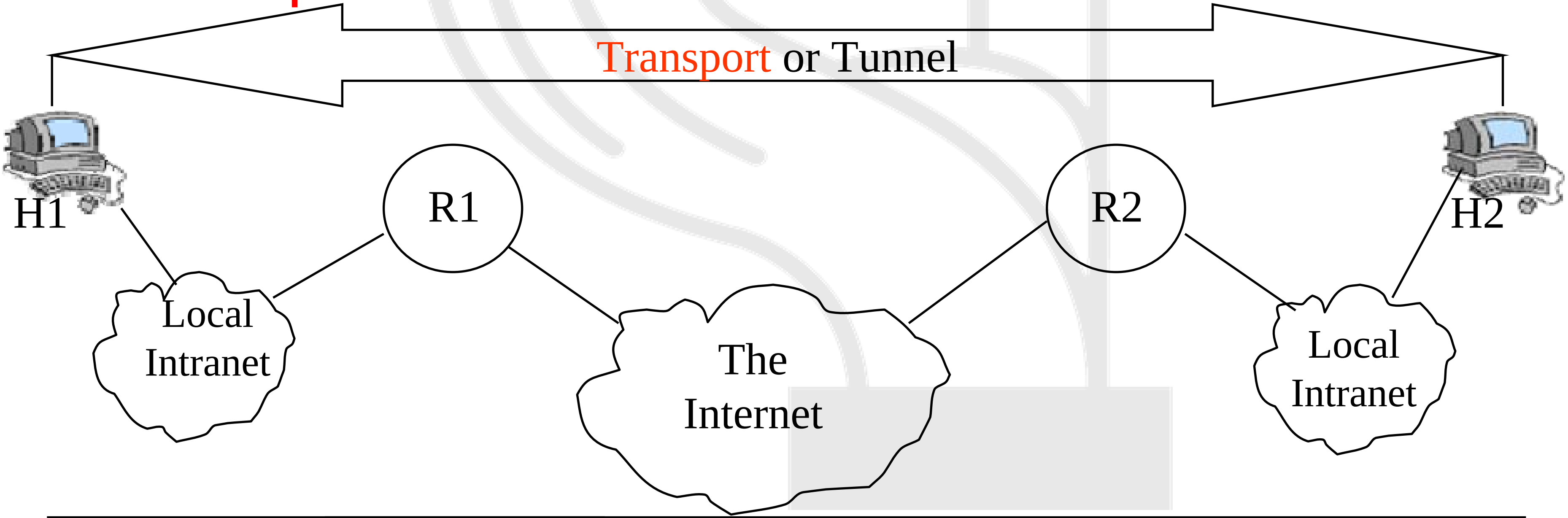
IPsec Modes

- Transport Mode
  - Above the IP level
  - Below the Transport level
  - Only the IP datagram payload is protected

- Tunnel Mode
  - IP within IP
  - Below the transport level
  - All the tunneled IP datagram is protected

IPsec Scenarios
Scenario 1: H2H

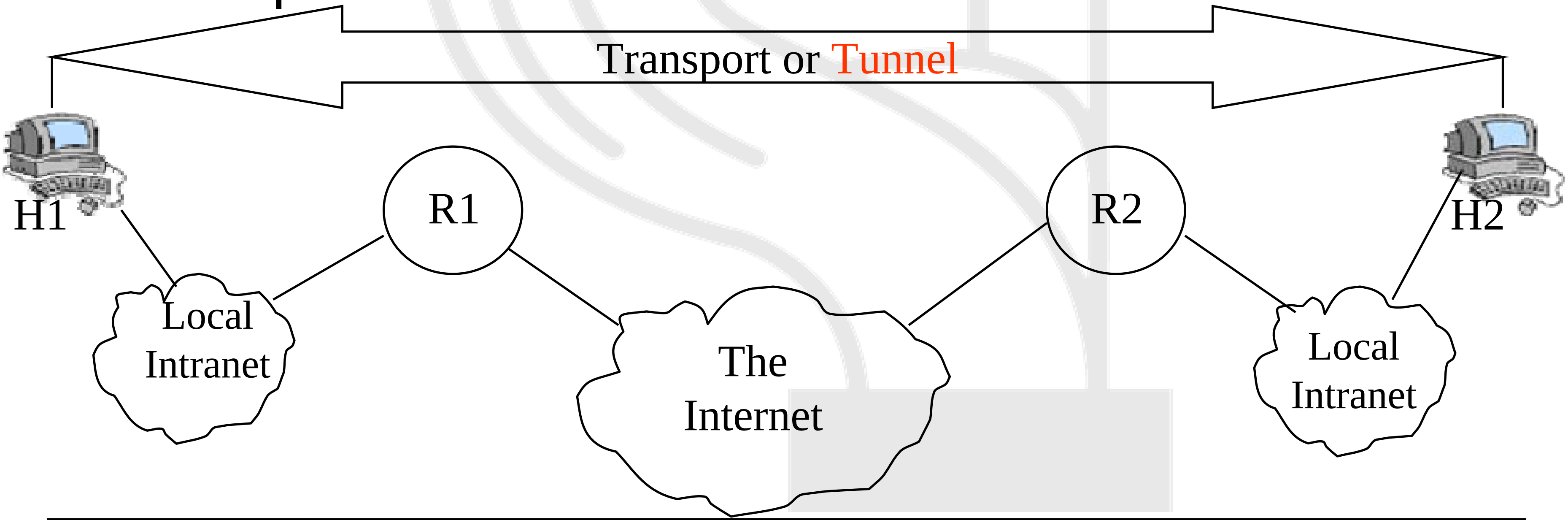
- End-to-end service
- Transport/Tunnel mode between the 2 hosts



IP header	**IPsec ext** **AH/ESP**	Payload

IPsec Scenarios
Scenario 1: H2H

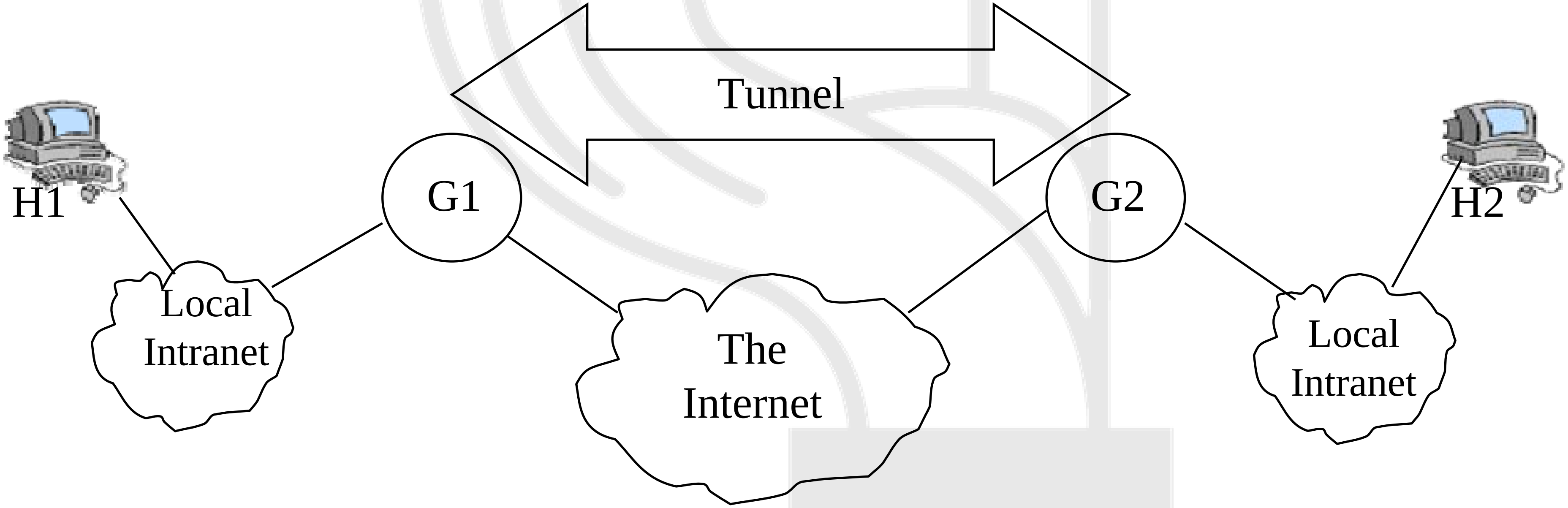
- End-to-end service
- Transport/Tunnel mode between the 2 hosts



IP header	IPsec ext AH/ESP	Inner IP header	Payload

IPsec Scenarios
Scenario 2: G2G

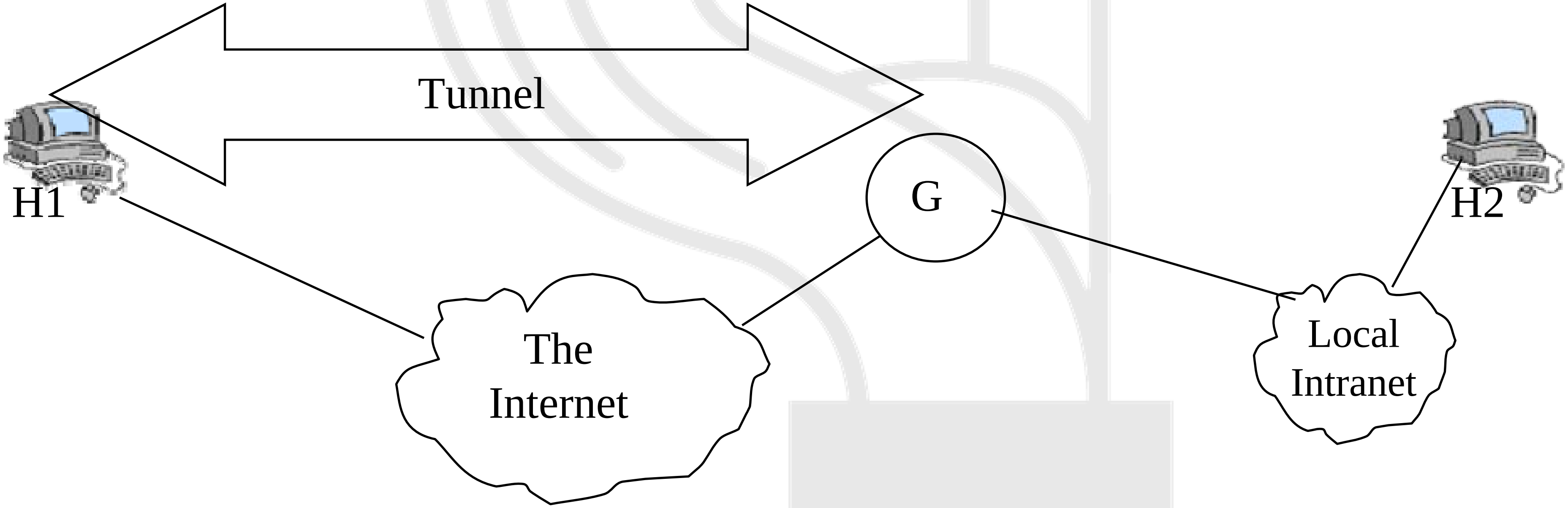
- VPN, Site-to-Site/ISP agreements, …
- Tunnel between the 2 gateways



IP header	**IPsec ext AH/ESP**	**Inner IP header**	Payload

IPsec Scenarios
Scenario 3: H2G, G2H

- Dial-in users
- Tunnel between the “external” host and the gateway



IP header	**IPsec ext AH/ESP**	**Inner IP header**	Payload

IPsec Protocols

- Authentication Header (AH)
  - RFC 2402
  - Protocol# (Next Header) = 51
  - Provides:
    - Connectionless Integrity
    - Data origin authentication
    - Replay protection
  - Is inserted
    - In Transport mode: After the IP header and before the upper layer protocol (UDP, TCP, …)
    - In Tunnel mode: Before the original IP header (the entire IP header is protected)

- Encapsulation Security Payload Header (ESP)
  - RFC 2406
    - Protocol# (Next Header) = 50
  - Provides:
    - Connectionless Integrity
    - Data origin authentication
    - Replay protection
    - Confidentiality
  - Is inserted
    - In Transport mode: After the IP header and before the upper layer protocol
    - In Tunnel mode: before an encapsulated IP header

IPsec: Protocols, services & modes combinations

	Transport Mode	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header	Authenticates entire inner IP datagram (header + payload), + selected portions of the outer IP header
ESP	Encrypts IP payload	Encrypts inner IP datagram
ESP with Authentication	Encrypts IP payload and authenticates IP payload but not IP header	Encrypts and authenticates inner IP datagram

IPsec : Key Management

- Manual
  - Keys configured on each system
- Automatic: IKE (Internet Key Exchange, RFC 2409)
  - Security Association negotiation: ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408)
    - Different blocs (payloads) are chained together after ISAKMP header
  - Key Exchange Protocols: Oakley, Scheme
  - IKEv2: much simpler (work in progress)
- Algorithms: Authentication and Encryption

IPv6 Security infrastructure

Firewalls

See earlier and the references

Summary

- IPv6 has potential to be a foundation of a more secure Internet
- Elements of the IPv6 security infrastructure
  - Firewalls, IPSec, AAA, Mobile IP etc.
- are mature enough to be deployed in production environment.
- Other elements are in prototype state
    - CGA, PANA, VPNs

But even these are ready for experimental deployment

A Few Specific References

- 6NET D3.5.1: Secure IPv6 Operation: Lessons learned from 6NET
- J. Mohacsi, “IPv6 firewalls”, presentation on the 5th TF-NGN meeting, October 2001 available at http:///skye.ki.iif.hu/~mohacsi/athens_tf_ngn_ipv6_firewalls.pdf
- J.Mohacsi, “Security of IPv6 from firewalls point of view”, presentation on TNC2004 conference, June 2004, available at http://www.terena.nl/conferences/tnc2004/programme/presentations/show.php?pres_id=115
- 6NET D6.2.2: Operational procedures for secured management with transition mechanisms
- S. Convery, D Miller, IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)", presentation at the 17th NANOG, May 24, 2004
- János Mohácsi, Elwyn Davis: Draft-v6ops-icmpv6-filtering-bcp-00.txt