Security Considerations for IPv6 Networks

Yannis Nikolopoulos
yanodd@otenet.gr

Ημερίδα Ενημέρωσης Χρηστών για την Τεχνολογία IPv6 - Αθήνα, 25 Μαίου 2011

Agenda

- Introduction – Major Features in IPv6
- IPv6 more secure than IPv4?
- IPSec
- IPv4 vs IPv6: a Threat Comparison
- ND revisited
- ND-related Threats: an Overview
- Security Risks During IPv4→IPv6 Transition
- Home IPv6 Network
- References
- Appendix I

Major Features in IPv6

- Extended Address Space
- Autoconfiguration
- Header Structure / Extension Headers
- Mandatory IPSec Support
- QoS
- Route Aggregation
- Efficient Transmission

IPv6 more secure than IPv4?

Lets agree that IPv6 is (will) not inherently be more or less secure than IPv4

IPv6 more secure than IPv4?

Lets agree that IPv6 is (will) not inherently be more or less secure than Ipv4

In many cases, IPv4 security practices and policies can be replicated for IPv6

IPv6 more secure than IPv4?

- Fairly new and undiscovered territory
- Uncalculated Factors: tunneling and all 6to/in4
- Lack of understanding
- Vulnerabilities unknown

IPv6 more secure than IPv4?

- Fairly new and undiscovered territory
- Uncalculated Factors: tunneling and all 6to/in4
- Lack of understanding
- Vulnerabilities unknown

What about IPSec??

IPSec

- Authenticate and (optionally) encrypt IP packets end-to-end
- Mandatory implementation in IPv6

but...

IPSec

- Authenticate and (optionally) encrypt IP packets end-to-end
- Mandatory implementation in IPv6

but...

- Use of IPSec not required
- Will IPSec be used more frequently in IPv6? Probably not!
- Complexity Issues (key management, configuration complexity etc)

IPv4 vs IPv6: a Threat Comparison

- Reconnaissance Attacks harder to achieve with IPv6 (but still possible)
- ARP (IPv4) attacks replaced by ND-related (IPv6) attacks
- Lack of Broadcast in IPv6 means no more amplification attacks (maybe)
- Unauthorized access to IPv6 networks could be more widespread (at first)
- No significant change in Application-level attacks (after a slow start)

IPv4 vs IPv6: a Threat Comparison

- **Reconnaissance Attacks harder to achieve with IPv6 (but still possible)**
- ARP (IPv4) attacks replaced by ND-related (IPv6) attacks
- Lack of Broadcast in IPv6 means no more amplification attacks (maybe)
- Unauthorized access to IPv6 networks could be more widespread (at first)
- No significant change in Application-level attacks (after a slow start)

IPv4 vs IPv6: a Threat Comparison

- Reconnaissance Attacks harder to achieve with IPv6 (but still possible)
- **ARP (IPv4) attacks replaced by ND-related (IPv6) attacks**
- Lack of Broadcast in IPv6 means no more amplification attacks (maybe)
- Unauthorized access to IPv6 networks could be more widespread (at first)
- No significant change in Application-level attacks (after a slow start)

IPv4 vs IPv6: a Threat Comparison

- Reconnaissance Attacks harder to achieve with IPv6 (but still possible)
- ARP (IPv4) attacks replaced by ND-related (IPv6) attacks
- **Lack of Broadcast in IPv6 means no more amplification attacks (maybe)**
- Unauthorized access to IPv6 networks could be more widespread (at first)
- No significant change in Application-level attacks (after a slow start)

IPv4 vs IPv6: a Threat Comparison

- Reconnaissance Attacks harder to achieve with IPv6 (but still possible)
- ARP (IPv4) attacks replaced by ND-related (IPv6) attacks
- Lack of Broadcast in IPv6 means no more amplification attacks (maybe)
- **Unauthorized access to IPv6 networks could be more widespread (at first)**
- No significant change in Application-level attacks (after a slow start)

IPv4 vs IPv6: a Threat Comparison

- Reconnaissance Attacks harder to achieve with IPv6 (but still possible)
- ARP (IPv4) attacks replaced by ND-related (IPv6) attacks
- Lack of Broadcast in IPv6 means no more amplification attacks (maybe)
- Unauthorized access to IPv6 networks could be more widespread (at first)
- **No significant change in Application-level attacks (after a slow start)**

IPv4 vs IPv6: a Threat Comparison - Mitigation

- Efficient use of different types of addressing
- Increase difficulty in network scanning (random subnets, random interface IDs)
- Use IPSec for authentication
- Devise a proper ICMPv6 filtering policy *(see Appendix I)*
- Secure tunnelled environments (complicated)

IPv4 vs IPv6: a Threat Comparison - Mitigation

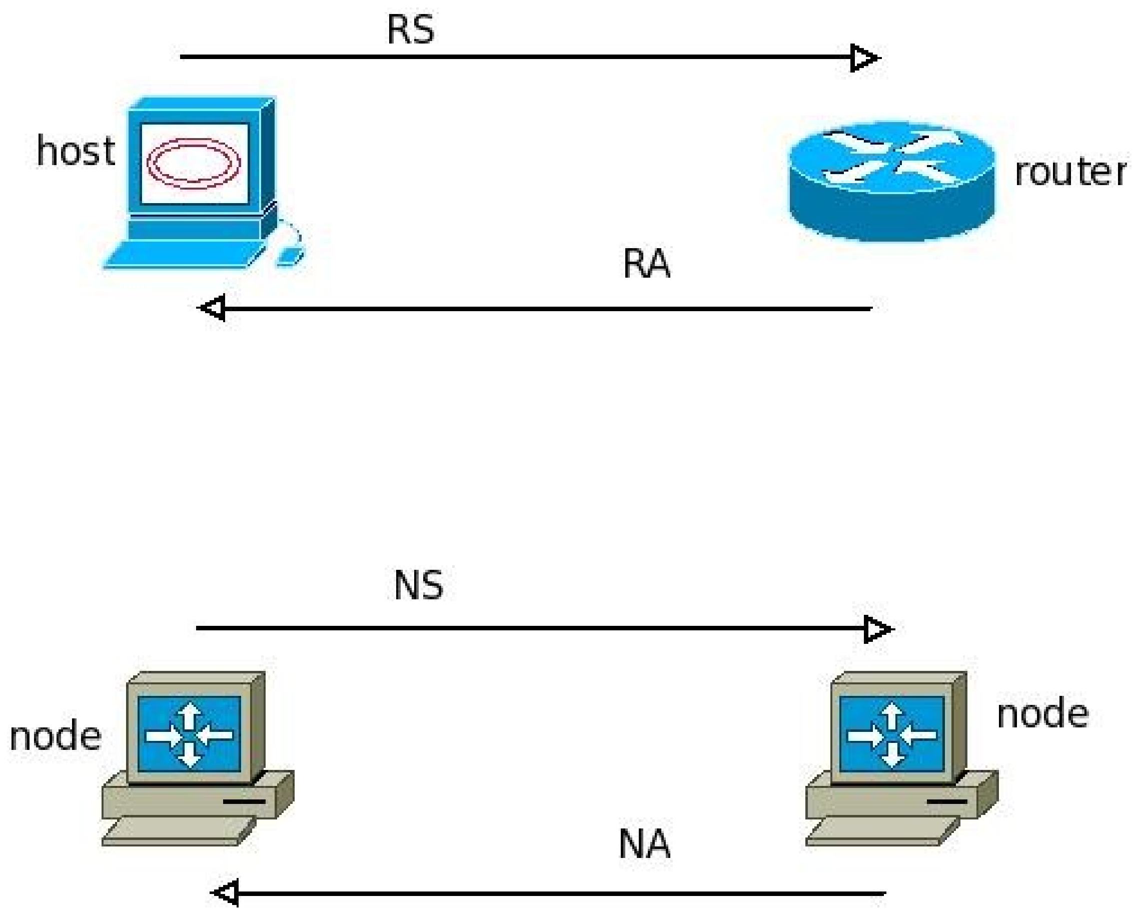
- Default DENY is still considered best practice

- Block IPv6 traffic on IPv4-only networks and vice-versa

ND Revisited

- IPv6 Address Autoconfiguration
- Determine Network Prefixes (and other configuration info)
- Duplicate Address Detection (DAD)
- Neighbor Unreachability Detection (NUD)
- Detect changes in link-layer addresses

ND Revisited



ND-Related Threats: an Overview

- Rogue RAs: rogue routers inserted on LAN
- Rogue RAs: rogue RAs from “legitimate” nodes
- Spoofed responses to DAD messages = DOS attack
- Spoofed NS/NA messages can cause redirect attacks

SeND (Secure ND) addresses some of the issues

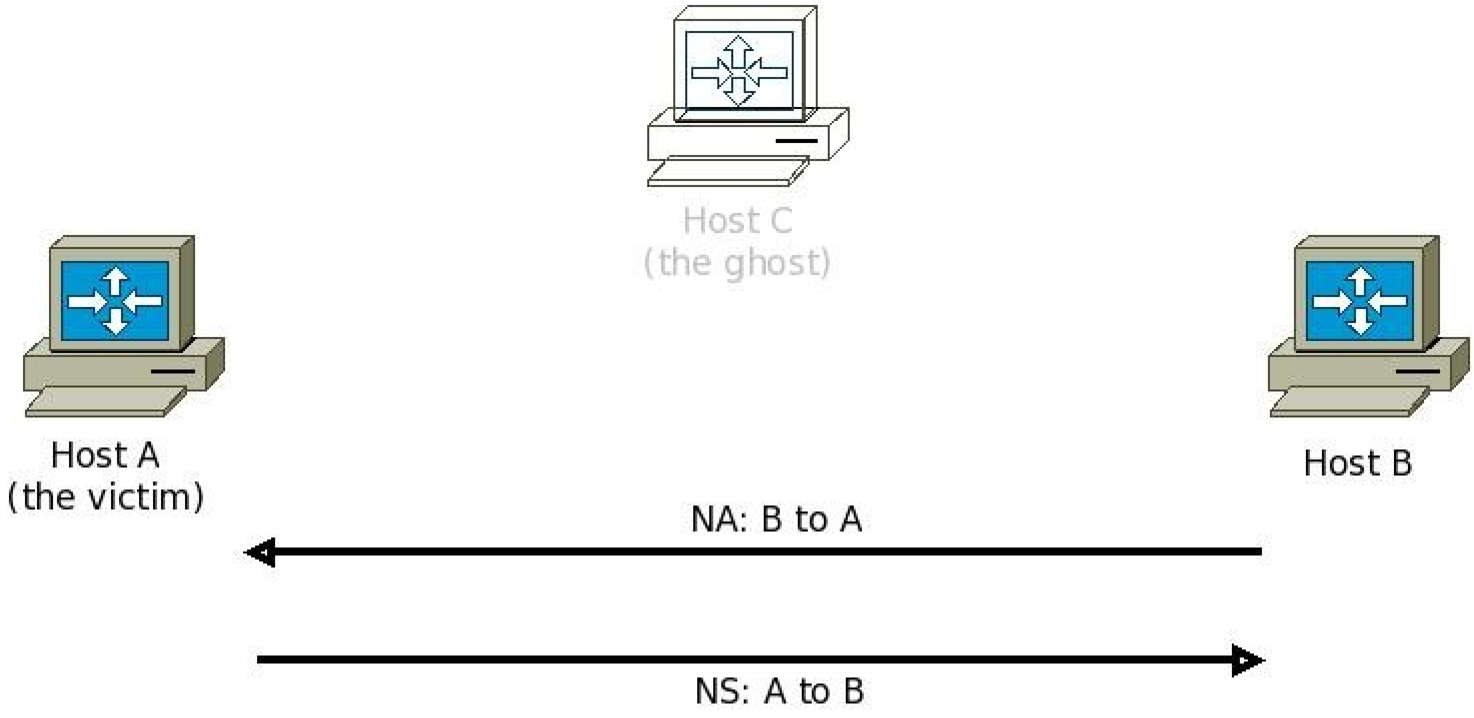
ND-Related Threats: a Case Study

Neighbor Solicitation/Advertisement Spoofing

- Host A (AKA “the victim”) sends Neighbor Solicitation (NS) to Host B
- Host C (AKA “the attacker”) replies with Neighbor Advertisement (NA) instead of the real host B to gracious Neighbor Solicitation (NS) message by host A.
- Host A updates its NDP cache binding the link-layer address of the attacker to the legitimate IP address of host B.
- The victim will send packets to the attacker instead of legitimate Host B.

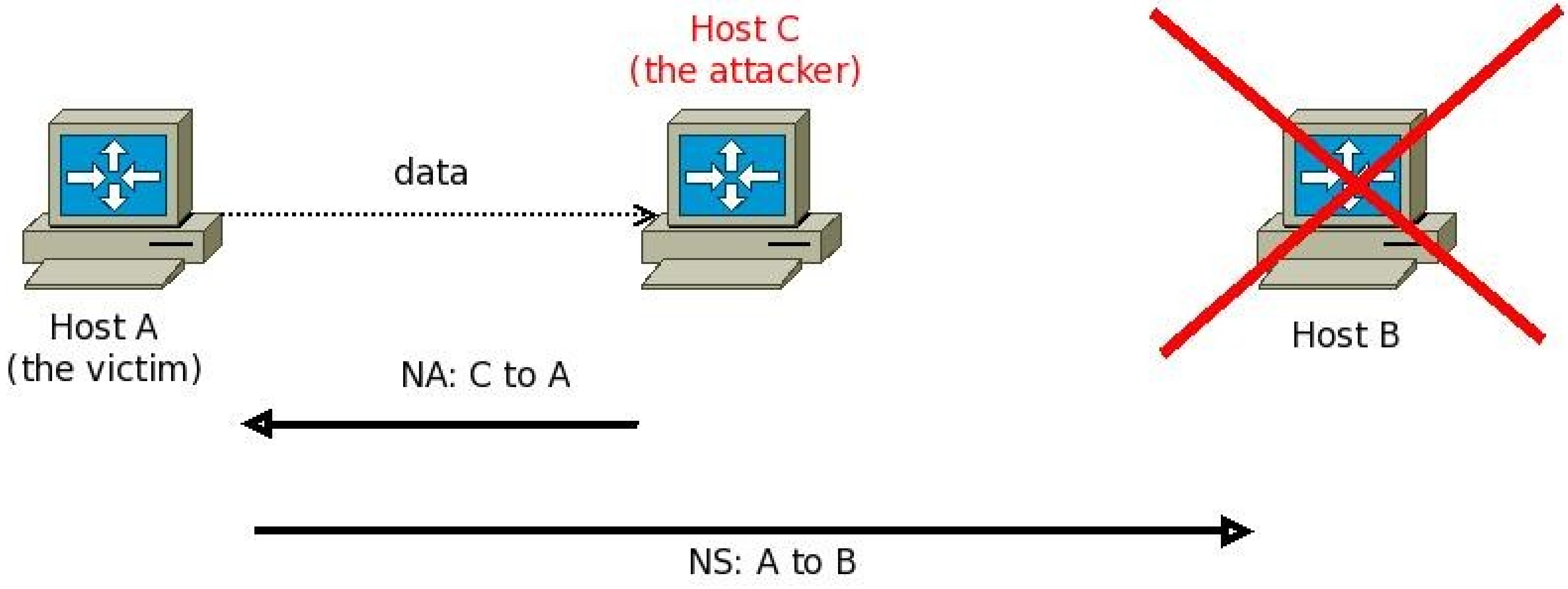
ND-Related Threats: a Case Study

Neighbor Solicitation/Advertisement Spoofing



ND-Related Threats: a Case Study

Neighbor Solicitation/Advertisement Spoofing



Security Risks During IPv4 to IPv6 Transition

- Added Complexity by dual stack operations
- Immaturity (or even lack) of IPv6 security products / lack of vendor support
- Unauthorized/unknown IPv6 clients
- Use of IPv6 by the “attacker” community
- Vulnerabilities in IPv6

Security Risks During IPv4 to IPv6 Transition

- **Added Complexity by dual stack operations**
  - 2 x configurations = 2 x things that can go wrong
  - Security infrastructure possibly not aware of dual environment
  - IPv4 still supported for legacy systems
- Immaturity (or lack) of IPv6 security products / lack of vendor support
- Unauthorized/unknown IPv6 clients
- Use of IPv6 by the “attacker” community
- Vulnerabilities in IPv6

Security Risks During IPv4 to IPv6 Transition

- Added Complexity by dual stack operations
- **Immaturity (or lack) of IPv6 security products / lack of vendor support**
    - Security vendors are waiting for customer demand
    - Various levels of IPv6 “support” offered
    - Lack of standardization of IPv6 support
- Unauthorized/unknown IPv6 clients
- Use of IPv6 by the “attacker” community
- Vulnerabilities in IPv6

Security Risks During IPv4 to IPv6 Transition

- Added Complexity by dual stack operations
- Immaturity (or even lack) of IPv6 security products / lack of vendor support
- **Unauthorized/unknown IPv6 clients**
  - IPv6 support is often enabled by default
  - Active 6to4 interfaces
- Use of IPv6 by the “attacker” community
- Vulnerabilities in IPv6

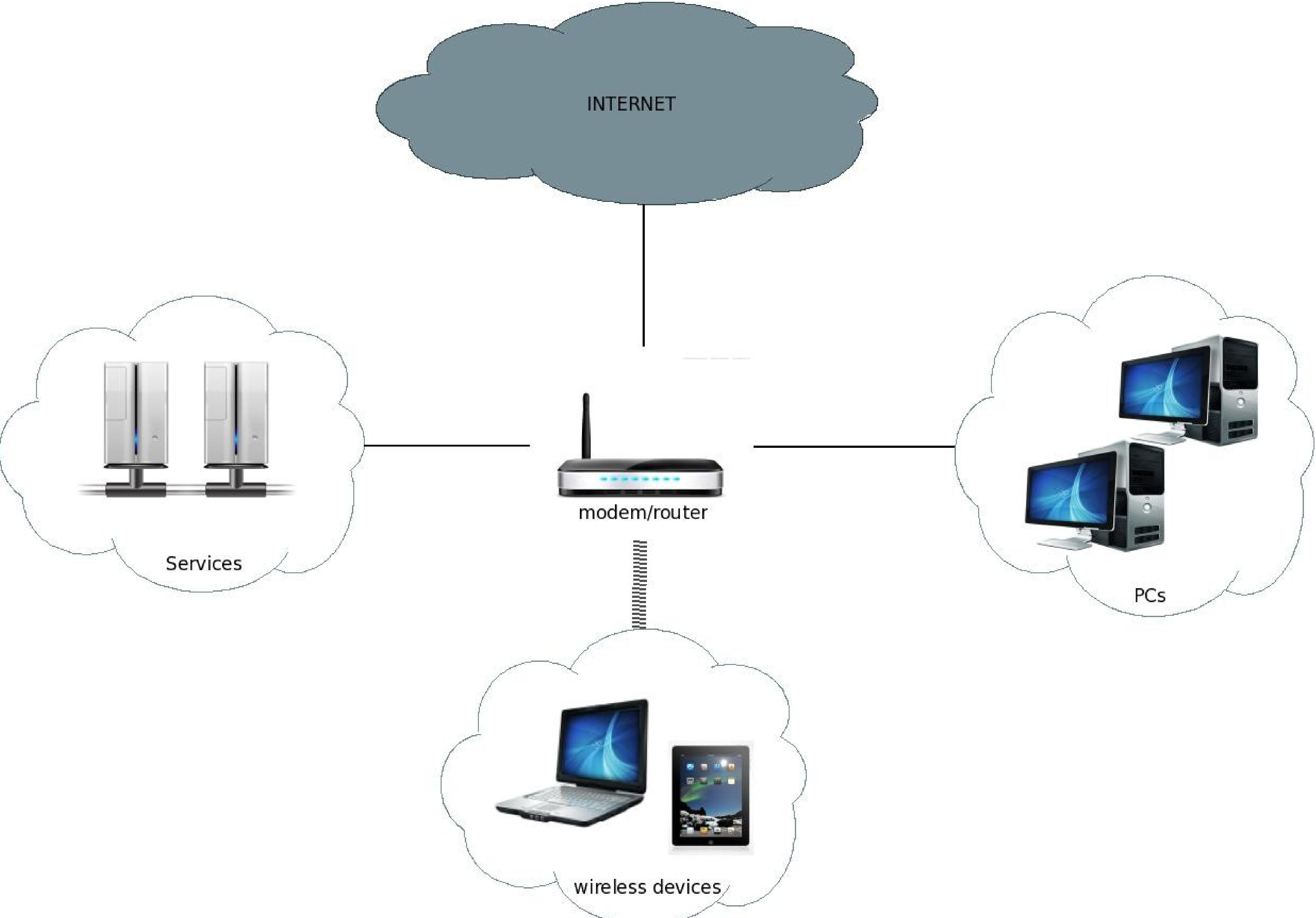
Security Risks During IPv4 to IPv6 Transition

- Added Complexity by dual stack operations
- Immaturity (or even lack) of IPv6 security products / lack of vendor support
- Unauthorized/unknown IPv6 clients
- **Use of IPv6 by the “attacker” community**
  - Firewalls often ignore IPv6 traffic
  - Attackers enabling IPv6 on compromised systems
  - IPv6 traffic usually not monitored
- Vulnerabilities in IPv6

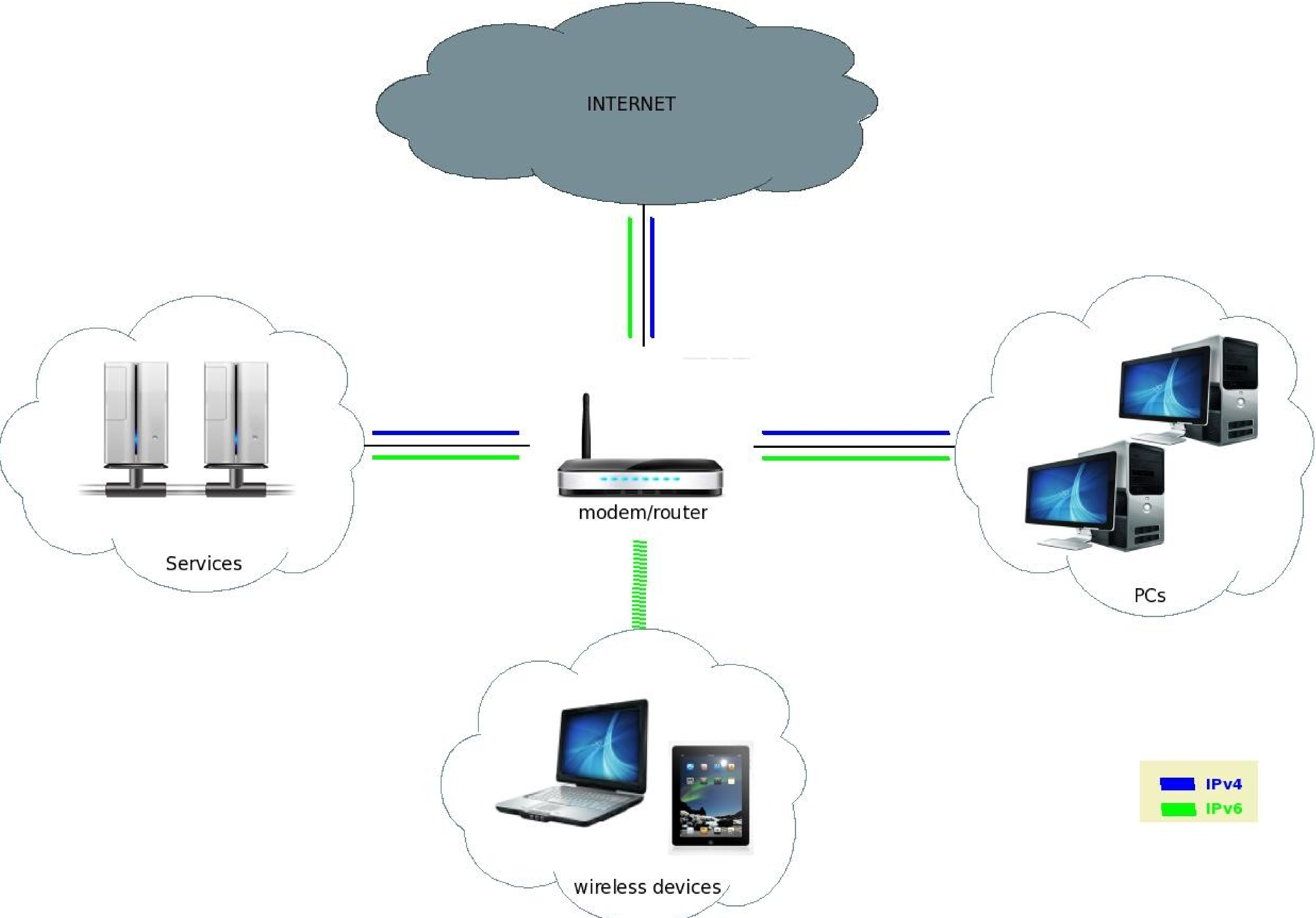
Security Risks During IPv4 to IPv6 Transition

- Added Complexity by dual stack operations
- Immaturity (or even lack) of IPv6 security products / lack of vendor support
- Unauthorized/unknown IPv6 clients
- Use of IPv6 by the "attacker" community
- **Vulnerabilities in Ipv6**
  - ND-related (as discussed)
  - 0-day exploits

Home IPv6 Network



Home IPv6 Network

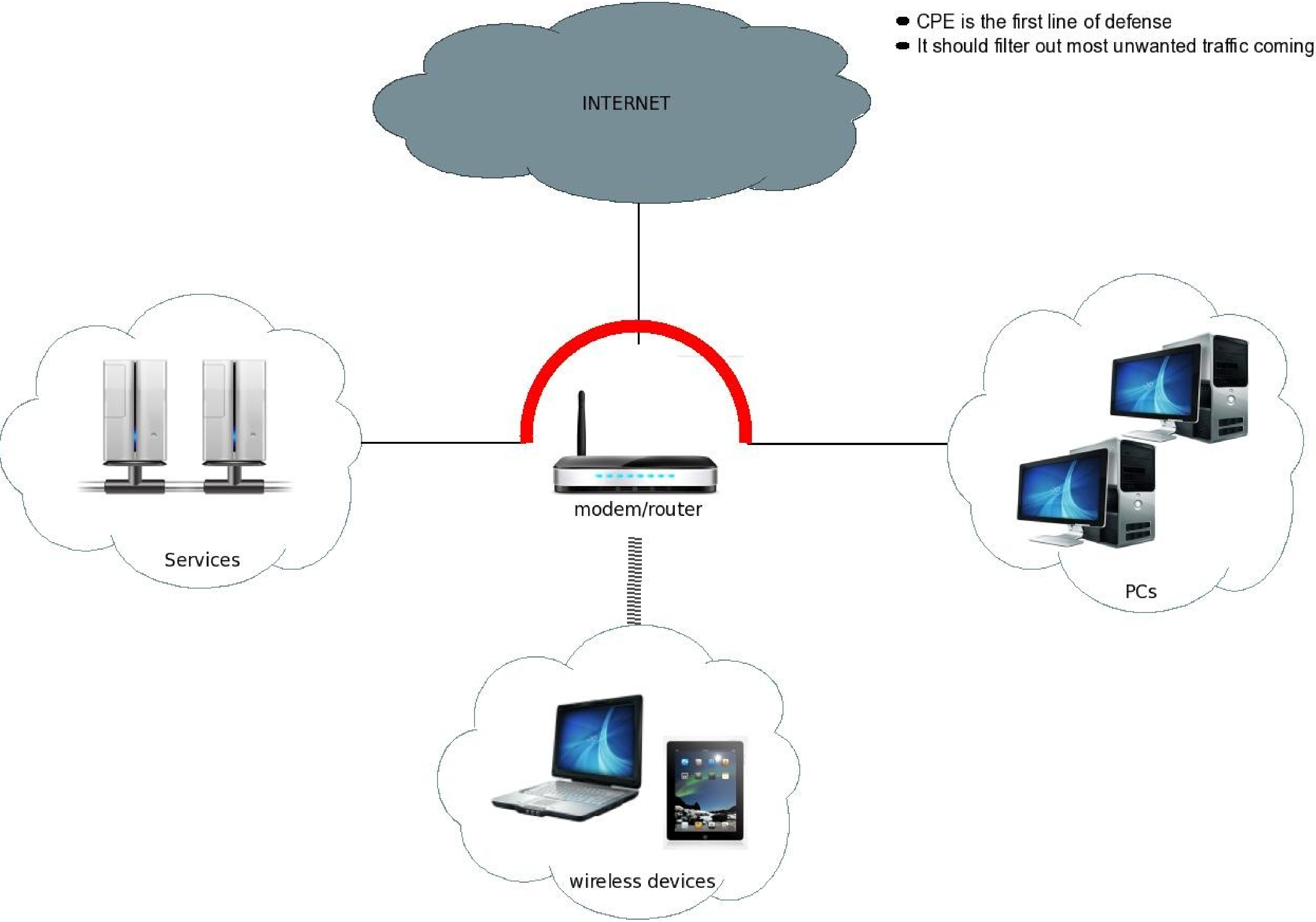


Home IPv6 Network - CPE

Layered Approach: CPE is the first layer

Home IPv6 Network - CPE

- CPE is the first line of defense
- It should filter out most unwanted traffic coming in



Home IPv6 Network - CPE

- Use Network Filters (stateless)to block unwanted traffic (spoofed, Martians etc)
- Use stateful firewalls for fine grained access
- ICMPv6 Filtering (as discussed)
- Management Interfaces should not be offered via WAN
- Use SeND (if available)

- When in bridged mode, beware of router vulnerabilities

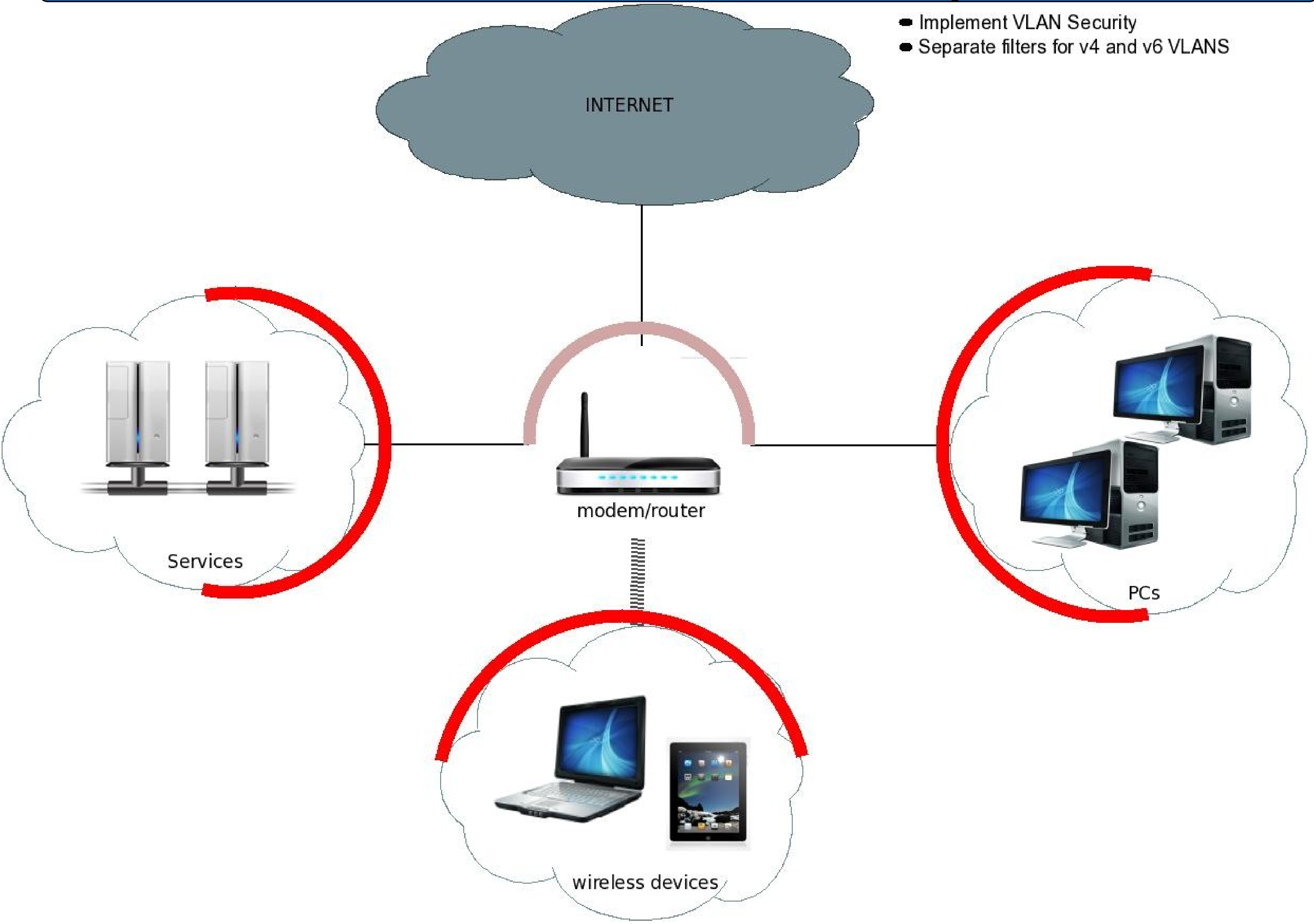
(e.g. linux with no firewall turned on)

Home IPv6 Network – CPE: VLAN protection

Layered Approach: Protect your VLANS

Home IPv6 Network – CPE: VLAN protection

- Implement VLAN Security
- Separate filters for v4 and v6 VLANS

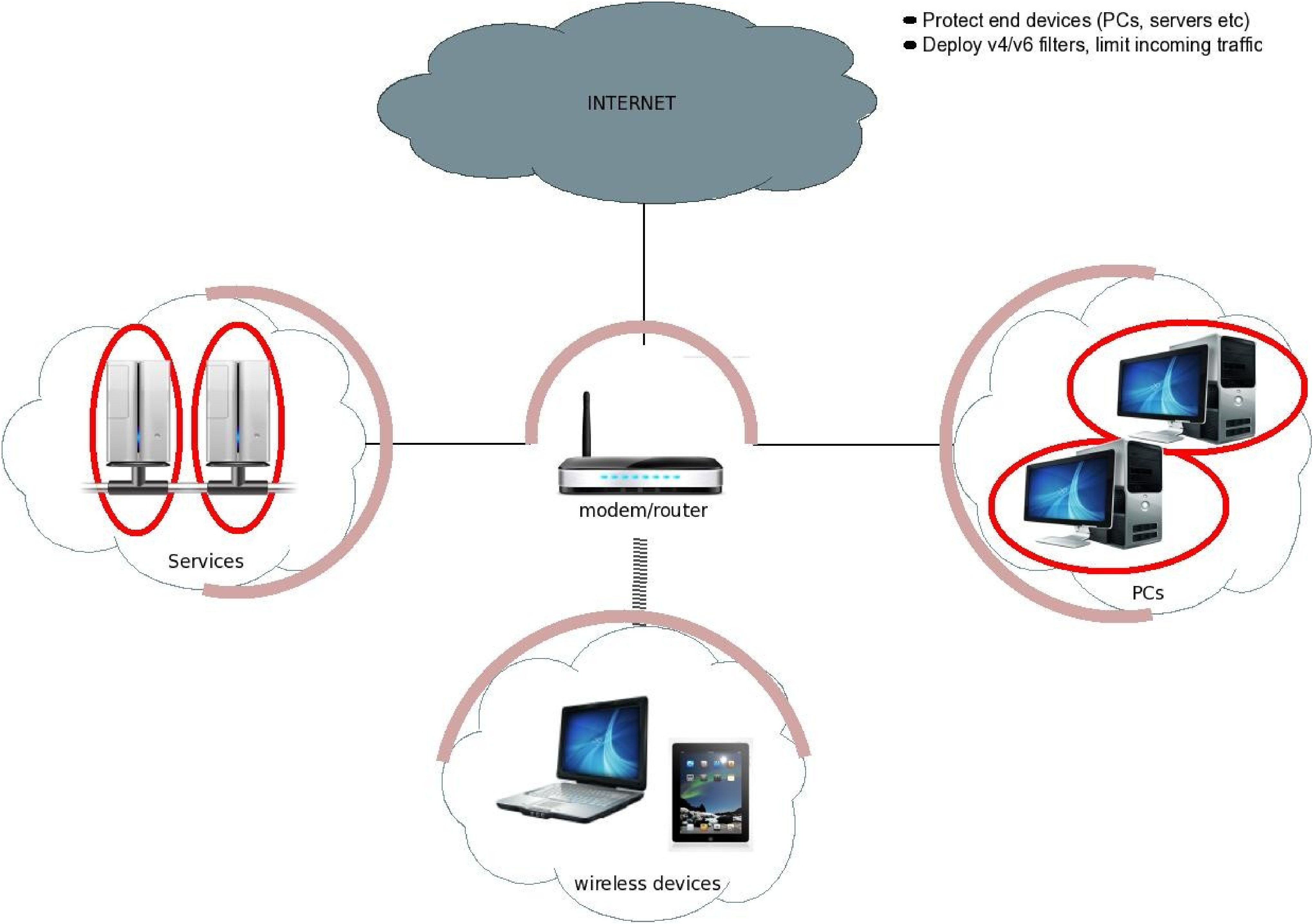


Home IPv6 Network - LAN

Layered Approach: End Devices

Home IPv6 Network - LAN

- Protect end devices (PCs, servers etc)
- Deploy v4/v6 filters, limit incoming traffic



Home IPv6 Network - LAN

- Deploy packet filters (iptables, pf etc)
- Use RA guards (if applicable)
- No “hiding” behind NAT anymore! Use privacy extensions
- Avoid Man In The Middle (MITM) attacks : use IPSec

Home IPv6 Network - LAN

Semi-Paranoid:

Exposed MAC addresses due to SLAAC (eui-64) may result to specific h/w flaw

Paranoid:

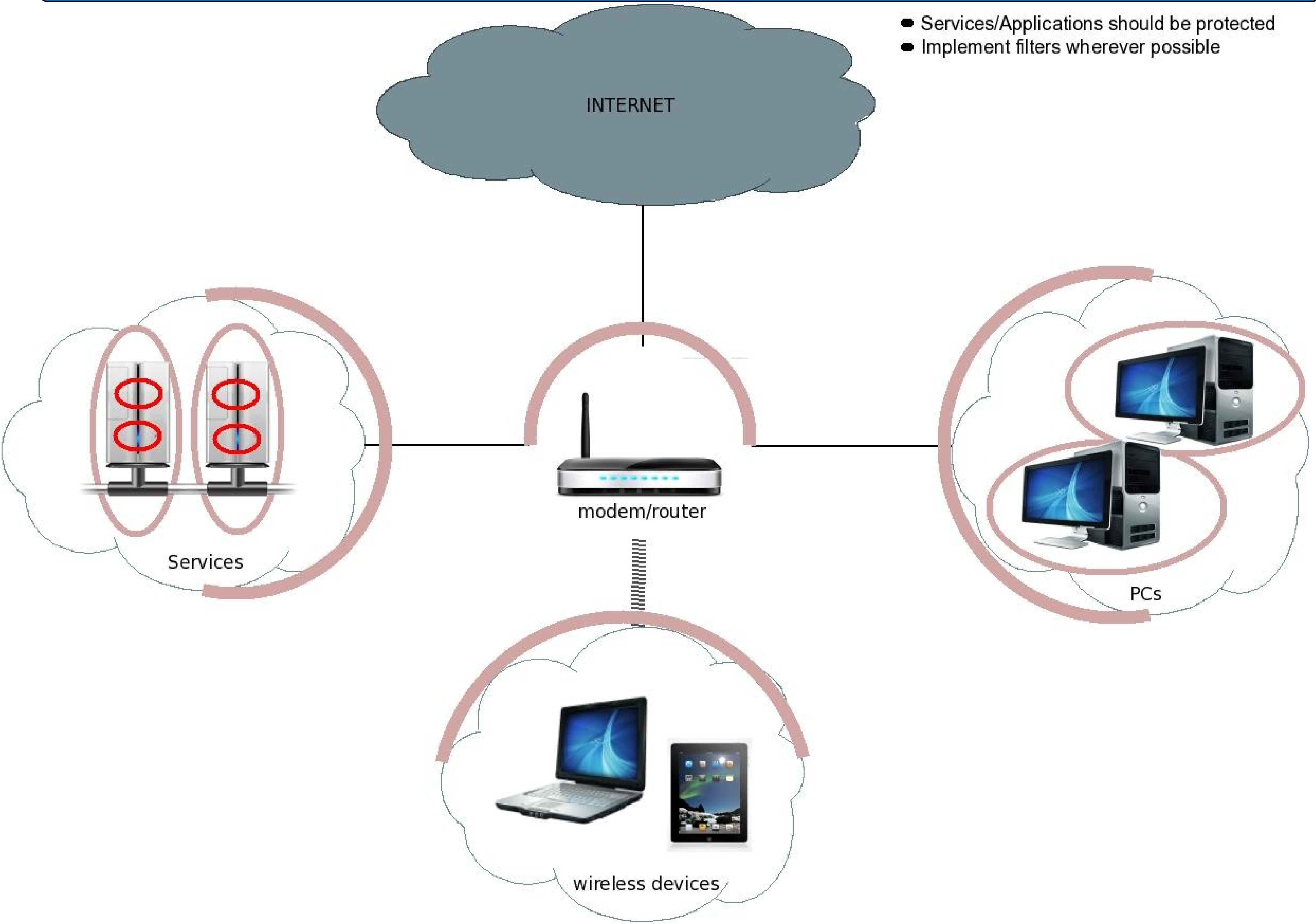
Interface can be tracked when moving around (from static interface ID)

Home IPv6 Network - Services

Layered Approach: Services Protection

Home IPv6 Network - Services

- Services/Applications should be protected
- Implement filters wherever possible



Home IPv6 Network - Summary

As mentioned, lessons learned from IPv4, can be re-used

➔Defense in depth

Home IPv6 Network - Summary

As mentioned, lessons learned from IPv4, can be re-used

- ➔Defense in depth
- ➔Patching

Home IPv6 Network - Summary

As mentioned, lessons learned from IPv4, can be re-used

- Defense in depth
- Patching
- Sane Configuration Management

Home IPv6 Network - Summary

As mentioned, lessons learned from IPv4, can be re-used

- ➔Defense in depth
- ➔Patching
- ➔Sane Configuration Management
- ➔Access Control

Home IPv6 Network - Summary

As mentioned, lessons learned from IPv4, can be re-used

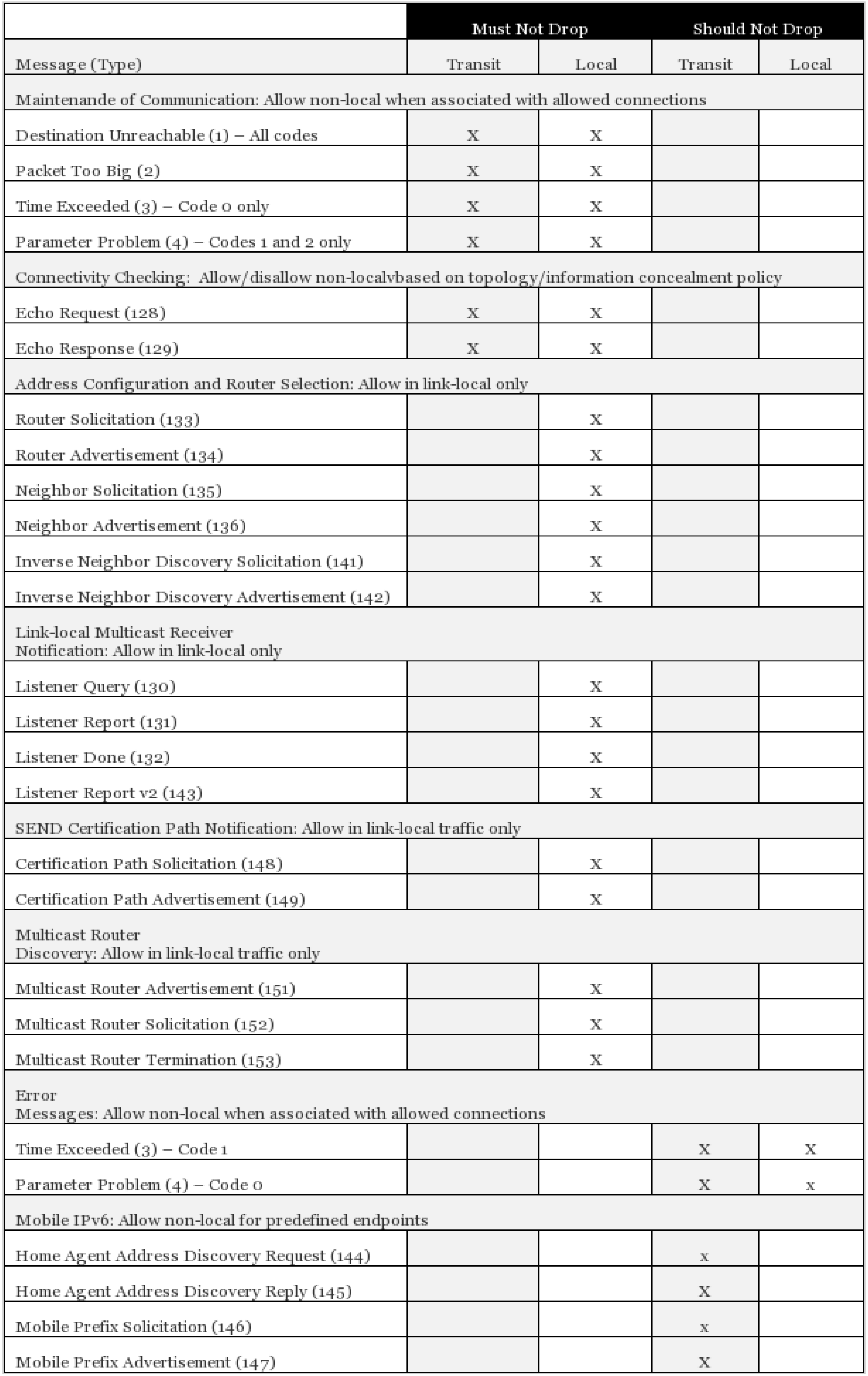
- Defense in depth
- Patching
- Sane Configuration Management
- Access Control
- Frequent revision of security policies

References / Further Reading

- IPv6 Security (Theory vs Practice) – Merike Kaeo www.doubleshotsecurity.com
- IPv6 Routing Header Security - Philippe Biondi, Arnaud Ebalard
- Guidelines for the Secure Deployment of IPv6 – NIST Special Publication 800-119
- SeND - http://tools.ietf.org/html/rfc3971
- Rogue RAs - http://tools.ietf.org/html/rfc6104
- RA Guard - http://tools.ietf.org/html/rfc6105
- Simple Security for IPv6 CPEs - http://tools.ietf.org/html/rfc6092
- Privacy Extensions for SLAAC in IPv6 - http://tools.ietf.org/html/rfc4941
- IPv6 Implications for Network Scanning - http://tools.ietf.org/html/rfc5157
- Filtering ICMPv6 in Firewalls - http://tools.ietf.org/html/rfc4890
- Routing Loop Attack w/ auto Ipv6 Tunnels -

  http://tools.ietf.org/search/draft-ietf-v6ops-tunnel-loops-07

Appendix I – ICMPv6 Filtering



	Must Not Drop		Should Not Drop	
Message (Type)	Transit	Local	Transit	Local
Maintenande of Communication: Allow non-local when associated with allowed connections				
Destination Unreachable (1) – All codes	X	X		
Packet Too Big (2)	X	X		
Time Exceeded (3) – Code 0 only	X	X		
Parameter Problem (4) – Codes 1 and 2 only	X	X		
Connectivity Checking: Allow/disallow non-localvbased on topology/information concealment policy				
Echo Request (128)	X	X		
Echo Response (129)	X	X		
Address Configuration and Router Selection: Allow in link-local only				
Router Solicitation (133)		X		
Router Advertisement (134)		X		
Neighbor Solicitation (135)		X		
Neighbor Advertisement (136)		X		
Inverse Neighbor Discovery Solicitation (141)		X		
Inverse Neighbor Discovery Advertisement (142)		X		
Link-local Multicast Receiver Notification: Allow in link-local only				
Listener Query (130)		X		
Listener Report (131)		X		
Listener Done (132)		X		
Listener Report v2 (143)		X		
SEND Certification Path Notification: Allow in link-local traffic only				
Certification Path Solicitation (148)		X		
Certification Path Advertisement (149)		X		
Multicast Router Discovery: Allow in link-local traffic only				
Multicast Router Advertisement (151)		X		
Multicast Router Solicitation (152)		X		
Multicast Router Termination (153)		X		
Error Messages: Allow non-local when associated with allowed connections				
Time Exceeded (3) – Code 1			X	X
Parameter Problem (4) – Code 0			X	x
Mobile IPv6: Allow non-local for predefined endpoints				
Home Agent Address Discovery Request (144)			x	
Home Agent Address Discovery Reply (145)			X	
Mobile Prefix Solicitation (146)			x	
Mobile Prefix Advertisement (147)			X	

http://ipv6.ote.gr
http://twitter.com/oteipv6
ipv6@otenet.gr