



Security issues with Neighbor Discovery

From an attacker point of view, IPv6 attacks are:

- **Difficult** from remote network:
 - Scanning IPv6 network is hard (2^{64} addresses)
 - use random IID instead of MAC-based IID
 - No broadcast address
 - Remote attacks will target hosts exposed in DNS
- **Easy** from local network:
 - Neighbor Discovery is not (yet) secured
 - Attacks inspired by ARP flaws + new attacks
 - Implementations not (yet) heavily tested

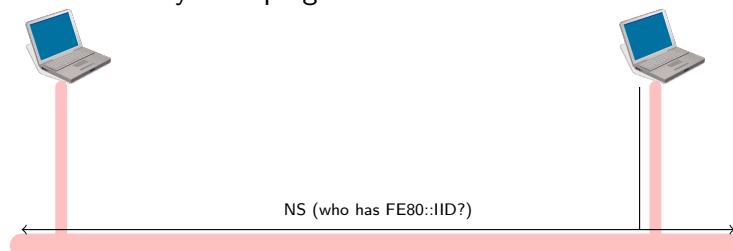
Attacker toolkits already available !

See <http://www.thc.org/thc-ipv6/>



Examples of attacks using ND

Neighbor Discovery Snooping



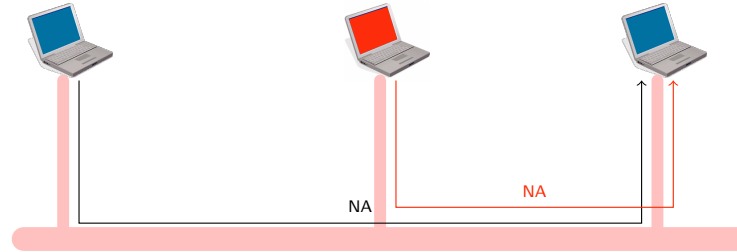
Host use Neighbor discovery for two cases :

- To get MAC address of another host (ARP-like)
- To verify address uniqueness (DAD)



Examples of attacks using ND

Neighbor Discovery Snooping



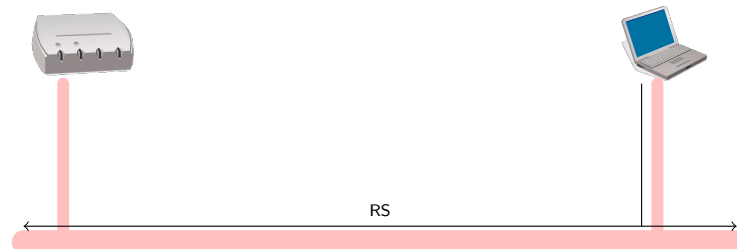
An attacker on the LAN can perform attack by responding to ND messages

- ARP-like: Pretend to be any host on the LAN => **Man in the Middle**
- DAD: Pretend to have any address on the LAN => **Deny of Service**



Examples of attacks using ND

Rogue router

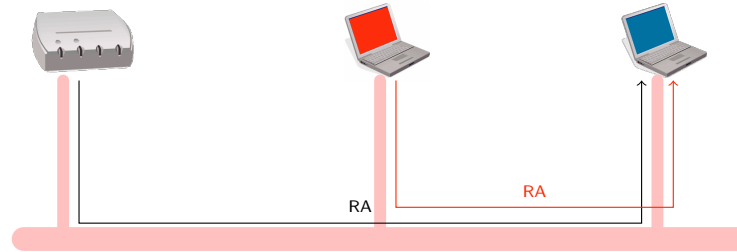


Host use Router Solicitation to get address of the exit router and prefix used on the LAN.



Examples of attacks using ND

Rogue router



An attacker on the LAN can perform attack by responding to RS messages

- Pretend to be the exit router => **Man in the Middle**
- Pretend to route another prefix on the LAN => **Deny of Service**



Solutions to reduce or prevent attacks ?

Prevention of attacks:

- SEND (Secure Neighbor Discovery)
 - IETF solution (Work in Progress)
 - Use signed ND messages, with a trust relationship
- Level-2 Filtering
 - Filter ND on switch port (ex. only one port allowed to send RA)
 - A few switch still implements it ... (Cisco ?)

Detection of attacks: ndpmon

- Similar to ARP-watch
- Detect Snooping and Denial of Services
- <http://ndpmon.sf.net>



SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key



issuer: router1.test.g6.asso.fr
prefix: R1,...,Rn
subject: test.g6.asso.fr
public key: public
hash: *private*_{test.g6.asso.fr}(certif)



issuer: g6.asso.fr
prefix: P1,...,Pn
subject: g6.asso.fr
public key: public
hash: *private*_{g6.asso.fr}(certif)



SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key



issuer: router1.test.g6.asso.fr
prefix: R1,...,Rn
subject: test.g6.asso.fr
public key: public
hash: *private*_{test.g6.asso.fr}(certif)



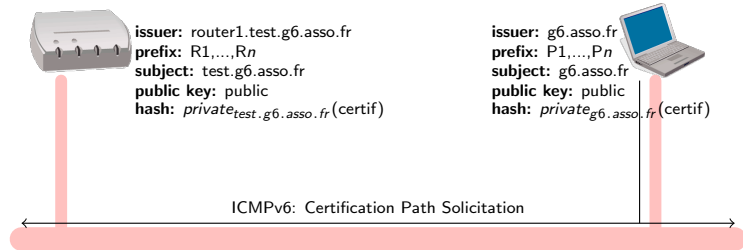
issuer: g6.asso.fr
prefix: P1,...,Pn
subject: g6.asso.fr
public key: public
hash: *private*_{g6.asso.fr}(certif)

ICMPv6: Certification Path Solicitation



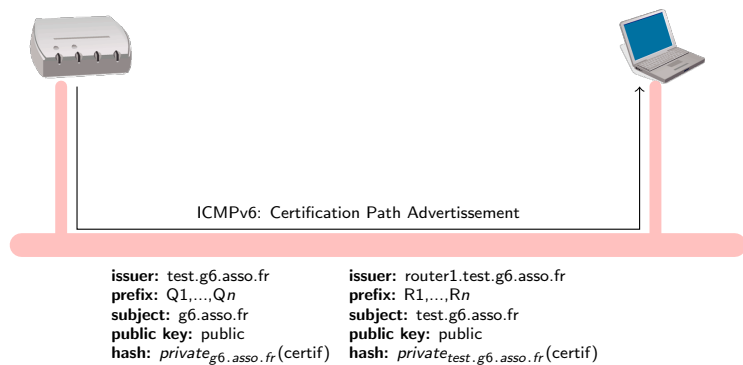
SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key



SEND (RFC 3971)

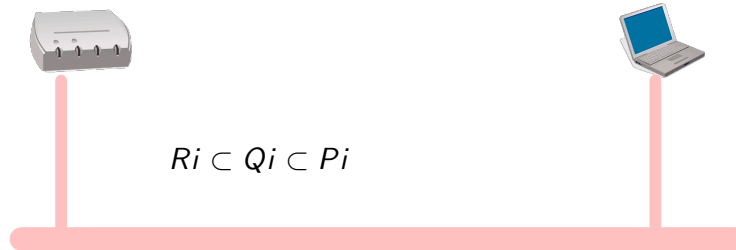
- Sign prefixes with a certificate
- IID is derived from the certificate public key





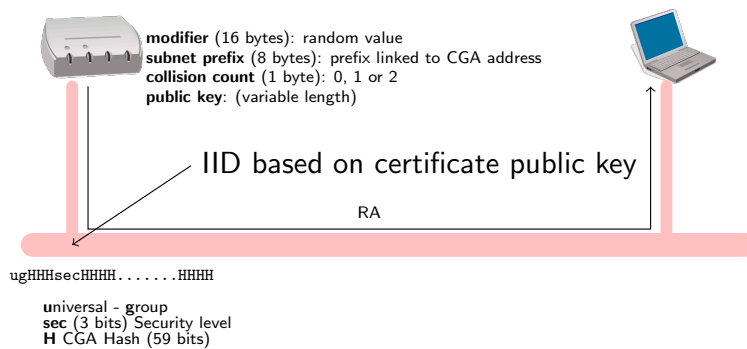
SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key



SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key

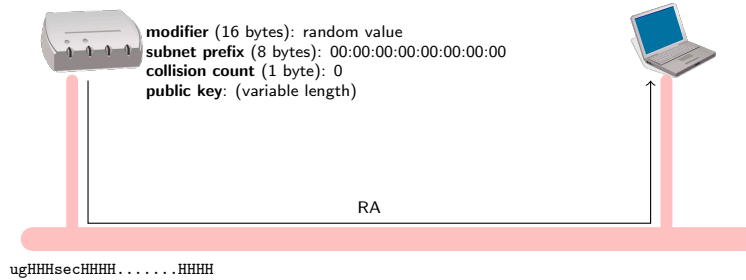


59 bits in IID could be too small in the futur



SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key

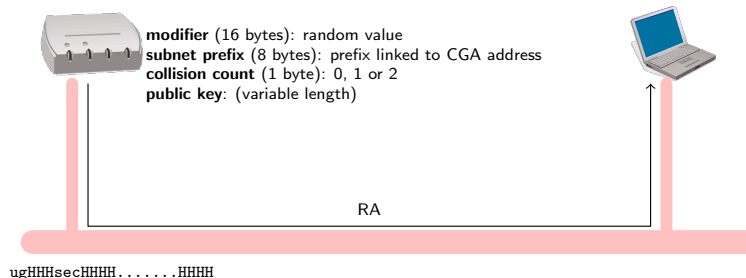


First step: set prefix and collision count to 0
find modifier so SHA-1 hash starts with 2 * sec bytes to 0



SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key

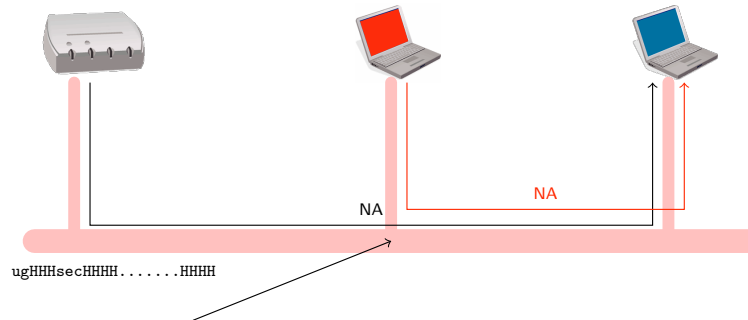


Second step: compute SHA-1 hash with all fields
IID = 64 leftmost bits of the SHA-1



SEND (RFC 3971)

- Sign prefixes with a certificate
- IID is derived from the certificate public key



IID incorrect or wrong certificate



New options

- New options have been defined for RA:
 - CGA option:
 - public key
 - modifier
 - subnet prefix
 - collision count
 - Nonce: random number used only once to avoid replay attacks
 - Timestamp: to limit announcement period
 - RSA Signature:
 - key hash
 - Digital signature: IPv6 source and dest. addresses, ICMPv6 type, code checksum, ND options, SEND options.



SEND pros and cons

- Pros
 - only router with the appropriate certificate can announce valuable prefixes
- Cons
 - Hash calculation can be complex => DoS
 - Hosts must be configured with initial certificate
 - if too generic any router will be accepted
 - if too restrictive, no mobility inside the company network
 - Clock must be synchronized to accept SEND messages
 - NTP cannot be used, GPS ?



Solutions in a closed environment

- Link Layer is protected either physically or by cryptographic
- Attacks/Misconfiguration comes from inside
 - Misconfiguration is more important to solve than attacks
 - Attacks are almost the same than in IPv4
 - Auto-configuration leads to catastrophic behavior in case of misconfiguration
- Auto-configuration looks more dangerous than in IPv4:
 - A centralized DHCPv4 server allows IPv4 addresses allocation
 - Does not avoid to forge a IPv4 address
- Authentication has not to be done at IPv6 level
 - IEEE 802.1X, IEEE 802.11i (WPA), PANA authenticates users, not MAC addresses
 - If allowed them auto-configuration.

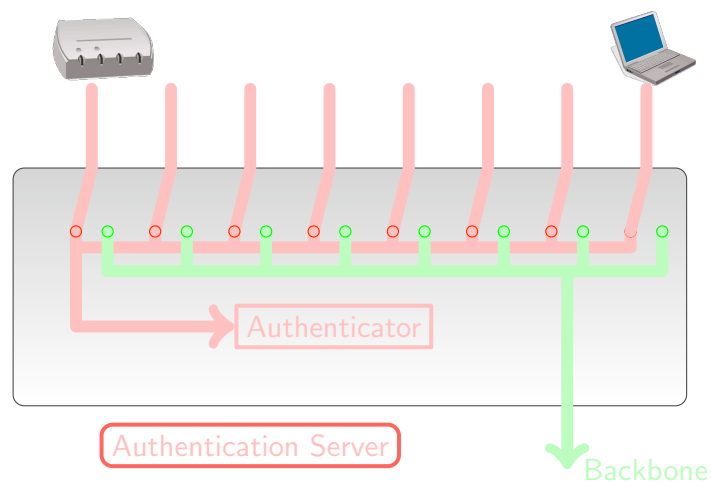


NDP filtering

- Switches should understand IPv6
 - MLD Snooping (like IGMP snooping)
 - Only port assigned to routers may send RA
 - More complex than in IPv4
 - No Layer 2 type for NDP, IPv6|ICMPv6|RA
 - With extensions, information may be at different places
 - Should be able to register IPv6 addresses per port
 - To monitor network
- This can also be done in IEEE 802.11 architecture
 - Only specific MAC addresses can send RA
 - MAC address can be spoofed
 - No Wep
 - WPA
 - Do not work in ad hoc mode

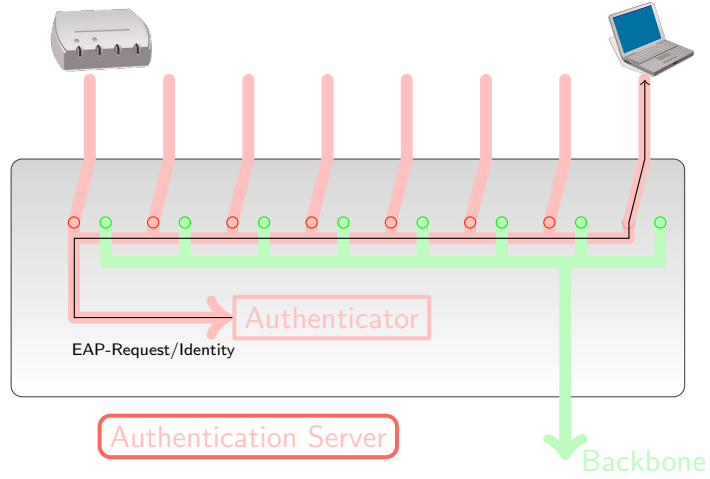


IEEE 802.1X

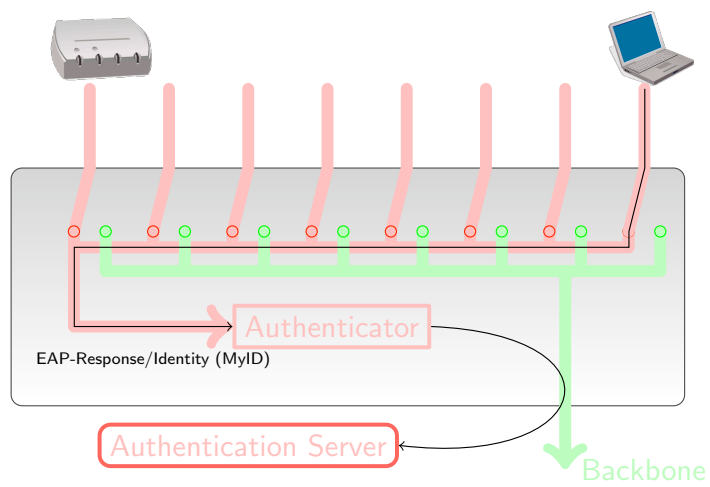




IEEE 802.1X

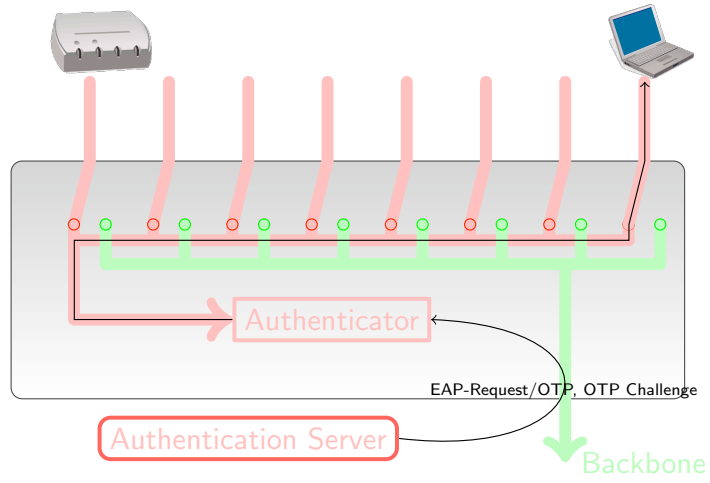


IEEE 802.1X

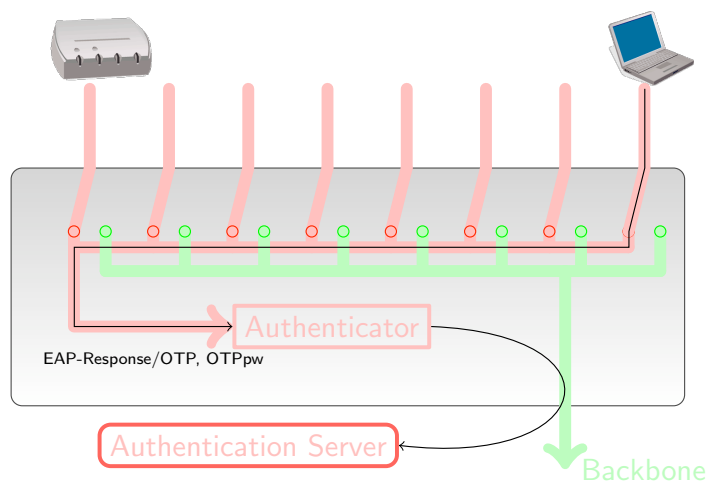




IEEE 802.1X

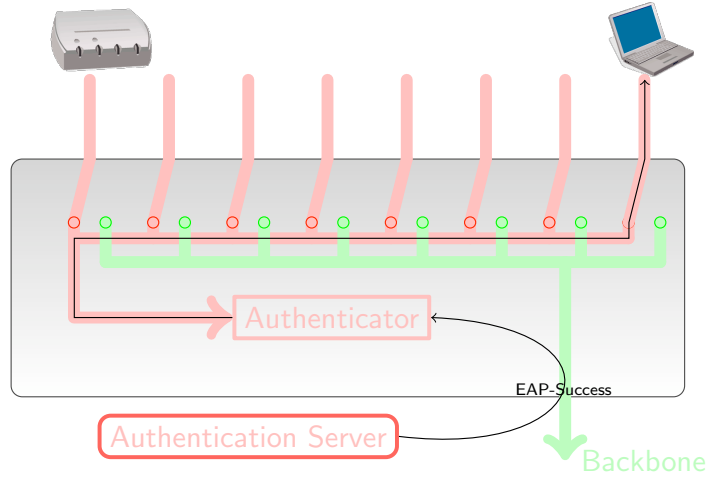


IEEE 802.1X

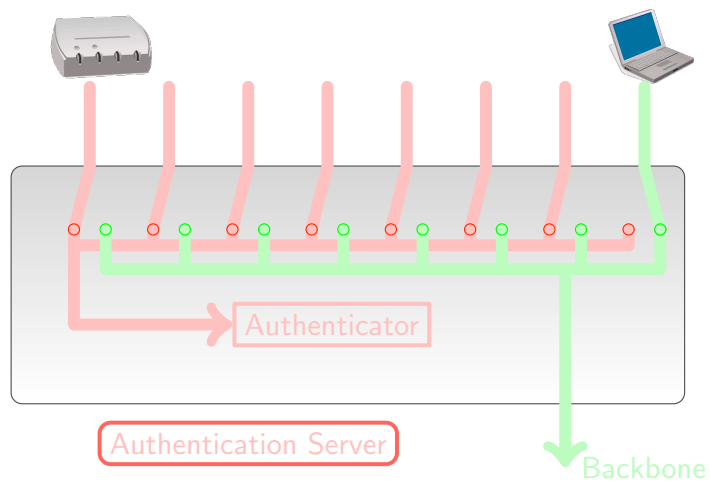




IEEE 802.1X

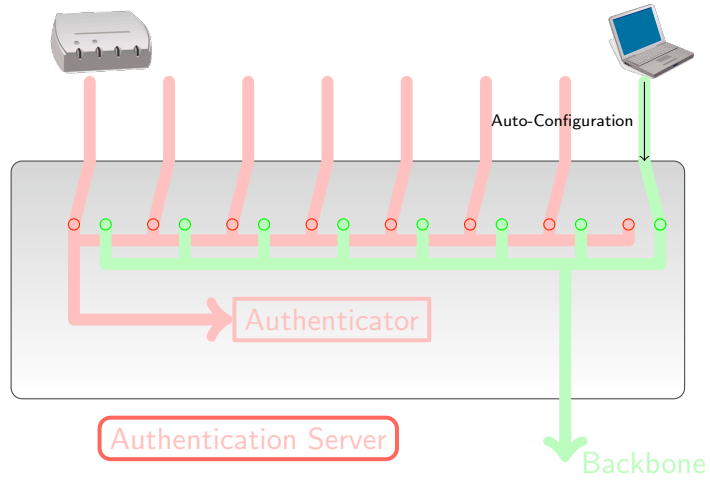


IEEE 802.1X





IEEE 802.1X



IPv6 and Firewalls



Concept of firewalling

- What is a firewall: a border equipment between different policy areas
- What are the roles of a firewall ?
 - Filter packets according rules
 - Alter packets (i.e. NAT)
 - Route packets between policy areas (in/out/DMZ)
- What does IPv6 change ?
 - New rules to filter IPv6
 - Need of NAT in IPv6 not yet identified
 - Routing should handle IPv6



IPv6 Filtering rules: Address scope

- Need to filter invalid scopes of addresses
- See `draft-ietf-v6ops-rfc3330-for-ipv6-03.txt`
- What should be filtered as source/destination :
 - Link-local Unicast (`fe80::/10`)
 - Host-scoped addresses (`::1`)
 - Host,Link,Site-local multicast as source/destination and global multicast as source
 - ULA addresses (in site border)
 - IPv4 compatible/mapped addresses



IPv6 Filtering rules: Other principles

- ICMP is no more harmful (see RFC4890)
 - Network scan is improbable
 - ICMPv6 is needed (Path MTU disc, Error reporting)
- IPv6 extensions need to be considered
 - Should be allowed: Fragmentation, IPSec
 - Should be considered with care : Hop-by-Hop, Destination (IPv6 Mobility), Routing
- Stateful rules are needed for a NAT-like filtering
- Beware of tunnels (6to4, Teredo) that can be backdoors



IPv6 Filtering rules: Application Headers

- Filter needs to inspect Application header (HTTP, SIP, etc.)
- IPv6 addresses may be present inside these headers (cf. SIP)
- Requirements:
 - Firewall need to handle presence of these IPv6 addresses
 - Filter need to check validity of these addresses (scope, etc.)



Routing between policy areas

- IPv6 introduces a second topology to manage
- Policy areas should be coherent between IPv4 and IPv6
 - A host should be placed in the same policy area in IPv4 and IPv6
- IPv4 and IPv6 rules should be coherent in the same policy area
 - Same access restriction should apply in both IPv4 and IPv6



IPv6 Firewalls implementations

Implementation	IPv6 Support	Stateful Filter	Extension support
pf (*BSD)	X	X	X
iptables (Linux)	X	X	X
MS Vista	X	X	X
Cisco PIX/ASA	X	X	?
Cisco ACL	X	X	?
Juniper ScreenOS	X	X	?
CheckPoint	X	X	?