IPv6 Addressing Security and Privacy



Piotr Wojciechowski (CCIE #25543)
Senior Network Consultant
Kraków, May 26, 2010

A little about me :)

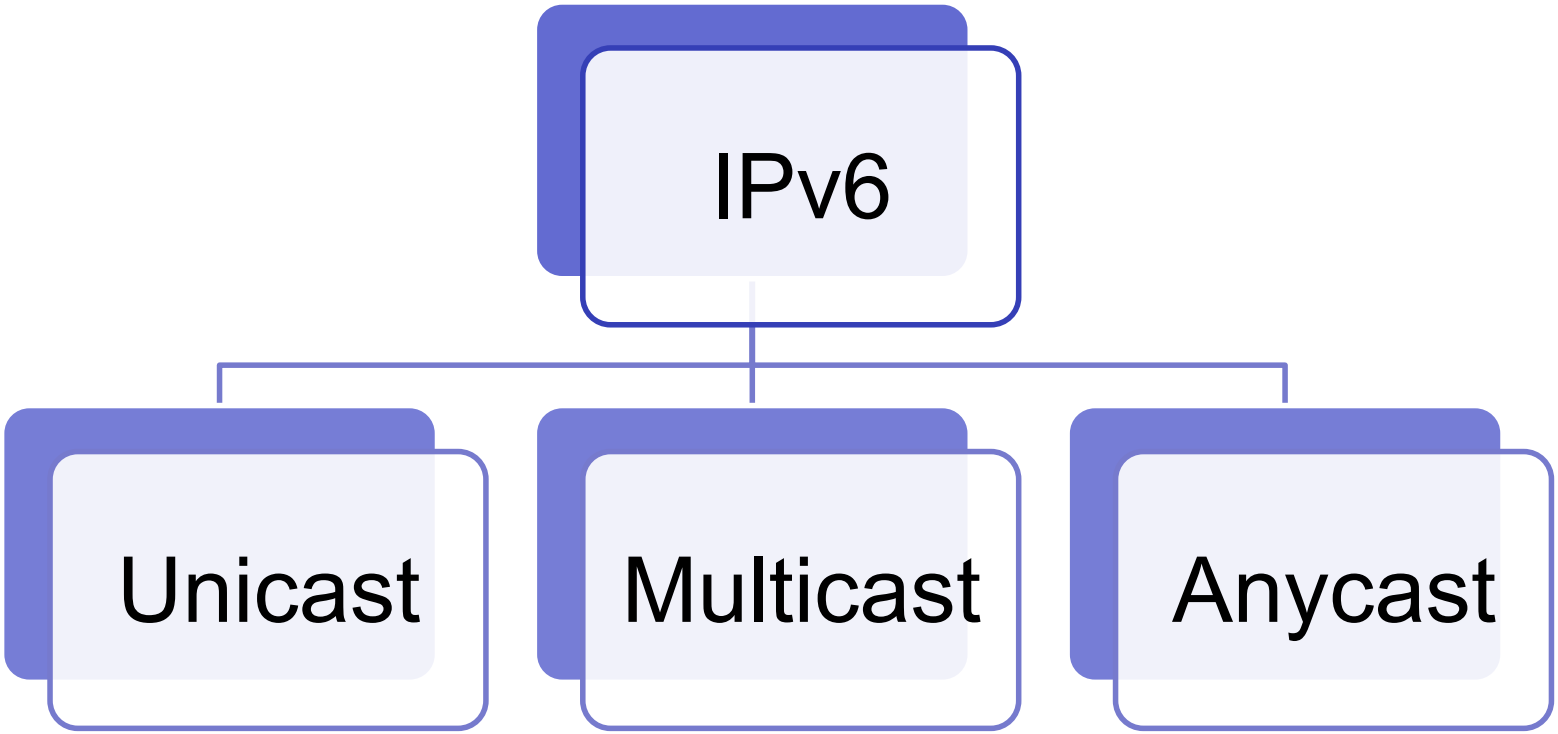
ATM SI

- Currently working as Senior Network Consultant at ATM Systemy Informatyczne
- Contributing editor at *LinuxPlus*, *Chip*, *Chip Special*, currently at *IT w Administracji* (*IT in Public Sector*)
- Admin of CCIE.PL board

Agenda

- Address assignment in IPv6 overview
- Stateless Address Autoconfiguraton (SLAAC)
- Duplicate Address Detection
- ICMPv6 Protocol Protection
- IPv6 Autoconfiguration Privacy Issues

IPv6 address types



Network Discovery Protocol

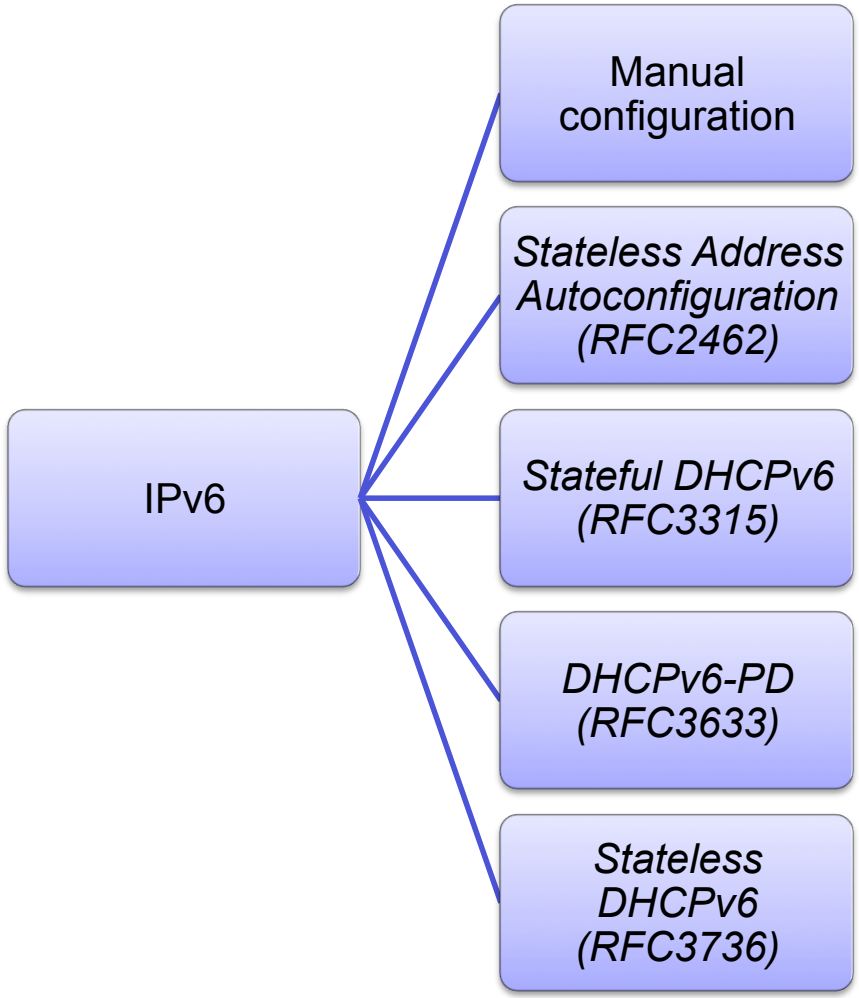
- Operates at Link Layer
- Similar functions as ARP+ICMP Router Discovery+ICMP Router Redirect from IPv4
- Uses ICMPv6 protocol, where it defines five different packet types:
  - Router Solicitation
  - Router Advertisement
  - Neighbor Solicitation
  - Neighbor Advertisement
  - Redirect

ICMPv4 vs. ICMPv6

ATM SI

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational and Error Massaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Multicast Group Management		X
Mobile IPv6 Support		X

IPv6 address assignment



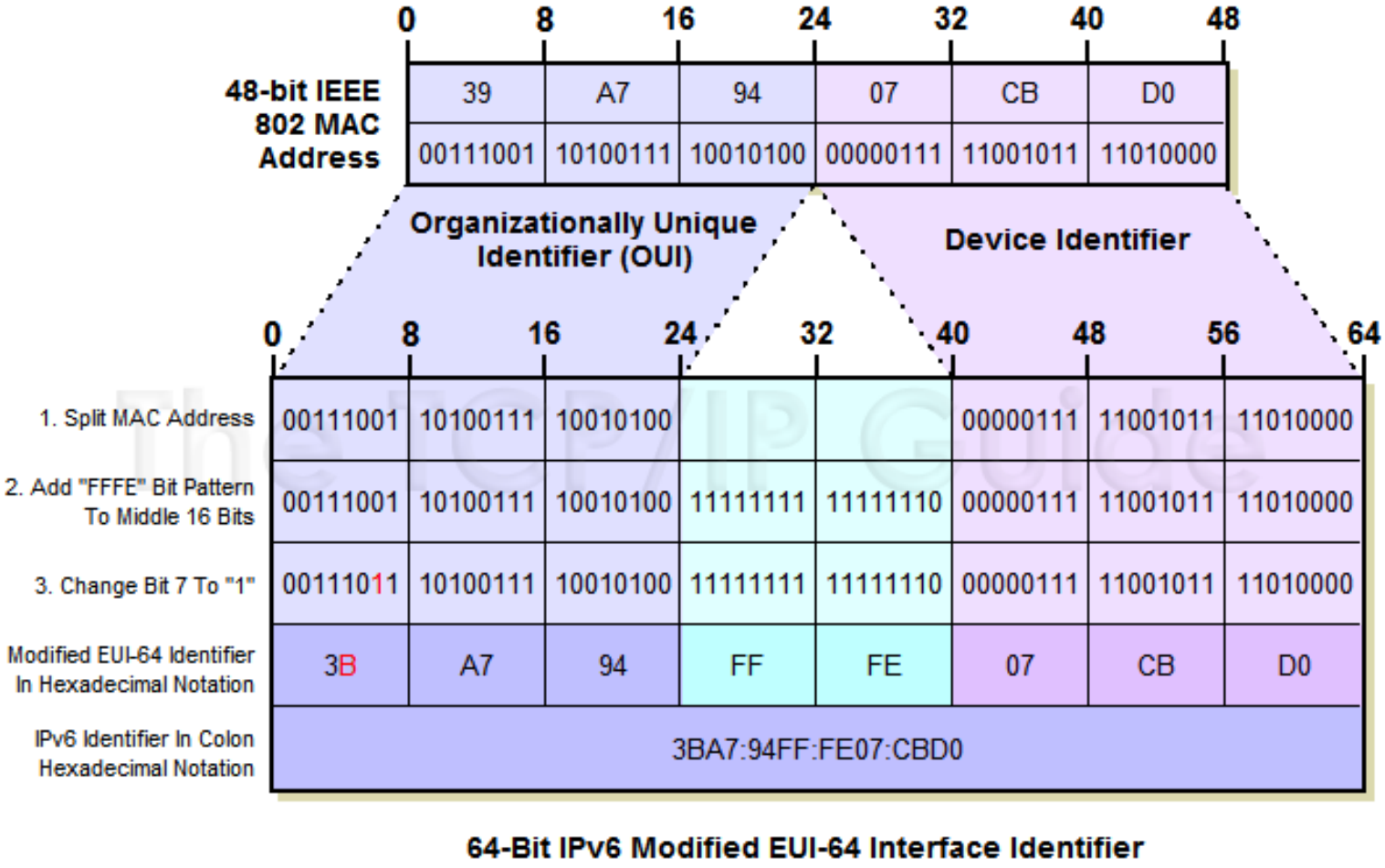
Agenda

- Address assignment in IPv6 overview
- **Stateless Address Autoconfiguraton (SLAAC)**
- Duplicate Address Detection
- ICMPv6 Protocol Protection
- IPv6 Autoconfiguration Privacy Issues

IPv6 Address Assignment
Stateless Address Autoconfiguration (RFC2462)

- Also known as SLAAC
- Easiest of the methods – administrator don't have to do anything on end device, just simple configuration on router
- End device gets it's IPv6 address basing on MAC address of interface, which is converted into EUI-64 identifier
- End devices configure it's IPv6 address and set router's link-local address as their default gateway.

IPv6 Address Assignment
EUI-64



Source: www.tcpipguide.com/free/diagrams/ipv6eui64.png

IPv6 address assignment
Stateless Address Autoconfiguration (RFC2462)

ATM SI

- Router Advertisement contains:
  - Local prefix – first 64-bits of IPv6 address
  - Router link-layer address
  - Lifetime
  - Priority
  - Additional flags – M and O
  - MTU

IPv6 address assignment
Stateless Address Autoconfiguration (RFC2462)

1

Router Solicitation (RS) – ICMPv6 133
Src: link-local
Dst: FF02::2 (All routers)

2

Router Advertisement (RA) – ICMPv6 134
Src: link-local
Dst: FF02::1 (All hosts)

Prefix = 2001::/64
Lifetime (valid and preferred)
Default router = link-local address
O and M bits

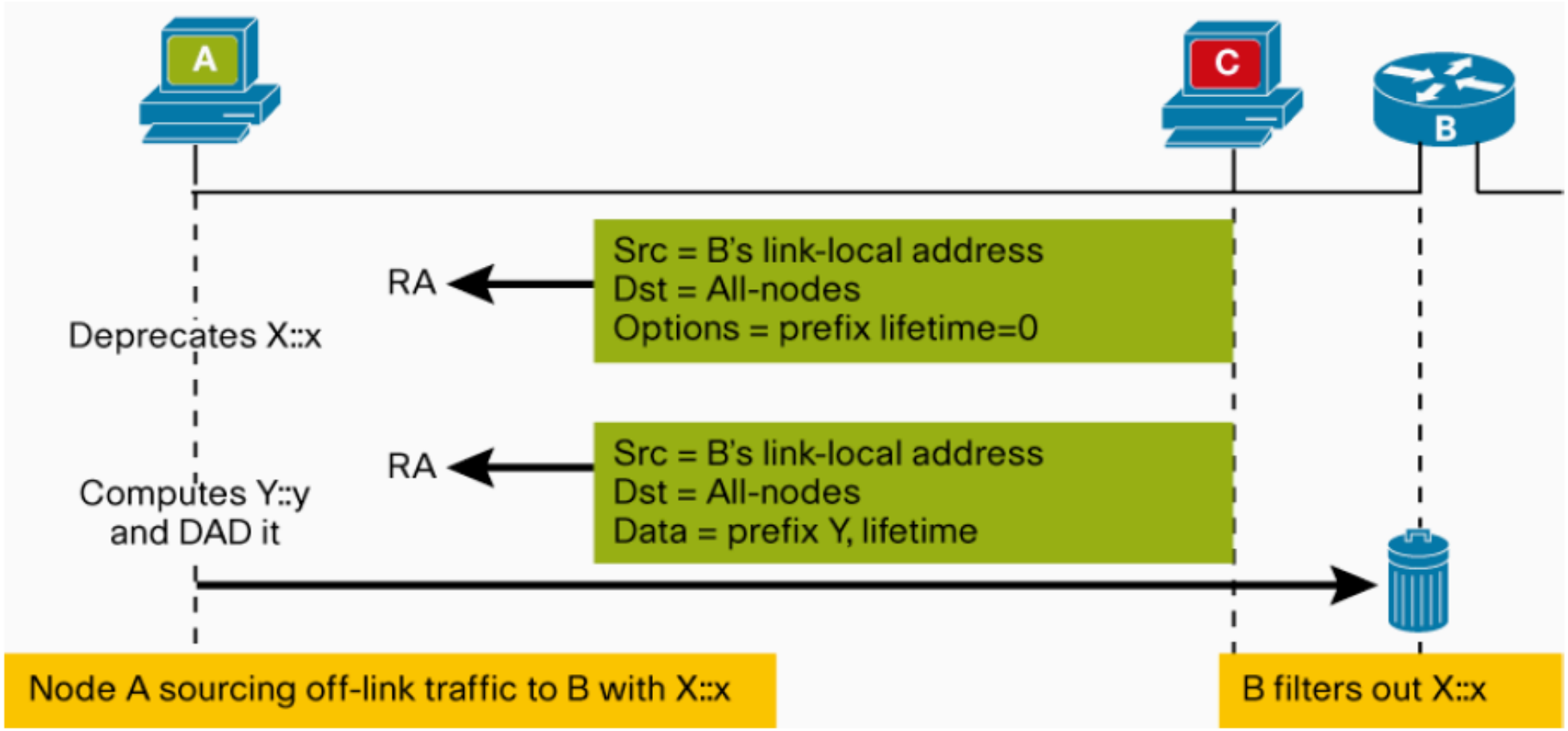
IPv6 address assignment
Stateless Address Autoconfiguration (RFC2462)

ATM SI

- Why it's easy to perform attack against SLAAC:
  - Malicious user can send rogue RA due to no authentication built-in into protocol – easy way to perform DoS or Man-in-the-Middle attack
  - This can even not be an attack – inexperienced administrator can misconfigure SLAAC on his host

- This can lead to Man-In-The-Middle attack

IPv6 address assignment
Stateless Address Autoconfiguration (RFC2462)



Source: IPv6 Secure Neighbor Discovery: Protecting Your IPv6 Layer 2 Access Network, Cisco.com

Agenda

- Address assignment in IPv6 overview
- Stateless Address Autoconfiguraton (SLAAC)
- **Duplicate Address Detection**
- ICMPv6 Protocol Protection
- IPv6 Autoconfiguration Privacy Issues

Duplicate Address Detection (DAD)

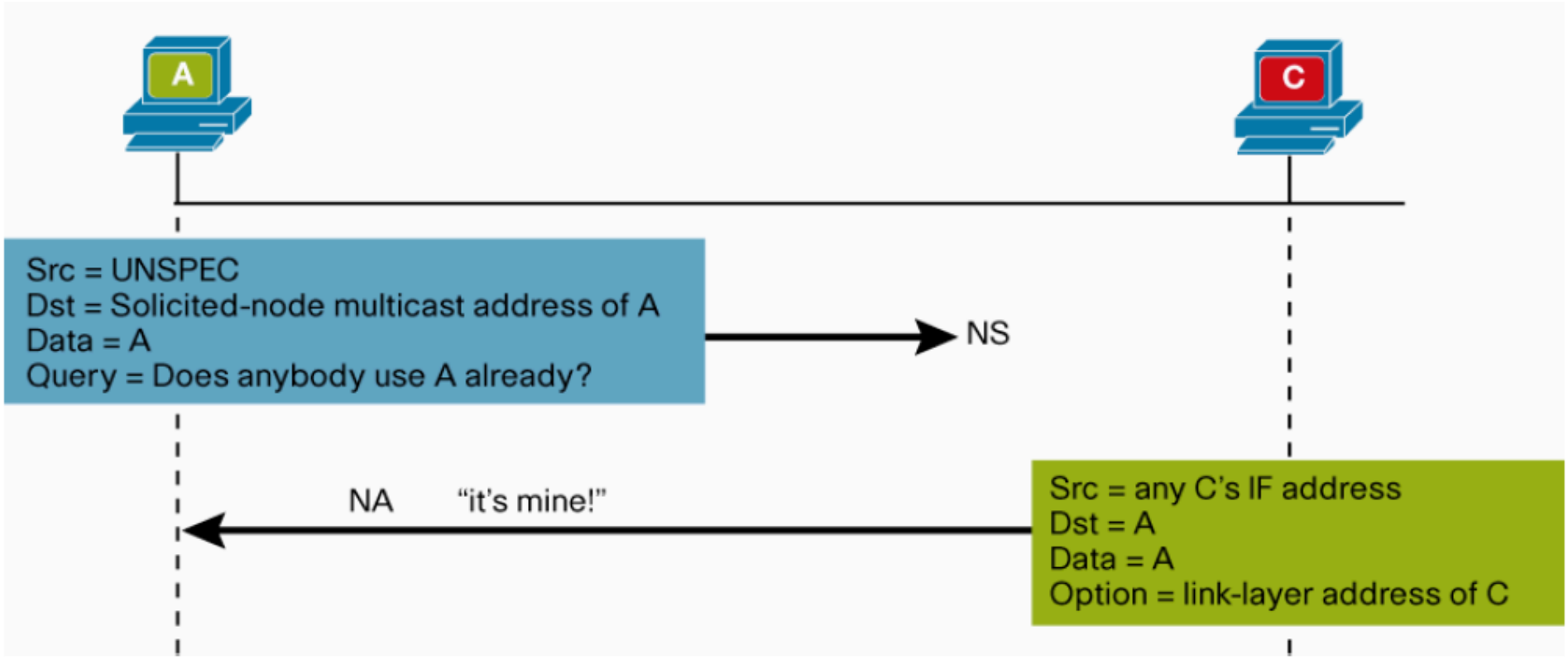
- With SLAAC host have to check if his IPv6 is not already used on the network segment by another node
- DAD is executed before host use IPv6 address including link-local address
- Neighbor Solicitation messages are used – in normal operation host should never hear reply for sent query
- No authentication of messages is used

Duplicate Address Detection (DAD)
DoS attack scenario

ATM SI

- Attacker can reply to every NS query he receives and pretend to own all IPv6 addresses on the segment
- This will results in DoS attack – no host can assign new IPv6 address anymore
- Hosts with addresses already assigned will loose them when their lifetime specified in RA message expire

Duplicate Address Detection (DAD)
DoS Attack Scenario



Source: IPv6 Secure Neighbor Discovery: Protecting Your IPv6 Layer 2 Access Network, Cisco.com

Agenda

- Address assignment in IPv6 overview
- Stateless Address Autoconfiguraton (SLAAC)
- Duplicate Address Detection
- **ICMPv6 Protocol Protection**
- IPv6 Autoconfiguration Privacy Issues

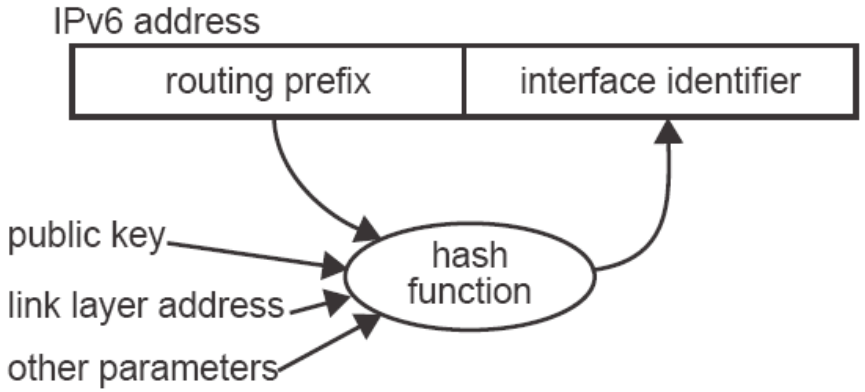
ICMPv6 Protocol Protection

ATM SI

- ICMPv6 have following security built-in mechanisms:
  - Source address must be link-local or unspecified (::/128) for RA and NS messages
  - Hop limit have to be set as 255
- This prevents before attacks being sent from other network segment
- There is no mechanism defined in ICMPv6 RFC's that would protect against local attacker

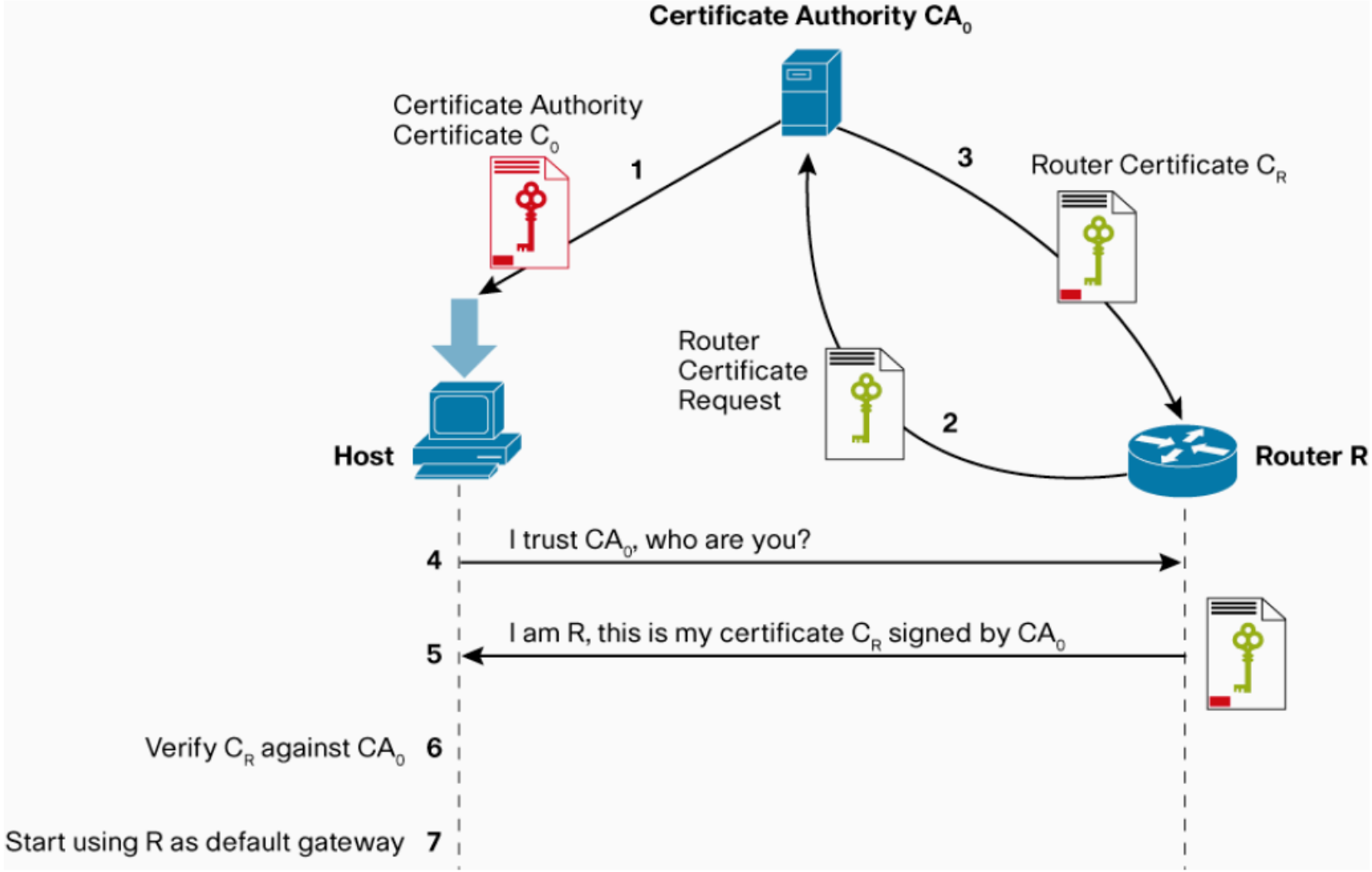
ICMPv6 Protocol Protection
SEcure Neighbor Discovery (SEND) – RFC 3971

- Defined in 2005, three deployment models available
- ND message is extended by few options
- Pair of keys exists for every IPv6 node
- Host cannot create interface identifier portion of IPv6 address using EUI-64 algorithm
- Interface identifier is cryptographically generated basing on subnet prefix, public key and modifier using SHA-1 hash algorithm



Source: Implementing IPv6 Secure Neighbor Discovery, Cisco.com

ICMPv6 Protocol Protection
SEcure Neighbor Discovery (SEND) – RFC 3971



Source: Implementing IPv6 Secure Neighbor Discovery, Cisco.com

ICMPv6 Protocol Protection
SEcure Neighbor Discovery (SEND) – RFC 3971

ATM SI

```
crypto key generate rsa label SEND modulus 1024

ipv6 cga generate modifier rsakeypair SEND

interface GigabitEthernet0/0

ipv6 cga rsakeypair SEND

ipv6 address FE80::/64 cga

ipv6 address 2001:db8::/64 cga
```

ICMPv6 Protocol Protection
SEcure Neighbor Discovery (SEND) – RFC 3971

ATM SI

- On IOS routers support for SEND is already available with release 12.4(24)T
- Linux support is available
- Microsoft XP and Vista will never support SEND

- Using SEND produced new security thread – attacker can flood SEND-enabled host with ND packets forcing responder to process thousands of public key operations – it's CPU consuming

ICMPv6 Protocol Protection
Detecting Rogue RA Messages

ATM SI

- IDS with customized signatures that checks if RA message source MAC or IPv6 does not match the configured one – but we need that sensor on every network segment
- Deployment of public domain utility called NDPMon which analyzes all RA messages and checks their validity against an XML configuration file – it's an IDS software

ICMPv6 Protocol Protection
Detecting Rogue RA Messages

ATM SI

- Sending RA Messages with High priority – something that should be done by default!

```
interface GigabitEthernet0/0
 ipv6 nd router-preference High
```

- Won't prevent planned attack but might help with nonmalicious misconfigured IPv6 hosts.
- Mechanisms to mitigate those kind of attacks should be implemented on switches – support from vendors is required.

ICMPv6 Protocol Protection
Responding on Rogue RA Messages

ATM SI

- *Rafixd* and *ramond* are open-source tools
- Daemon is listening on RA Messages. If rogue message is detected application sends immediately another rogue message but with lifetime of 0 seconds to clear rogue information on all nodes
- This won't prevent an attack, but may reduce it's lifetime.

ICMPv6 Protocol Protection
Switch Security

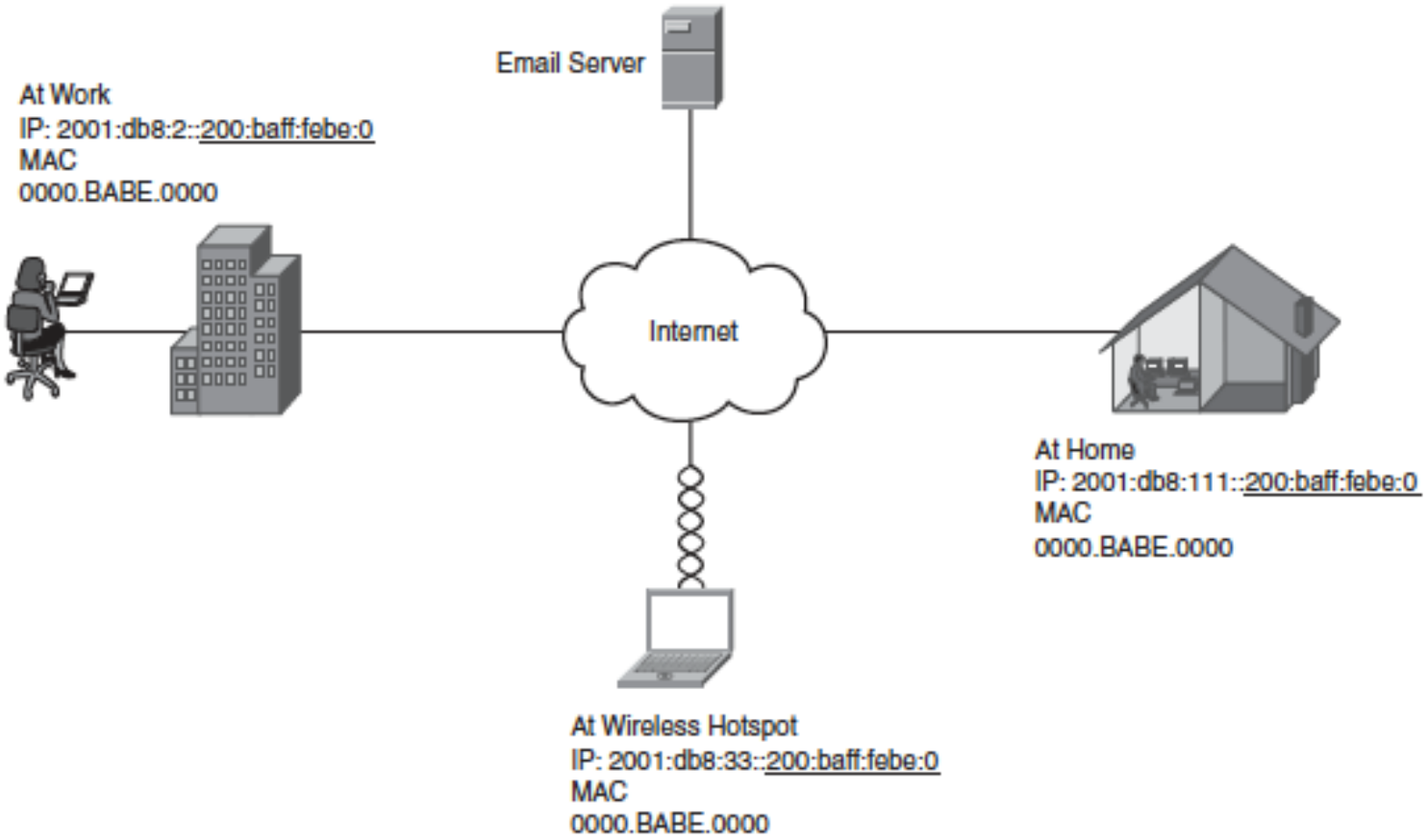
ATM SI

- Switches should implement set of security features similar to those known from IPv4:
  - **IPv6 VLAN ACL –** could be used to drop all RA Messages sent with wrong source MAC address
  - **IPv6 port ACL –** could be used to drop all RA Messages sent from a nontrusted port
  - **IPV6 RA Guard –** RA can be sent only on trusted ports
  - **DHCPv6 Snooping –** switch learns bindings between IPv6 and MAC addrtess
  - **Dynamic NA Inspection –** once mapping between IPv6 and MAC is known switch inspects NA and drops those that contains forged information

Agenda

- Address assignment in IPv6 overview
- Stateless Address Autoconfiguraton (SLAAC)
- Duplicate Address Detection
- ICMPv6 Protocol Protection
- **IPv6 Autoconfiguration Privacy Issues**

IPv6 – Privacy Issue with EUI-64 Address



Source: IPv6 Security, CiscoPress

IPv6 – Privacy Issue with EUI-64 Address

ATM SI

- Problem was described in 1999, in 2001 RFC 3041 “Privacy Extensions for Stateless Address Autoconfiguration in IPv6” has been released, updated by RFC 4941
- Solution to privacy problem – generate host-related portion of IPv6 address using MD5 hash with random number on EUI-64 address
- Probability close to 0 with two same IPv6 addresses in segment, but even if, we still have DAD.
- Hosts periodically change addresses, but usually keeps previous one to not break existing communication

IPv6 – Privacy Issue with EUI-64 Address

ATM SI

- By default Cisco routers does not use privacy extensions – why should they?
- Windows VP, Vista, 7 and several Linux distributions uses privacy extensions
- It can be disabled and many corporations actually do that – they said they have to do forensic investigation and track down IPv6 address

ATM SI

QUESTIONS?