Cisco.com

Are the security issues of IPv4 resolved with IPv6?

Franjo Majstor
EMEA Consulting Engineer
Cisco Systems, Inc.
fmajstor@cisco.com

Agenda

Cisco.com

- IPv6 Protocol Security
- IPv4 vs IPv6 Security
- MS Windows 2K/XP and IPv6
- Summary

IPv6 & Security

Cisco.com

- All implementations required to support authentication and encryption headers (AH and ESP of IPsec)
- Authentication separate from encryption for use in situations where encryption is prohibited or prohibitively expensive
- Key distribution protocols are under development (independent of IP v4/v6)
- Support for manual key configuration required

Authentication Header (AH)

Cisco.com

Next Header	Hdr Ext Len	Reserved
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data		

- Destination Address + SPI identifies security association state (key, lifetime, algorithm, etc.)
- Provides ***origin authentication***, ***data integrity*** and ***anti-replay protection*** for all fields of IPv6 packet that do not change en-route
- Default algorithms are MD5/SHA-1

Encapsulating Security Payload (ESP)

Cisco.com

Security Parameters Index (SPI)		
Sequence Number		
Payload		
Padding	Padding Length	Next Header
Authentication Data		

- Provides ***origin authentication***, ***data integrity***, ***anti-replay protection*** and ***confidentiality*** of the IPv6 packet payload
- Default algorithms are DES/3DES, MD-5,SHA-1

What else does IPv6 for Security?

Cisco.com

- **Security**
  - **Nothing IP4 doesn't do - IPsec runs in both and IPv6 *mandates* IPsec implementation.**
  - **Does a lot dynamically on L3 (via ICMP), hence remove part of L2 problems, right?**
  - **Supports "privacy" addressing scheme**
  - **Migration via dual stacks!**

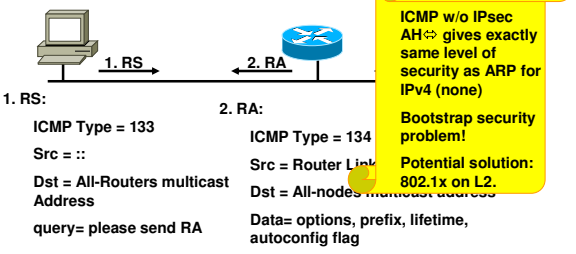
IPv6 Security Exposures…

Cisco.com

- **Autoconfiguration**
  - *stateless configuration and discovery, contradicting requirements with security*
- **ICMPv6 protected by IPsec**
  - *security bootstrap problem*
- **DAD**
  - *duplicate address detection mechanism*

Stateless autoconfiguration

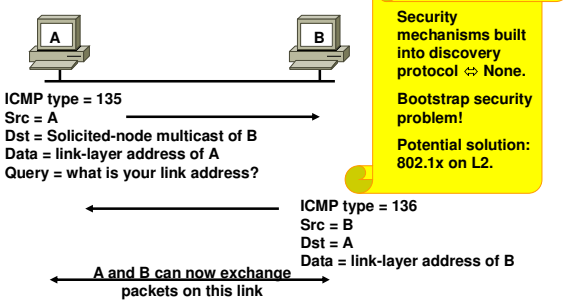
Cisco.com



Router solicitation are sent by booting nodes to request RAs for configuring the interfaces.

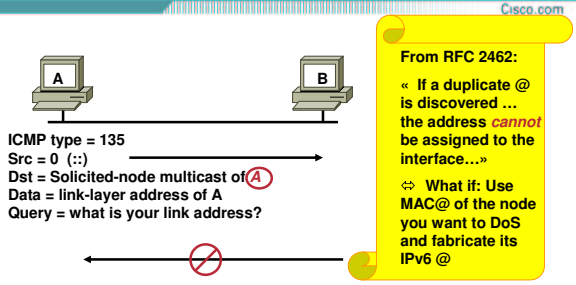
Neighbor Discovery - Neighbor Solicitation

Cisco.com



DAD (Duplicate Address Detection)

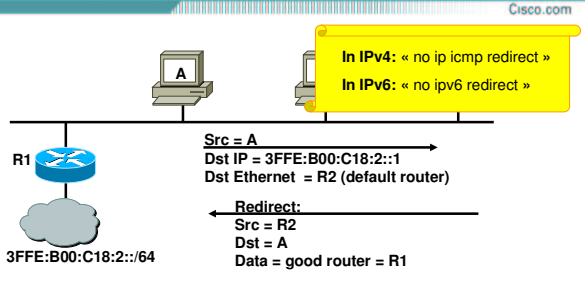
Cisco.com



- **Duplicate Address Detection (DAD) uses neighbor solicitation to verify the existence of an address to be configured.**

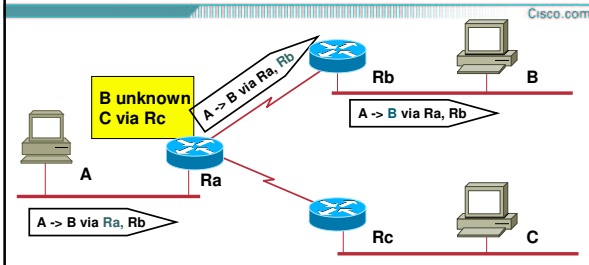
Neighbor Discovery - Redirect

Cisco.com



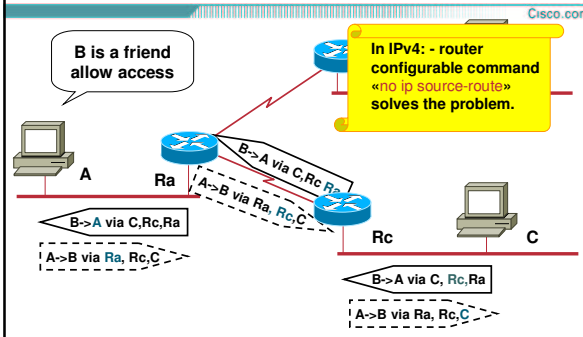
- **Redirect is used by a router to signal the reroute of a packet to a better router.**

IPv4: Source Routing Security Problem



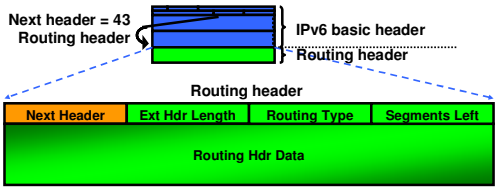
Routing based on IPv4 datagram option

IPv4 Spoofing Using Source Routing



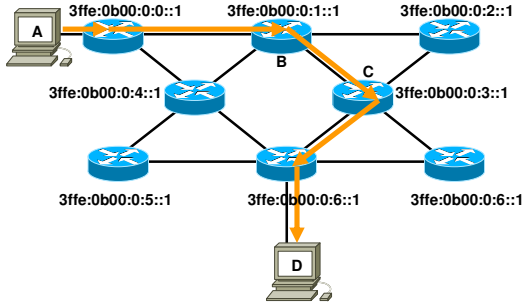
Back traffic uses the same source route

IPv6 Routing Header



- Routing header is:
  - An extension header.
  - Processed by the listed intermediate routers.

IPv6 Routing Header



- Routing type 0: Routers list = 3ffe:0b00:0:1::1, 3ffe:0b00:0:3::1

IPv6 Routing Header (cont.)

IPv6 header fields | Routing

	Src. Add.	Dest. Add.	Seg left	R a
A->B	A	B	2	
B->C	A	C	1	
C->D	A	D	0	

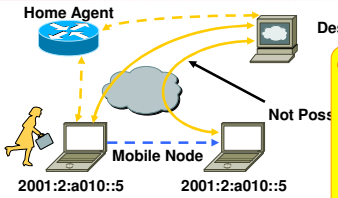
Packet flowing through the network

Routing header IPv6 ⇔ Source routing in IPv4

« Cannot be turned off (like 'no ip source-route' in IPv4) cause it is REQUIRED for mobile IPv6 !»

Solution: Use extended ACL (if mobile IPv6 not required)

Mobile IP - security still work in progress



Mobility and security elements of mobile IPv6 still work in progress… (MIPv6 draft 18/19 authentication).

- Mobility means:
  - Mobile devices are fully supported while moving
  - Built-in on IPv6
    - Any node can use it
  - Efficient routing means performance for end-users

IPv4 Normal Fragmentation/Reassembly

Cisco.com

Received from the network:

TL=500, FO=0	data length 480
TL=360, FO=960	data length 340
TL=500, FO=480	data length 480

Reassembly buffer, 65.535 bytes

Kernel memory at destination host

IPv4 Reassembly Attack

Cisco.com

Received from the network:

TL=1020, FO=0	data length 1000

… 64 IP fragments with data length 1000 …

TL=1020, FO=65000	data length 1000

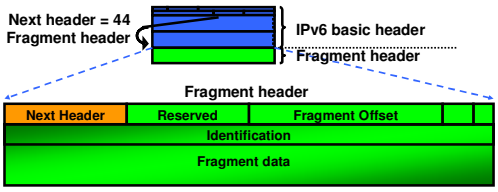
BUG: buffer exceeded

Reassembly buffer, 65.535 bytes

Kernel memory at destination host

Fragment Header - IPv6

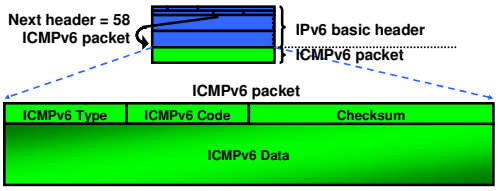
Cisco.com



- In IPv6 fragmentation is done *ONLY* by the end system
- Reassembly done by end system like in IPv4

ICMPv6

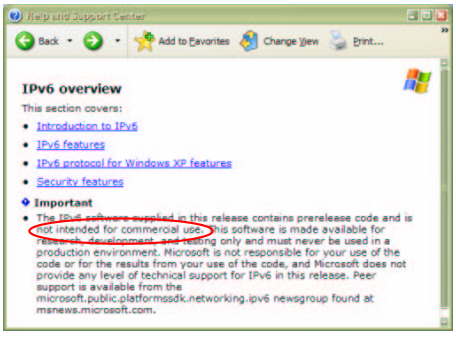
Cisco.com



- ICMPv6 is similar to IPv4:
  - Provides diagnostic and error messages
  - Is used for path MTU discovery
  - Runs *on top* of IPv6!

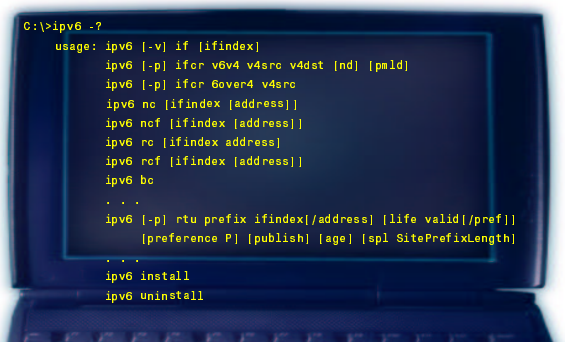
IPv6 protocol for MS WinXP *(DISCLAIMER!)*

Cisco.com



IPv6 & MS 2K/XP

Cisco.com



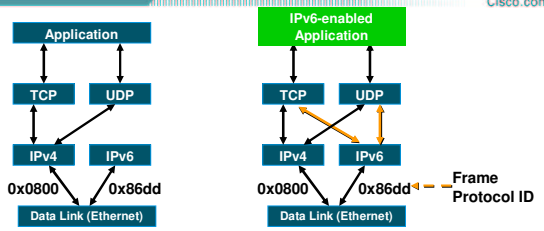
IPv6 protocol for Win XP/2K features

Cisco.com

- 6to4 tunneling *(RFC 3056)*
- ISATAP
  - *Intrasite Automatic Tunnel Addressing Protocol*
  - *(draft-ietf-ngtrans-isatap-00.txt)*
- 6over4 tunneling *(RFC 2529)*
- Anonymous addresses *(64-bit rnd)* [***privacy***]
- Site prefixes in router advertisements
- DNS support *(RFC 1886)*
- IPsec support *(AH-MD5, Null-ESP, ESP-MD5 auth*only*)* [***integrity***, ***auth***]
- Static router support *(ipv6 rtu)*
- Application support *(IExplorer, telnet, ftp, ping6, tracert6, RPC)*

IPv6/IPv4 Dual Stack Approach

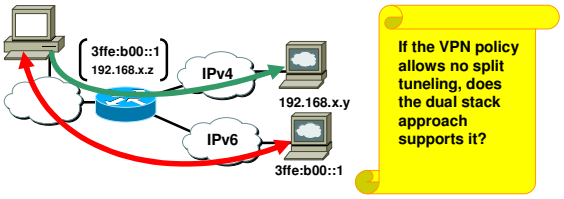
Cisco.com



- Dual stack node means:
  - Both IPv4 and IPv6 stacks enabled
  - Applications can talk to both
  - Choice of the IPv4 or IPv6 is based on name lookup and app. preference

Dual Stack Approach & VPN

Cisco.com



- In a dual stack case & VPN tunnel with non-split tunnelling policy:
  - All IPv4 traffic is non-split tunnelled through VPN tunnel
  - All IPv6 traffic is going out (and in) in the clear as a policy violation(?)

IPv6 vs. IPv4 Security Summary

Cisco.com

Service	*IPv4 Solution*	*IPv6 Solution*
Fragmentation	Router or end node can fragment	Only end nodes can fragment
Source routing	Could be disabled	Routing Hdr required for Mobile IPv6
ICMP Redirection	no ip icmp redirect	no ipv6 redirect
Duplicate addressing	No protection	No protection
Privacy	Layer 3	Layer 2-3
Integ/Auth/Confid.	IPsec	IPsec Mandated

Questions?

Cisco.com

Thank you!

Cisco.com

Are the security issues of IPv4 resolved with IPv6?

fmajstor@cisco.com


Cisco Systems
Empowering the
Internet Generation℠
www.cisco.com
31