2003
iSSE
INFORMATION SECURITY SOLUTIONS EUROPE

IPv6 Protocol

Does it solve all the security problems of IPv4?

Franjo Majstor

EMEA Consulting Engineer

fmajstor@cisco.com

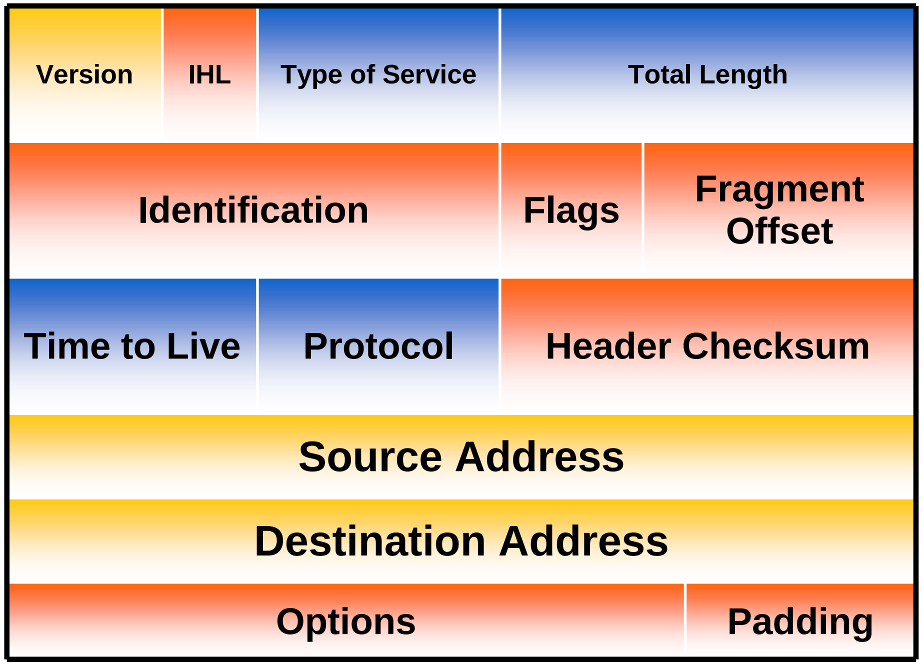
Cisco Systems, Inc.

Agenda

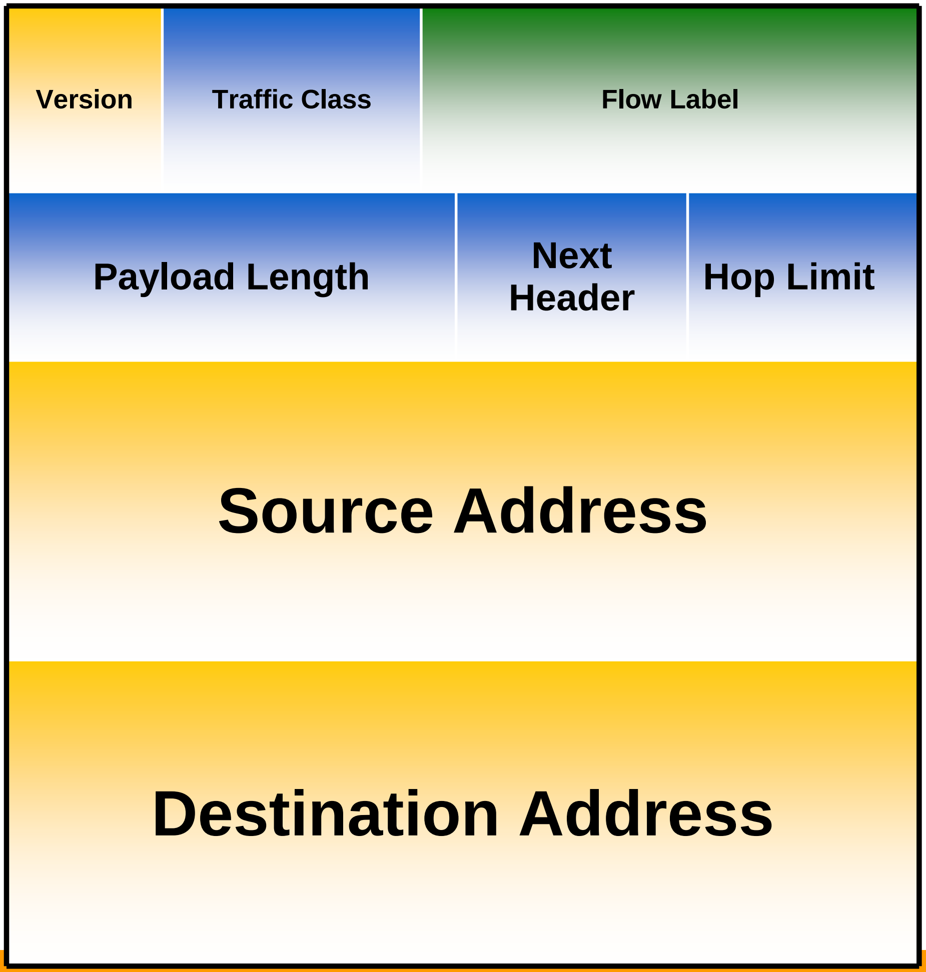
- IPv6 Primer
- IPv6 Protocol Security
- Dual stack approach
- Q&A

IPv4 & IPv6 Header Comparison

IPv4 Header



IPv6 Header



Legend

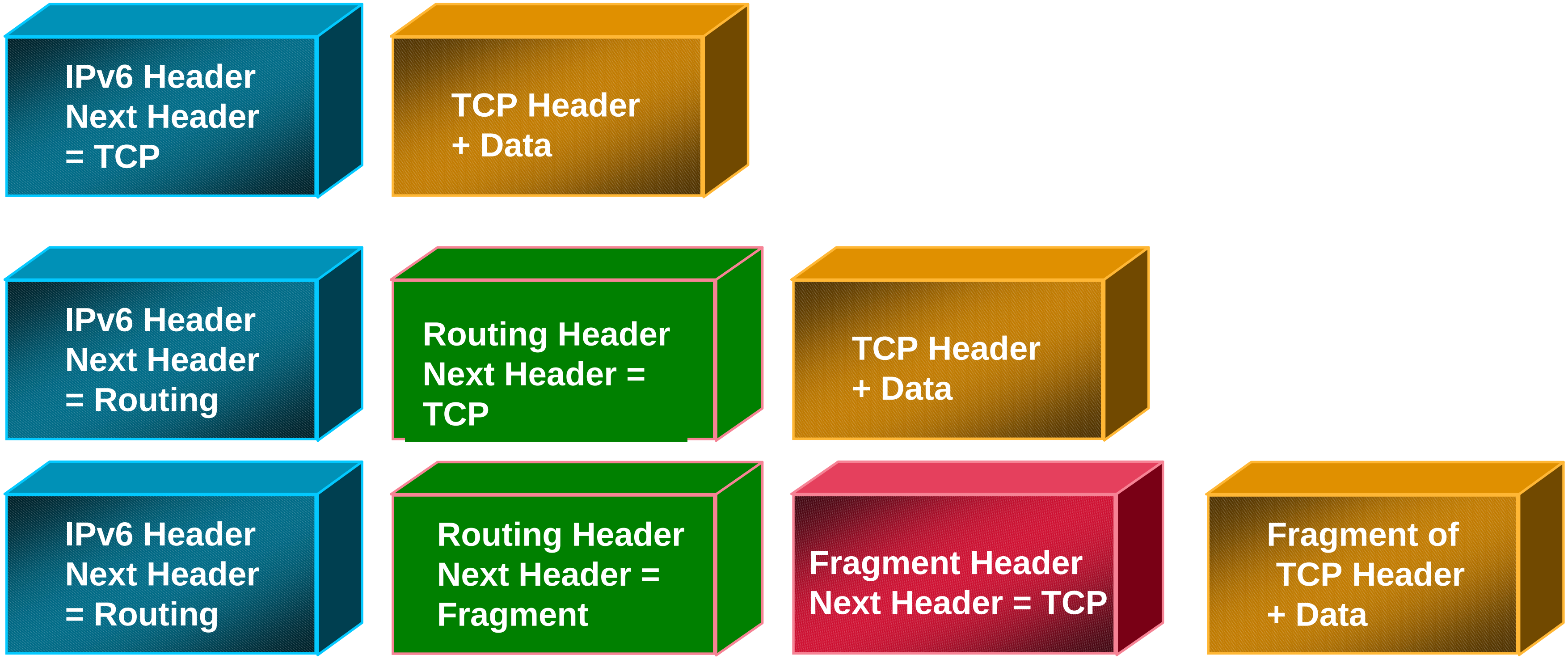
🟨 - field’s name kept from IPv4 to IPv6

🟥 - fields not kept in IPv6

🟦 - Name & position changed in IPv6

🟩 - New field in IPv6

IPv6 Header Options (RFC 2460)



- Processed only by node identified in IPv6 Destination Address field => much lower overhead than IPv4 options
  - exception: Hop-by-Hop Options header
- Eliminated IPv4’s 40-octet limit on options
  - in IPv6, limit is total packet size, or Path MTU in some cases

IPv6 Security Options

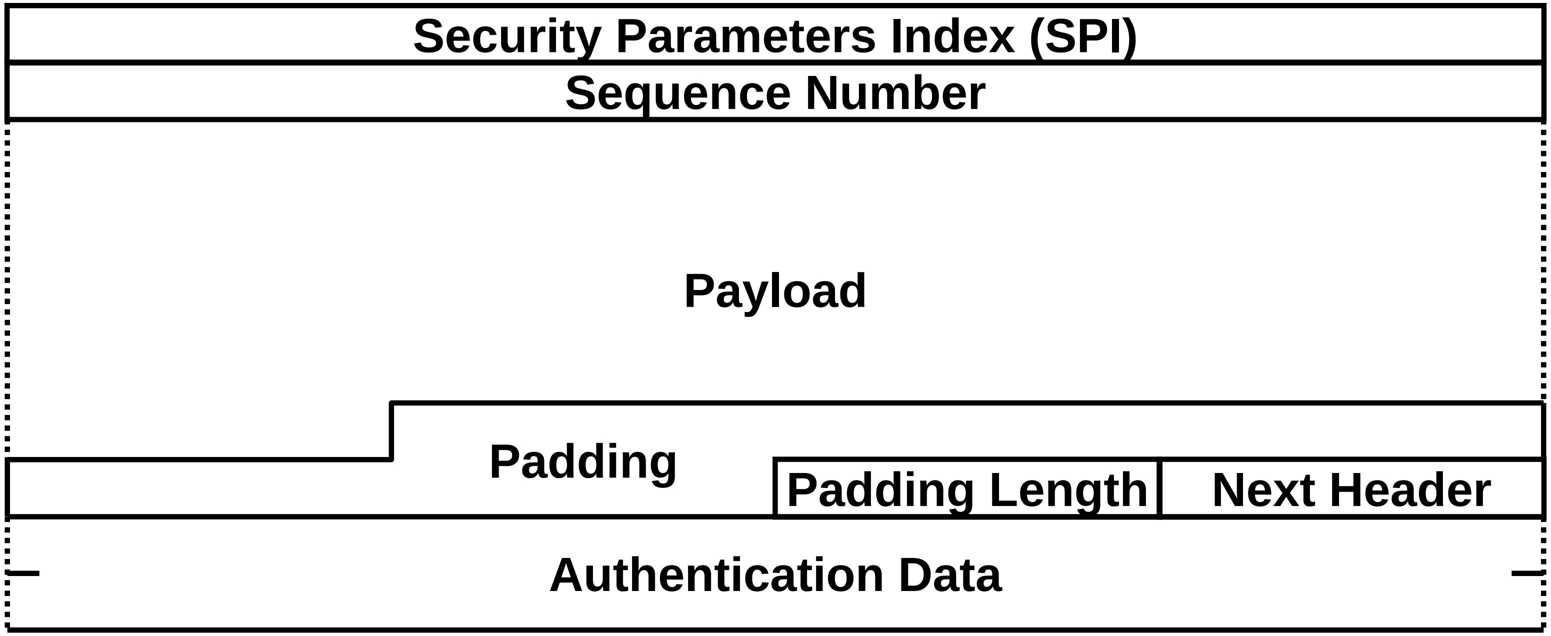
- All implementations required to support authentication and encryption headers (AH and ESP of IPsec)
- Authentication separate from encryption for use in situations where encryption is prohibited or prohibitively expensive
- Key distribution protocols are under development (independent of IP v4/v6)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

Authentication Header (AH)

<table>
<tr><td>Next Header</td><td>Hdr Ext Len</td><td colspan="2">Reserved</td></tr>
<tr><td colspan="4">Security Parameters Index (SPI)</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Authentication Data</td></tr>
</table>

- 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)


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

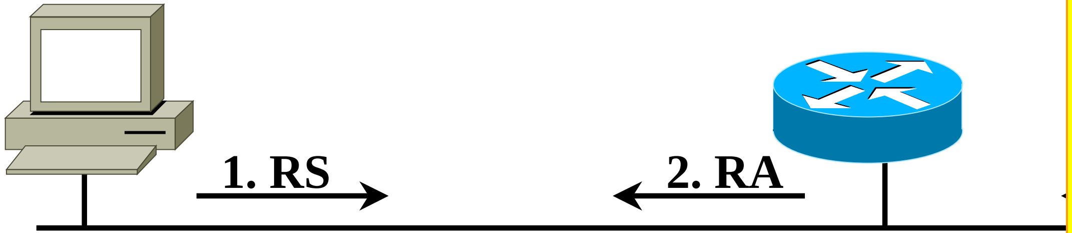
What else does IPv6 for Security?

- Security
  - Nothing IP4 doesn’t do - IPsec runs on 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…

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

Stateless autoconfiguration



ICMP w/o IPsec AH⇔ gives exactly same level of security as ARP for IPv4 (none)

Bootstrap security problem!

Potential solution: 802.1x or CGA

1. RS:

ICMP Type = 133

Src = ::

Dst = All-Routers multicast Address

query= please send RA

2. RA:

ICMP Type = 134

Src = Router Link-

Dst = All-nodes multicast address

Data= options, prefix, lifetime, autoconfig flag

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

Neighbor Discovery - Neighbor Solicitation

ICMP type = 135 Src =
A Dst =
Solicited-node multicast of B Data =
link-layer address of A
Query = what is your link address?

Security mechanisms built into discovery protocol ⇔ None.

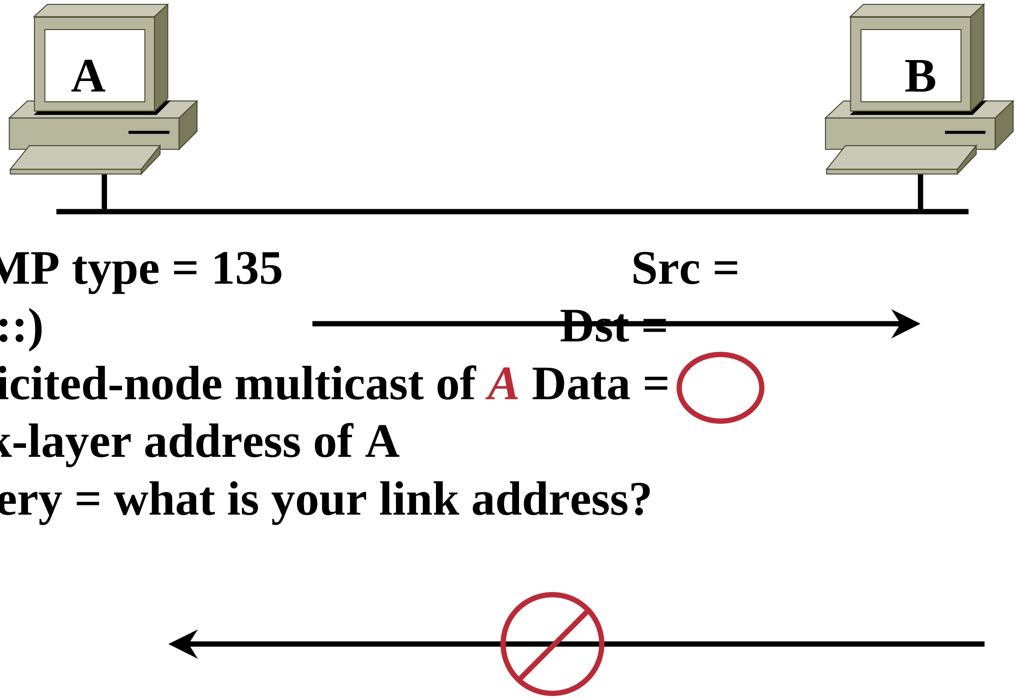
Bootstrap security problem!

Potential solution: 802.1x or CGA

ICMP typ
B
Data = link-layer address of B

A and B can now exchange packets on this link

DAD (Duplicate Address Detection)



ICMP type = 135 Src =
0 (::) Dst =
Solicited-node multicast of *A* Data =
link-layer address of A
Query = what is your link address?

From RFC 2462:

« If a duplicate @ is discovered … the address *cannot* be assigned to the interface…»

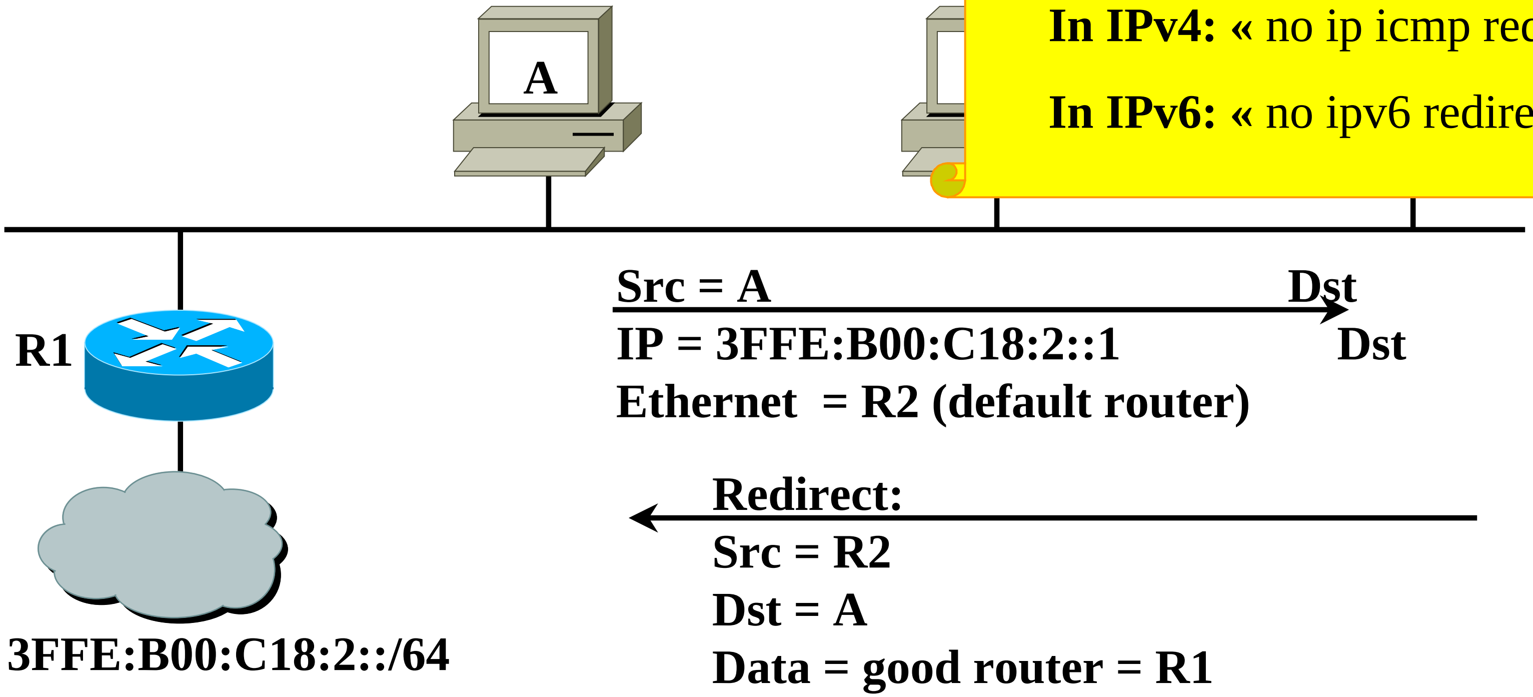
⇔ What if: Use MAC@ of the node you want to DoS and fabricate its IPv6 @

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

Neighbor Discovery - Redirect

In IPv4: « no ip icmp redirect »

In IPv6: « no ipv6 redirect »

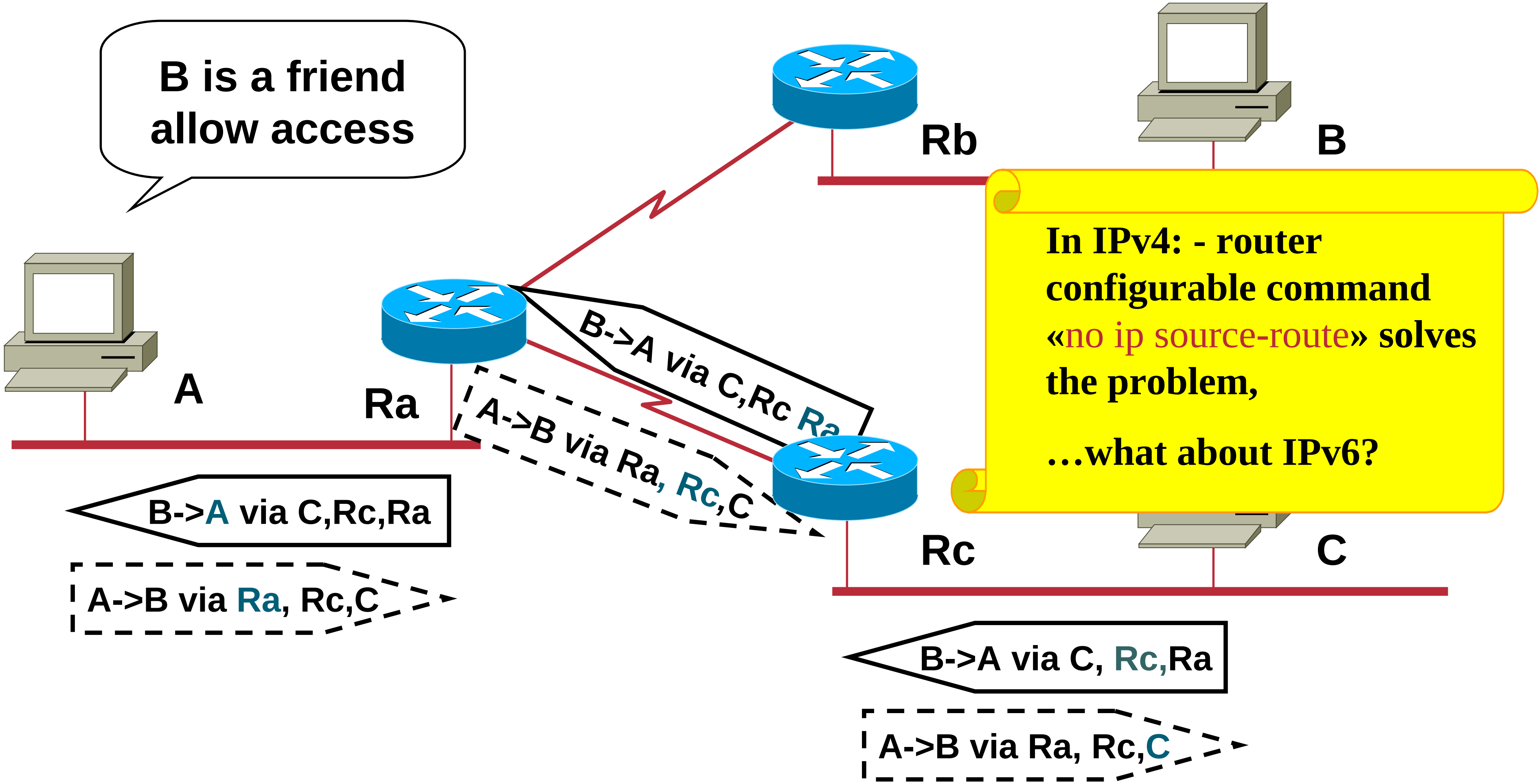


Src = A
IP = 3FFE:B00:C18:2::1
Ethernet = R2 (default router)

Redirect:
Src = R2
Dst = A
Data = good router = R1

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

IPv4 Spoofing using Source Routing

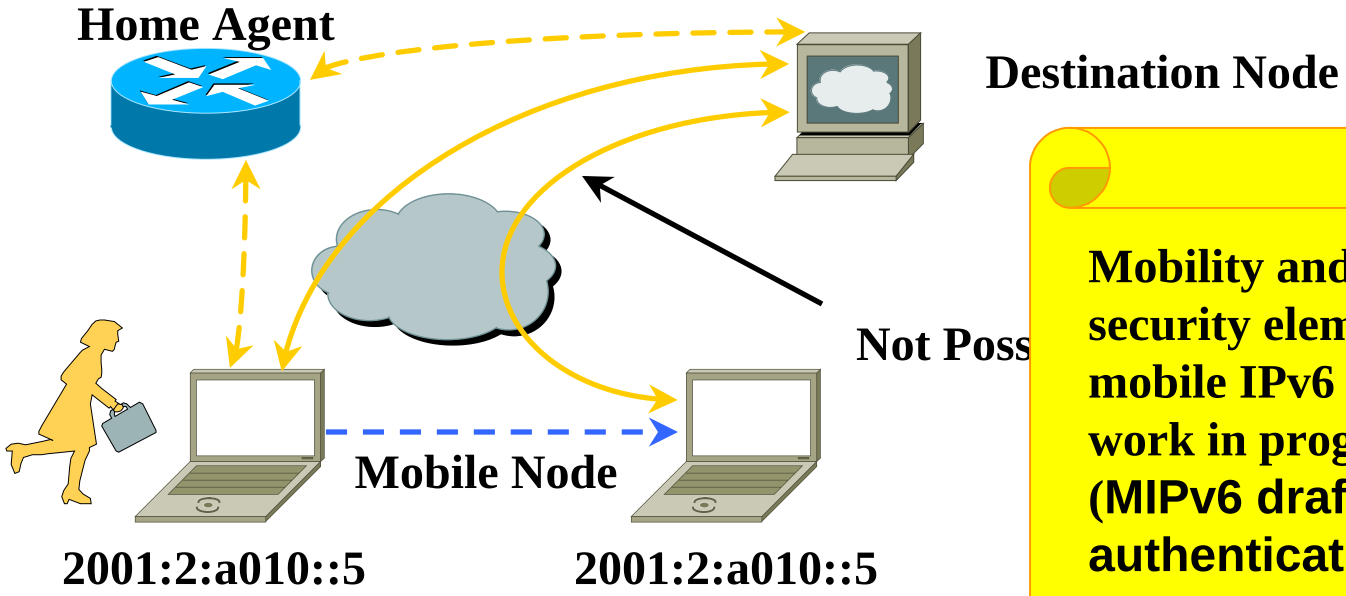


In IPv4: - router configurable command «no ip source-route» solves the problem,

…what about IPv6?

Back traffic uses the same source route

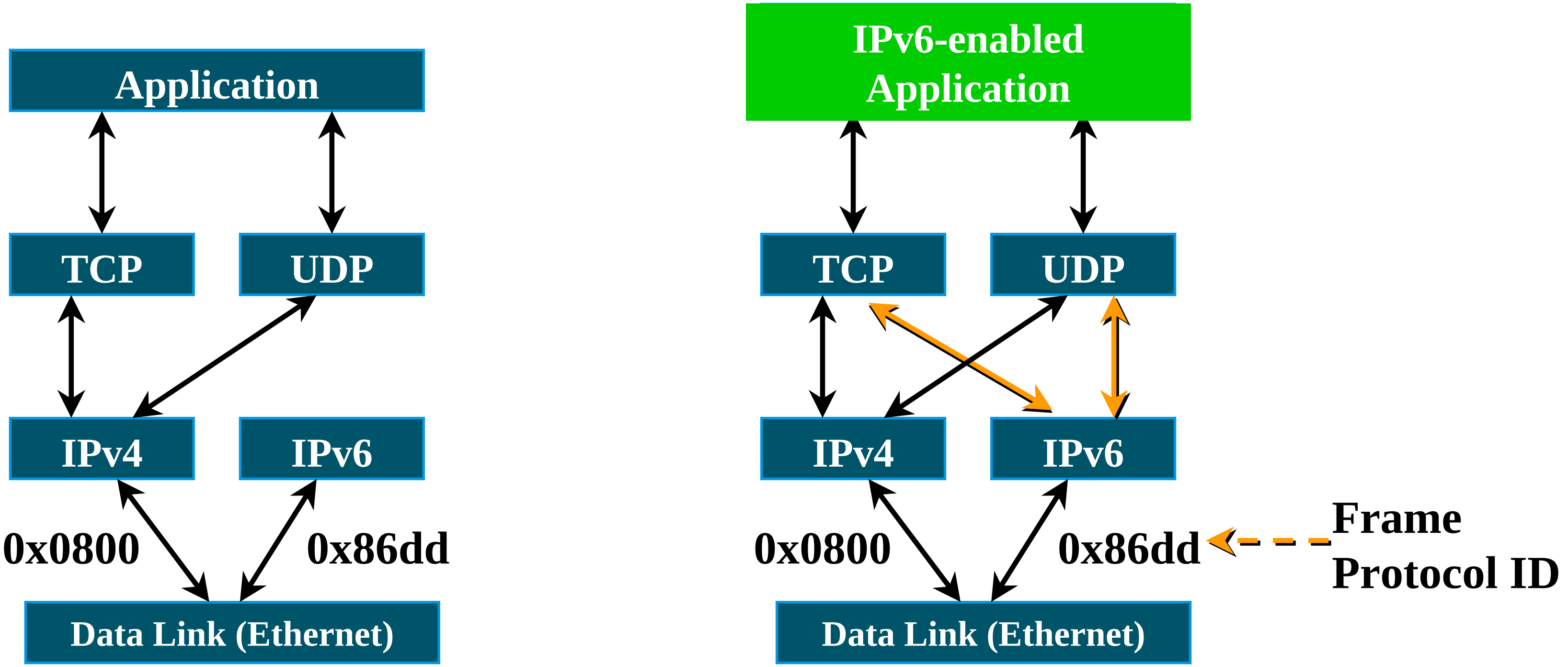
Mobile IP
- security still work in progress



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

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

IPv6/IPv4 Dual Stack Approach



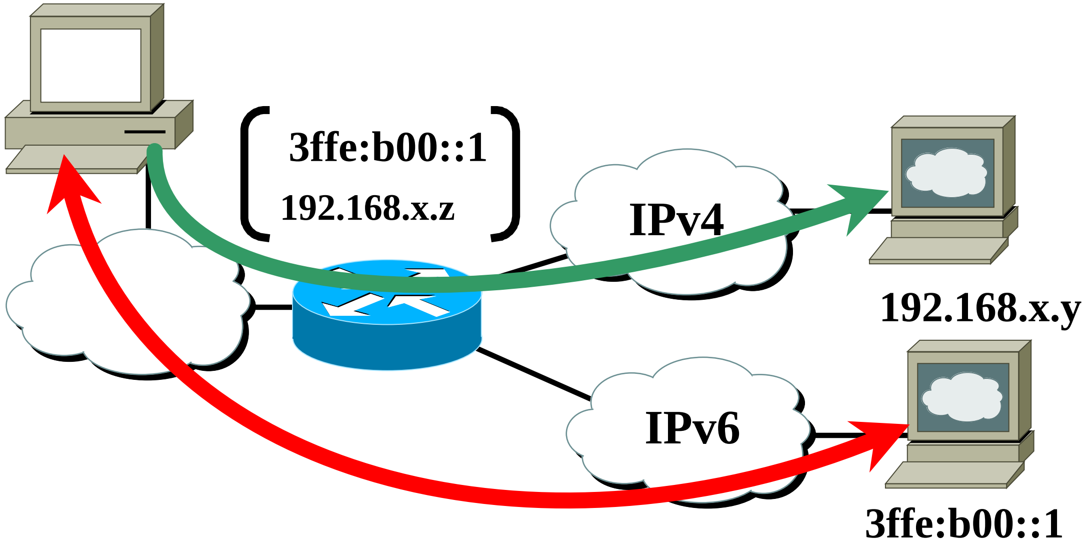
- **Dual stack node means:**

  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



If the VPN policy allows no split tunneling, does the dual stack approach supports it?

- **In a dual stack case & VPN tunnel with non-split tunneling policy:**

  - All IPv4 traffic is non-split tunneled through VPN tunnel

  - All IPv6 traffic is going out (and in) in the clear as a policy violation(?)

IPv6 vs. IPv4 Security Summary

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?

References

Forums and test beds:

- www.6net.org
- www.6bone.net
- www.ipv6forum.com

Vendor links:

- www.cisco.com/ipv6
- www.microsoft.com/ipv6

Other useful links:

- www.kame.net
- www.bieringer.de/linux/IPv6 IPv6 ready
- www.hs247.com
- www.ietf.org/internet-drafts/draft-ietf-send-psreq-03.txt
- www.ietf.org/internet-drafts/draft-ietf-send-cga-01.txt

Thank you!

IPv6 Protocol

Does it solve all the security problems of IPv4?

fmajstor@cisco.com