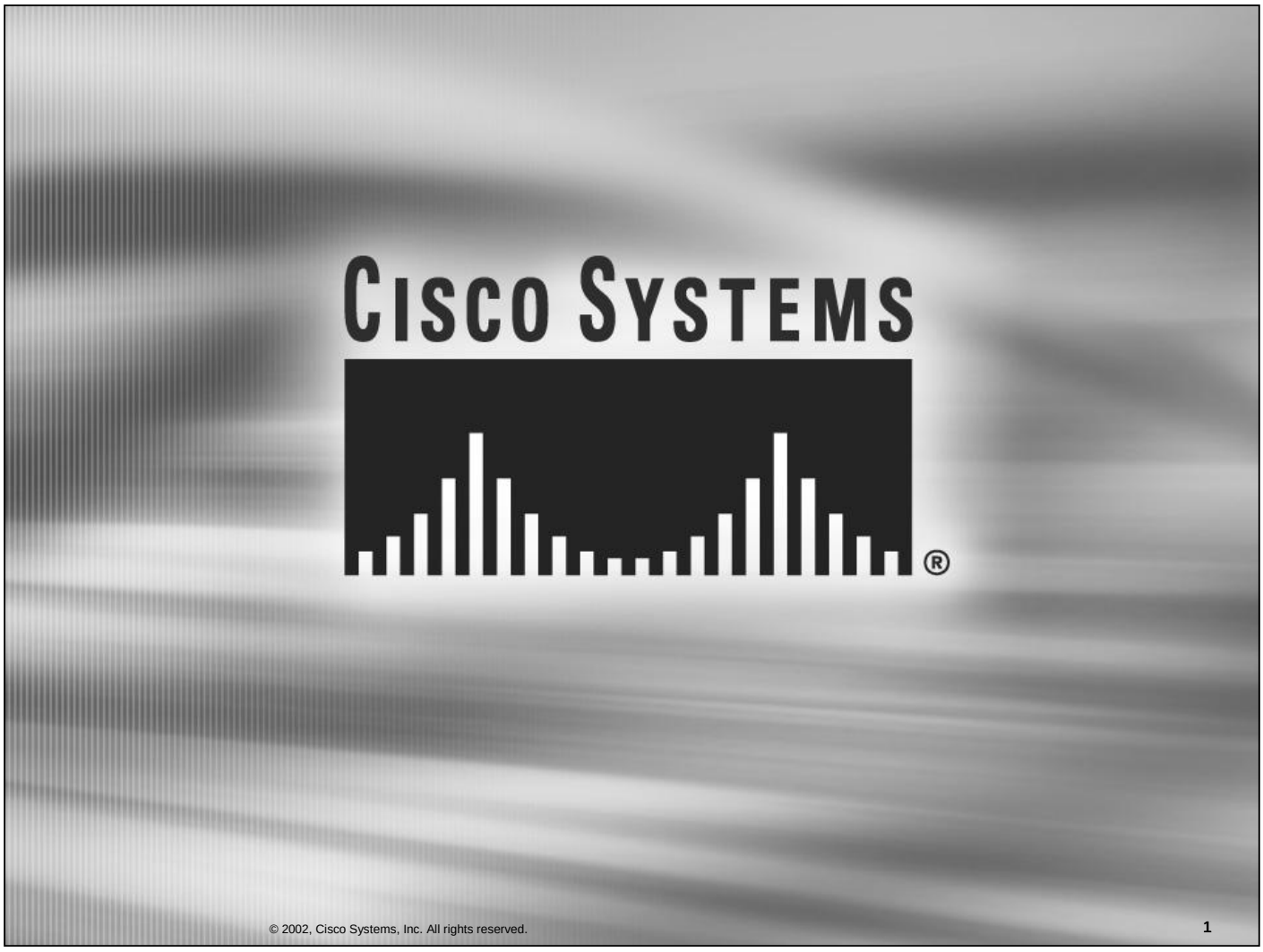
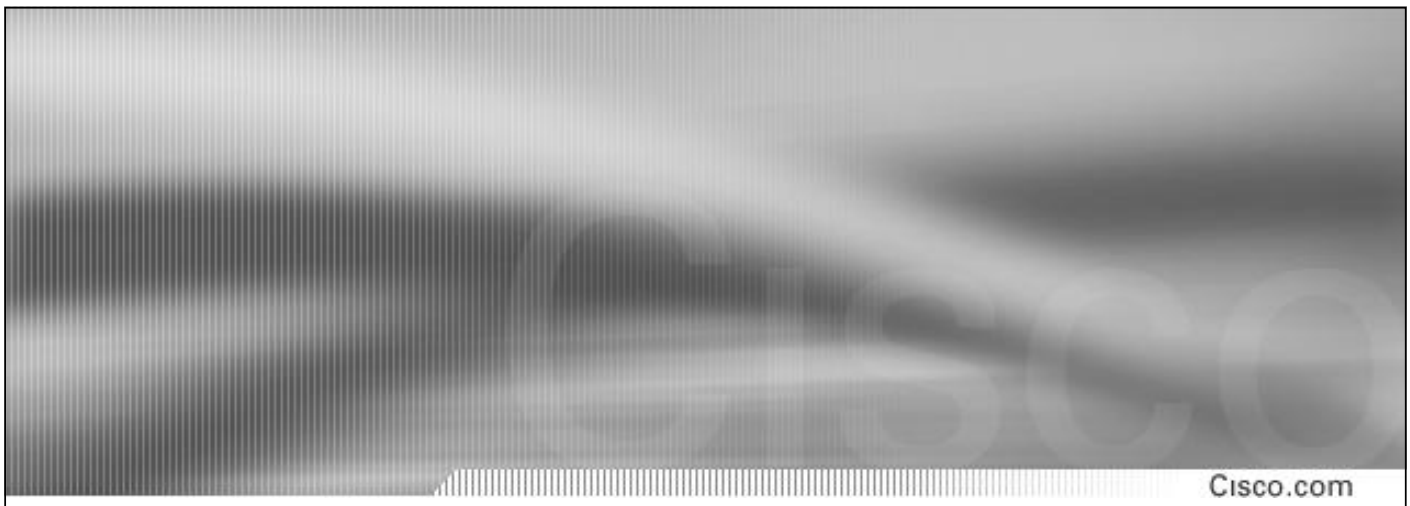




IPv6 Security

Franjo Majstor

EMEA Consulting Engineer

fmajstor@cisco.com

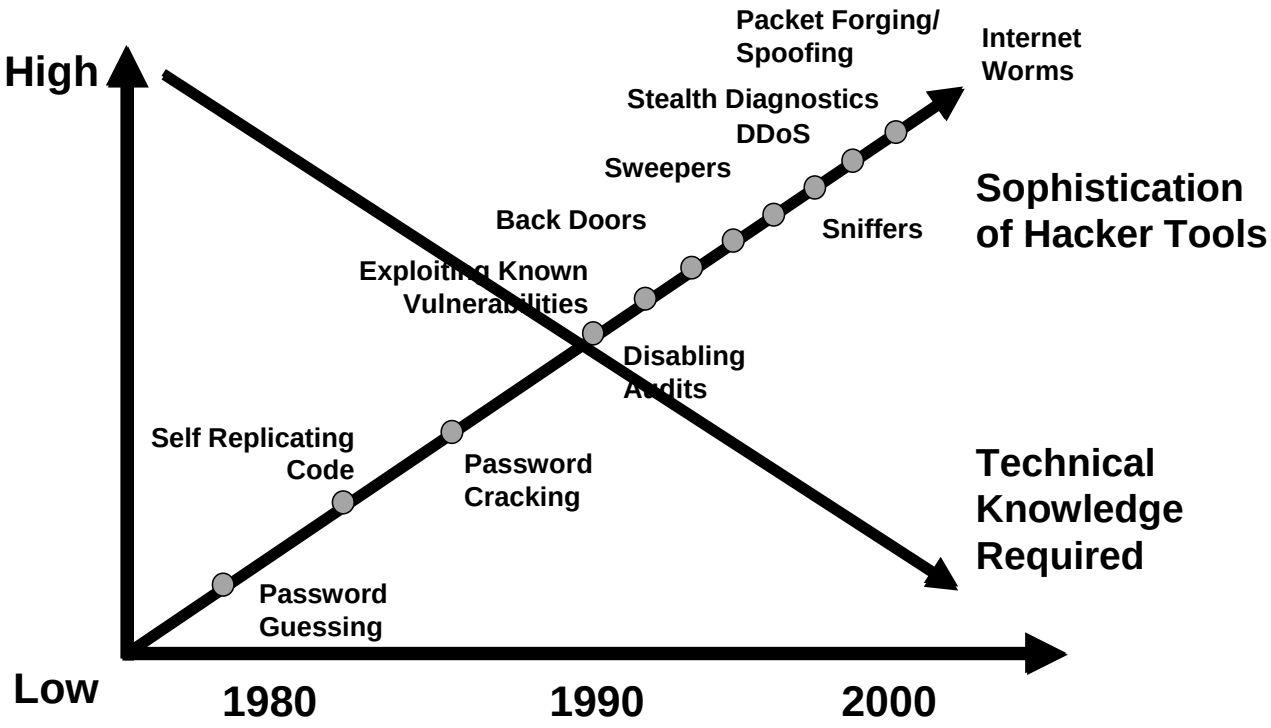
Agenda

- IPv6 Primer
- IPv6 Protocol Security
- IOS IPv6
- MS Windows 2K/XP and IPv6
- Q&A

IPv6 Primer

Threat Trends

Cisco.com



Short History of IPv6

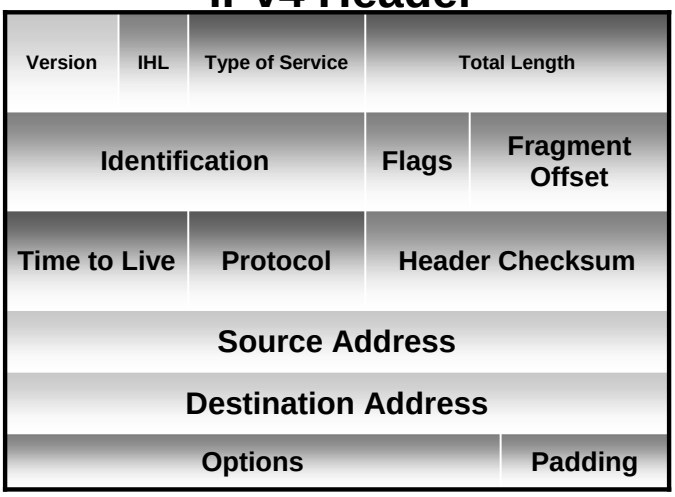
Cisco.com

- 1990 — Prediction of the exhaustion of IPv4 Class B by 1994.
- 1991 — ROAD group formed to address routing.
- 1992 — Prediction of the exhaustion of IPv4 Class C by 1994.
- 1993 — IPng Proposals solicitation (RFC 1550).
- 1994 — CATNIP, SIPP, TUBA analyzed. SIPP+ chosen. IPng wg started.
- 1995 — First specification: RFC 1883.
- 1996 — 6bone started.
- 1997 — First attempt for provider-based address format.
- 1998 — First IPv6 exchange: 6tap.
- 1999 — Registries assign IPv6 prefixes. IPv6Forum formed.
- 2001 — Vendor Support in Main Product Lines

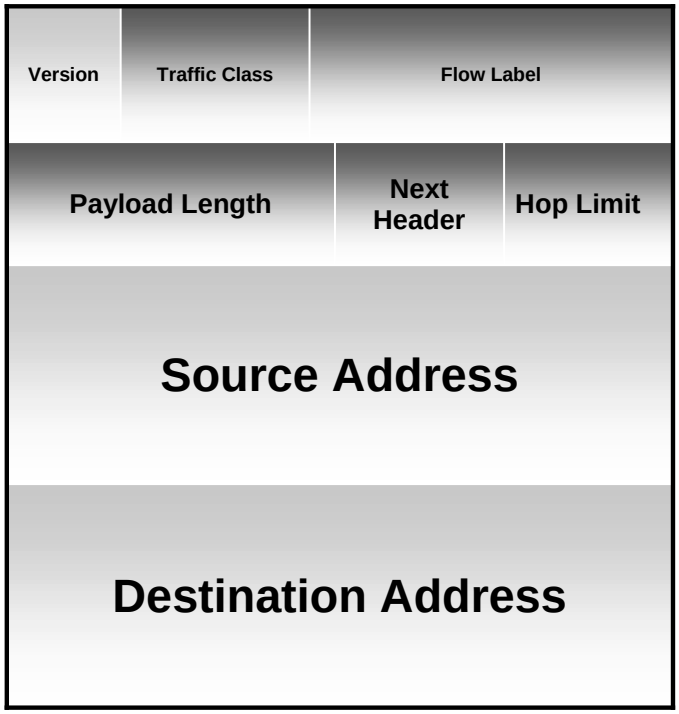
IPv4 & IPv6 Header Comparison

Cisco.com

IPv4 Header



IPv6 Header

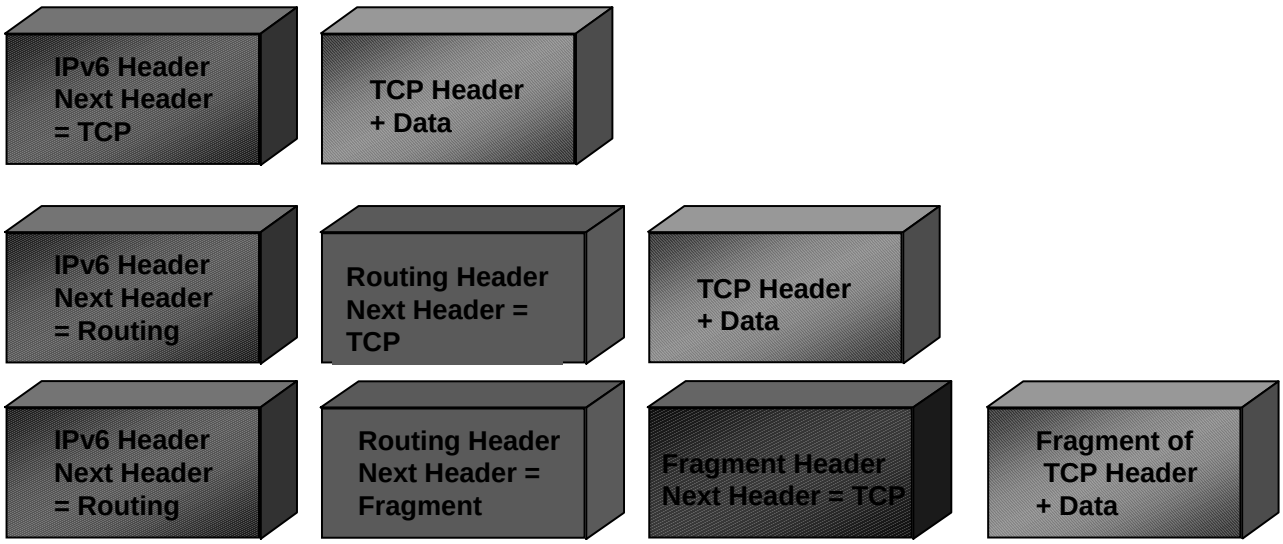


Legend

- 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)

Cisco.com



- 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 Address Representation

Cisco.com

- **Format:**

x:x:x:x:x:x:x:x where x is 16 bits hexadecimal field.

2031:0000:130F:0000:0000:09C0:876A:130B

Case insensitive

Leading zeros in a field are optional:

2031:0:130F:0:0:9C0:876A:130B

Successive fields of 0 are represented as ::, but only once in an address:

2031:0:130F::9C0:876A:130B

2031::130F::9C0:876A:130B

FF01:0:0:0:0:0:0:1 => FF01::1

0:0:0:0:0:0:0:1 => ::1

0:0:0:0:0:0:0:0 => ::

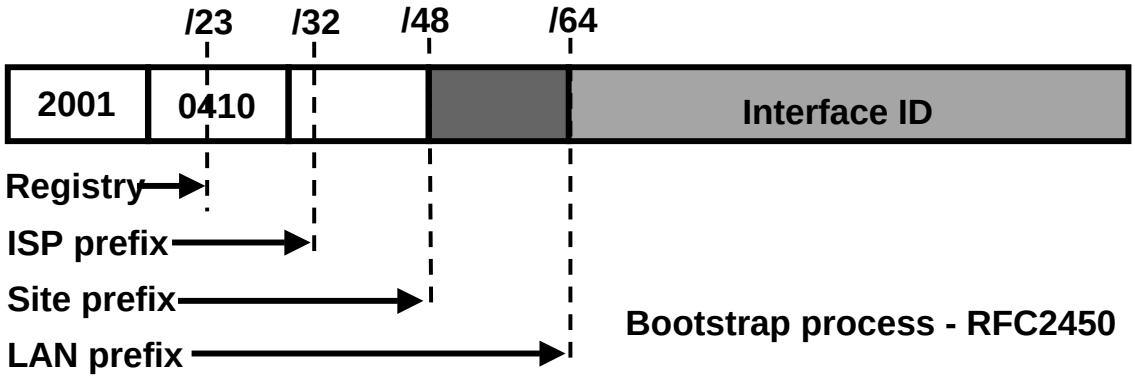
IPv6 Addressing

Cisco.com

- **IPv6 Addressing rules are covered by multiples RFC's**
  - **Architecture defined by RFC 2373**
- **Address Types are :**
  - **Unicast : One to One (Global, Link local, Site local, Compatible)**
  - **Anycast : One to Nearest (Allocated from Unicast)**
  - **Multicast : One to Many**
  - **Reserved**
- **A single interface may be assigned multiple IPv6 addresses of any type (unicast, anycast, multicast)**
  - **No Broadcast Address -> Use Multicast**

Address Allocation

Cisco.com



- The allocation process is under reviewed by the Registries:
  - IANA allocates 2001::/16 to registries
  - Each registry gets a /23 prefix from IANA
  - Formerly, all ISP were getting a /35
  - With the new proposal, Registry allocates a /36 (immediate allocation) or /32 (initial allocation) prefix to an IPv6 ISP
  - Policy is that an ISP allocates a /48 prefix to each end customer
  - ftp://ftp.cs.duke.edu/pub/narten/ietf/global-ipv6-assign-2002-06-26.txt

IPv6 Addressing Mechanism for Privacy

Cisco.com

- Temporary addresses
  - Inhibit device/user tracking
  - Random 64 bit interface ID
  - Rate of change based on local policy

  From RFC 3041: "…interface identifier …facilitates the tracking of individual devices (and thus potentially users)…"

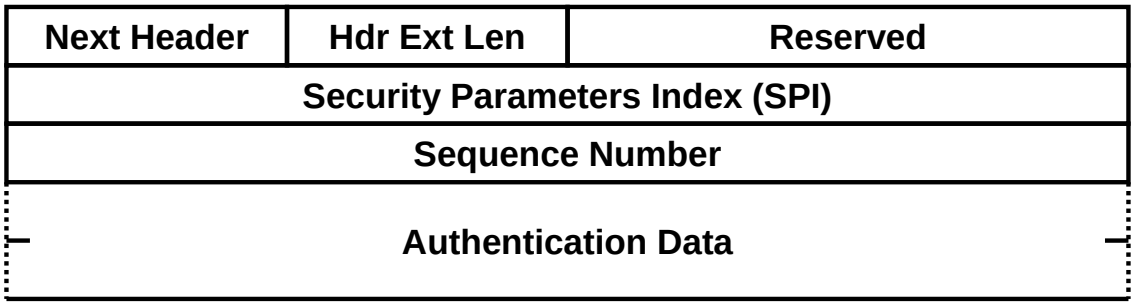
IPv6 Protocol Security

IPv6 Security

Cisco.com

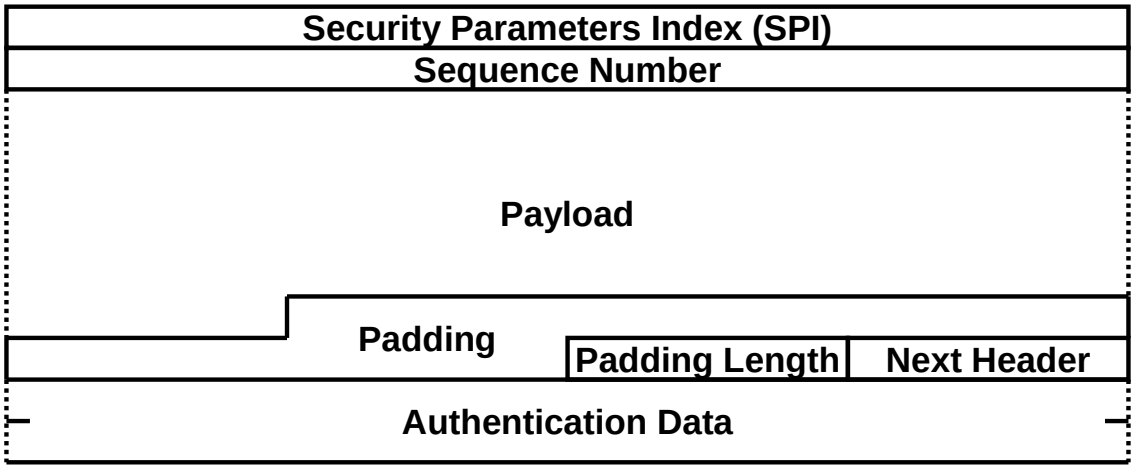
- All implementations required to support authentication and encryption headers (AH and ESP of IPsec)
- Authentication separate from encryption for use in situations where encryption is prohibited or prohibitively expensive
- Key distribution protocols are under development (independent of IP v4/v6)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

Authentication Header (AH)



- **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)



- **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!**

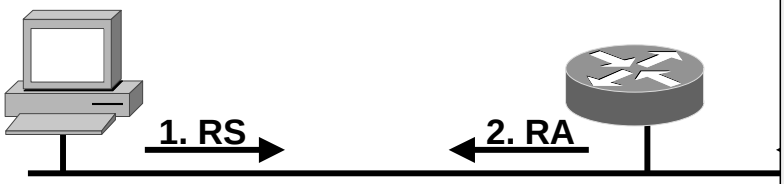
IPv6 Security Exposures…

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



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**

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

Bootstrap security problem!

Potential solution: 802.1x on L2.

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

Neighbor Discovery - Neighbor Solicitation

Cisco.com

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

ICMP type = 136
Src = B
Dst = A
Data = link-layer address of B

A and B can now exchange packets on this link

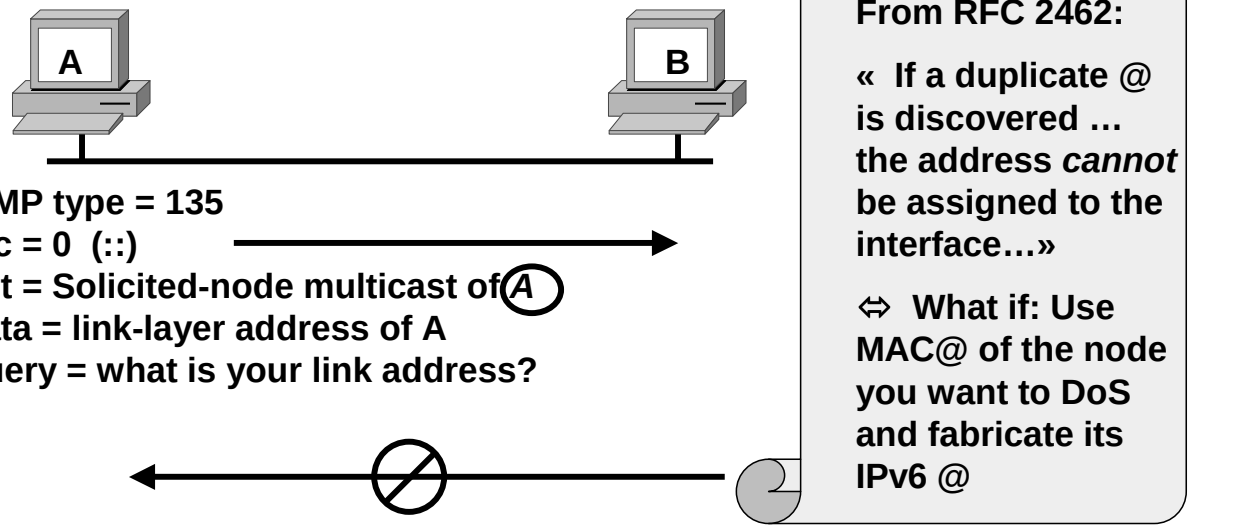
Security mechanisms built into discovery protocol ⇔ None.

Bootstrap security problem!

Potential solution: 802.1x on L2.

DAD (Duplicate Address Detection)

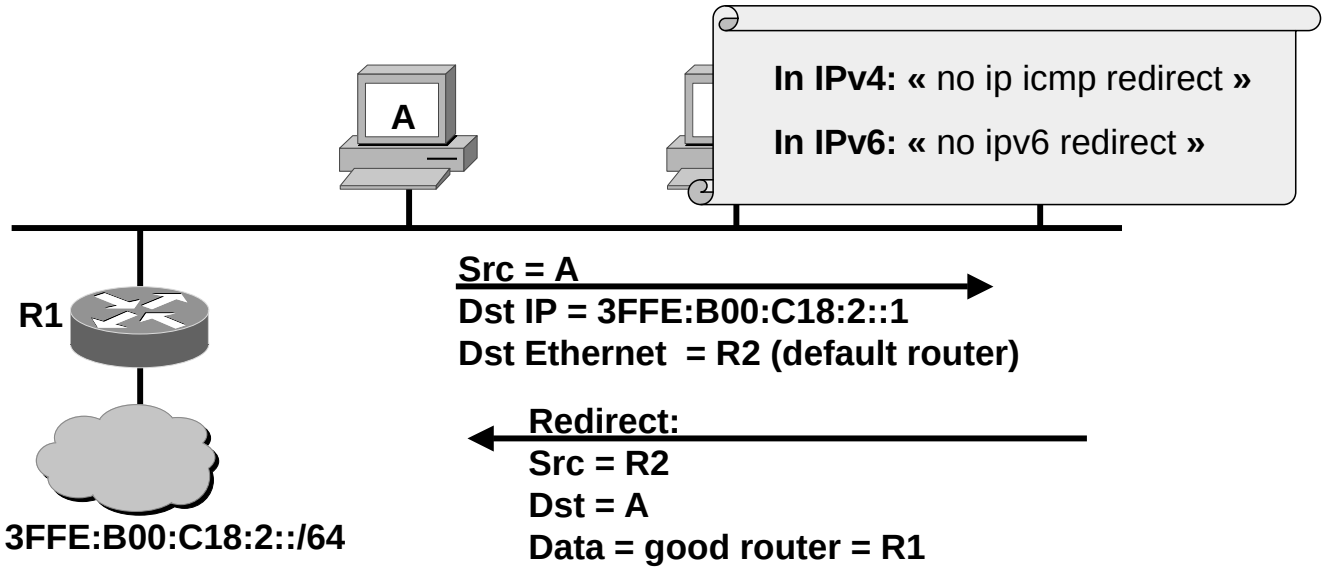
Cisco.com



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

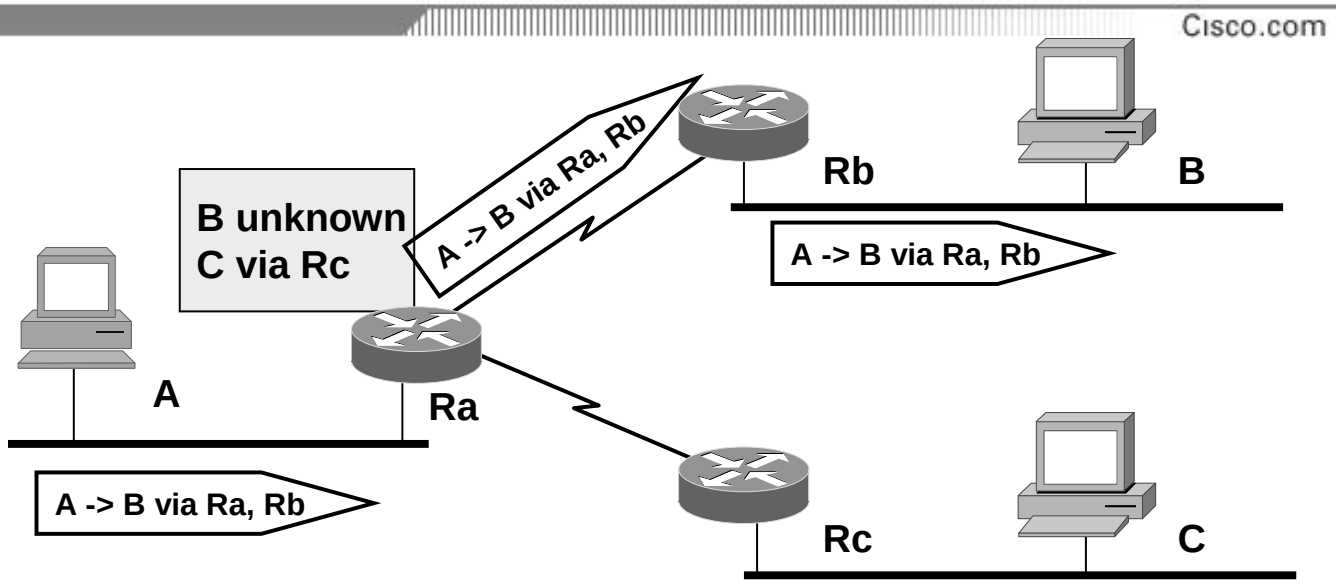
Neighbor Discovery - Redirect

Cisco.com



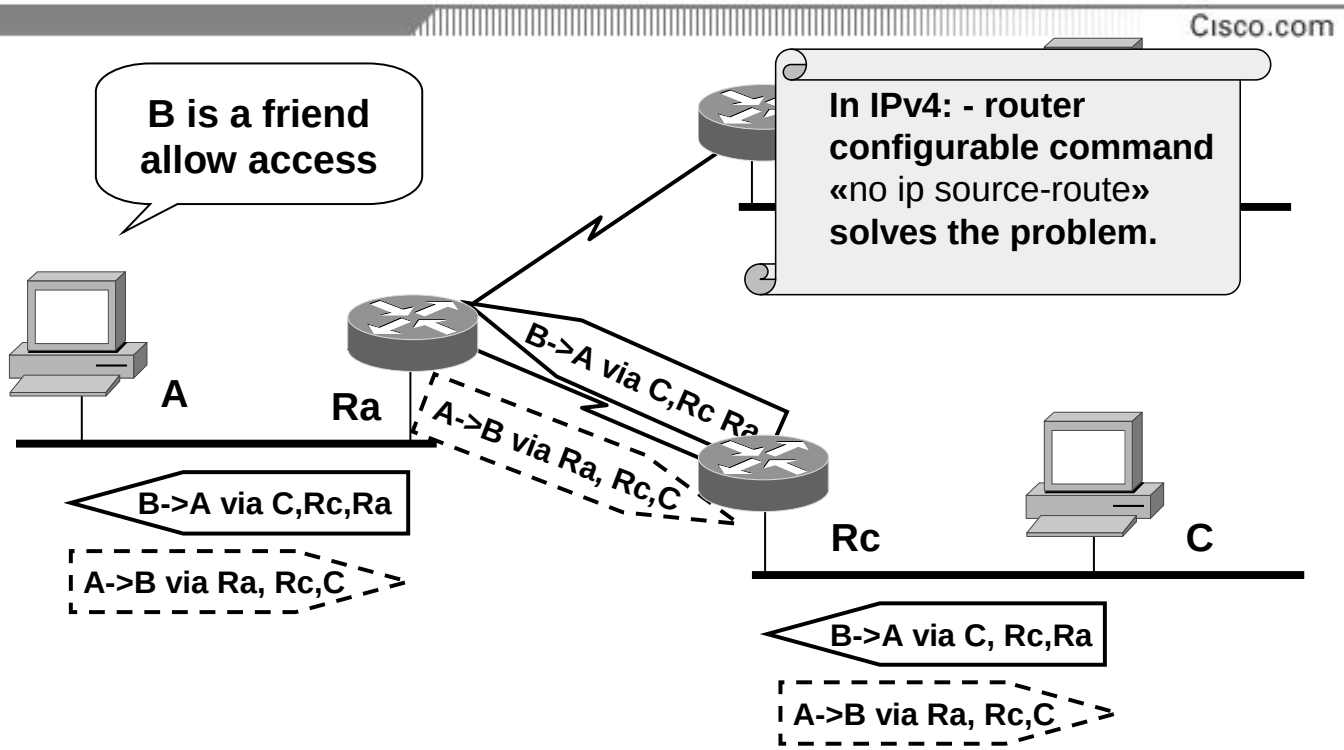
- **Redirect is used by a router to signal the reroute of a packet to a better router.**

IPv4: Source Routing Security Problem



Routing based on IPv4 datagram option

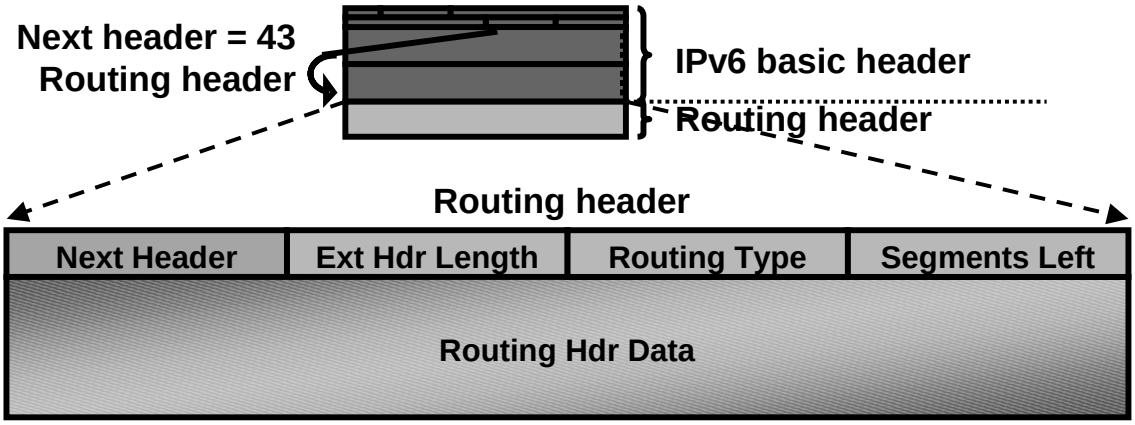
IPv4 Spoofing Using Source Routing



Back traffic uses the same source route

IPv6 Routing Header

Cisco.com



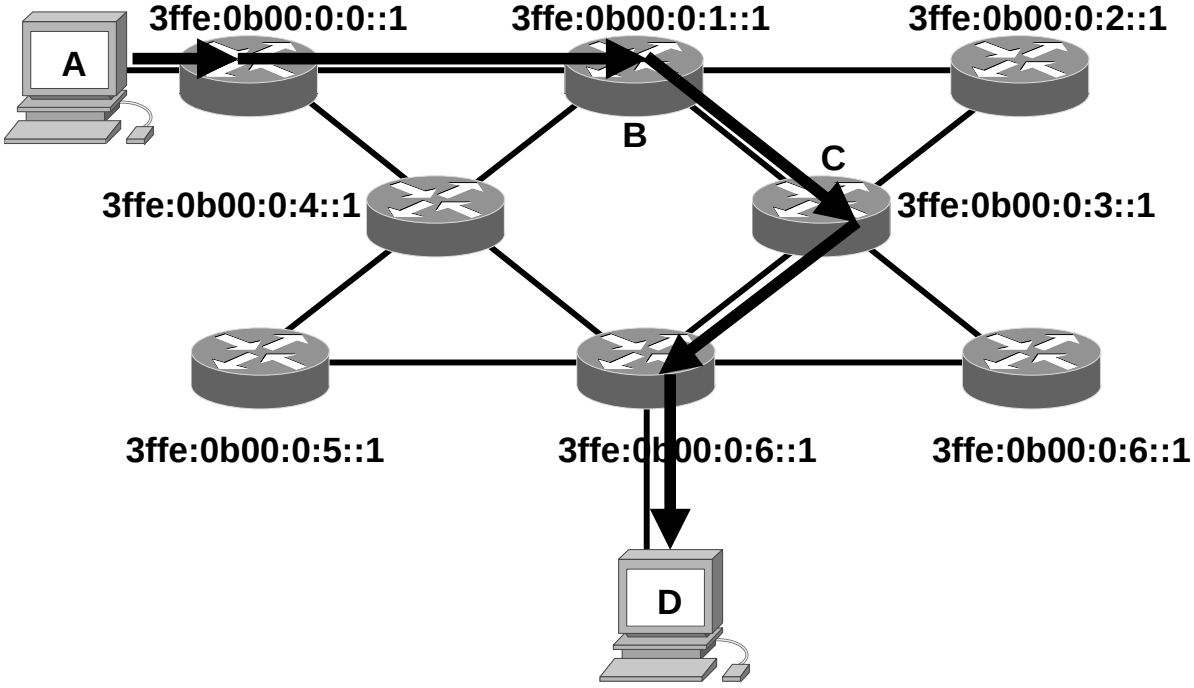
- **Routing header is:**

  An extension header.

  Processed by the listed intermediate routers.

IPv6 Routing Header

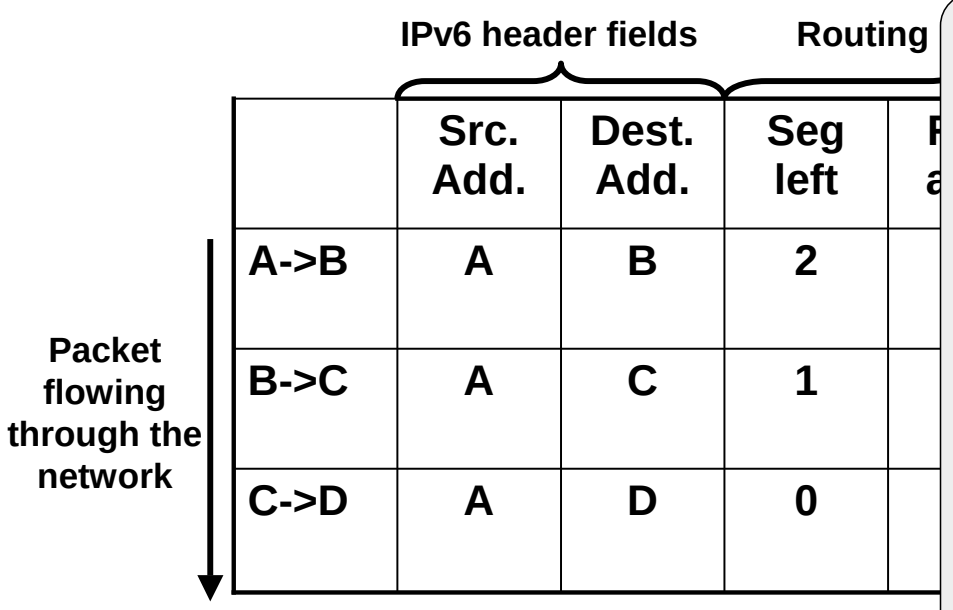
Cisco.com



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

IPv6 Routing Header (cont.)

Cisco.com



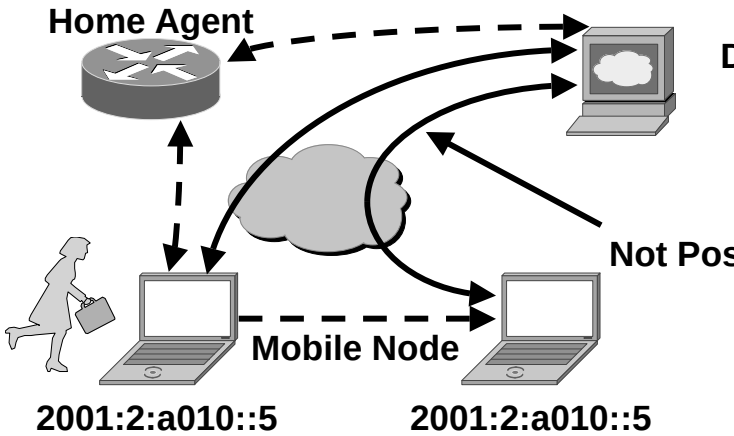
Routing header IPv6 ⇔ Source routing in IPv4

« 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

Cisco.com



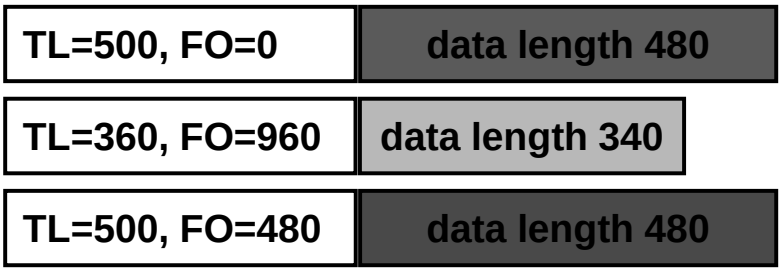
Mobility and security elements of mobile IPv6 still work in progress… (MIPv6 draft 18/19 authentication).

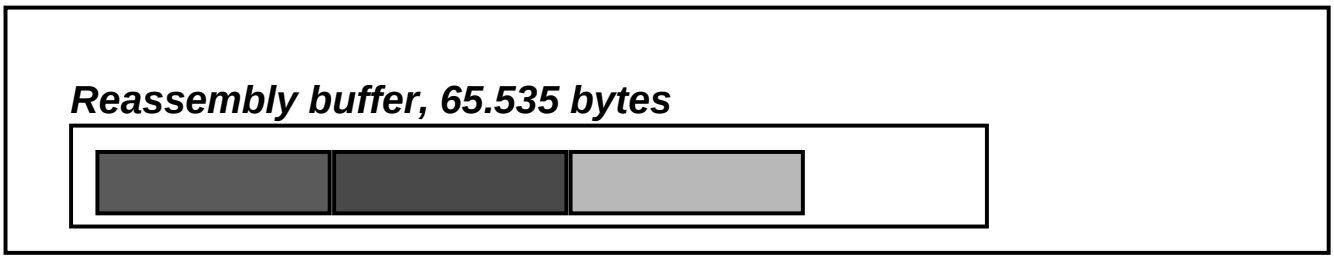
- **Mobility means:**
  - **Mobile devices are fully supported while moving**
  - **Built-in on IPv6**
    - **Any node can use it**
  - **Efficient routing means performance for end-users**

IPv4 Normal Fragmentation/Reassembly

Cisco.com

Received from the network:





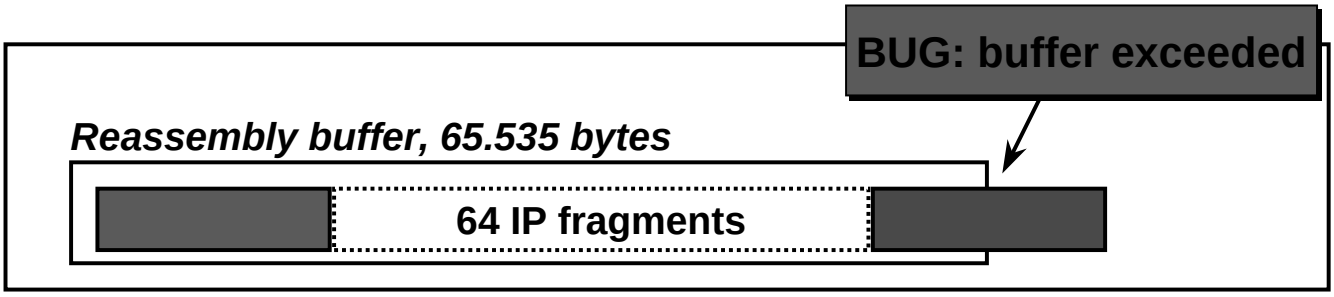
Kernel memory at destination host

IPv4 Reassembly Attack

Cisco.com

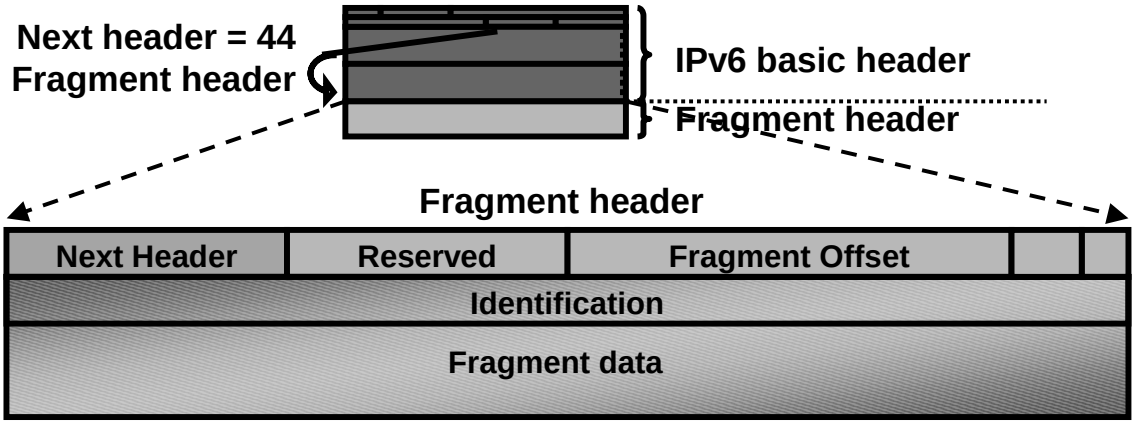
Received from the network:

… 64 IP fragments with data length 1000 ...



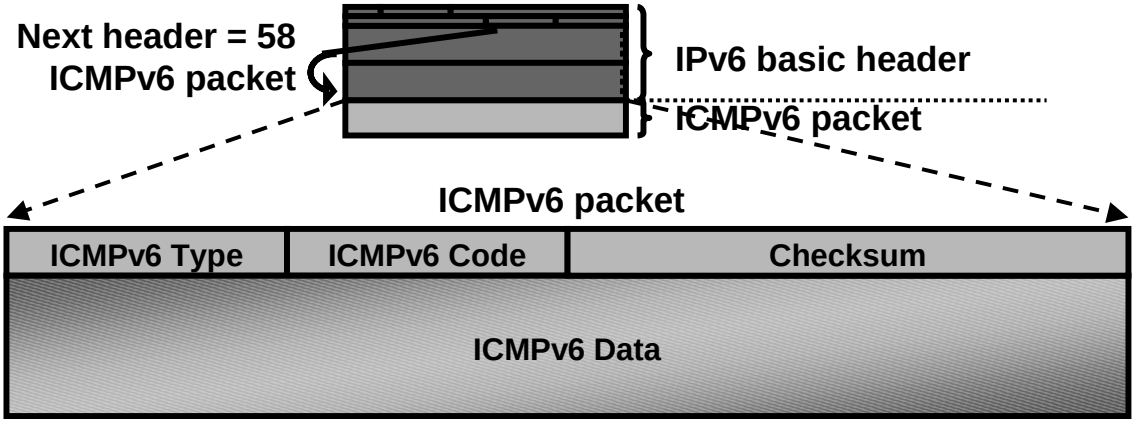
Kernel memory at destination host

Fragment Header - IPv6



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

ICMPv6



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

What does IPv6 do for securing DNS?

	IPv4	IPv6
Hostname to IP address	A record: www.abc.test. A 192.168.30.1	AAAA record: www.abc.test AAAA 3FFE:B00:C18:1::2
IP address to hostname	PTR record: 1.30.168.192.in-addr.arpa. PTR www.abc.test.	PTR record: 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.int. PTR www.abc.test.

Not much!

IOS IPv6

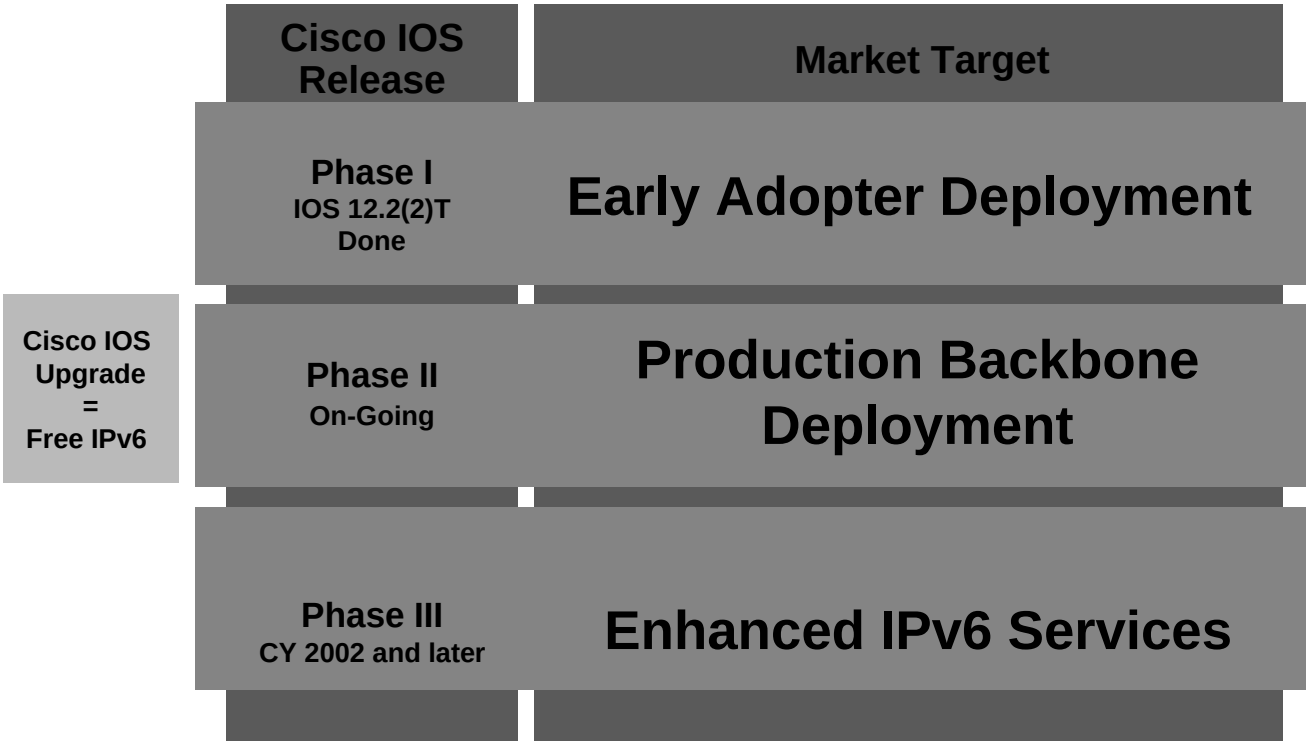
IPv6 @Cisco Systems

Cisco.com

- Co-chair of IETF IPv6 WG and NGtrans WG
- Well Known Cisco 6Bone router
  - ~ 70 tunnels with other companies
  - acts as 6to4 Relay
  - Official Cisco IPv6 prefix registered to ARIN (2001:0420::/35)
- 'Founding Member' of the IPv6 Forum
- Official CCO IPv6 page is www.cisco.com/ipv6
  - Cisco IPv6 Statement of Direction published last June
  - Cisco IOS IPv6 EFT available for free over 3 years
  - ~around 500 sites running Worldwide
- Cisco IOS 12.2(2)T offers official IPv6 support
  - including Cisco IOS IPv6 training & Worldwide TAC

Cisco IOS Roadmap: The Confluence of IPv4/IPv6

Cisco.com



Cisco IOS IPv6 Phase I

Cisco.com

Cisco IOS Release	IPv6 Features Supported
Phase I Early Adopters Cisco IOS 12.2(2)T, (4)T Any router able to run 12.2T, from Cisco 800 to Cisco 7500 IP Plus, Enterprise and SP images	IPv6 Basic specification (RFC 2460) ICMPv6, Neighbor Discovery Stateless auto-configuration RIPv6 (RFC 2080) Multi-Protocol extensions for BGP4 (RFC 2545 & 2858) Configured and Automatic Tunnels 6to4 Tunnel Standard Access List IPv6 over Ethernet (10/100/1000Mb/s), FDDI, Cisco HDLC, ATM and FR PVC, PPP (Serial, POS, ISDN) Ping, Traceroute, Telnet, TFTP

Cisco IOS IPv6 Phase II

Cisco.com

Cisco IOS Release	IPv6 Features Development Done
Phase II Backbone Deployment On-Going 12.2(8)T, (13)T 12.0(21)ST1, (22)S 12.2(9)S, (11)S	i/IS-ISv6 CEFv6/dCEFv6 IPv6 Access (Encap/AAA/Dialer Pool), NAT-PT Extended Access Control List IPv6 over IPv4 GRE Tunnels IPv6 Provider Edge router (6PE) over MPLS DNS AAAA client, Static ND cache entry Link-Local Address for BGP Peering CDP, SSH, IPv6 MIB Phase I Sustaining

Cisco IOS IPv6 Phase III

Cisco.com

Cisco IOS Release	Evaluation of IPv6 Phase III Features
Phase III Enhanced Protocols **Target date: H2 CY 2002 And Later**	**Routing: OSPFv3, MT-ISIS & E-IGRP** **Enhanced Services: *Mobile IPv6*, *IPsec*, IPv6 Multicast, IPv6 QoS** **Management: *Netflow IPv6 record*, SNMP over IPv6, MIB's enhancements** **Tunnels: IPv6 over IPv6, IPv4 over IPv6 tunnels, ISATAP** **IETF IPv6 Enhancements: eg. R.A. extensions, Prefix delegation,** **Hardware Acceleration: in-progress** **Encapsulation: Add enhanced support for DPT, Cable and DSL**

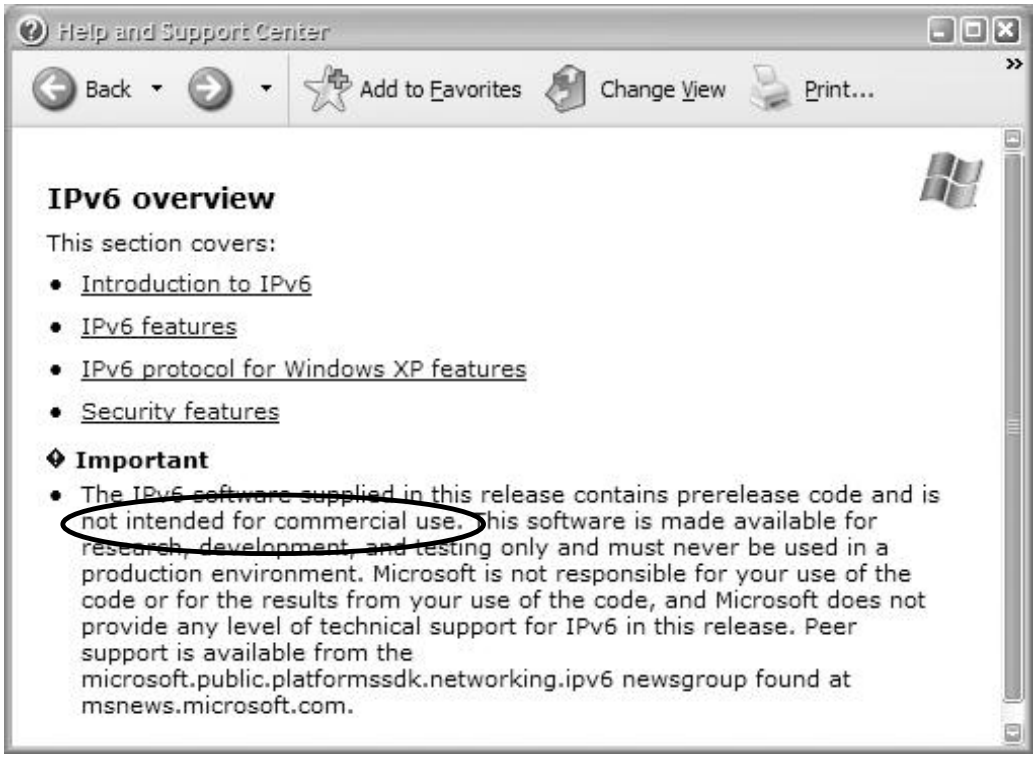
IOS IPv6 aware apps

Cisco.com

- **telnet <destination> /ipv6**
- **traceroute ipv6 <destination>**
- **tftp ("myhost /ipv6")**
- **ssh <destination>**
- **ping ipv6 <destination>**
- **DNS lookups**
- **ip http server**

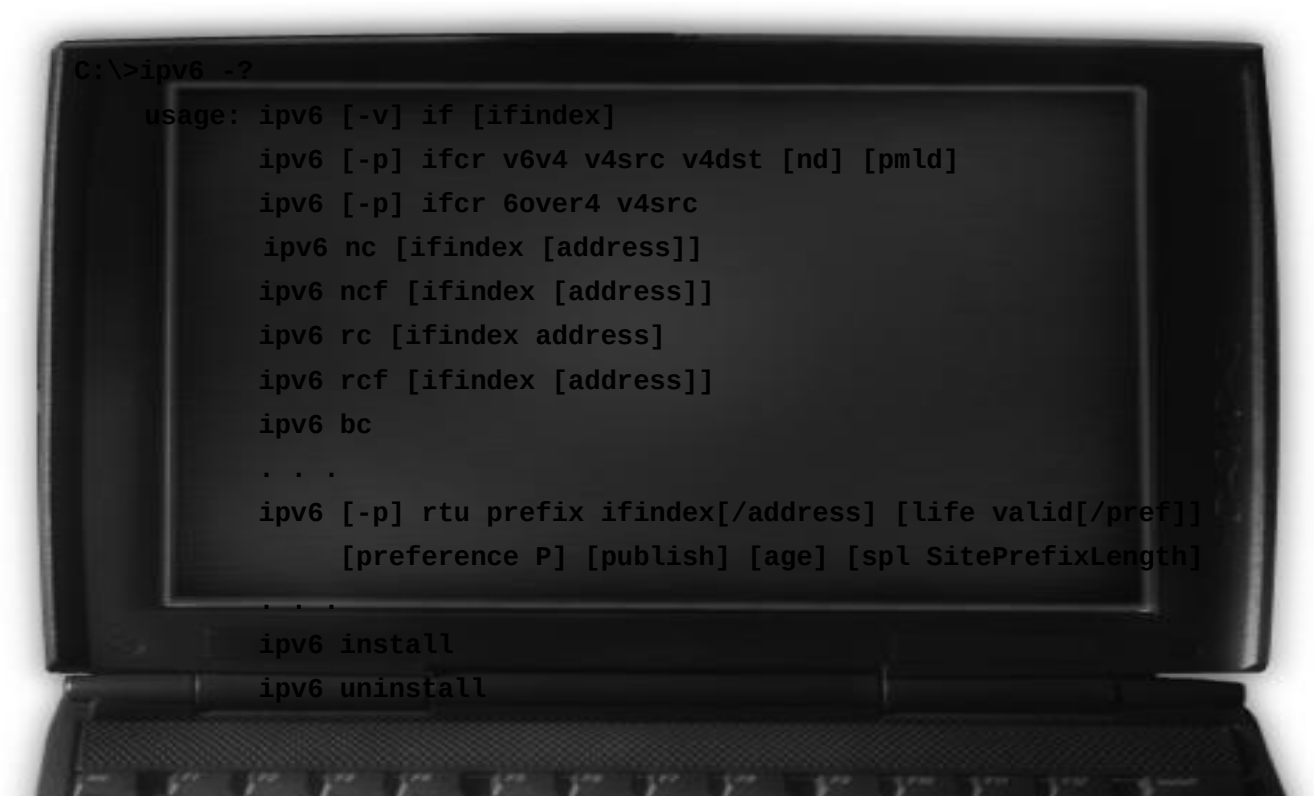
MS Windows 2K/XP and IPv6

IPv6 protocol for MS WinXP *(DISCLAIMER!)*



IPv6 & MS XP

Cisco.com



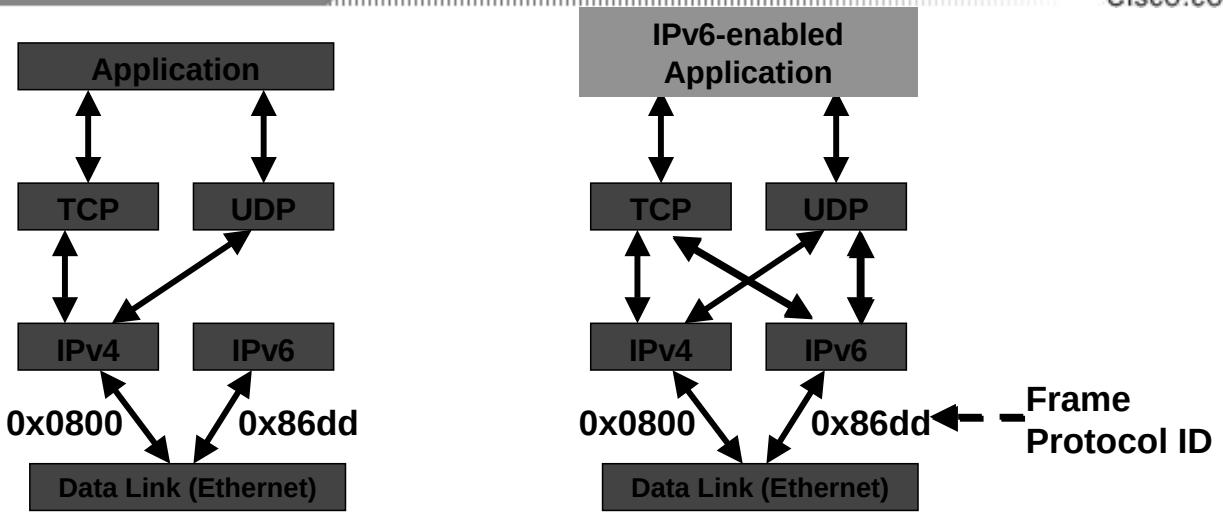
IPv6 protocol for Win XP features

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

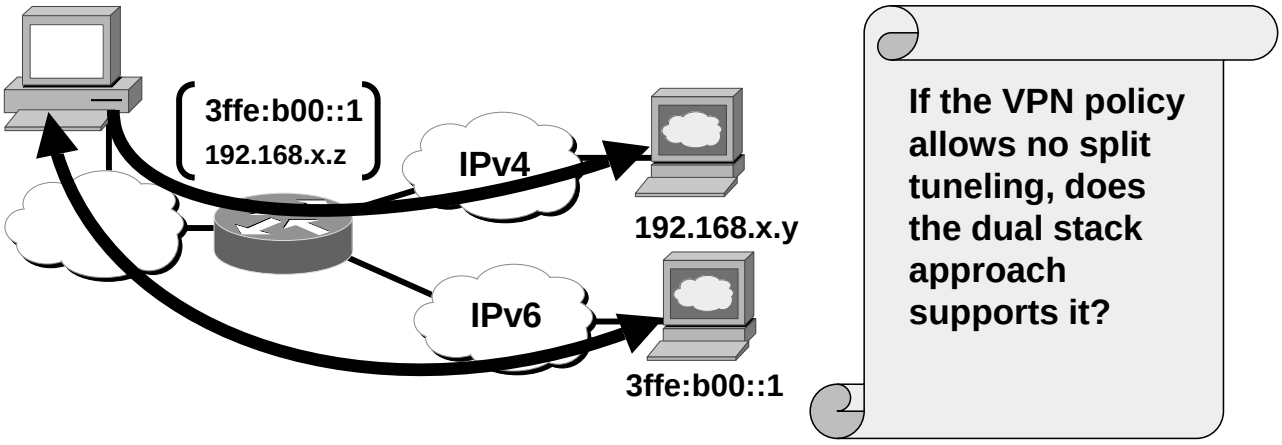
Cisco.com



- **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

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 to IPv6:

- www.kame.net
- www.bieringer.de/linux/IPv6
- www.hs247.com

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION