Computer Networks (CS F303)

BITS Pilani
Pilani Campus

Virendra Singh Shekhawat
Department of Computer Science and Information Systems

innovate achieve lead

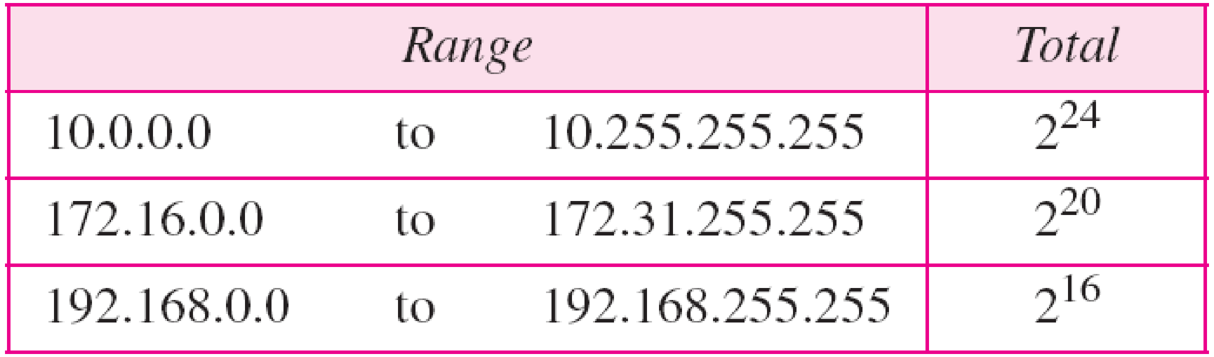
BITS Pilani
Pilani Campus

Second Semester 2020-2021
Module-4 <Network Layer>

Agenda

- NAT Firewall
- ICMP Protocol
- IPv6 Protocol

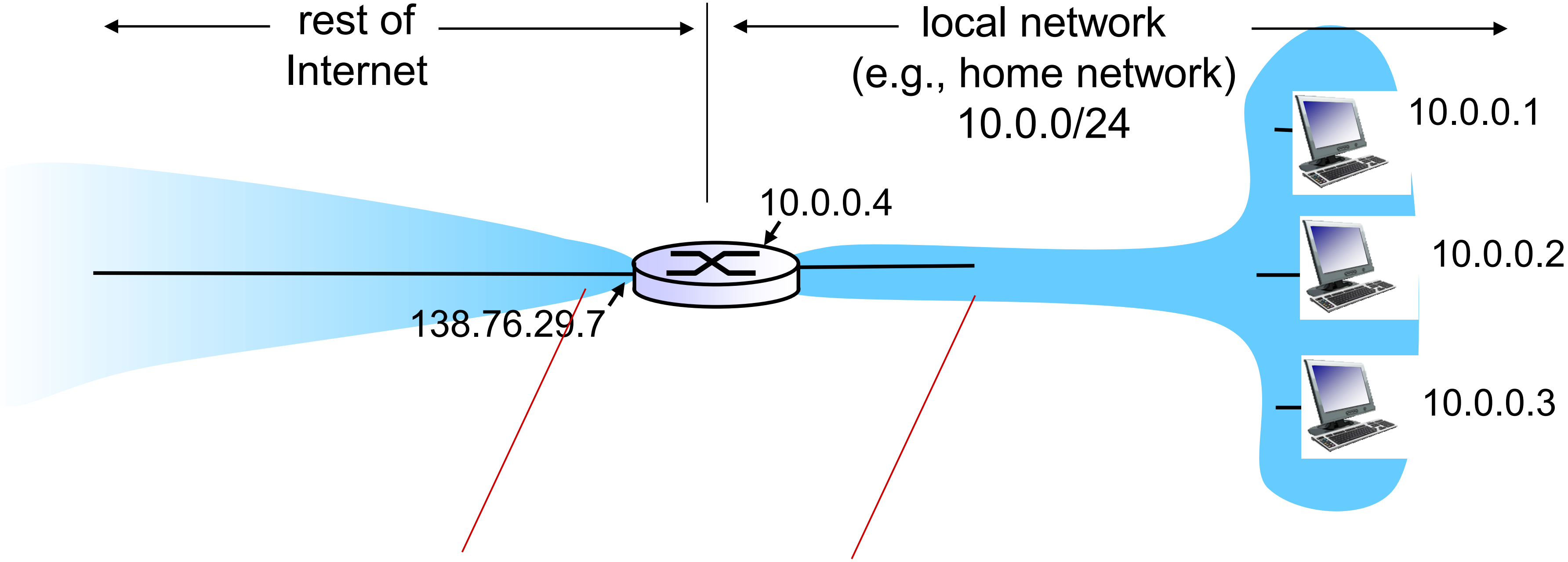
Network Address Translation (NAT)



Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

- *Motivation:* local network uses just one IP address as far as outside world is concerned
  - Can change addresses of devices in local network without notifying outside world
  - Can change ISP without changing addresses of devices in local network
  - Devices inside local net not explicitly addressable, visible by outside world (a security plus)

NAT: Motivation???



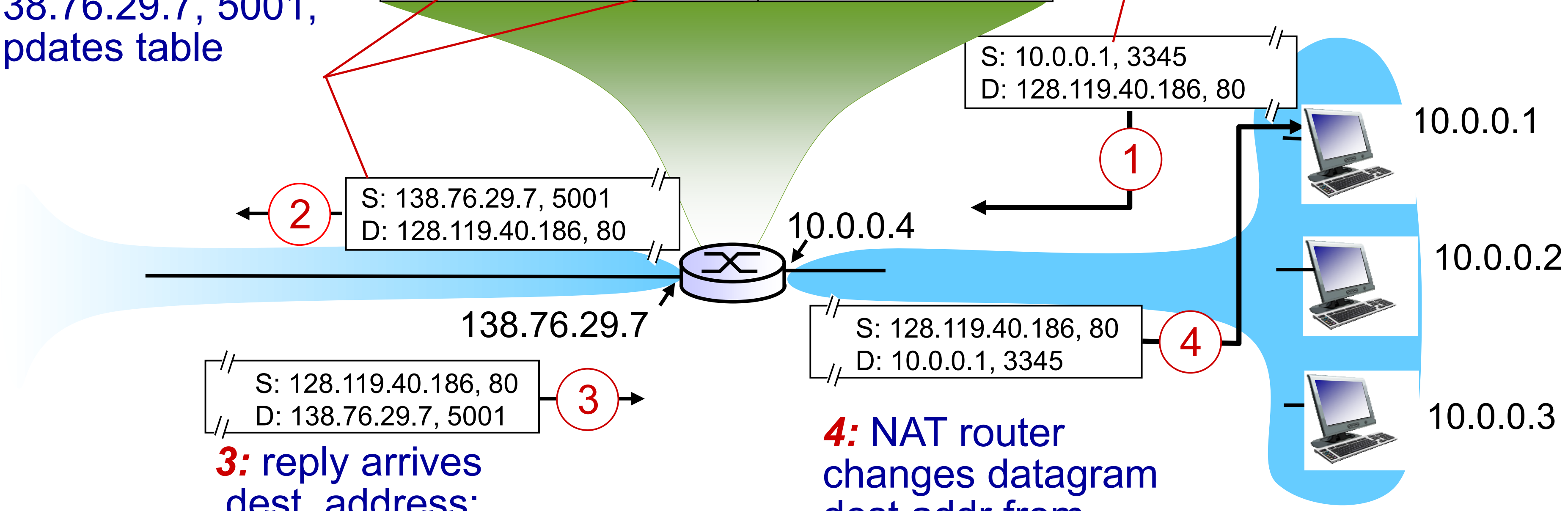
all datagrams *leaving* local network have *same* single source NAT IP address: 138.76.29.7,different source port numbers

datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

How it Works???

NAT translation table

WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……



1: host 10.0.0.1 sends datagram to 128.119.40.186, 80

2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

3: reply arrives dest. address: 138.76.29.7, 5001

4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

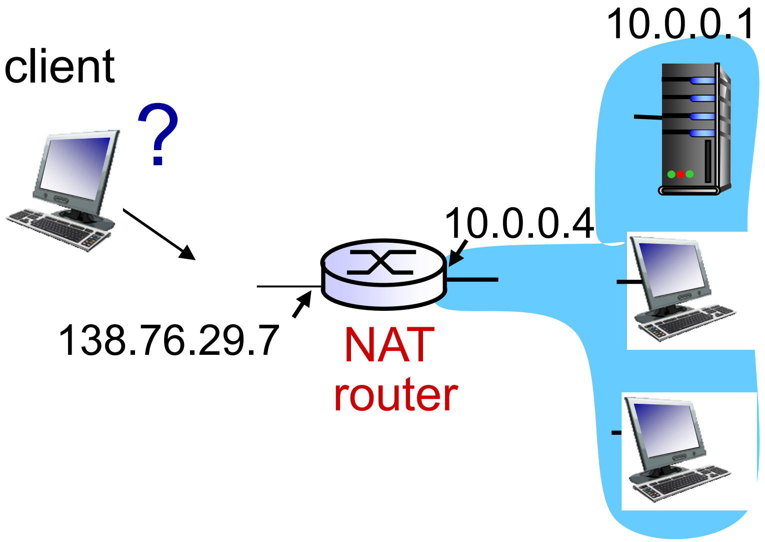
Facts about NAT

- 16-bit port-number field
  - How many devices can be connected?

- NAT is controversial
  - Routers should only process up to layer 3
  - Violates end-to-end argument
  - Address shortage should instead be solved by IPv6

NAT Traversal Problem

- Client wants to connect to server with address 10.0.0.1
  - Server address 10.0.0.1 local to LAN (client can't use it as destination address)
  - Only one externally visible NATed address: 138.76.29.7

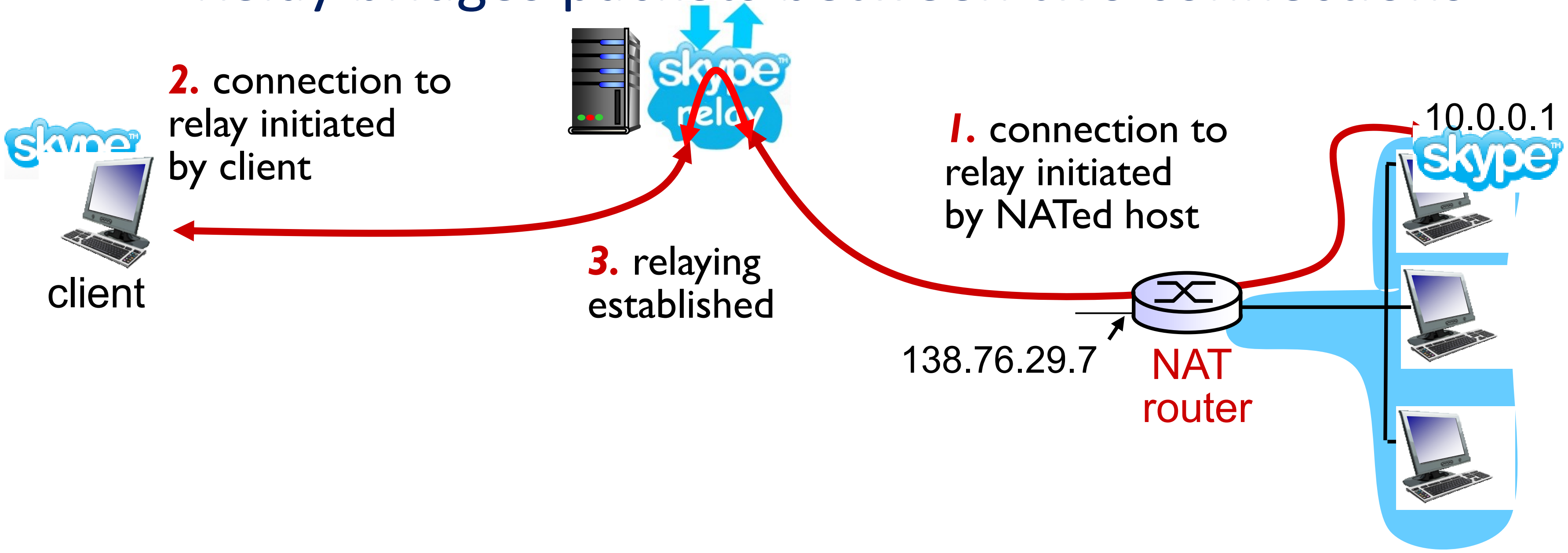


Solutions [.1]

- Statically configure NAT to forward incoming connection requests at given port to server
  - e.g., (138.76.29.7, port 25000) always forwarded to 10.0.0.1 port 25000
- Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATed host to:
  - Learn public IP address (138.76.29.7)
  - e.g., BitTorrent application in the host asks NAT to create a hole that maps (10.0.0.1,3345) to (138.76.29.7,5001)
  - Add/remove port mappings (with lease times)

Solutions [..2]

- Relaying (used in Skype)
  - NATed client establishes connection to relay
  - External client connects to relay
  - Relay bridges packets between two connections

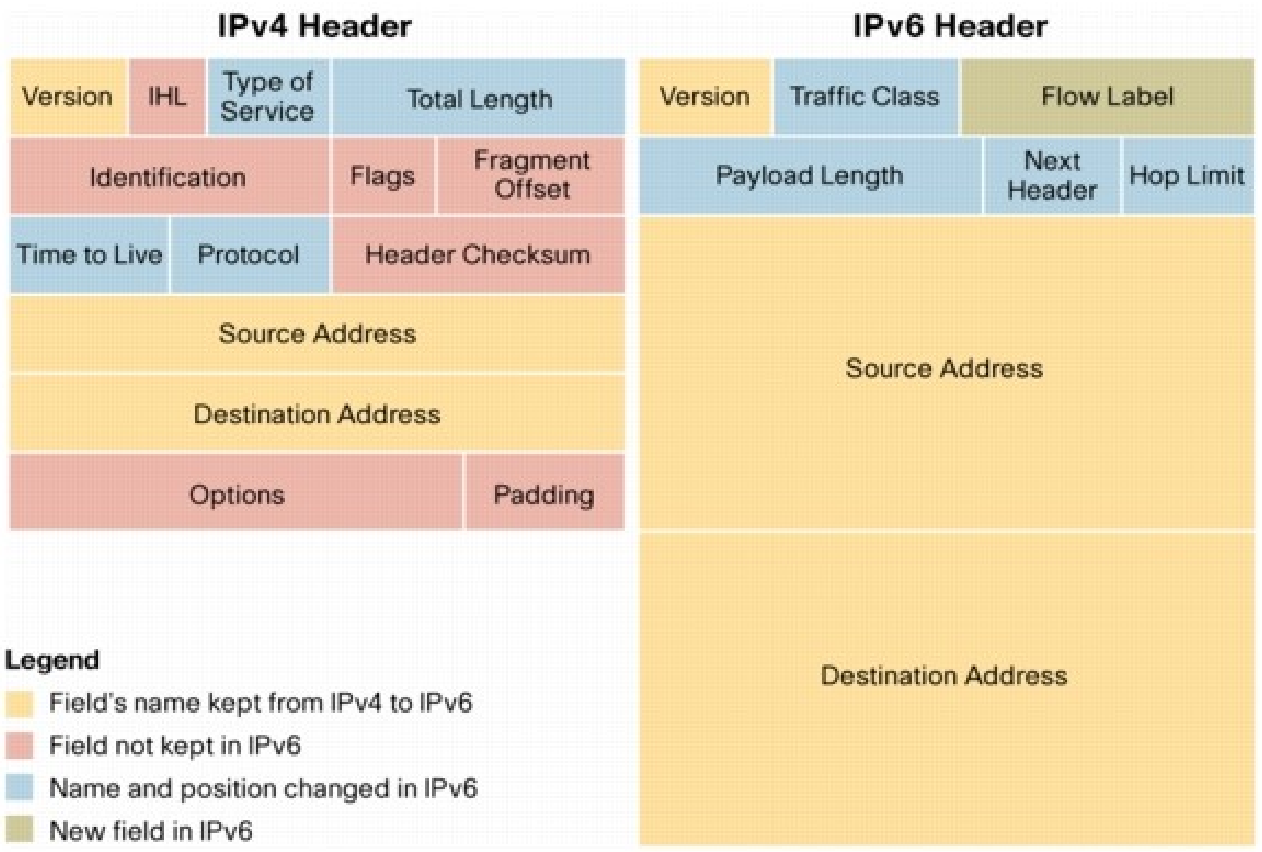


skype relay
2. connection to relay initiated by client
skype
client
3. relaying established
1. connection to relay initiated by NATed host
10.0.0.1
skype
138.76.29.7
NAT router

IPv6 Motivation

- ***Initial Motivation:*** 32-bit address space soon to be completely allocated.
- Additional motivation:
  - Header format helps speed processing/forwarding
  - Header changes to facilitate QoS
- *IPv6 datagram format:*
  - Fixed-length 40 byte header
  - No fragmentation allowed
- Ipv6 deployment status
  - https://en.wikipedia.org/wiki/IPv6_deployment

IPv4 vs IPv6



IPv4 Header

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options | Padding

IPv6 Header

Version | Traffic Class | Flow Label

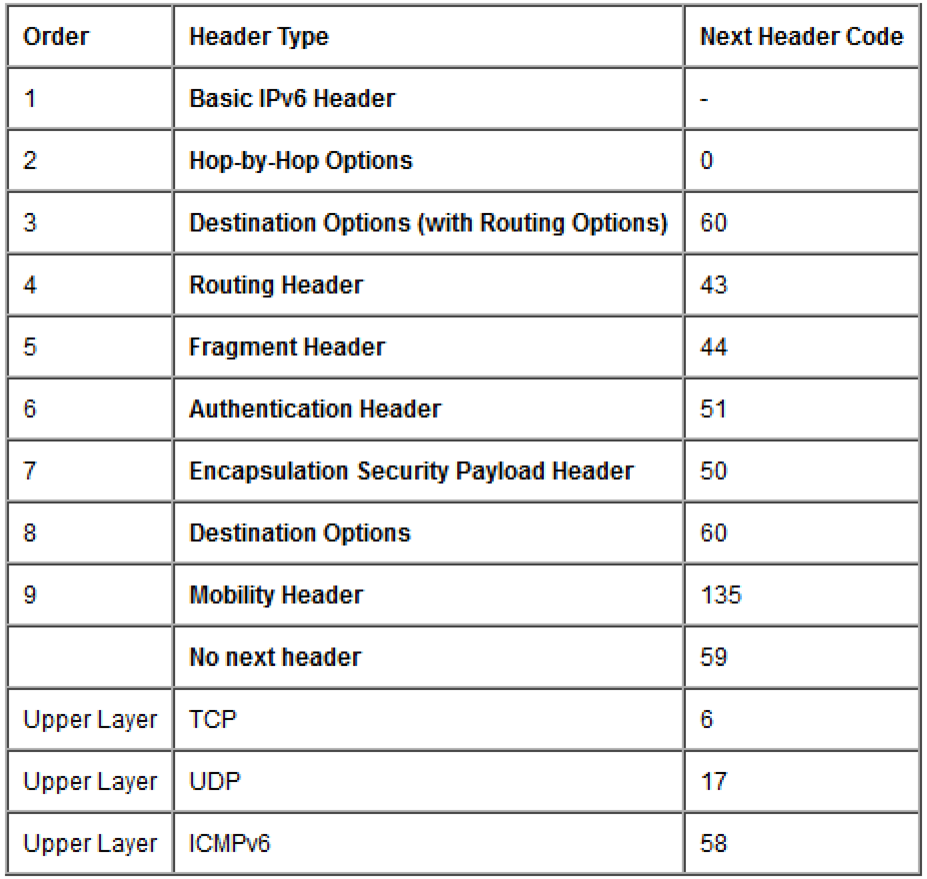
Payload Length | Next Header | Hop Limit

Source Address

Destination Address

Legend

- 🟨 Field's name kept from IPv4 to IPv6
- 🟥 Field not kept in IPv6
- 🟦 Name and position changed in IPv6
- 🟩 New field in IPv6

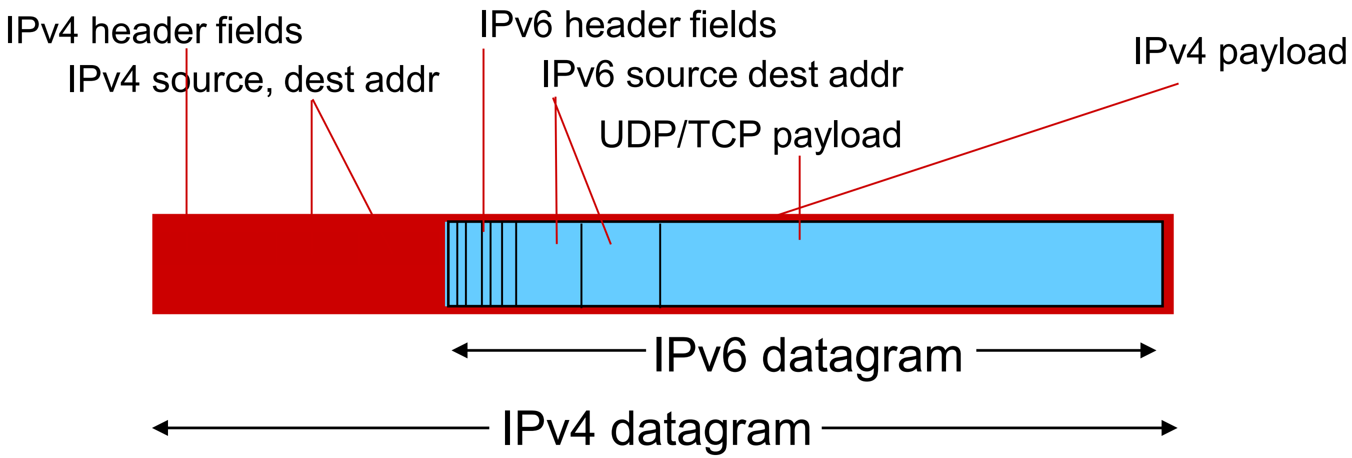


Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

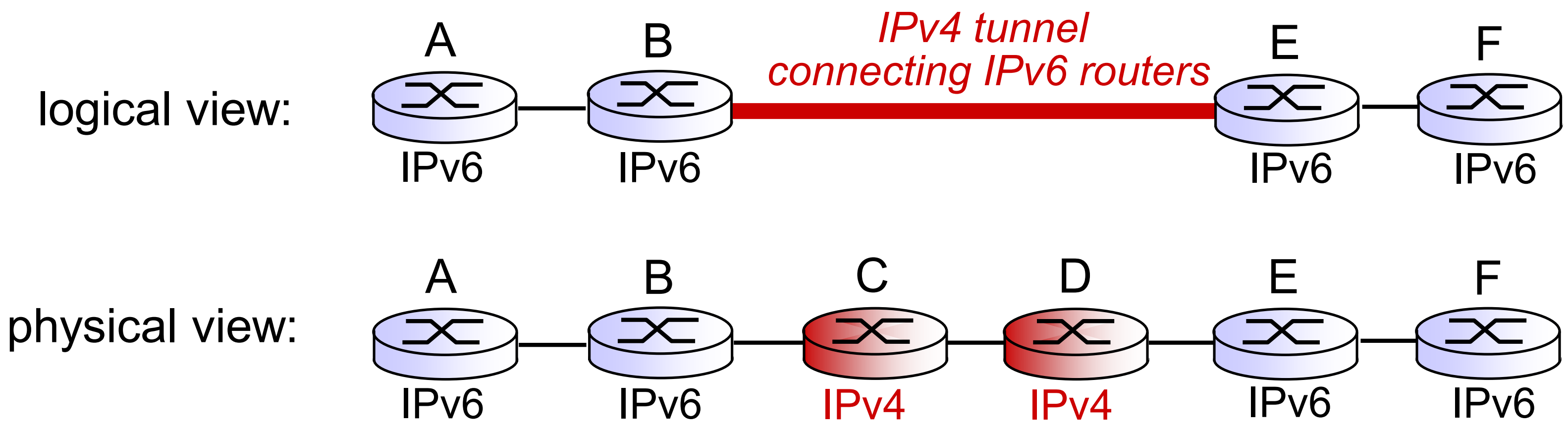
Source: www.cisco.com

Transition from IPv4 to IPv6

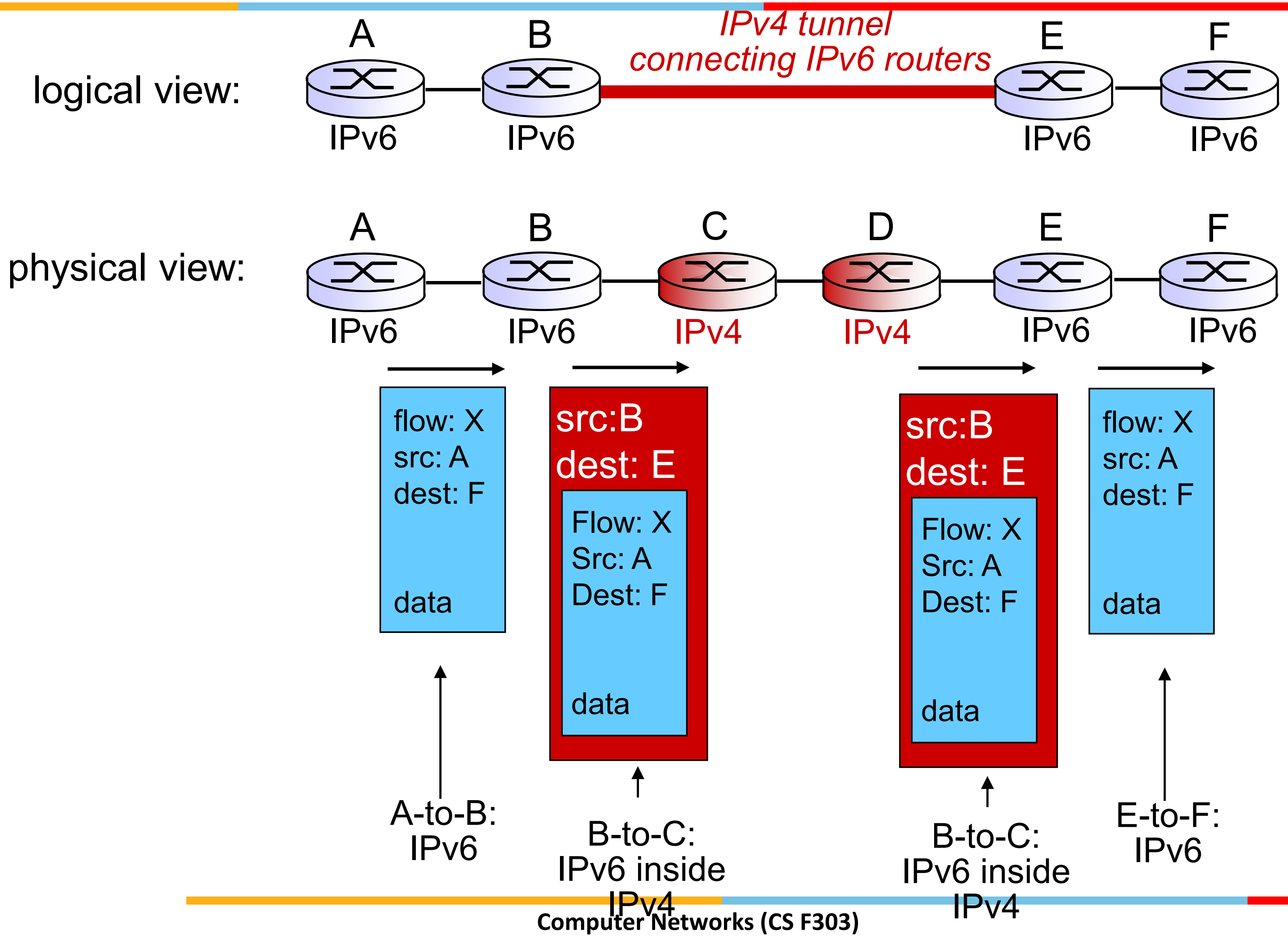
- Not all routers can be upgraded simultaneously
  - No “flag days”
  - How will network operate with mixed IPv4 and IPv6 routers?
- *Tunneling:* IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers



Tunneling [.1]

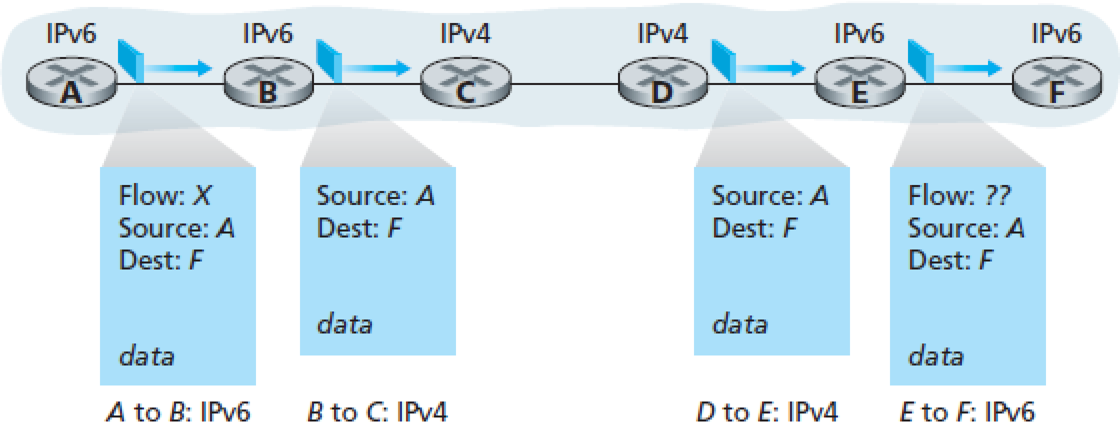

IPv4 tunnel
connecting IPv6 routers
logical view:
A
B
E
F
IPv6
IPv6
IPv6
IPv6
physical view:
A
B
C
D
E
F
IPv6
IPv6
IPv4
IPv4
IPv6
IPv6

Tunneling [..2]



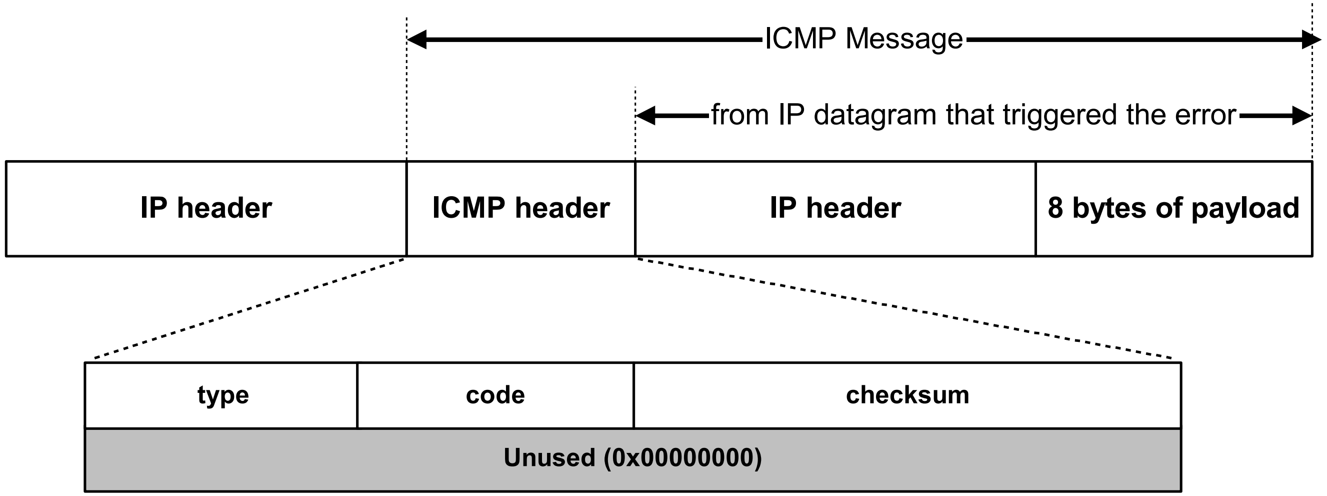
logical view:
A
B
IPv4 tunnel
connecting IPv6 routers
E
F
IPv6
IPv6
IPv6
IPv6
physical view:
A
B
C
D
E
F
IPv6
IPv6
IPv4
IPv4
IPv6
IPv6
flow: X
src: A
dest: F
data
src:B
dest: E
Flow: X
Src: A
Dest: F
data
src:B
dest: E
Flow: X
Src: A
Dest: F
data
flow: X
src: A
dest: F
data
A-to-B:
IPv6
B-to-C:
IPv6 inside
IPv4
B-to-C:
IPv6 inside
IPv4
E-to-F:
IPv6

Dual Stack Approach



ICMP Protocol

- The **Internet Control Message Protocol (ICMP)** is a helper protocol that supports IP with facility for
  - Error reporting and Simple queries
  - Used by hosts and routers to communicate network layer information to each other
- ICMP lies just above IP
  - ICMP messages are encapsulated as IP datagrams

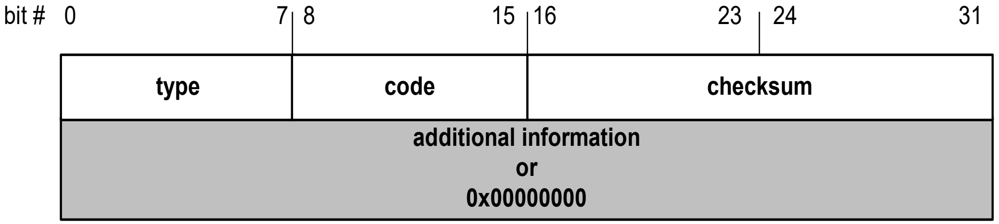


ICMP Message

from IP datagram that triggered the error

IP header	ICMP header	IP header	8 bytes of payload

type	code	checksum
Unused (0x00000000)		



type	code	checksum
additional information or 0x00000000		

When a host receives an IP packet with ICMP specified as the upper layer protocol, it de-multiplexes the packet to ICMP, just as it would de-multiplex a packet to TCP/UDP

ICMP Message Types

Type	Message Type	Description
3	Destination Unreachable	Packet could not be delivered
11	Time Exceeded	Time to live field hit 0
12	Parameter Problem	Invalid header field
4	**Source Quench**	Choke Packet
5	Redirect	Teach a router about geography
8	Echo	Ask a machine if it is alive
0	Echo Reply	Yes, I am alive
13	Timestamp Request	Same as Echo request, but with timestamp
14	Timestamp Reply	Same as Echo reply, but with timestamp

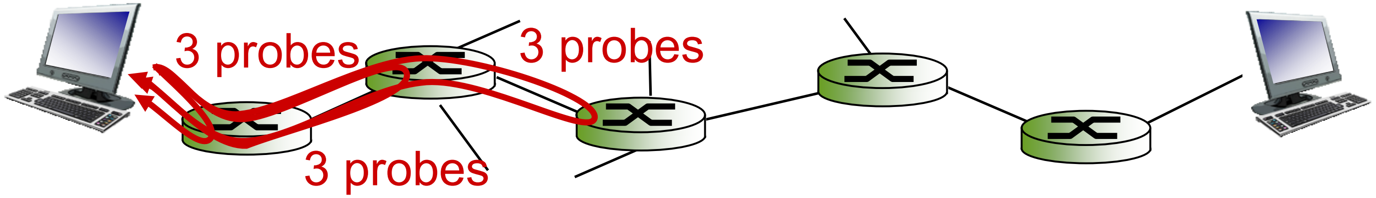
Code	Definition
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation needed & Don’t Fragment was set
5	Source Route failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication Destination Network is Administratively Prohibited
10	Communication Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence Cutoff Violation

Traceroute and ICMP

- Source sends series of UDP segments to dest
  - first set has TTL =1
  - second set has TTL=2, etc.
  - unlikely port number
- When *n*th set of datagrams arrives to nth router:
  - router discards datagrams
  - and sends source ICMP messages (type 11, code 0)
  - ICMP messages includes name of router & IP address
- When ICMP messages arrives, source records RTTs

Stopping criteria:

- UDP segment eventually arrives at destination host
- Destination returns ICMP "port unreachable" message (type 3, code 3)
- Source stops



Thank You!