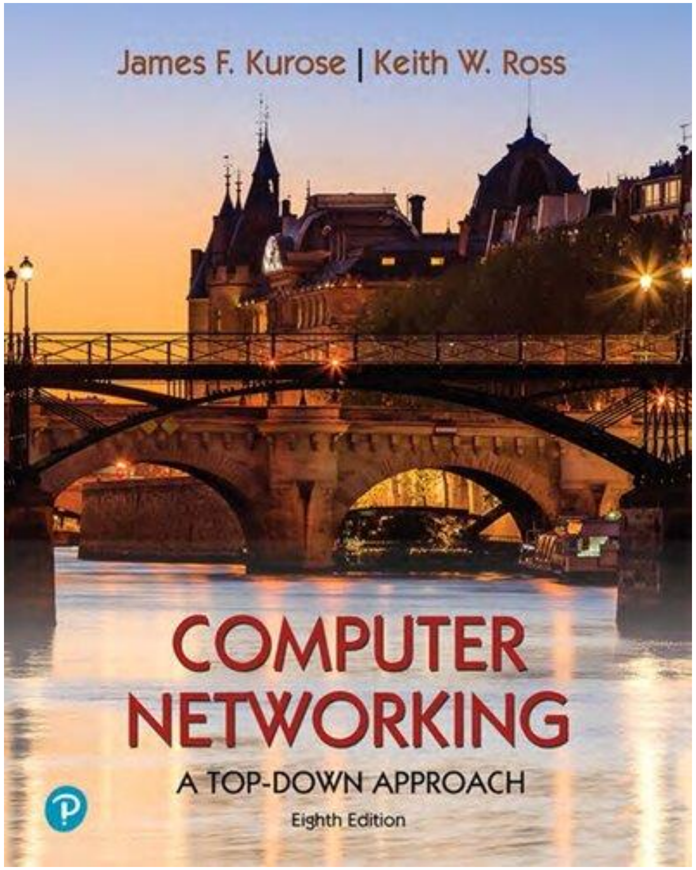
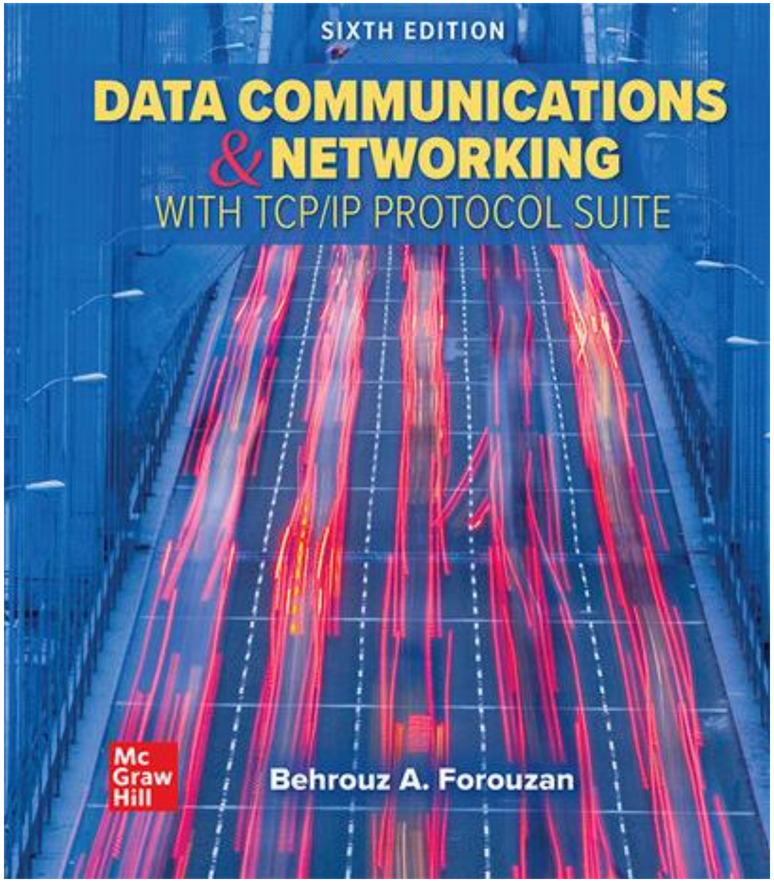
الجامعة اللبنانية
UNIVERSITE LIBANAISE

I3304
Network administration and security

Ahmad Fadlallah

Reference Textbooks





Outline

- Introduction
  - Introduction to the course
  - Recall Network Basics (I2208)
- Network Layer
  - Static Routing
  - Dynamic Routing
    - Dynamic Routing Algorithm
    - Dynamic Routing Protocols
  - NAT (Network Address Translation)
  - IPv6
- Transport Layer
  - Function of the transport layer
  - UDP Protocol
  - TCP Protocol
    - Connection management
    - Flow control
    - Congestion control
- Application Layer
  - HTTP protocol
  - FTP protocol
  - Mail protocols
  - DNS
- Introduction to Security
  - Security services
  - Cryptography
  - Digital Signature
  - Principle of network security protocols

References

- The slides are based on the:
  - Jim Kurose, Keith Ross Slides for the Computer Networking: A Top-Down Approach, 8th edition, Pearson, 2020

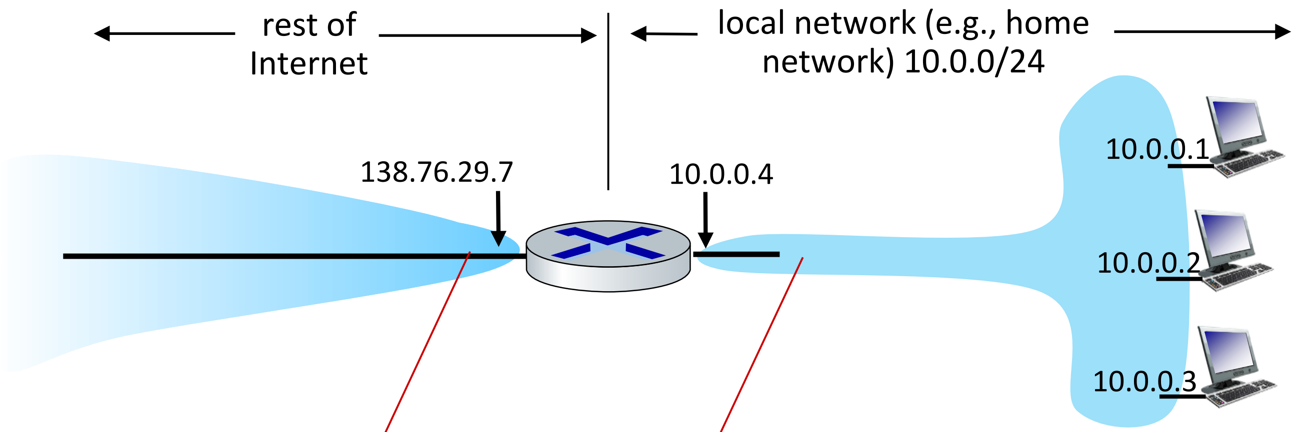
Network Layer
Network Address Translation (NAT)

Motivation

- Every IP-capable device needs an IP address
- Proliferation of Small Office, Home Office (SOHO) subnets
- Need to allocate a range of addresses (by the ISP) to cover all of the SOHO's IP devices (including phones, tablets, gaming devices, IP TVs, printers and more)
  - The address block size depends on the number of devices
- But what if the ISP had already allocated the contiguous portions of the SOHO network's current address range?
- Is the public IPv4 address space sufficient for all connected devices?

NAT: Network Address Translation

- NAT: all devices in local network share just one IPv4 address as far as outside world is concerned



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

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

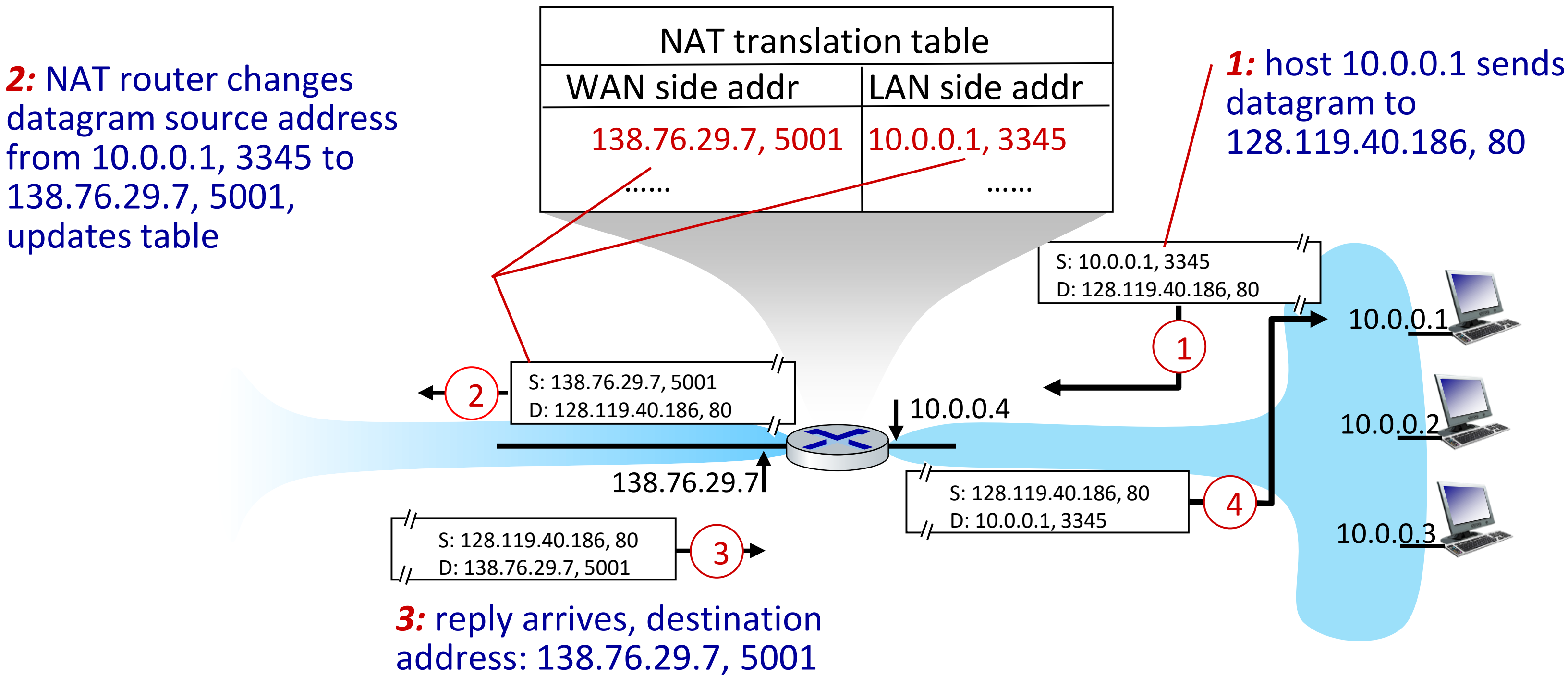
NAT: Network Address Translation

- All devices in local network have 32-bit addresses in a “private” IP address space (10/8, 172.16/12, 192.168/16 prefixes) that can only be used in local network
- **Advantages**:
  - Just one IP address needed from provider ISP for all devices
  - Can change addresses of host in local network without notifying outside world
  - Can change ISP without changing addresses of devices in local network
  - **Security**: devices inside local network not directly addressable → not visible by outside world

NAT: Network Address Translation

- Implementation: NAT router must (transparently):
  - **Outgoing datagrams:** Replace *(source IP address, port #)* of every outgoing datagram to *(NAT IP address, new port #)*
    - Remote clients/servers will respond using *(NAT IP address, new port #)* as destination address
  - Remember (in **NAT translation table**) every *(source IP address, port #)* to *(NAT IP address, new port #)* translation pair
  - **Incoming datagrams:** Replace *(NAT IP address, new port #)* in destination fields of every incoming datagram with corresponding *(source IP address, port #)* stored in NAT table

NAT: Network Address Translation



NAT: network address translation

- NAT has been **controversial**:
  - ⊙**Routers "should" only process up to layer 3**
    - Port numbers are meant to be used for addressing processes, not for addressing hosts.
  - ⊙**Address "shortage" should be solved by IPv6**
  - ⊙**Violates end-to-end argument** (port # manipulation by network-layer device)
  - ⊙**NAT traversal**: what if client wants to connect to server behind NAT?
- But NAT is here to stay:
  - ⊙Extensively used in home and institutional nets, 4G/5G cellular nets

Network Layer
Internet Protocol version 6 (IPv6)

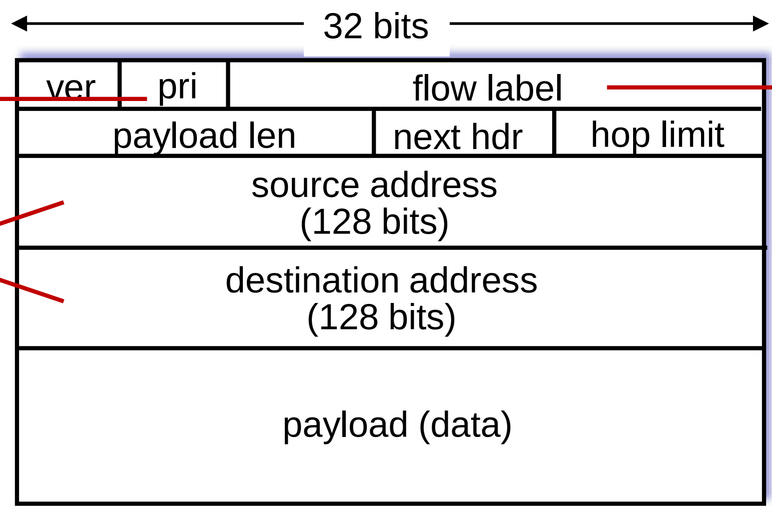
IPv6: motivation

- **Initial Motivation:** 32-bit IPv4 address space would be completely allocated
- The designers of IPv6 also took this opportunity to tweak and augment other aspects of IPv4, based on the accumulated operational experience with IPv4.
- Additional motivation:
  - Speed processing/forwarding: 40-byte fixed length header
  - enable different network-layer treatment of “flows”

IPv6 datagram format

priority: identify priority among datagrams in flow

128-bit IPv6 addresses



flow label: identify datagrams in same "flow.” (concept of “flow” not well defined).

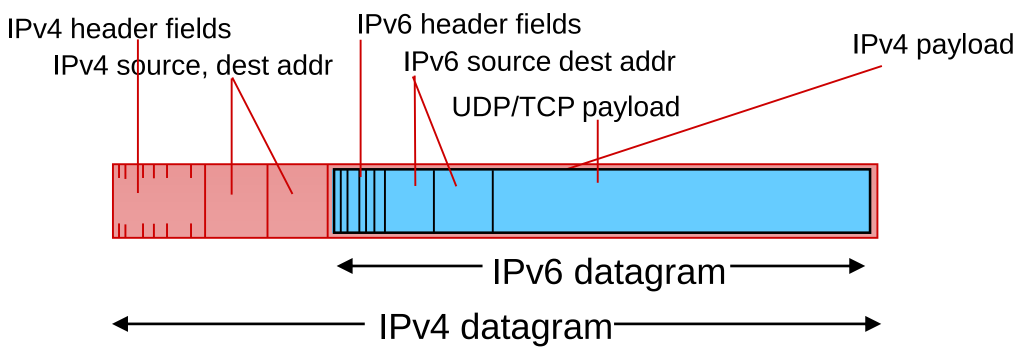
What’s missing (compared with IPv4):

- No checksum (to speed processing at routers)
- No fragmentation/reassembly
- No options (available as upper-layer, next-header protocol at router)

Transition from IPv4 to IPv6

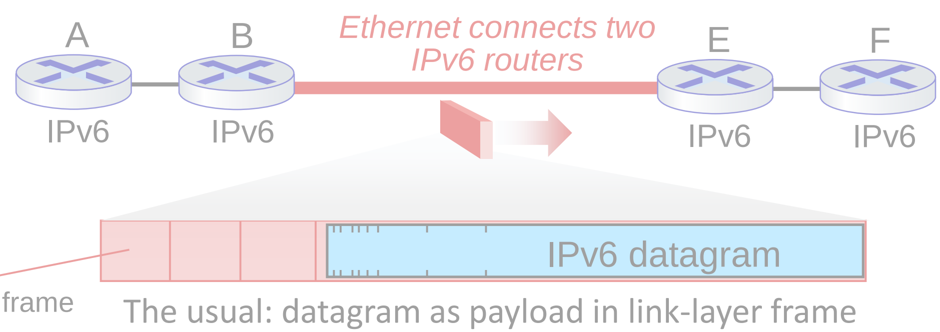
- Not all routers can be upgraded simultaneously
  - ⊙No “flag days”
  - ⊙How will network operate with mixed IPv4 and IPv6 routers?

- Tunneling: IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers (“packet within a packet”)
  - tunneling used extensively in other contexts (4G/5G)

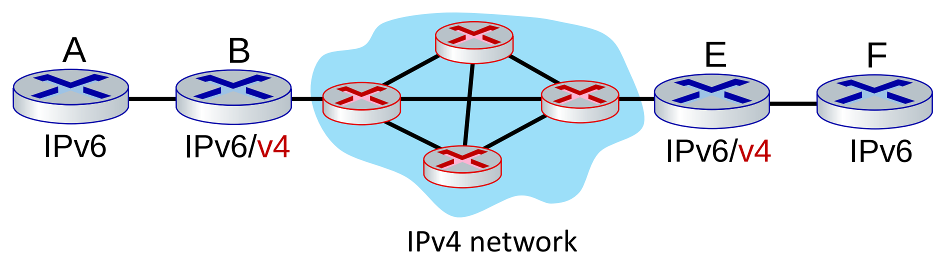


Tunneling and encapsulation

Ethernet connecting two IPv6 routers:

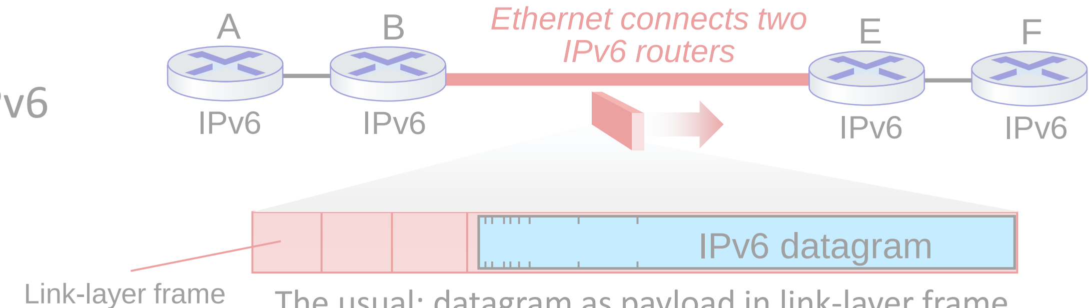


IPv4 network connecting two IPv6 routers



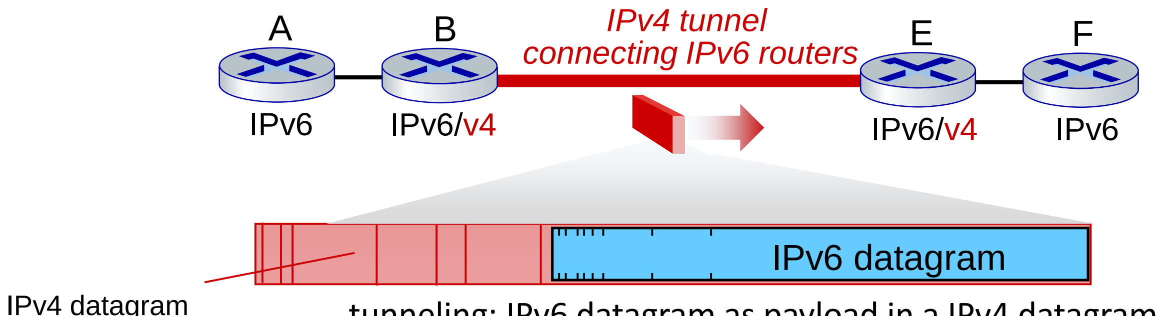
Tunneling and encapsulation

Ethernet connecting two IPv6 routers:



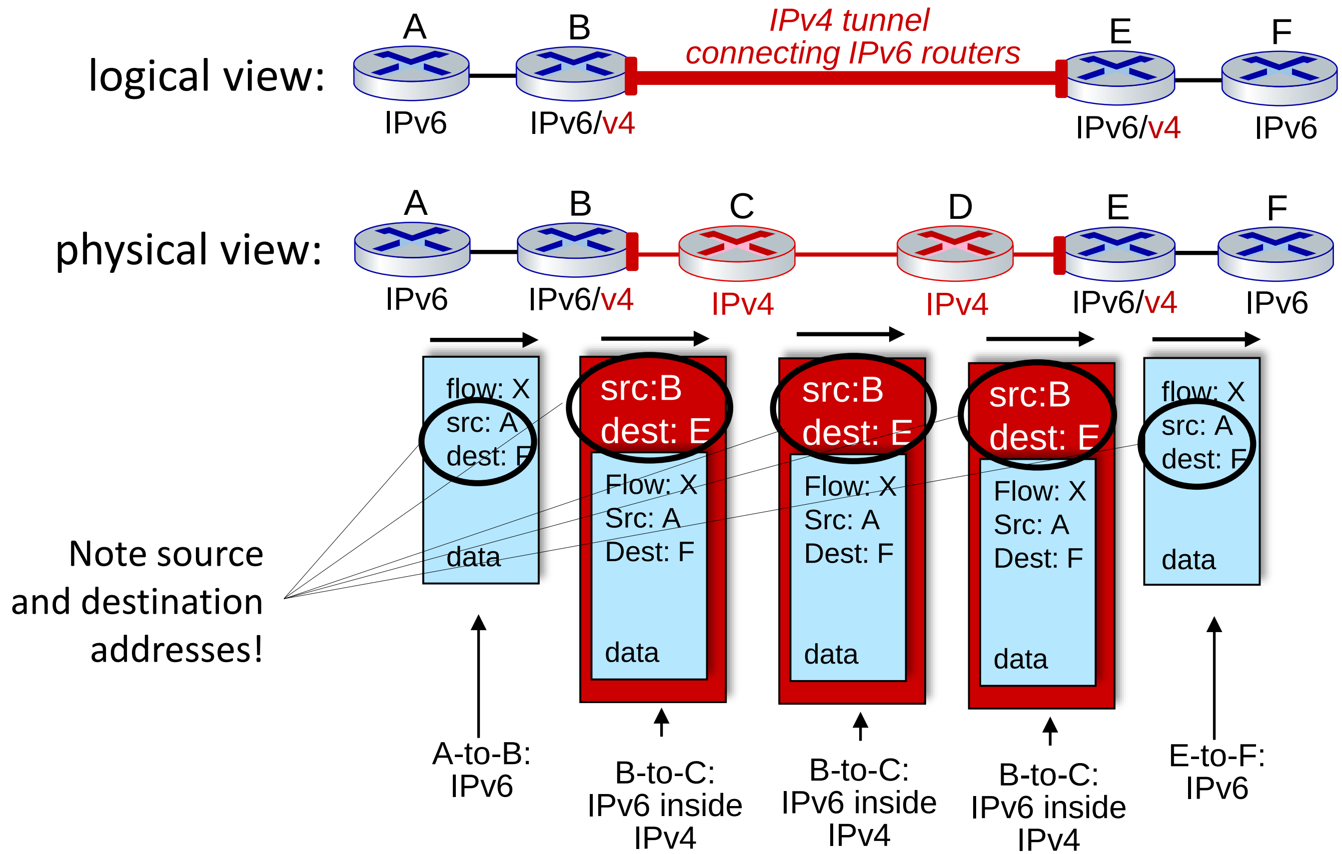
The usual: datagram as payload in link-layer frame

IPv4 tunnel connecting two IPv6 routers



tunneling: IPv6 datagram as payload in a IPv4 datagram

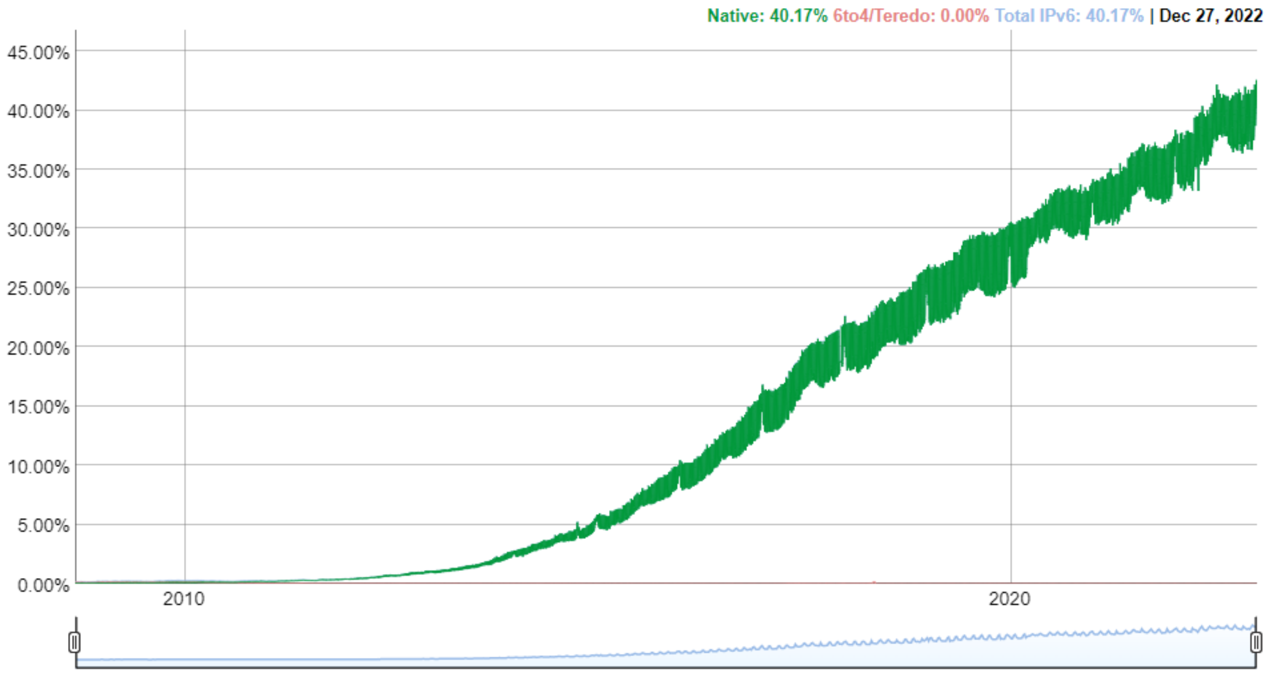
Tunneling



logical view:
A
B
IPv4 tunnel
connecting IPv6 routers
E
F
IPv6
IPv6/v4
IPv6/v4
IPv6
physical view:
A
B
C
D
E
F
IPv6
IPv6/v4
IPv4
IPv4
IPv6/v4
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
src:B
dest: E
Flow: X
Src: A
Dest: F
data
flow: X
src: A
dest: F
data
Note source
and destination
addresses!
A-to-B:
IPv6
B-to-C:
IPv6 inside
IPv4
B-to-C:
IPv6 inside
IPv4
B-to-C:
IPv6 inside
IPv4
E-to-F:
IPv6

IPv6: adoption

- Google[1]: ~ 40% of clients access services via IPv6
- NIST: 1/3 of all US government domains are IPv6 capable



1 https://www.google.com/intl/en/ipv6/statistics.html

IPv6: adoption

- Google[1]: ~ 40% of clients access services via IPv6
- NIST: 1/3 of all US government domains are IPv6 capable
- Long (long!) time for deployment, use
  - 25 years and counting!
  - think of application-level changes in last 25 years: WWW, social media, streaming media, gaming, telepresence, …
  - *Why?*

[1] https://www.google.com/intl/en/ipv6/statistics.html