National University of Computer & Emerging Sciences

CS 3001 - COMPUTER NETWORKS

Lecture 19

Chapter 4

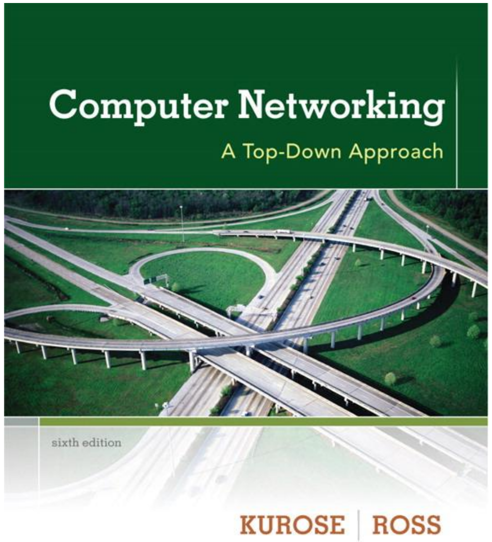
27th October, 2022

Nauman Moazzam Hayat

nauman.moazzam@lhr.nu.edu.pk

Office Hours: 02:30 pm till 06:00 pm (Every Tuesday & Thursday)

Chapter 4
Network Layer



Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Chapter 4: outline

4.1 introduction

4.2 virtual circuit and datagram networks

4.3 what's inside a router

4.4 IP: Internet Protocol
- datagram format
- IPv4 addressing
- ICMP
- IPv6

4.5 routing algorithms
- link state
- distance vector
- hierarchical routing

4.6 routing in the Internet
- RIP
- OSPF
- BGP

4.7 broadcast and multicast routing

IP addresses: how to get one?

Q: How does a *host* get IP address?

- hard-coded by system admin in a file
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play"

DHCP: Dynamic Host Configuration Protocol

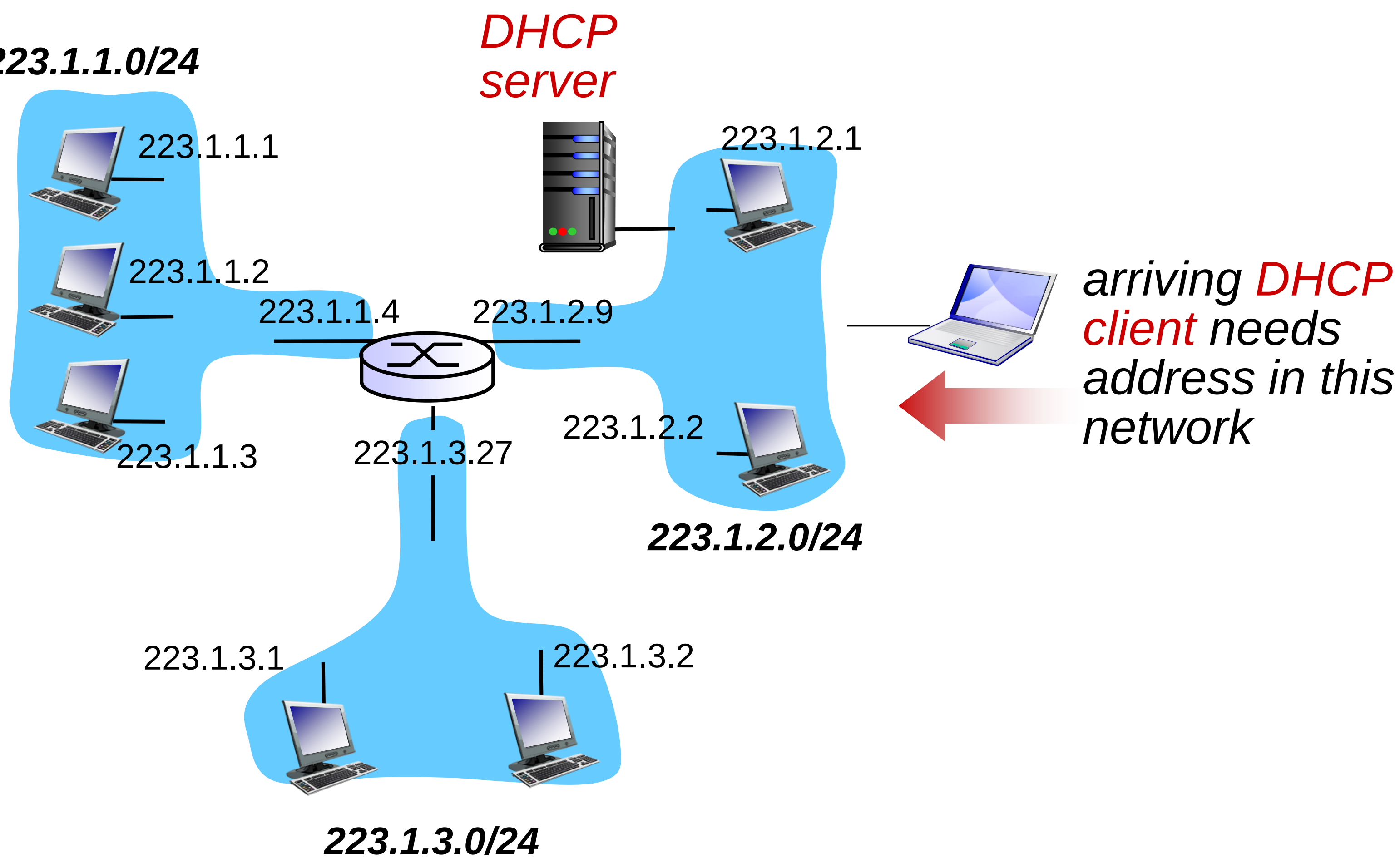
goal: allow host to *dynamically* obtain its IP address from network server when it joins network

- can renew its lease on address in use
- allows reuse of addresses (only hold address while connected/"on")
- support for mobile users who want to join network (more shortly)
- App layer protocol used by the Network Layer
- DHCP uses UDP at the Transport Layer

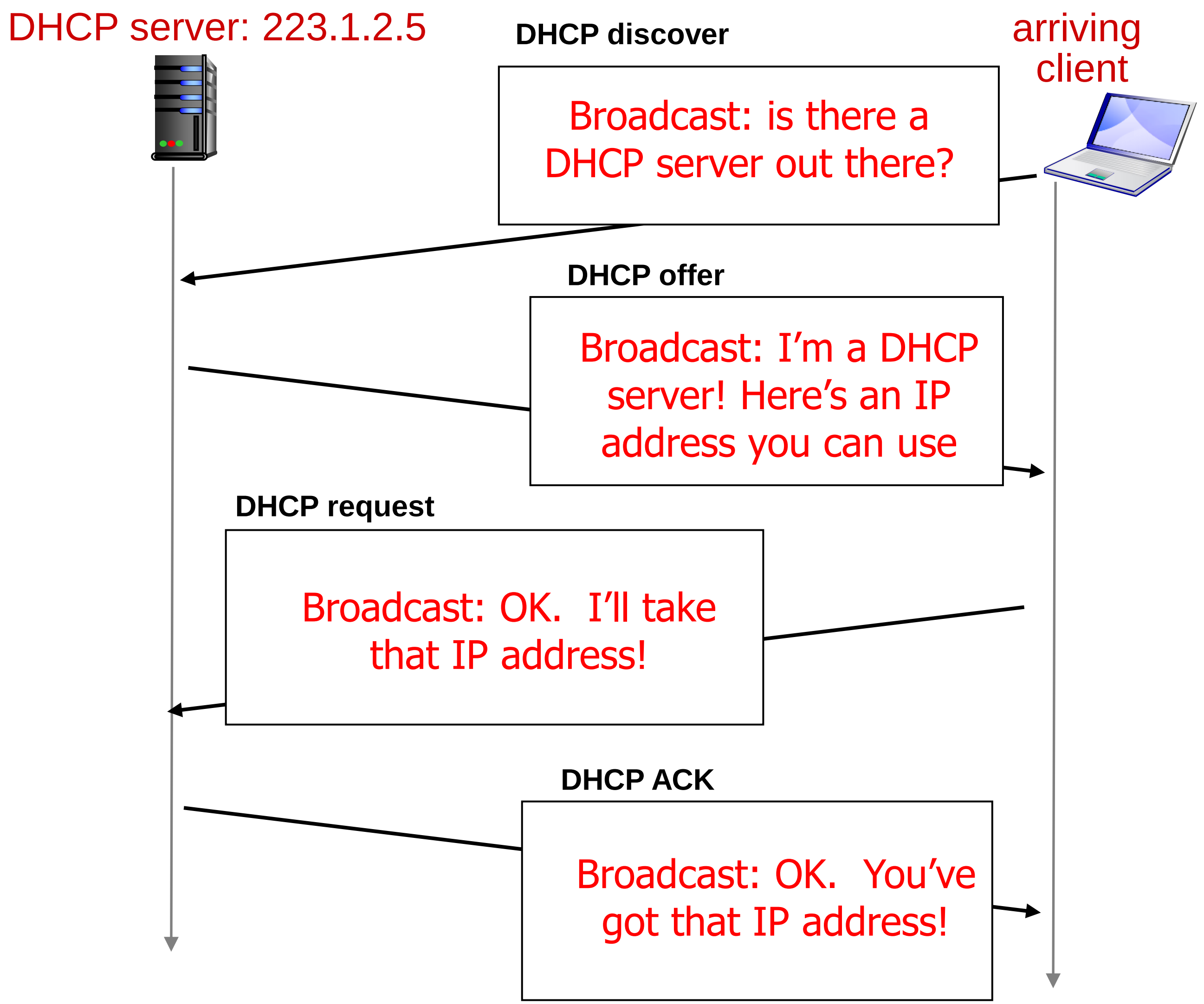
DHCP overview (DHCP Summary):

- host broadcasts "DHCP discover" msg [optional]
- DHCP server(s) responds with "DHCP offer" msg [optional]
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

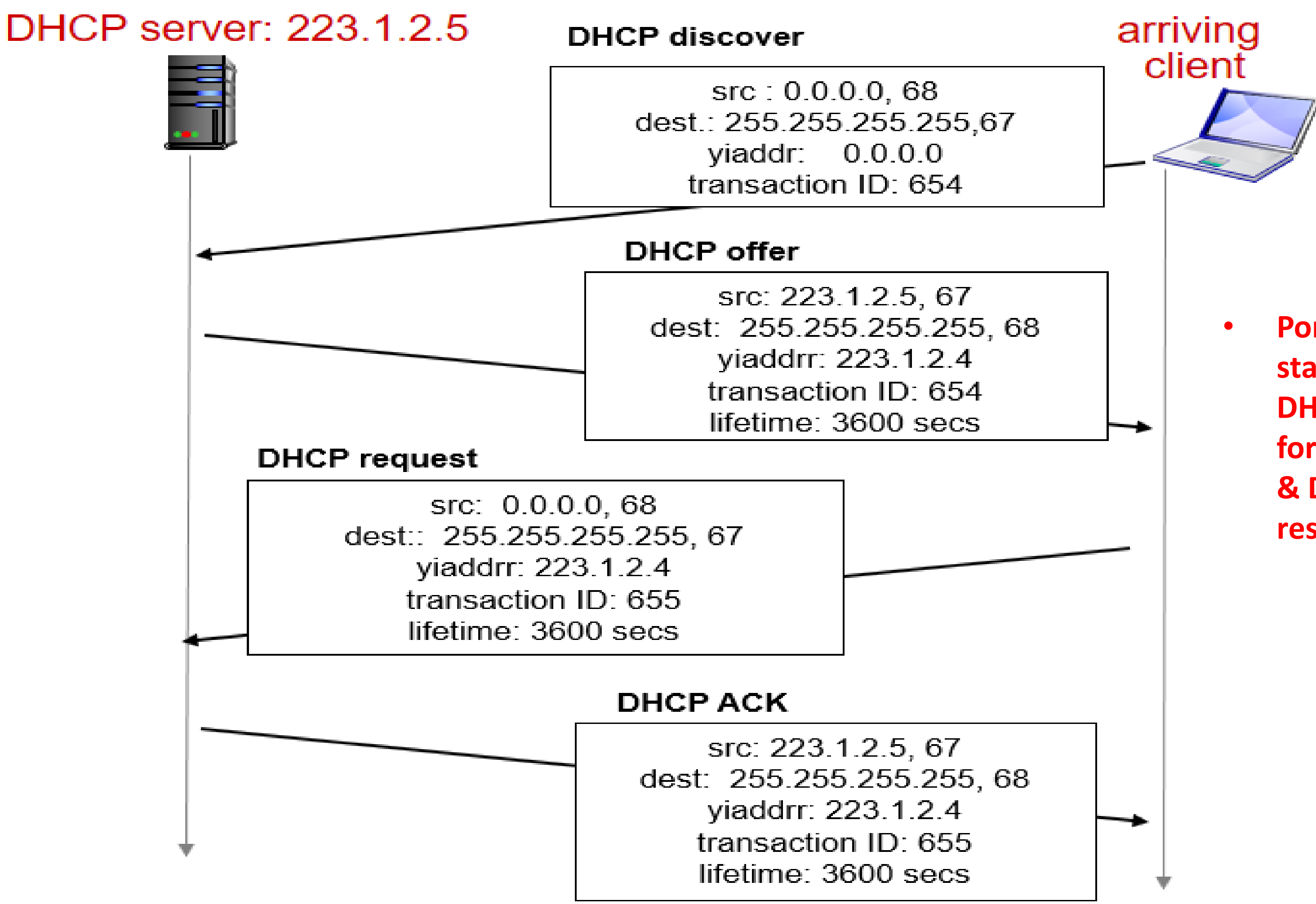
DHCP client-server scenario



DHCP client-server scenario



DHCP client-server scenario



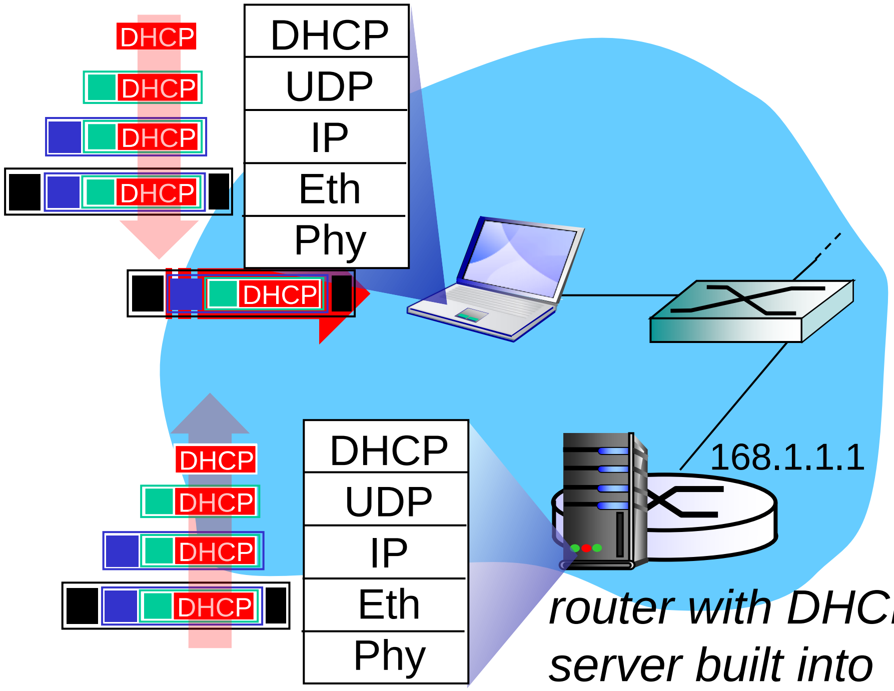
- **Port 67 & 68 are standard ports in DHCP Protocol for DHCP Server & DHCP Client respectively**

DHCP: more than IP addresses

DHCP can return more than just allocated IP address on subnet:

- address of first-hop router for client
- name and IP address of DNS sever
- network mask (indicating network versus host portion of address)

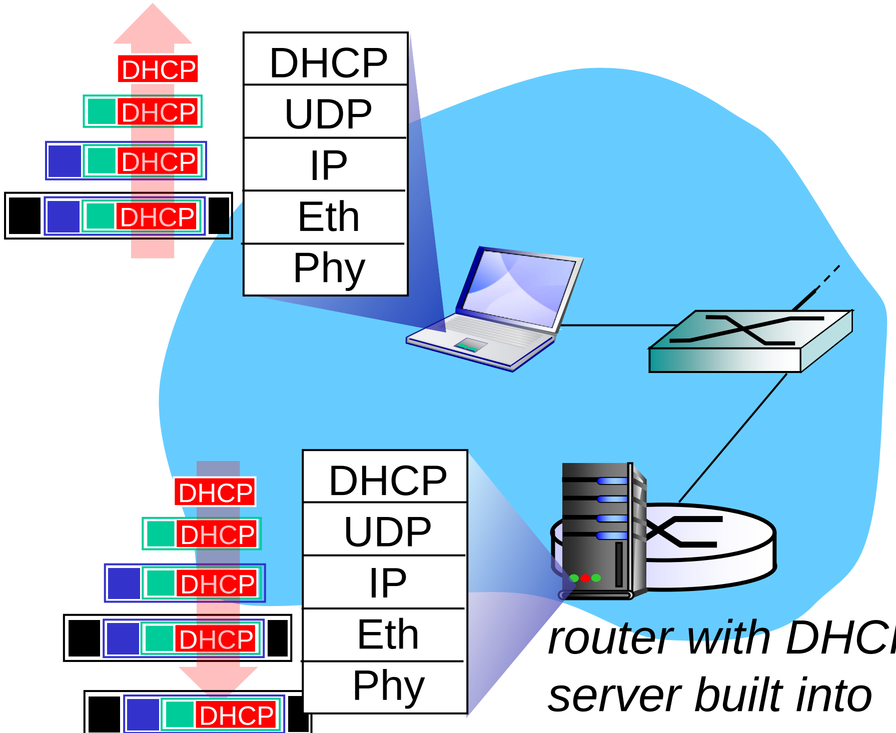
DHCP: example



router with DHCP server built into router

- connecting laptop needs its IP address, addr of first-hop router, addr of DNS server: use DHCP
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.1 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demuxed to IP demuxed, UDP demuxed to DHCP

DHCP: example



router with DHCP server built into router

- DCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- encapsulation of DHCP server, frame forwarded to client, demuxing up to DHCP at client
- client now knows its IP address, name and IP address of DNS server, IP address of its first-hop router

IP addresses: how to get one?

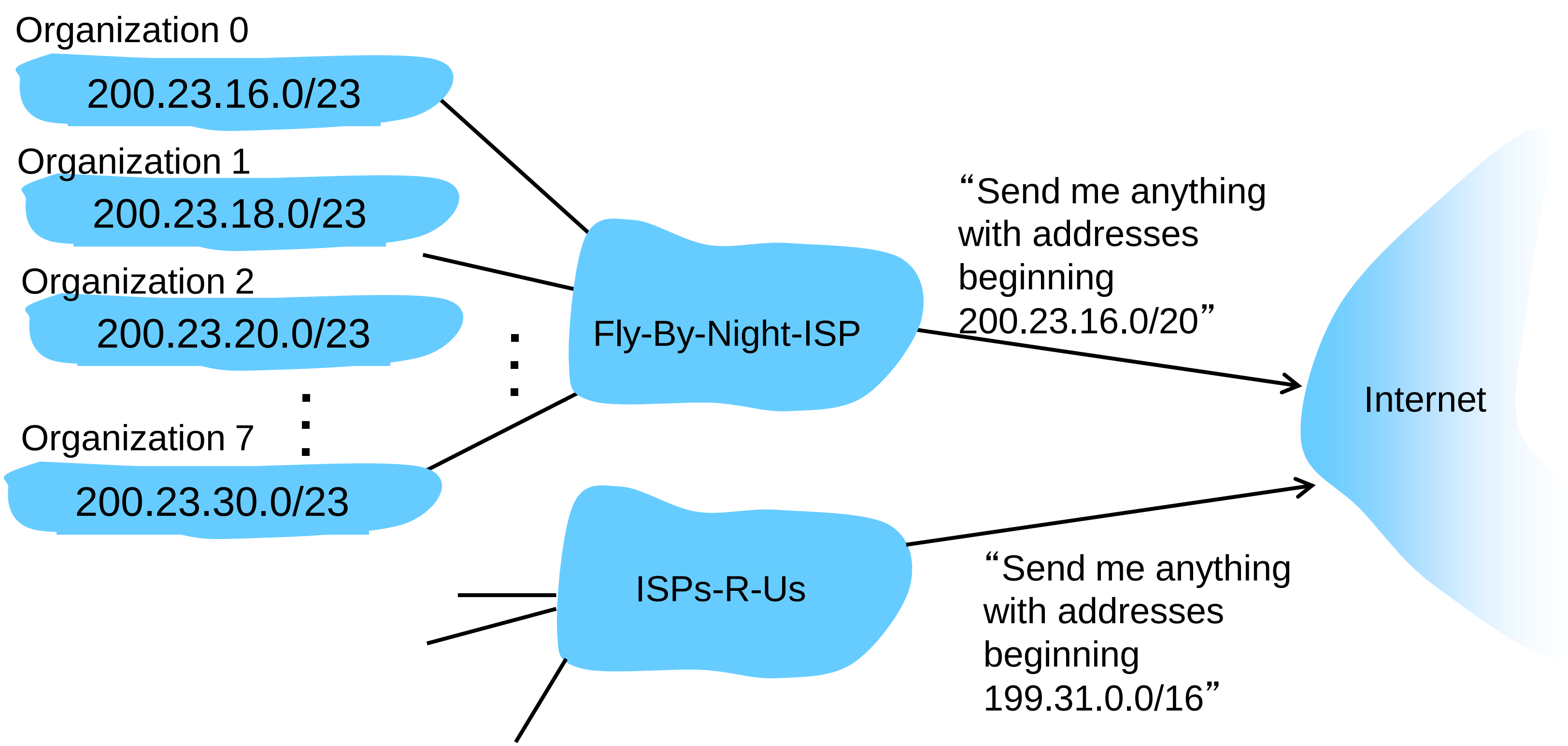
Q: how does *network* get subnet part of IP addr?

A: gets allocated portion of its provider ISP's address space

ISP's block	<u>11001000 00010111 0001</u>0000 00000000	200.23.16.0/20
Organization 0	<u>11001000 00010111 0001000</u>0 00000000	200.23.16.0/23
Organization 1	<u>11001000 00010111 0001001</u>0 00000000	200.23.18.0/23
Organization 2	<u>11001000 00010111 0001010</u>0 00000000	200.23.20.0/23
...	....	....
Organization 7	<u>11001000 00010111 0001111</u>0 00000000	200.23.30.0/23

Hierarchical addressing: route aggregation
(Route Summarization / Address Aggregation)

hierarchical addressing allows efficient advertisement of routing information:



Hierarchical addressing: route aggregation (Route Summarization / Address Aggregation)

- As was shown in the previous Figure, the ISP Fly-By-Night advertises to the outside world that it should be sent any datagrams whose first 20 address bits match 200.23.16.0/20.

- The rest of the world need not know that within the address block 200.23.16.0/20 there are in fact eight other organizations, each with their own subnets.

- This ability to use a single prefix to advertise multiple networks is often referred to as address aggregation (also route aggregation or route summarization or loosely can be called supernetting).

- This works extremely well when addresses are allocated in blocks to ISPs and then from ISPs to client organizations.

Hierarchical addressing: route aggregation (Route Summarization / Address Aggregation)

What if the addresses are not allocated in such a hierarchical manner?

- For example , what would happen if ISP Fly-By-Night acquires ISPs-R-Us and then has Organization 1 connect to the Internet through its subsidiary ISPs-R-Us?
- As was shown in the Figure, ISPs-R-Us owns the address block 199.31.0.0/16 but Organization 1's IP addresses are unfortunately outside of this address block.
- What should be done here?

Hierarchical addressing: route aggregation (Route Summarization / Address Aggregation)

Proposed Solutions

- **Organization 1 could renumber all of its routers and hosts to have addresses within the ISPs-R-Us address block.**

  - It's a costly solution.
  - Organization 1 might well be reassigned to another subsidiary in the future.

- **Organization 1 keeps its IP addresses in 200.23.18.0/23 and ISPs-R-Us advertises the block of addresses for Organization 1 (in addition to its own block of addresses.)**

  - When routers in the Internet see the address block 200.23.16.0/20 (from Fly-By-Night) and 200.23.18.0/23 (from ISPs-R-Us), and want to route to an address in the block 200.23.18.0/23, they will use longest prefix matching and route towards ISPs-R-Us as it advertises the longest (most specific) address prefix that matches the destination address.

Hierarchical addressing: route aggregation (Route Summarization / Address Aggregation)

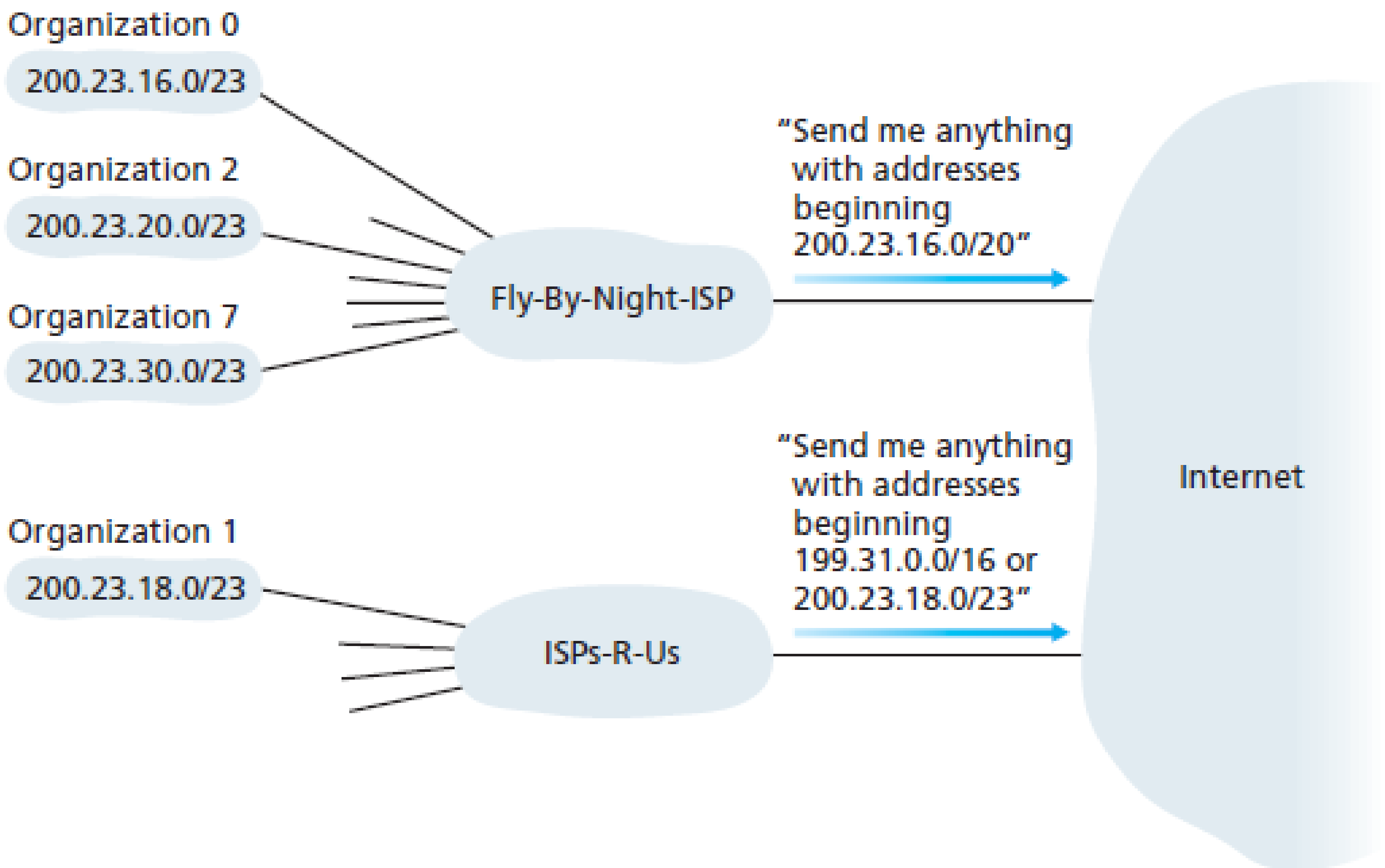


Figure 4.19 ♦ ISPs-R-Us has a more specific route to Organization 1

Route Summarization / Address Aggregation

- For revision of Route Summarization / Address Aggregation (Supernetting) discussed in the Class, please watch and review my video shared via Google Classroom. (Please watch the complete video, where I explain & solve an example for this in detail.)

Important topic of Computer Networks !!!!!!!

IP addressing: the last word...

Q: how does an ISP get block of addresses?

A: ICANN: Internet Corporation for Assigned Names and Numbers http://www.icann.org/

- allocates addresses
- manages DNS
- assigns domain names, resolves disputes

Chapter 4: outline

4.1 introduction

4.2 virtual circuit and datagram networks

4.3 what's inside a router

4.4 IP: Internet Protocol

- datagram format
- IPv4 addressing
- ICMP
- IPv6

4.5 routing algorithms

- link state
- distance vector
- hierarchical routing

4.6 routing in the Internet

- RIP
- OSPF
- BGP

4.7 broadcast and multicast routing

ICMP: internet control message protocol

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams (similar to UDP & TCP segments)
- ICMP message: type, code plus first 8 bytes of IP datagram causing error (so the source host can identify which datagram caused the error)

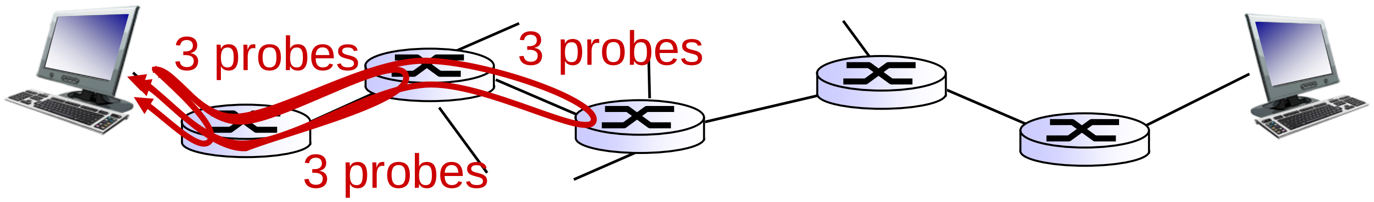
Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

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 (not known to destination host)
- when *n*th set of datagrams arrives to nth router (i.e. when timer TTL expires):
  - 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



Default HOP Limit (IPv6) Or TTL (IPv4) Values

Default TTL and Hop Limit values vary between different operating systems, here are the defaults for a few:

- Linux kernel 2.4 (circa 2001): 255 for TCP, UDP and ICMP
- Linux kernel 4.10 (2015): 64 for TCP, UDP and ICMP
- Windows XP (2001): 128 for TCP, UDP and ICMP
- Windows 10 (2015): 128 for TCP, UDP and ICMP
- Windows Server 2008: 128 for TCP, UDP and ICMP
- Windows Server 2019 (2018): 128 for TCP, UDP and ICMP
- MacOS (2001): 64 for TCP, UDP and ICMP

As you can see, the TTL or Hop Limit seen in packets from a host could, in part, be used to identify the operating system in use on that host.

Chapter 4: outline

4.1 introduction

4.2 virtual circuit and datagram networks

4.3 what's inside a router

4.4 IP: Internet Protocol

- datagram format
- IPv4 addressing
- ICMP
- IPv6

4.5 routing algorithms

- link state
- distance vector
- hierarchical routing

4.6 routing in the Internet

- RIP
- OSPF
- BGP

4.7 broadcast and multicast routing

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 at routers. If a router receives a datagram too big, it discards it and send a "Packet Too Big" ICMP Message, thus the host has to re-send a smaller packet

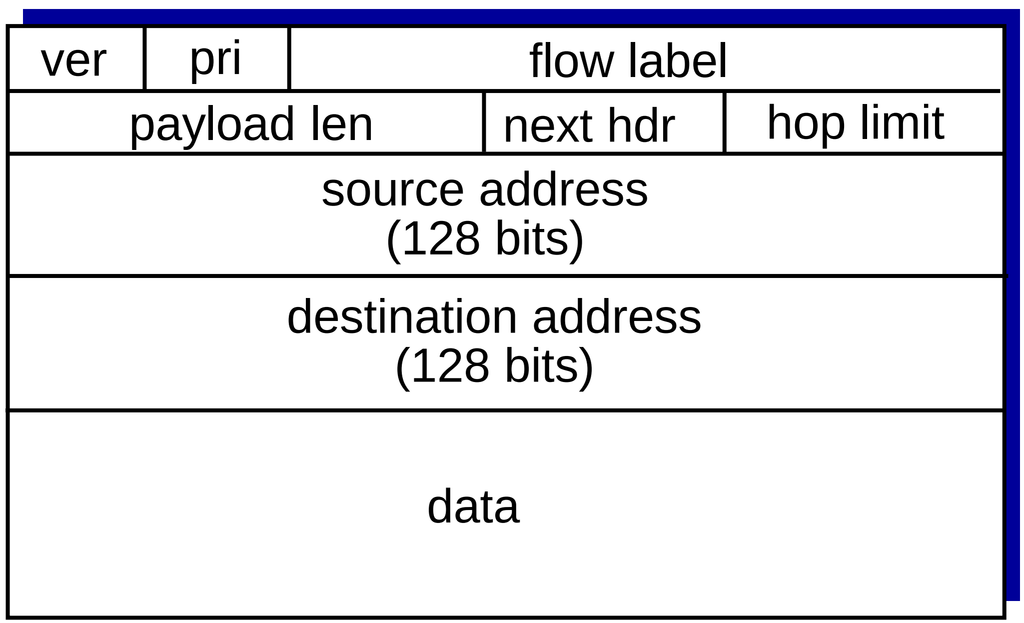
IPv6 datagram format

Priority/traffic class: identify priority among datagrams in flow

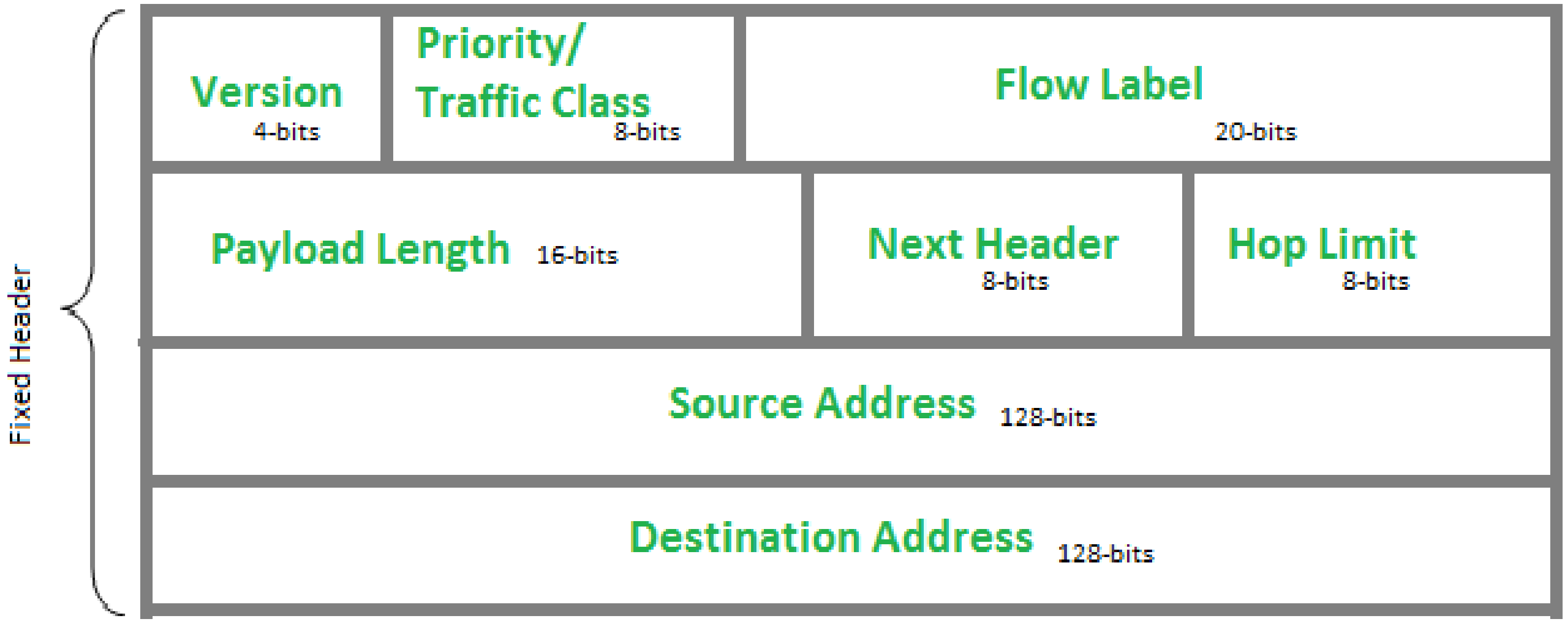
flow Label: identify datagrams in same "flow."

(concept of"flow" not well defined).

next header: identify upper layer protocol for data



IPv6 Header



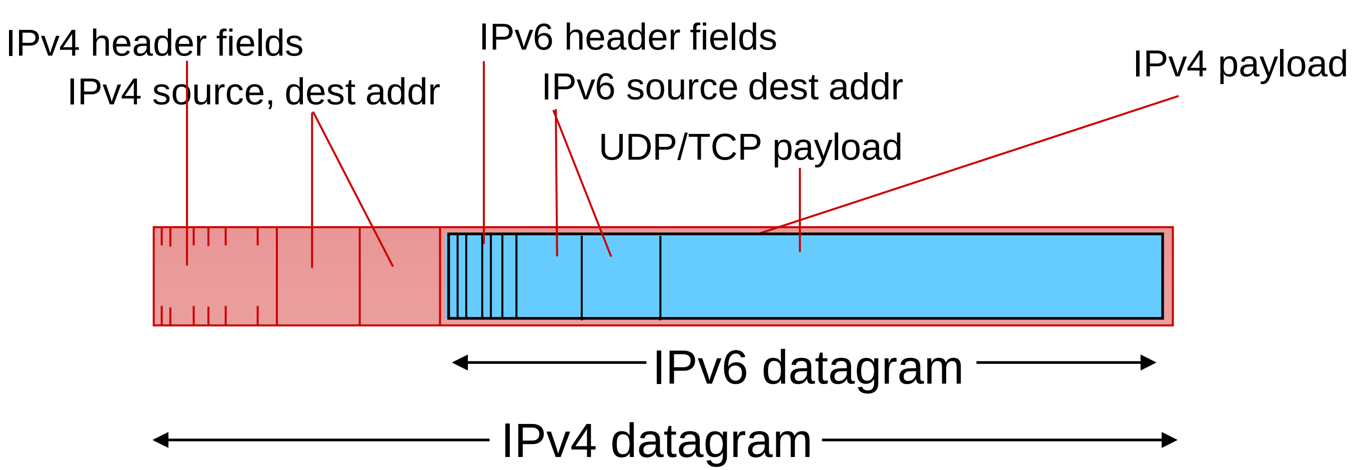
Fixed Header
Version
4-bits
Priority/
Traffic Class
8-bits
Flow Label
20-bits
Payload Length
16-bits
Next Header
8-bits
Hop Limit
8-bits
Source Address
128-bits
Destination Address
128-bits

Other changes from IPv4

- *checksum:* removed entirely to reduce processing time at each hop
- *options:* allowed, (but not part of the standard IP header), can be outside of header, indicated by "Next Header" field
- *ICMPv6:* new version of ICMP
  - additional message types, e.g. "Packet Too Big"
  - multicast group management functions

Transition from IPv4 to IPv6

- not all routers can be upgraded simultaneously
  - no "flag days" (i.e. a day announced where change will happen)
  - how will network operate with mixed IPv4 and IPv6 routers? (~~Dual Stack Approach~~ or Tunneling.)
- *tunneling:* IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers



Dual Stack Approach

- *IPv6 nodes have a complete implementation of IPv4 as well (referred to as IPv6/IPv4 node) & have both IPv6 & IPv4 addresses*

- Such nodes can speak in both i.e. in IPv4 to IPv4 nodes and in IPv6 to IPv6 nodes

- *Such nodes should be able to determine whether the other node is IPv4 or IPv6 (can be done via DNS, IP address returned via DNS can identify)*

- **Issue**: Two IPv6 nodes can end up speaking in IPv4 with each other. (e.g. Node *A* to F, both can speak IPv6, but intermediate nodes *C* & D can only speak IPv4, thus header fields (e.g. flow identifier) are lost from *A* to F although both understand this field

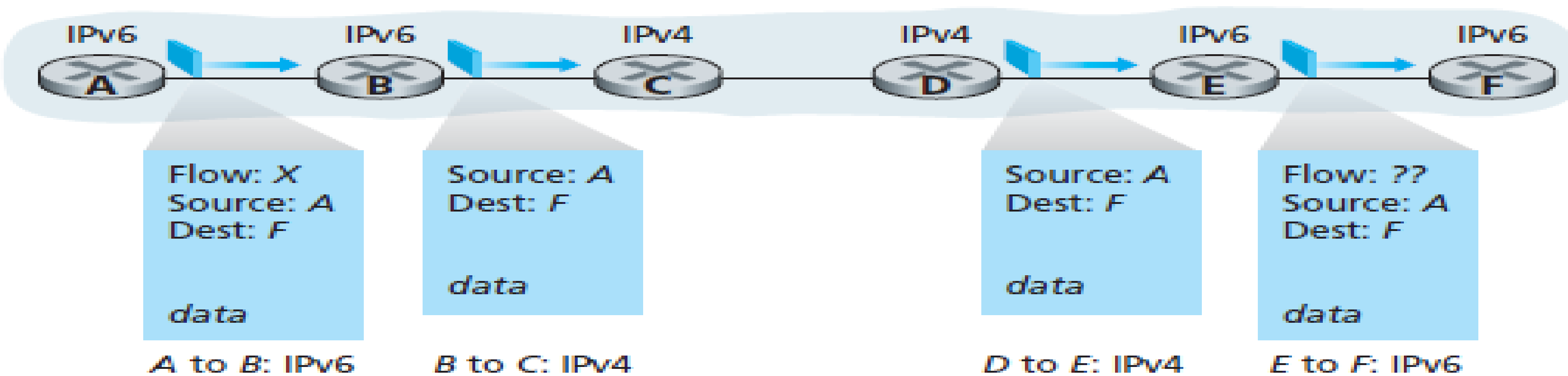


Figure 4.25 • A dual-stack approach

Tunneling

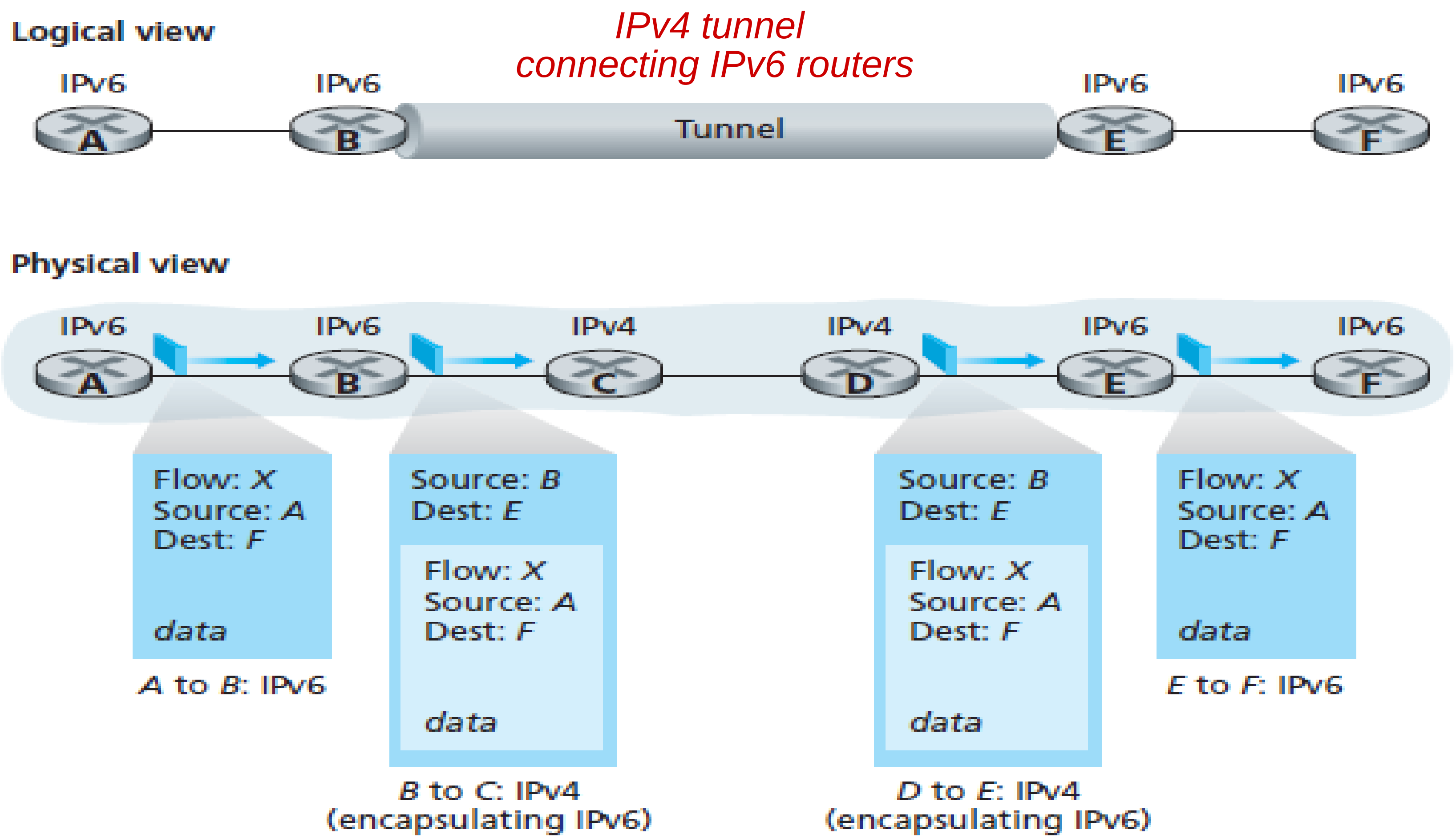


Figure 4.26 ◆ Tunneling

IPv6: adoption

- US National Institutes of Standards estimate [2013]:
  - ~3% of industry IP routers
  - ~11% of US gov't routers
- *Long (long!) time for deployment, use*
  - 20 years and counting! While network layer changes are taking too long (***akin to changing the foundation of a house***), Application layer changes are rapid (***akin to applying a new layer of paint to a house***)
  - think of application-level changes in last 20 years: WWW, Facebook, …
  - *Why? (Expensive, Solutions like NAT take some of the pressure off.)*

Quiz # 4 (Chapter - 4)

- ***On: Tuesday 8th November, 2022 (During the lecture)***

- ***Topics Included from Chapter 4 of the textbook:***

  - 4.1
  - 4.4

- ***Quiz to be taken during own section class only***