IP addresses, NAT, DHCP and OpenFlow

CE 352, Computer Networks

Salem Al-Agtash

Lecture 14

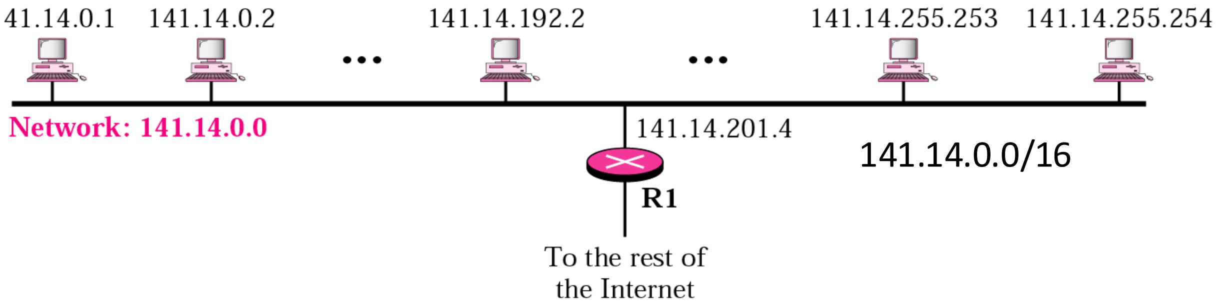
Slides are adapted from Computer Networking: A Top Down Approach, 7^{th} Edition © J.F Kurose and K.W. Ross

Recap (IP addresses)

IPv4: 32 bit address space - dotted decimal notation

- Network ID (Prefix) and /n mask
- No subnetting – two level hierarchy (network ID and host) – too many hosts on same LAN

*



- Subnetting – 3-level hierarch: setup a cluster of networks (subnets)
  - Overall traffic is reduced and performance enhanced
  - Smaller networks to manage and trouble shoot
  - Increase manager control over the address space
  - Reduce routing table entries and size

* Source: Behrouz Forouzan, *Data Communications and Networking*, 4th Edition, McGraw-Hill

Subnetting example

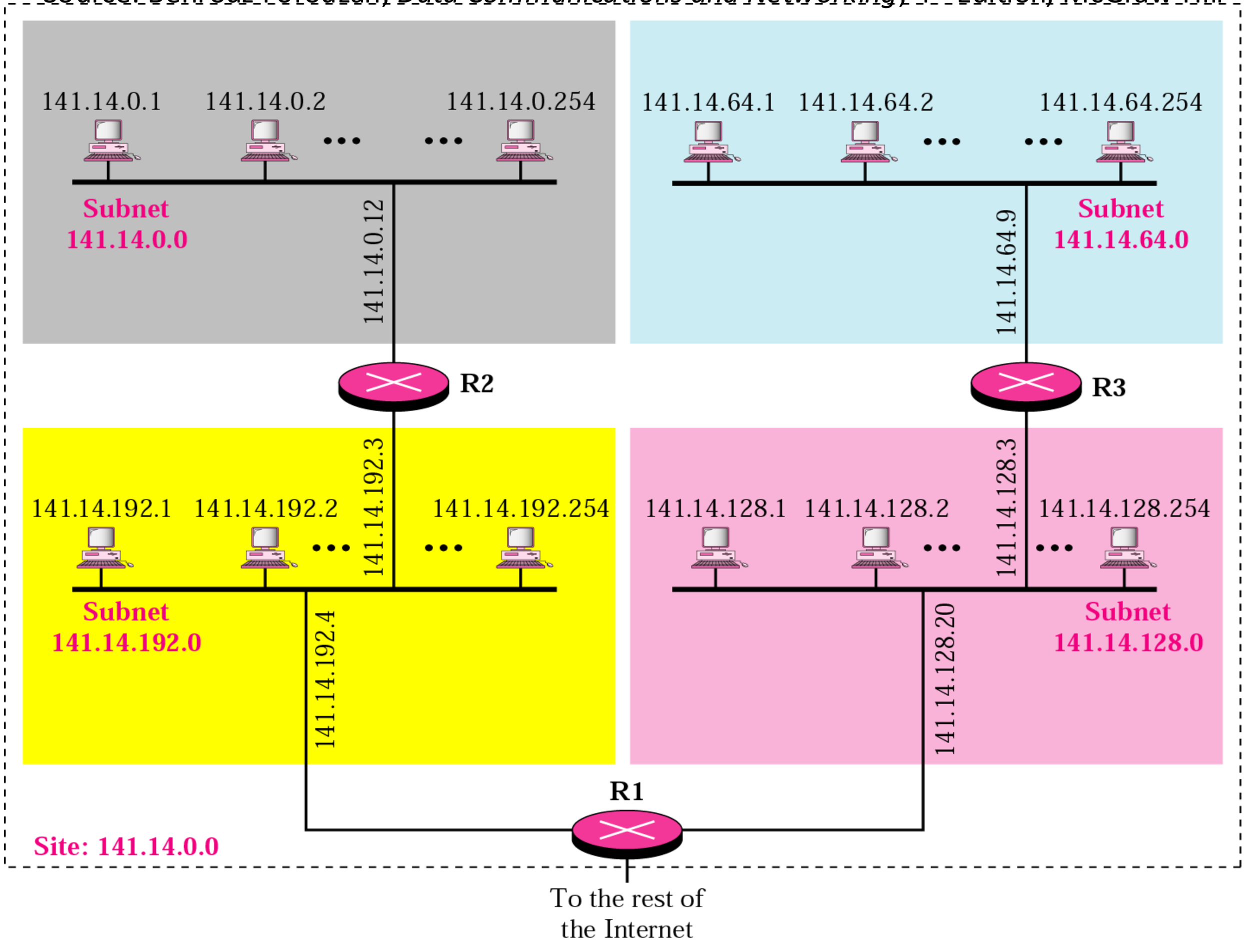
3-level hierarchy

- site: 141.1.14.0.0
- subnet 141.14.0.0
- subnet 141.14.64.0
- subnet 141.14.128.0
- subnet 141.14.192.0
- Routers will use subnet mask /18

- Mask is often written as 1_s:

/18 → 255.255.192.0

Source: Behrouz Forouzan, *Data Communications and Networking*, 4th Edition, McGraw-Hill



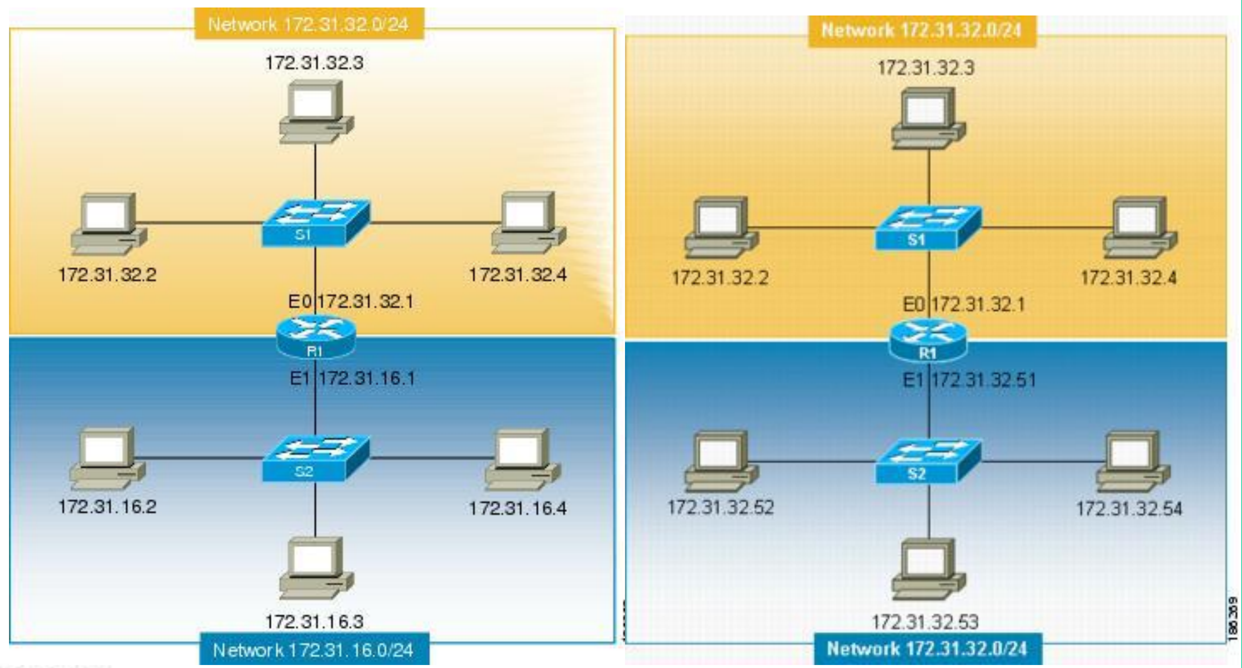
141.14. | 0000 0000 0000 0000 → Subnet prefix: 00, 01, 10, 11 (0, 64, 128, 192)

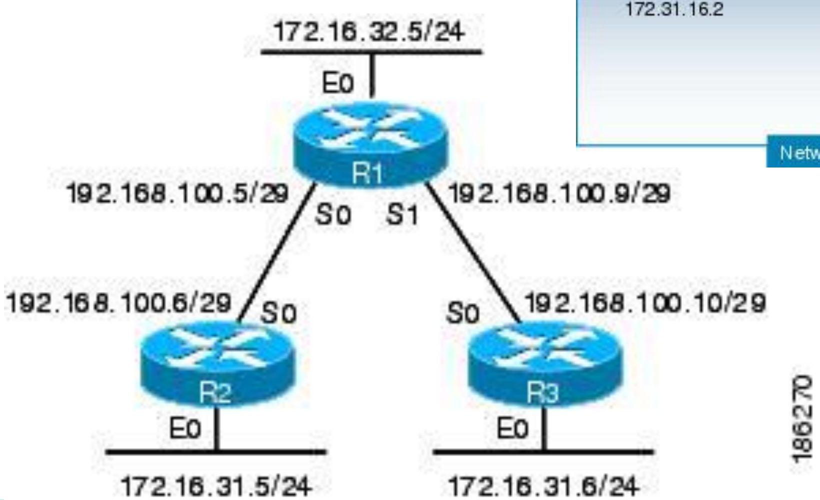
Subnetting example2

```
Router(config)#
interface
   FastEthernet0/1
Router(config)#
ip address 172.31.16.1
   255.255.255.0
```

* practice: router takes 1st address in network ID and broadcast for (1....)

Source: IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS XE Release 3S





Routing Table for incorrectly Configured Network

Interface Ethernet 0 Interface Ethernet 1

172.31.32.0/24 (Con) 172.31.32.0/24 (Con)

Routing Table for a Correctly Configured Network

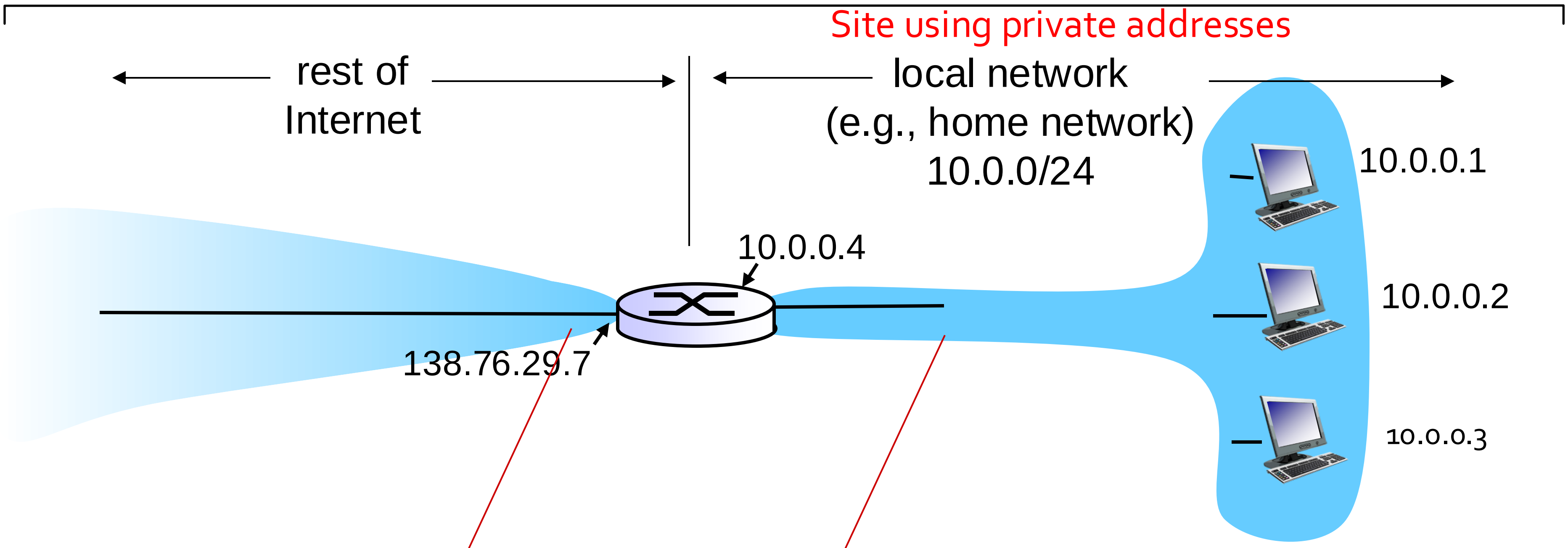
Interface Ethernet 0 Interface Ethernet 1

172.31.32.0/24 (Con) 172.31.16.0/24 (Con)

Recap (Private Addressing)

- Internet authorities have reserved three sets of addresses as private addresses:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- Unique inside the organization and not globally
- No router forwards a packet that has one of these addresses as the destination address

NAT: network address translation



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)

NAT: network address translation

motivation: local network uses just one IP address as far as outside world is concerned:

- range of addresses not needed from ISP: just one IP address for all devices
- 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: network address translation

implementation: NAT router must:

- *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 addr

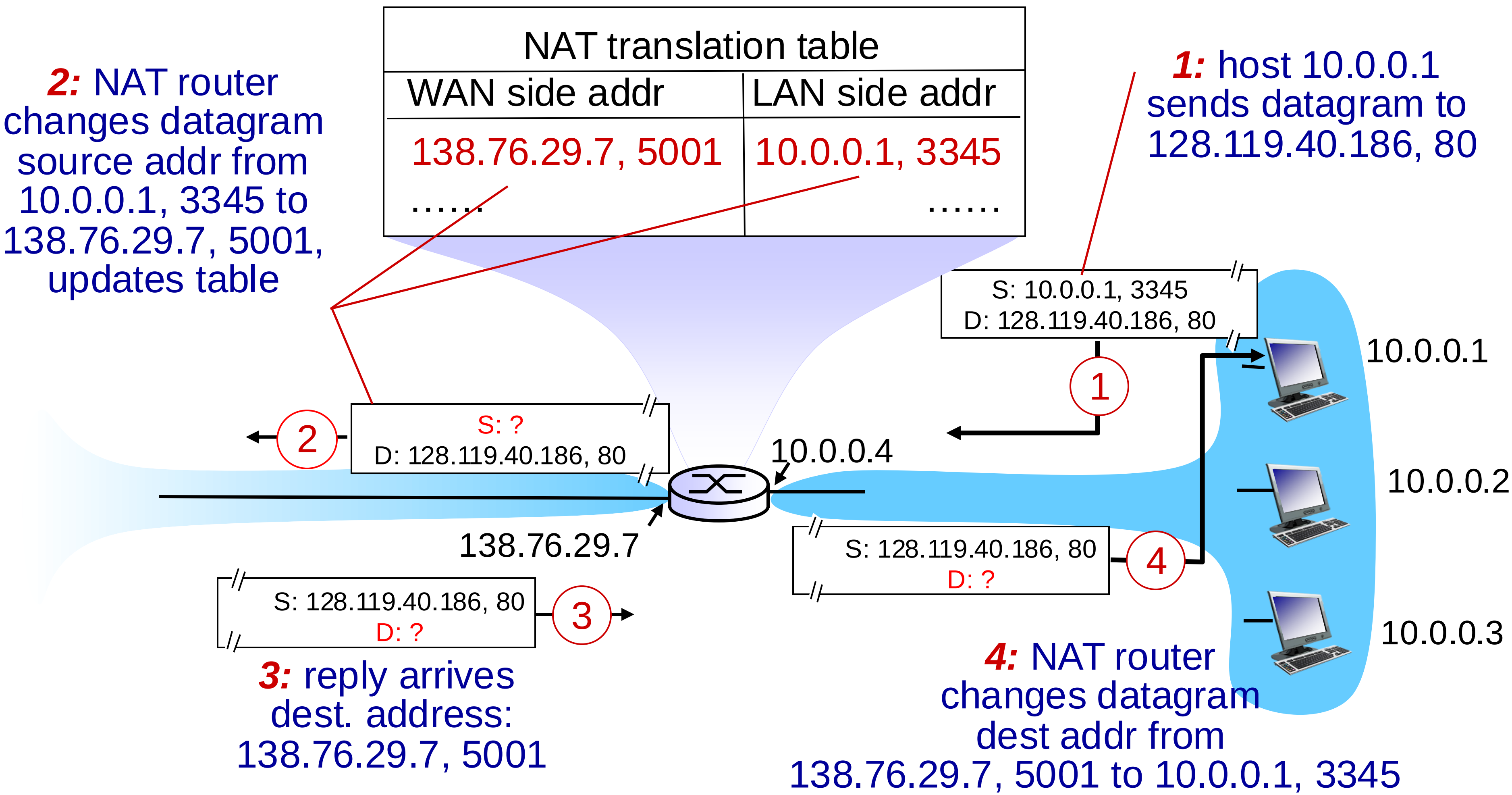
- *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair

- *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

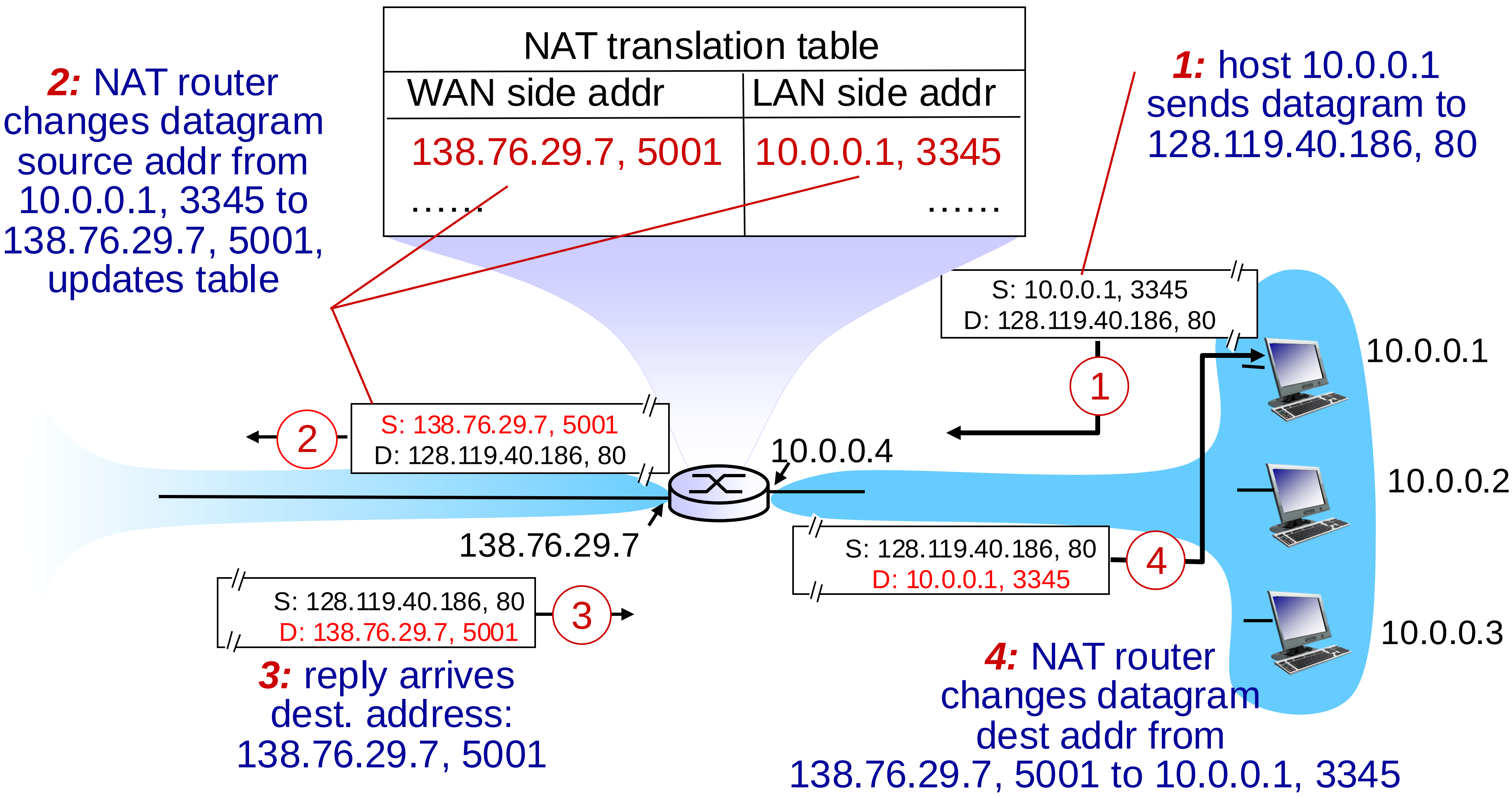
Private (local) ***source Address***	*Private (local)* ***source Port***	*NAT Port*	*External (remote) Address*
10.0.0.1	3345	5001	138.76.29.7
10.0.0.3	3455	10001	138.76.29.7
...	...	…	...

allows more than one host to contact same destination

NAT: network address translation



NAT: network address translation



NAT: network address translation

16-bit port-number field:

- 60,000 simultaneous connections with a single LAN-side address!

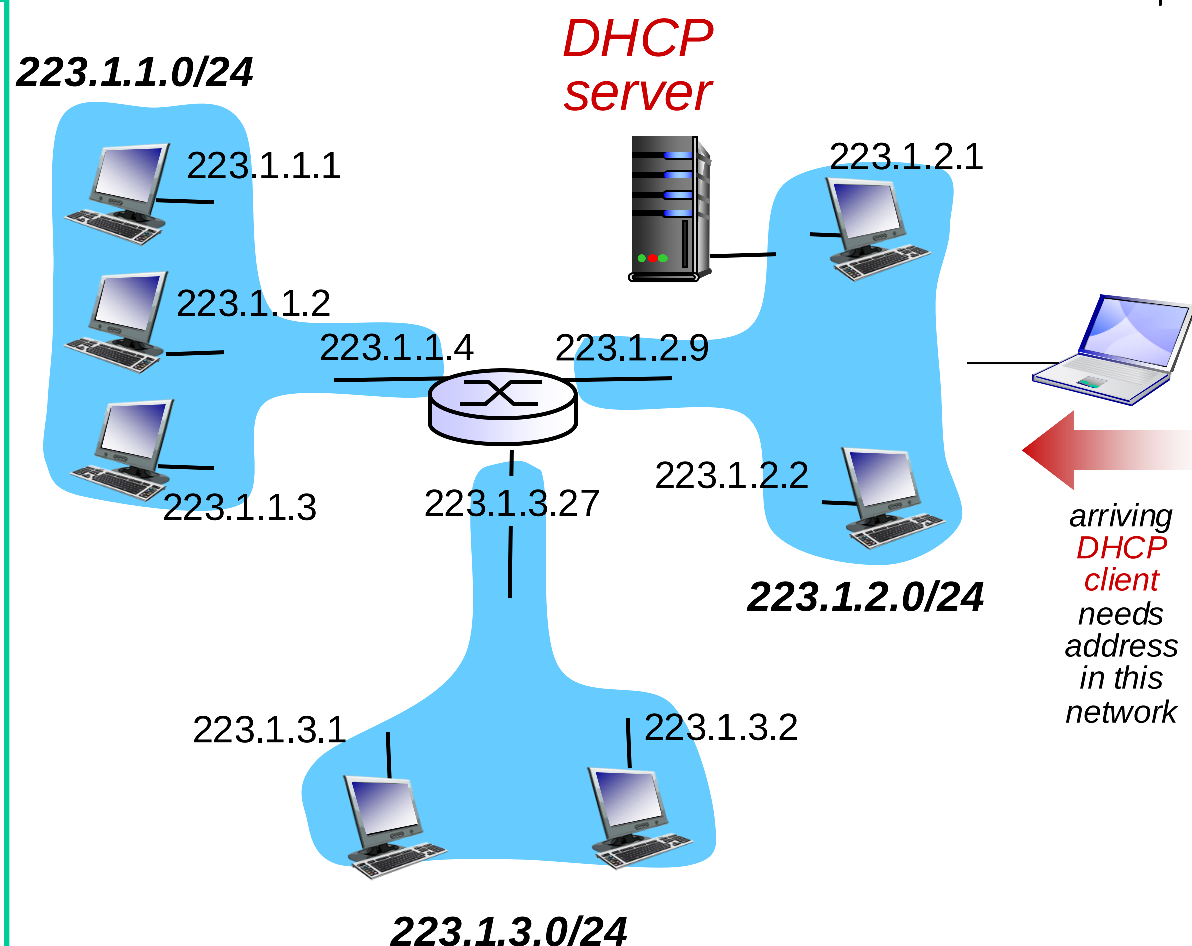
NAT is controversial:

- routers should only process up to layer 3
- address shortage should be solved by IPv6
- violates end-to-end argument
  - NAT possibility must be taken into account by app designers, e.g., P2P applications

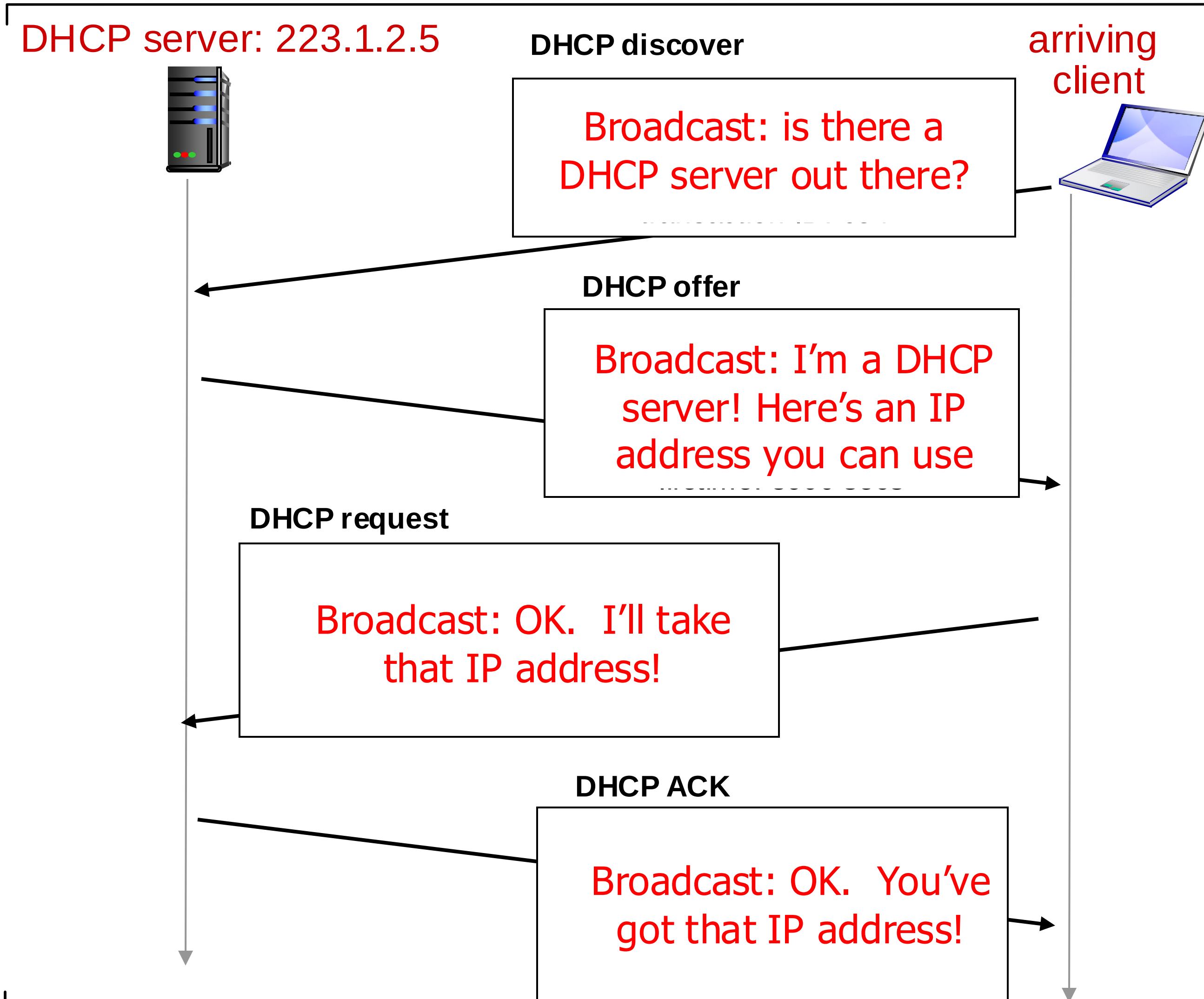
DHCP: Dynamic Host Configuration Protocol

Host *dynamically* obtains its IP address from network server when it joins network

- host broadcasts "DHCP discover" msg
- DHCP server responds with "DHCP offer" msg with an IP address
- host requests IP address: "DHCP request" msg - taking the offered IP
- DHCP server sends address: "DHCP ack" msg – IP is yours



DHCP client-server scenario



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)

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

Allocation of IP addresses

ICANN: Internet Corporation for Assigned Names and Numbers

http://www.icann.org/ operates via 5 Regional Internet Registries – ARIN (North America), APNIC (Asia Pacific), RIPE NCC (Europe and Middle East), LACNIC (Latin America), and AFRINIC (Africa)

- allocates addresses
- manages DNS
- assigns domain names

e.g. Organization 0 -7 and ISP's address space

ISP's block	11001000 00010111 0001|0000	00000000	200.23.16.0/20
Organization 0	11001000 00010111 0001		
Organization 1	11001000 00010111 0001	?	
Organization 2	11001000 00010111 0001		
...	.....	....	....
Organization 7	11001000 00010111 0001		

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Allocation of IP addresses

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

- allocates addresses
- manages DNS
- assigns domain names

e.g. Organization 0 -7 and ISP's address space

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

IPv6 addresses

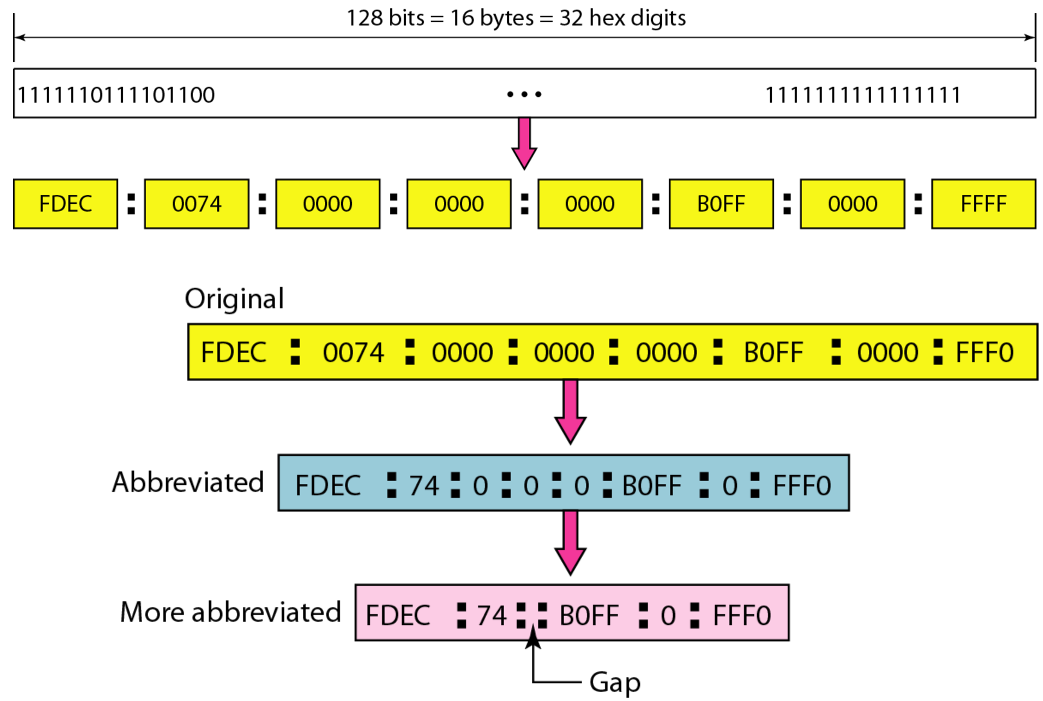
Despite all short-term solutions, address depletion is still a long-term problem for the Internet

Furthermore, a need for:

- header format helps speed processing/forwarding
- header changes to facilitate QoS

An IPv6 address is 128 bits long

address space = 2^{128}



Source: Behrouz Forouzan, *Data Communications and Networking*, 4th Edition, McGraw-Hill

IPv6 datagram

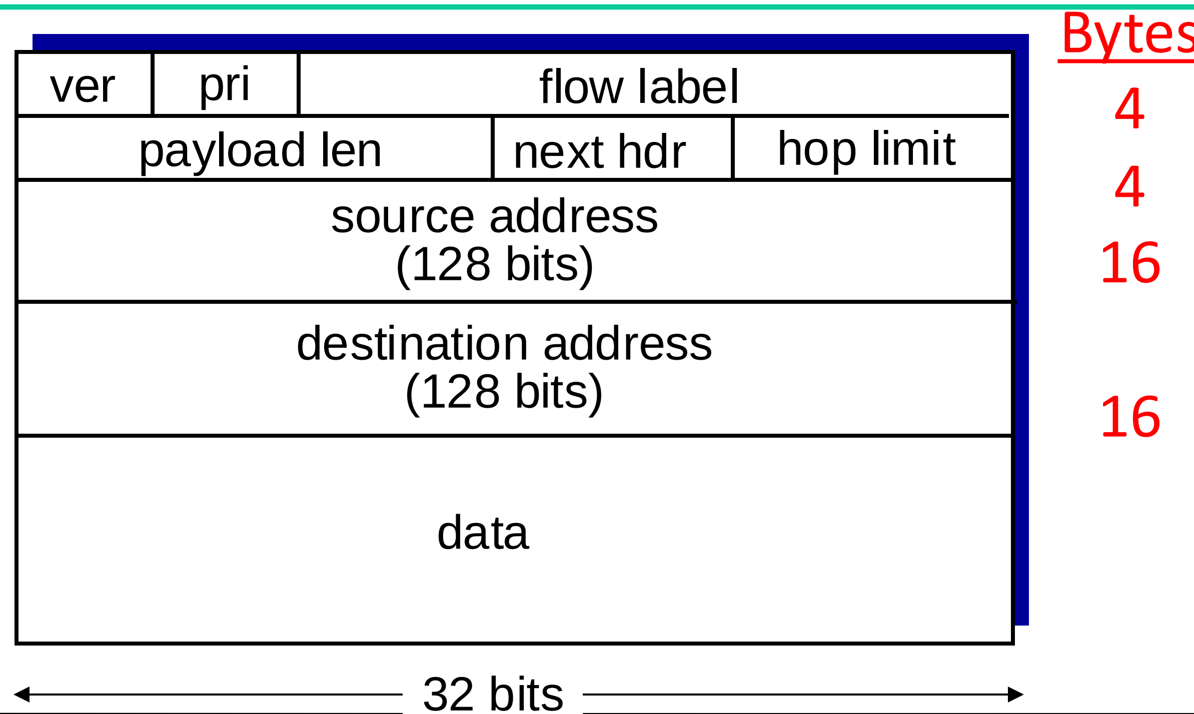
IPv6 datagram format:

- fixed-length 40 byte header
- no fragmentation allowed

priority: 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



Other changes from IPv4

checksum: removed entirely to reduce processing time at each hop

options: allowed, but outside of header, indicated by "Next Header" field

ICMPv6: new version of ICMP

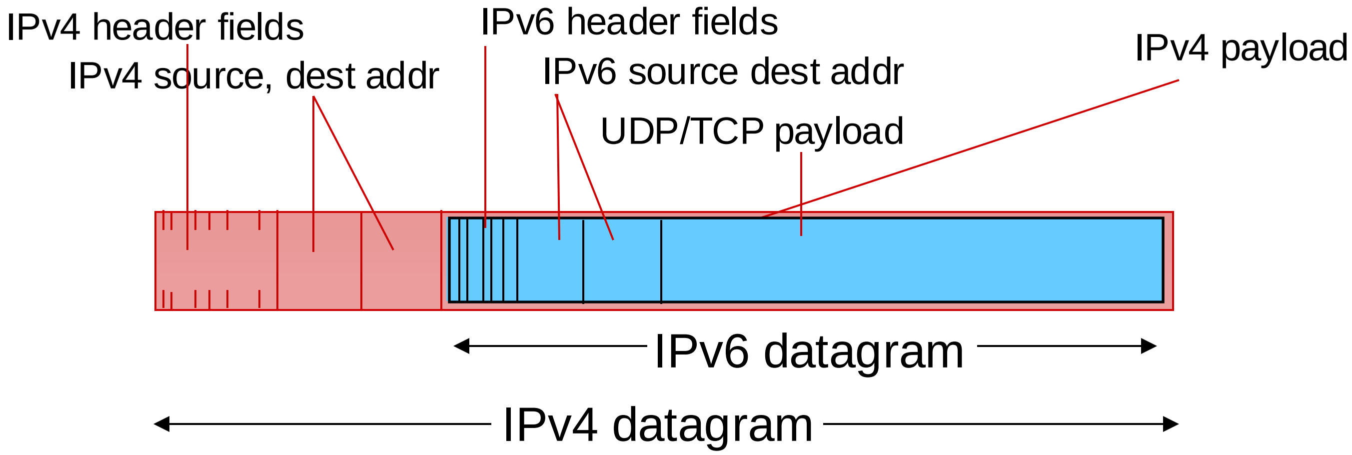
- additional message types, e.g. "Packet Too Big"
- multicast group management functions

Transition from IPv4 to IPv6

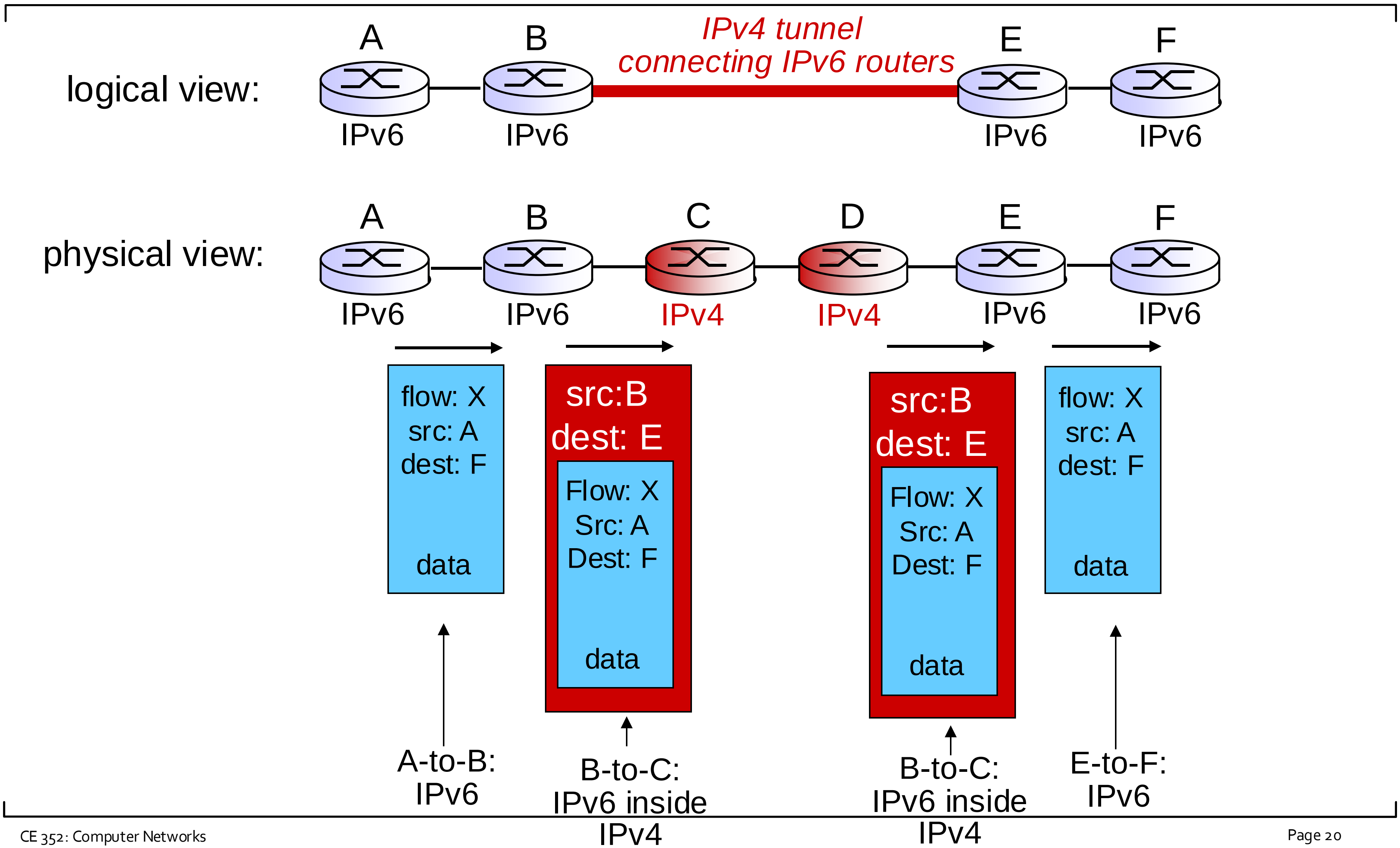
not all routers can be upgraded simultaneously

- no "flag days"
- how will network operate with mixed IPv4 and IPv6 routers?

tunneling: IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers



Tunneling


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

IPv6: adoption

Google: 41.23% of users globally access services using native IPv6 connectivity.

41% of all US government domains are IPv6-capable

https://www.hpc.mil/

https://www.hpc.mil/solution-areas/networking/ipv6-knowledge-base/ipv6-knowledge-base-general-information/ipv6-and-iot-policy-guidance-and-best-practices

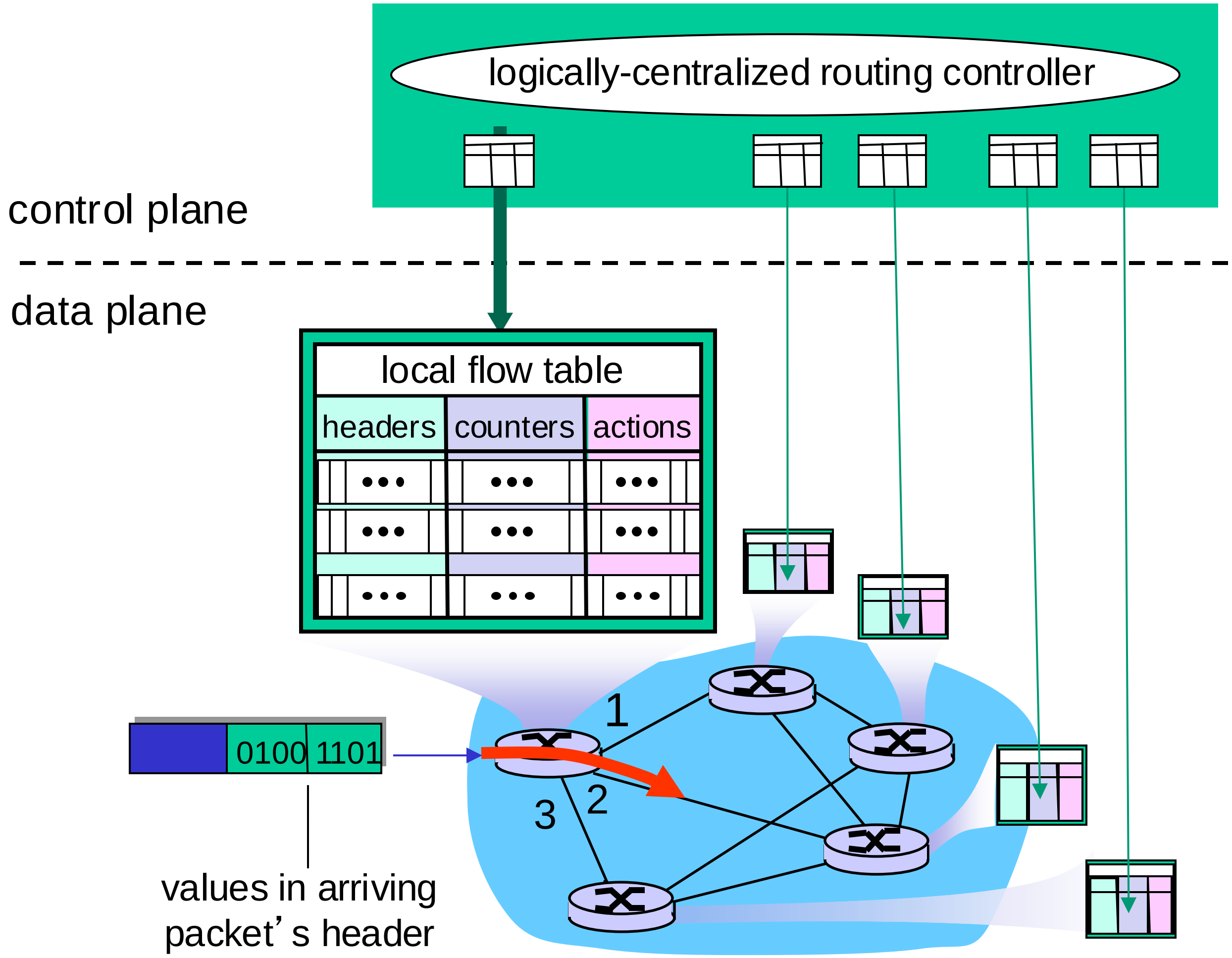
Long (long!) time for deployment, use

- 20 years and counting!
- think of application-level changes in last 20 years: WWW, Facebook, streaming media, …

Generalized Forwarding and SDN

Unified approach to providing many network layer functions [router, NAT, Firewall]

Each router contains a *flow table* that is computed and distributed by a *logically centralized* routing controller

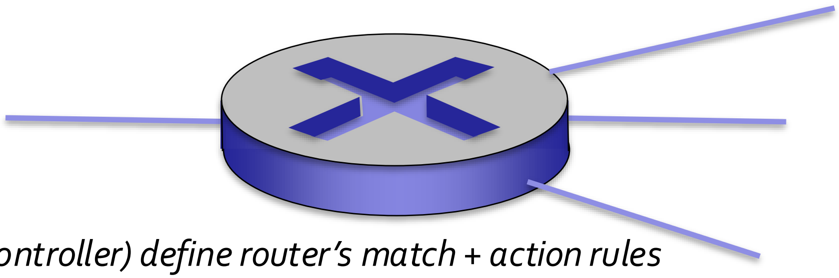


OpenFlow data plane abstraction

OpenFlow (OF): SDN standards for communication protocol and the flow is defined by header fields

generalized forwarding: simple packet-handling rules which allows router to perform traditional IP forwarding as well as a rich set of other functions (firewalling, NAT,..), traditionally implemented in separate devices.

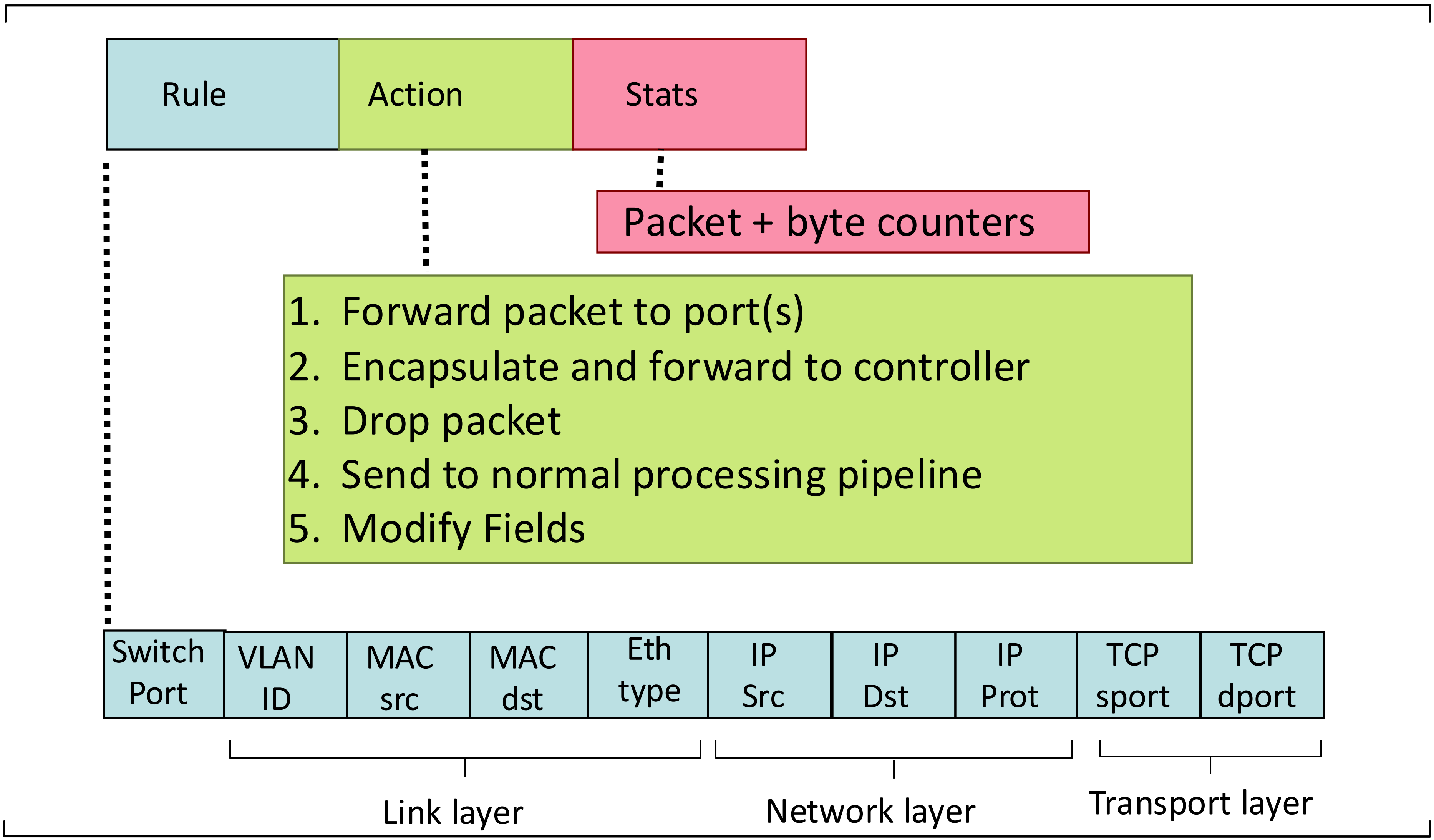
- *Pattern:* match values in packet header fields
- *Actions for matched packet:* drop, forward, or modify matched packet or send matched packet to controller
- *Counters:* #bytes and #packets



Flow table in a router (computed and distributed by controller) define router's match + action rules

1. src=182.2.*.*, dest=321.4.5.* → drop
2. src = *.*.*.*, dest=3.4.*.* → forward(2)
3. src=10.1.2.3, dest=*.*.*.* → send to controller

OpenFlow: Flow Table Entries



Examples

Destination-based forwarding:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	51.6.0.8	*	*	*	port6

IP datagrams destined to IP address 51.6.0.8 should be forwarded to router output port 6

Firewall:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	*	*	*	22	drop

do not forward (block) all datagrams destined to TCP port 22

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	128.119.1.1	*	*	*	*	drop

do not forward (block) all datagrams sent by host 128.119.1.1

Destination-based layer 2 (switch) forwarding:

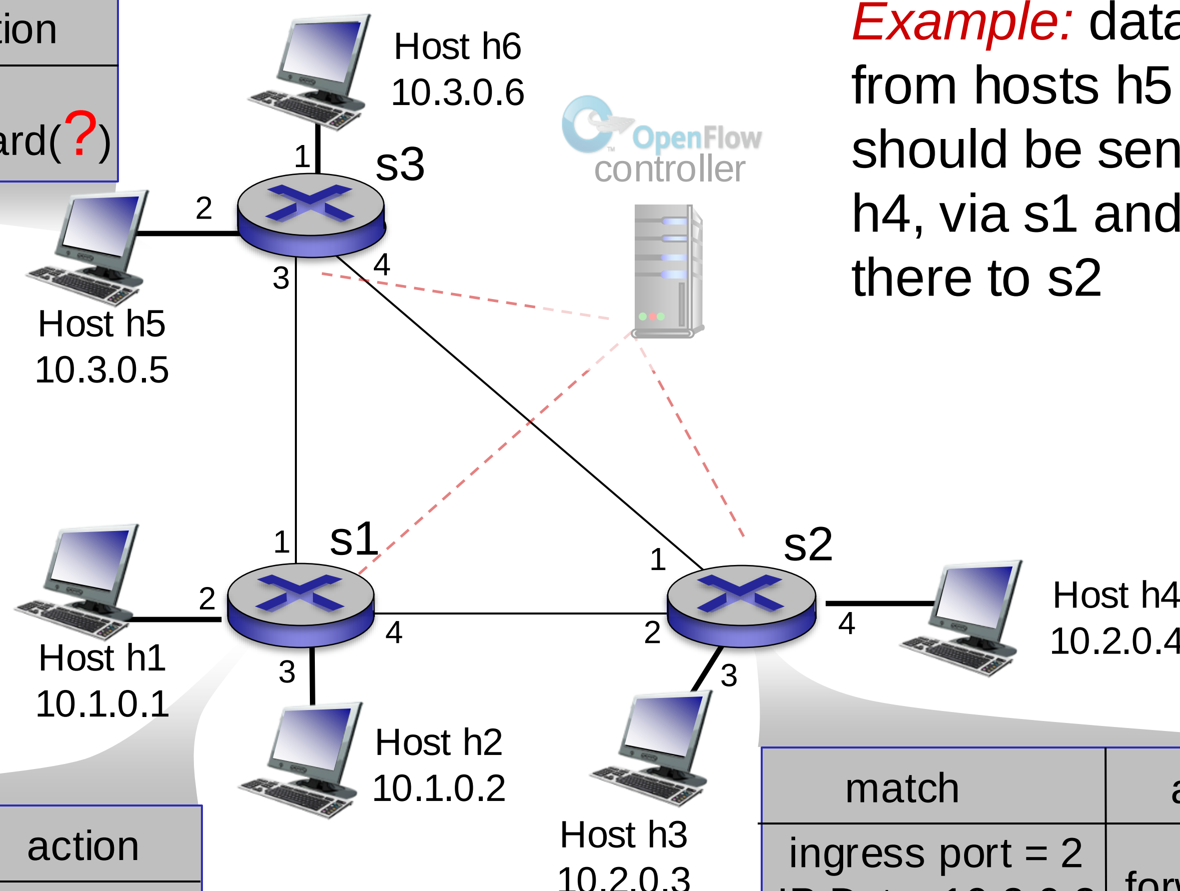
Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	22:A7:23: 11:E1:02	*	*	*	*	*	*	*	*	port3

layer 2 frames from MAC address 22:A7:23:11:E1:02 should be forwarded to output port 3

OpenFlow example

match	action
IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(?)

Example: datagrams from hosts h5 and h6 should be sent to h3 or h4, via s1 and from there to s2



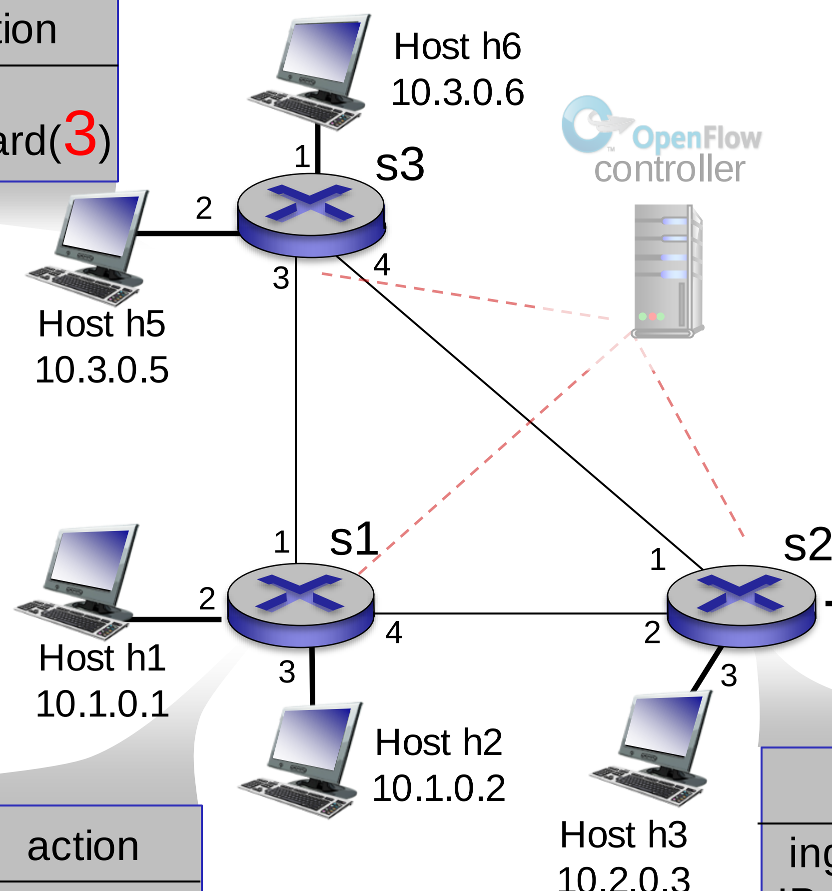
match	action
ingress port = 1 IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(?)

match	action
ingress port = 2 IP Dst = 10.2.0.3	forward(?)
ingress port = 2 IP Dst = 10.2.0.4	forward(?)

OpenFlow example

Example: datagrams from hosts h5 and h6 should be sent to h3 or h4, via s1 and from there to s2

match	action
IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(3)

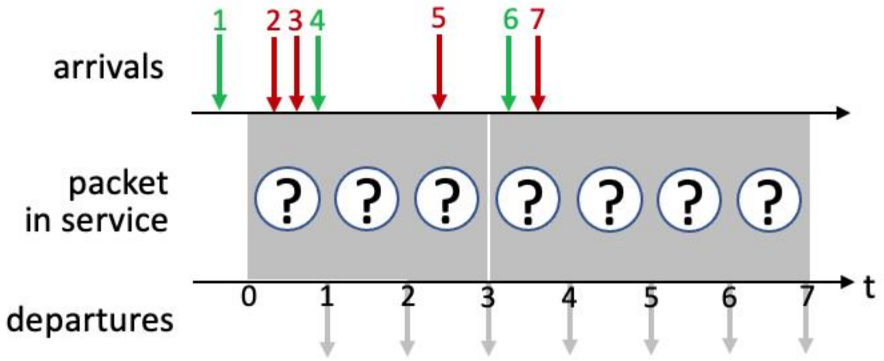


match	action
ingress port = 1 IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(4)

match	action
ingress port = 2 IP Dst = 10.2.0.3	forward(3)
ingress port = 2 IP Dst = 10.2.0.4	forward(4)

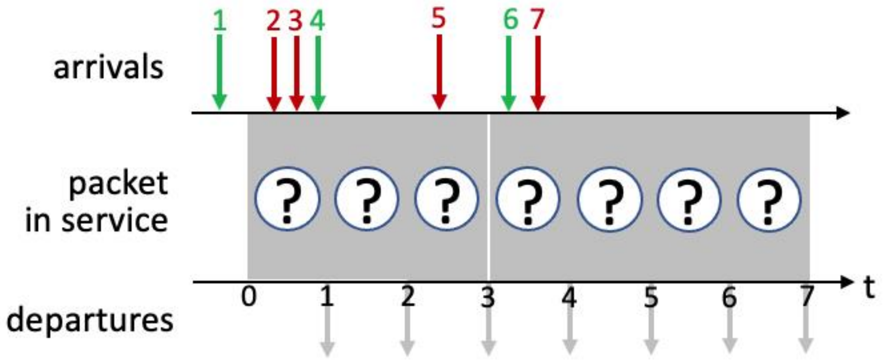
Review Example

- Consider the same pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 6, 7) under **round robin** scheduling. Assume a round-robin scheduling cycle begins with green packets. Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).



Example

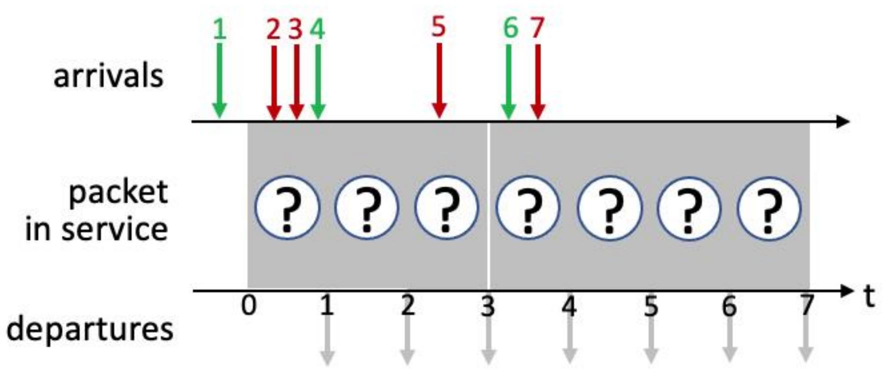
- Consider the same pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 6, 7) under **round robin** scheduling. Assume a round-robin scheduling cycle begins with green packets. Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).



1 2 4 3 6 5 7

Example

- Consider the same pattern of red and green packet arrivals to a router's output port queue, shown below. Suppose each packet takes one time slot to be transmitted, and can only begin transmission at the beginning of a time slot after its arrival. Indicate the sequence of departing packet numbers (at t = 1, 2, 3, 4, 5, 6, 7) under **Priority** scheduling. Assume a round-robin scheduling cycle begins with green packets. Give your answer as 7 ordered digits (each corresponding to the packet number of a departing packet), with a single space between each digit, and no spaces before the first or after the last digit, e.g., in a form like 7 6 5 4 3 2 1).



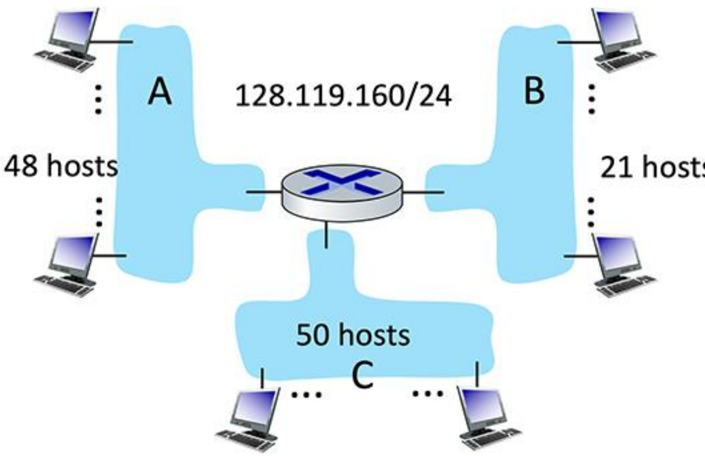
1 2 3 5 7 4 6

Example

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

- Consider the three subnets below, each in the larger 128.119.160/24 network. The following questions are concerned with subnet addressing.



- What is the maximum number of hosts possible in the larger 128.119.160/24 network?

- How many bits are needed to be able to address all of the host in subnet A?

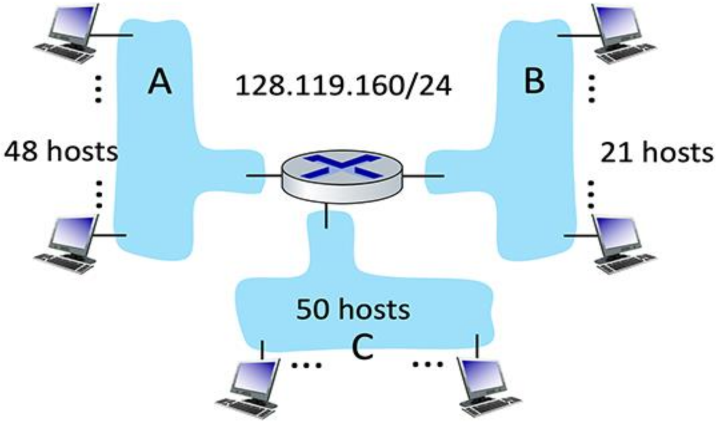
- Suppose that subnet A has a CIDRized subnet address range of 128.119.160.128/26; Subnet B has an CIDRied subnet address range of 128.119.160.64/27. We now want a valid CIDRized IP subnet address range for subnet C of the form 128.119.160.*x*/26. What is a valid value of *x*?

Example

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

- Consider the three subnets below, each in the larger 128.119.160.0/24 network. The following questions are concerned with subnet addressing.



- What is the maximum number of hosts possible in the larger 128.119.160/24 network?

So 24 bits for the network ID (prefix) and 8 bits for the host (postfix) → number of hosts = 2^8 → 256

- How many bits are needed to be able to address all of the hosts in subnet A, B, and C?

A: 48 → 2^6 B: 21 → 2^5 C: 50 → 2^6

128.119.160.10|00 0000 128.119.160.010|0 0000 128.119.160.00|00 0000

- Suppose that subnet A has a CIDRized subnet address range of 128.119.160.128/26; Subnet B has an CIDRied subnet address range of 128.119.160.64/27. We now want a valid CIDRized IP subnet address range for subnet C of the form 128.119.160.*x*/26. What is a valid value of *x*?

3 subnets → 2 bits: 10 for .128 (subnet A), 01 for .64 (subnet B), 00 -> .0 or 11 -> .192 (subnet C)

Example

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

- Consider a router that interconnects three subnets: Subnet A, Subnet B, and Subnet C. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also suppose that Subnet A is required to support at least 60 hosts, Subnet B is to support at least 90 hosts, and Subnet C is to support at least 12 hosts. Provide three network addresses (of the form a.b.c.d/x) that satisfy these constraints.

60 → 2^6

223.1.17.00|00 0000

223.1.17.0/26

223.1.17.00|00 0000

90 → 2^7

223.1.17.1|000 0000

223.1.17.128/25

223.1.17.1|000 0000

12 → 2^4

223.1.17.0100| 0000

223.1.17.64/28

223.1.17.0100| 0000

Example

- What field in the IP header can be used to ensure that a packet is forwarded through no more than *N* routers and that it does not remain in the network indefinitely?
- Do routers have IP addresses? If so, how many?
- Suppose you purchase a wireless router and connect it to your cable modem. Also suppose that your ISP dynamically assigns your connected device (that is, your wireless router) one IP address. Also suppose that you have five PCs at home that use 802.11 to wirelessly connect to your wireless router. How are IP addresses assigned to the five PCs? Does the wireless router use NAT? Why or why not?

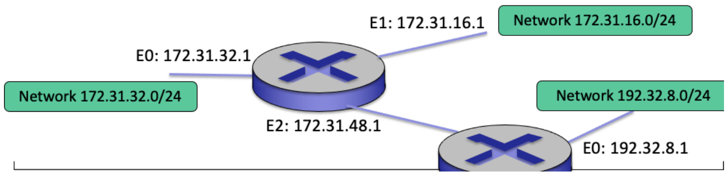
Example

- What field in the IP header can be used to ensure that a packet is forwarded through no more than *N* routers and that it does not remain in the network indefinitely?

Time-to-live

- Do routers have IP addresses? If so, how many?

Yes. They have one address for each interface



- Suppose you purchase a wireless router and connect it to your cable modem. Also suppose that your ISP dynamically assigns your connected device (that is, your wireless router) one IP address. Also suppose that you have five PCs at home that use 802.11 to wirelessly connect to your wireless router. How are IP addresses assigned to the five PCs? Does the wireless router use NAT? Why or why not?

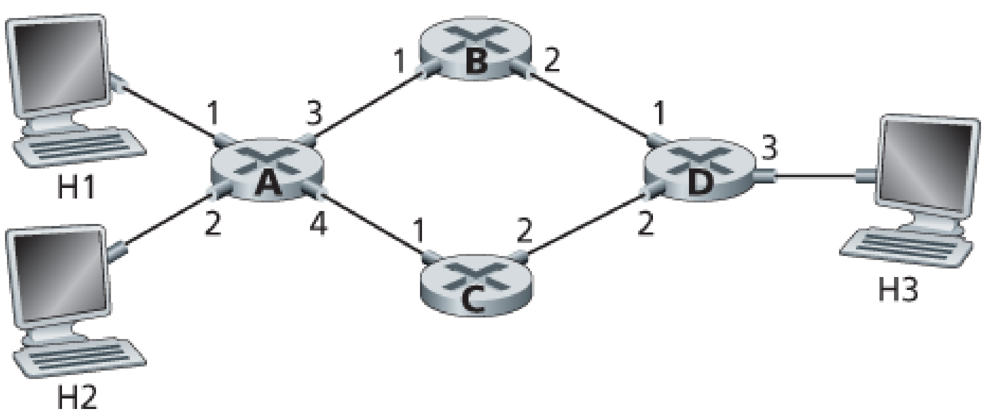
Typically the wireless router includes a DHCP server. DHCP is used to assign IP addresses to the 5 PCs and to the router interface. Yes, the wireless router also uses NAT as it obtains only one IP address from the ISP.

Example

- Consider the network below.
  - Show the forwarding table in router A, such that all traffic destined to host H3 is forwarded through interface 3.

Data destined to host H3 is forwarded through interface 3

Destination Address	Link Interface
?	?

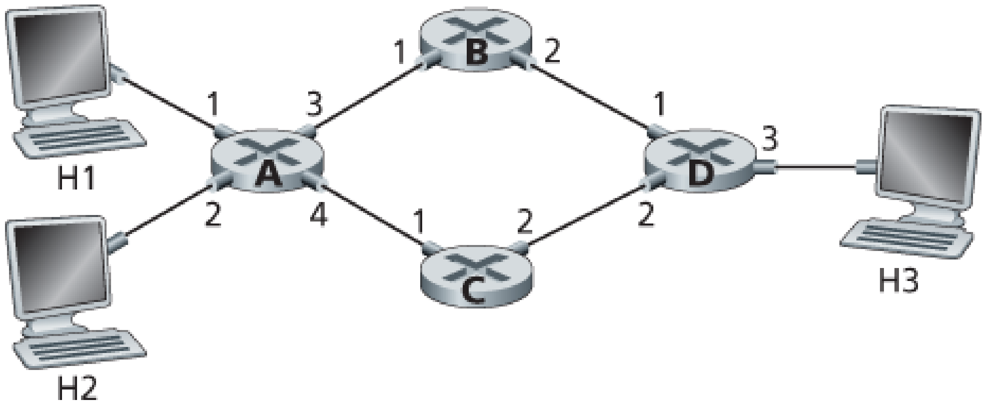


Example

- Consider the network below.
  - Show the forwarding table in router A, such that all traffic destined to host H3 is forwarded through interface 3.

Data destined to host H3 is forwarded through interface 3

Destination Address	Link Interface
H3	3



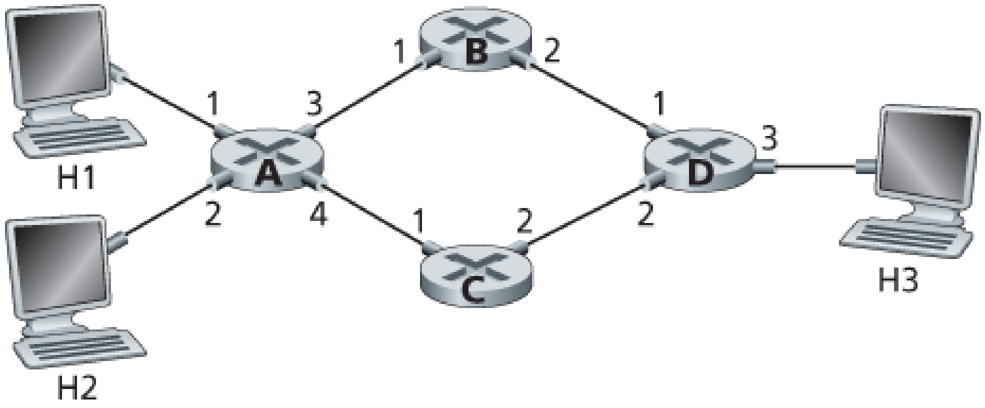
- Can you write down a forwarding table in router A, such that all traffic from H1 destined to host H3 is forwarded through interface 3, while all traffic from H2 destined to host H3 is forwarded through interface 4?

Example

- Consider the network below.
  - Show the forwarding table in router A, such that all traffic destined to host H3 is forwarded through interface 3.

Data destined to host H3 is forwarded through interface 3

Destination Address	Link Interface
H3	3



- Can you write down a forwarding table in router A, such that all traffic from H1 destined to host H3 is forwarded through interface 3, while all traffic from H2 destined to host H3 is forwarded through interface 4?

  No, because forwarding rule is only based on destination address

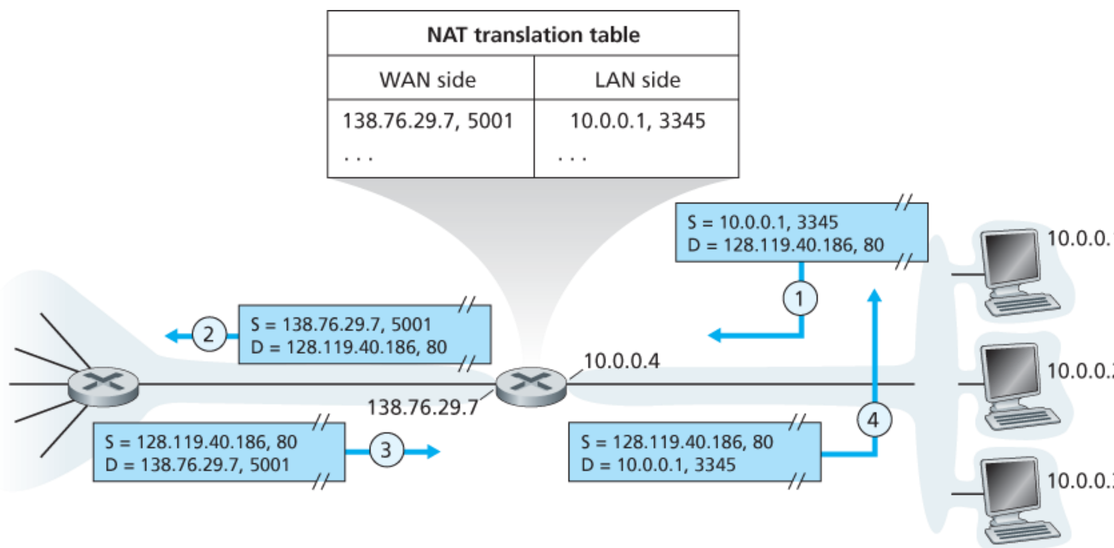
Example

- Consider the following network setup. Suppose that the ISP instead assigns the router the address 24.34.112.235 and that the network address of the home network is 192.168.1/24. Assign addresses to all interfaces in the home network. Suppose each host has two ongoing TCP connections, all to port 80 at host 128.119.40.86. Provide the six corresponding entries in the NAT translation table.
- Home addresses: ? with the router interface being ?

NAT Translation Table

WAN Side LAN Side

? ?

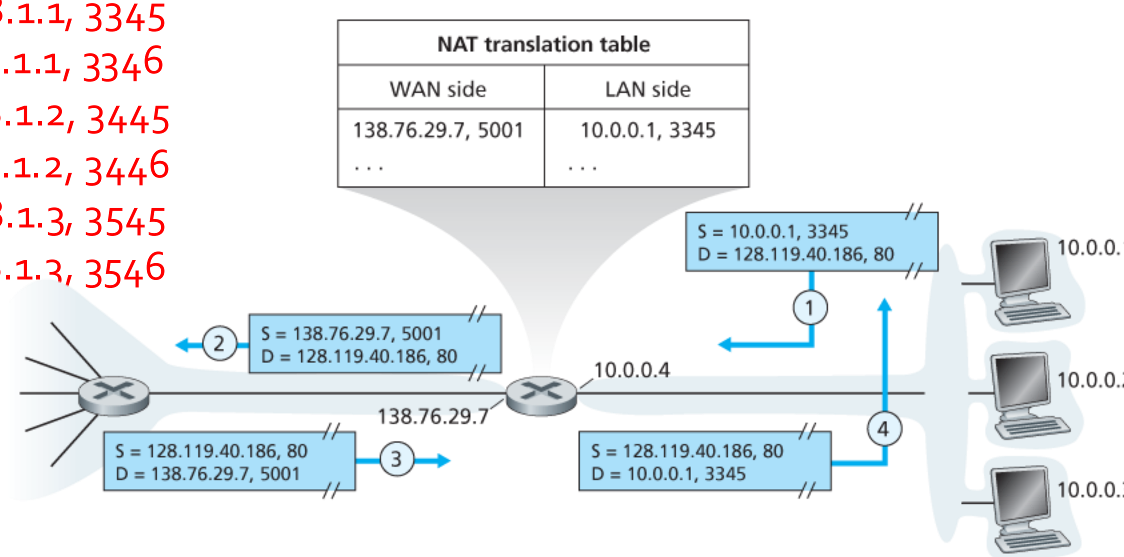


Example

- Consider the following network setup. Suppose that the ISP instead assigns the router the address 24.34.112.235 and that the network address of the home network is 192.168.1/24. Assign addresses to all interfaces in the home network. Suppose each host has two ongoing TCP connections, all to port 80 at host 128.119.40.86. Provide the six corresponding entries in the NAT translation table.
- Home addresses: 192.168.1.1, 192.168.1.2, 192.168.1.3 with the router interface being 192.168.1.4

NAT Translation Table

WAN Side	LAN Side
24.34.112.235, 5000	192.168.1.1, 3345
24.34.112.235, 5001	192.168.1.1, 3346
24.34.112.235, 5002	192.168.1.2, 3445
24.34.112.235, 5003	192.168.1.2, 3446
24.34.112.235, 5004	192.168.1.3, 3545
24.34.112.235, 5005	192.168.1.3, 3546



Summary

Today:

- Subnetting
- Private addressing
- NAT
- DHCP
- IPv6
- Open flow - SDN

Camino discussion:

- Reflection
- Exit ticket

Next time:

- read 5.1, 5.2 of K&R (control plane – routing protocols)
- follow on Canvas! material and announcements

Any questions?