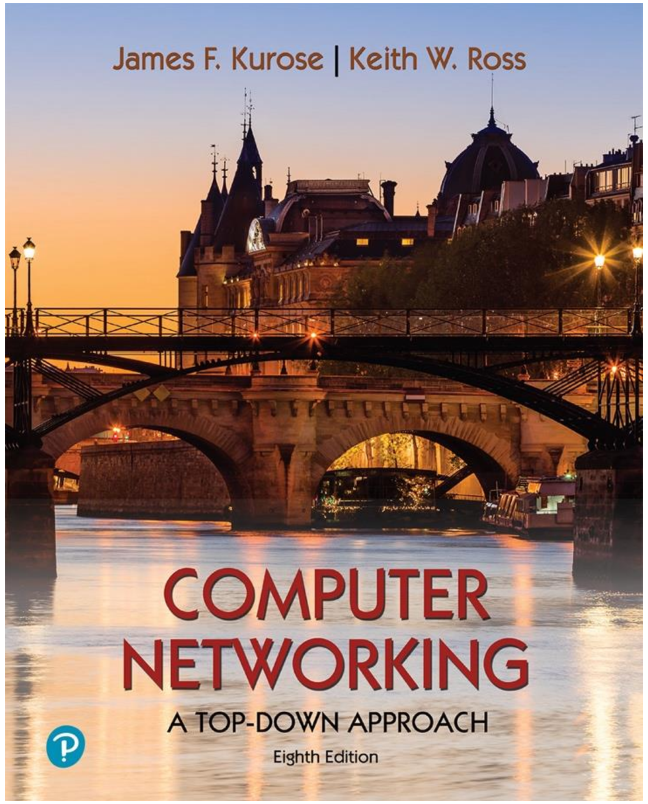
Final-exam Review

Yaxiong Xie

Department of Computer Science and Engineering
University at Buffalo, SUNY



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Adapted from the slides of the book's authors

Several Points

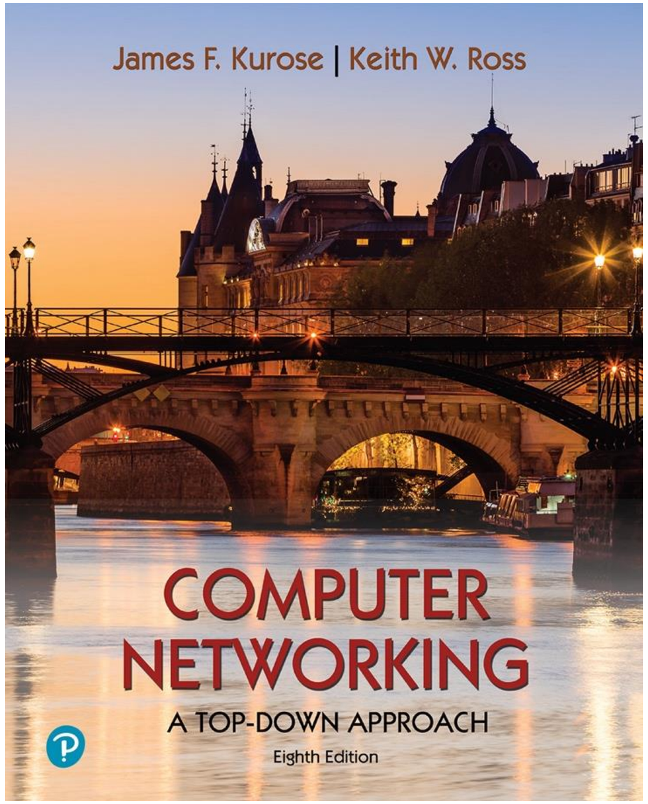
- Here, I will list all the ***topics*** that I think are important
  - If one topic I didn't mention, then I won't test it
  - It is about the topic, not the slides
    - If I didn't mention one slides, but I do mention the topic, I probably will cover it
    - There are too many slides if I include every slides about that topic
- It will be fast, I won't teach it again
- Ask questions, if you have any

Chapter 4
Network Layer: Data Plane

Yaxiong Xie

Department of Computer Science and Engineering
University at Buffalo, SUNY

Adapted from the slides of the book's authors



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Two key network-layer functions

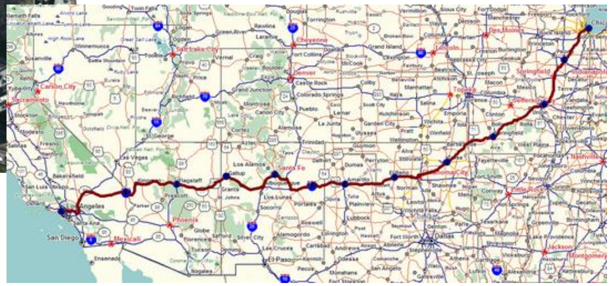
network-layer functions:

- *forwarding:* move packets from a router's input link to appropriate router output link
- *routing:* determine route taken by packets from source to destination
  - *routing algorithms*

analogy: taking a trip

- *forwarding:* process of getting through single interchange
- *routing:* process of planning trip from source to destination

forwarding

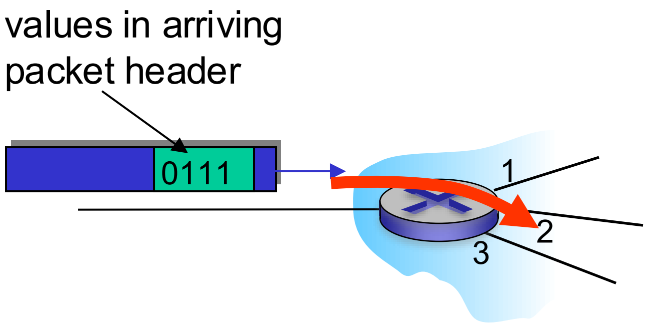


routing

Network layer: data plane, control plane

Data plane:

- *local*, per-router function
- determines how datagram arriving on router input port is forwarded to router output port

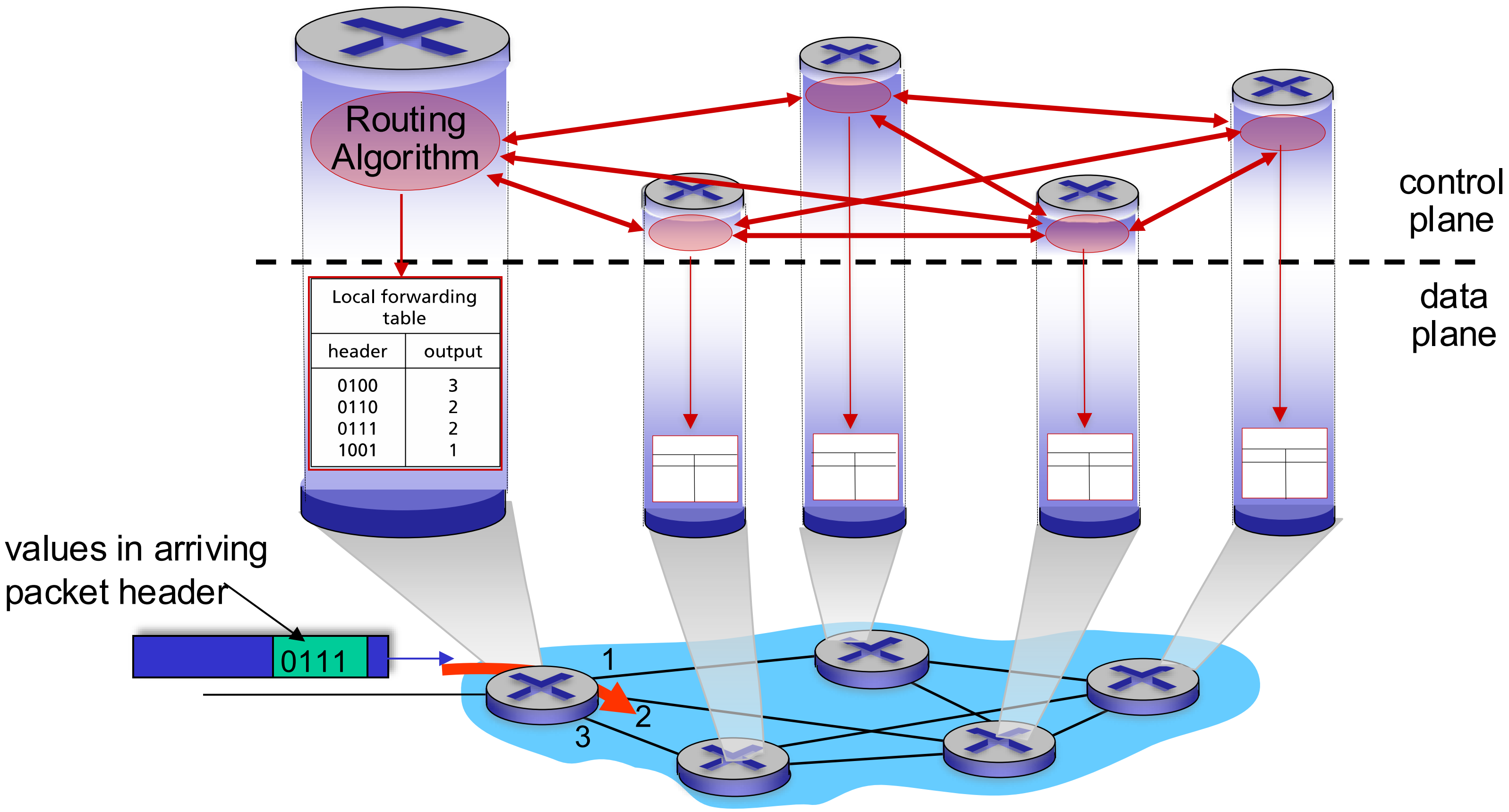


Control plane

- *network-wide* logic
- determines how datagram is routed among routers along end-end path from source host to destination host
- two control-plane approaches:
  - *traditional routing algorithms:* implemented in routers
  - *software-defined networking (SDN)*: implemented in (remote) servers

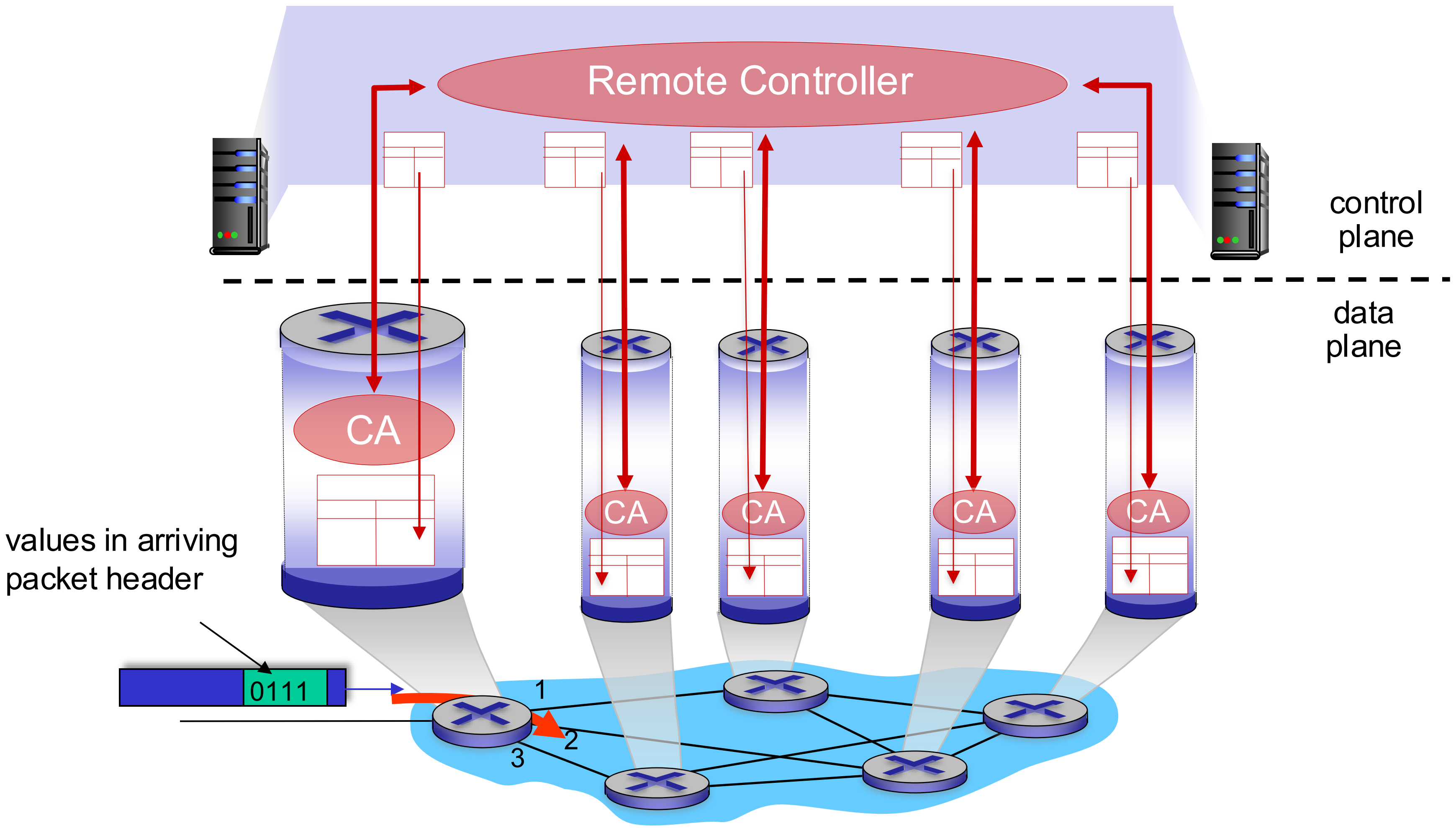
Per-router control plane

Individual routing algorithm components *in each and every router* interact in the control plane



Software-Defined Networking (SDN) control plane

Remote controller computes, installs forwarding tables in routers

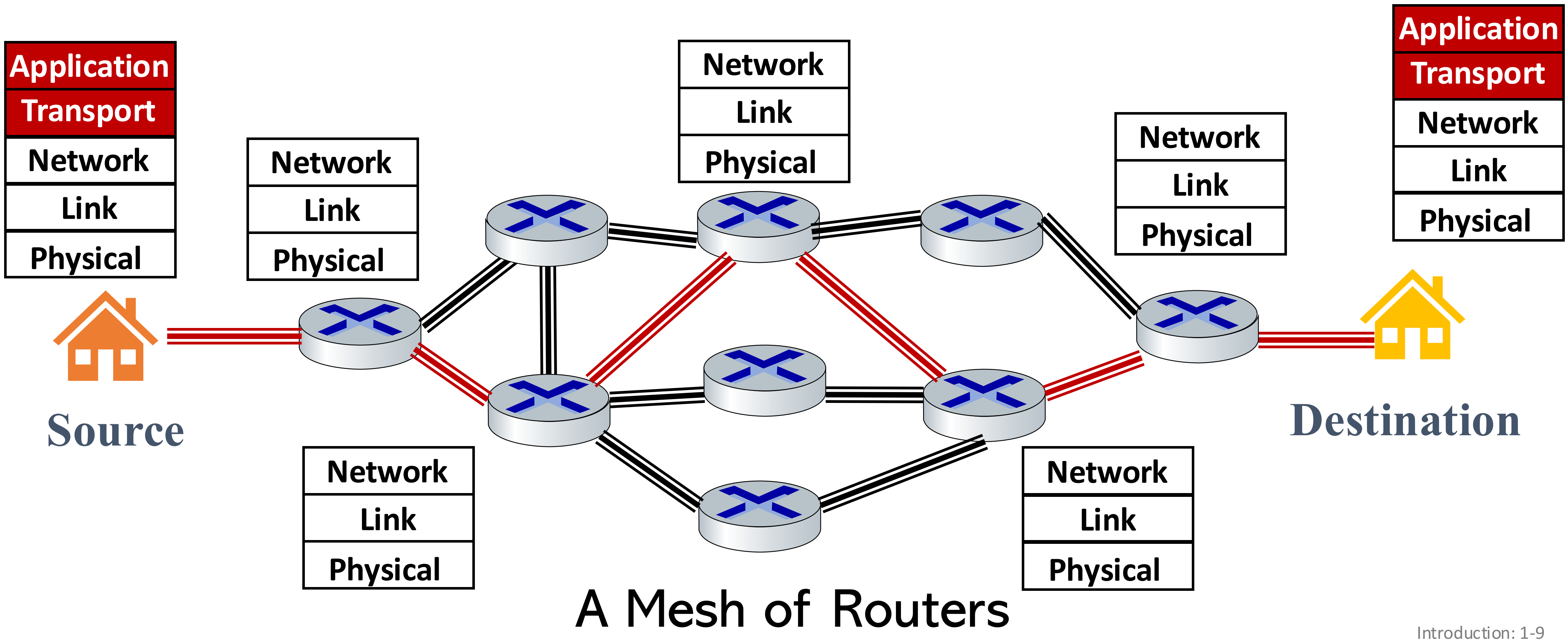


Network layer: “data plane” roadmap

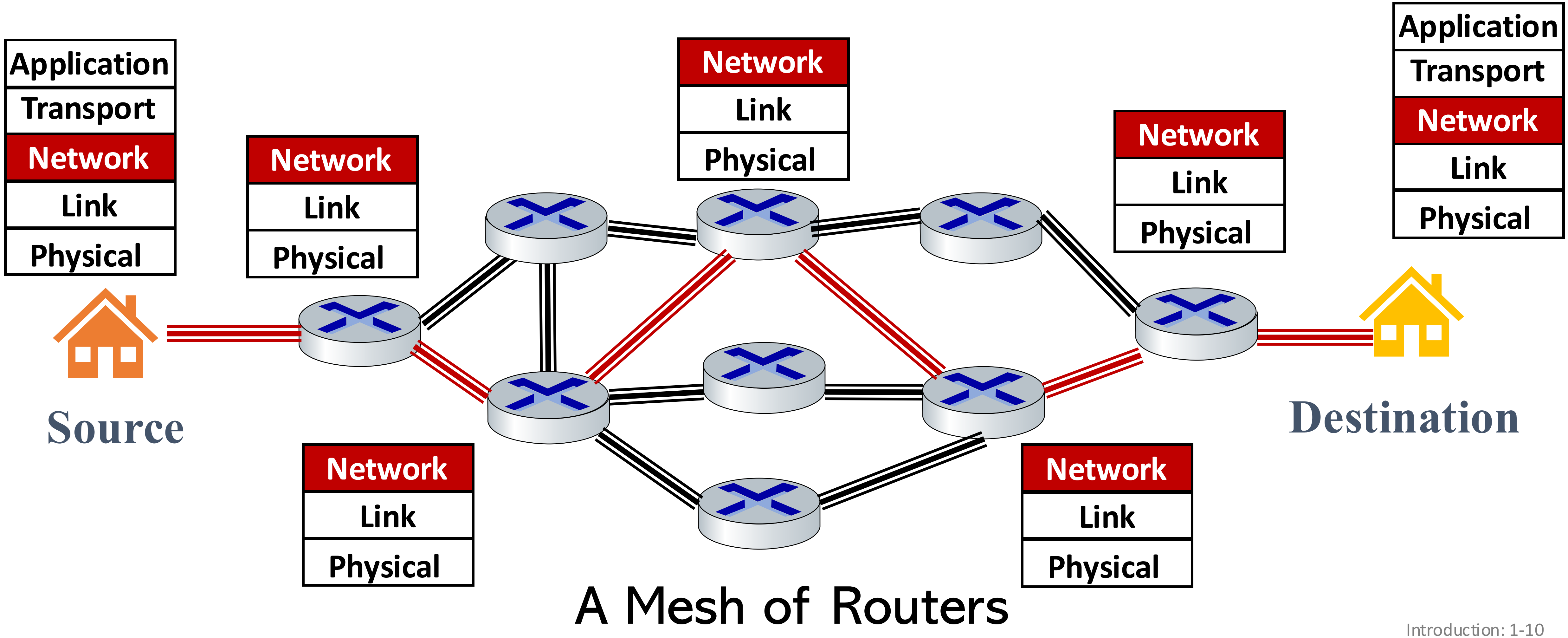
- Network layer: overview
  - data plane
  - control plane
- What’s inside a router
  - input ports, switching, output ports
  - buffer management, scheduling
- IP: the Internet Protocol
  - datagram format
  - addressing
  - network address translation
  - IPv6

- Generalized Forwarding, SDN
  - Match+action
  - OpenFlow: match+action in action
- Middleboxes

Application and transport layer is end-to-end



Network-layer is in every network device



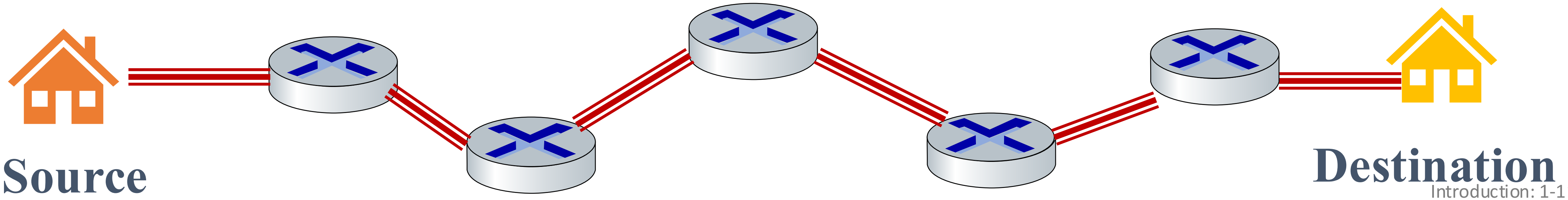
Network layer: data plane, control plane

Data plane:

- *local*, per-router function
- determines how datagram arriving on router input port is forwarded to router output port

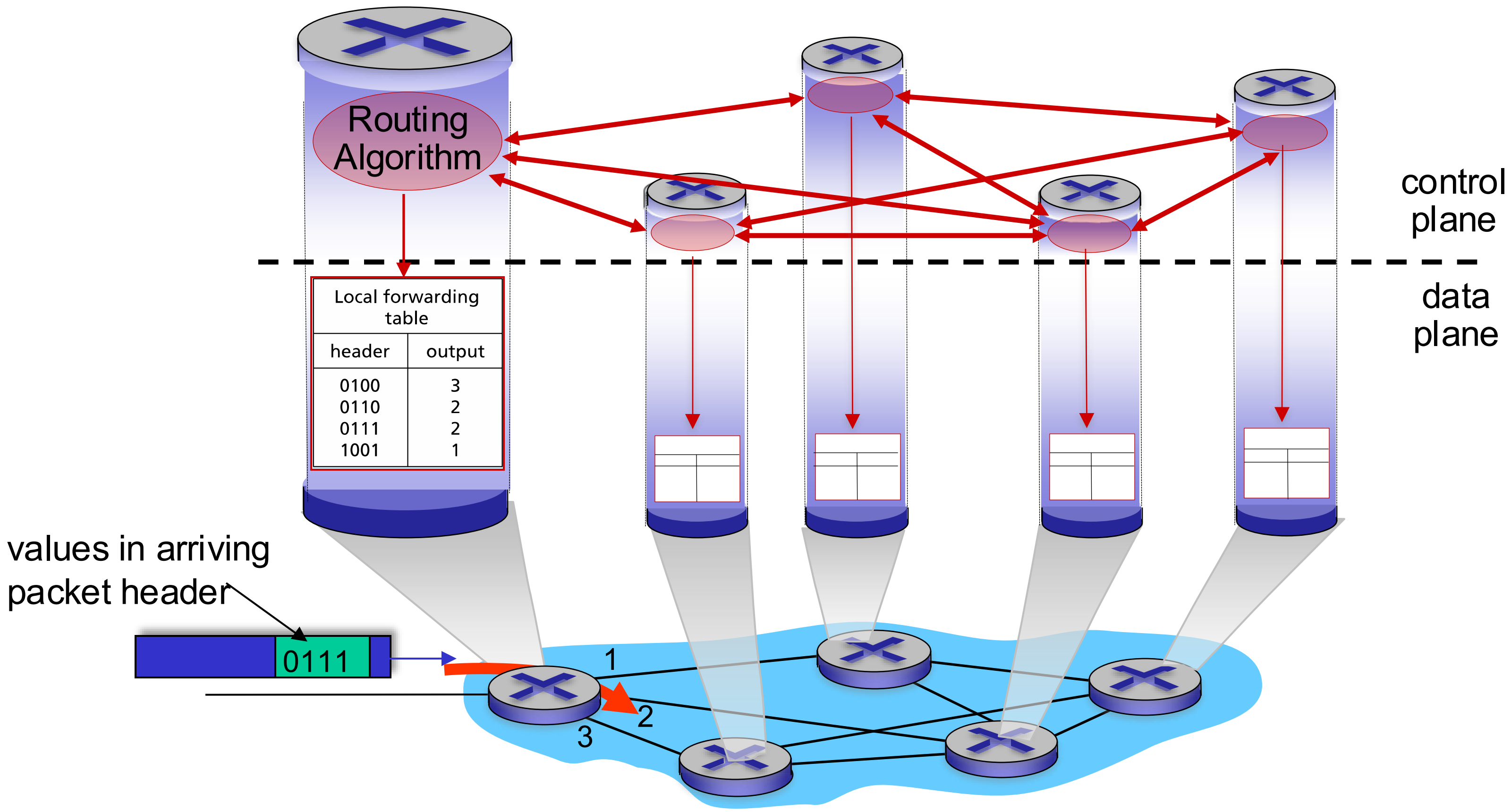
Control plane

- *network-wide* logic
- two control-plane approaches:
  - *traditional routing algorithms:* implemented in routers
  - *software-defined networking (SDN)*: implemented in (remote) servers



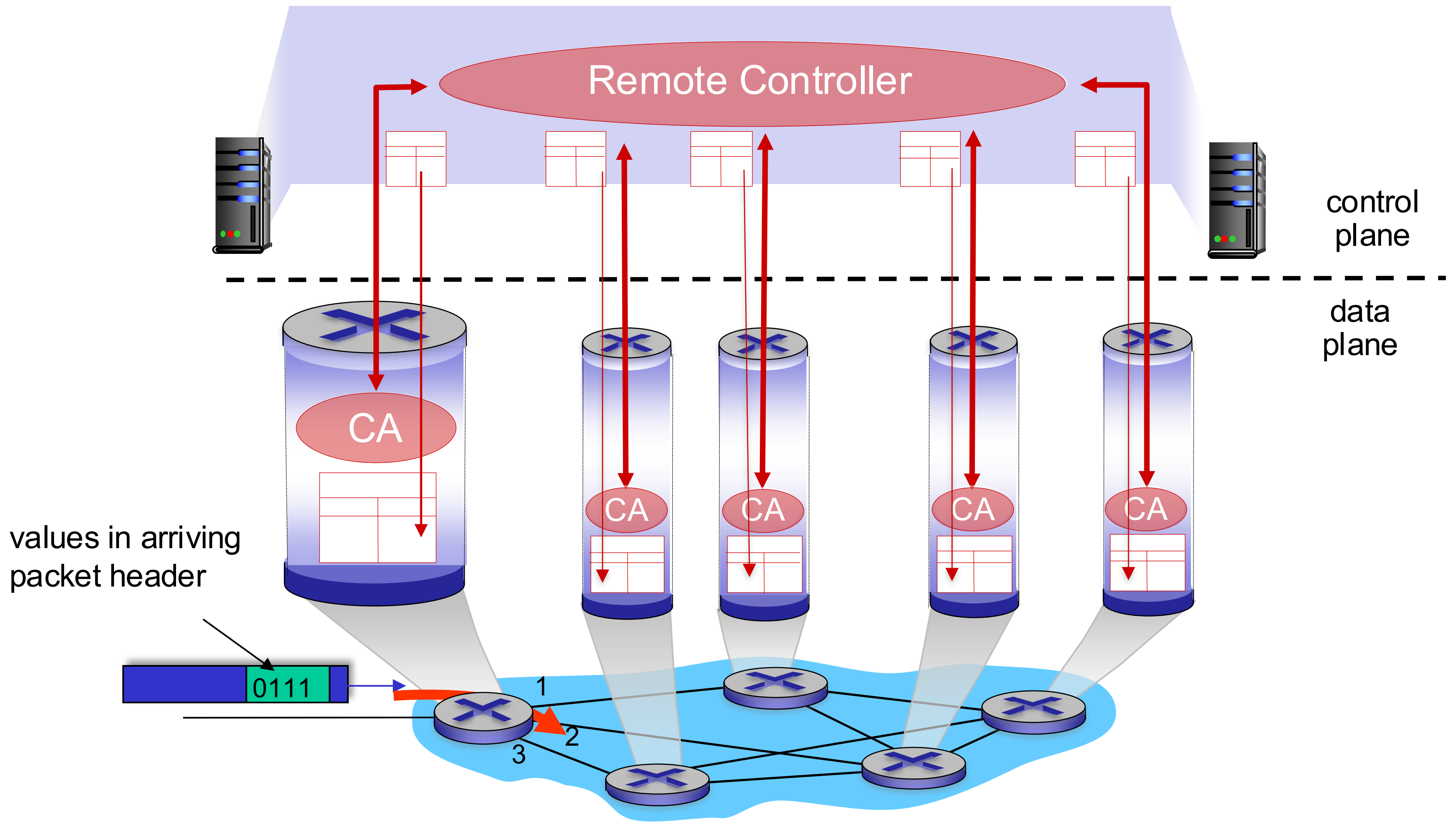
Control plane: Per-router control plane

Individual routing algorithm components *in each and every router* interact in the control plane



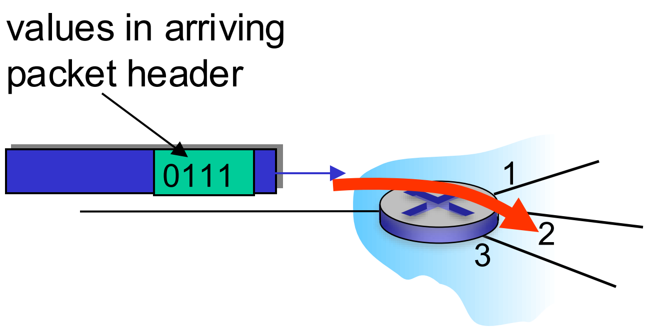
Control plane: Software-Defined Networking (SDN) control plane

Remote controller computes, installs forwarding tables in routers



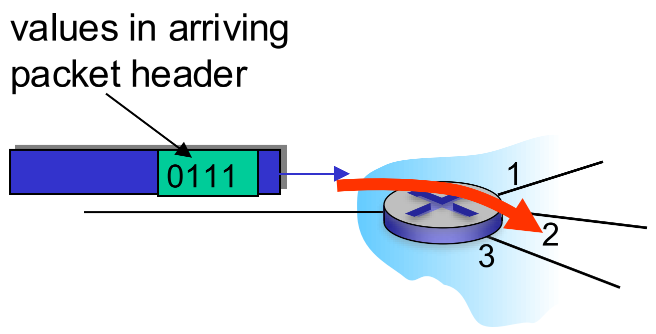
Forwarding Table

IP Address Range		Forwarding Interface
192.168.0.1	192.168.0.20	**1**
192.168.0.40	192.168.0.60	**2**
192.168.0.80	192.168.0.100	**3**



Forwarding Table

IP Address Range		Forwarding Interface
192.168.0.1	192.168.0.20	**1**
192.168.0.10	192.168.0.15	**3**
192.168.0.40	192.168.0.60	**2**
192.168.0.80	192.168.0.100	**3**



Longest prefix matching

IP Address Range		Forwarding Interface
192.168.0.1	192.168.0.20	1

IP Address Range	Forwarding Interface
11000000.10101000.00000000.00000001 11000000.10101000.00000000.00010100	1

Longest prefix matching

11000000.10101000.00000000.000*****

11000000.10101000.00000000.00000000

192.168.0.1

11000000.10101000.00000000.00011111

192.168.0.31

11000000.10101000.00000000.0000****

11000000.10101000.00000000.00000000

192.168.0.1

11000000.10101000.00000000.00001111

192.168.0.15

Longest prefix matching

Highly important

longest prefix match

when looking for forwarding table entry for given destination address, use *longest* address prefix that matches destination address.

Destination Address Range	Link interface
11001000 00010111 00010*** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011*** ********	2
otherwise	3

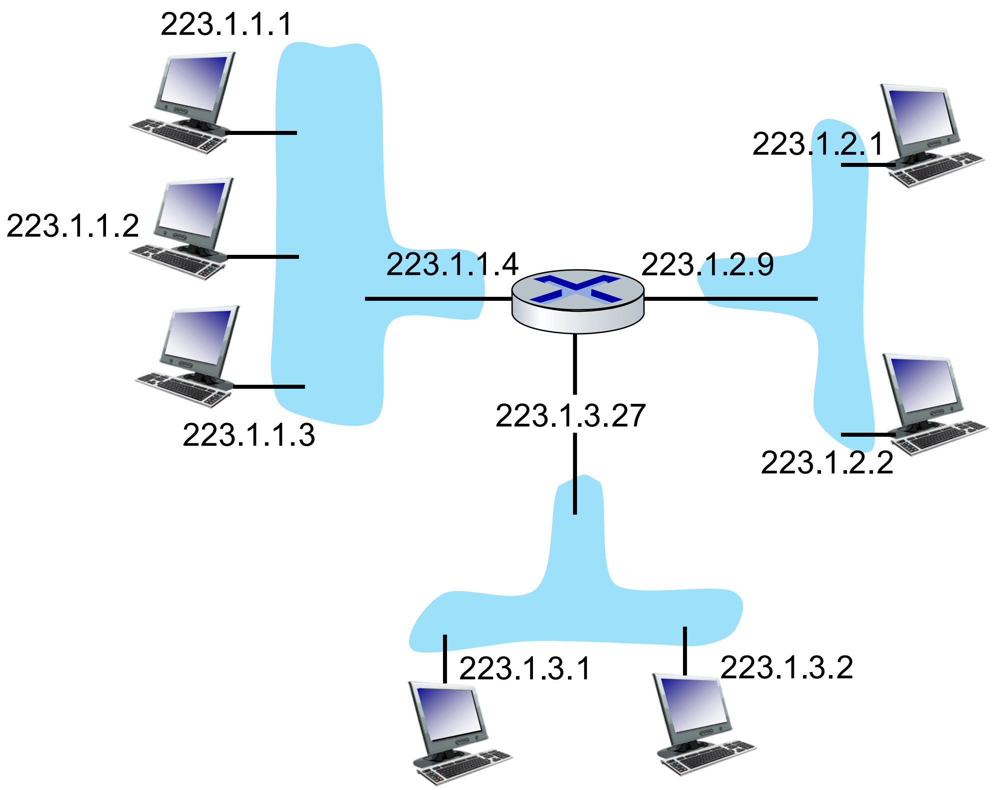
examples:

11001000 00010111 00010110 10100001 which interface?

11001000 00010111 00011000 10101010 which interface?

IP addressing: introduction

- IP address: 32-bit identifier associated with each host or router *interface*
- interface: connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)



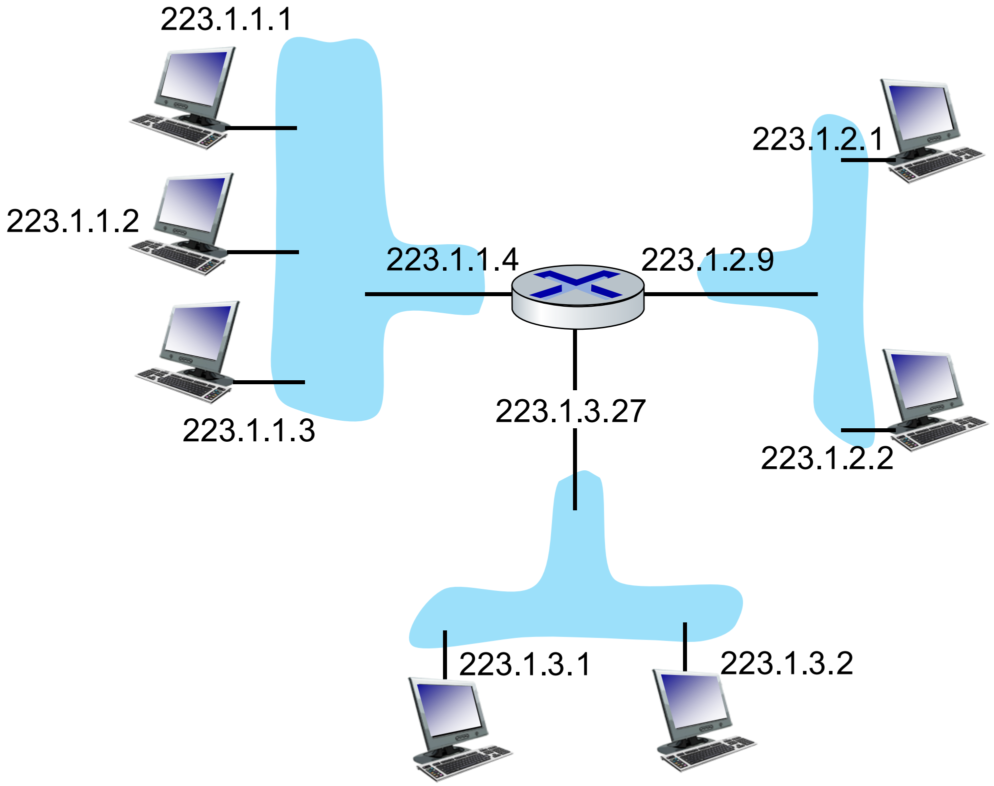
dotted-decimal IP address notation:

223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

IP addressing: introduction

- IP address: 32-bit identifier associated with each host or router *interface*
- interface: connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)



dotted-decimal IP address notation:

223.1.1.1 = 11011111 00000001 00000001 00000001

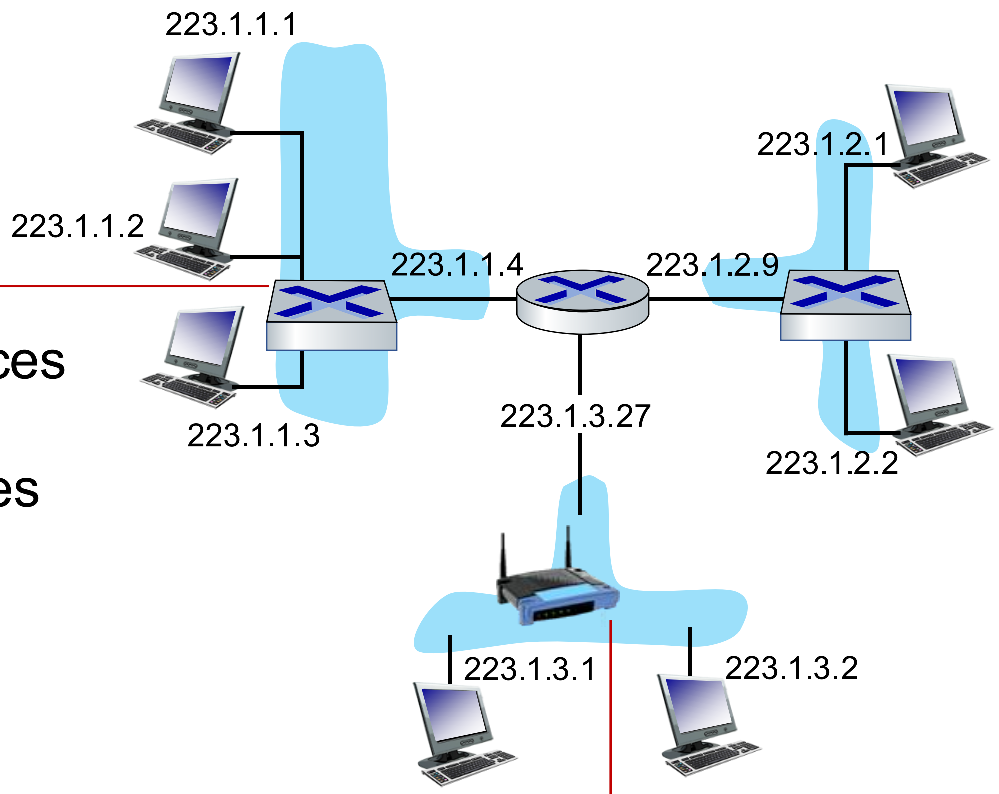
223 1 1 1

IP addressing: introduction

Q: how are interfaces actually connected?

A: we'll learn about that in chapters 6, 7

A: wired Ethernet interfaces connected by Ethernet switches



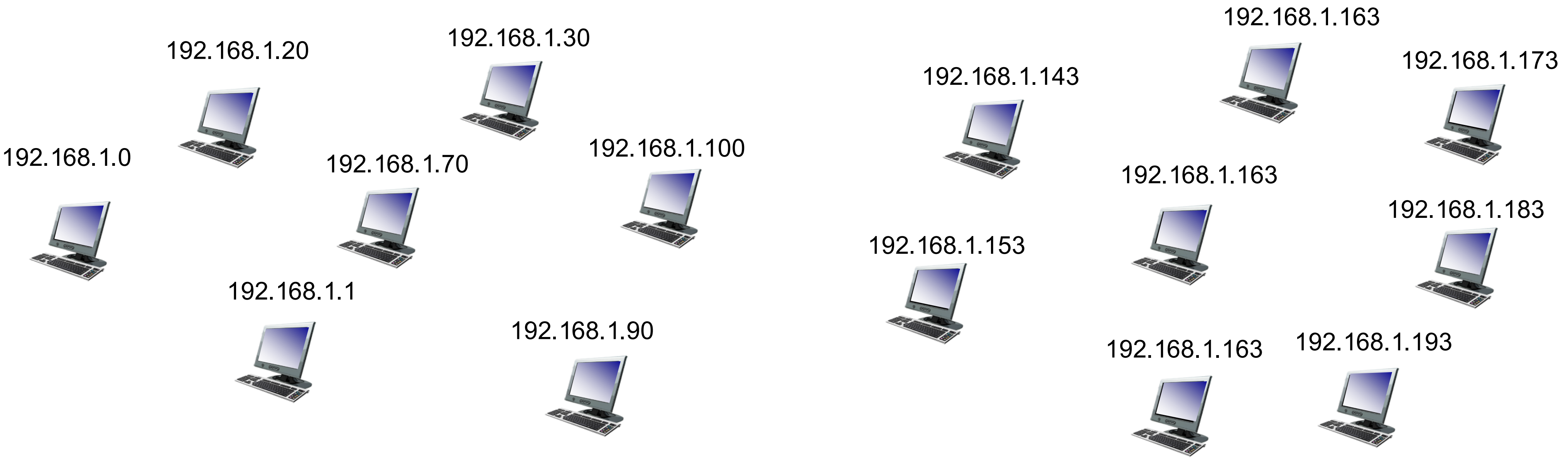
For now: don't need to worry about how one interface is connected to another (with no intervening router)

A: wireless WiFi interfaces connected by WiFi base station

Subnets

Highly important

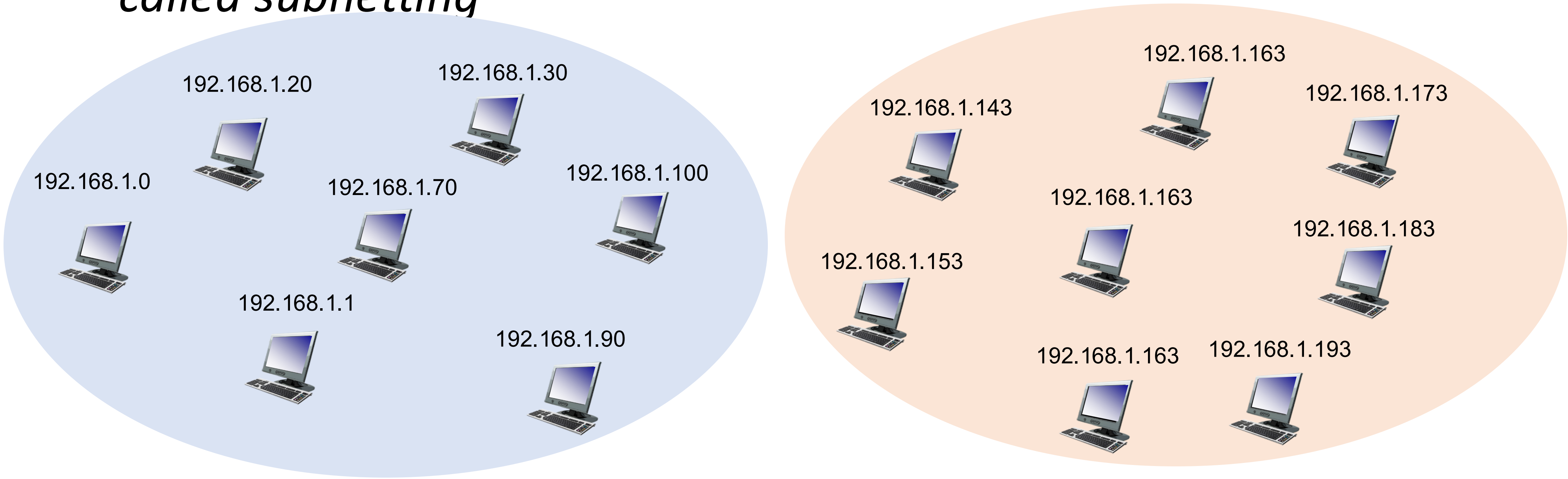
- *What's a subnet ?*
  - Subnet is a logical subdivision of an IP network.
  - *The practice of dividing a network into two or more networks is called subnetting*



An IP network: **192.168.1.0** to **192.168.1.255**

Subnets

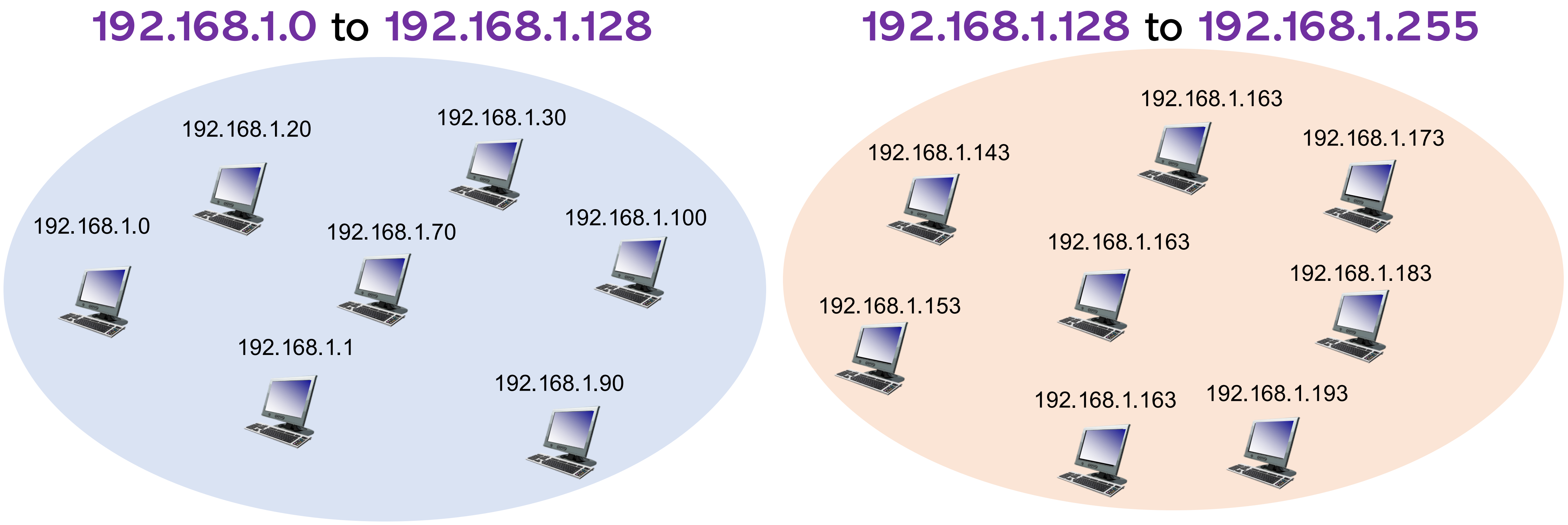
- *What's a subnet ?*
  - Subnet is a logical subdivision of an IP network.
  - *The practice of dividing a network into two or more networks is called subnetting*



An IP network: **192.168.1.0** to **192.168.1.255**

Subnets

- *What's a subnet ?*
  - Subnet is a logical subdivision of an IP network.



An IP network: 192.168.1.0 to 192.168.1.255

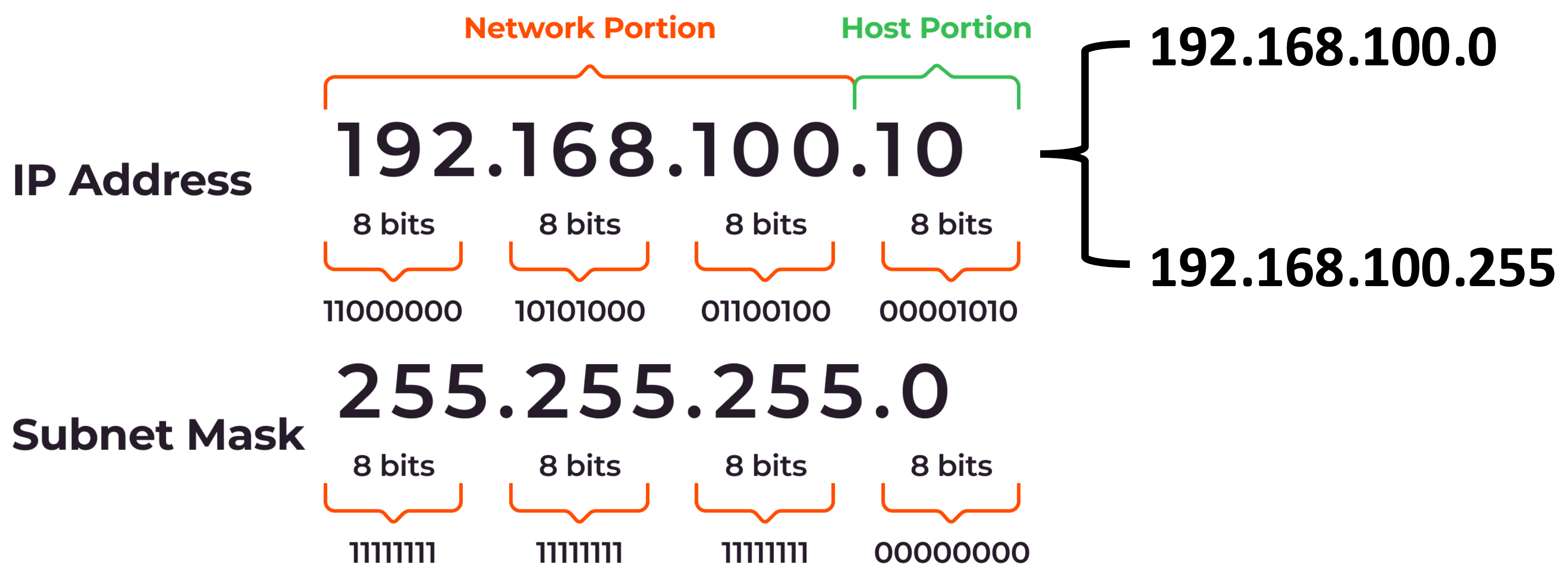
Subnet Mask

Highly important

An IP address has two parts: the network portion and the host portion

- Network portion identifies the network
- Host portion identifies the specific device within that network.

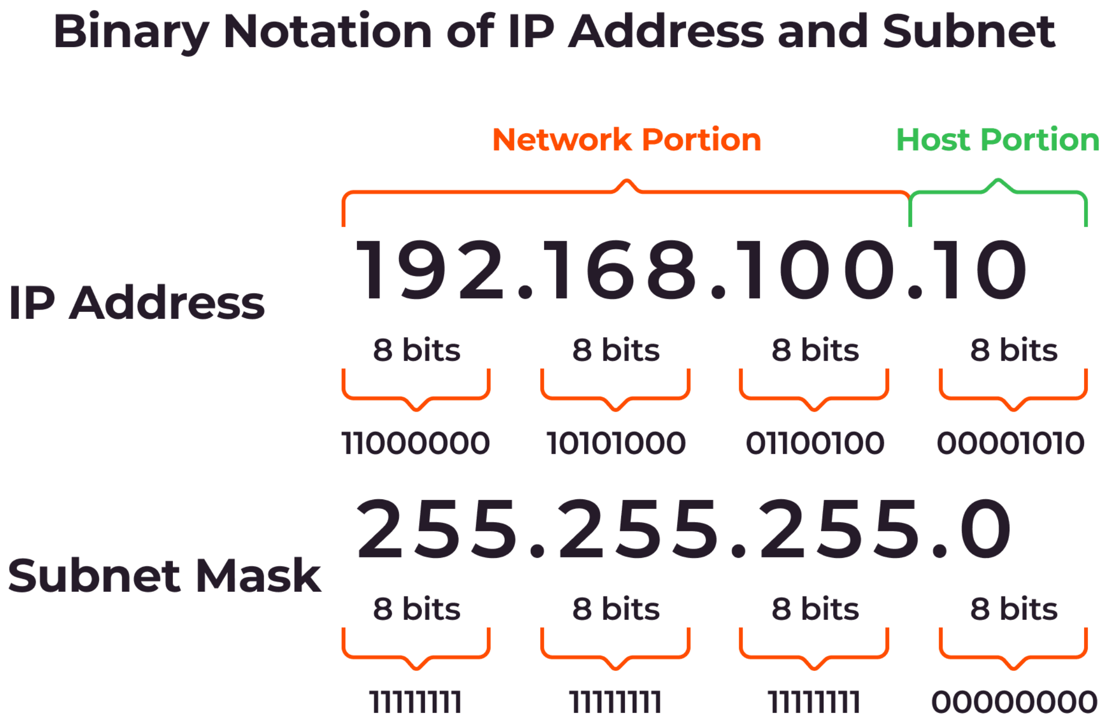
Binary Notation of IP Address and Subnet



Subnet Mask

An IP address has two parts: the network portion and the host portion

- Network portion identifies the network
- Host portion identifies the specific device within that network.



- The sequence of 1s in the subnet mask indicates which bits of the IP address belong to the network portion
- The **sequence of 0s** indicates which bits belong to the **host portion**.

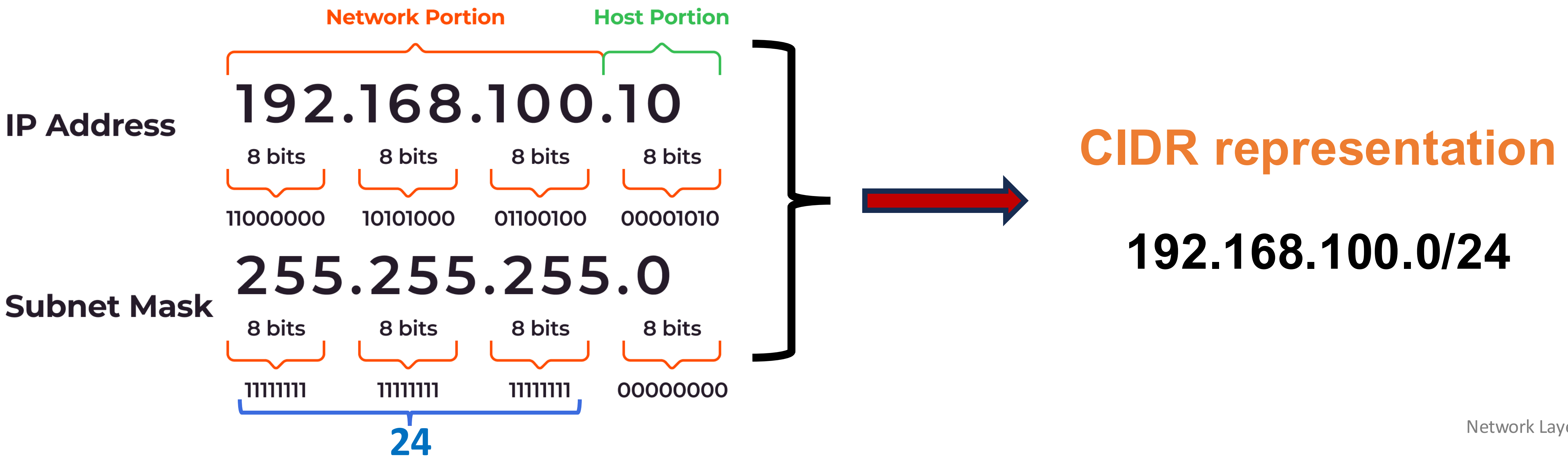
Subnet and CIDR

Highly important

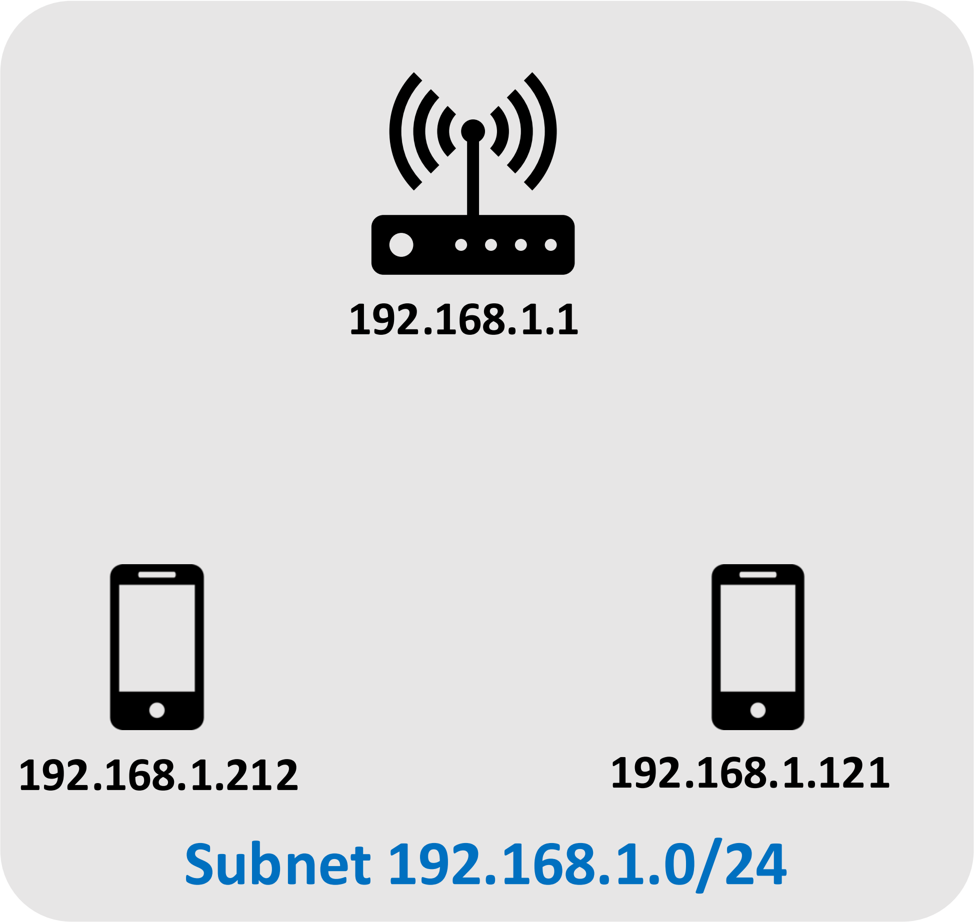
CIDR: Classless InterDomain Routing (pronounced "cider")

- address format: a.b.c.d/x, where x is # bits in subnet portion of address

Binary Notation of IP Address and Subnet



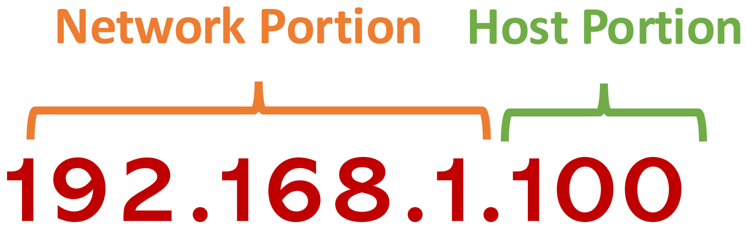
IP address: How to obtain it?



How does *host* get IP address?

- hard-coded by sysadmin in config file (e.g., /etc/rc.config in UNIX)
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play"

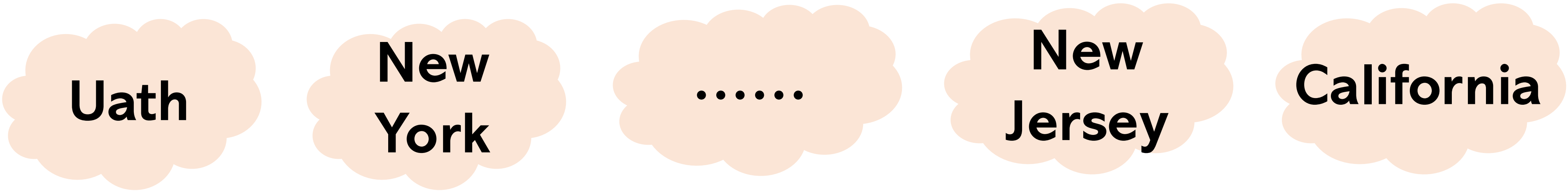
IP addresses: how to get one?



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

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

ISP's block	11001000 00010111 00010000 00000000	200.23.16.0/20



ISP can then allocate out its address space in 8 blocks:

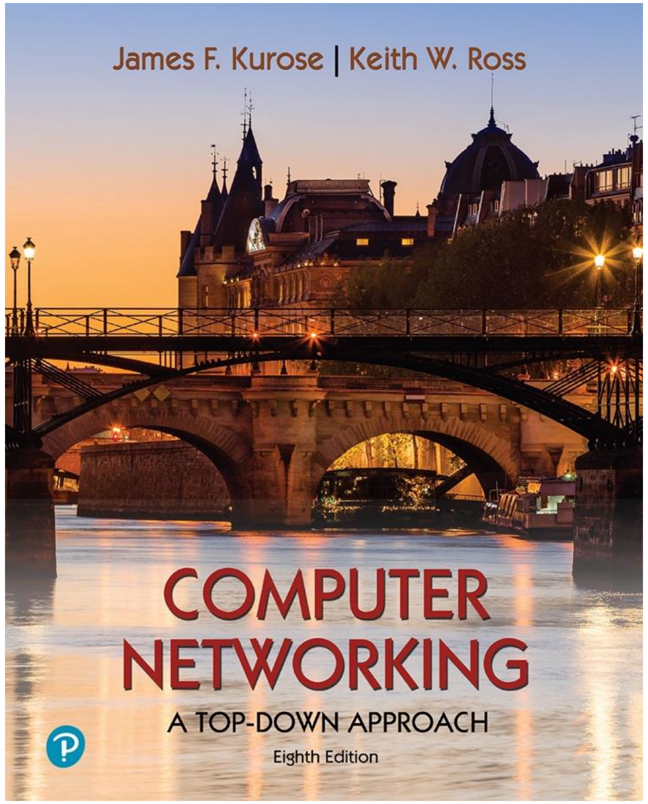
Organization 0	11001000 00010111 00010000 00000000	200.23.16.0/23
Organization 1	11001000 00010111 00010010 00000000	200.23.18.0/23
Organization 2	11001000 00010111 00010100 00000000	200.23.20.0/23
...	….. ….	….
Organization 7	11001000 00010111 00011110 00000000	200.23.30.0/23

Chapter 5
Network Layer: Control Plane

Yaxiong Xie

Department of Computer Science and Engineering
University at Buffalo, SUNY

Adapted from the slides of the book's authors



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Network layer: “control plane” roadmap

- introduction
- routing protocols
  - link state
  - distance vector
- intra-ISP routing: OSPF
- routing among ISPs: BGP
- SDN control plane
- Internet Control Message Protocol

Highly important

- network management, configuration
  - SNMP
  - NETCONF/YANG

Network layer: "control plane" roadmap

- introduction
- routing protocols
- intra-ISP routing: OSPF ✓
- routing among ISPs: BGP ✓
- SDN control plane
- Internet Control Message Protocol

No calculations

- network management, configuration
  - SNMP
  - NETCONF/YANG

Internet approach to scalable routing

aggregate routers into regions known as "autonomous systems" (AS) (a.k.a. "domains")

intra-AS (aka "intra-domain"): routing among routers *within same AS ("network")*

- all routers in AS must run same intra-domain protocol
- routers in different AS can run different intra-domain routing protocols
- gateway router: at "edge" of its own AS, has link(s) to router(s) in other AS'es

inter-AS (aka "inter-domain"): routing *among* AS'es

- gateways perform inter-domain routing (as well as intra-domain routing)

Network layer: "control plane" roadmap

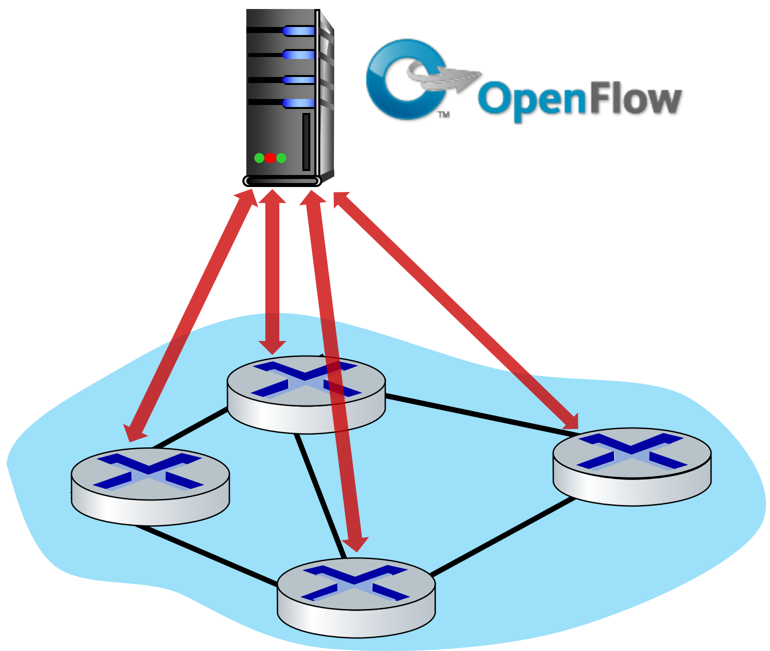
- introduction
- routing protocols
- intra-ISP routing: OSPF
- routing among ISPs: BGP
- SDN control plane
- Internet Control Message Protocol

- Measurement

OpenFlow protocol

- operates between controller, switch
- TCP used to exchange messages
  - optional encryption
- three classes of OpenFlow messages:
  - controller-to-switch
  - asynchronous (switch to controller)
  - symmetric (misc.)
- distinct from OpenFlow API
  - API used to specify generalized forwarding actions

OpenFlow Controller

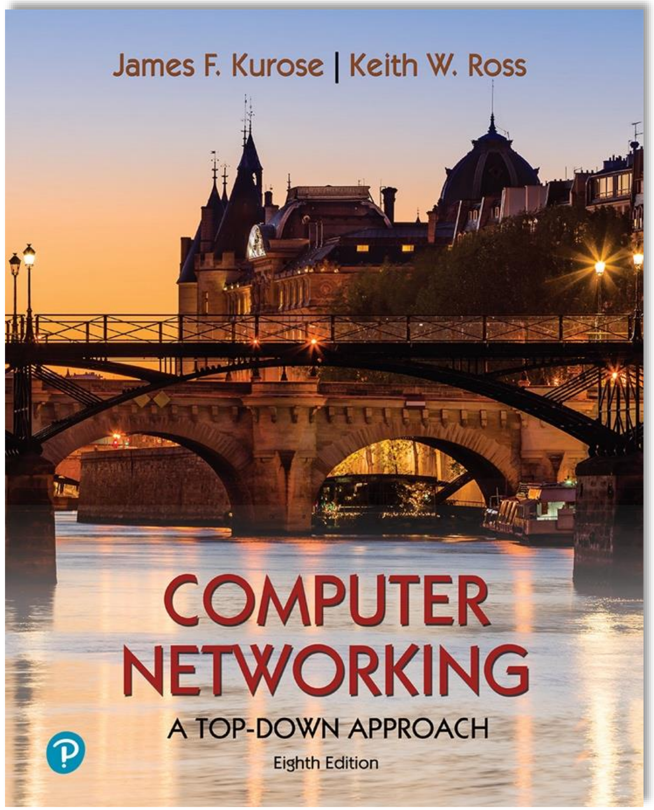


Chapter 6
The Link Layer and LANs

Yaxiong Xie

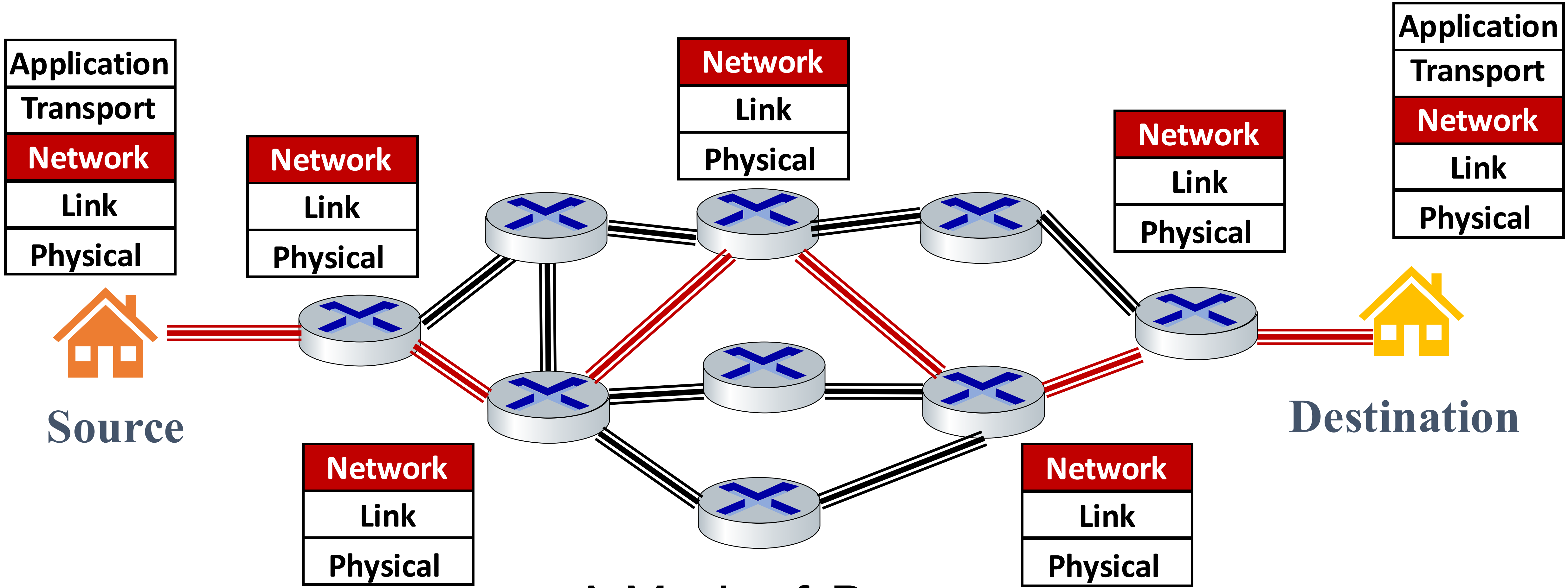
Department of Computer Science and Engineering
University at Buffalo, SUNY

Adapted from the slides of the book's authors



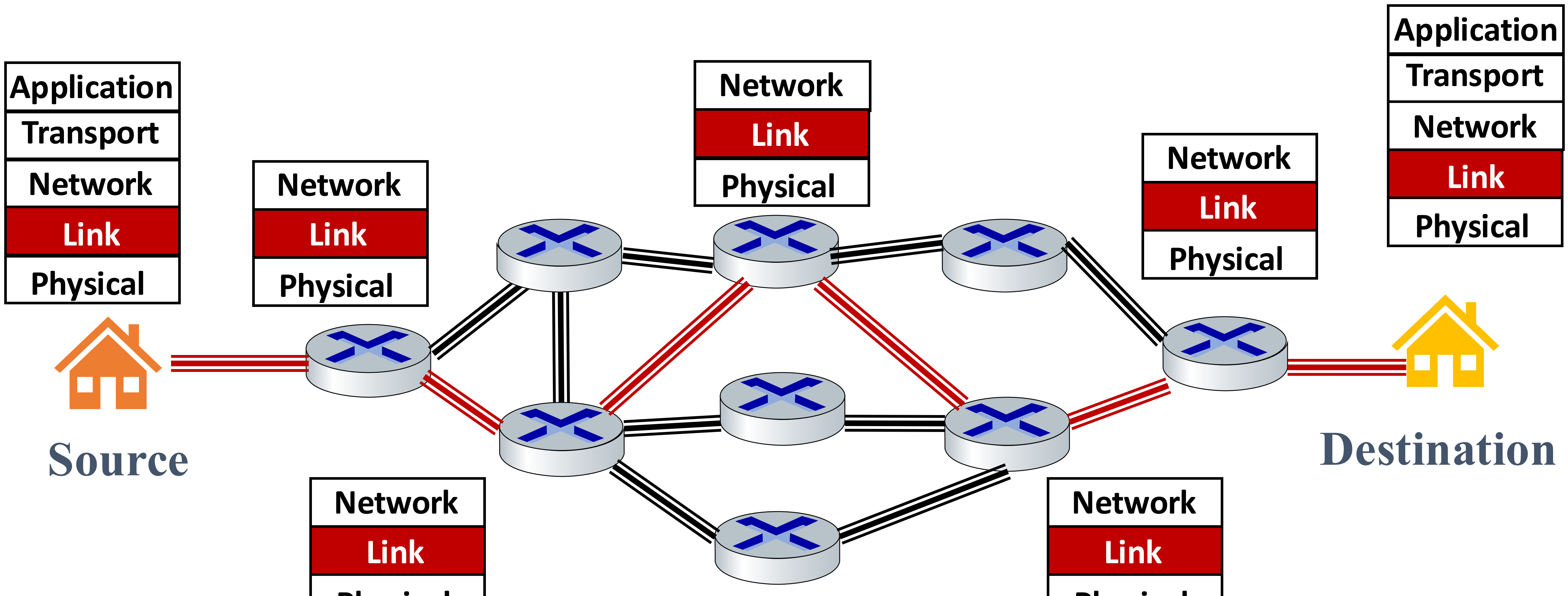
Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Network layer and Link layer is in every network device



A Mesh of Routers

Network layer and Link layer is in every network device



A Mesh of Routers

Link layer, LANs: roadmap

- introduction
- error detection, correction
- multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs
- link virtualization: MPLS
- data center networking

- a day in the life of a web request

MAC protocols: taxonomy

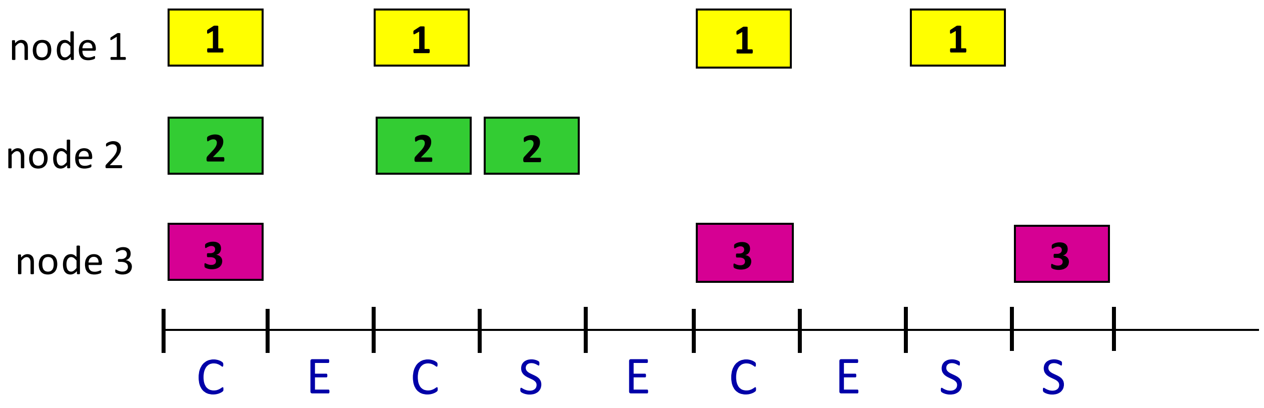
three broad classes:

- channel partitioning
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - allocate piece to node for exclusive use
- *random access*
  - channel not divided, allow collisions
  - "recover" from collisions
- "taking turns"
  - nodes take turns, but nodes with more to send can take longer turns

Slotted ALOHA

assumptions:

- all frames same size
- time divided into equal size slots (time to transmit 1 frame)
- nodes start to transmit only slot beginning
- nodes are synchronized
- if 2 or more nodes transmit in slot, all nodes detect collision



C: collision
S: success
E: empty

CSMA (carrier sense multiple access)

simple CSMA: listen before transmit:

- if channel sensed idle: transmit entire frame
- if channel sensed busy: defer transmission

- human analogy: don't interrupt others!

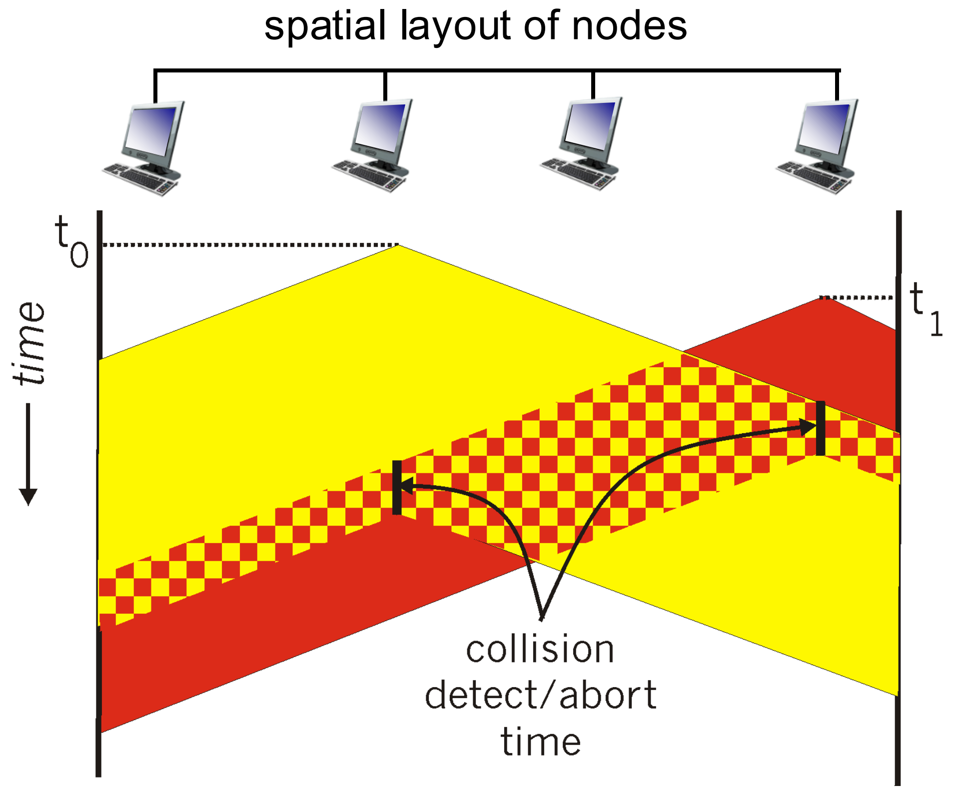
CSMA/CD: CSMA with *collision detection*

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- collision detection easy in wired, difficult with wireless

- human analogy: the polite conversationalist

CSMA/CD:

- CSMA/CS reduces the amount of time wasted in collisions
  - transmission aborted on collision detection



Link layer, LANs: roadmap

- introduction
- error detection, correction
- multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs
- link virtualization: MPLS
- data center networking

- a day in the life of a web request

Link layer, LANs: roadmap

- introduction
- error detection, correction
- multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs
- link virtualization: MPLS
- data center networking

- a day in the life of a web request

Link layer, LANs: roadmap

- introduction
- error detection, correction
- multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs
- link virtualization: MPLS
- data center networking

- a day in the life of a web request

Link layer, LANs: roadmap

- introduction
- error detection, correction
- multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs
- link virtualization: MPLS
- data center networking
- a day in the life of a web request

Self-learning

Forwarding table

Switch/Router difference

Link layer, LANs: roadmap

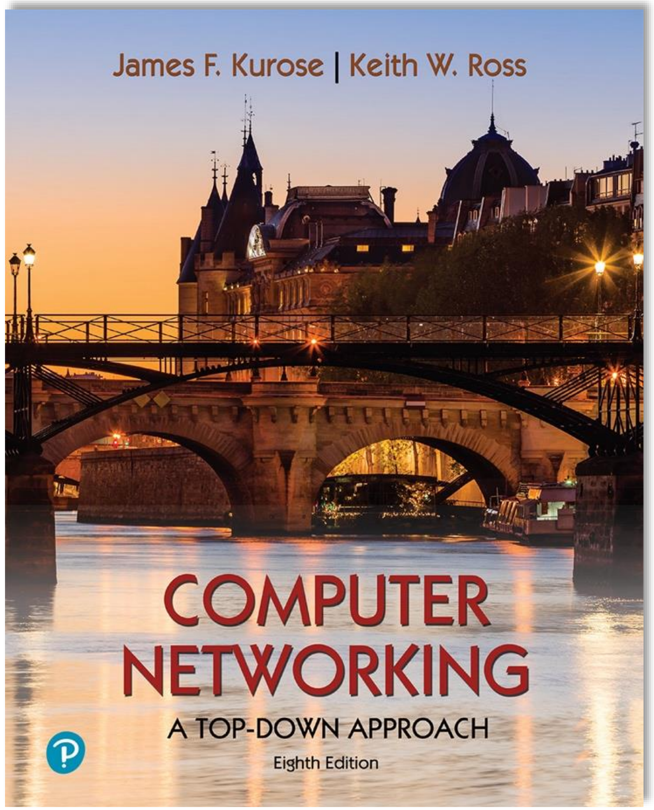
- introduction
- error detection, correction
- multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs
- link virtualization: MPLS
- data center networking

- a day in the life of a web request

Chapter 7
Wireless and Mobile Networks

Yaxiong Xie

Department of Computer Science and Engineering
University at Buffalo, SUNY



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

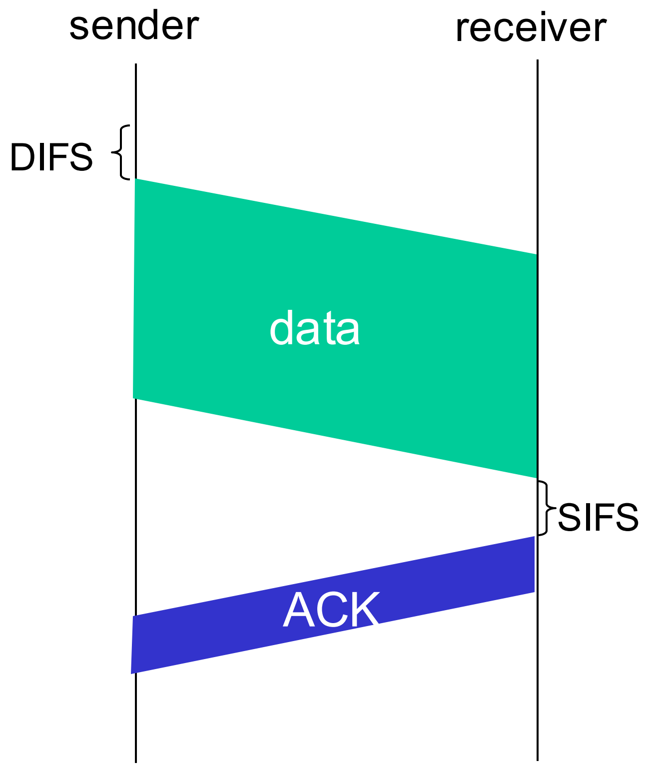
Adapted from the slides of the book's authors

IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)

2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2

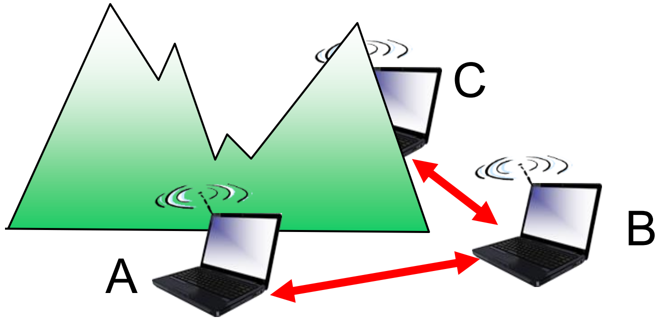


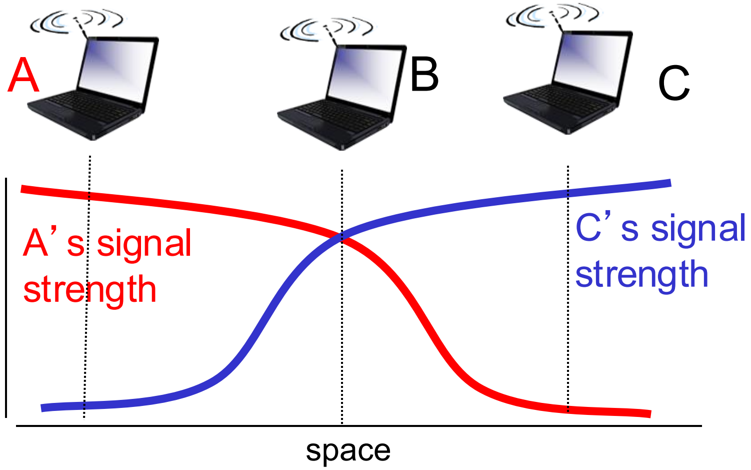
802.11 receiver

if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)

Wireless link characteristics (3)

Multiple wireless senders, receivers create additional problems (beyond multiple access):





Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B

Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

IEEE 802.11: multiple access

- avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with detected ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to sense collisions: high transmitting signal, weak received signal due to fading
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/<u>C</u>ollision<u>A</u>voidance