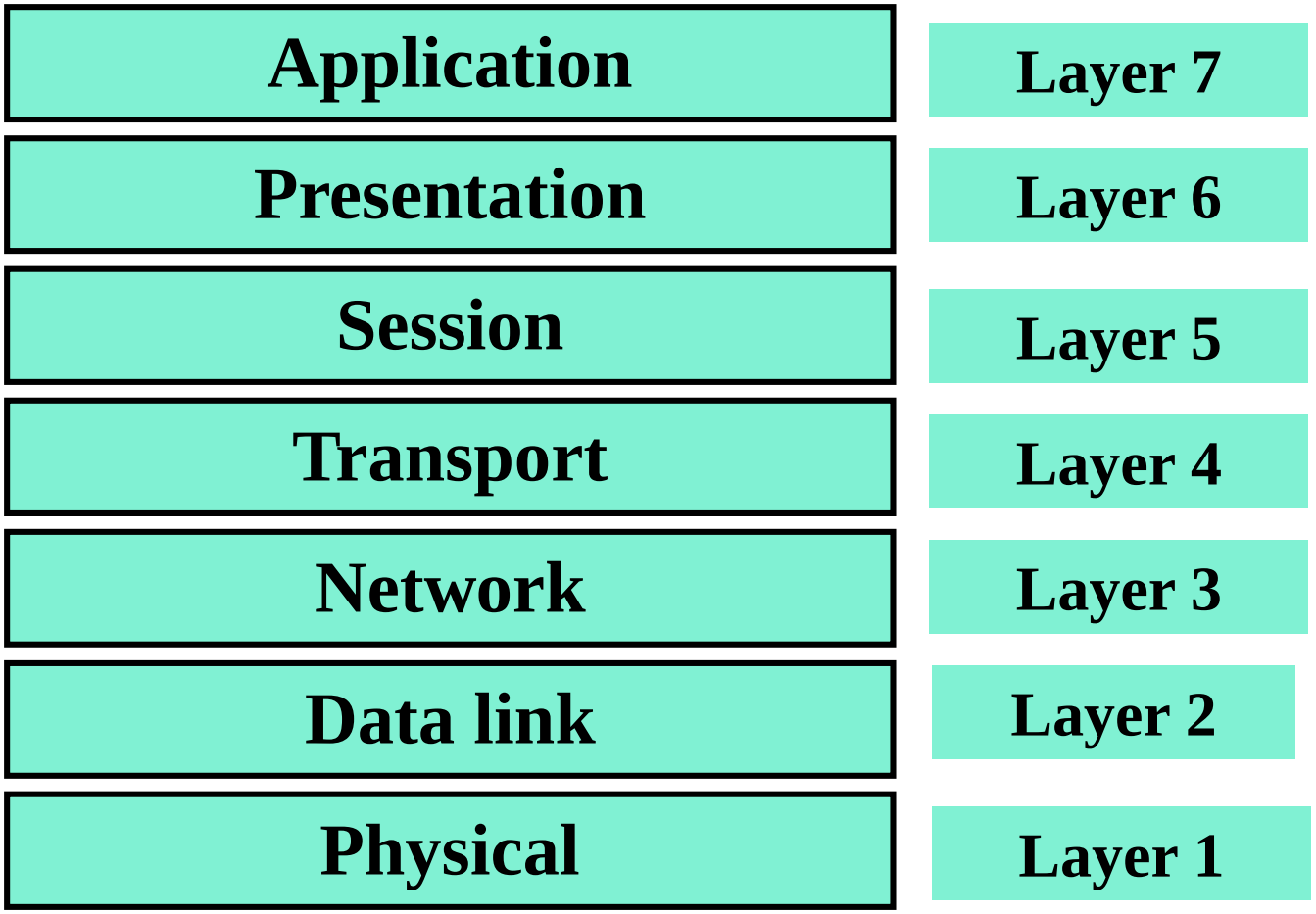
Chapter 10
Network Protocols

Outline

- Protocol: Set of defined rules to allow communication between entities
- Open Systems Interconnection (OSI)
- Transmission Control Protocol / Internetworking Protocol (TCP/IP)
- TCP over wireless
- Internet Protocol version 6 (IPv6)
- Summary

OSI Model



7 layers OSI model

Physical Layer Functions

- Establishment and termination of a connection to a communication medium
- Process for effective use of communication resources (e.g., contention resolution and flow control)
- Conversion between representation of digital data in the end user's equipment

Data Link Layer Functions

- Responds to service requests from the network layer and issues requests to the physical layer.
- Provides functional and procedural means to transfer data between network entities and to detect and correct errors that may occur in the physical layer.
- Concerned with:
  - Framing
  - Physical addressing (MAC address)
  - Flow Control
  - Error Control
  - Access Control

Network Layer Functions

- Provides for transfer of variable length sequences from source to destination via one or more networks
- Responds to service requests from the transport layer and issues requests to the data link layer
- Concerned with:
  - Data Packet
  - Logical addressing (IP address)
  - Routing

Transport Layer Functions

- **Provides transparent data transfer between end users**
- **Responds to service requests from the session layer and issues requests to the network layer.**
- **Concerned with:**
  - **Service-point addressing**
  - **Segmentation and reassembly**
  - **Connection control and Flow Control (end-to-end)**
  - **Error Control**

Session Layer Functions

- Provides mechanism for managing a dialogue between end-user application processes
- Responds to service requests from the presentation layer and issues requests to the transport layer
- Supports duplex or half- duplex operations.
- Concerned with:
  - Dialogue control
  - Synchronization (Check point)

Presentation Layer Functions

- Relieves application layer from concern regarding syntactical differences in data representation with end-user systems
- Responds to service requests from the application layer and issues requests to the session layer
- Concerned with:
  - Translation
  - Encryption
  - Compression

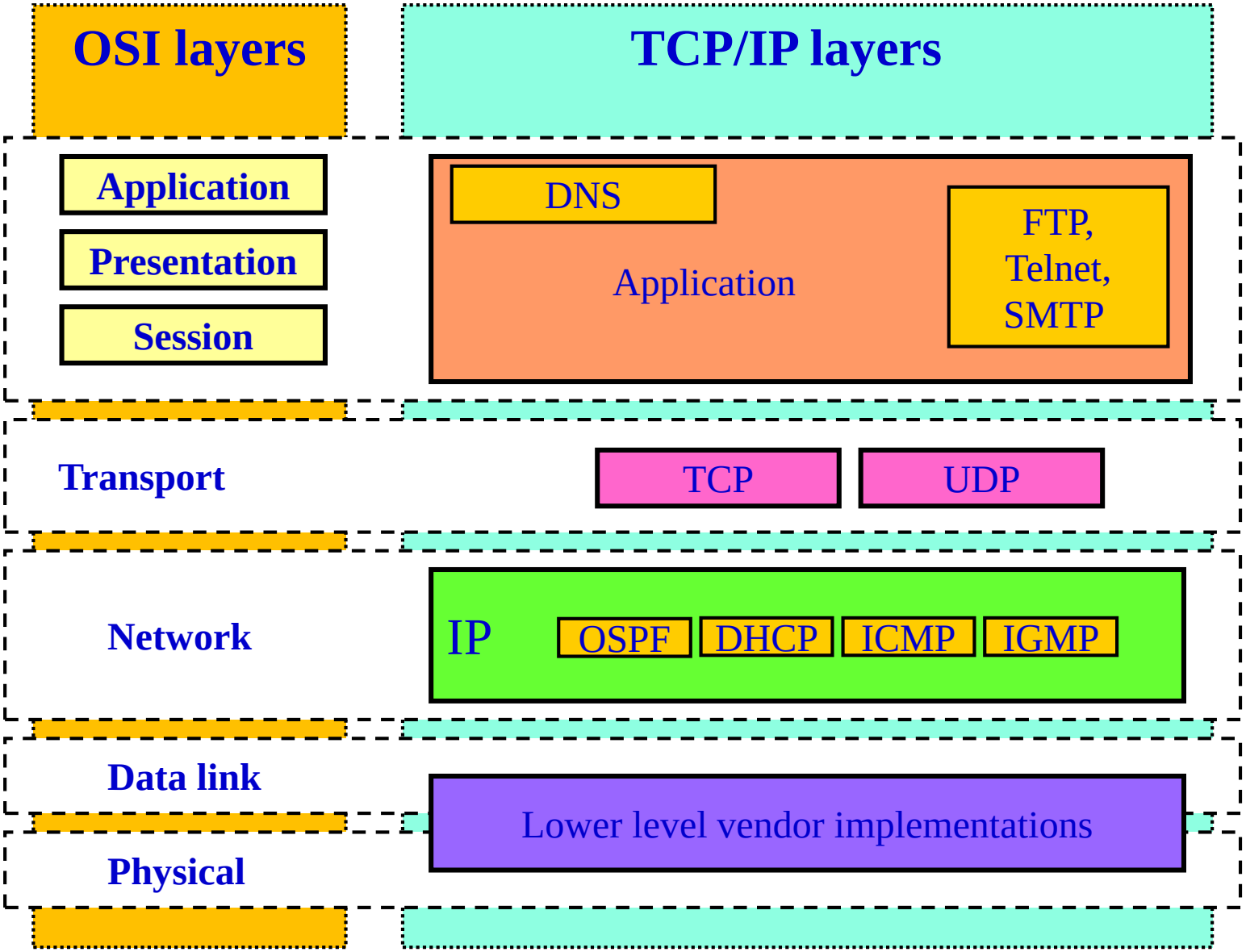
Application Layer Functions

- Interfaces directly to and performs common application services for application processes
- Issues service requests to the Presentation layer
- Specific services provided:
  - Network virtual terminal
  - File transfer, access and management
  - Mail services:SMTP
  - Directory services: DNS
  - HTTP, FTP, DHCP…

TCP/IP Protocol

- TCP/IP protocol consists of five layers
- The lower four layers correspond to the layer of the OSI model
- The application layer of the TCP/IP model represents the three topmost layers of the OSI model

TCP/IP Protocol stack



Internet Protocol (IP)

- Provides connection-less, best-effort service for delivery of packets through the inter-network
- Best-effort: No error checking or tracking done for the sequence of packets (datagrams) being transmitted
- Upper layer should take care of reliability of packet delivery
- Datagrams transmitted independently and may take different routes to reach same destination
- Fragmentation and reassembly supported to handle data links with different maximum – transmission unit (MTU) sizes

Internet Control Message Protocol (ICMP)

- Companion protocol to IP
- Provides mechanisms for error reporting and query to a host or a router
- Query message used to probe the status of a host or a router
- Error reporting messages used by the host and the routers to report errors

Internet Group Management Protocol (IGMP)

- Used to maintain multicast group membership within a domain
- Similar to ICMP, IGMP query and reply messages are used by routers to maintain multicast group membership
- Periodic IGMP query messages are used to find new multicast members within the domain of a router
- A member sends a IGMP join message to the router, which takes care of joining the multicast tree

Dynamic Host Configuration Protocol (DHCP)

- Used to assign IP addresses dynamically in a domain
- Extension to Bootstrap Protocol (BOOTP)
- Node Requests an IP address from DHCP server
- Helps in saving IP address space by using same IP address to occasionally connecting hosts

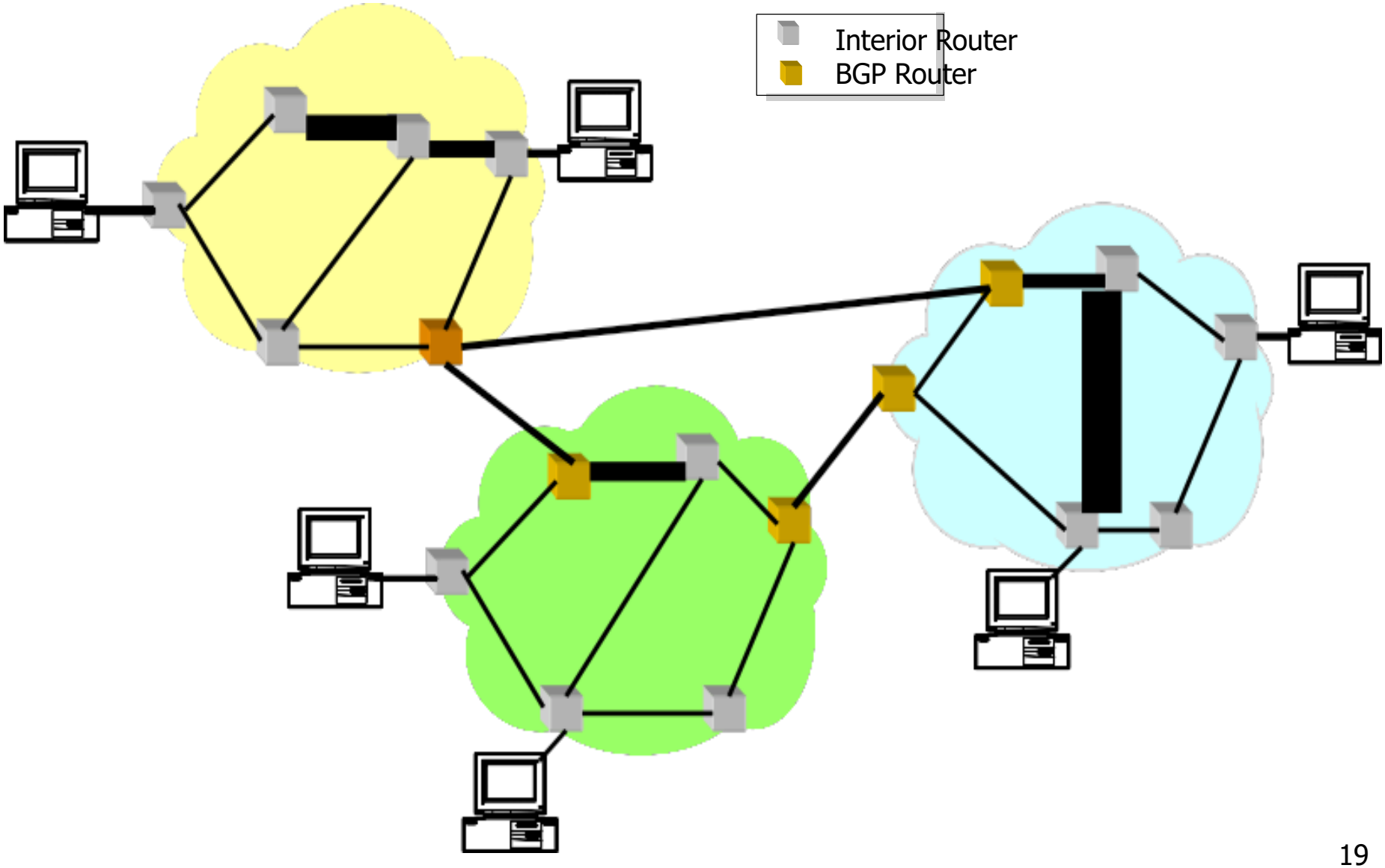
Internet Routing Protocols

- Routing Information Protocol (RIP)
  - An intra-domain distance vector routing protocol
  - Uses the Bellman-Ford algorithm to calculate routing table
  - Distance information about all the nodes is conveyed to the neighbors.
- Open Shortest Path First (OSPF)
  - Based on shortest path algorithm, sometimes also known as Dijkstra algorithm
  - Hosts are partitioned into autonomous systems (AS)
  - AS is further partitioned into OSPF areas that helps boarder routers to identify every single node in the area
  - Link-state advertisements sent to all routers within the same hierarchical area

Internet Routing Protocols

- **Border Gateway Protocol (BGP)**
  - **Inter-autonomous systems communicate with each other using path vector routing protocol**
  - **Each entry in the routing table contains the destination network, the next router, and the path to reach the destination**

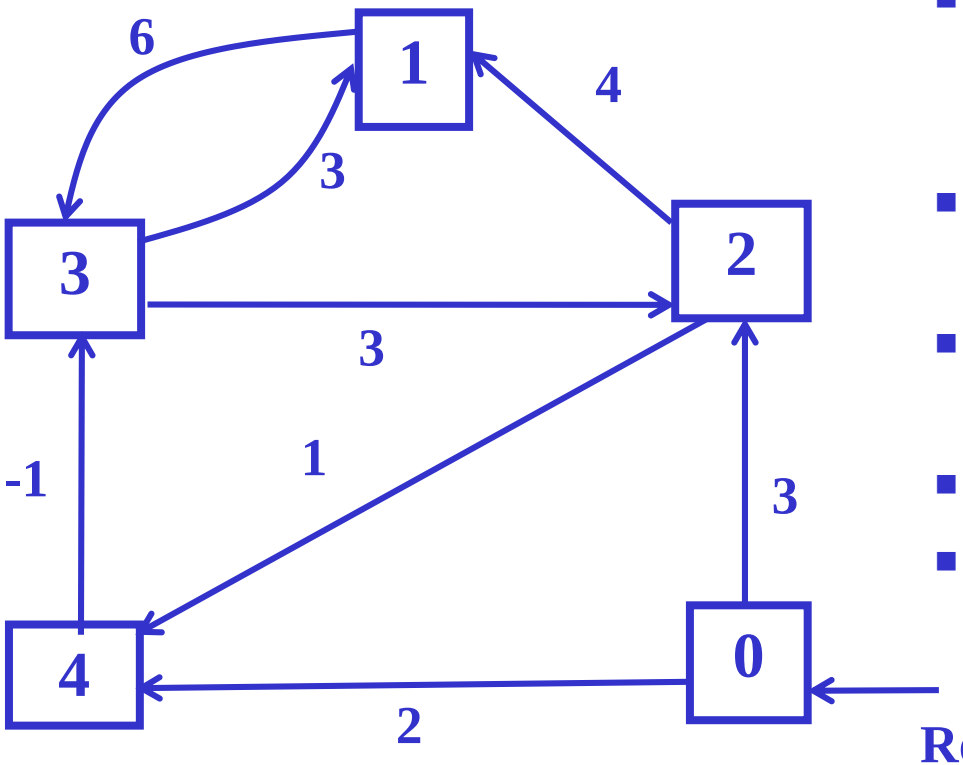
Example



TCP

- A connection-oriented reliable transport protocol that sends data as a stream of bytes.
- Divides the stream of data into smaller units called segments and mark each segment with a sequence number.
- Flow control and congestion control

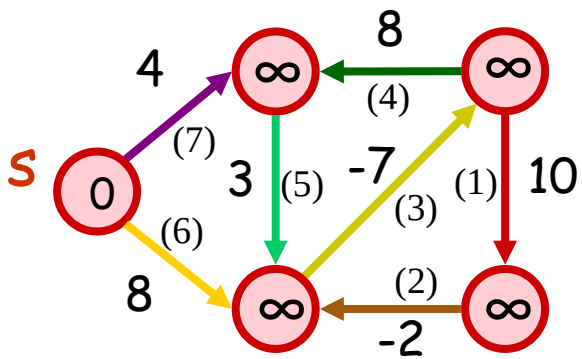
Bellman-Ford Algorithm



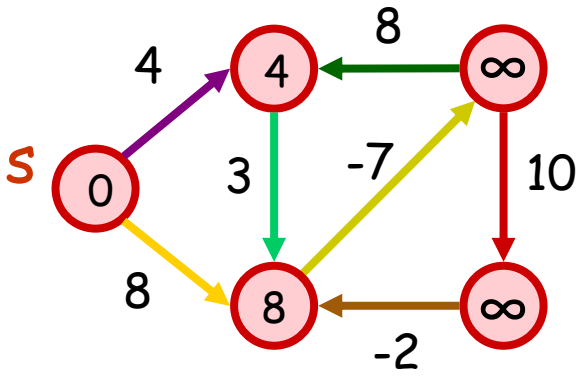
- A routing table maintained at each node, indicating the best known distance and next hop to get there
- Calculate ***w*(*u*,*v*)**, is the cost associated with edge ***uv***
- Calculate ***d*(*u*)**, the distance of node ***u*** from a root node
- For each ***uv***, find minimum ***d*(*u*,*v*)**
- Repeat ***n*-1** times for ***n*-nodes**

Abstract model of a wireless network in the form of a graph

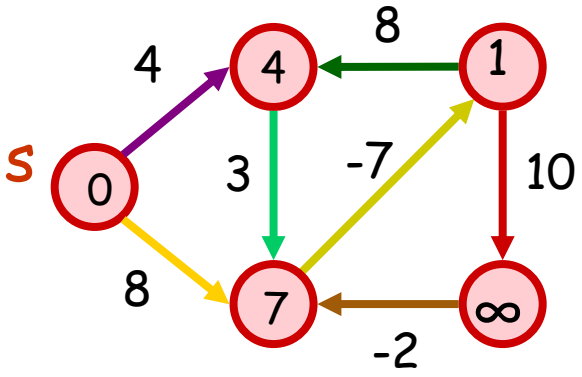
Example: Bellman-Ford Algorithm



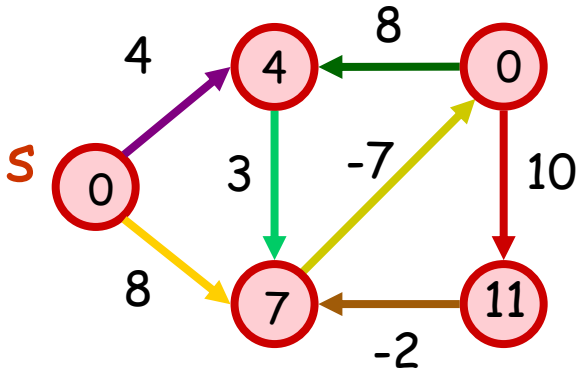
Relax all



Relax all

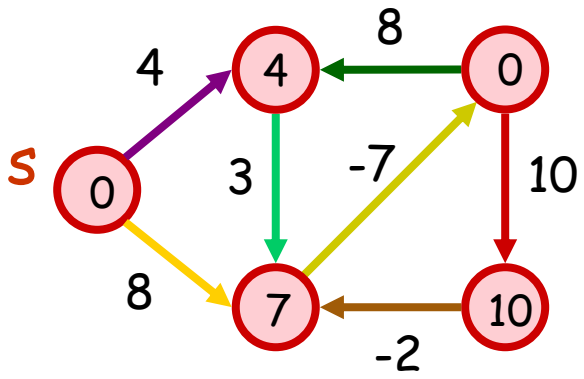


Relax all



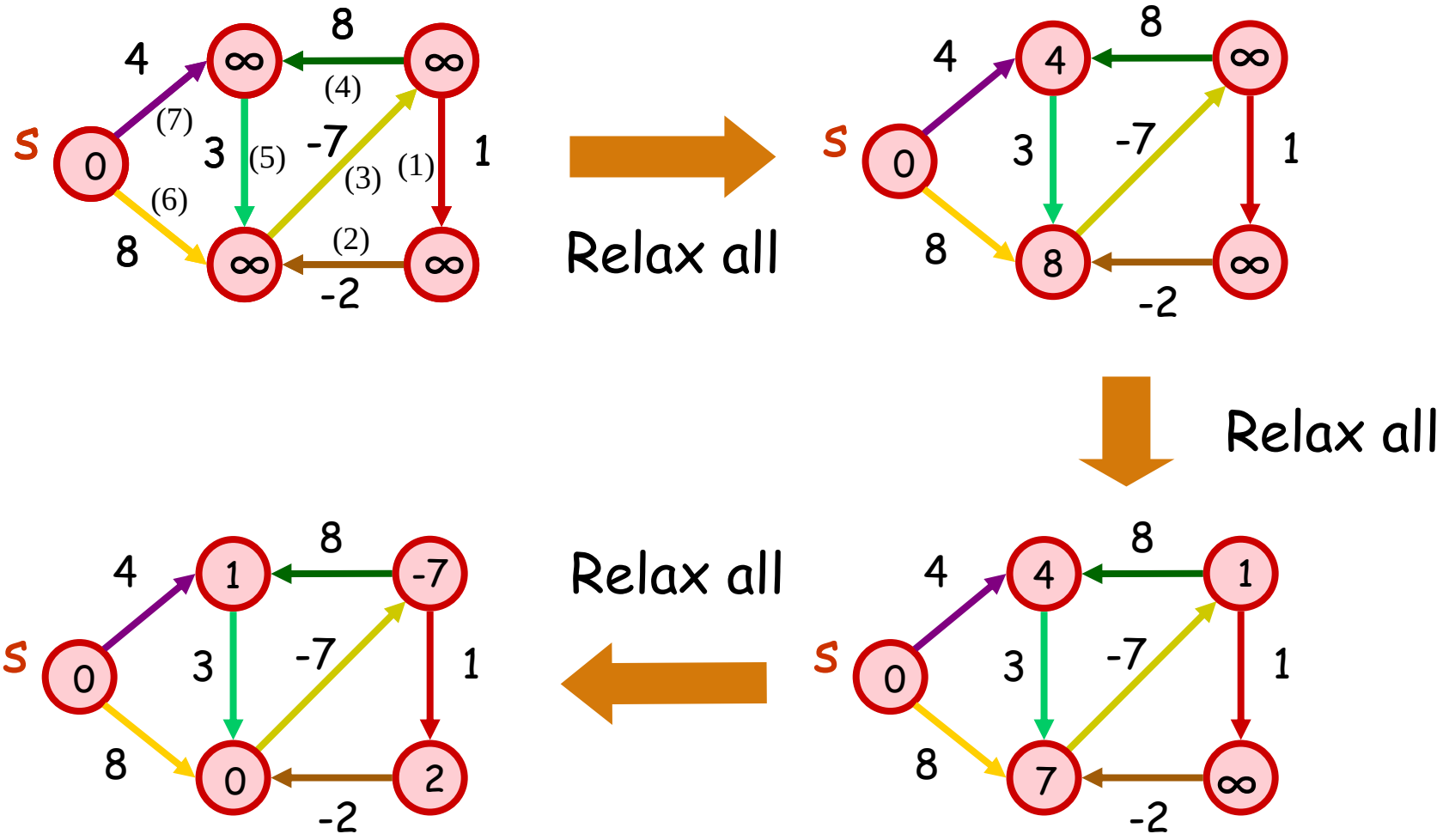
Example: Bellman-Ford Algorithm

After the 4th Relax all



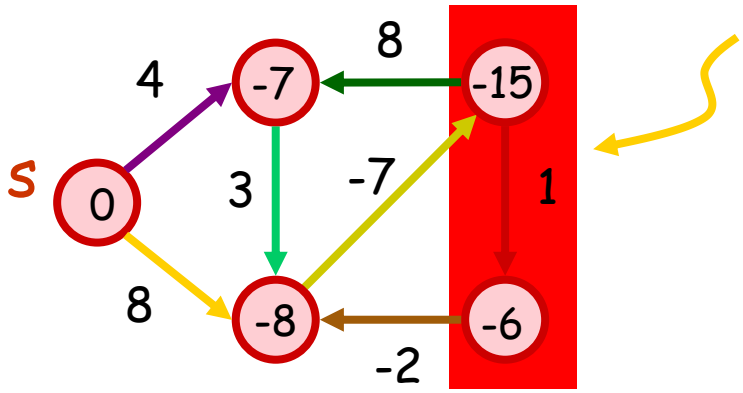
After checking, we found that there is nothing wrong ➔ distances are correct

Example: Bellman-Ford Algorithm



Example: Bellman-Ford Algorithm

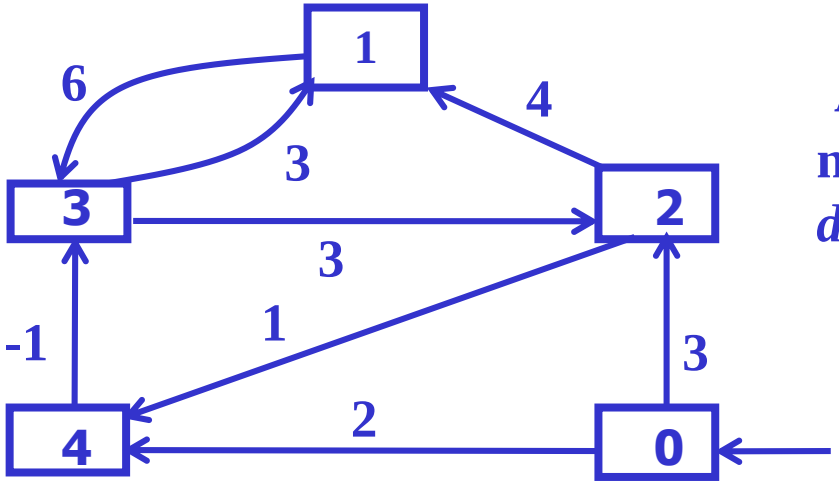
After the 4th Relax all



This edge shows something must be wrong …

After checking, we found that something must be wrong ➔ distances are incorrect

TCP (ctd)



Root

Abstract model of a wireless network in the form of a graph

$d(v) = \min[d(v), d(u) + w(u, v)]$

To Node	0	1	2	3	4
Pass 0	0	∞	∞	∞	∞
Pass 1	0	∞	3	∞	2
Pass 2	0	7	3	1	2
Pass 3	0	4	3	1	2
Pass 4	0	4	3	1	2

Successive calculation of distance $D(u)$ from node 0

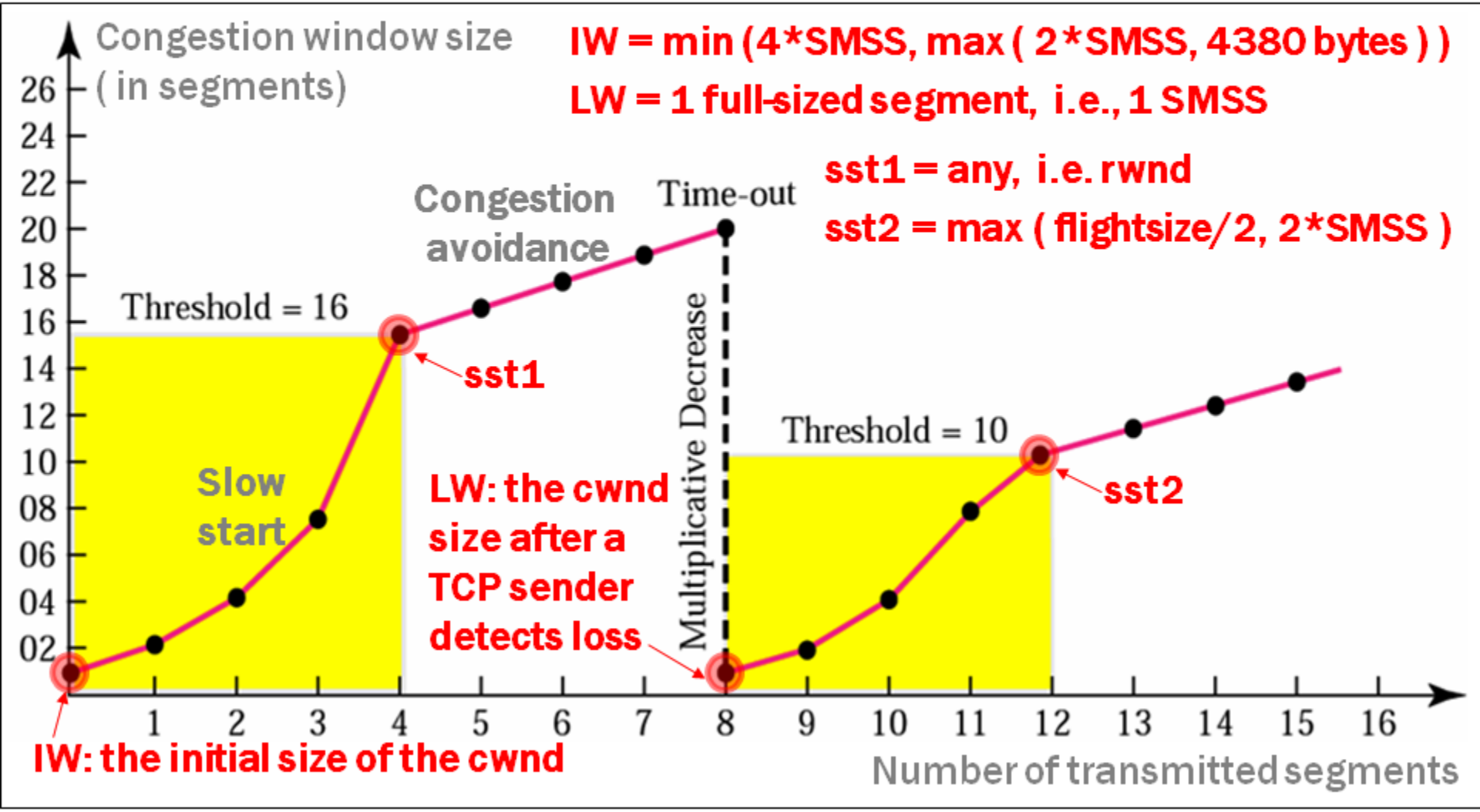
To Node	0	1	2	3	4
Pass 0	*	∞	∞	∞	∞
Pass 1	*	∞	0	∞	0
Pass 2	*	2	0	4	0
Pass 3	*	3	0	4	0
Pass 4	*	3	0	4	0

Predecessor from node 0 to other network nodes

TCP over Wireless

- The wireless domain is not only plagued by the mobility problem, but also by high error rates and low BW
- Traditional TCP: provides a connected-oriented, reliable, and byte stream service
- TCP functions: flow-control (controlled by sliding window), congestion-control (congestion window), data segmentation, retransmission, and recovery
- Slow Start: resets the congestion window (CW) size to one and let *threshold* to half of the current CW size
  - Double the CW on every successful transmission until the CW reach *threshold* and after that increases the CW by one for each successful transmission

Slow Start and Congestion Avoidance



Solutions for Wireless Environment

- Network layering provides good abstraction in the network design
- Wireless networks are interference limited, and the information delivery capability is closely dependent on current channel quality
- Adoption in physical and link layer broadcast could lead to efficient resource usage
- Protocol changes need to be made in MSs and mobile access points to ensure compatibility with existing TCP applications

End-to-End Solutions

- **TCP-SACK**
  - Selective Acknowledgement and Selective Retransmission.
  - Sender can retransmit missing data due to random errors/mobility
- **WTCP Protocol**
  - Separate flows for wired (Sender to AP) and wireless (AP to MS) segments of TCP connections
  - Local retransmission for mobile link breakage
  - AP sends ACK to sender after timestamp modification to avoid change in round trip estimates
- **Freeze-TCP Protocol**
  - Mobile detects impending handoff
  - Advertises Zero Window size, to force the sender into Zero Window Probe mode and prevent it from dropping its congestion window

End-to-End Solutions (Cont'd)

- Explicit Bad State Notification (EBSN)
  - Local Retransmission from BS (AP) to shield wireless link errors
  - EBSN message from BS to Source during local recovery
  - Source Resets its timeout value after EBSN
- Fast Retransmission Approach
  - Tries to reduce the effect of MS handoff
  - MS after handoff sends certain number of duplicate ACKs
  - Avoids coarse time-outs at the sender, accelerates retransmission

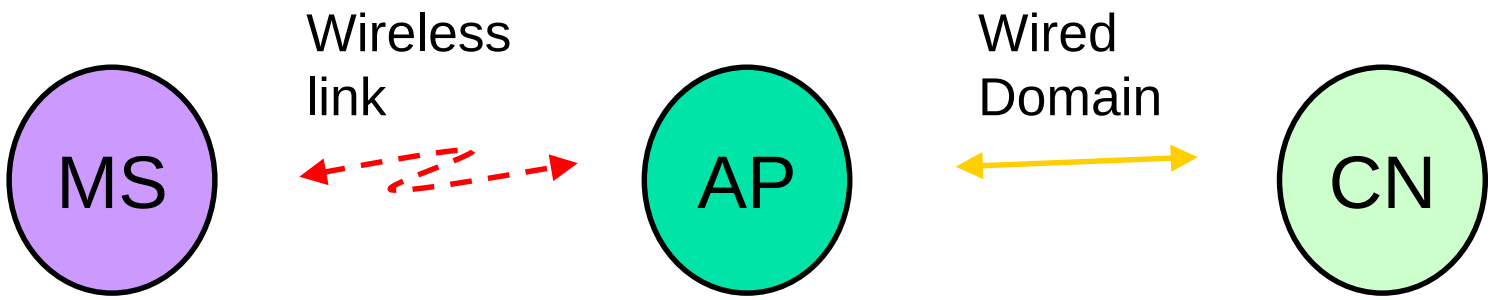
Link Layer Protocols

- **Snoop Protocol**
  - **Transport layer aware Snoop Agent at BS**
  - **Agent monitors all TCP segments destined to MS, caches it in buffer**
  - **Also monitors ACKs from MS**
  - **Loss detected by duplicate ACKs from MS or local time-out**
  - **Local Retransmission of missing segment if cached**
  - **Suppresses the duplicate ACKs**

Split TCP Approach

- **Indirect TCP: splits the TCP connection into two distinct connections, one is MS and BS and another is BS and corresponding node (CN)**
  - **The AP acts as a proxy for MS**
  - **The AP acknowledges CN for the data sent to MS and buffers this data until it is successfully transmitted to MS**
  - **Handoff may take a longer time as all the data acknowledged by AP and not transmitted to MS must be buffered at the new AP**

Indirect TCP



(Acts as proxy)

Split TCP Approach (Cont'd)

- **M-TCP Protocol**
  - **Split the connection into wired component and wireless component**
  - **BS relays ACKs for sender only after receiving ACKs from MS**
  - **In case of frequent disconnections, receiver can signal sender to enter in persist mode by advertising Zero Window size**

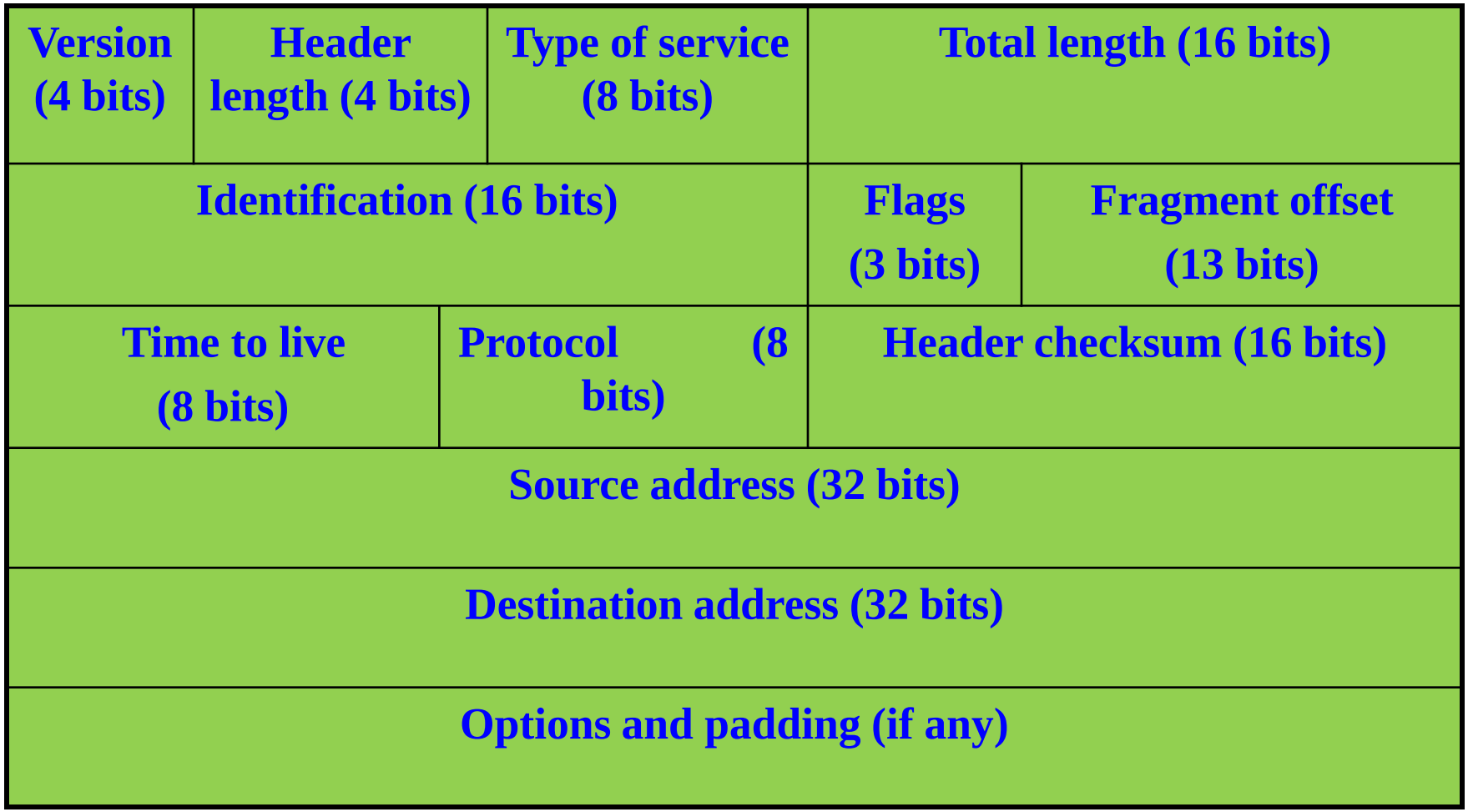
Impact of Mobility

- Handoffs occur in wireless domains when an MN moves into a new BS's domain
- The result of the packet loss during handoff is slow start
  - The solution involves artificially forcing the sender to go into fast retransmission mode immediately, by sending DUP ACK after the handoff, instead of go into slow start
- Using multicast: the MN is required to define a group of BSs that it is likely to visit in the near future
  - Reduce the handoff latency: Only one BS is in contact with the MN and the others buffer the packets addressed to the multicast address

Internet Protocol Version 6 (IPv6)

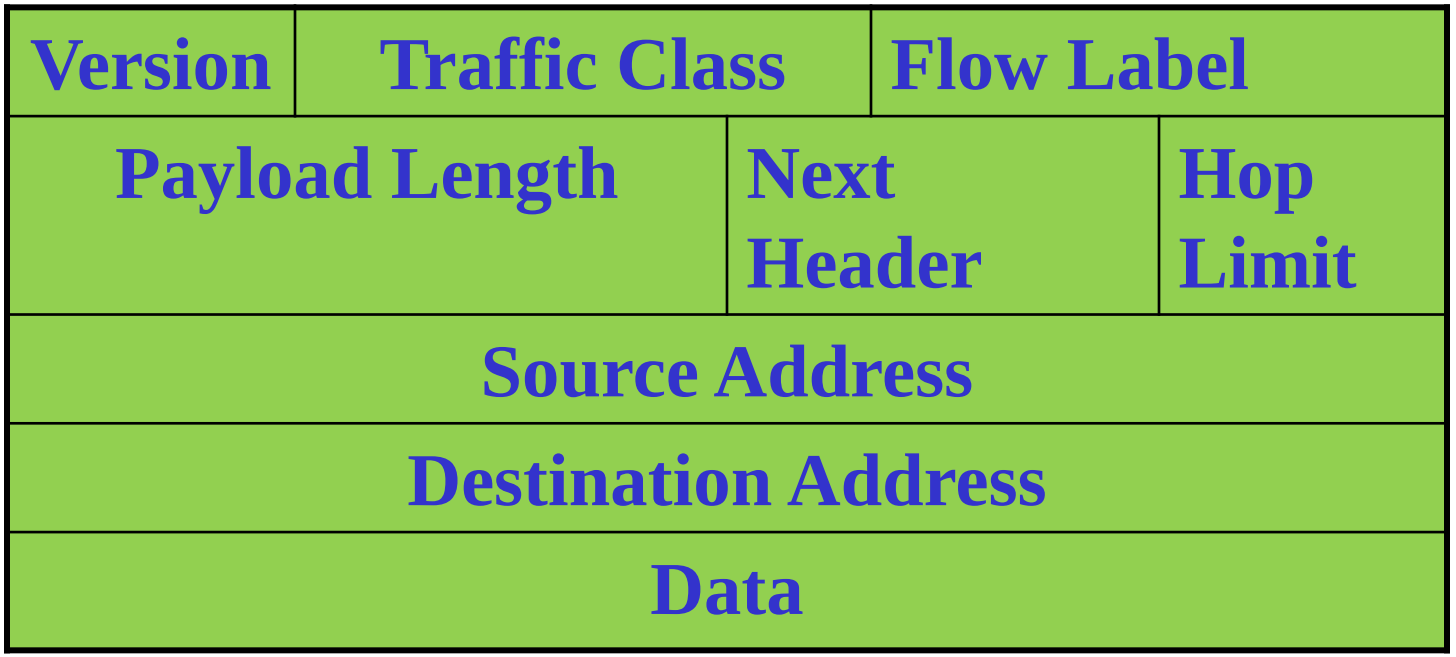
- **Designed to address the unforeseen growth of the internet and the limited address space provided by IPv4**
- **Features of IPv6:**
  - ✓ **Enhanced Address Space:** ***128 bits long, can solve the problem created by limited IPv4 address space (32 bits)***
  - ✓ **Resource Allocation:** ***By using "Flow Label", a sender can request special packet handling***
  - ✓ **Modified Address Format:** ***Options and Base Header are separated which speeds up the routing process***
  - ✓ **Support for Security:** ***Encryption and Authentication options are supported in option header***

IPv4 Header Format



IPv6 Header Format

- ✓Address Space
- ✓Resource Allocation
- ✓Modified Header Format
- ✓Support for Security



Format of IPv6

Name	Bits	Function
Version	4	IPv6 version number
Traffic Class	8	Internet traffic priority delivery value
Flow Label	20	Used for specifying special router handling from source to destination(s) for a sequence of packets
Payload Length	16, unsigned	Specifies the length of the data in the packet. When set to zero, the option is a hop-by-hop Jumbo payload
Next Header	8	Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field
Hop Limit	8, unsigned	For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit
Source Address	128	The IPv6 address of the sending node
Destination Address	128	The IPv6 address of the destination node

Differences between IPv4 and IPv6

- **Expanded Addressing Capabilities**
- **Simplified Header Format**
- **Improved Support for Options and Extensions**
- **Flow Labeling Capabilities**
- **Support for Authentication and Encryption**

Network Transition from IPv4 to IPv6

- **Dual IP-Stack:**
  - **IPv4-hosts and IPv4-routers have an IPv6-stack, this ensures full compatibility to not yet updated systems**
- **IPv6-in-IPv4 Encapsulation (Tunneling):**
  - **Encapsulate IPv6 datagram in IPv4 datagram and tunnel it to next router/host**

Homework

- Exercises: 10.4, 10.15, 10.19, 10.20 (Select anyone)
- Exercises: 10.2, 10.8, 10.11, 10.13, 10.16 (Select any one)