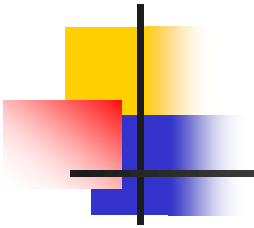


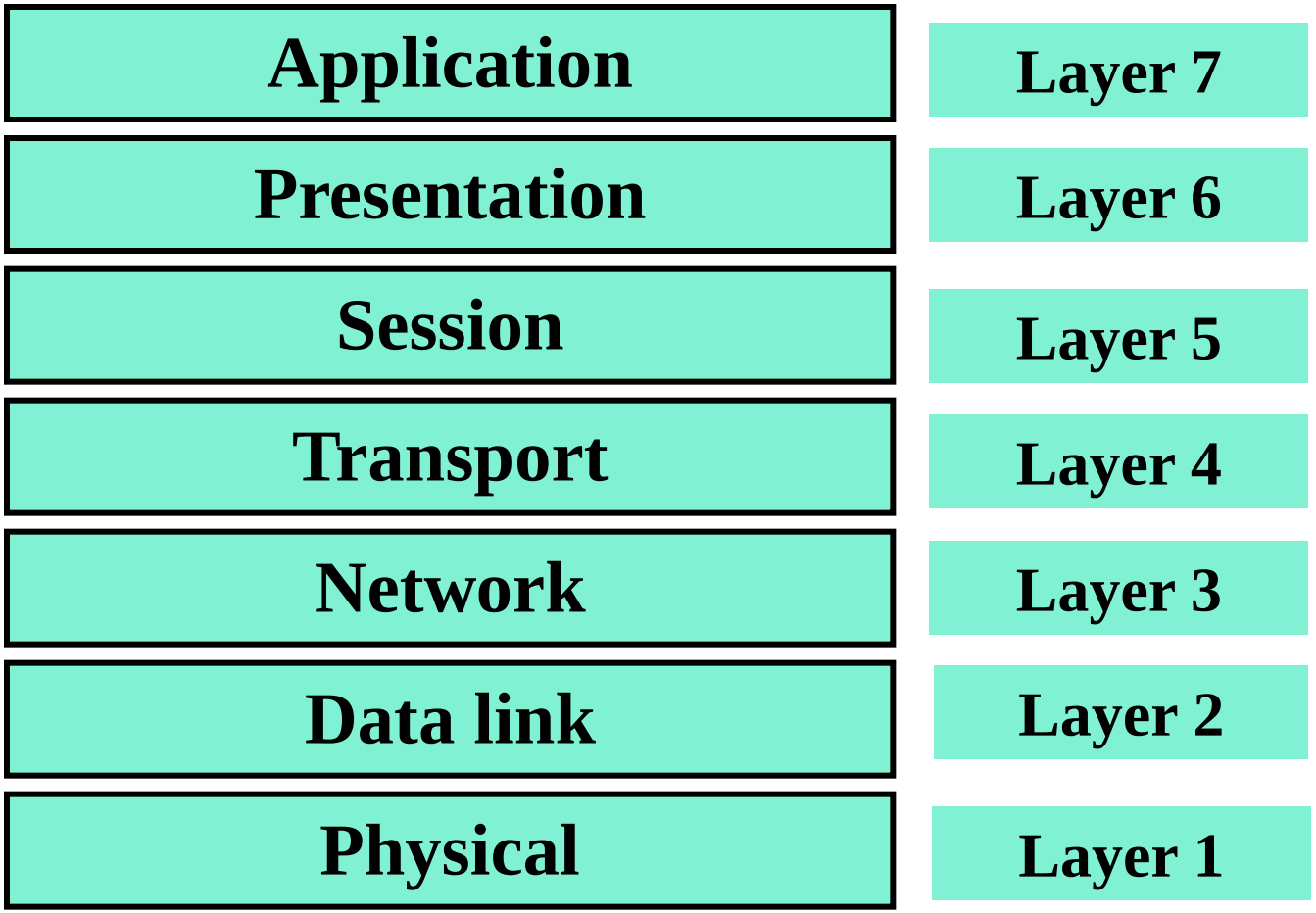
Chapter 10

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 layer OSI (Open Systems Interconnection) model

Physical Layer Functions

- Establishment and termination of a connection to a communication medium
- Process for effective use of communication resources
- Conversion between representation of digital data
- Physical characteristics of interfaces and media
- Representation of bits, transmission rate, synchronization of bits
- Link configuration
- Physical topology, and transmission mode

Data Link Layer Functions

- Provides functional and procedural means to transfer data between network entities
- Responds to service requests from the network layer and issues requests to the physical layer
- Concerned with:
  - Framing
  - Physical addressing
  - 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:
  - Logical addressing
  - 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
  - Flow Control
  - 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

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

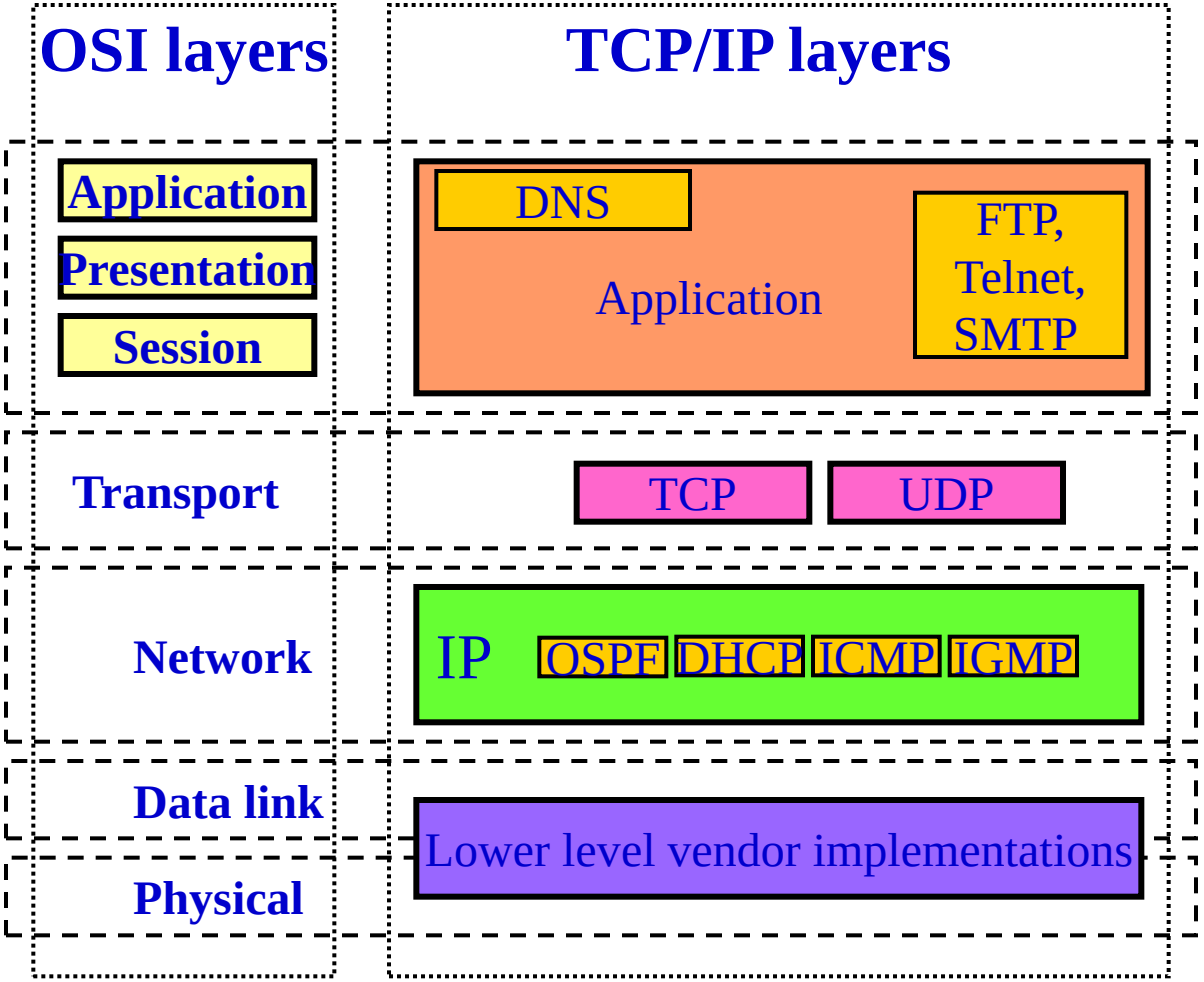
Application Layer Functions

- 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
  - Directory services

TCP/IP Protocol

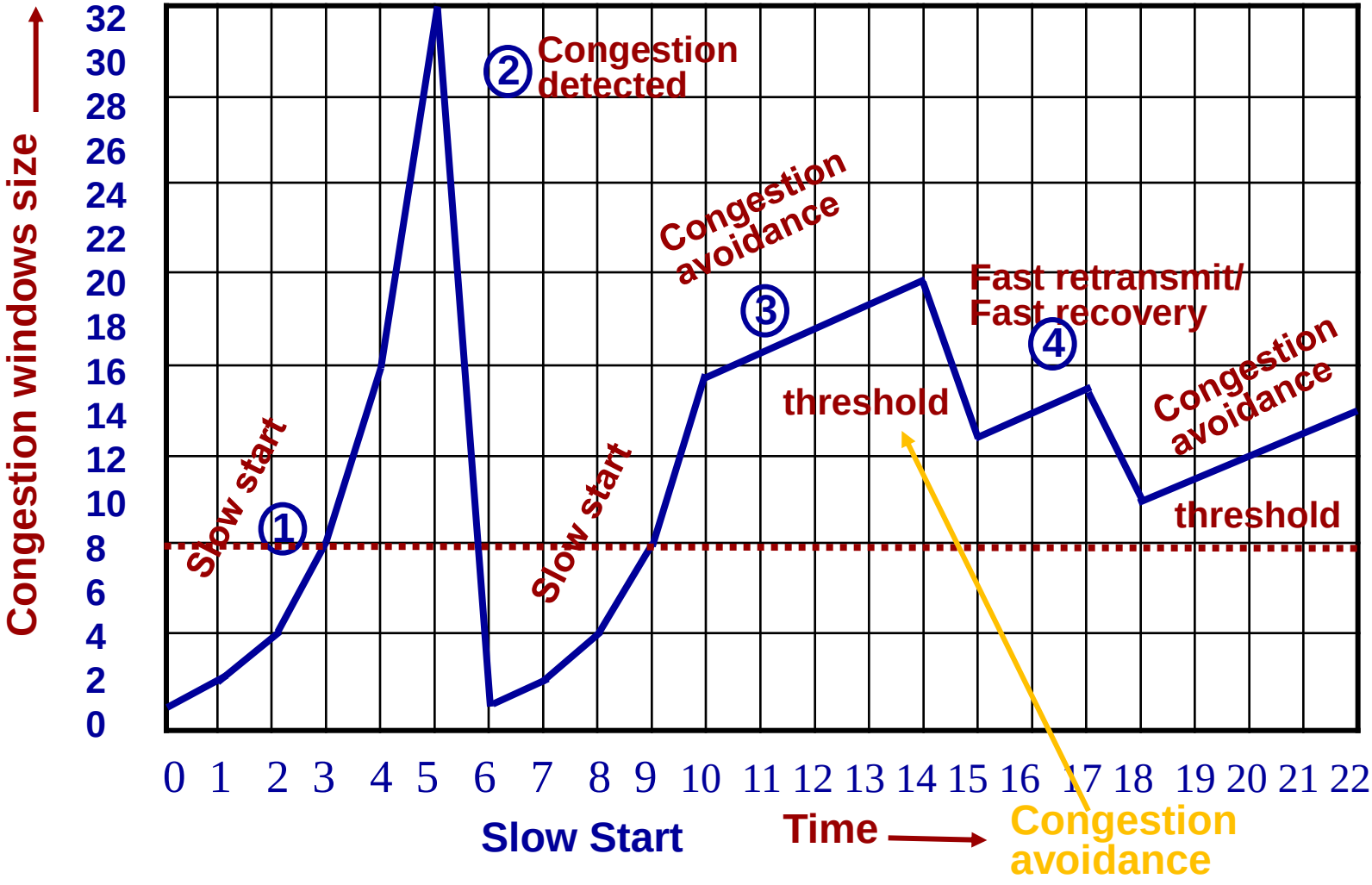
- TCP/IP protocol consists of five layers
- The lower four layers correspond to the layer of the OSI model
- The application layer of the TCP/IP model represents the three topmost layers of the OSI model

TCP/IP Protocol stack



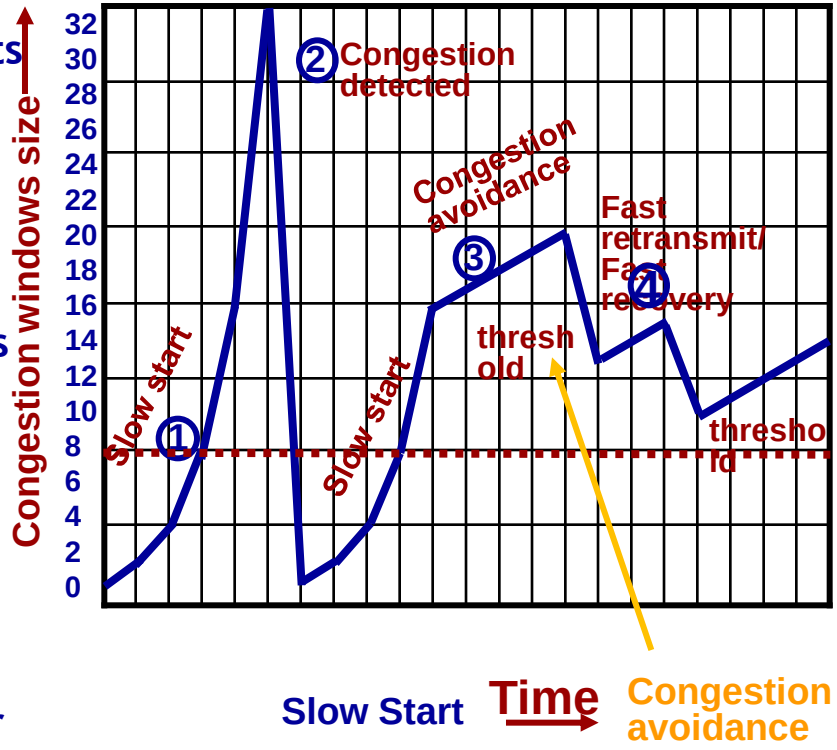
OSPF: Open Shortest Path First
DHCP: Dynamic Host Configuration Protocol
ICMP: Internet Control Message Protocol
IGMP: Internet Group Management Protocol

Overview of TCP concepts



Overview of TCP concepts

- Conventional TCP: Tahoe, Reno, New-Reno
- Sending rate is controlled by
  - Congestion window: limits the # of packets in flight
  - Slow-start threshold (*ssthresh*): when CA start
- Loss detection
  - 3 duplicate ACKs (faster, more efficient)
  - Retransmission timer expires (slower, less efficient)
- Overview of congestion control mechanisms
  - Slow-start phase: *cwnd* start from 1 and increase exponentially
  - Congestion avoidance (CA): increase linearly
  - Fast retransmit and fast recovery: Trigger by 3 duplicate ACKs



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 sequencing
- 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
- A member sends a IGMP join message to the router, which takes care of joining the multicast tree

Dynamic Host Configuration Protocol (DHCP)

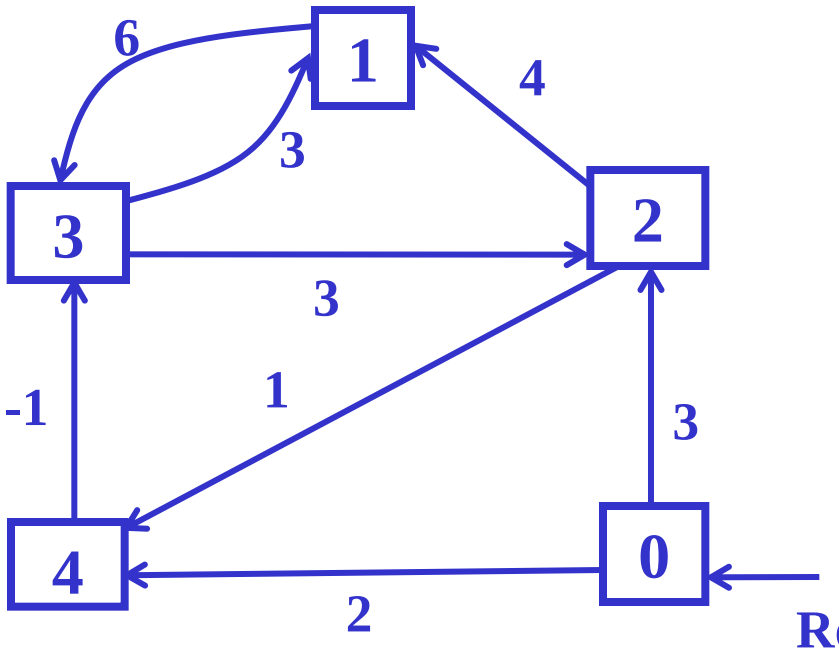
- Used to assign IP addresses dynamically in a domain
- Extension to Bootstrap Protocol (BOOTP)
- Node Requests an IP address from DHCP server
- Helps in saving IP address space by using same IP address to occasionally connecting hosts

Internet Routing Protocols

- **Intradomain Routing**
  - **Distance Vector**
    - **Routing Information Protocol (RIP)**
      - **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 in to autonomous systems (AS)**
    - **AS is further partitioned in to 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.**
  - **Border Gateway Protocol (BGP)**
    - **Intra-autonomous systems communicate with each other using path vector routing protocol**

TCP

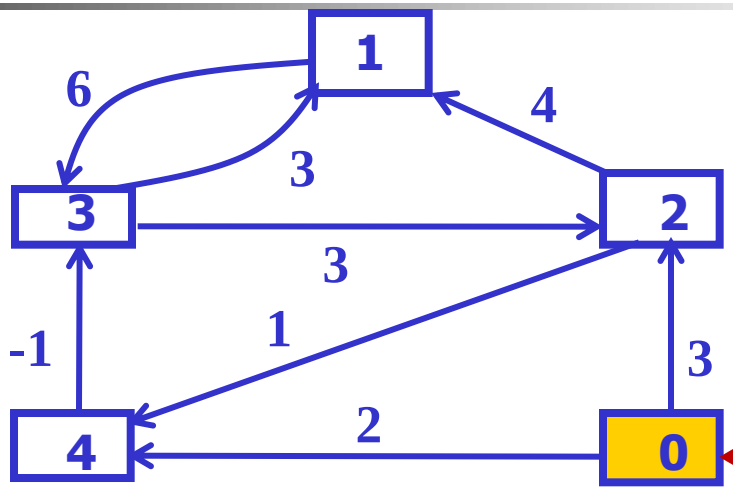
- **Application Layer**
  - **Top three layers (session, presentation, and application) merged into application layer**
- **Routing using Bellman-Ford Algorithm**



- **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

TCP (ctd)



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

Successive calculation of distance *D(u)* from Node 0

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

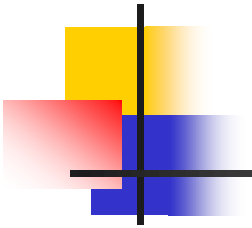
Predecessor from Node 0 to other network Nodes

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

Solutions for Wireless Environment (Split TCP Approach)

- **Indirect-TCP (I-TCP)**
  - Split the connection into wired component and wireless component
  - Specialized support for mobile applications for wireless side. Wired side is left unchanged
- **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

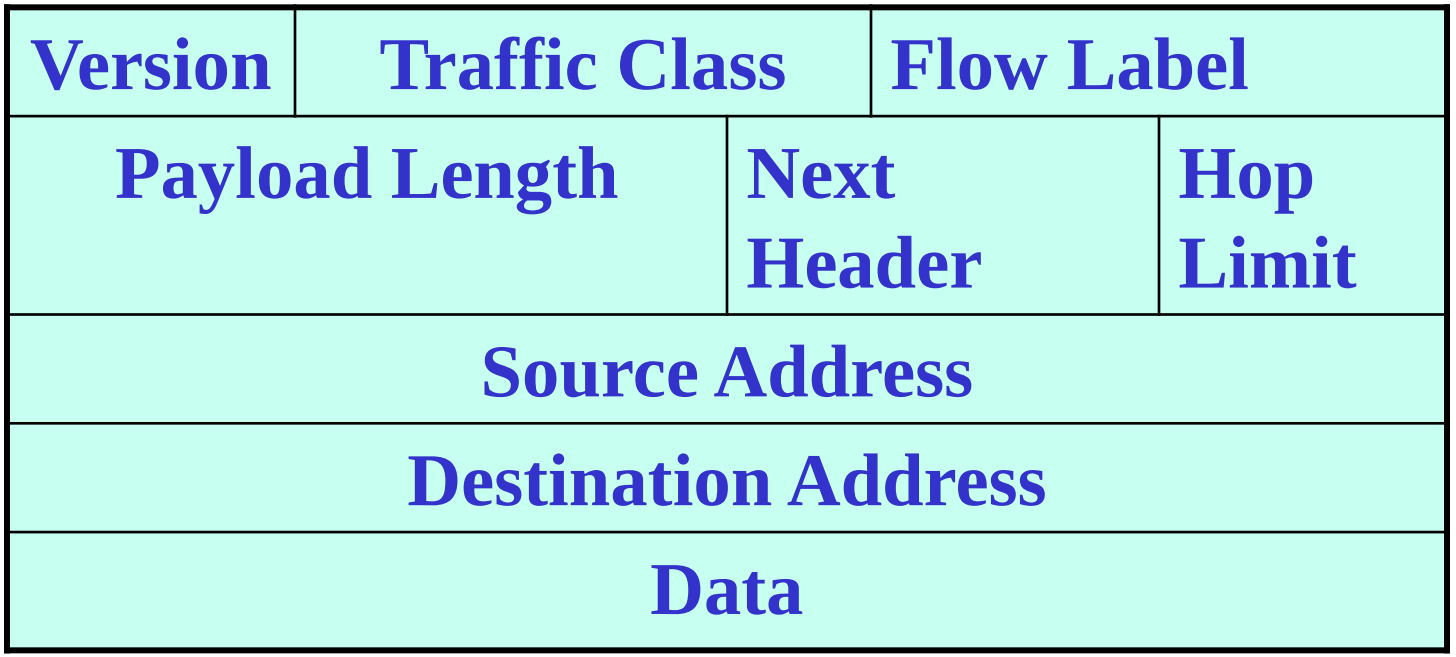
IPv4 Header Format



Version (4 bits)	Header length (4 bits)	Type of service (8 bits)	Total length (16 bits)	
Identification (16 bits)			Flags (3 bits)	Fragment offset (13 bits)
Time to live (8 bits)	Protocol (8 bits)		Header checksum (16 bits)	
Source address (32 bits)				
Destination address (32 bits)				
Options and padding (if any)				

IPv6 Header Format

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



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***

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

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.***

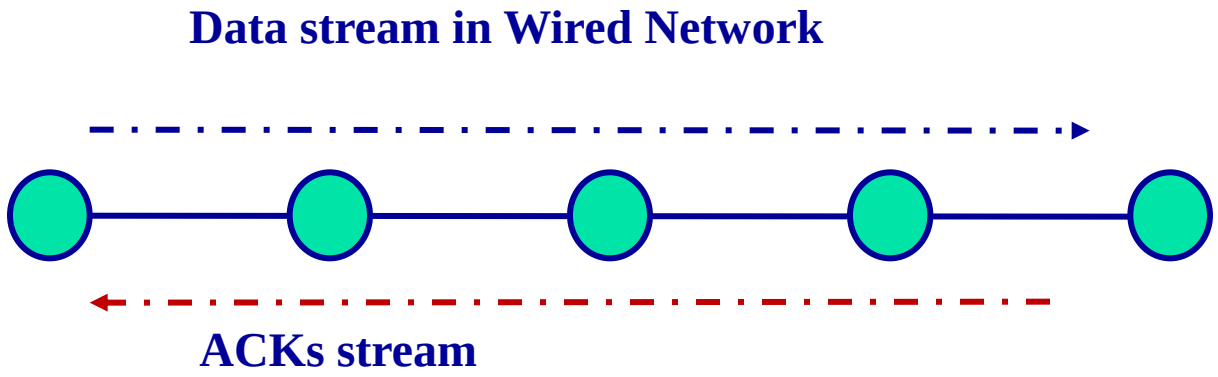
Differences between IPv4 and IPv6

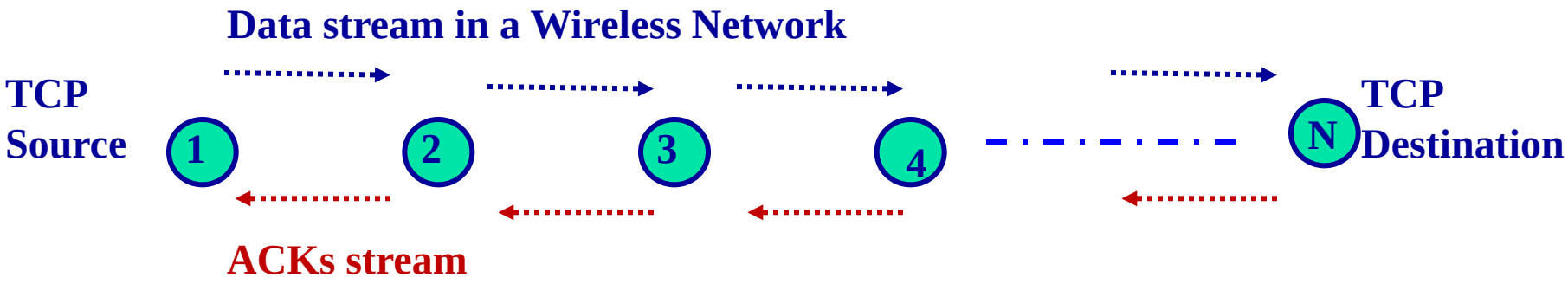
- Expanded Addressing Capabilities
- Simplified Header Format
- Improved Support for Options and Extensions
- Flow Labeling Capabilities
- Support for Authentication and Encryption

Solutions for Wireless Environment

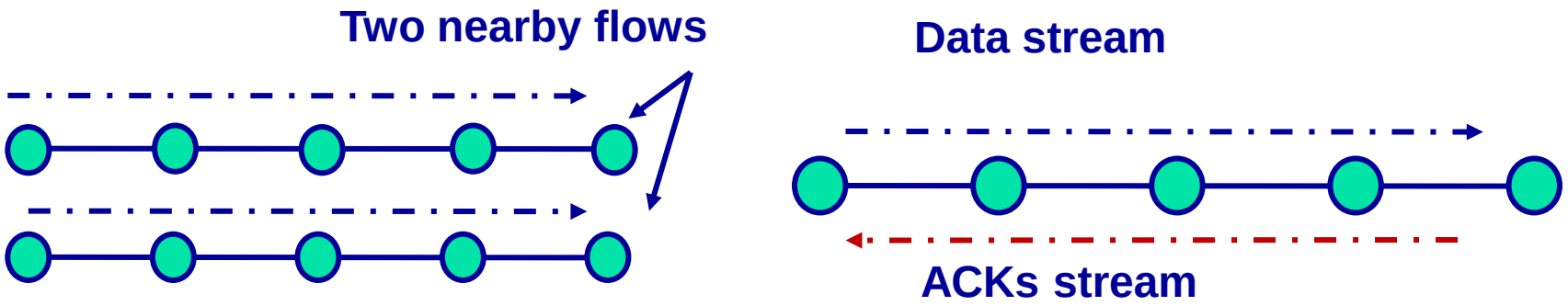
- Networking layering provides good abstraction
- Wireless networking interference limited
- Information delivery capability depends on current channel quality
- Adoption in physical and link layer broadcast could lead to efficient resource usage
- Changes need to be made in MSs and mobile access points to ensure compatibility

TCP in Wired Network and WSN





Problems of TCP over WSNs



Wired Line

- Intra-flow and inter-flow contention
  - Effects: Increased delay, unpredictability, and unfairness
  - *Inter*-flow contention: contention of *nearby* flows
  - *Intra*-flow contention: between packets of the *same* flow (e.g., forward data and reverse ACKs)
- Wireline: only packet on the same link "compete"
- Wireless: all close by devices compete for the channel

End-to-End Solutions

- Internet employs TCP/IP protocol stack
- Most of the applications require reliable transmission layer (mostly TCP)
- Wireless network must support existing applications
- Limitations of **wired** version of TCP
  - Routing Information Protocol (RIP)
  - Packet loss can occur because of random errors as well as due to congestion
  - Decreases efficiency due to TCP's Congestion avoidance
  - Many other problems like mobility support demands modification in TCP

Solutions for Wireless Environment

- 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 BS) and wireless (BS to MS) segments of TCP connections
  - Local Retransmission for mobile link breakage
  - BS 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

Solutions for Wireless Environment (Cont'd)

- Explicit Band State Notification (EBSN)
  - Local Retransmission from BS 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

Solutions for Wireless Environment (Link Layer Protocols)

- Transport Unaware Link Improvement Protocol (TULIP)
  - Provides Service Aware Link Layer
  - Reliable Service for TCP packets, unreliable service for UDP Packets
- AIRMAIL Protocol
  - Asymmetric Reliable Mobile Access in Link Layer
  - Uses combination of **FEC** and **ARQ** for loss recovery
- 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