Computer Networks
-Transport/Network layer II.-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W4 short test (1)

- Explain the DNS lookup process/name resolution!
  - 1. The stub resolver sends a query containing the name to a local DNS resolver 2. Local DNS resolver performs a recursive lookup for the name against a set of DNS resolvers 3. Local recursive resolver issues a sequence of queries to the respective name servers, and get the address from the authoritative name server 4. The local recursive resolver returns the IP address to the stub resolver, which passes the result to the function that issued the query
- What are the resource records?
  - When a resolver gives a domain name to DNS, it gets back an information entry called the resource records associated with that name. Common records include the IP address, domain name, name of the server, etc.

W4 short test (2)

- What is the main difference between the RFC 5322 and MIME?
  - RFC 5322 is the basic ASCII Internet message format used for electronic email with headers like To:, Cc:, From:, etc. MIME (Multipurpose Internet Mail Extensions): include multimedia extensions to the basic format, with e.g., audio, video, etc.
- Give 4 examples of common URL protocols!
  - http, https, ftp, file
- Which HTTP/HTTPS method is used to read a Webpage?
  - GET

W4 Recap (1)

- The network layer is concerned with getting packets from the source to the destination
- Store-and-Forward packet switching: packets or datagrams are injected into the network individually and routed independently of each other then forwarded to the next router until it reaches the destination
- The algorithm that manages the routing tables and makes the routing decisions is called the routing algorithm
- Router processes: forwarding and routing (static or dynamic)
- Congestion happens when too many packets introduce packet delay and loss that degrades performance
- Two main approaches to deal with congestion: increase the resources or decrease the load
- In general, networks do not need to be lossless for reliable file transfer (QoS)

W4 Recap (2)

- Connecting heterogeneous networks with machines using different protocols in layers raises multiple issues
  - Supporting different packet sizes with packet fragmentation
- If the source and destination hosts are on the same type of network but there is a different network between them, tunneling is used
- The IPv4 datagram consist of a header and a body/payload part
- IP addresses have a network portion and host portion
- Prefix length correspond to a binary mask of 1s in the network portion: subnet mask
- Subnetting is about allowing the block of addresses to be split into several parts for internal use as multiple networks while acting like a single network
- Combining multiple small prefixes into a single, larger prefix is called route aggregation

Agenda

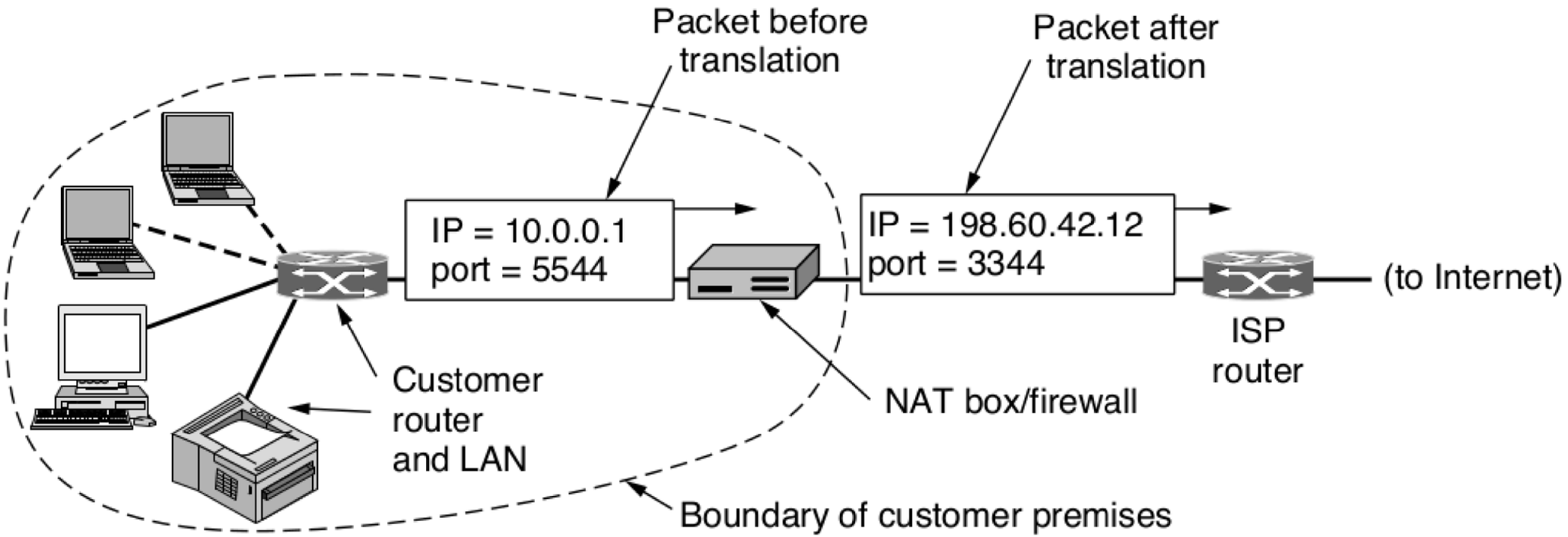
- Scarcity of IP addresses
- IPv6
- Internet Control Protocols
- The transport service
- Summary

NAT (1)

- One approach to deal with the scarcity of IP addresses is to dynamically assign an IP address to a computer when it is using the network, and take it back when the host becomes inactive
  - many businesses are expected to be on continuously, and can be problem even for home users (connect all devices into a home network via LAN and use a router on it that connects to the ISP)
- Running out of IP addresses: 128-bit IPv6 addresses
  - takes time to migrate, so the quick fix is **NAT** (Network Address Translation)
- Assign each home or business a single IP for traffic, but within the customer network, every computer gets a unique IP
- Before the packet exists the customer network and goes to the ISP, the address is translated from internal to a the shared public IP

NAT (2)

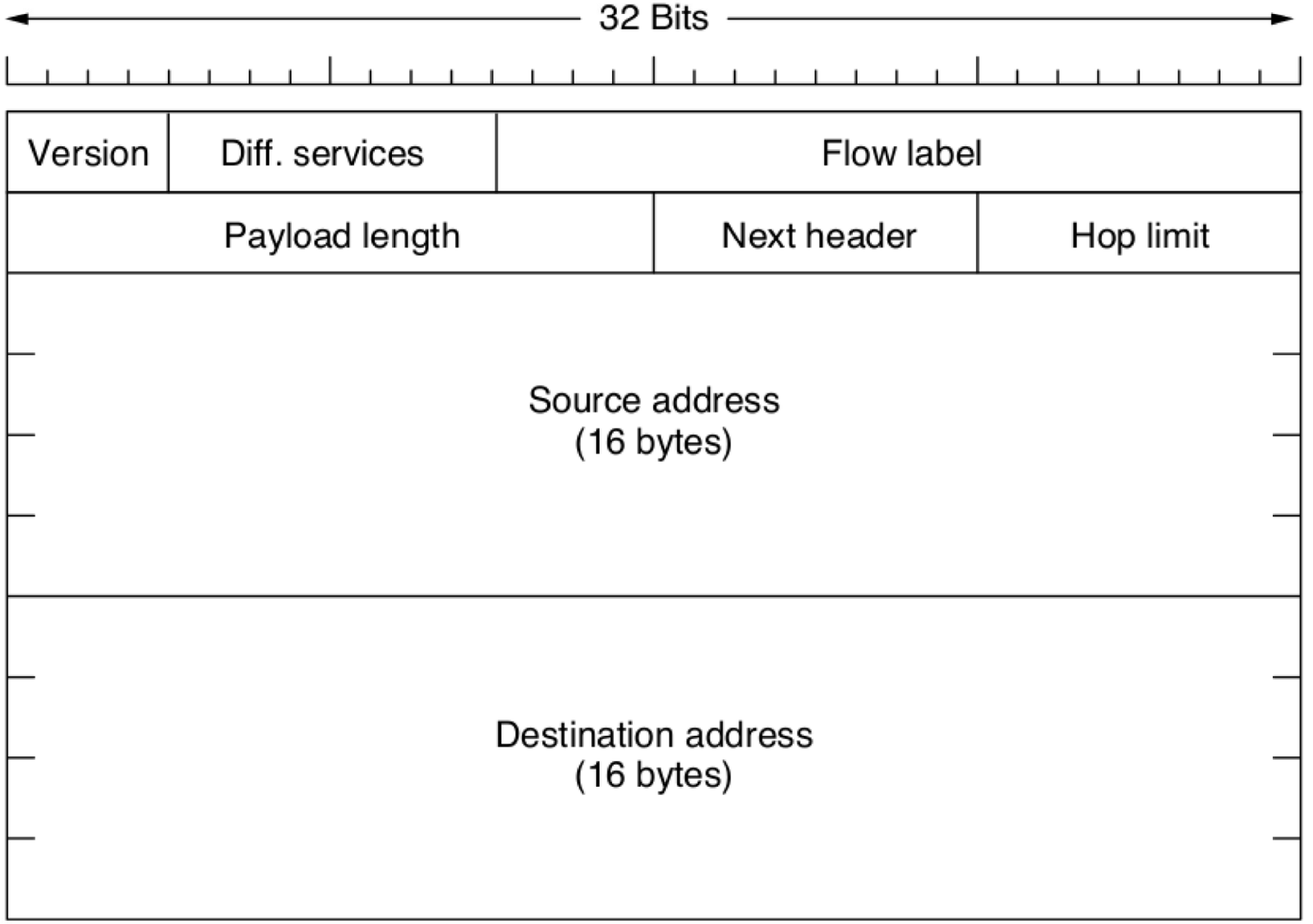
10.0.0.0	– 10.255.255.255/8	(16,777,216 hosts)
172.16.0.0	– 172.31.255.255/12	(1,048,576 hosts)
192.168.0.0	– 192.168.255.255/16	(65,536 hosts)



Why IPv6?

- Even with efficiently using CIDR and NAT, running out of addresses is a problem
  - last addresses were allocation in 2019, so the only long-term solution is to move to larger addresses
- **IPv6** is a different protocol that not interwork well with IPv4, so not used as much
  - longer addresses than IPv4 (128 bits, efficiently unlimited addresses)
  - simplified header, so faster to process packets for routers
  - better support for options, and easier to skip over them
  - initially better security on sense of authentication and privacy (but IPv4 was also improved in this matter)

The IPv6 header (1)



The IPv6 header (2)

- **Differentiated services** is used to distinguish the class of service for packets with different real-time delivery requirements
- **Flow** provides a way for a source and destination to mark groups of packets that have the same requirements and should be treated in the same way by the network
- **Payload length** tells how many bytes follow the header
- The **Next header** tells which of the six extensions headers, if any, follows this one (of this header is the last, it tells which transport protocol handler to pass the packet to, e.g. TCP)
- **Hop limit** is essentially the Time to live

Source and Destination addresses, extension headers

- 16-byte addresses of eight groups of four hexadecimal digits with colons between the groups: 8000:0000:0000:0000:0123:4567:89AB:CDEF
- Leading zeros can be omitted, one or more groups of 16 zero bits can be replaced by a pair of colons: 8000::123:4567:89AB:CDEF
- The extension headers can provide extra information encoded in an efficient way

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

ICMP

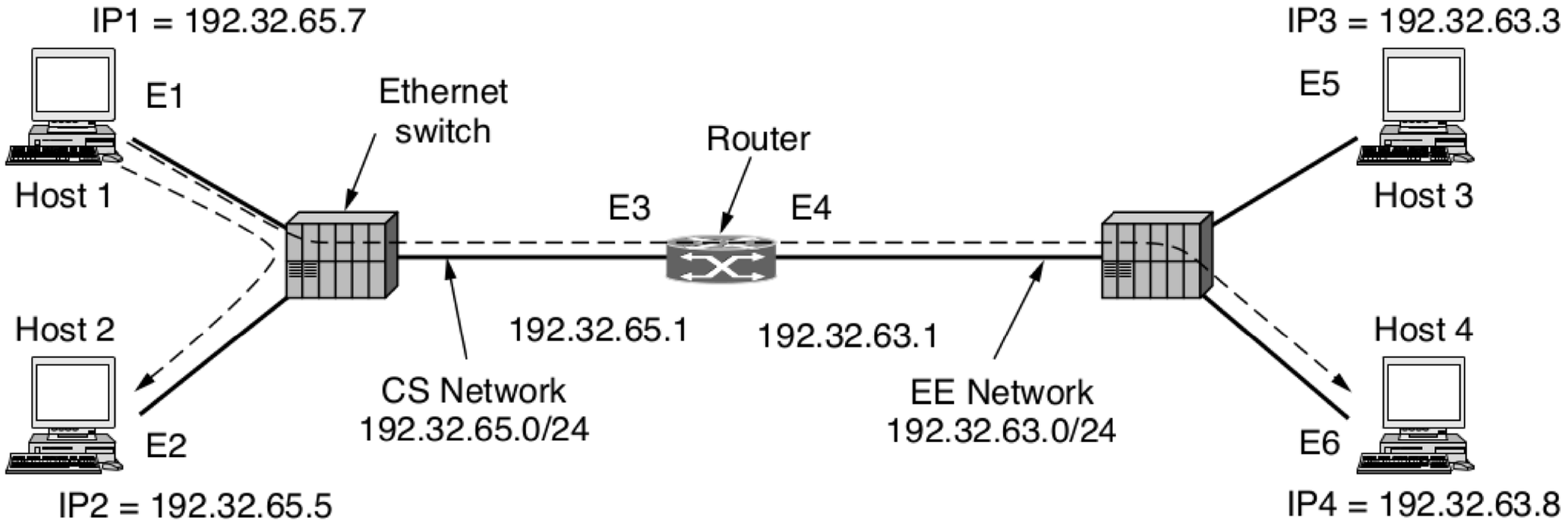
- There are other protocols in the network layer than IP
- The **ICMP** (Internet Control Message Protocol) is used by routers to send operational information and error messages to other addresses

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

- The **traceroute** utility finds the routers along the path from the host to a destination IP address, using time to live

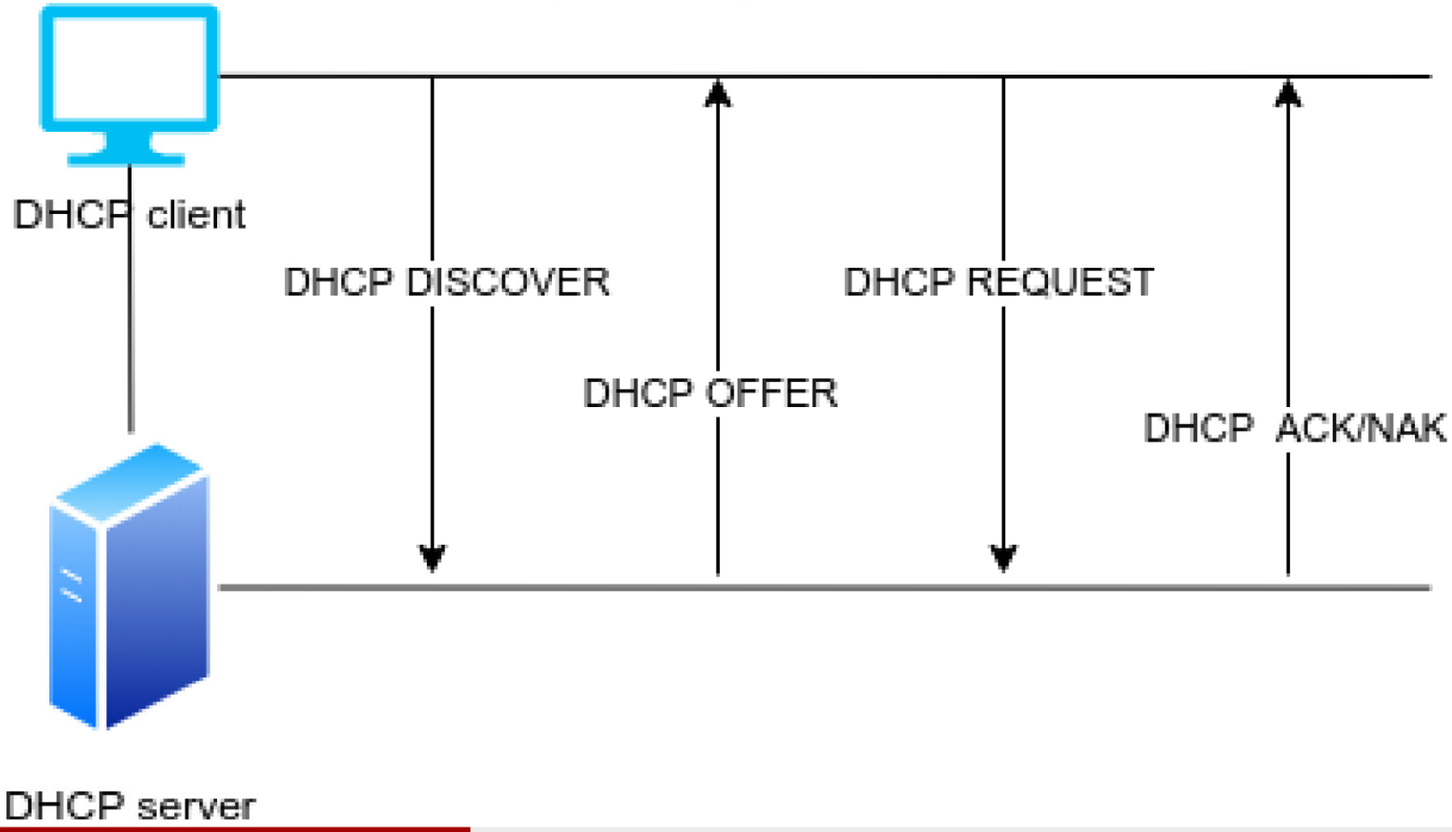
ARP

- The **ARP** (Address Resolution Protocol) is used to identify data link layer addresses (e.g., MAC address) associated with an IP address
  - NICs (Network Interface Cards) do not understand Internet addresses, but have a physical machine address called **MAC** (Media Access Control) address of 48 bits (sometimes called Ethernet hardware addresses)



DHCP

- With using **DHCP** (Dynamic Host Configuration Protocol), there is no need to individually configure network devices, because the DHCP server automatically assigns an IP address per request



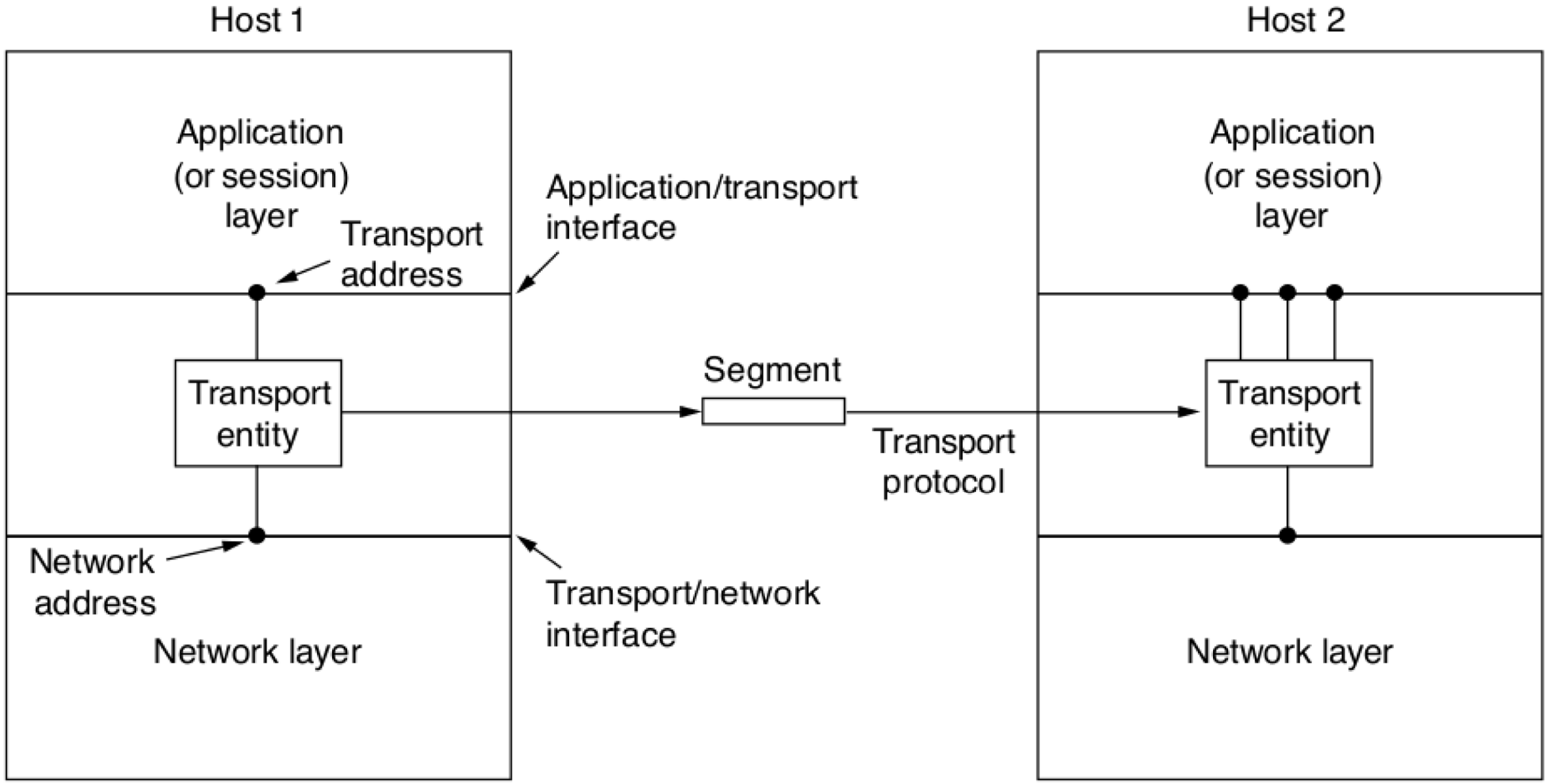
Interior and Exterior Gateway Routing Protocols

- Inside its own network, an organization can use its own algorithm for internal routing or intradomain routing
- The intradomain routing protocol is commonly referred to as the **IGP** (Interior Gateway Protocol)
  - one of the popular IGPs is OSPF (Open Shortest Path First), used to find the optimal path between source and destination routers
- In the case of routing between independently operated networks with interdomain routing, the same exterior gateway protocol must be used
  - called **BGP** (Border Gateway Protocol) for the Internet, hopping between autonomous systems efficiently

Transfer from source to destination

- The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability
- The ultimate goal is to provide reliable data-transmission service to users in the application layer, using the services from the network layer
  - the software/hardware doing this job is a **transport entity**
  - developers can write code according to a standard set of primitives and have the programs work on a variety of networks, without having to worry about different network interfaces

Network, transport, application layers



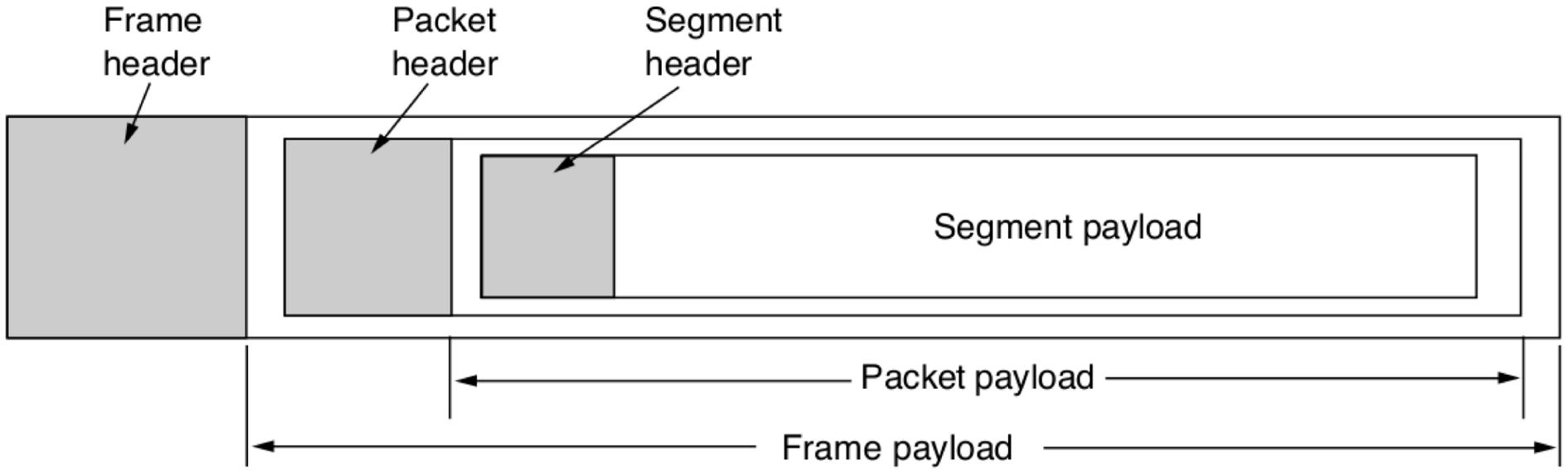
Transport service primitives

- To allow users to access the transport service, the layer must provide operations to application programs: a transport service interface
- **Segments** are messages sent from transport entity to another transport entity

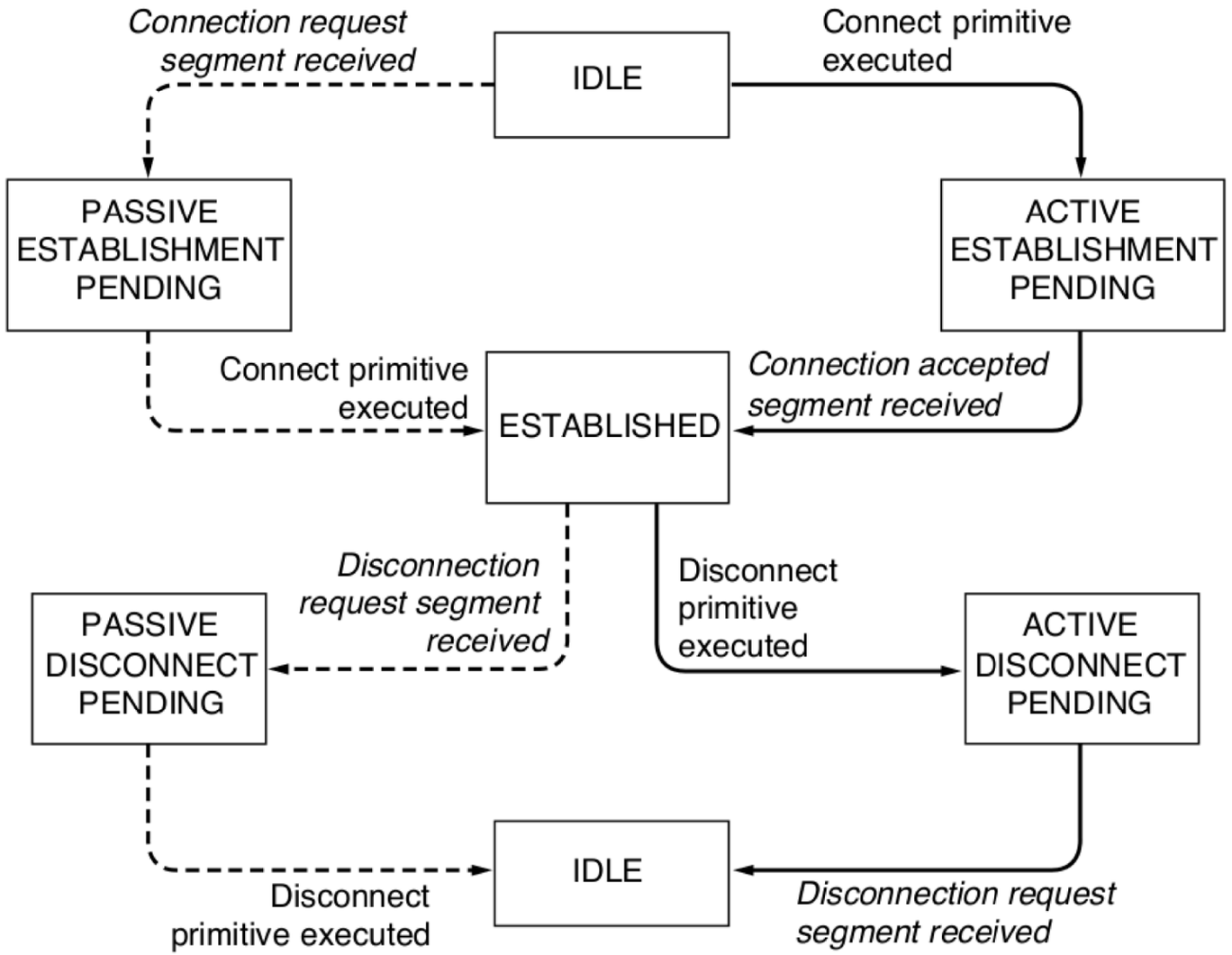
Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	Request a release of the connection

Nesting of segments, packets, and frames

- Segments exchanged by the transport layer are contained in packets which are exchanged by the network layer
- Packets are contained in frames exchanged by the data link layer
  - when a frame arrives, the data link layer processes the frame header and if the destination address matches for local delivery, passes the contents of the frame payload field up to the network entity



A simple connection management scheme



Socket primitives

- The socket primitives are the same used for TCP

Primitive	Meaning
SOCKET	Create a new communication endpoint
BIND	Associate a local address with a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Passively establish an incoming connection
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

W5 summary (1)

- Running out of IP addresses: assign each home or business a single IP for traffic, but within the customer network, every computer gets a unique IP
- Using NAT, before the packet exists the customer network and goes to the ISP, the address is translated from internal to a the shared public IP
- Even with efficiently using CIDR and NAT, running out of addresses is a problem
- IPv6 has longer addresses than IPv4, simplified header, better support for options, and generally better security
  - headers: differentiated services, flow, payload length, next header, hop limit, source and destination addresses
  - extension headers
- The ICMP is used by routers to send operational information and error messages to other addresses
- The ARP is used to identify data link layer addresses associated with an IP address

W5 summary (2)

- Inside its own network, organizations can use their own IGPs, but routing between independently operated networks must be done with the same exterior gateway protocol (BGP for the Internet)
- Using DHCP, the DHCP server automatically assigns an IP address per request
- The transport layer builds on the network layer to provide data transport with a desired level of reliability
- The goal is to provide reliable data-transmission service to users in the application layer, using the services from the network layer
- Segments exchanged by the transport layer are contained in packets which are exchanged by the network layer, while packets are contained in frames exchanged by the data link layer