Cloud computing and distributed systems

Chapter #3
Networking and Internetworking

Zeynep Yücel

Ca' Foscari University of Venice
zeynep.yucel@unive.it
yucelzeynep.github.io

System models

- Different types of networks: e.g. LANs, WANs.
- Transmission media:
  - Hardware: routers, switches.
  - Software: protocol stacks.
- *Communication subsystem*: hardware/software components.
- *Hosts*
- *Node*
- Internet: consists of *subnets*.
  - *subnet*: reachable nodes on the same physical network.

Networking issues for distributed systems

- Early networks: simple tasks
- Distributed systems: complex applications
- Increased network demands:
  - high-performing
  - scalable
  - reliable
  - mobile
  - secure
  - quality service, multicasting

Networking issues for distributed systems

Performance

- Time required to transfer a message of *length* bits:

$$MessageTransmissionTime = latency + length/dataTransferRate$$

- Key performance factors:
  - Latency: initial delay
    - Affected by load
  - Data transfer rate: speed
    - Influenced by physical characteristics

Networking issues for distributed systems

Performance

- Maximum message length determined by technology
- Longer messages: smaller segments
- Small messages common
  - Latency more important than rate
- Latency: significant performance factor

Networking issues for distributed systems

Performance

- Total system bandwidth: traffic volume
  - LAN bandwidth: data transfer rate
- Client-server communication: slow
- Network access: faster than disk
- Internet latency: slower than LAN

Scalability

- Rapid growth
- Many more nodes in the future
- Technology limitations
  - Routing changes underway
  - Economic factors

Reliability

- Applications handle communication issues
- End-to-end argument
- Most physical communication methods are reliable
- Software errors more often than network errors

Security

- Firewalls defense
  - Protect internal computers
  - Gateway control
  - Message filtering
- Secure applications beyond firewalls
  - Cryptographic techniques
- Protection of network components

Mobility, Quality of service and Multicasting

- Mobility
  - Different places
  - Addressing issues
  - Need improvements
- Quality of service (QS)
  - Multimedia data
  - Guaranteed bandwidth
  - Minimum acceptable quality
- Multicasting
  - Often one-to-one but sometimes also one-to-many
  - Individual messages between each pair costly
  - Multiple recipients at once

Types of network

- Main types:
  - PAN
  - LAN
  - WAN
  - MAN
  - Wireless versions of these
- *Internetwork*: combining many interconnected networks
- E.g. Internet
- Described by area covered and/or technology

Types of network

Personal Area Networks (PANs)

- User devices
- Low-cost, low-energy
- Wired PAN: not significant
- Wireless PAN: gaining importance
- E.g. Bluetooth (WPAN)

Types of network

Local Area Networks (LANs)

- LANs connect to computers with cables
- *Segment*: computers with direct communication
- Computers in a segment share bandwidth
- Larger networks consist of multiple segments
- High bandwidth, low-latency

Types of network

Local Area Networks (LANs)

- Ethernet limitations in multimedia applications
- "Asynchronous transfer mode (ATM)" networks fill this gap but with high costs
- "High-speed Ethernet" reduces issues, not effective as ATM

Types of network

Wide Area Networks (WANs)

- WANs connect computers over long distances
- Routers for communication
- Routing introduces delays
- Speed of signals sets minimum delay
  - Europe-Australia 0.13 sec by terrestrial.
  - 0.20 seconds satellite.

Types of network

Metropolitan area networks (MANs)

- MANs use high-speed cables
- Handle video, voice, data
- Common examples: DSL
- Family of technologies: xDSL
- Newer versions support high-definition video

Types of network

Wireless local/metropolitan/wide area networks (WLANs, WMANs, WWANs)

- WLANS, e.g. WiFi
- WMANs, e.g. WiMAX
- WWANs, e.g. GSM

Types of networks

Internetworks

- Internetwork connects multiple networks
- Individual networks: Limited addresses, performance issues
- Internetworks support large systems
- Software layer for transmission
- Creates a virtual network
- Internet with TCP/IP

Types of networks

Summary of types, technologies, ranges etc

	Example	*Range*	*Bandwidth (Mbps)*	*Latency (ms)*
Wired:				
LAN	Ethernet	1–2 kms	10–10,000	1–10
WAN	IP routing	worldwide	0.010–600	100–500
MAN	ATM	2–50 kms	1–600	10
Internetwork	Internet	worldwide	0.5–600	100–500
Wireless:				
WPAN	Bluetooth (IEEE 802.15.1)	10–30m	0.5–2	5–20
WLAN	WiFi (IEEE 802.11)	0.15–1.5 km	11–108	5–20
WMAN	WiMAX (IEEE 802.16)	5–50 km	1.5–20	5–20
WWAN	3G phone	cell: 1–-5 km	348–14.4	100–500

Network principles

Packet transmission

- Messages sent as data sequences
- Large messages broken into packets
- Packet contains binary data and addressing info
- Benefits of packets:
  - Allows storage preparation
  - Prevents delays

Network principles

Data streaming

- Streaming is real-time transmission of audio, video
- Needs more bandwidth, low delays
- When compressed, requires less bandwidth
- Typically sent using UDP packets
  - Frames displayed at specific time
  - Late frames discarded
  - E.g. for frame rate of 24 fps, timing of frame N is N/24 sec
  - Late elements dropped

Network principles

Data streaming

- Good quality of service needed
  - Internet struggles with high-quality streams
  - Dedicated path ideal
  - ATM networks designed for high bandwidth, low latency
  - IPv6 identifies packets
  - RSVP negotiates pre-allocation of bandwidth
  - RTP includes timing details
- Effective protocols require upgrades to the infrastructure

Network principles

Switching schemes

- To transmit information between two arbitrary nodes, a switching system is required.
  - Four types:
    - Broadcasting
    - Circuit switching
    - Packet switching
    - Frame relay
  - Broadcasting: no switching.
    - Nodes decide relevance.
    - Used in Ethernet, wireless.
  - Circuit Switching: traditional telephony.
    - Dedicated connection for calls.
    - Plain old telephone system (POTS).

Network principles

Switching schemes

- Packet Switching: small data packets.
  - Stored, forwarded at nodes.
  - Similar to postal system.
- Frame Relay: reduces delays.
  - Switching delay concerns.
    - Depends on packet size, speed, traffic.
  - Small packets (frames) sent rapidly without being stored.
    - Combines circuit switching and packet switching advantages.
  - Useful for real-time applications.

Network principles

Protocols

- Protocol: rules for communication.
- Two main parts:
  - Message sequence.
  - Data format.
- Enables separate software development.
- Pair of software modules (sending and receiving).
  - Transport protocol.
  - Network protocol.

Network principles

Protocols - Protocol layers

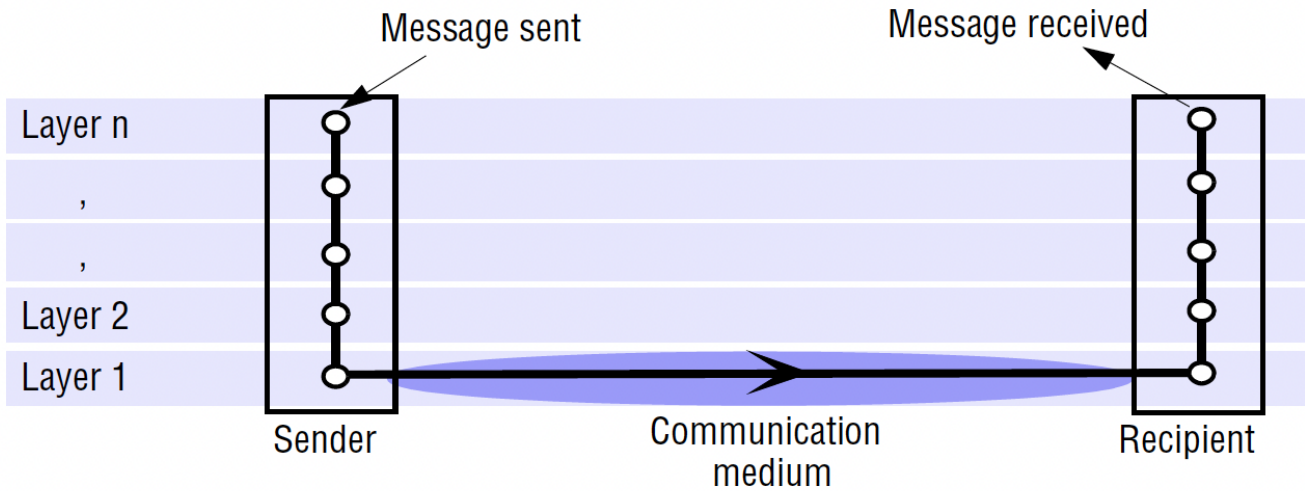
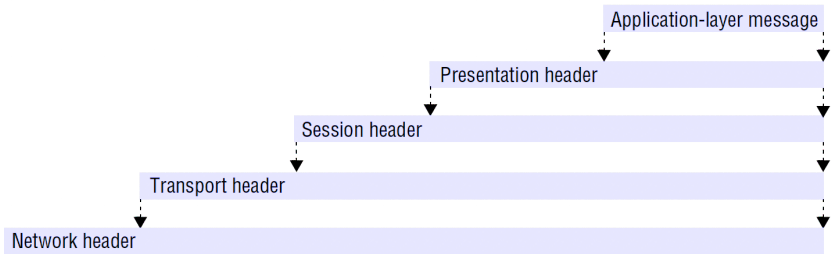


Figure: Conceptual layering of protocol software.

- Network software is organized in layers.
- Each layer communicates with adjacent layers.

Network principles

Protocols - Protocol layers



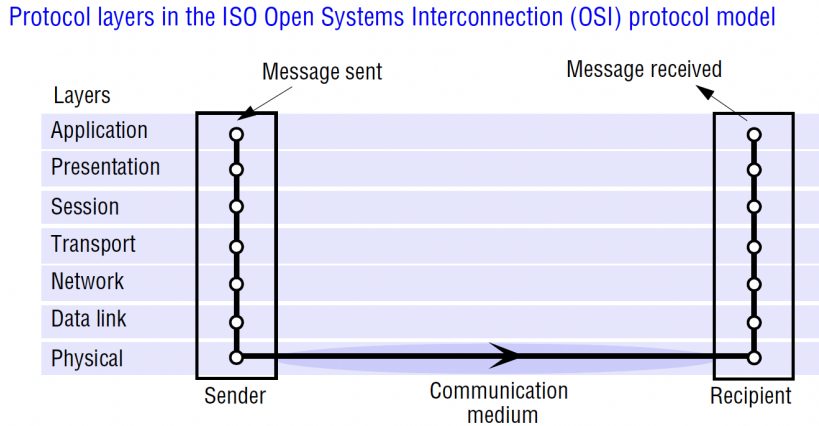


Figure: Encapsulation in (a) layered protocols and (b) OSI.

- Sending: layers receive, wrap and send data to below.
- Receiving: process is reversed.
- Protocol layers simplify communication, but can slow performance.
- Multiple layers require data copies, control transfer etc., reducing rates.

Network principles

Protocols - Protocol suites - OSI

- Protocol suite: complete protocol layers.
- Open Systems Interconnection (OSI): seven-layer model.

Layer	*Description*	*Examples*
Application	Protocols at this level are designed to meet the communication requirements of specific applications, often defining the interface to a service.	HTTP, FTP, SMTP, CORBA IIOP
Presentation	Protocols at this level transmit data in a network representation that is independent of the representations used in individual computers, which may differ. Encryption is also performed in this layer, if required.	TLS security, CORBA data representation
Session	At this level reliability and adaptation measures are performed, such as detection of failures and automatic recovery.	SIP
Transport	This is the lowest level at which messages (rather than packets) are handled. Messages are addressed to communication ports attached to processes. Protocols in this layer may be connection-oriented or connectionless.	TCP, UDP
Network	Transfers data packets between computers in a specific network. In a WAN or an internetwork this involves the generation of a route passing through routers. In a single LAN no routing is required.	IP, ATM virtual circuits
Data link	Responsible for transmission of packets between nodes that are directly connected by a physical link. In a WAN transmission is between pairs of routers or between routers and hosts. In a LAN it is between any pair of hosts.	Ethernet MAC, ATM cell transfer, PPP
Physical	The circuits and hardware that drive the network. It transmits sequences of binary data by analogue signalling, using amplitude or frequency modulation of electrical signals (on cable circuits), light signals (on fibre optic circuits) or other electromagnetic signals (on radio and microwave circuits).	Ethernet base-band signalling, ISDN

Network principles

Protocols - Protocol suites - OSI

- Internet combines application, presentation, session layers.

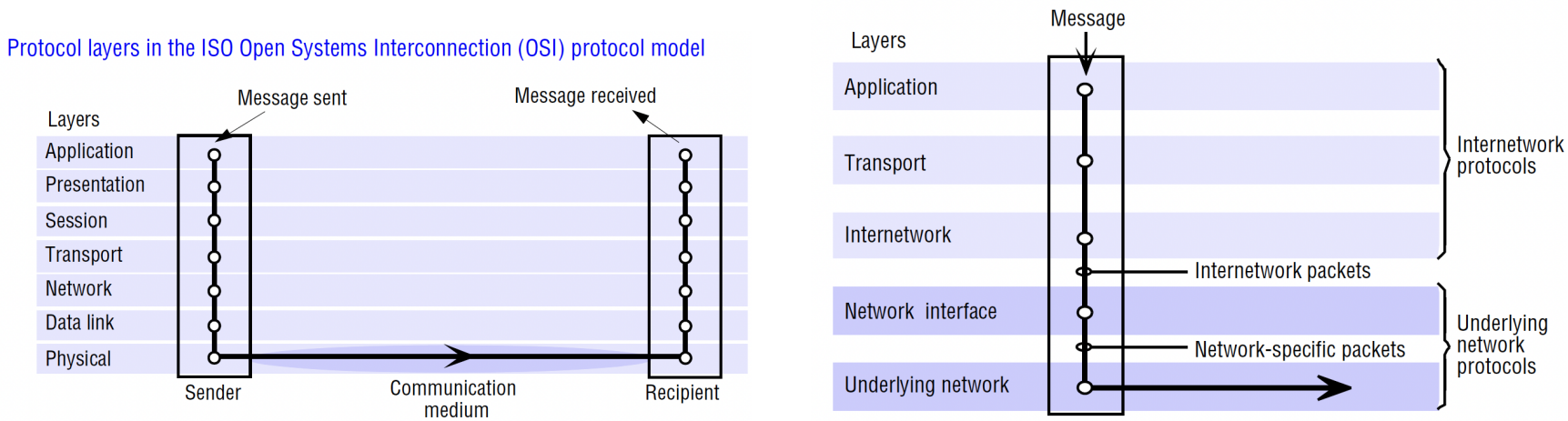


Figure: Protocol layers of OSI and internetwork layers.

Network principles

Protocols - Packet assembly

- Messages divided into smaller packets.
- Each packet has a header, data field.
- Maximum packet size: maximum transfer unit (MTU).
- Larger messages must be split, sequenced.
- MTU: Ethernet 1500 bytes, IP up to 64 kbytes.

Network principles

Protocols - Ports and addressing

- Ports: software-defined destination points.
  - Connect to processes, reach applications.
  - Each message has a transport address.
  - Network address uniquely identifies computers.
- Transport layer delivers messages.
  - Every computer has an IP address.
  - Services have registered port numbers.
  - Fixed ports can limit distributed systems.
    - Solutions: dynamically assigned, symbolic names.

Network principles

Protocols - Two ways of packet delivery

- Datagram Delivery
- Packet sent without setup
- Forget packet after delivery.
- Packets have full sender/receiver addresses.
- Packets can take different paths.
- Used in most networks.

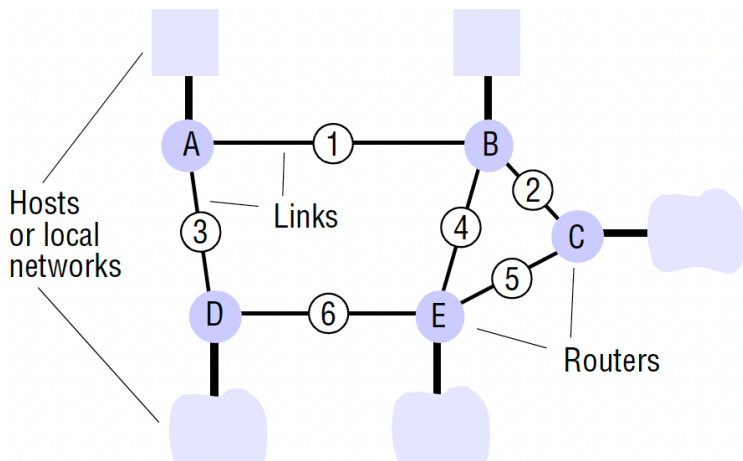
- Virtual Circuit Delivery
- Route setup before sending.
- Nodes track packet path.
- Packets have virtual circuit numbers.
- Reduces delays for packets.
- E.g. ATM.

Datagram delivery is quick, simple, while virtual circuit delivery involves setup and helps manage packet flow efficiently.

Network principles

Routing

- Essential for all networks except certain LANs.
- Adaptive routing: the best route between two points re-evaluated periodically
- Packets transmitted over hops.
- Routing algorithm functions:
  - Route determination.
  - Update of network knowledge.



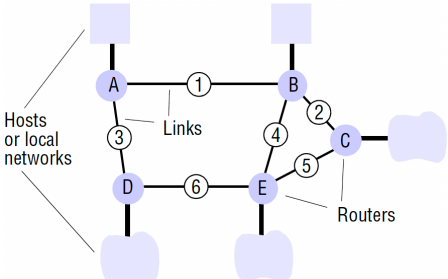
Network principles

Routing - Distance vector routing algorithm

- Distance vector routing: foundational routing method.
- Path finding graphs.
- Bellman' shortest path algorithm basis.
- Adaptation to distributed case by Ford and Fulkerson.

Network principles

Routing - Distance vector routing algorithm



Routings from A		
To	*Link*	*Cost*
A	local	0
B	1	1
C	1	2
D	3	1
E	1	2

Routings from B		
To	*Link*	*Cost*
A	1	1
B	local	0
C	2	1
D	1	2
E	4	1

Routings from C		
To	*Link*	*Cost*
A	2	2
B	2	1
C	local	0
D	5	2
E	5	1

- Routing tables maintain.
  - Outgoing link.
  - Cost (number of hops).
- Routers use tables to determine outgoing links.
  - Let a packet addressed to C be submitted to A.
  - From A to B via link 1.
  - From B to C is via link 2.
  - C is "local"

Network principles

Routing - Distance vector routing algorithm

- Routing tables maintained through Routing Information Protocol (RIP).
  - Routers periodically share updates.
  - Local tables updated.
- Link failure marked infinite.
- Link-state algorithms share database.
  - Nodes compute optimum routes.

Network principles

Congestion control

- Limited network capacity.
- High loads leading to queues.
- If queues exceed limits, packets dropped
  - If occasional, acceptable
  - High loss harms throughput.
- Congestion control techniques.

Network principles

Congestion control

- Principles congestion control.
  - Dropped packets cause waste.
  - Retransmission costs resources.
  - Hold packets at earlier nodes, until congestion reduced.
  - "Choke packets" to request reduction of transmission rate.

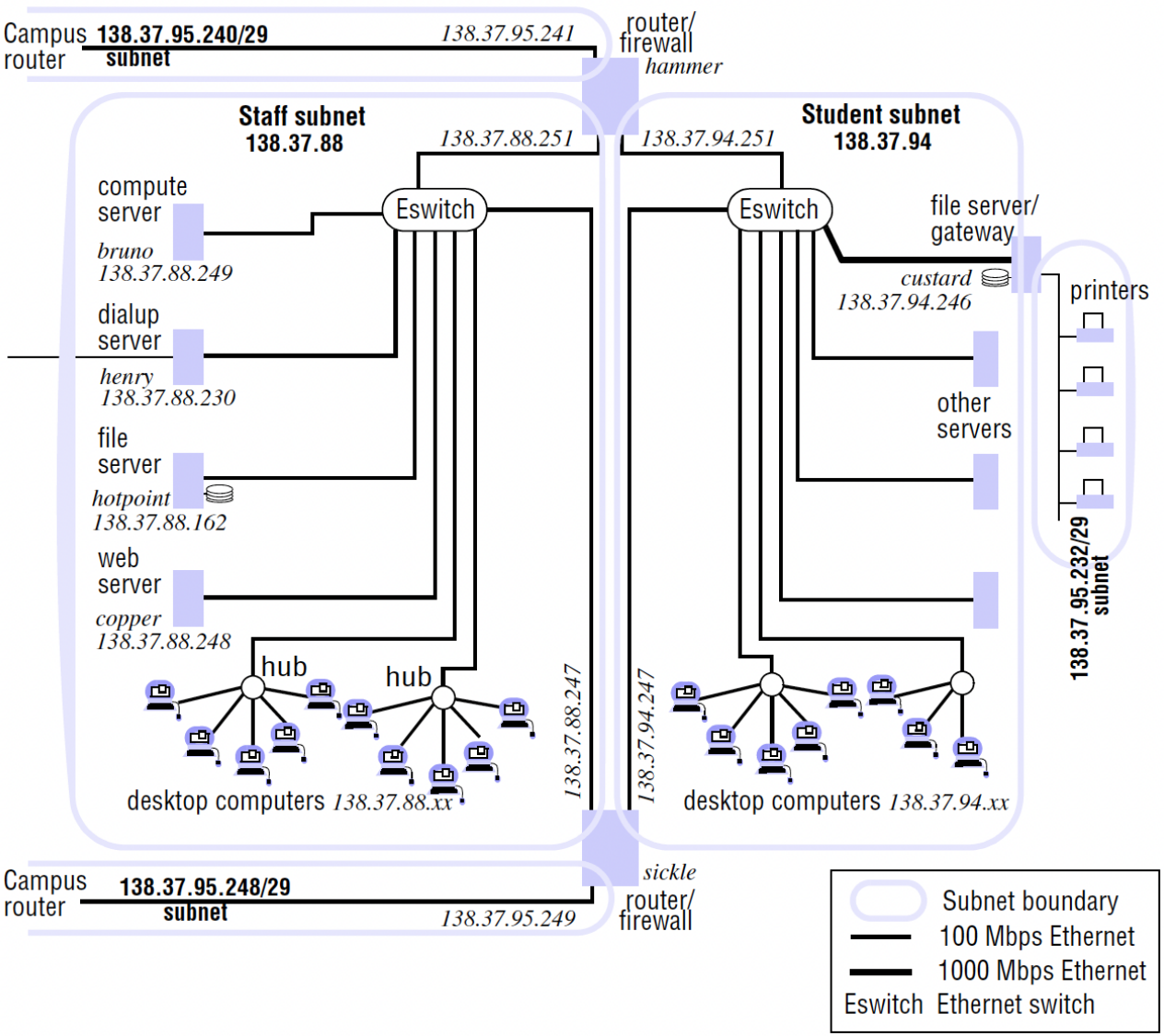
Network principles

Internetworking

- Various network technologies.
  - Ethernet, satellite etc.
  - Modem, wireless, DSL etc.
- Create internetwork integration.
  - 1. Unified addressing scheme.
  - 2. Internetwork packet protocols.
  - 3. Routers.
- Internet components: IP addresses, IP protocol, IP routers.

Network principles

Internetworking components - Simplified view of part of a university campus network



- Routers: also firewall function.
- Subnets: staff, student.
- File servers: custard.
- Links: all Ethernet.
- Ethernet switches.

Network principles

Internetworking components

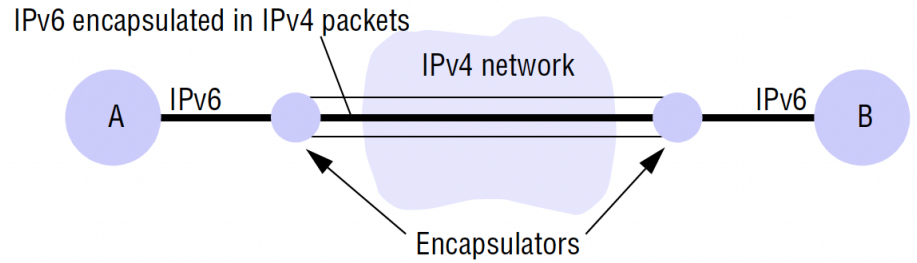


Figure: Tunnelling for IPv6 migration

- Routers: essential in networking.
  - Forward packets correctly, maintain tables.
- Bridges connect networks.
- Hubs connect hosts.
  - Extend network segments.
- Switches route locally.
  - Reduce traffic congestion.
- Tunneling: communication between nodes on different networks.
  - Transmits packets securely.
  - Used to encapsulate IPv6 packets within IPv4 packets so they can be transmitted over IPv4 networks.

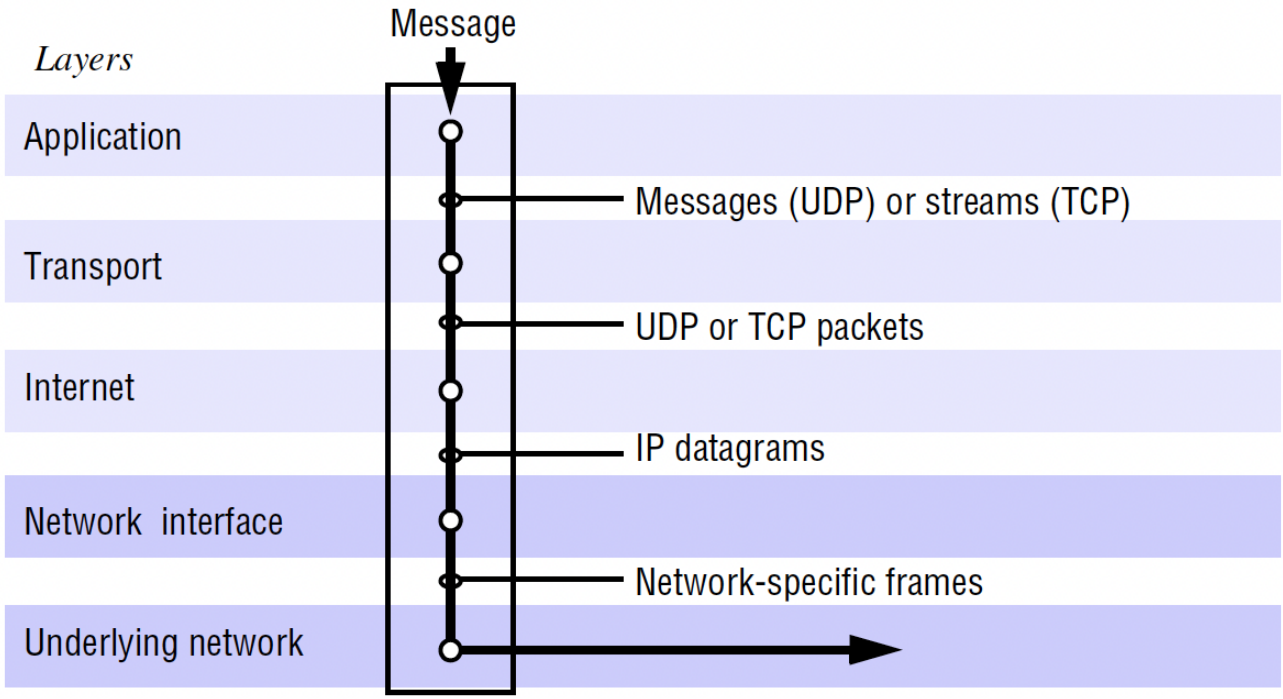
Internet protocols

TCP/IP protocol suite

- TCP: Transmission Control Protocol.
- IP: Internet Protocol.
- Key application protocols.
  - HTTP, SMTP, FTP, Telnet.

Internet protocols

TCP/IP layers



- TCP: reliable.
- UDP: non-reliable.
- IP: primary network protocol.

Internet protocols

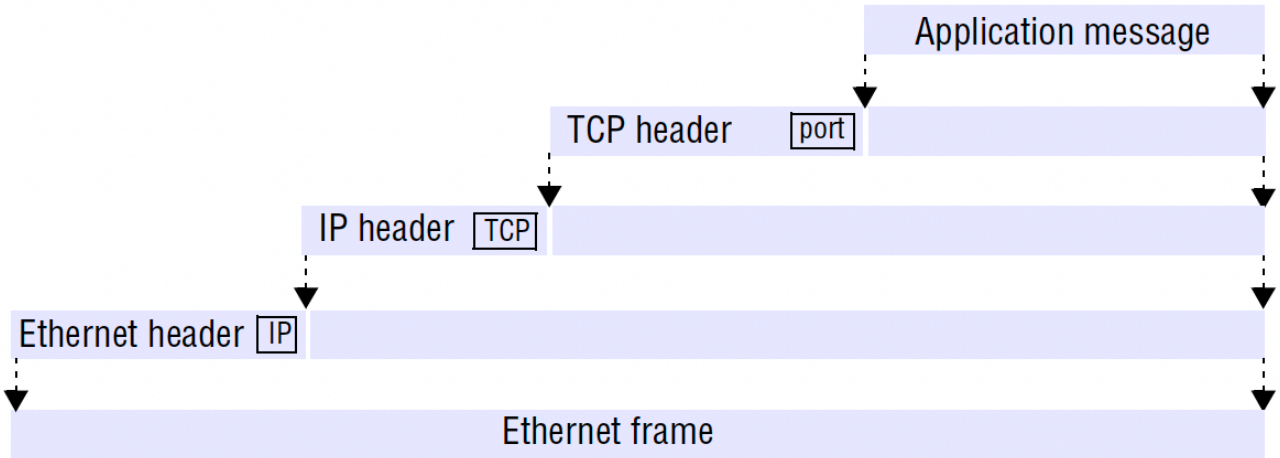
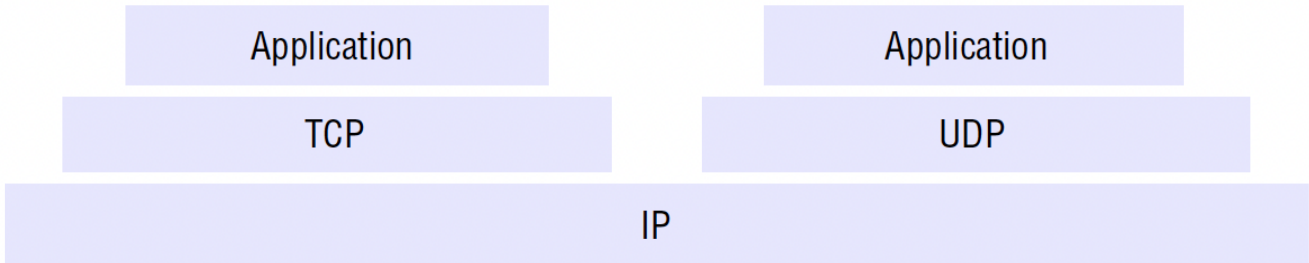


Figure: Encapsulation as it occurs when a message is transmitted via TCP over an Ethernet.

- Tags in the headers: Protocol types for the next layer

Internet protocols

The programmer's conceptual view of a TCP/IP Internet



- IP layered over other technologies.
- Operates across networks.
- Independence from underlying technologies.

Internet protocols

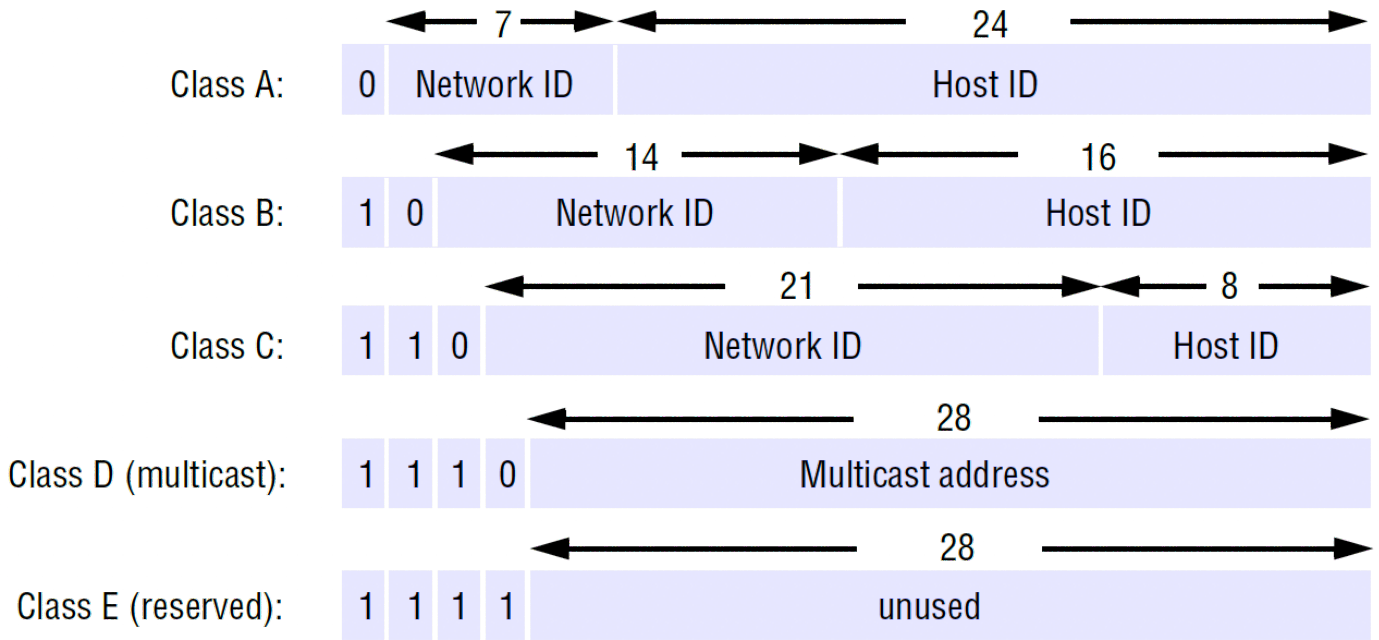
IP addressing

- Designing protocols: naming, addressing, routing.
- Addressing scheme: universal, efficient, anticipating growth.
  - Host assignment: universal.
  - Efficient usage of address space.
    - Predictions inadequate
    - Growth faster-than-expected.
    - Allocation issues.
  - Routing process: flexible, efficient, no extensive routing info.

Internet protocols

IP addressing

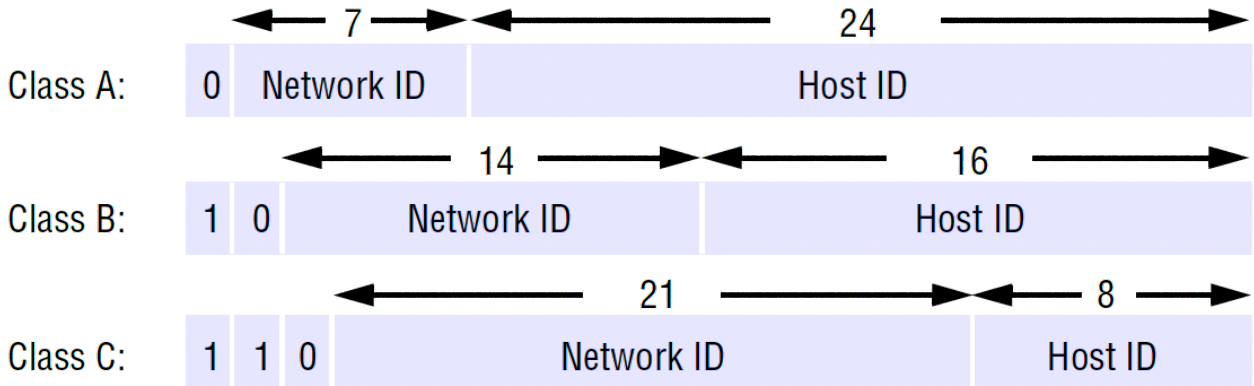
Internet address structure, showing field sizes in bits



- Most traffic relies on old IPv4.
- Address classes: A to E.
- Class D: multicast
- Class E: unallocated, for future use.

Internet protocols

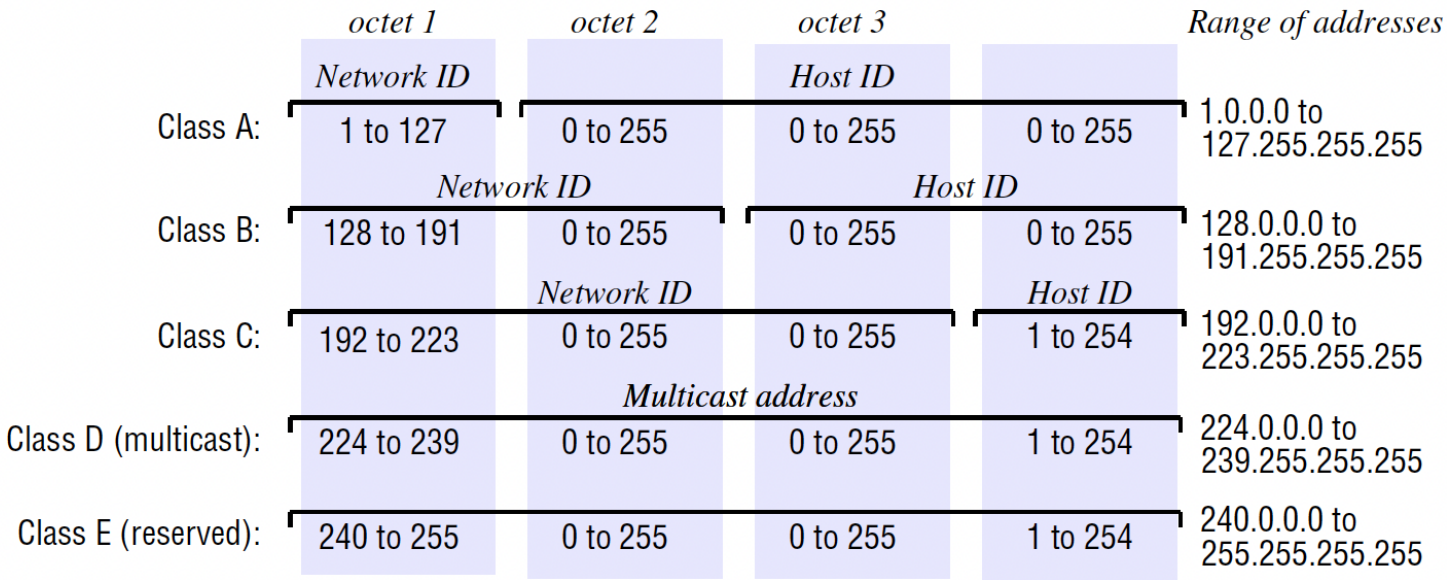
IP addressing



- Network and host identifiers.
- Initially 32-bit deemed sufficient.

Internet protocols

IP addressing



- Decimal number: one of the four bytes, an octet.
- Four octets separated by dots.
- See figure for permissible values.

Internet protocols

IP addressing

- Host identifiers with special purposes.
  - Identifier 0: "this host".
  - All 1s: broadcast message to all hosts.
- Network identifiers by IANA, host identifiers by network administrators.
- Multiple networks, different addresses.
  - Administration complexity

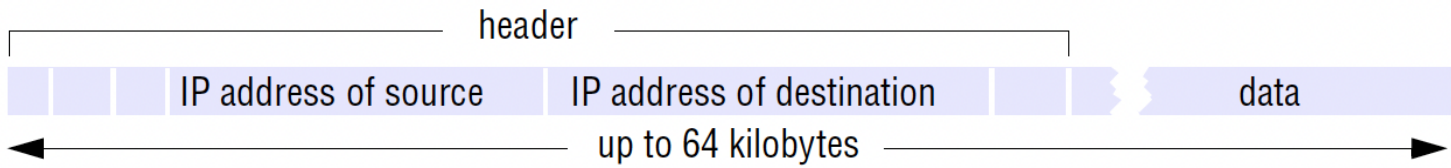
Internet protocols

IP addressing

- Ineffective allocation: running out of IP addresses.
- Solutions:
  - IPv6 development.
  - CIDR scheme.
  - NAT access enabled.

Internet protocols

IP protocol



- IP protocol: datagrams between two hosts.
  - Packet format
- Packets can be lost, duplicated, out of order.
- Checksum in header: addressing errors.
- No checksum in data: leaving it to e.g. TCP, UDP.
- Datagrams fragmented: MTU limit.

Internet protocols

Address resolution

- Resolution module: translates addresses.
- Translation depends on network technology (e.g. Ethernet and ARP).
  - ARP: dynamic enquiries.
  - Cache pairs of Ethernet address - IP address.
  - If in cache, send response immediately.
  - If not in cache, send ARP request.
  - ARP request by Ethernet broadcast.
  - All computers on Ethernet receive and check.
  - Matching computer replies.
  - Cache update with new pairs.
  - Cache accumulation reduces broadcasts.
  - When a new computers joins, broadcasts needed

Internet protocols

IP protocol - IP spoofing

- IP packets include source address.
- Used by servers to respond senders.
- Malicious sender changes source address.
- Vulnerability to distributed denial of service (DDoS) attacks.
  - Attackers send numerous ping requests with target's IP.
  - All responses to target overwhelm input buffers.

Internet protocols

IP routing - Backbones

- Internet - autonomous systems
  - Large organizations - own ASs
  - Each AS - backbone area
    - Backbone - routers, links
  - High bandwidth - reliable links
  - ASs - divided areas
- For resource management and maintenance

Internet protocols

IP routing - Routing protocols

- RIP-1 - first routing protocol
- RIP-2 - improvements over RIP-1
- Shift towards link-state - faster convergence
- New routing algorithms
  - IP protocol remains unchanged
  - Version numbers
- Same routing algorithm in the same topological area
- Backward compatibility

Internet protocols

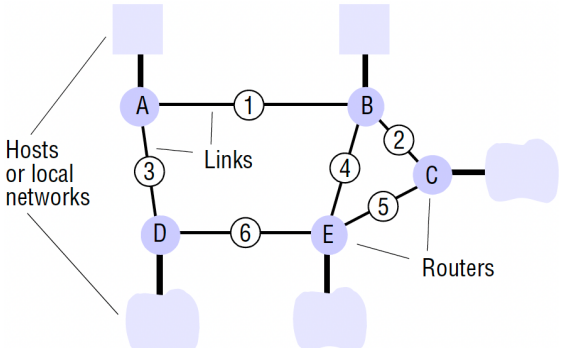
IP routing - Default routes

- Full routing table - impractical
- Two solutions
  - Topological Grouping
  - Default Routes
- Topological Grouping - geographical allocation

Addresses 194.0.0.0 to 195.255.255.255 are in Europe
Addresses 198.0.0.0 to 199.255.255.255 are in North America
Addresses 200.0.0.0 to 201.255.255.255 are in Central and South America
Addresses 202.0.0.0 to 203.255.255.255 are in Asia and the Pacific

Internet protocols

IP routing - Default routes



Routings from C		
To	*Link*	*Cost*
A	2	2
B	2	1
C	local	0
D	5	2
E	5	1

Routings from C		
To	*Link*	*Cost*
B	2	1
C	local	0
E	5	1
Default	5	-

- Default Routes for unlisted destinations
  - Routing table of C change from left to right
  - No specific info on A and D
  - All packets to A and D take link 5
  - Packets to D - efficient
  - Packets to A - extra hop
- Reduce table size

Internet protocols

IP routing - Routing on a Local Subnet

- Local network - packets sent directly
- Different network - packets go to local router

Internet protocols

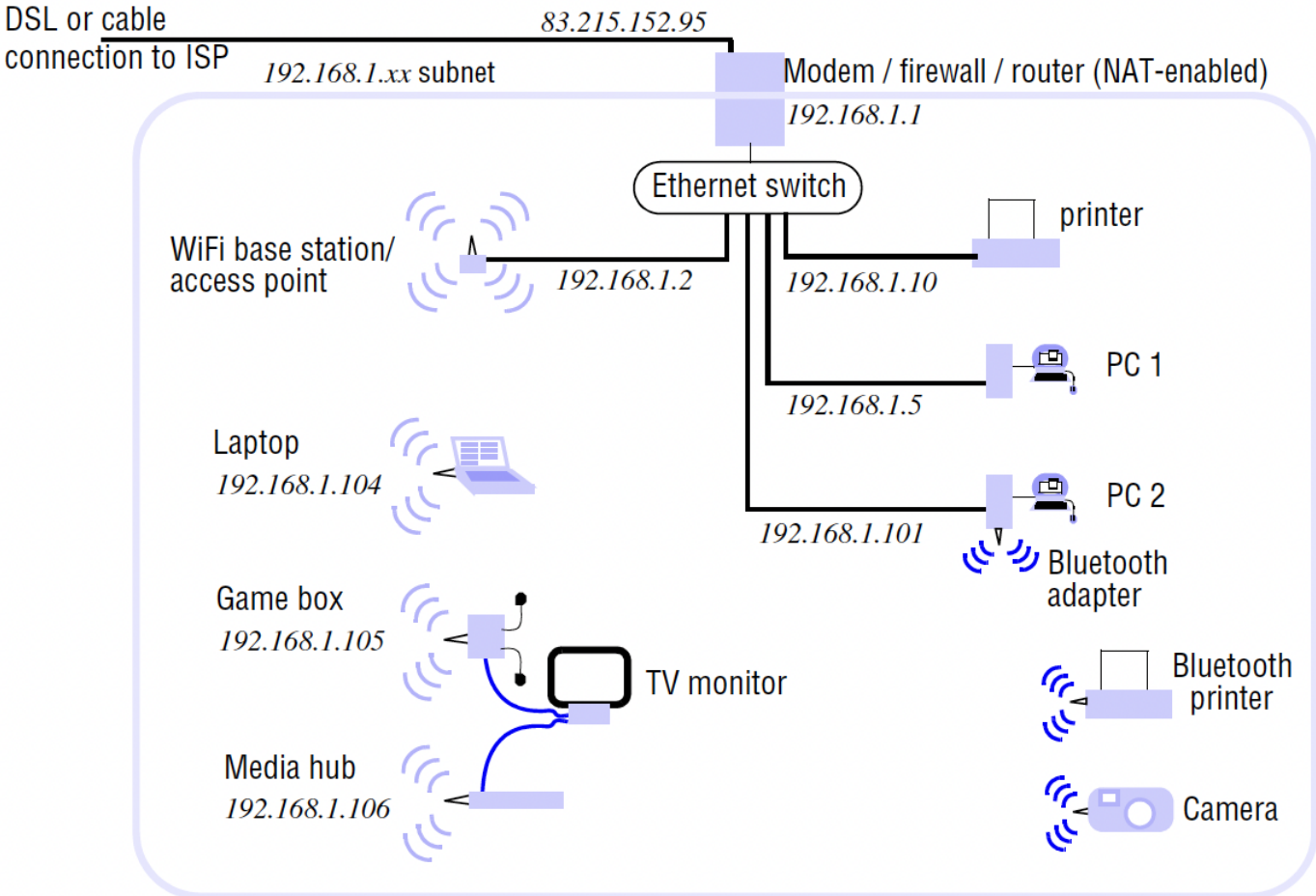
IP routing - Classless inter-domain routing (CIDR)

- CIDR - to address IP shortage
  - Class B: scarcity
- Class C: abundance
- Batch of contiguous Class C allocated
- Mask field - for changing routing tables
  - More flexible addressing than classes - hence, classless

Internet protocols

IP routing - Network Address Translation (NAT)

- Not all devices need a unique - IP
- Local network - NAT router



Internet protocols

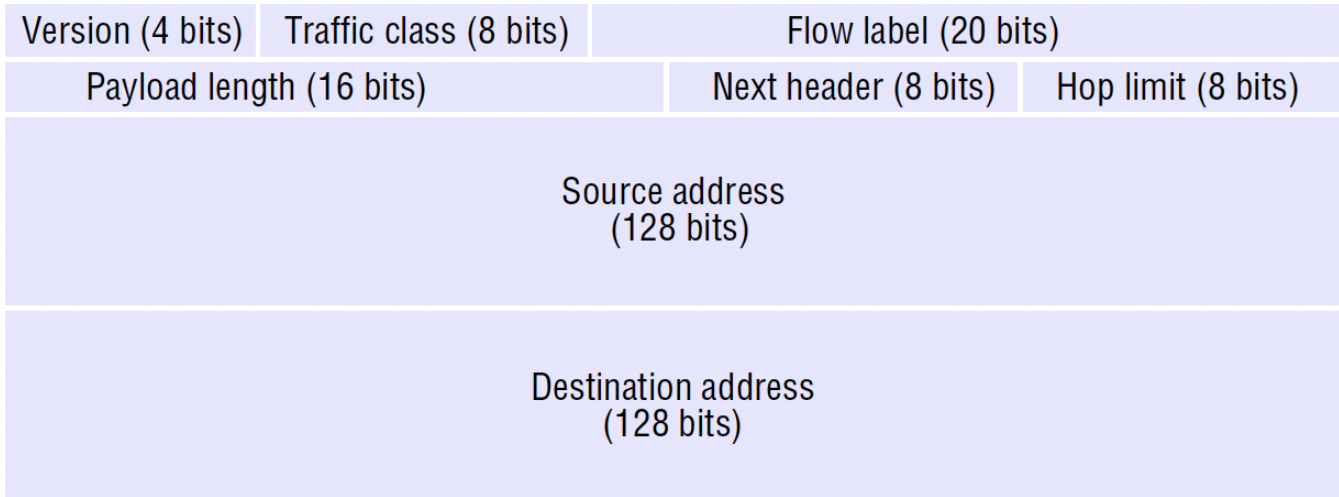
IP routing - Network Address Translation (NAT)

- NAT hides internal IPs
- Maintains an address translation table
  - Internal computer sends a packet - Source IP, port saved in table
  - Router changes source IP to its own, port to a virtual port
  - Modified packet forwarded to external destination
  - Translation table maps virtual ports to internal addresses and ports
  - Router receives packet - Finds internal address
  - Updates destination IP and packet - Forwards to internal computer
- Short term - IP shortage solution

Internet protocols

IP routing - IPv6 Overview

IPv6 header layout



- Address Space - 128-bit addresses
  - Exceeds IPv4 - capacity
  - Partitioned space - address allocation

Internet protocols

IP routing - IPv6 Overview

- Routing speed
  - Simplified headers
  - Eliminates checksums - higher-level errors
  - No fragmentation
- Real-time and other special services
  - Traffic class, flow labels
  - Limited resources - infrastructure enhancements

Internet protocols

IP routing - IPv6 Overview

- Future Evolution: "Next header" extensions.
  - Route definition, fragment handling, authentication, etc.
- Support multicast and introduce anycast
- Security: Built-in security.
  - IP-level security: No need for security-aware application programs.
  - Cost-effective: No encryption needed.
  - Can be used by routers to secure routing table updates.

Internet protocols

IP routing - Migration from IPv4

- Slow Migration: CIDR, NAT effects.
- Growth in mobile: Increased IPv6 need.
- Mixed Traffic: IPv4 and IPv6.
- Major OSs: IPv6 UDP/TCP support.
- Migration strategy: Tunnels between islands, gradually merging islands.

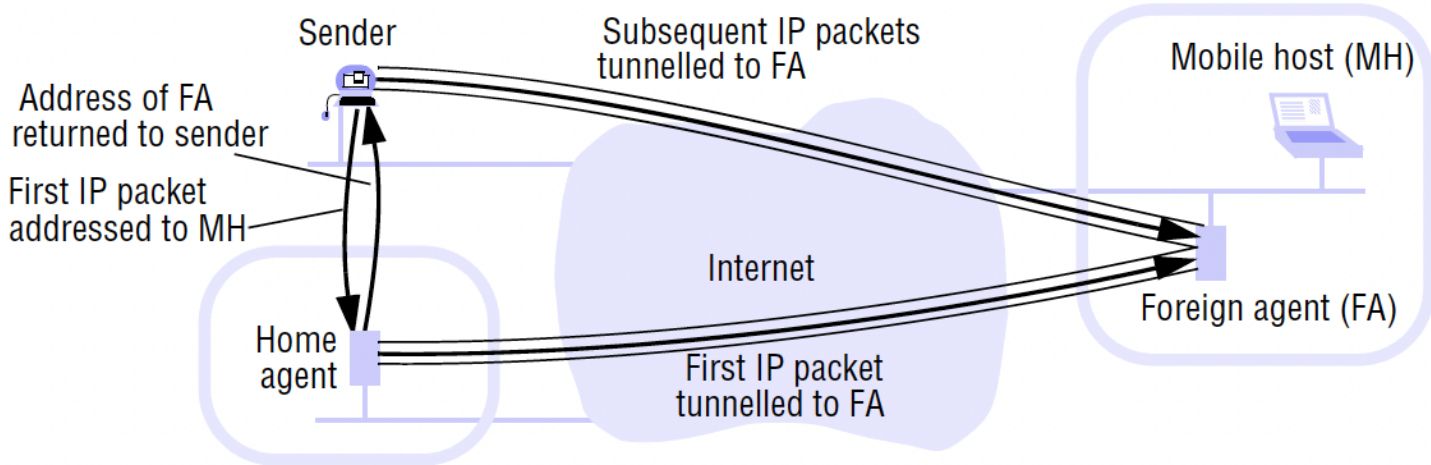
Internet protocols

Mobile IP

- Dynamic IPs: DHCP for mobility.
- Discovery services: Local resource finding.
- Single IP address: Accessibility while moving.
- MobileIP: IP retention across subnets.

Internet protocols

Mobile IP



- MobileIP agents: Home, Foreign.
  - Home base connection: Normal routing.
  - Rerouting: HA and FA coordination.
  - Arrival at new site: FA notified.
  - Temporary IP: Assigned by FA.
  - Tunneled packets: HA to FA delivery.
- Effective, but less efficient less than cellular networks.

Internet protocols

TCP and UDP and Ports

- Protocols: TCP, UDP communication.
- Process-to-process: Using port numbers.
  - IP communication: Computer pairs.
- Port numbers: 16-bit integers.
- TCP, UDP reflect IPv4 capabilities, but is supported also by IPv6.
- IPv6 additional features: New transport services.

Internet protocols

TCP and UDP - UDP features

- UDP: Almost a transport-level replica of IP.
- Data encapsulation: IP packets.
- Short header: Source, destination ports, length, (optional) checksum.
- No delivery guarantee: Packet loss possible.
- Checksum: Error detection.
- No setup costs, no acknowledgment messages.
- Suitable when unreliable delivery is fine.

Internet protocols

TCP and UDP - TCP features

- Reliable delivery.
- Connection-oriented: Bidirectional channel established before data transfer starts.
- Involved the following to ensure reliability:
  - Sequencing
  - Flow Control
  - Retransmission
  - Buffering
  - Checksum

Internet protocols

TCP and UDP - TCP features

- Sequencing: Segments with sequence numbers.
- Flow Control: Prevents sender from overwhelmig receiver.
  - Receiver records the number of the last successfully received segment.
  - Acknowledgment: Highest sequence number and window size.
    - Window size: How much data can be transmitted before next acknowledgement.
  - Timeout T: Local buffer management.
  - Data is sent either when it reaches timeout or MTU.

Internet protocols

TCP and UDP - TCP features

- Retransmission: Unacknowledged segments resent.
  - Segments stored at outgoing buffer until acknowledgement.
  - If acknowledged, deleted. If not acknowledged until T, resent.
- Buffering: Flow management.
  - Incoming buffer (at receiver) used to balance flow
  - If *receive* is slower, than *send*, grows. If buffer full, packets dropped.
- Checksum: Data integrity verification.

Internet protocols

Domain names

- DNS: Translates symbolic names to IP addresses.
- Hierarchical structure:
  - Simple Domain: example.com.
  - Subdomain: shop.example.com.

Internet protocols

Domain names

- DNS servers: Manage domain tree.
- Multiple servers hold domain and host names.
- Resolve requests by recursively contacting other servers.
- Caching crucial for efficiency.

Internet protocols

Firewall

- Internet is essential for service provision.
  - Individual protection, yet weaknesses inevitable.
- Firewalls: Monitor communication into and out of an intranet according organization's policies.
- Policies: Service control, behavior control, user control.

Internet protocols

Firewall

Filters operate: Different levels.

- IP packet filtering: Individual packets.
  - Source/destination checks.
  - TCP filtering: Using port numbers.
  - Router filtering: IP filtering.
  - Multiple firewalls: Cascaded filters.
- TCP gateways:
  - Checks TCP segments to prevent disruptions.
- Application-level gateway: Proxy for applications.

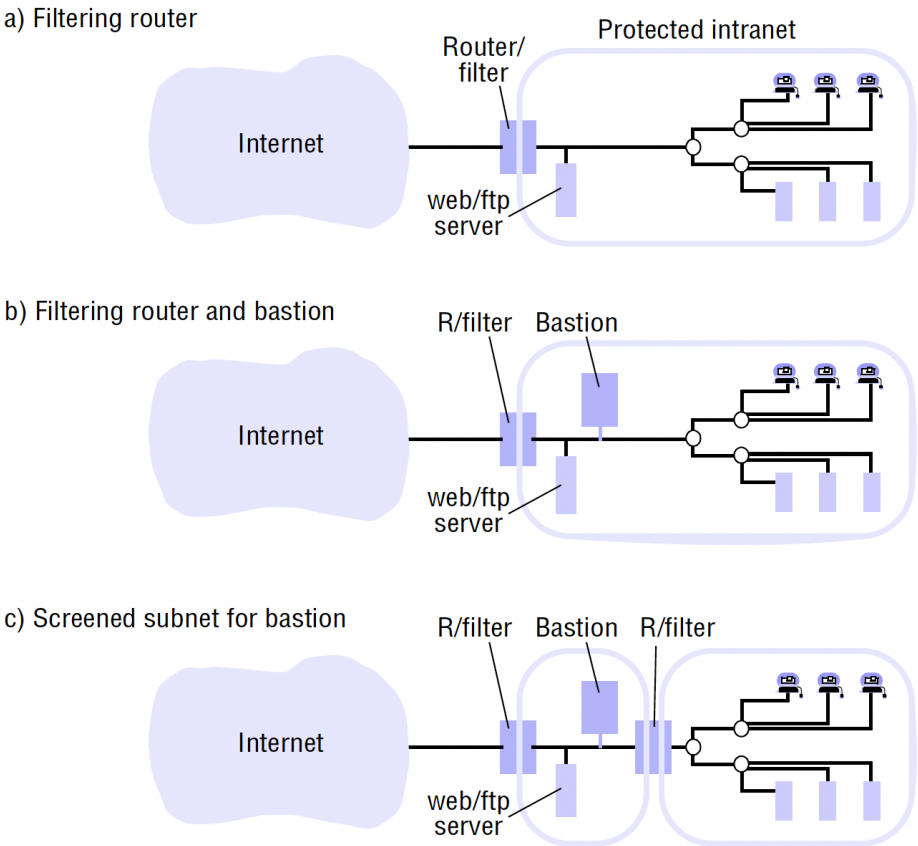
Internet protocols

Firewall

- Firewall composed of multiple processes with shared duties.
- Secure configurations involve also a bastion host.
  - Attack resilience.
  - Acts as barrier.
  - Fortified measures to enhance security.

Internet protocols

Firewall



- (a) Simple IP filtering.
- (b) More complex configuration.
  - Bastion may run TCP or application-level gateway processes.
- (c) Composite firewall.
  - Series of two router/filters.

Internet protocols

Virtual private networks (VPNs)

- VPNs: Enhanced firewall protection.
- Encrypted channels at IP level.
  - Intranet access: Like internal user.
  - Local host shares cryptographic keys with the firewall.

Discussion topic

What is the task of an Ethernet switch? What tables does it maintain?

Discussion topic

Compare connectionless (UDP) and connection-oriented (TCP) communication for the implementation of each of the following application-level or presentation-level protocols:
i) virtual terminal access (for example, Telnet);
ii) file transfer (for example, FTP);
iii) user location (for example, rwho, finger);
iv) information browsing (for example, HTTP);
v) remote procedure call.

Discussion topic

Explain how it is possible for a sequence of packets transmitted through a wide area network to arrive at their destination in an order that differs from that in which they were sent. Why can't this happen in a local network?