Deployment and Operations for Software Engineers 2nd Ed

Chapter 3—Networking

Outline

- **Introduction**
- IP addresses
- DNS
- Ports
- Bridged and NAT networks
- TCP
- Structuring your network

Messages

- The only method of communication between two nodes in a distributed system is a message – a collection of bits passed from a sender to a recipient.
- A message reflects an agreement between the sender and the recipient about the meaning of the bits.
- A protocol is a standardized agreement about the meaning of the bits.
- A portion of the boot process is connecting to a network adaptor. E.g. Wi-Fi or cabled.

Layers of the internet

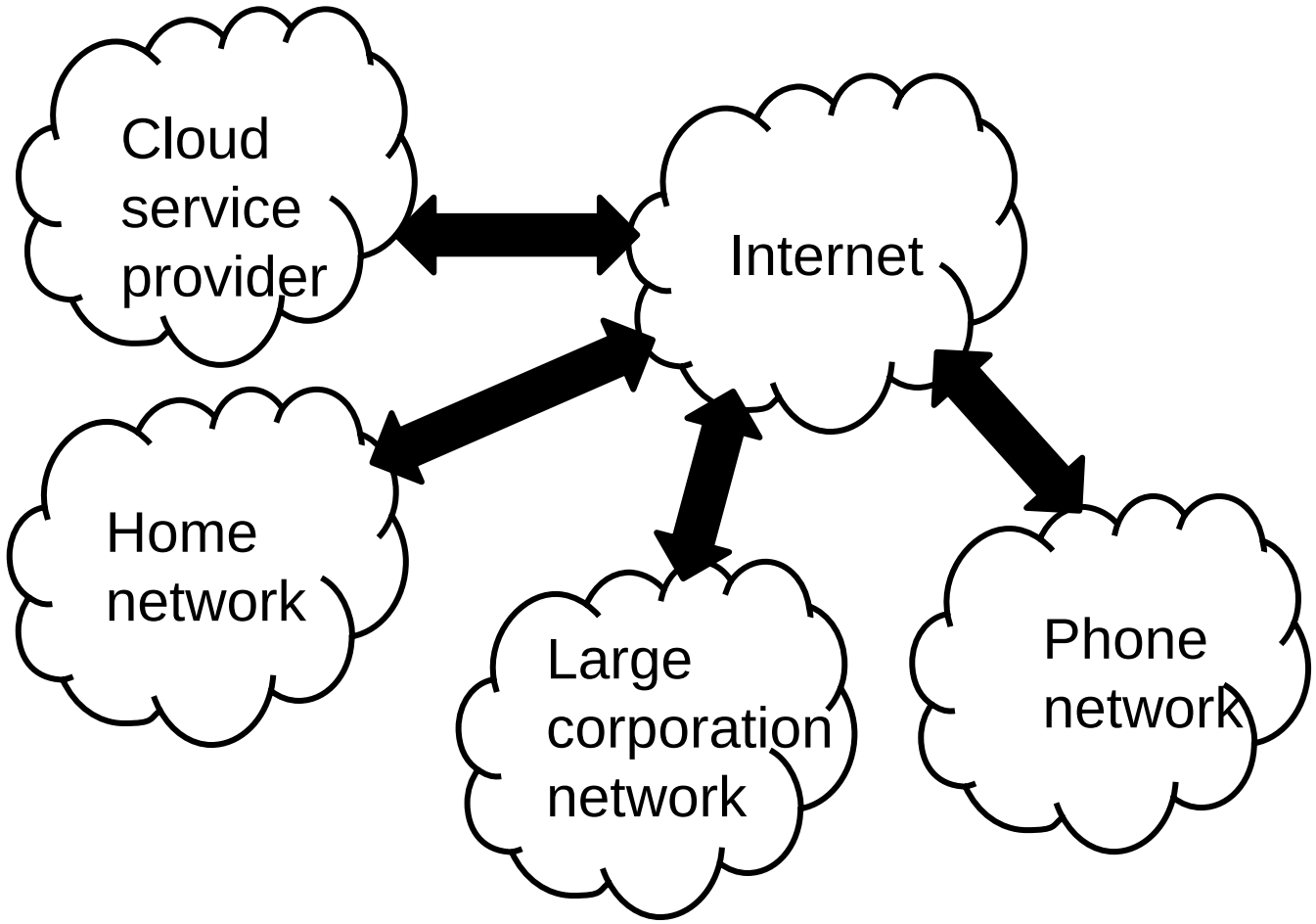
- The internet is logically divided into four layers and each layer has a collection of protocols.
- The ISO 7-layer model is (arguably) no longer used.

Layers	Typical Protocols
Application	HTTP, IMAP, LDAP, DHCP, FTP
Transport	TCP, UDP, RSVP
Internet	IPv4, IPv6, ECN, IPsec
Datalink	Ethernet, ATM, DSL, L2TP

Multiple networks

- Your device is on a local network that may use one type of protocol.
- You wish to send a message to a device on another local network, possibly through a third network and possibly using a different protocol.
- Connection terminology
  - A gateway connects two networks and converts information, data or other communications between the protocols used by these two networks.
  - A firewall is a gateway that monitors incoming and outgoing network traffic and permits or blocks data packets. Firewalls are configured by specifying rules:
  - A proxy is a gateway that manages internet traffic on your behalf. A proxy server hides your IP address from the outside world.

Connecting different types of networks



- A gateway (⟷) joins two different networks

Common misunderstandings about networks

1. The network is reliable.
2. Latency is zero.
3. Bandwidth is infinite.
4. The network is secure.
5. Technology does not change.
6. There is one administrator.
7. Transport cost is zero.
8. The network is homogeneous.

Discussion questions

1. What is the benefit of viewing the internet as a collection of layers?
2. Why would you use one protocol in a given layer instead of another?
3. What are the limitations of using messages as a communication mechanism?

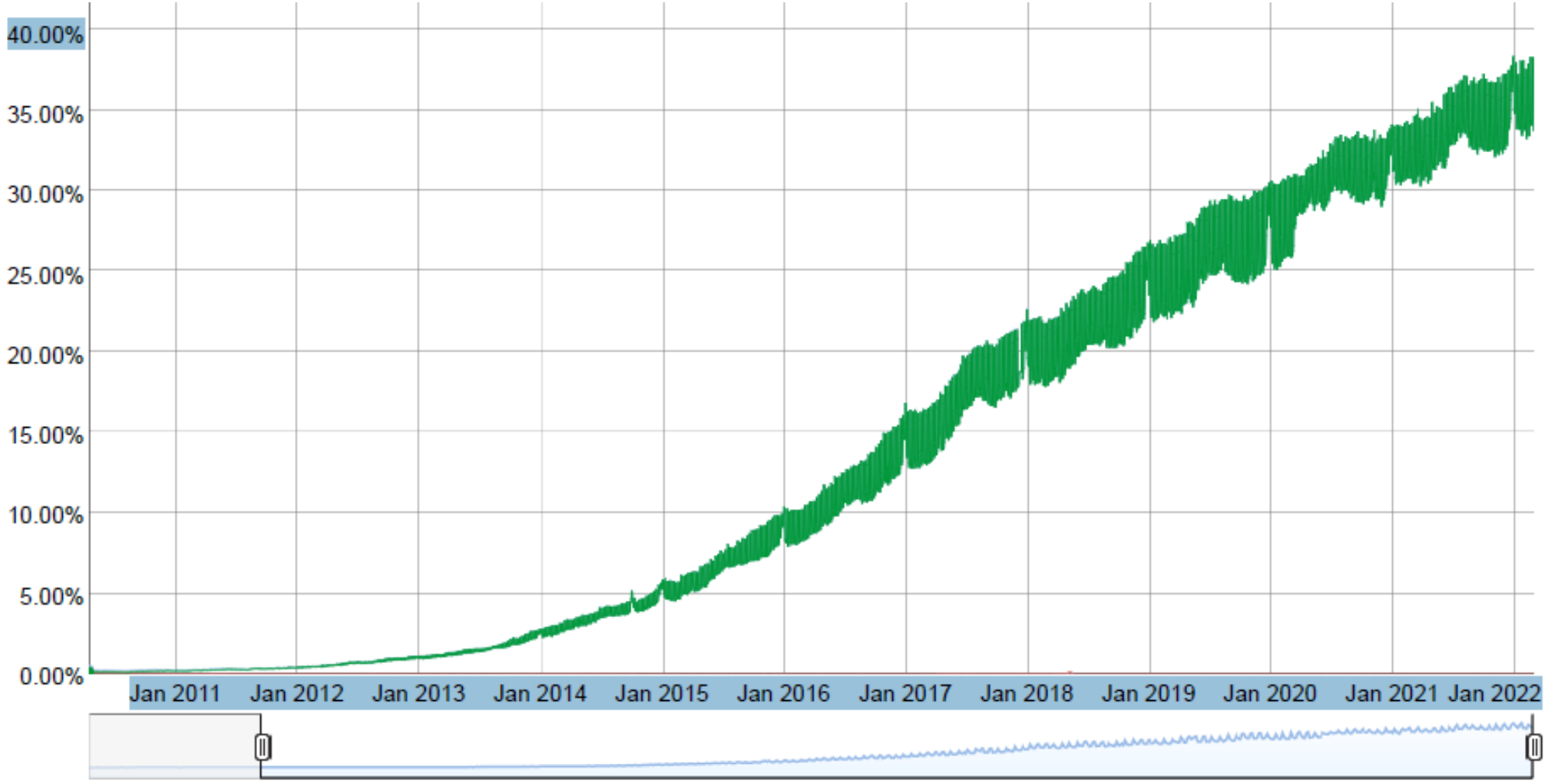
Outline

- Introduction
- **IP addresses**
- DNS
- Ports
- Bridged and NAT networks
- TCP
- Structuring your network

Internet Protocol (IP)

- IP is a protocol for the internet layer in the four layer view of networks.
- Two versions of IP
  - IPv4--32 bits
  - IPv6—128 bits
- IPv6 standardized in 1996
- Representing IP addresses
  - IPv4—xxx.xxx.xxx.xxx where xxx is a decimal number between 0 and 255. E.g. 4.31.198.44
  - IPv6 – eight groups of four hexadecimal numbers separated by colons. E.g 2001:1900:3001:11::2c.

Adoption of IPv6 – less than 40%



Assigning IP addresses

- Every device (real or virtual) on the internet is assigned an IP address.
  - VMs
  - Containers
  - Internet of Things (IoT) – toasters, refrigerators, thermostats, etc
- he Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization with the responsibility for assigning domain names and IP addresses.
- It allocates addresses in large blocks (X.0.0.0 through X.255.255.255) to regional entities.
- A recipient of one these large blocks is authorized by ICANN to split up the block and further allocate the addresses in smaller blocks.

IP addresses

- Your ISP has been allocated a collection of IP addresses
- Each address is either public or private
  - A public IP address is available from anywhere in the network
  - A private IP address is restricted to a local network.
- Each address is either static or dynamic
  - A static IP address is assigned permanently to a device
  - A dynamic IP address is temporary.

Private IP addresses

- The following addresses are always private
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
- 127.0.0.1 is reserved for “localhost”
- A message sent to localhost will be delivered back to sender. Allows for testing.

Dynamic IP addresses

- Your ISP has been allocated a collection of IP addresses.
- It assigns one to your device when you log in and it remains until you log off.
- The Dynamic Host Configuration Protocol (DHCP) is used to assign an IP address to your device.
- Your local network has a DHCP server. Your device broadcasts a request which is recognized by the DHCP server.
- The DHCP server manages a pool of IP addresses and assigns one to your device

Composing a message

- Each message consists of a header and a payload.
- Suppose you wish to send a HTTP message over TCP/IP, how is wrapped?
- The HTTP message is the payload of the TCP message
- The TCP message is the payload of the IP message

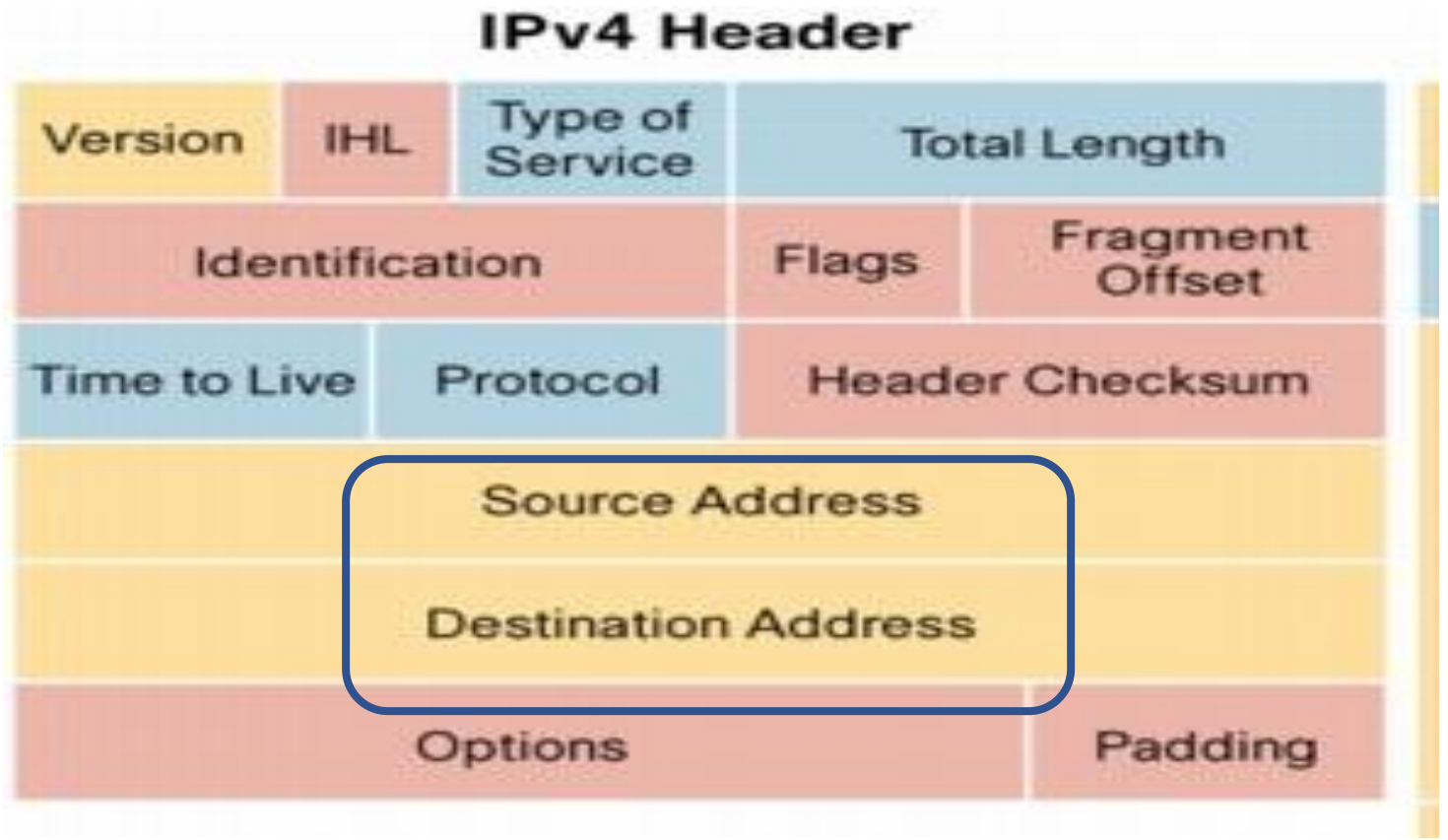
Mail Analogy

- Message to individual wrapped in an envelope (App level protocol)
- That envelope is enclosed in an envelope with house number (TCP)
- That envelope is, in turn, enclosed in an envelope with post office address (IP)
- Outer envelope arrives at a post office
- Opened to expose intermediate envelope which is delivered to a house
- Opened to expose inner envelope which is delivered to an individual
- Individual opens envelope to get message

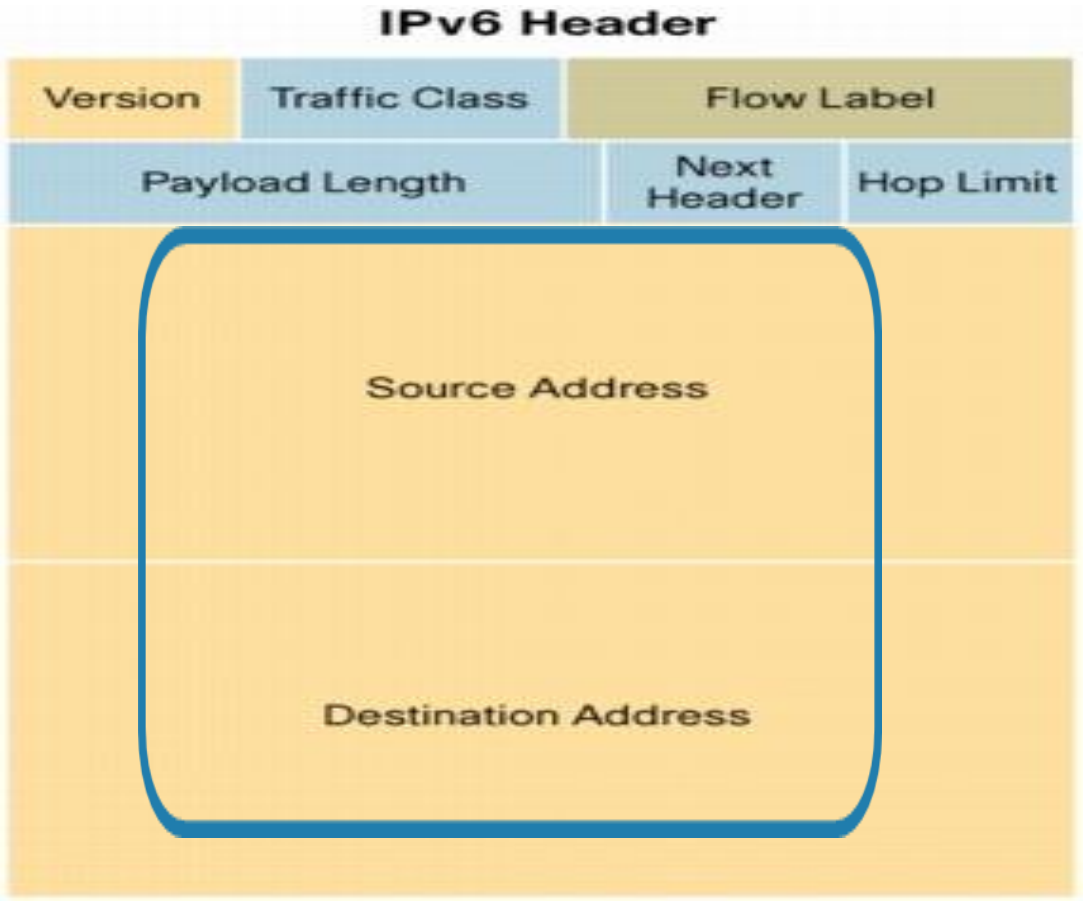
Message Format

- An IP message has a header and a payload. The header includes
  - IP address of the source
  - IP address of the destination

Internet Protocol packet structure (v4)



Internet Protocol packet structure (v6)



Message Structure

- A device creates a message by creating a header and adding a payload and placing it on the network.
- IP_A sends a message to IP_B and it consists of header+payload
- Recipient responds to source address in header

Manipulating messages

- When IP_A sends message to IP_B, i.e., IP_A+payload -> IP_B , a gateway can make it look like the message comes from the gateway. i.e. $IP_{gateway}$+payload -> IP_B
- In this case the gateway must have a mechanism so that it can manage the response from IP_B

Discussion questions

1. Why has the adoption of IPv6 been so slow?
2. Is the DHCP server on your local network or on the ISP's network?
3. What are some mechanisms a gateway can use to return a response to the original source?

Outline

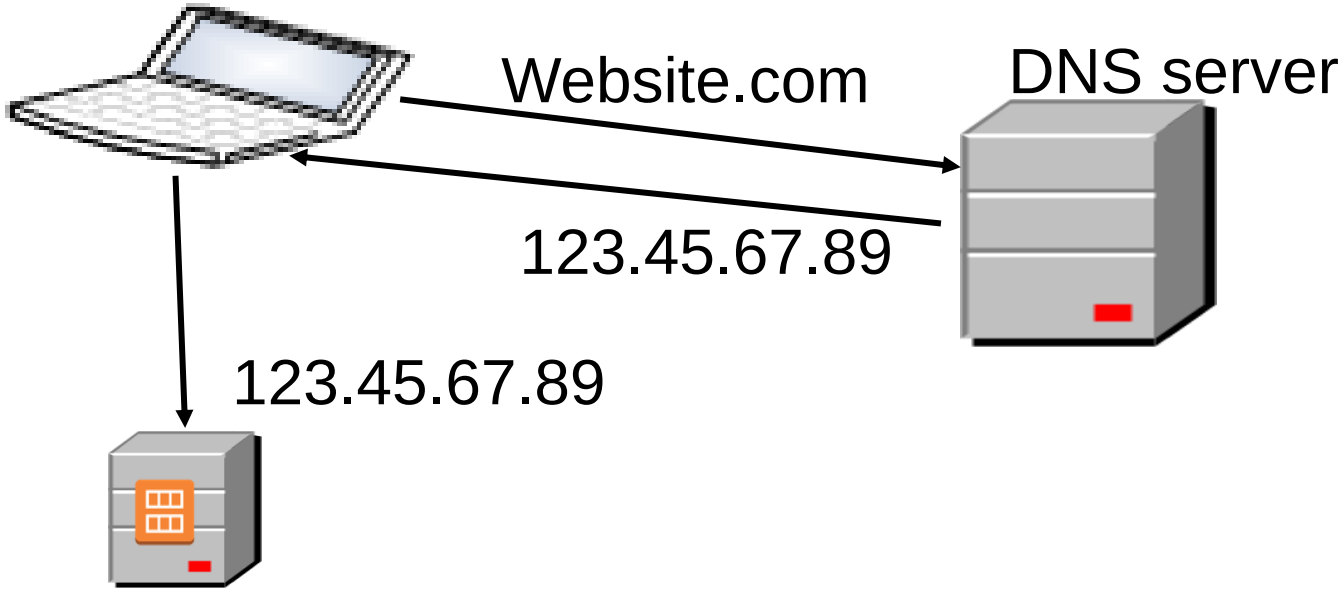
- Introduction
- IP addresses
- **DNS**
- Ports
- Bridged and NAT networks
- TCP
- Structuring your network

Domain Name System (DNS)

- IP addresses are too cumbersome for people to use.
- Uniform Resource Locators (URLs) are used to identify devices
- A directory service is used to map from names to IP addresses (think of a phone book)
- The Domain Name System (DNS) is a global directory service for VMs.
- DNS is managed by ICANN.

Domain Name System Server

- Client sends URL to DNS server
- DNS server takes as input a URL and returns an IP address
- Client uses IP address to send message to a site



Complications

- In reality, messages being transmitted from one computer to another is more complicated.
- The picture showed a single DNS server.
- There are multiple DNS servers
- There is a hierarchy of DNS servers.
- The picture showed a single line from client to server.
- There is a network of routers to transmit messages
- Shares load

DNS Hierarchy

- Consider URL www.mse.isri.cmu.edu
- If one server held all DNS -> IP mappings, it would both get overloaded and hold over 200 million mappings.
- DNS is arranged as a hierarchy.

Finding www.mse.isri.cmu.edu

- Begin with “root server”. There are 13 root servers with known IP addresses. These are built into the router. (https://www.iana.org/domains/root/servers)
- Access root server to get IP address of the .edu DNS server
- The .edu DNS server has the IP of the .cmu.edu DNS server and so forth.
- Eventually you get to a DNS server that is under local control
- This allows MSE to change the IP of the various local DNSs without changing anything up the hierarchy.

Map of the Root Servers

DNS system is tightly secured

- If an attacker could manipulate a DNS server, they could disrupt the portion of the internet specified by that server.
- Root servers have extensive physical and internet security and other servers also are secured.
- Means that changing IP addresses within a DNS server is restricted to authorized personnel.
- We will discuss DNSSEC later. This is another means of securing the DNS system.

Time to Live

- Clients do not access a DNS server for every request. It would generate too much internet traffic.
- Associated with each DNS entry is a Time To Live (TTL).
- This is also called a “Refresh Interval” in the DNS resource record called Start of Authority (SOA).
- The client or the ISP caches the IP addresses associated with DNS entries and these entries are valid for the TTL.
- This is distinct from the TTL listed in the IPv4 packet header.

TTL settings

- The value of the TTL depends where in the hierarchy the record exists.
- High in the hierarchy (authorative servers), TTLs are set to seven days since the likelihood of there being a change is low.
- Records under local control can have their TTLs set low (~seconds)
- Minimum is 1 second.

Client (browser) perspective on DNS, URL, and TTL

- Client gets ip addresses of an edu server from root
- TTL is 7 days
- Client gets IP addresses of a server cmu from edu server
- TTL is 7 days
- Client gets ip addresses of isri from cmu server
- TTL is 12 hours
- Client gets ip address of mse server from isri server
- TTL is 6 hours
- Client gets ip address of www server from mse server
- TTL is 5 minutes
- Times are estimates, actual values are probably different

Using DNS to Handle Overload and Failure

- The DNS server may return a list of IP addresses for a given URL
- By rotating the list (first time 1,2,3 -- second time 2,3,1 -- etc) load is distributed among different instances of given URL
- Instance may have failed. Browser will retry several times but having a list gives the browser a fall back IP.

Discussion questions

1. Why is DNS primarily for VMs and not containers?
2. What is the sequence of IPs from root to your device?

Outline

- Introduction
- IP addresses
- DNS
- **Ports**
- Bridged and NAT networks
- TCP
- Structuring your network

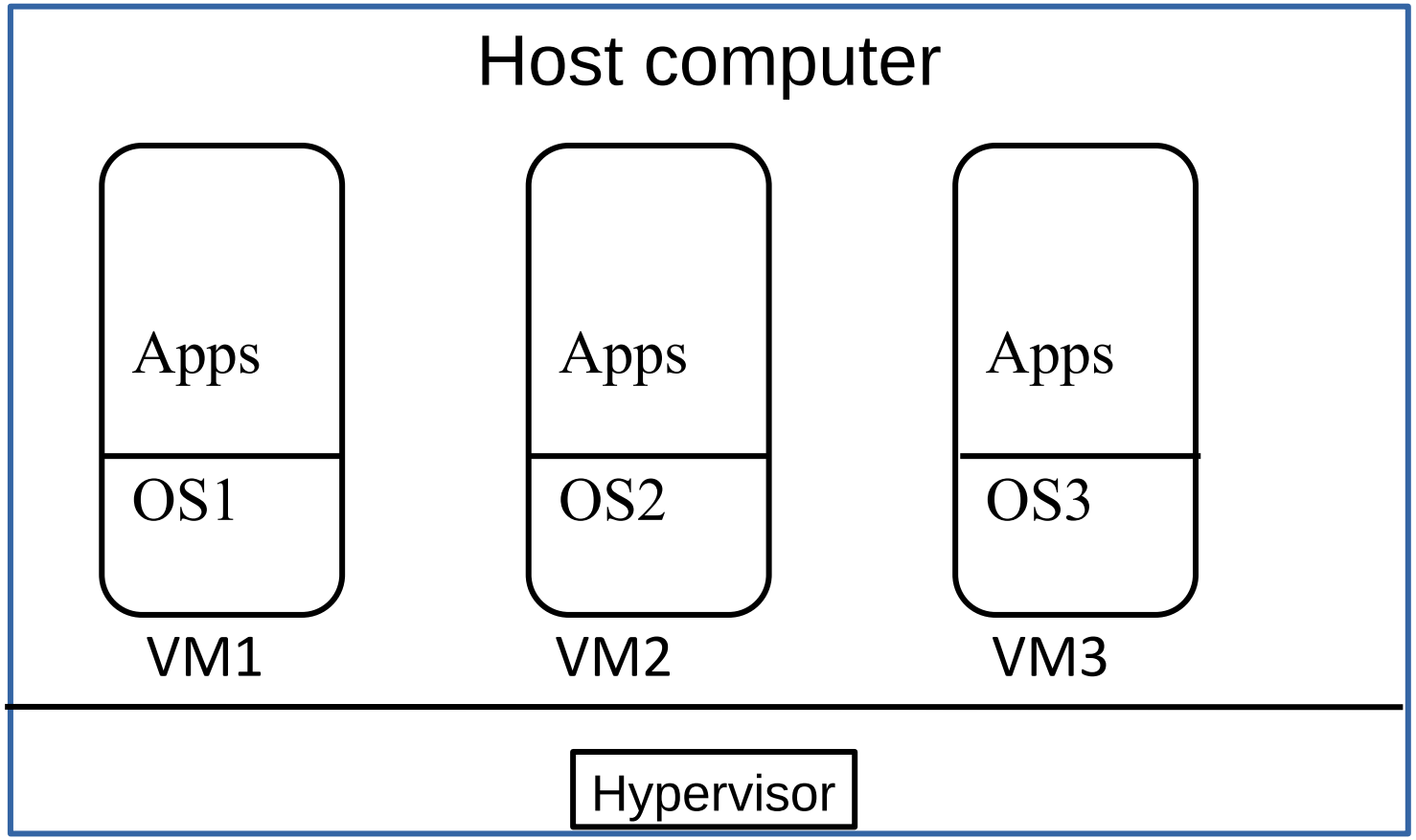
Getting a message to a service

- An IP address will get a message to a VM or container. It still must be routed to a service to have effect.
- A service listens for messages on a port.
- The analogy is with an old-fashioned telephone switchboard.
  - A call comes in to a hotel on the hotel's number.
  - The operator answers and asks, "what room?"
  - A cord is plugged into the room receptacle
  - The telephone rings in that room and the occupant of the room can then talk on the phone.

Port numbers

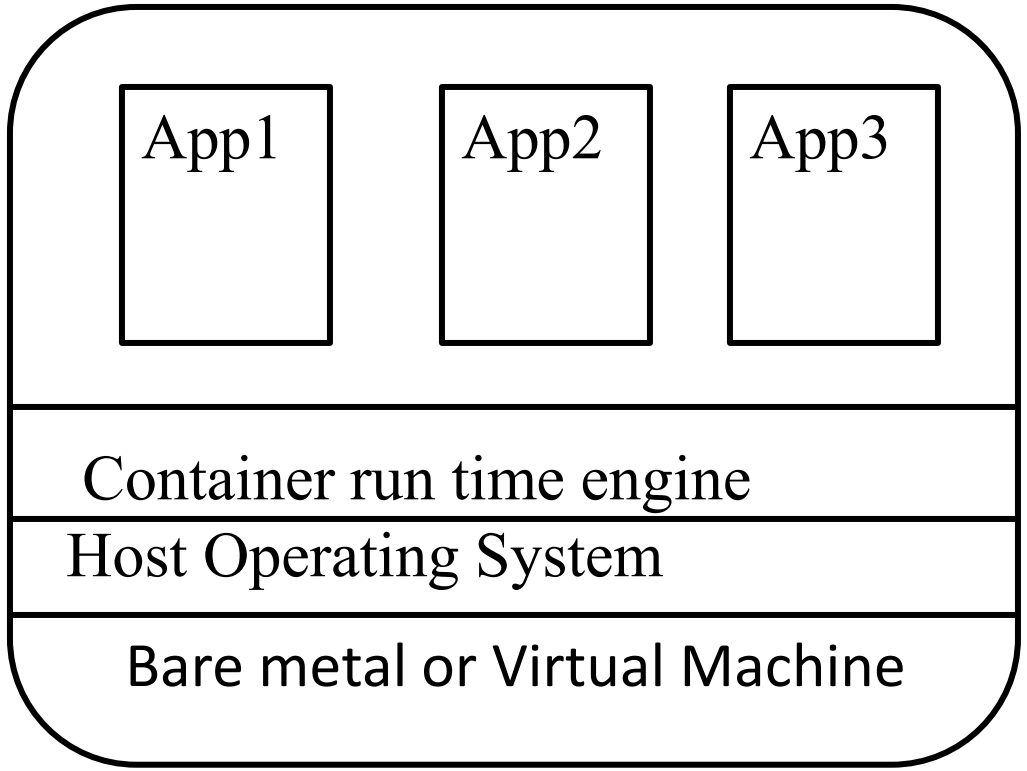
- Each service listens on one or more ports.
- Some port numbers are assigned by ICANN
  - 22 for Secure Shell (SSH)
  - 25 for mail service
  - 53 for DNS
  - 80 for HTTP (hypertext transfer protocol)
  - 443 for HTTPS (secure hypertext transfer protocol)
- Other port numbers are by agreement with sender and recipient.
- Operating system on IP destination will forward message to specified port.

Message intended for a VM



- Each VM has its own OS
- Each OS will manage ports in its VM

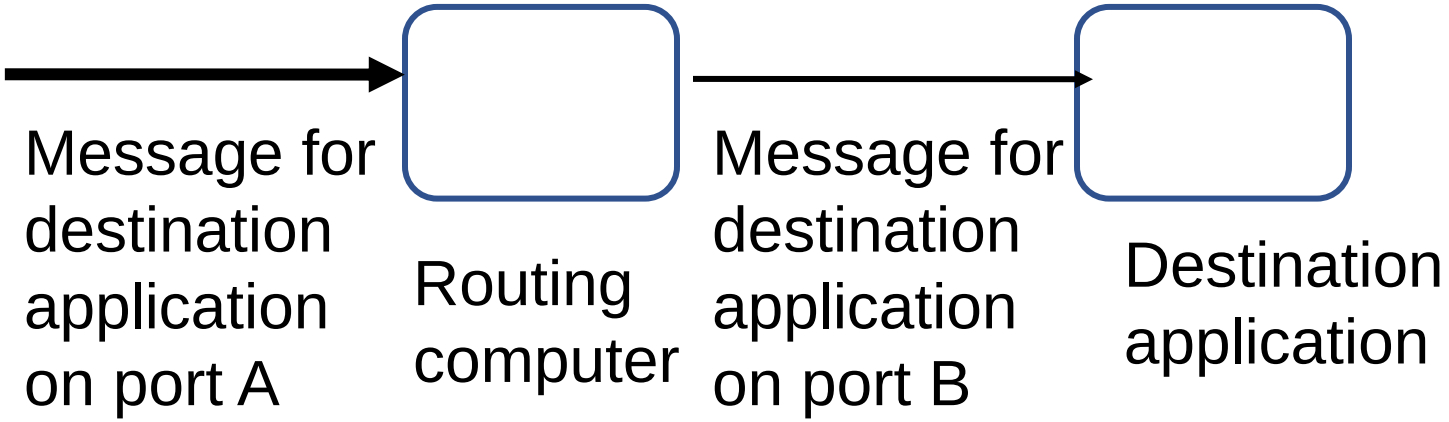
Message intended for a container



- Containers share OS
- Port collision can occur
  - E.g suppose App1 and App2 are web servers
  - They both listen on port 80
- OS does not know how to route a message.

Port forwarding

- Two services listening on the same port may cause a message destined for one application to be sent to another.
- Port forwarding tells a routing computer that a message specified for one port should actually be delivered to another.



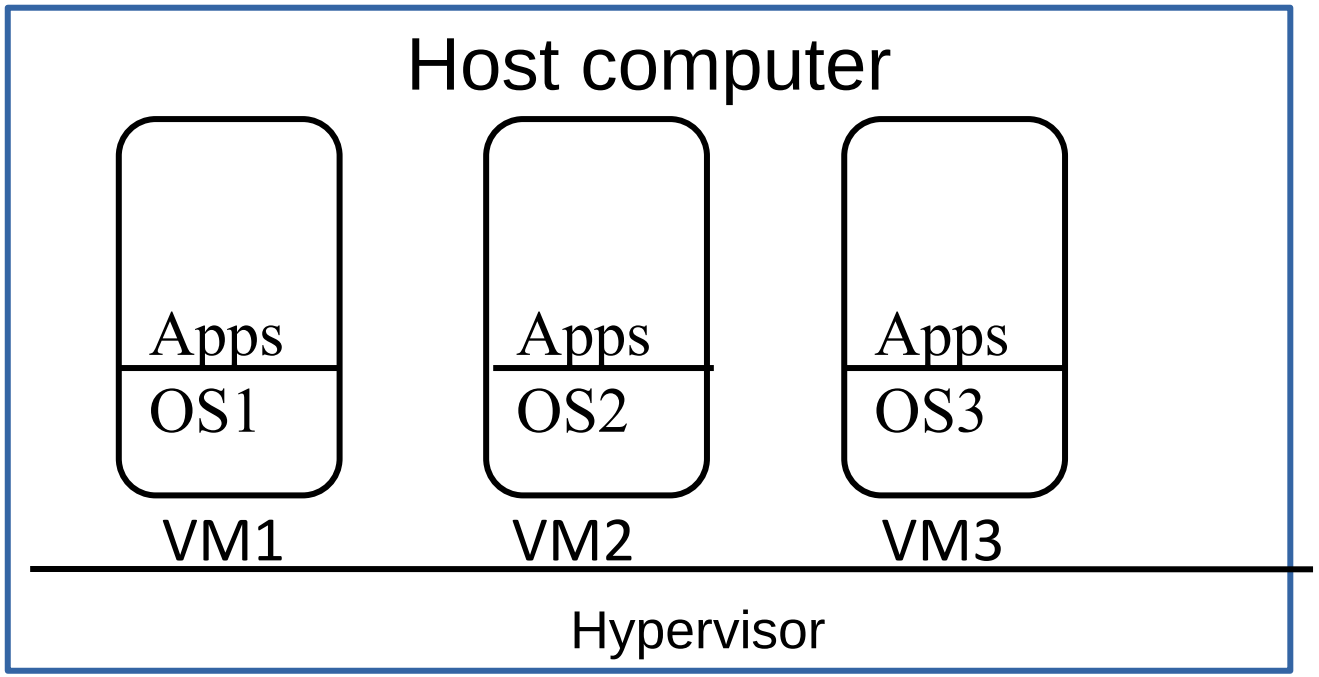
Discussion questions

1. What are some other dedicated port numbers?
2. What port numbers are not assigned?

Outline

- Introduction
- IP addresses
- DNS
- Ports
- **Bridged and NAT networks**
- TCP
- Structuring your network

Bridged networks

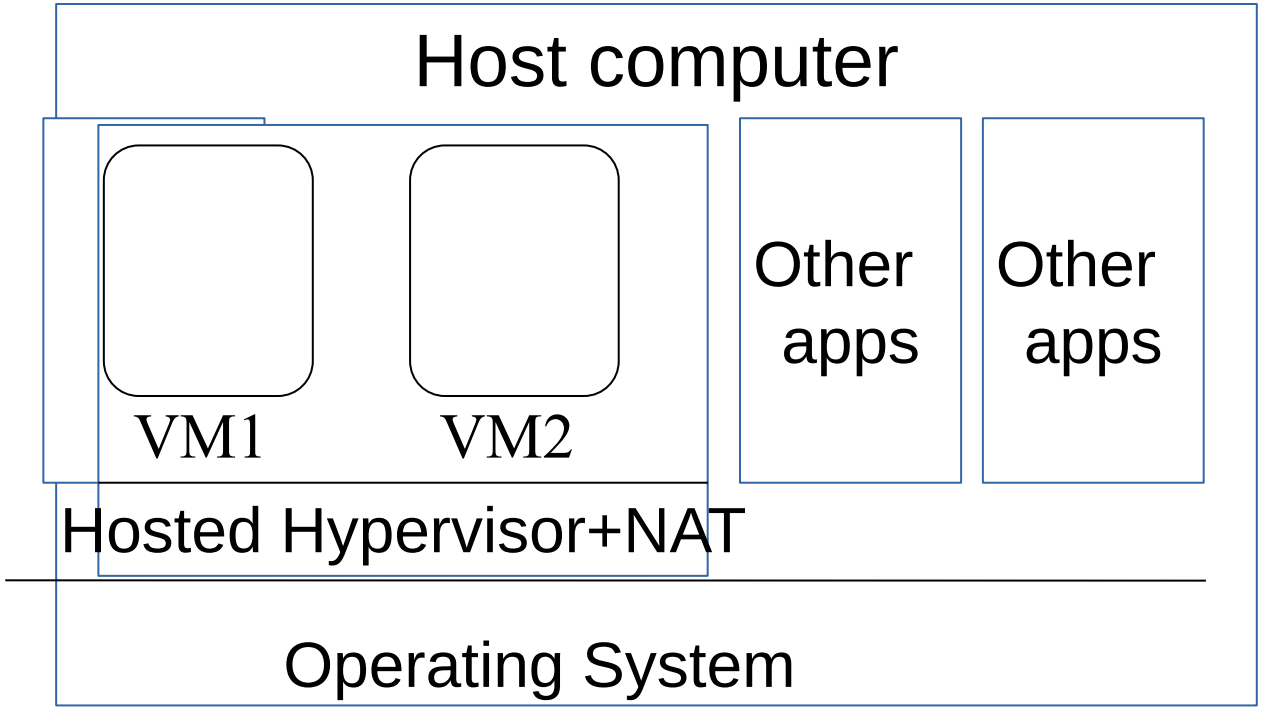


- Recall that booting a VM connects it to a network adapter on the host computer.
- A bridged network has all of the VMs connected to the host network adapter.

Bridged network IP management

- Each VM on the bridged network has its own IP address.
- The IP address can be public or private.
- The VMs on a bridged network may or may not be behind a gateway.
- Public IP addresses can be directly accessed from the internet.

NAT network



- NAT acts as gateway for VM IPs
- VM IPs are all private
- NAT is connected to host network adapter
- NAT can act as a firewall

Discussion questions

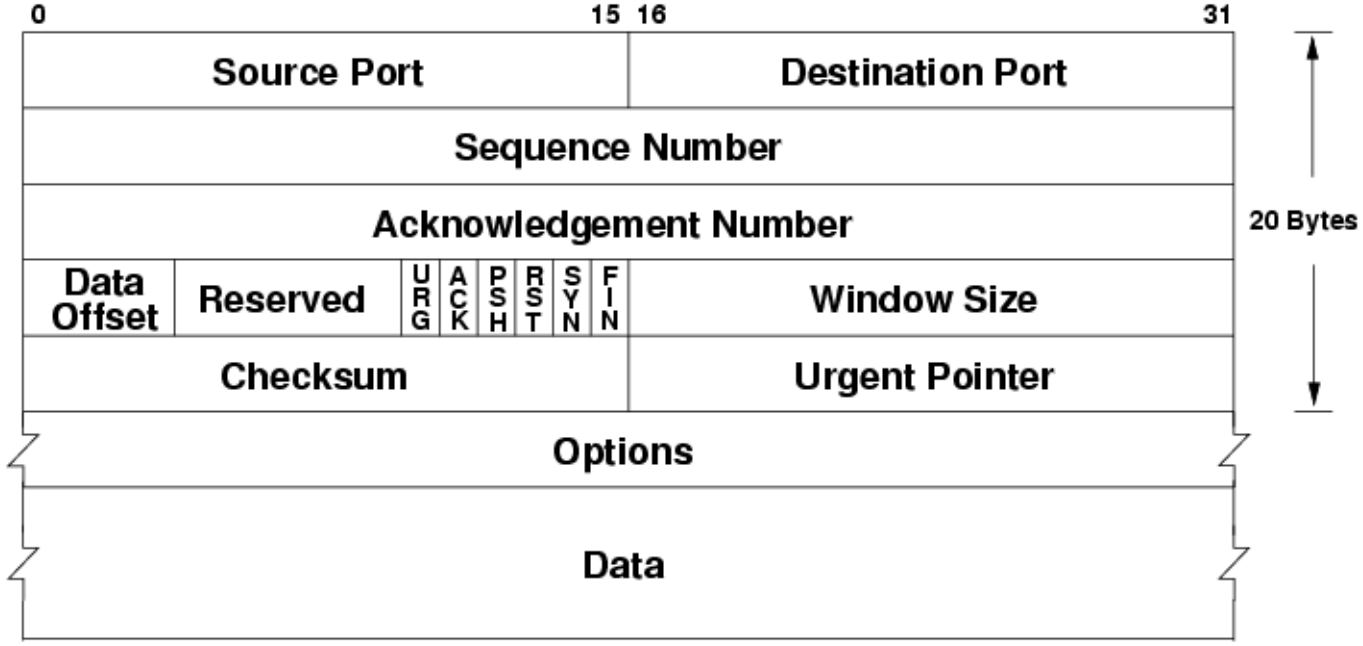
1. The slides show bridged networks for Type 1 hypervisors and NAT networks for Type 2 hypervisors. Is this necessary?
2. The slides show how messages are routed for VMs. What are the corresponding figures for containers?

Outline

- Introduction
- IP addresses
- DNS
- Ports
- Bridged and NAT networks
- **TCP**
- Structuring your network

TCP

- Transmission Control Protocol (TCP) is a layer 2 (transport) protocol
- It is commonly wrapped as the payload in an IP message.
- TCP header



Features of TCP

- Reliable. Recipient must acknowledge receipt or message is assumed not delivered.
- Ordered. Header has sequence number in cases messages get out of order in transit.
- Error checking. A checksum is used to detect errors in transmission.
- Header includes source port and destination port.
  - Destination port tells recipient OS how to route message. Destination service is listening on destination port.
  - Source port tells destination how to respond.
- Both destination and source ports can be modified in transit.

Discussion questions

1. Is it possible to use TCP on an internet layer protocol other than IP?
2. How long does the sender wait for an acknowledgement (usually)?

Outline

- Introduction
- IP addresses
- DNS
- Ports
- Bridged and NAT networks
- TCP
- **Structuring your network**

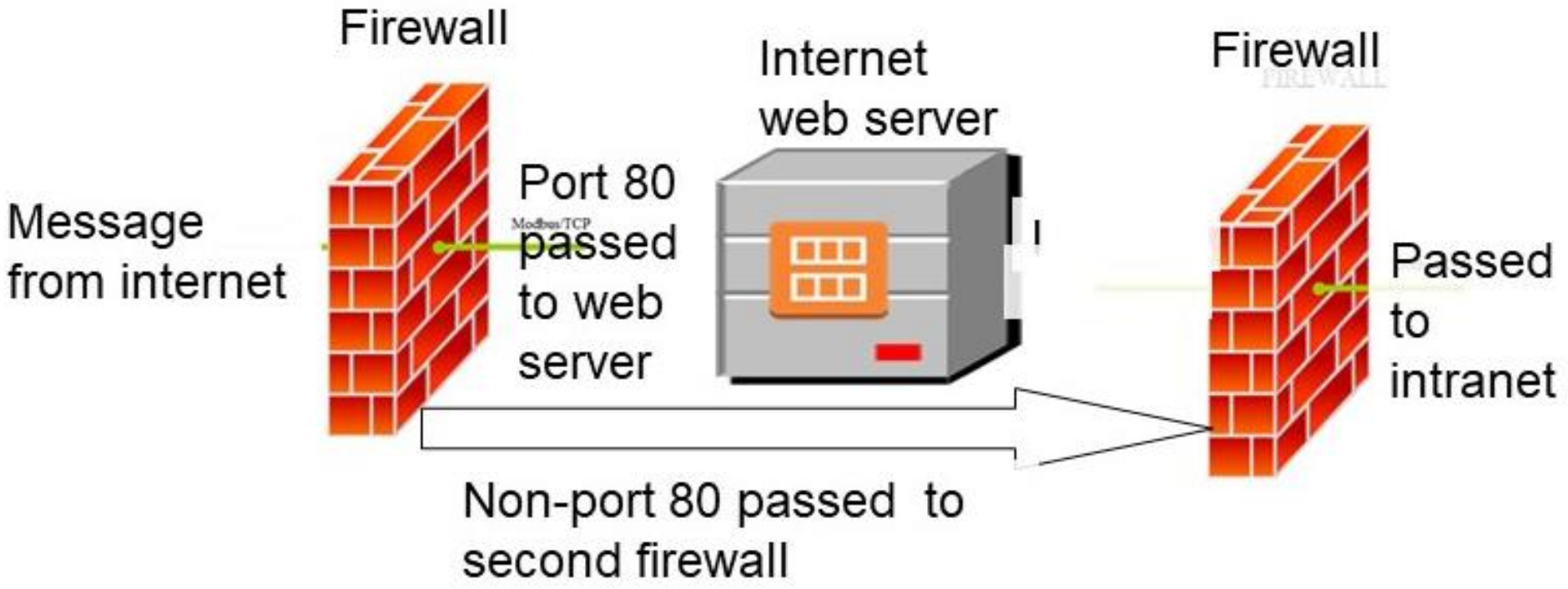
Subnets

- A subnet is a group of devices that are connected directly to each other. Messages between devices on a subnet do not pass through an IP router.
- A subnet is created within an address space by making the first portion of the IP address (the *subnet prefix*) the same for all the devices in the subnet. The remaining portion of the IP address will identify which device in the subnet a message is sent to.
- Reasons for creating a subnet
  - network performance. A subnet simplifies the work of a router.
  - security. A firewall for the subnet can verify that accesses to the resources on that subnet are allowed.

Partitioning your network

- Firewalls are used to protect one portion of your network from another. E.g. financial systems might be on separate subnet to limit access from other internal systems.
- Firewalls are also used to create a “Demilitarized Zone (DMZ)”
- DMZs are used to allow internet access to some servers and not to your Intranet.
  - Web servers can be made externally visible.
  - VPN servers can be made externally visible

DMZ



DMZ has rules to route messages for certain ports to servers in the DMZ

Tunneling

- One server in the DMZ supports Virtual Private Network (VPN).
- VPN allows devices on the internet access to the intranet.
- You are working from home and wish to access your intranet.
- You log in to the VPN server and it verifies your credentials by passing them to the authentication server in the intranet.
- Subsequent messages are sent using a tunneling protocol

Tunneling protocol

- A tunneling protocol encrypts your entire message, including the IP header that you created for the message, and puts it into the payload portion of a TCP message.
- The TCP messages is routed to the VPN server.
- The VPN server removes the TCP payload and decrypts your message, including the IP header that you created
- The message is then sent to the intranet.
  - If your destination IP address is a device within your organization, the message is delivered over your organization's intranet.
  - If your destination IP address is outside your organization, your message will be sent out to the internet through your organization's NAT and firewall.

Discussion questions

1. Create (or find) a map of your organization's intranet. How many firewalls are there? What subnets are protected by the firewalls?
2. In addition to routing rules based on port number, what other rules are there in an internet facing firewall?