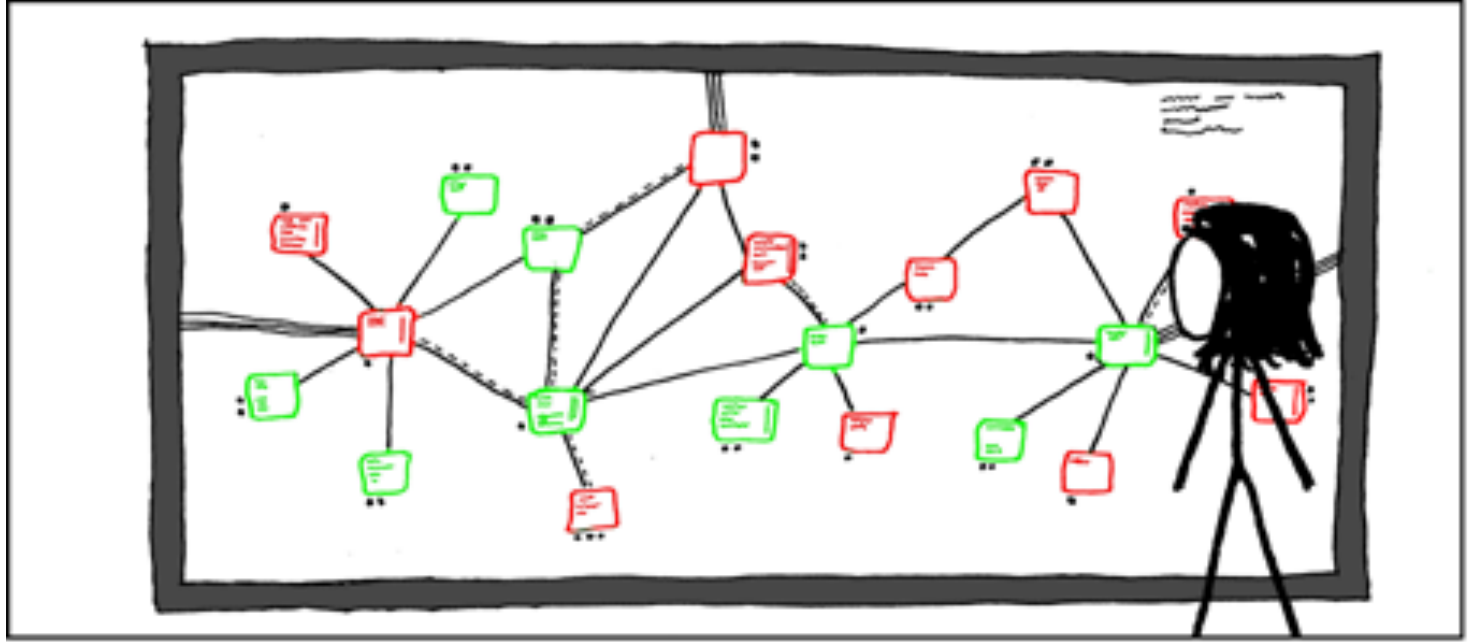
Fundamentals of Computer Networking

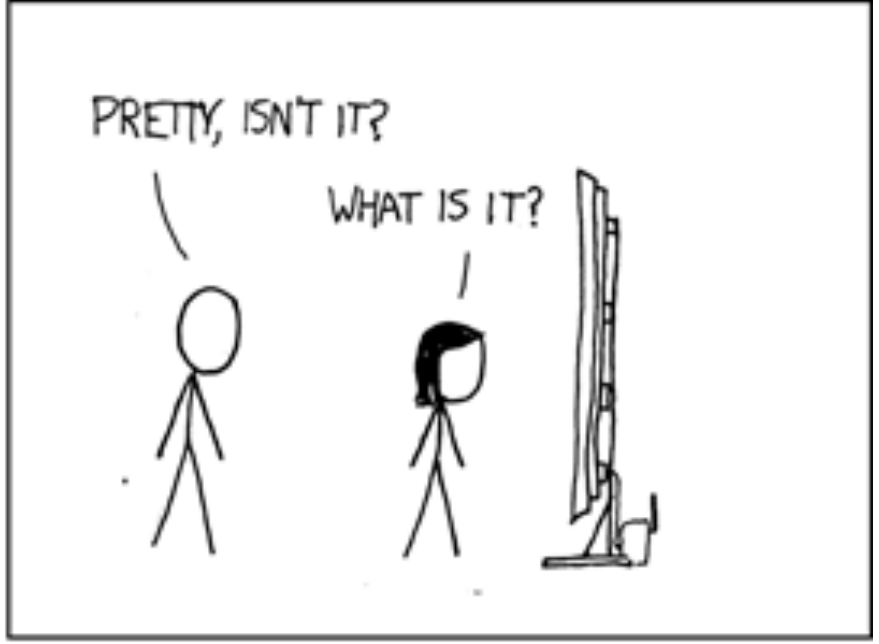
Tejas Parikh (t.parikh@northeastern.edu)

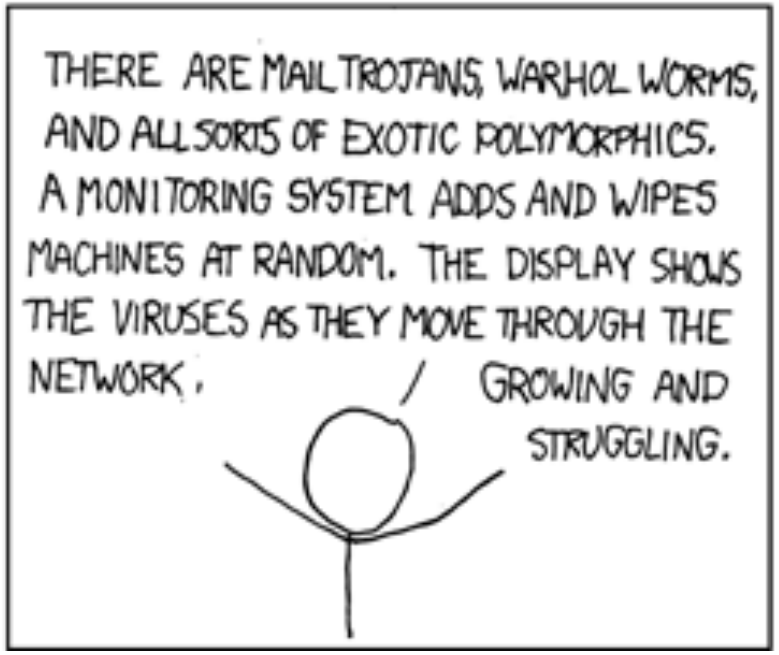
CSYE 6225

Spring 2020

Northeastern University







https://xkcd.com/350/

What is Network?

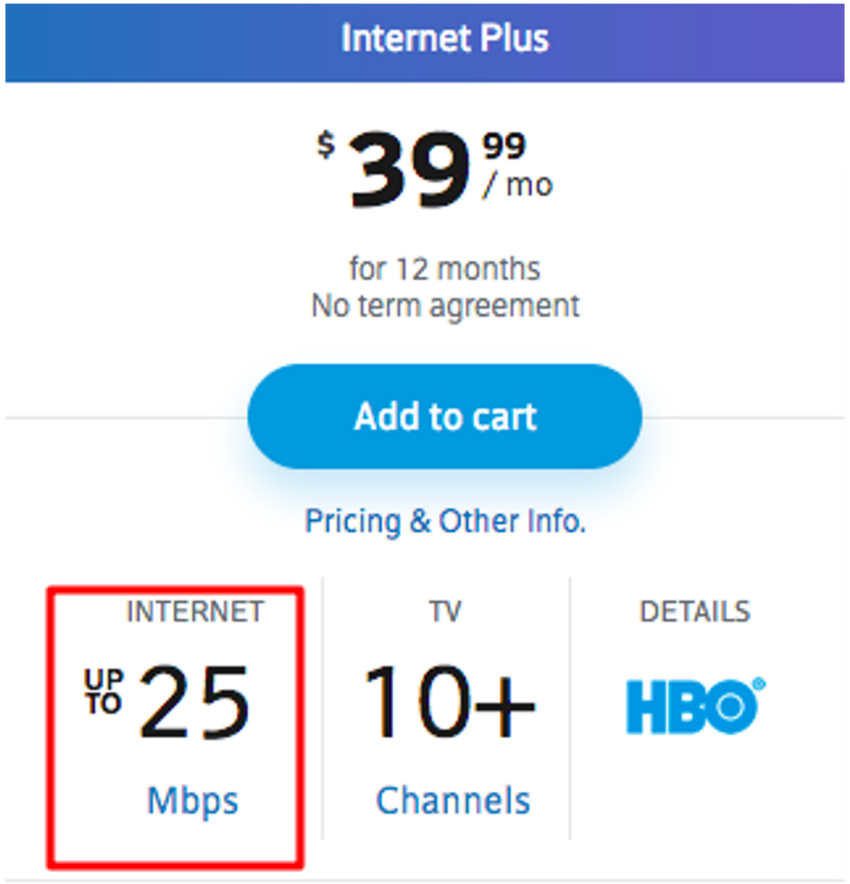
- A network is simply bunch of systems connected to each other via some kind of communication link.

- The common type of networks are:
  - LAN: Local Area Network
  - WAN: Wide Area Network

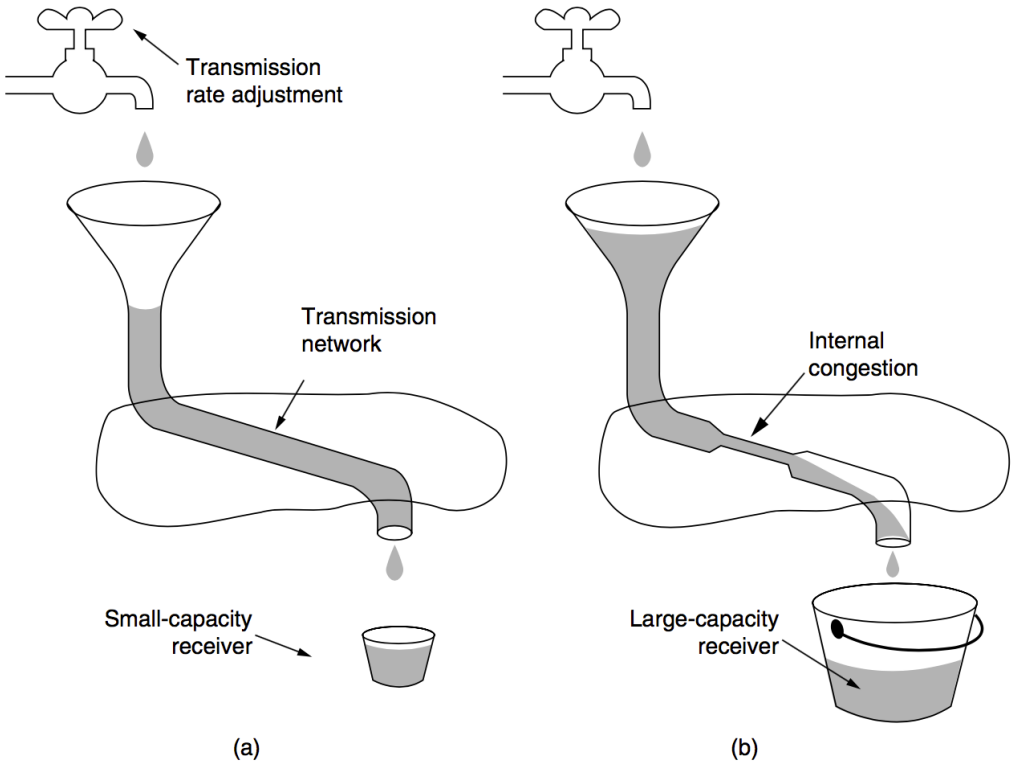
- The main difference between LAN and WAN is that LAN is usually confined to local geographic area where as WAN is spread across a larger geographic area. WAN is usually made of multiple LANs.
- Systems are not connected directly to each other. Instead they are indirectly connected to each other via a switch or router.

Communication Link

- Systems are connected to each other via communication link such as coaxial, copper or fiber cable or radio waves.
- Different communication links can transmit data at different rates.
- Data transmission rate of a link is measured in bits/second.
- Note that we use bits/second and not bytes per second. 1 byte is 8 bits.



Bandwidth

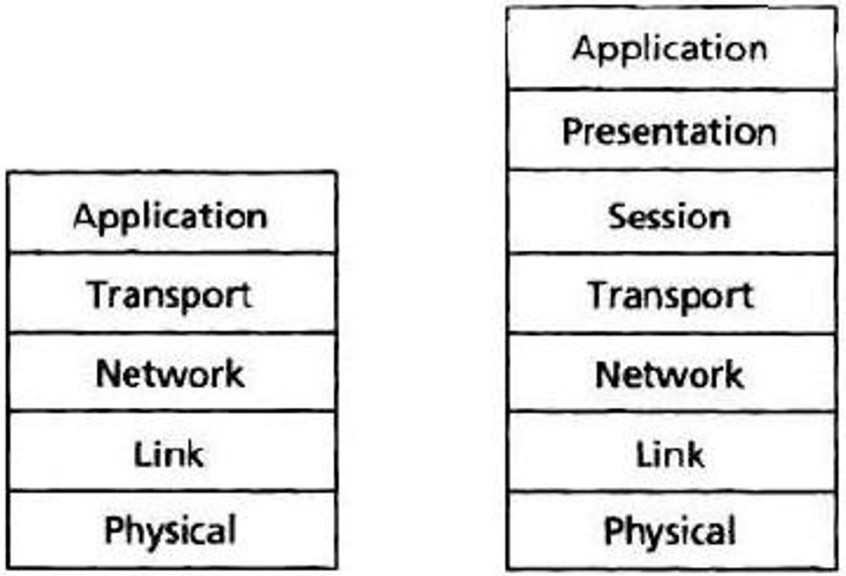


- In computing, **bandwidth** is the maximum rate of data transfer across a given path.

Network Protocols

Protocols define the format and order of messages exchanged between two or more communicating entities as well as the actions taken on transmission and/or receipt of a message or other event.

Network Protocol Stack & OSI Reference Model

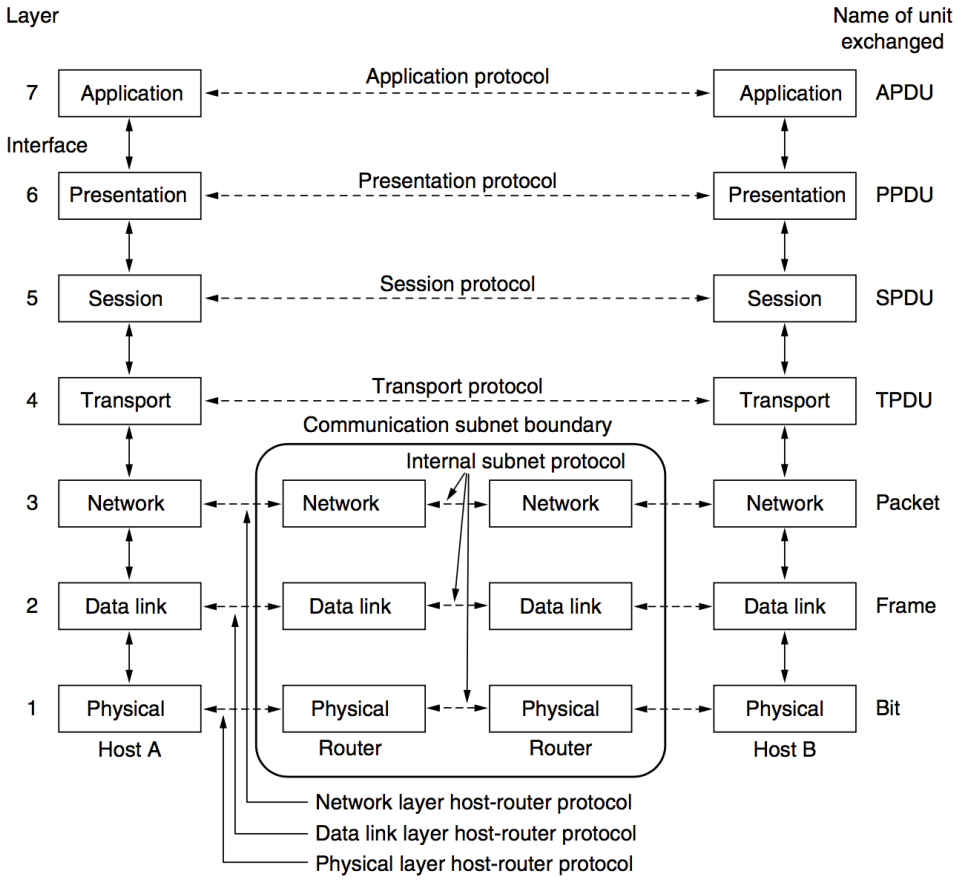


a. Five-layer Internet protocol stack

b. Seven-layer ISO OSI reference model

The Internet protocol stack (a) and OSI reference model (b)

The OSI Reference Model



Application Layer

This is the layer where network applications and application-layer protocols such as HTTP, FTP, etc. reside.

Transport Layer

- The transport layer transports application layer messages between client and server side of the application.
- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are examples of some popular transport layer protocols.

Network Layer

- The network layer is responsible for moving transport layer protocols from one host to another.
- The network layer defines the fields in data packet (datagram) as well as how the end systems and routers act on this field.
- If the data packet is too large, network layer might split it into multiple packets which will be combined into one at the receiving node.
- Most popular network layer protocol is the Internet Protocol (IP).

Link Layer

Link layer is responsible for moving packet from one node to the next node in the route.

Physical Layer

While the job of link layer is to move packets of data from one node to another, physical layer's job is to move the individual bits.

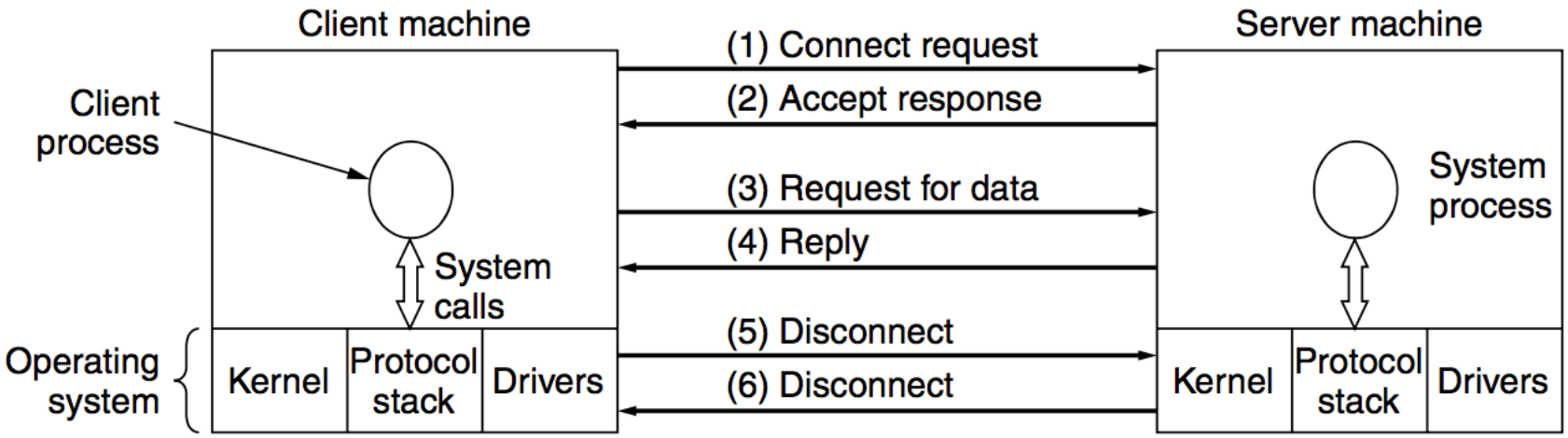
Presentation & Session Layer

- Session layer handles data related to particular user session.
- Presentation layer handles rendering of data. Example of presentation layer protocols are audio and video codes, different image formats such as PNG, JPEG, etc.

Transmission Control Protocol (TCP)

- Reliable Data Transfer - TCP ensures that data is delivered from sending process to receiving process correctly and in order.
- TCP is connection based - Sender will keep connection with receiver open until it is done successfully sending all the data packets.
- TCP does error checking and erroneous packets will be retransmitted from source to destination.
- TCP has congestion control. It will not send next chunk of data until it has received OK (ACK) from the receiver.
- Common application-layer protocol that use TCP/IP are HTTP, FTP, SMTP, etc.

A simple client-server interaction using acknowledged datagrams.



User Datagram Protocol (UDP)

- UDP protocol is designed to do as little work as possible to send data.
- UDP has no congestion control. Data is transmitted as soon as it can.
- UDP has no reliability guarantee. It does not care if the message was successfully received.
- UDP has not overhead of connection establishment.
- No connection state is maintained as we are not tracking successful delivery of data or the order in which data is sent.
- Common application-layer protocols that use UDP are Domain Name Systems (DNS), Dynamic Host Configuration Protocol (DHCP)

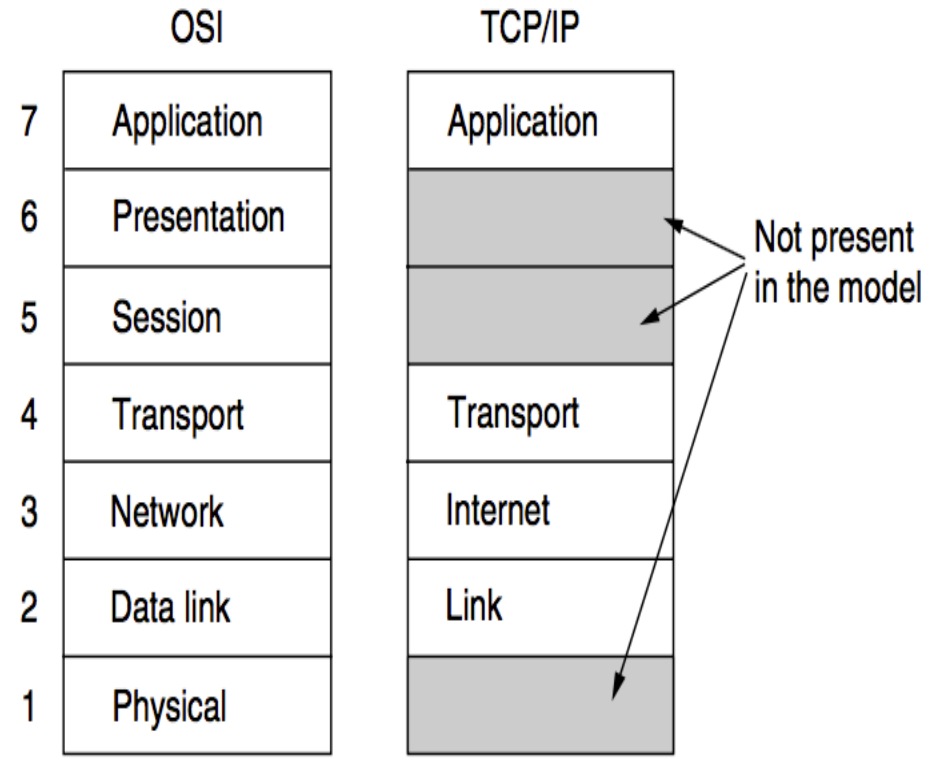
TCP

UDP

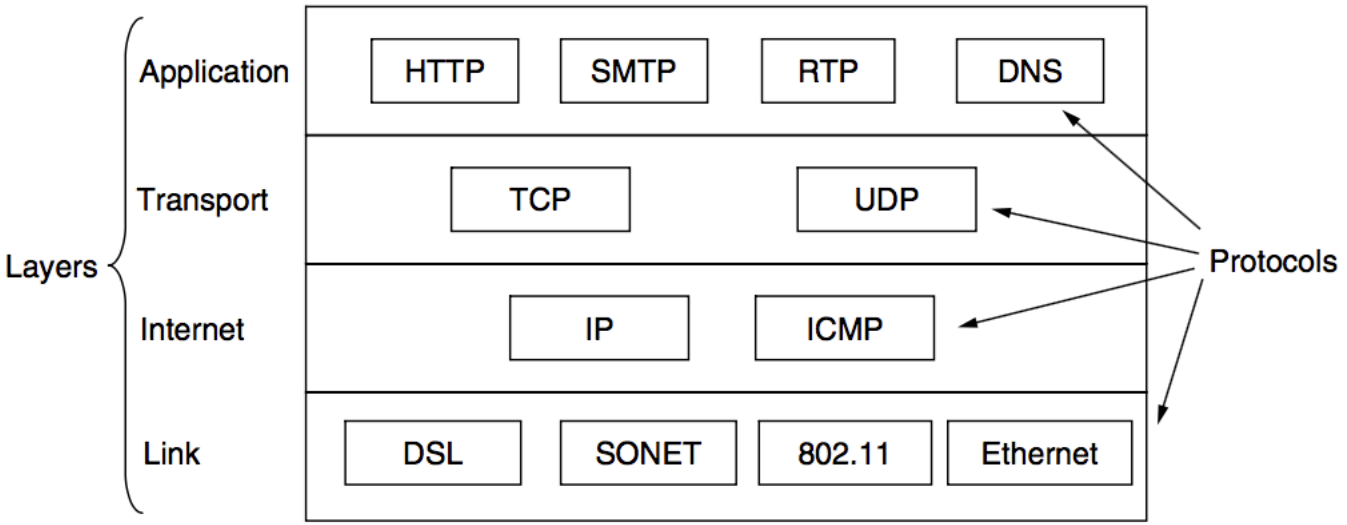
Internet Protocol (IP)

- The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
- IP is best-effort delivery service, makes no guarantee about delivering correct data, the order in which it is delivered or avoidance of delivering duplicate data pretty much like UDP.
- First major version of IP is Internet Protocol Version 4 (IPv4) and it's successor is Internet Protocol Version 6 (IPv6).

The TCP/IP reference model



Various TC/IP Models with Protocols

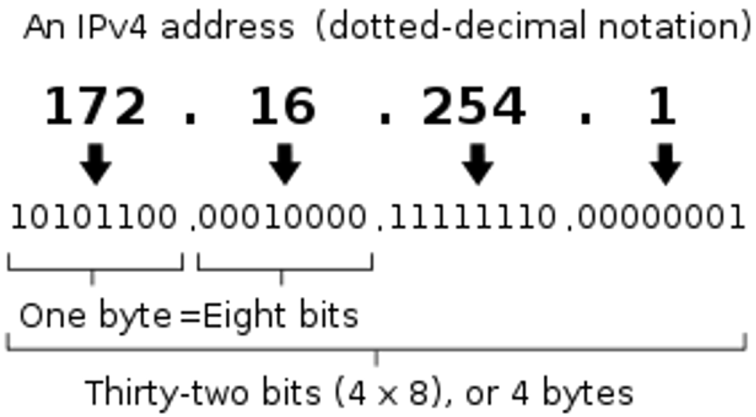


IPv4

- IPv4 uses 32 bit addressing system.
- IPv4 address space is 2^{32} which is approximately 4 billion IP addresses.
- Each system on network must have globally unique* IP address.

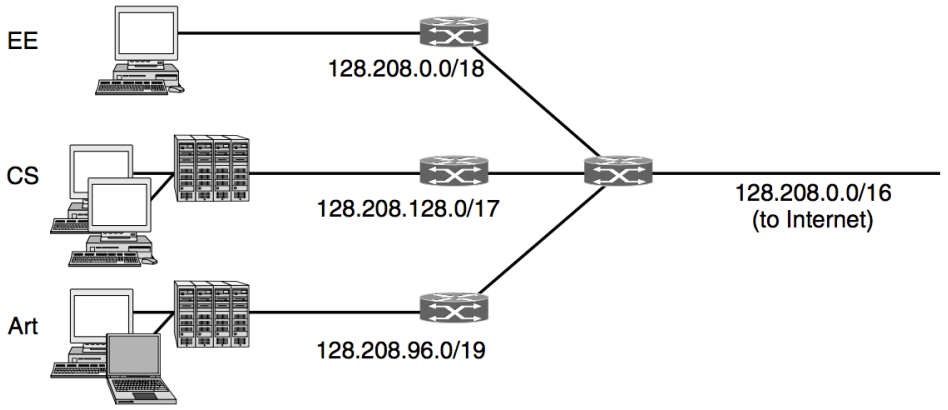
IPv4 Address Representation

IPv4 address is usually written in its decimal form and is separated by period (dot) from other bytes.



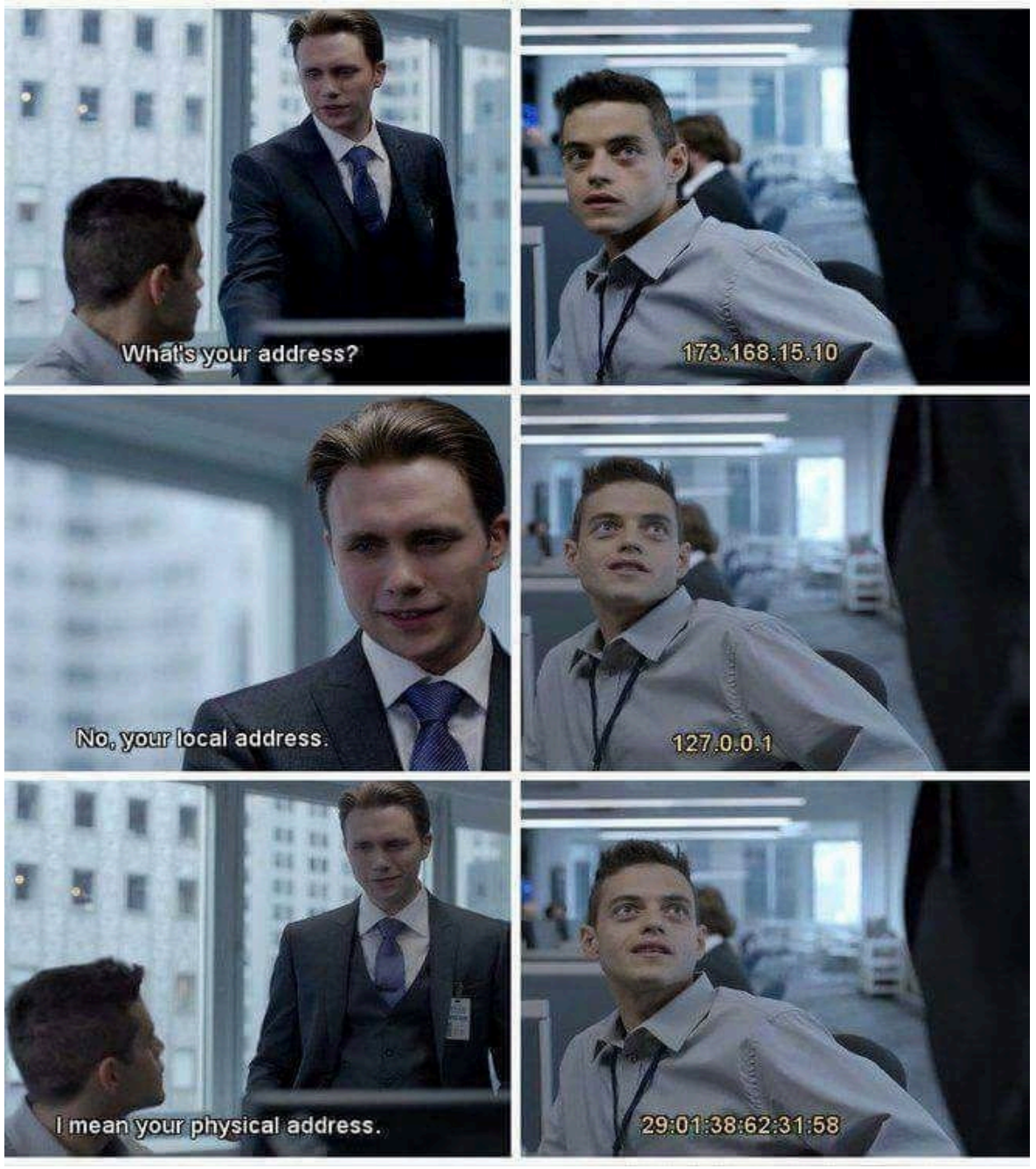
Subnet

- A subnet is isolated network.
- IP addresses are assigned to subnet with a subnet mask.
- Subnets are usually represented using CIDR notation that is written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix.
- For example, 192.168.1.0/24 is the prefix of the IPv4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing.



IPv4 Address Exhaustion

- IPv4 addresses have been exhausted since 2011.
- While IPv4 has approximately 4 billion IP addresses, not all of them are available for use. About ~18 million addresses are allocated for private network and ~270 million addresses for multicast addresses.

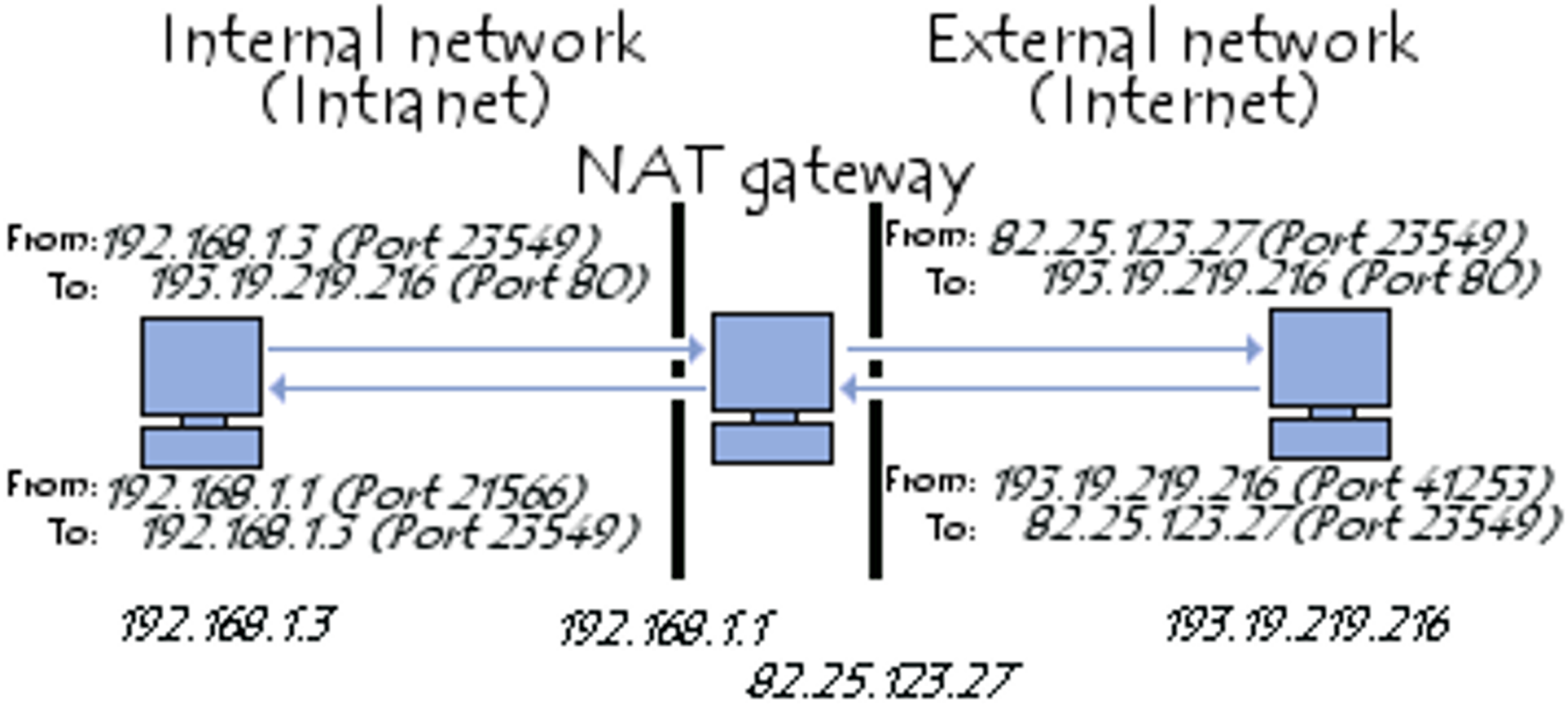

What's your address?
173.168.15.10
No, your local address.
127.0.0.1
I mean your physical address.
29:01:38:62:31:58


There's no place
like 127.0.0.1

Network Address Translation (NAT)

- NAT allows sharing of one Internet-routable IP address of a NAT gateway for an entire private network.
- NAT allows ISPs to support more systems with the limited availability of public IPs.
- Internet of Things (IoT) has significantly increased number of systems connected to internet.
- IPv6 adoption has been slow and older devices, systems and applications don’t support it.
- NAT does not work very well with Peer-to-peer (P2P) routing as P2P usually requires 2 hosts to be able to communicate with each other directly.

NAT Table Example

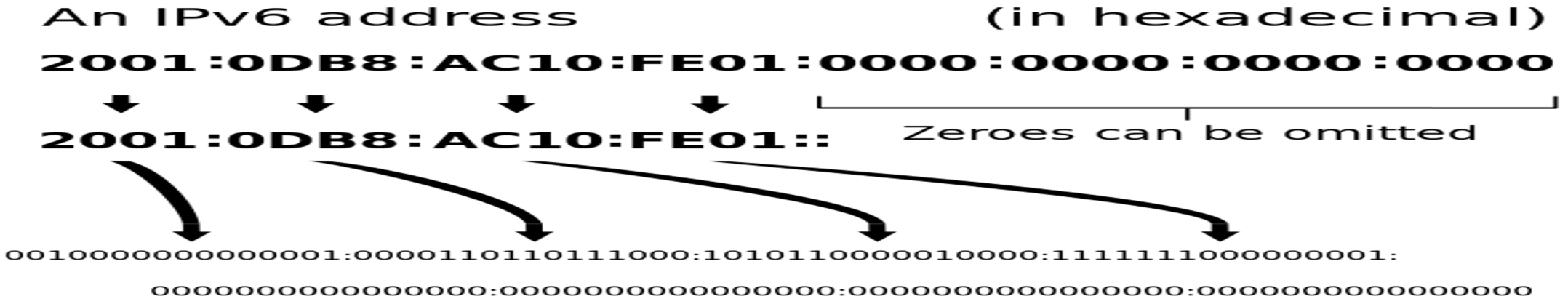


Internet Protocol version 6 (IPv6)

- Most recent version of Internet Protocol.
- IPv6 uses 128 bit addressing system theoretically allowing 2^{128} addresses.
- IPv6 does not support NAT.

IPv6 Address Representation

IPv6 addresses are represented as eight groups of four hexadecimal digits with the groups being separated by colons (:), for example 2001:0db8:0000:0042:0000:8a2e:0370:7334



Virtual Private Cloud & Its Components

Virtual Private Cloud (VPC)

- Virtual Private Cloud (VPC) allows you to launch resources into a virtual network you have defined.
- A VPC is a virtual network that belongs to you and is logically isolated from virtual networks that belong to other users.
- The default VPC on both AWS and GCP will include an internet gateway.
- An internet gateway enables your instances to connect to the internet.

Virtual Private Cloud (VPC) contd.

A VPC allows you to create or configure following:

- firewall
- routing table
- public or private subnets
- network gateway

Elastic Network Interfaces

An elastic network interface (referred to as a network interface in this documentation) is a virtual network interface that can include the following attributes:

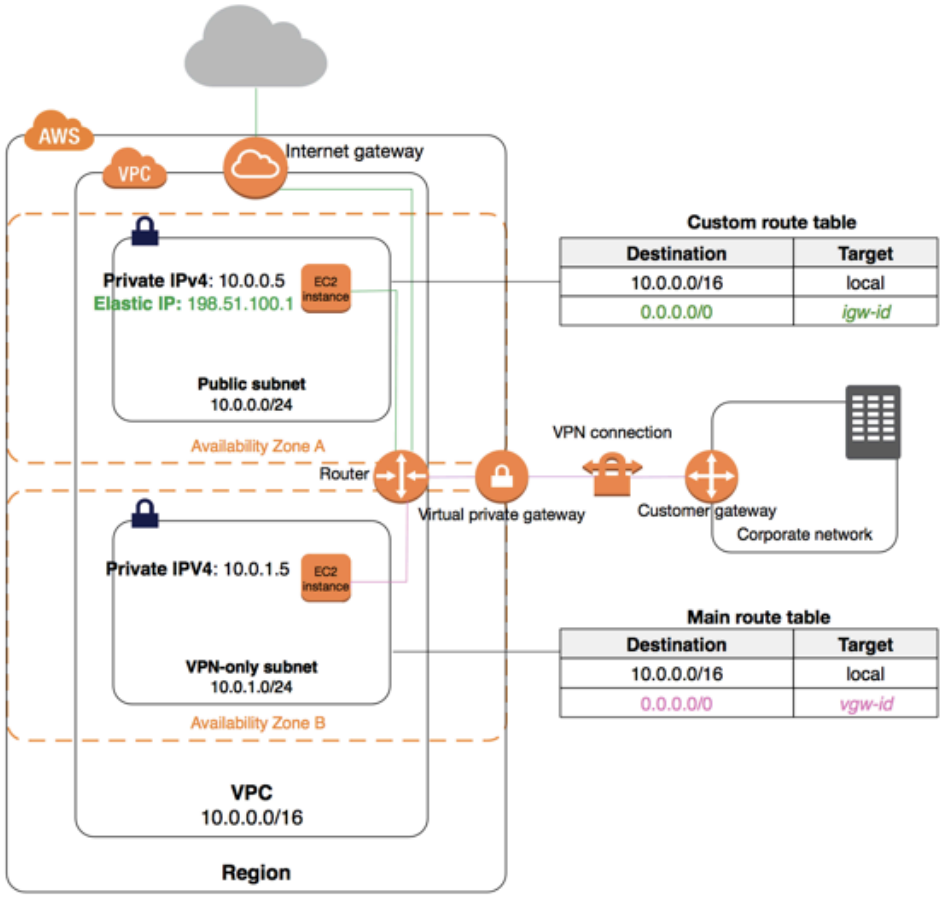
1. a primary private IPv4 address
2. one or more secondary private IPv4 addresses
3. one Elastic IP address per private IPv4 address
4. one public IPv4 address, which can be auto-assigned to the network interface for eth0 when you launch an instance
5. one or more IPv6 addresses
6. one or more security groups
7. a MAC address source/destination check flag
8. a description

Elastic Network Interfaces contd.

- You can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
- A network interface's attributes follow it as it is attached or detached from an instance and reattached to another instance.
- When you move a network interface from one instance to another, network traffic is redirected to the new instance.
- Each instance in your VPC has a default network interface (the primary network interface) that is assigned a private IPv4 address from the IPv4 address range of your VPC.
- You cannot detach a primary network interface from an instance.
- You can create and attach an additional network interface to any instance in your VPC. The number of network interfaces you can attach varies by instance type.

Route Tables

- A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.
- Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet.
- A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.



Route Table contd.

Destination	Target
10.0.0.0/16	Local
172.31.0.0/16	pcx-1a2b1a2b
0.0.0.0/0	igw-11aa22bb

- Any traffic from the subnet that's destined for the 172.31.0.0/16 IP address range uses the peering connection, because this route is more specific than the route for Internet gateway.
- Any traffic destined for a target within the VPC (10.0.0.0/16) is covered by the Local route, and therefore routed within the VPC.
- All other traffic from the subnet uses the Internet gateway.

Internet Gateways

- An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet.
- It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- An Internet gateway serves two purposes:
  - to provide a target in your VPC route tables for Internet-routable traffic, and
  - to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.
- An Internet gateway supports IPv4 and IPv6 traffic.

Elastic IP Addresses

- An Elastic IP address is a static, public IPv4 address designed for dynamic cloud computing.
- You can associate an Elastic IP address with any instance or network interface for any VPC in your account.
- With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.
- AWS does not support Elastic IP addresses for IPv6.

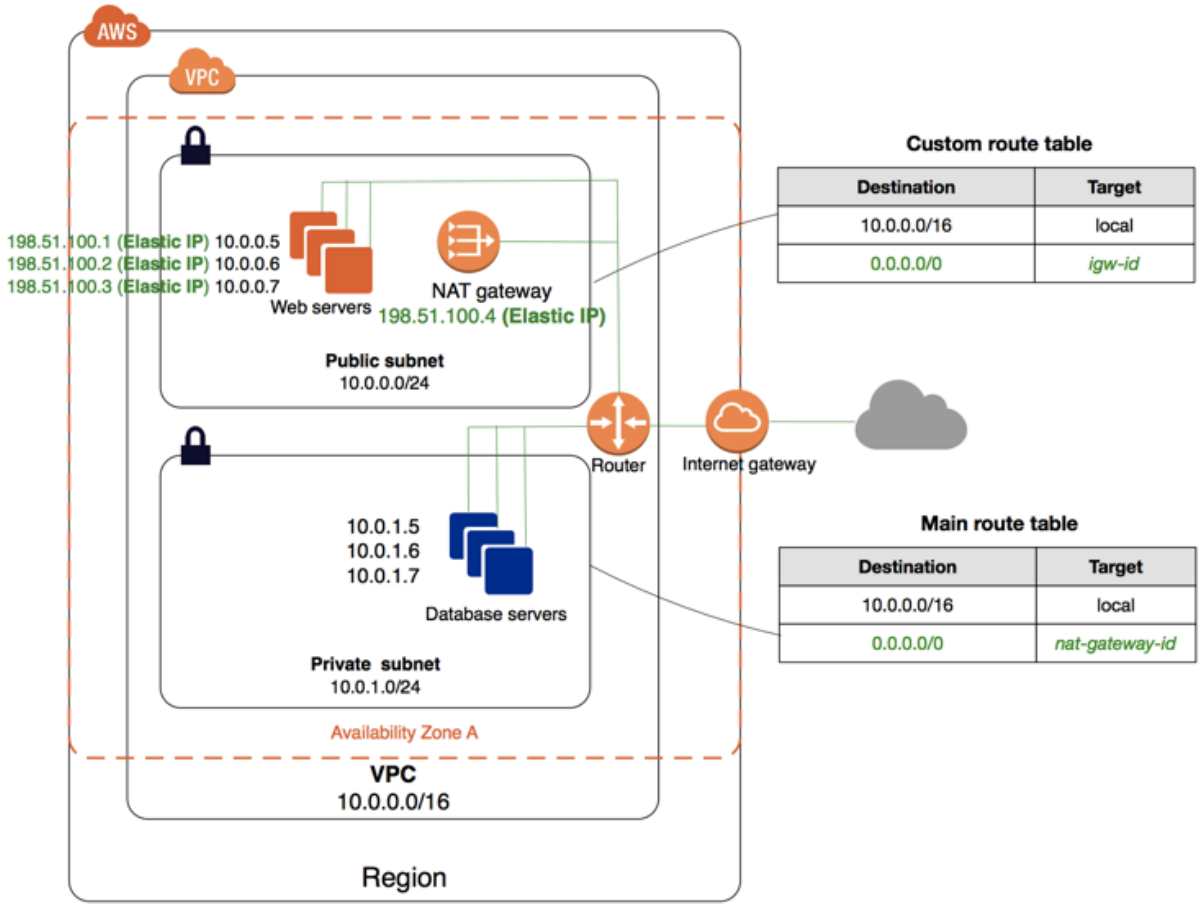
Security Groups

- A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.
- When you launch an instance in a VPC, you can assign up to five security groups to the instance.
- Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.
- For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

Security Groups Example

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
::/0	TCP	80	Allow inbound HTTP access from all IPv6 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
::/0	TCP	443	Allow inbound HTTPS access from all IPv6 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the Internet gateway)
Your network's public IPv4 address range	TCP	3389	Allow inbound RDP access to Windows instances from IPv4 IP addresses in your network (over the Internet gateway)
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
The ID of the security group for your database servers	TCP	1433	Allow outbound Microsoft SQL Server access to instances in the specified security group
The ID of the security group for your MySQL database servers	TCP	3306	Allow outbound MySQL access to instances in the specified security group

VPC with Public and Private Subnets



Additional Resources

https://csye6225.cloud/