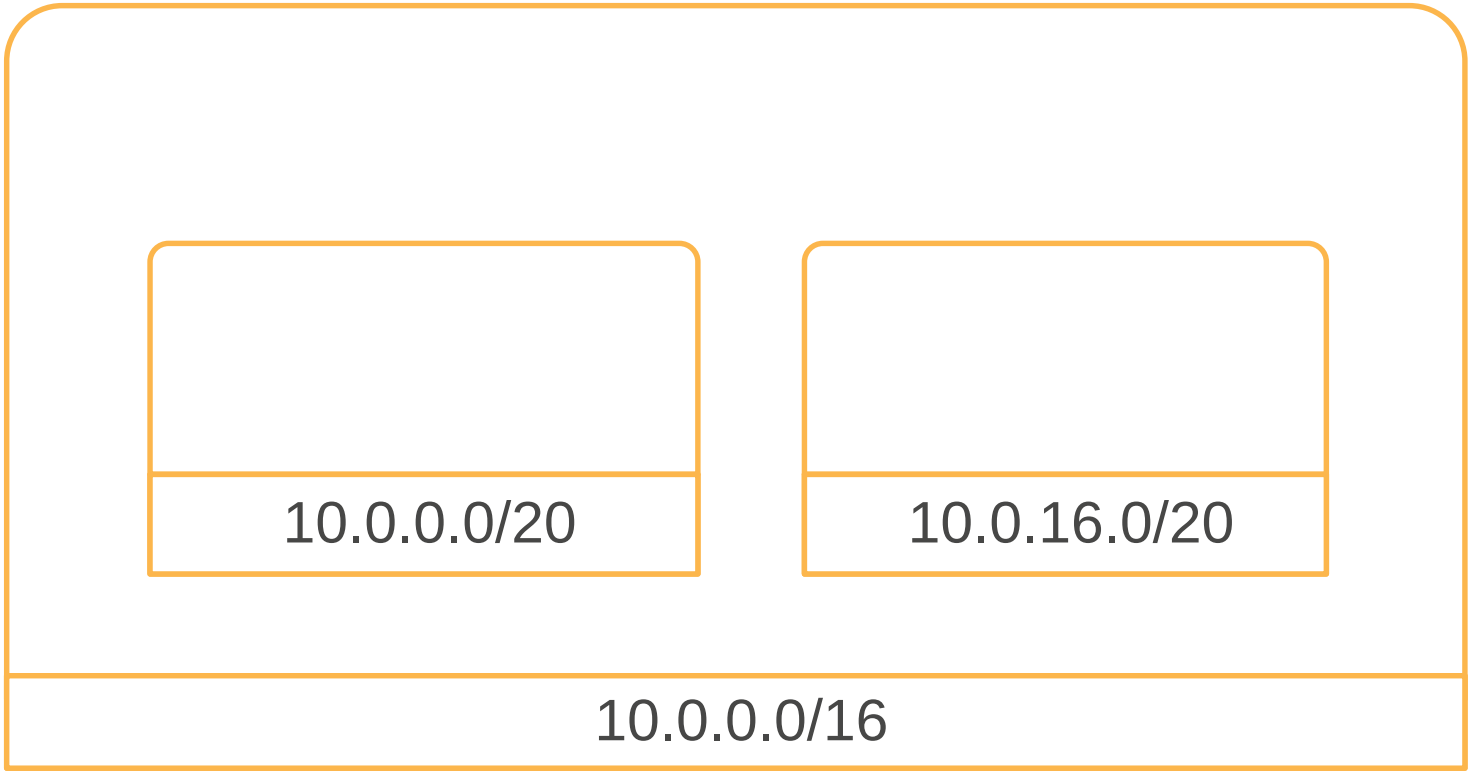
Network Primer

Network and Subnet Addressing

Content Prepared By: Chandra Lingam, Cotton Cola Designs LLC

amazon web services

Network and Subnet Addressing



What do these numbers mean?

IPv4 Addressing

2^{32} theoretical addresses. ~4.29 Billion addresses

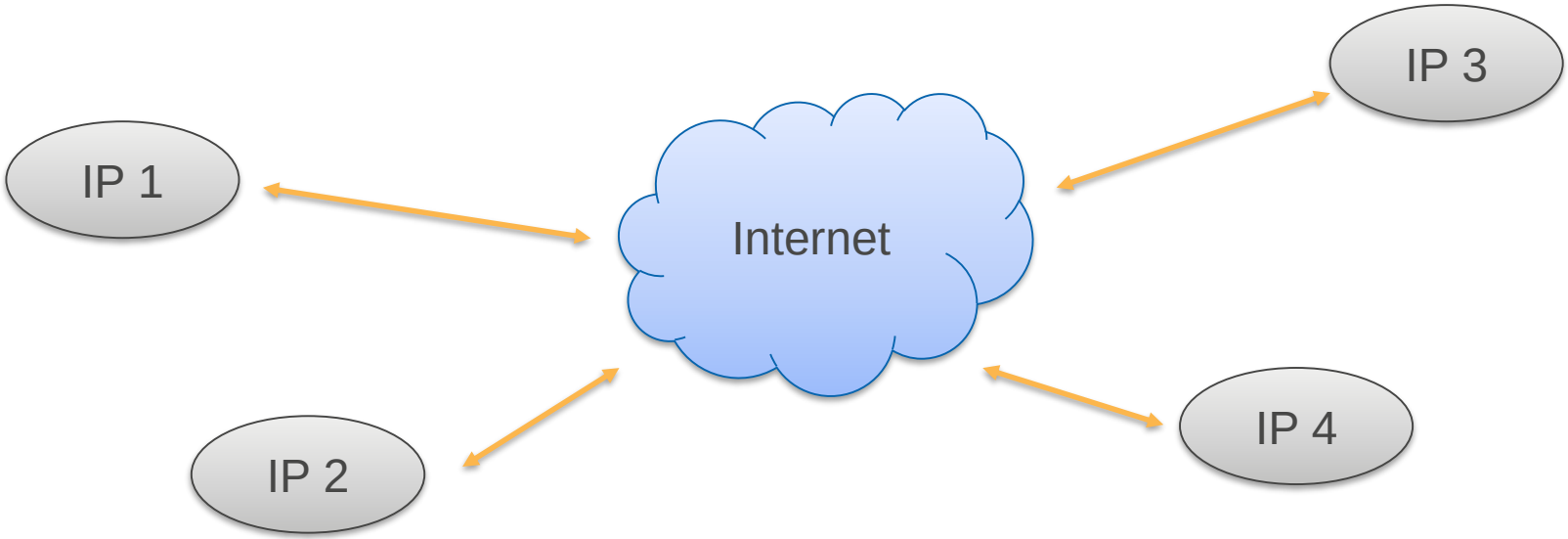
```
IP address: 216.239.32.21
Bits: 11011000.11101111.00100000.00010101
```

Out of 4.29B addresses, some are reserved: all 0s and 1s, private address, broadcast and so forth

Remaining Addresses are known as Public IP Addresses (~4B)

Public IP Addresses

- Globally unique and reachable from anywhere
- How to route the packets?



Routing

IP Address divided into two parts

- First part identifies the destination network
- Second part identifies a machine inside that network

Routing is simpler now. Packet is delivered to a destination network. Organization that owns the destination network is responsible for internally routing/delivering to machine

Three classes of network were defined as per Internet Protocol RFC791: Class A, B and C

Class A Network

Most Significant Bit is 0 and followed by 7 bits to identify the network. Remaining 24 bits identify machine

```
IP:  97.239.32.21

01100001.11101111.00100000.00010101
```

127 possible Class A networks

16.8 Million possible hosts connected to each network

Class B Network

Two Most Significant Bits are 1,0 and followed by 14 bits to identify the network. Remaining 16 bits identify machine

```
IP:   161.239.32.21
10100001.11101111.00100000.00010101
```

16 K possible Class B Networks (2^14)

65 K possible Hosts connected to each network

Class C Network

Three Most Significant Bits are 1,1,0 and followed by 21 bits to identify the network. Remaining 8 bits identify machine

```
IP:   193.239.32.21
11000001.11101111.00100000.00010101
```

2 Million possible Class C Networks (2^21)

256 Hosts connected to each network

Issues

- Class A – Too big with millions of hosts. Suitable for large ISPs
- Class C – Too few hosts supported
- Class B – Most in demand even when organizations had only couple of thousand computers. Rapid exhaustion of Class B addresses and wastage of address space
- Multiple Blocks of Class C – to meet organization needs. This caused multiple entries in routing table for the same destination.

Classless Inter Domain Routing (CIDR)

- Classless Inter-domain Routing (CIDR) was introduced to bring more flexibility to addressing scheme and to conserve IPv4 address space
- Number of bits used to identify network is explicitly stated with /<number> notation
- Address is allocated based on organization's actual need
- AWS uses CIDR blocks for VPC
- IPv6 Addresses these issues in a more comprehensive way

CIDR Example

201.239.0.0/16 (MSB 16 bits identify network)

11001001.11101111.00000000.00000000

193.239.32.0/20 (MSB 20 bits identify network)

11000001.11101111.00100000.00000000

193.239.32.115/32 – Identifies a specific host

Subnet

Network can be sub-divided into subnets inside an organization

Aides in manageability, security, isolation and so forth

CIDR block convention to identify subnets

Subnet Example

193.239.32.0/20 network is sub-divided into 4 subnets.
Additional 2 bits are needed to indicate the subnets.

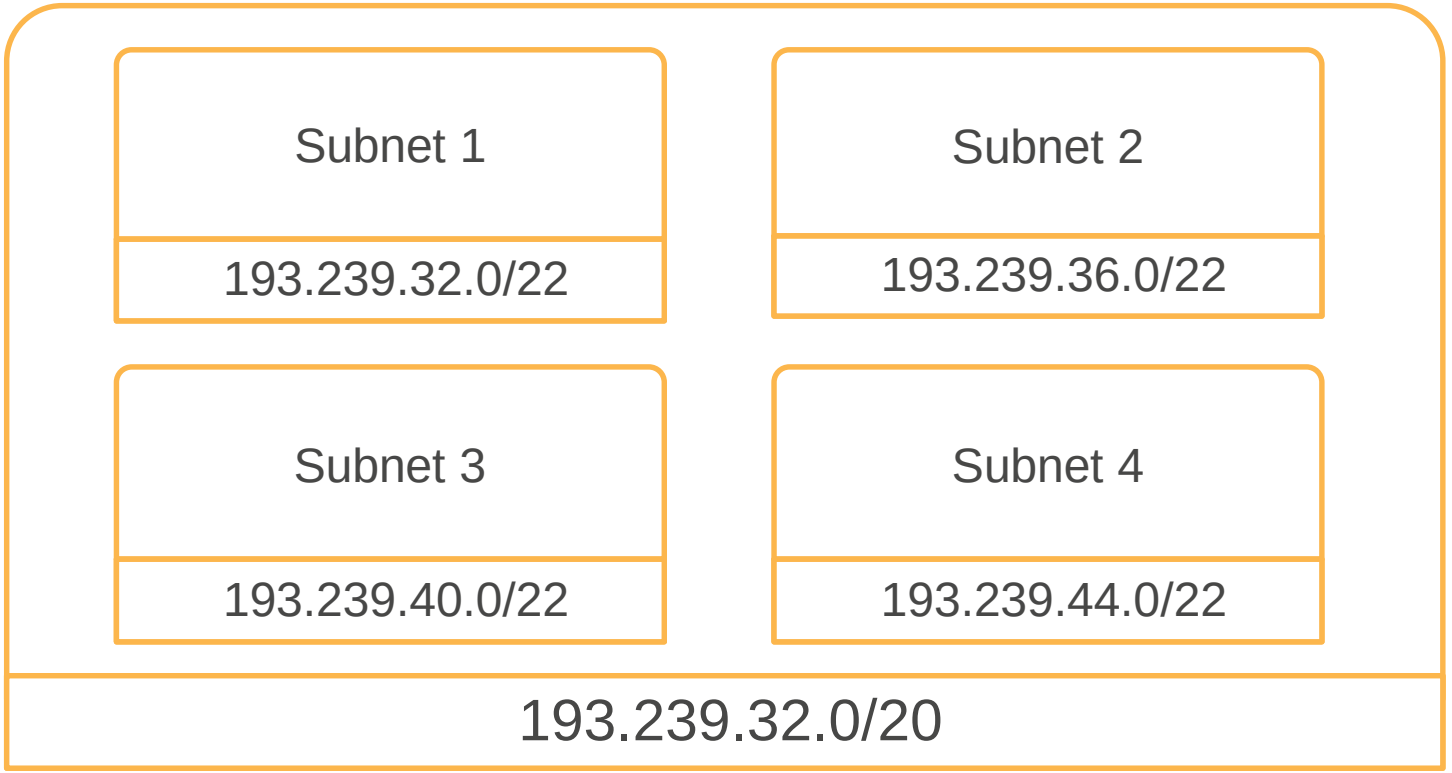
Network CIDR: 193.239.32.0/20

Subnet CIDR: 193.239.32.0/22

```
193.239.32.0/22   11000001.11101111.001000000.00000000
193.239.36.0/22   11000001.11101111.001001000.00000000
193.239.40.0/22   11000001.11101111.001010000.00000000
193.239.44.0/22   11000001.11101111.001011000.00000000
```

1,019 hosts in each subnet (1024 – 5)

Subnet Example



VPC requires you to specify network CIDR and subnet CIDR

Private Address Space

- Private address is a reserved space (RFC1918)
- Organization is free to use this space for its own internal private network
- These addresses cannot be used for public address
- Reserved Spaces are:
  - 10.0.0.0 - 10.255.255.255 (10.0.0.0/8 prefix)
  - 172.16.0.0 - 172.31.255.255 (172.16.0.0/12 prefix)
  - 192.168.0.0 - 192.168.255.255 (192.168.0.0/16 prefix)
- AWS VPC uses Private Address Blocks for Network and Subnet CIDR

NetMask

- Network Mask is useful to find out if a particular IP address is part of a network
- Network Mask is an IPv4 pattern with all MSB network identifier bits set to 1 and remaining bits set to 0
- For example in a /20 network, Mask is made up of first 20 bits set to 1 and remaining bits set to 0

```
Network:      193.239.32.0/20
Network Mask: 255.255.240.0
11111111 . 11111111 . 11110000 . 00000000
```

NetMask Example 1

Network: `193.239.32.0/20`

NetMask: `255.255.240.0`

A machine in the above network needs to send a packet to destination IP `193.239.35.210`. Is the destination machine part of same network or a different network?

IP:	`193.239.35.210`	`11000001.11101111.00100011.11010010`
Mask:	`255.255.240.0`	`11111111.11111111.11110000.00000000`
Bitwise AND		`11000001.11101111.00100000.00000000`
Result:		`193.239.32.0`

Destination machine is in the same network!

NetMask Example 2

Network: `193.239.32.0/20`

NetMask: `255.255.240.0`

A machine in the above network needs to send a packet to destination IP `193.239.52.210`. Is the destination part of same network or a different network?

IP:	`193.239.52.210`	`11000001.11101111.00110100.11010010`
Mask:	`255.255.240.0`	`11111111.11111111.11110000.00000000`
Bitwise AND		`11000001.11101111.00110000.00000000`
Result:		`193.239.48.0`

Destination machine is NOT in the same network and needs to be routed to a different network

AWS VPC: IPv4 and IPv6 Comparison

Table: IPv4 and IPv6 comparison