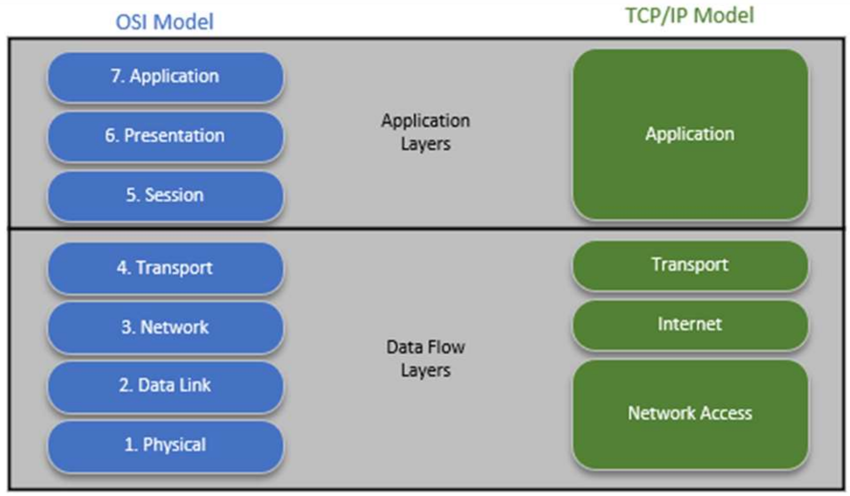
SecureSet and Flatiron School have joined forces with a mission of enabling people to pursue careers they love.

We are tackling the cyber skills gap together, using our collective strengths to provide transformative cybersecurity education.

Networking 100

IPv4 and IPv6

REVIEW: OSI AND TCP/IP MODELS



OSI LAYER 1 - PHYSICAL LAYER

The “Physics” layer

Concerned with transmission medium

- Wires (Copper Cables), Light (Fiber), Electromagnetic waves (WiFi)
- Encoding, light modulation

Information Labeled as: **Bits**

OSI LAYER 2 - DATA LINK LAYER

Transfer of data between nodes on same LAN segment

Provides error detection

Sub-layers

- Logical Link control (LLC)
- Media Access Control (MAC)

Addressing via “MAC Address”

Information Labeled as: **Frames**

TCP/IP NETWORK INTERFACE LAYER

TCP/IP layer the encompasses OSI layers 1&2

Focused on delivering the IP Packets across a single network segment

Network Interface Layer Protocols also make use of headers, to include the information needed to deliver data from one point to another

Information Labeled as: **Frame**

Note that both the OSI and TCP/IP models use the term Frame and they can be thought of as the same definition.

ARP & RARP

Address Resolution Protocol (ARP)

- Helps to bridge information between OSI Layer 3 and 2.
- “I know the IP address; I need to know the MAC address”
- More later - this is more interesting/useful/risky than it would seem at first

Reverse Address Resolution Protocol (RARP)

- Just like it sounds - “I know the MAC Address, what is the IP?”
- Obsolete protocol, but comes up occasionally in discussion

Internet Protocol Fundamentals

NETWORK LAYER ADDRESSING

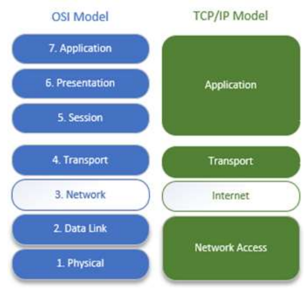
Routing

- Provides Network Layer Interaction with Data Link Layer
- Why is ARP important?

Layer 3 Addressing highlights

- Provides Logical Grouping and physical location
- Handles future expansion
- Unique address assignment / Dynamic?

Routing vs. Routed protocols



From: https://www.certificationkits.com/cisco-routing-protocols/#:~:text=A%20routed%20protocol%20is%20a,IP%2C%20IPX%2C%20and%20AppleTalk.&text=All%20hosts%20on%20an%20internetwork,is%20only%20used%20between%20routers.

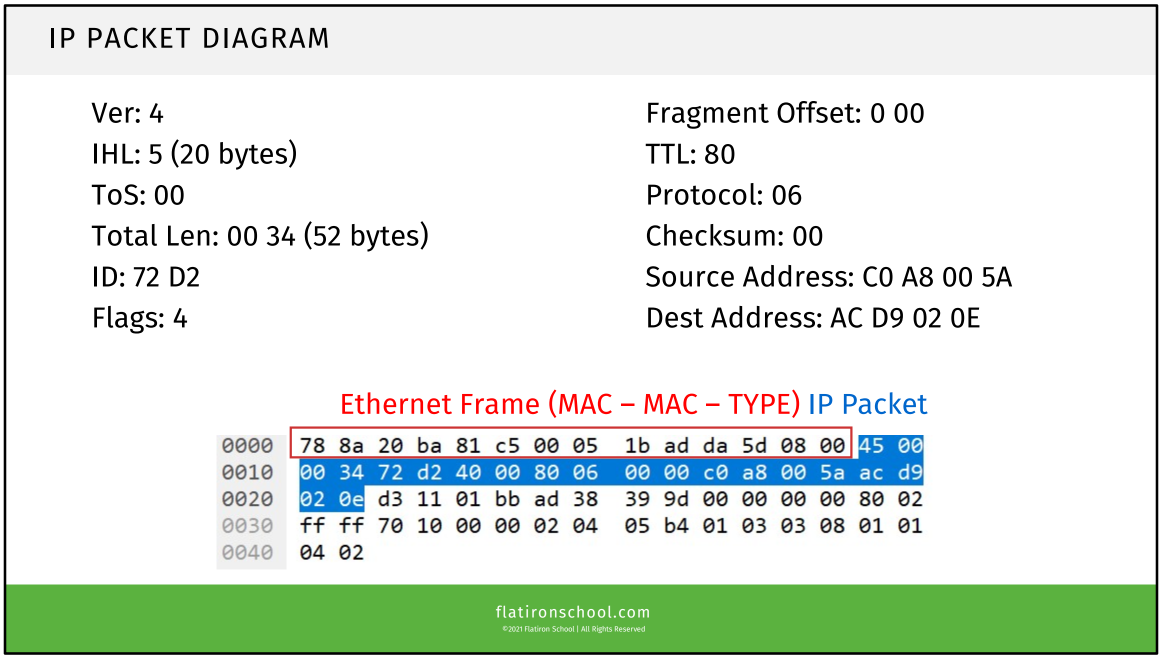
A routed protocol is a protocol by which data can be routed. Examples of a routed protocol are IP, IPX, and AppleTalk. Required in such a protocol is an addressing scheme. Based on the addressing scheme, you will be able to identify the network to which a host belongs, in addition to identifying that host on that network. All hosts on an internetwork (routers, servers, and workstations) can utilize the services of a routed protocol.
A routing protocol, on the other hand, is only used between routers. Its purpose is to help routers building and maintain routing tables. The only two routed protocols you should worry about are IP and IPX (although Cisco has dropped IPX from the latest CCNA exam, it is helpful to understand the concepts behind it).

IP PACKET STRUCTURE

4 bytes/octets

<table>
<tr><td>Ver</td><td>IHL</td><td>ToS</td><td colspan="2">Tot Len</td></tr>
<tr><td colspan="3">ID</td><td>Flags</td><td>Frgmt Offst</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">Hdr Chksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Option + Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

4*5 = 20 bytes



Destination MAC Address: 78-8a-20-ba-81-c5
Source MAC Address: 00-05-1b-ad-da-5d
EtherType: 08 00 (IPv4 See: [https://en.wikipedia. g/wiki/EtherType](https://en.wikipedia.org/wiki/EtherType))

Ver: 4 indicates IPv4. What would it be for IPv6?

Note: IHL is 5, which corresponds to 20 bytes (why?) Two hex characters is a byte. So, 45 00 00 34 72 d2 40 00 80 06 00 00 c0 a8 00 5a ac d9 02 0e is 20 bytes.

Total Length: 00 34 (52 bytes, IP header and IP payload)

ID: 72 D2 If there are multiple packets in this IP stream (fragmentation), then all related packets will have the same ID.

Flags: 4

Fragment Offset: 0 00

TTL: 80

Protocol: 06 (Indicates TCP, if this were a UDP packet it would be 17)

Checksum: 00

Source Address: C0 A8 00 5A (IP Address see subsequent slides)

Destination Address: AC D9 02 0E (IP Address see subsequent slides)

WHAT IS AN IP ADDRESS?

An IP address is a unique global address for a network interface

An IP address is a 32-bit long identifier

Encodes:

- a network number (network prefix)
- a host number

How many bytes is 32 bits? How many hex characters?

Remember a byte is 8 bits, so 32 bits is 4 bytes. A single byte can be represented by 2 hex characters.

IP ADDRESSES

Source: 192.168.0.90

```
0000  78 8a 20 ba 81 c5 00 05  1b ad da 5d 08 00 45 00
0010  00 34 72 d2 40 00 80 06  00 00 c0 a8 00 5a ac d9
0020  02 0e d3 11 01 bb ad 38  39 9d 00 00 00 00 80 02
0030  ff ff 70 10 00 00 02 04  05 b4 01 03 03 08 01 01
0040  04 02
```

Destination: 172.217.2.14

```
0000  78 8a 20 ba 81 c5 00 05  1b ad da 5d 08 00 45 00
0010  00 34 72 d2 40 00 80 06  00 00 c0 a8 00 5a ac d9
0020  02 0e d3 11 01 bb ad 38  39 9d 00 00 00 00 80 02
0030  ff ff 70 10 00 00 02 04  05 b4 01 03 03 08 01 01
0040  04 02
```


192 = 0xC0

168 = 0xA8

0 = 0x00

90 = 0x5A

172 = 0xAC

217 = 0xD9

2 = 0x02

14 = 0x0E

IP ADDRESSING FUNDAMENTALS (KEY TOPIC)

Definitions

- 32-bit number = 4 bytes = 4 octets = 4 dotted decimal values
- 1 IP address per IP Host's NIC / Router Interface

IP Grouping

- Address Prefix
- Same group?
- Share Intermediate Router?
- Same Location?

NETWORK CLASSES

IP Address: octet.octet.octet.octet

- Class A: network.host.host.host
- Class B: network.network.host.host
- Class C: network.network.network.host

2 reserved host addresses per network

- Network Number
- Network/Directed Broadcast
- The rest is valid IP range

IPv4 addressee were supposed to last until the end of time…no so much. Due to mismanagement and unexpected growth we have run out of IPv4 addresses, which allegedly occurred 24 Sept 2015. IPv4 provides for 232 (4,294,967,296) possible addresses or as some round up 4.3 Billion.

It is good to memorize the classes of addresses:
Class A: 0-126 (some will consider 127 to be part of class A as others will not due to 127 being reserved)
Class B: 128-191
Class C: 192-223
Class D: 224-251 (multicast traffic ie: routers)
Class E: 252-255 (reserved, not used)

DOTTED DECIMAL NOTATION

IP addresses are written in a dotted decimal notation

Each byte is identified by a decimal number in the range [0-255]

Example:

1100 0000	1010 1000	0110 0100	0000 0001
1st Byte	2nd Byte	3rd Byte	4th Byte
= 192	= 168	= 100	= 1

192.168.100.1

192 = 0xC0

168 = 0xA8

100 = 0x64

1 = 0x01

NETWORK PREFIX AND HOST NUMBER

The network prefix identifies a network, and the host number identifies a specific host (actually, interface) on the network.

network prefix	host number

How do we know how long the network prefix is?

- The network prefix used to be implicitly defined (class-based addressing, A,B,C,D...)
- The network prefix now is flexible and is indicated by a prefix/netmask (classless).

EXAMPLE

Example: IP address is 192.168.100.1

Is that enough info to route datagram??? -> No, need netmask or prefix at every IP device (host and router)

Using Prefix notation IP address is: 192.168.100.1/16

Network prefix is 16 bits long

11111111 11111111 00000000 00000000

Network mask is: 255.255.0.0 or hex format: ffff0000

-----> Network id (IP address AND Netmask) is: 192.168.0.0

-----> Host number (IP address AND inverse of Netmask) is: 100.1

192.168	100.1

Classful IP Addresses

THE OLD WAY: CLASSFUL IP ADRESSES

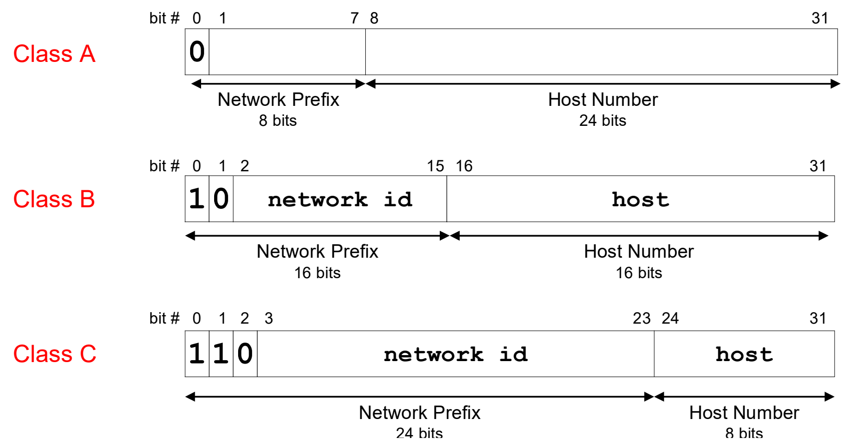
When Internet addresses were standardized (early 1980s), the Internet address space was divided up into classes:

- Class A: Network prefix is 8 bits long
- Class B: Network prefix is 16 bits long
- Class C: Network prefix is 24 bits long

Each IP address contained a key which identifies the class:

- Class A: IP address starts with “0”
- Class B: IP address starts with “10”
- Class C: IP address starts with “110”

THE OLD WAY: INTERNET ADDRESS CLASSES



THE OLD WAY: INTERNET ADDRESS CLASSES

We will learn about multicast addresses later in this course.

PROBLEMS WITH CLASSFUL IP ADDRESSES

The original classful address scheme had several problems

Problem 1. Too few network addresses for large networks

- Class A and Class B addresses are gone
- Fix #1: Subnetting

Problem 2. Two-layer hierarchy is not appropriate for large networks with Class A and Class B addresses.

- Fix #1: Subnetting

PROBLEMS WITH CLASSFUL IP ADDRESSES

Problem 3. Inflexible. Assume a company requires 2,000 addresses

- Class A and B addresses are overkill
- Class C address is insufficient (requires 8 Class C addresses)
- Fix #2: Classless Interdomain Routing (CIDR)

Problem 4: Exploding Routing Tables:

Routing on the backbone Internet needs to have an entry for each network address.

In 1993, the size of the routing tables started to outgrow the capacity of routers.

Fix #2: Classless Interdomain Routing (CIDR)

PROBLEMS WITH CLASSFUL IP ADDRESSES

Problem 5. The Internet is going to outgrow the 32-bit addresses

Fix #3: IP Version 6

flatironschool.com

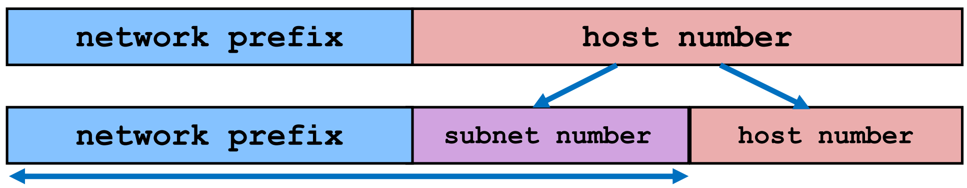
When we say we have outgrown the IPv4 space, we are truly on borrowed time. Subnetting is a stopgap that has allowed us to continue (along with NAT and other technologies we will study later), but we are squeezing an ever shrinking space.

Subnetting & CIDR

BASIC IDEA OF SUBNETTING

Split the host number portion of an IP address into a subnet number and a (smaller) host number

Result is a 3-layer hierarchy

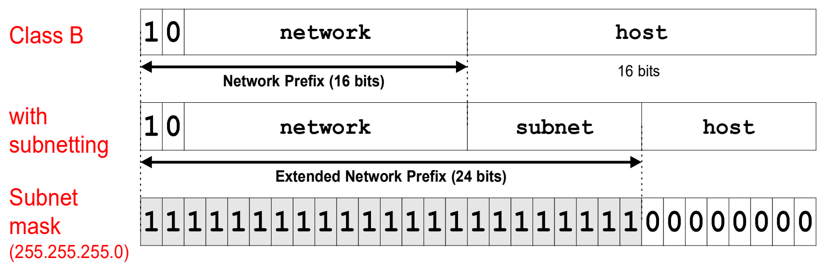


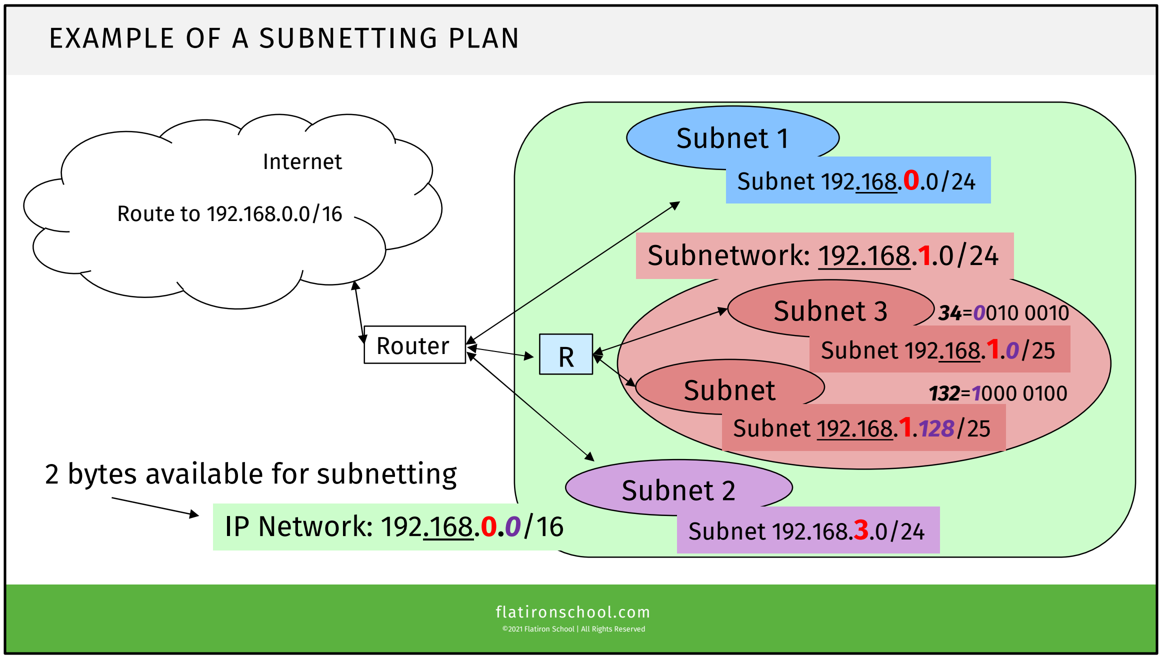
Then:

- Subnets can be freely assigned within the organization
- Internally, subnets are treated as separate networks
- Subnet structure is not visible outside the organization

SUBNET MASKS

Routers and hosts use an extended network prefix (subnet mask) to identify the start of the host numbers





Routing: 192.168.0.0/16
/16 Mask 11111111 11111111 00000000 00000000

Subnet 1: 192.168.0.0/24
/24 Mask 11111111 11111111 11111111 00000000
Available IPs: 192.168.0.0 – 192.168.0.255 (some of these are reserved)

Subnet 2: 192.168.3.0/24
Available IPs: 192.168.3.0 – 192.168.3.255 (some of these are reserved)

Subnet: 192.168.1.0/24
Break into 2 subnets:
Subnet 3: 192.168.1.0/25
/25 Mask 11111111 11111111 11111111 10000000
Available IPs: 192.168.1.0 – 192.168.0.127 (some of these are reserved)
Subnet 4: 192.168.1.128/25
Available IPs: 192.168.1.128 – 192.168.1.255 (some of these are reserved)

ADVANTAGES OF SUBNETTING

With subnetting, IP addresses use a 3-layer hierarchy:

- Network
- Subnet
- Host

Improves efficiency of IP addresses

- Does not consuming an entire address space for each physical network

Reduces router complexity

- Since external routers do not know about subnets, the complexity of routing tables at external routers is reduced

Note: Length of the subnet mask need NOT be identical at all subnetworks.

flatironschool.com

Subnetting will be covered in detail in NET200

IPv6

IPV6 - IP VERSION 6

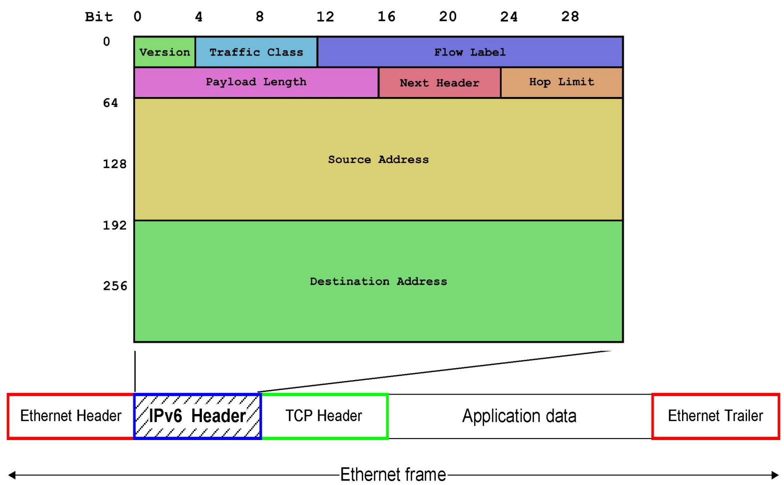
IP Version 6

- Is the successor to the currently used IPv4
- Common now in data centers, backbone traffic
- Used almost exclusively in Mobile 4G/5G networks
- Specification completed in 1994
- Makes improvements to IPv4 (no revolutionary changes)

One (not the only !) feature of IPv6 is a significant increase in size of the IP address to 128 bits (16 bytes)

- IPv6 will solve – for the foreseeable future – the problems with IP addressing

IPV6 HEADER



Bit
0
4
8
12
16
20
24
28
0
64
128
192
256
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Ethernet Header
IPv6 Header
TCP Header
Application data
Ethernet Trailer
Ethernet frame

IPV6 VS. IPV4: ADDRESS COMPARISON

IPv4 has a maximum address space of

$2^{32} \approx 4$ billion addresses

IPv6 has a maximum address space of

$2^{128} = (2^{32})^4 \approx 4$ billion x 4 billion x 4 billion x 4 billion address

$= 3.402823669209385 \times 10^{38}$

This roughly 10^{24} addresses for every square meter of the earth's surface

NOTATION OF IPV6 ADDRESSES

Convention: The 128-bit IPv6 address is written as eight 16-bit integers (using hexadecimal digits for each integer)

CEDF:BP76:3245:4464:FACE:2E50:3025:DF12

Short notation allows abbreviation of leading zeroes:

CEDF:BP76:0000:0000:009E:0000:3025:DF12 => CEDF:BP76:0:0:9E:0:3025:DF12

“:0000:0000:” can be written as “:::”

CEDF:BP76:0:0:FACE:0:3025:DF12 => CEDF:BP76:::FACE::3025:DF12

2002:808f:8990::/48

The /48 notation gives a prefix length of 48 bits, which leaves room for a 16-bit subnet field and 64 bit host addresses within the subnets.

NOTATION OF IPV6 ADDRESSES (IPV4 DERIVED)

IPv6 addresses derived from IPv4 addresses have different formats. Convention allows to use IPv4 notation for the last 32 bits.

128.143.137.144 = 0x808f 8990

128.143.137.144 -> 0:0:0:0:0:ffff:808F:8990 or

128.143.137.144 -> 2002:808f:8990:0:0:0:0:0 (called 6to4 address)

Could also write 2002:808f:8990::/48

flatironschool.com

2002:808f:8990::/48

The /48 notation gives a prefix length of 48 bits, which leaves room for a 16-bit subnet field and 64 bit host addresses within the subnets.

IPV6 PROVIDER-BASED ADDRESSES

The first IPv6 addresses will be allocated to a provider-based plan

- **Type**: Set to “010” for provider-based addresses
- **Registry**: identifies the agency that registered the address

The following fields have a variable length (recommended length)

- **Provider**: Id of Internet access provider (16 bits)
- **Subscriber**: Id of the organization at provider (24 bits)
- **Subnetwork**: Id of subnet within organization (32 bits)
- **Interface**: identifies an interface at a node (48 bits)

010	Registry ID	Provider ID	Subscriber ID	Subnetwork ID	Interface ID

MORE ON IPV6 ADDRESSES

Provider-based addresses have a similar flavor as CIDR addresses

IPv6 provides address formats for:

- **Unicast** – identifies a single interface
- **Multicast** – identifies a group. Datagrams sent to a multicast address are sent to all members of the group
- **Anycast** – identifies a group. Datagrams sent to an anycast address are sent to one of the members in the group.

[redacted]