Introduction to Data Communications and Networks
CYB 204

Network Layer

By

Egena Onu, Ph.D.

Department of Computer Science

Bingham University

Network Layer

- The network layer responsibilities are:
  - ***Logical Addressing***: uniquely addresses a device and the network to which it belongs.
  - ***Routing***: determine the best to a destination network which data packets go through.

- The network layer is therefore totally responsible for the transfer of traffic across the network.

- The key protocols of this layer include:
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)

Network Layer

- Internet Protocol (IP)
  - The IP is the fundamental protocol of this layer. Any other layer exists to support it.
  - The IP accounts for the existence of the internet through the addressing procedure.
  - The IP realises addressing by packing all necessary information into the IP header; which is an overhead of about 20bytes.
  - There are currently two versions of the IP:
    - IP version 4 (IPv4)
    - IP version 6 (IPv6)

Network Layer

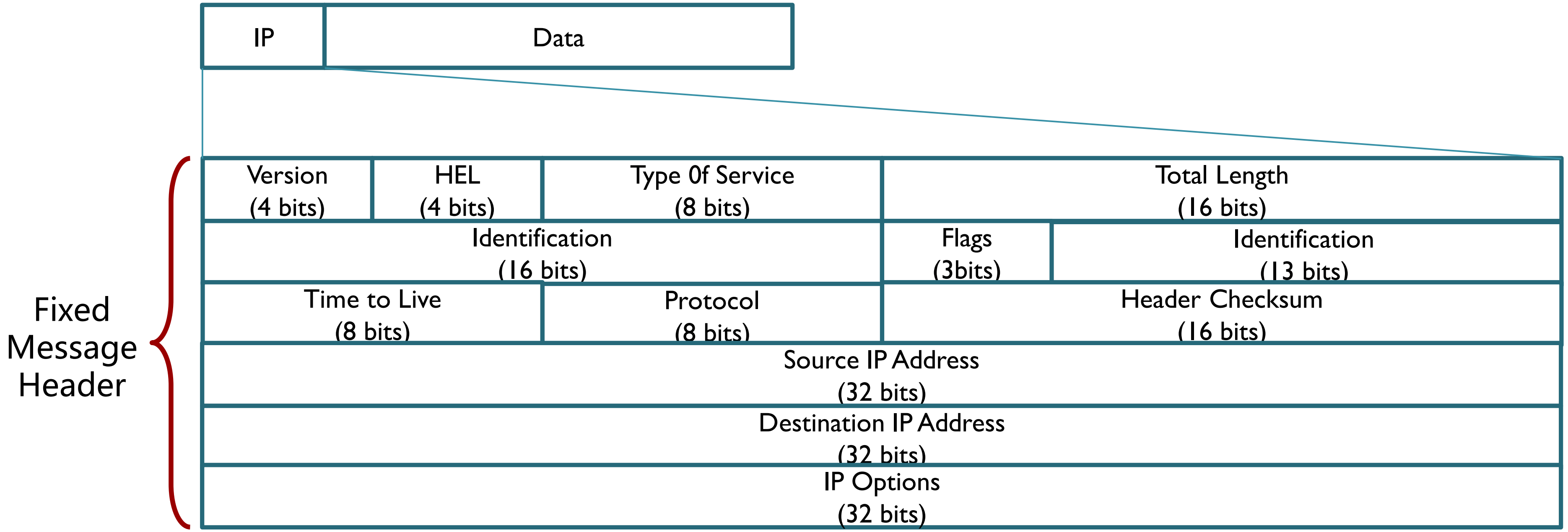
- Internet Protocol (IP)
  - The IP protocol has two primary responsibilities:
    - Performs connectionless, best-effort delivery of datagrams through an internetwork
    - Fragmentation and reassembly of datagrams to support data links with different maximum transmission unit (MTU) sizes.
    - Logical addressing by the network layer depends entirely on IP

Network Layer

- Internet Protocol (IP)
  - An encapsulated data from the network layer is referred to as a packet.
  - The network layer inserts a header to the data segment from the transport layer.
  - This transforms the segment into a data packet, otherwise known as datagram
  - The header is responsible for the packet delivery.
  - The header contains the source address and the destination address along with other necessary information that would ensure packet delivery on the network.

Network Layer

- Internet Protocol (IP)
  - IPv4 Header



IP	Data

Fixed Message Header

Version (4 bits)	HEL (4 bits)	Type 0f Service (8 bits)	Total Length (16 bits)
Identification (16 bits)		Flags (3bits)	Identification (13 bits)
Time to Live (8 bits)	Protocol (8 bits)	Header Checksum (16 bits)	
Source IP Address (32 bits)			
Destination IP Address (32 bits)			
IP Options (32 bits)			

Network Layer

- IPv4 Addressing
  - IPv4 support five different classes of address: A, B, C, D and E.
  - Only classes A, B and C are available for commercial use.
  - Each class fixes a boundary between the network number and the host number at a different point within the 32-bit address.

Network Layer

- IPv4 Addressing
  - Class A:
    - Has 8 bits network prefix number (/8).
    - Highest-order bit is set to 0 and 7-bit network number.
    - Uses 24-bit host number for host addressing.
    - Defines 126 networks
    - Supports 16,777,214 host addresses per network.
    - The address range is 1.0.0.0 to 126.0.0.0.

Network Layer

- IPv4 Addressing
  - Class B
    - 16 bit network prefix number (/16)
    - Two highest-order bits are set to 1-0 and 14-bit network number.
    - 16 bits for host number
    - Has 16,384 networks
    - Supports up to 65,534 host addresses.
    - The address range is from 128.1.0.0 to 191.254.0.0

Network Layer

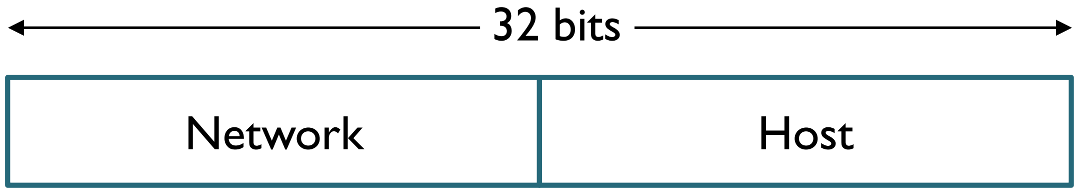
- IPv4 Addressing
  - Class C
    - Network address uses 24 bits (/24).
    - Three highest-order bits are set to 1-1-0 and 21-bit network number.
    - Reserves 8 bits for host addressing.
    - Supports a maximum of 2,097,152 network addresses.
    - A class C network can have up to 254 hosts/devices attached.
    - The network range is 192.0.1.0 to 223.255.254.0.

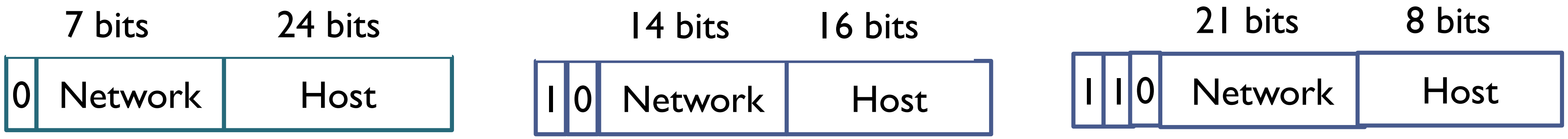
Network Layer

- IPv4 Addressing
  - The IPv4 is a 32-bit value that uniquely identifies (addresses) every device that is attached to the data network.
  - IP addressing is integral to the process of routing datagrams through the Internet.
  - Each IP address has specific components and follows a basic format.
  - Each device on a network is assigned its own unique 32-bit logical address.

Network Layer

- IPv4 Addressing
  - The address is divided into two main parts:
    - Network number identifies the network to which an IP belongs. An ISP can obtain a block of network numbers.
    - Host number identifies a host on the network. This number is unique throughout the network and it assigned by the local network administrator.





Network Layer

- IPv4 Addressing
  - The network number field of the IP address is referred to as the network prefix.
  - The leading portion of the IP address identifies the network number.
  - All hosts/devices on a given network share the same network number but each has a unique host number.
  - Hosts on different networks have different network numbers.

Network Layer

- IPv4 Addressing
  - The 32-bit IP address is divide into 8 bits at a time, called octet.
    - Each octet is separated a dot.
    - Each octet is represented in decimal form known as the dotted decimal notation.
    - Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1).
    - The minimum value for an octet is 0 and the maximum is 255.
    - 00000000.00000000.00000000.00000000
    - 11111111.11111111.11111111.11111111

Translated in binaries because that is the language of computing.

Network Layer

- IPv4 Addressing
  - An example is
    - 192.168.1.0
    - 11000000. 10101000. 00000001.00000000 expressed in the binary form

11000000	10101000	00000001	00000000

192 . 168 . 1 . 0

Network Layer

- IPv4 Addressing
  - Netmask
    - A netmask, often called “subnet mask” is a 32-bit value that divides an IP address into a network address and a host address.
    - In this case, for each of the address classes, we have:

Class A	
Network Address:	126.0.0.0
Netmask:	255.0.0.0
Class B:	
Network Address:	191.254.0.0
Netmask:	255..255.0.0
Class C:	
Network Number:	192.0.1.0
Netmask:	255.255.255.0

Network Layer

- IPv4 Addressing
  - Rules of Netmasking:
    - The subnet mask follows two rules:
      - If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies the network.
      - If a binary bit is set to a 0 (or off) in a subnet mask, the corresponding bit in the address identifies the host.
      - Following these rules, suppose our IP address, 192.168.1.0 has a netmask of 255.255.2555.0:

IP Address: 192.168.1.0	11000000.10101000.00000001.00000000
Netmask: 255.255.255.0	11111111.11111111.11111111.00000000

Network Layer

- IPv4 Addressing
  - Rules of Netmasking:
    - The first 16 bits of the netmask are set to 1. Thus, the first 24 bits of the address (192.168.1) identifies the network.
    - The last 8 bits of the netmask are set to 0. Thus, the last 8 bits of the address (0) identifies the unique host on that network.
    - The network portion of the subnet mask must be contiguous. For example, a subnet mask of 255.0.0.255 is not valid.
    - Hosts on the same logical network will have identical network addresses, and can communicate freely.

Network Layer

- IPv4 Addressing
  - Subnetting
    - The original intent of IP addresses was that the network part would uniquely identify exactly one physical network.
    - This intention was however faced with different challenges due to the explosive growth of the Internet as the principle of assigned IP became too inflexible to allow easy changes to local network configuration.
    - Some of these challenges include:
      - Installing a new network.
      - Growth in the number of hosts/devices requires splitting the local network into two or more separate networks.
      - Growing distances require splitting a network into smaller networks with gateways between them.
      - Exponential growth of Internet routing tables.
      - Local administrators had to request another network number from the Internet before a new network could be installed at their site.

Network Layer

- IPv4 Addressing
  - Subnetting
    - Subnetting is achieved by locally modifying the structure of the IP address using some of the host address bits as part of the network address bits.
    - Subnetting creates additional networks but reduces the number of networks that can be supported by each network.

Network Layer

- IPv4 Addressing
  - Subnetting
    - Subnetting is the process of creating new networks (or subnets) by stealing bits from the host portion of a subnet mask.
    - There is one caveat: stealing bits from hosts creates more networks but fewer hosts per network.
    - Consider the network number: 192.168.1.0. The default subnet mask for this network is 255.255.255.0.
    - This single network can be segmented, or subnetted, into multiple networks.
    - For example, assume an engineer is required separate the address into five departments,
    - Resolving this is possible using the following magical formula: 2^n.
    - The exponent 'n' identifies the number of bits to steal from the host portion of the subnet mask.

Network Layer

- IPv4 Addressing
  - Subnetting
    - Subnet Design Considerations
      - The deployment of an addressing plan requires careful thought. Four key questions that must be answered before any design should be undertaken are:
        1. How many total subnets do you need today?
        2. How many total subnets will you need in the future?
        3. How many hosts are on are on your network's largest subnet today?
        4. How many hosts will there be on your network's largest subnet in the future?

Network Layer

- IPv4 Addressing
  - Subnetting
    - Stealing bits essentially involves changing host bits (set to 0 or off) in the subnet mask to network bits (set to 1 or on).
    - Remember, network bits in a subnet mask must always be contiguous - skipping bits is not allowed.
    - So, suppose the engineer is required to separate 192.168.1.0 255.255.255.0 into four networks, each for admin, marketing, production and accounting.
    - This can be achieved by applying $2^3 = 8$

192.168.1.0	11000000.10101000.00000001.00000000
255.255.255.0	11111111.11111111.11111111.00000000
192.168.1.0	11000000.10101000.00000001.**000**00000
255.255.255.224	11111111.11111111.11111111.**111**00000

Bits borrowed
from the
subnetmask to
create more
networks.

Network Layer

- IPv4 Addressing
  - Subnetting
    - From the example above, we have borrowed 2 bits from the host number which leaves $2^6 - 2 = 62$ addressable device addresses to each subnet.
    - Now, each network has new numbers as follows:

This leaves us with a problem here leaves us with just 6 usable network addresses in the mix.

Even though this is a valid subnet number, since it ends in 0s, it is still the route to primary network thus confusing packet delivery.

192.168.1.0 11000000.10101000.00000001.**00**000000
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.32 11000000.10101000.00000001.**001**00000
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.64 **11000000.10101000.00000001.010**00000
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.96 **11000000.10101000.00000001.011**00000
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.128 **11000000.10101000.00000001.100**00000
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.160 **11000000.10101000.00000001.101**00000
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.192 **11000000.10101000.00000001.110**00000
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.224 **11000000.10101000.00000001.111**00000
255.255.255.224 11111111.11111111.11111111.11100000

Useable Addresses

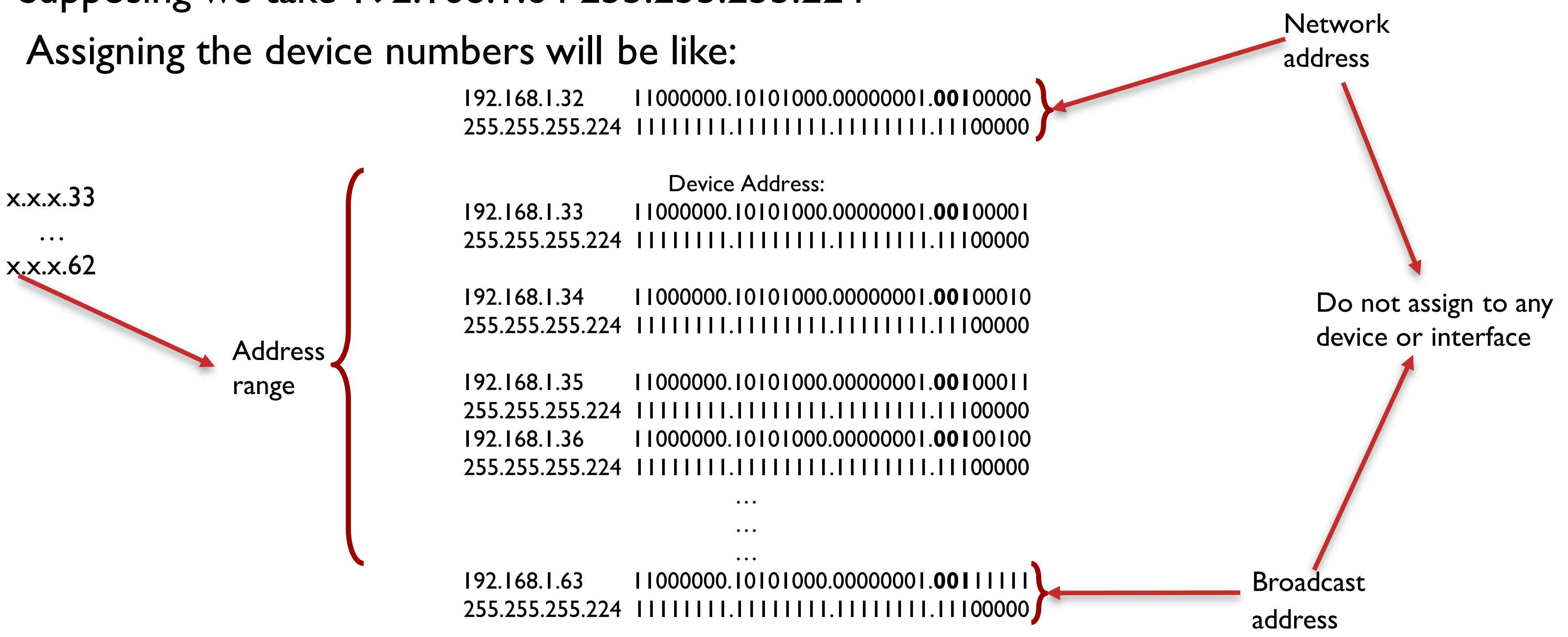
This problem is due to the network number and broadcast number where the 0s represent the network number and the 1s represents the broadcast number.

In the same manner, this guy here is also the primary network's broadcast number.

Note that the use of the all 0s and 1s subnets are prohibited. This is to eliminate situations that could potentially confuse classful routing.

Network Layer

- IPv4 Addressing
  - Subnetting
    - Supposing we take 192.168.1.64 255.255.255.224
    - Assigning the device numbers will be like:



192.168.1.32 11000000.10101000.00000001.**001**00000
255.255.255.224 11111111.11111111.11111111.11100000

Device Address:

192.168.1.33 11000000.10101000.00000001.**001**00001
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.34 11000000.10101000.00000001.**001**00010
255.255.255.224 11111111.11111111.11111111.11100000

192.168.1.35 11000000.10101000.00000001.**001**00011
255.255.255.224 11111111.11111111.11111111.11100000
192.168.1.36 11000000.10101000.00000001.**001**00100
255.255.255.224 11111111.11111111.11111111.11100000

…
…
…

192.168.1.63 11000000.10101000.00000001.**001**11111
255.255.255.224 11111111.11111111.11111111.11100000

Network Layer

Network prefix.
This signifies the number of bits in the subnetmask that are set to 1s.
e.g., 255.255.255.0 is 11111111.11111111.11111111.
00000000

- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)
    - Consider the example IPv4 address: 192.168.1.0 255.255.255.0 (or 192.168.1.0/24)
    - In the subnetting example, the engineer is required to split the network into four separate networks consisting of admin, marking, production and accounting.
    - By stealing three bits form the assigned address, the engineer realised six useable networks.
    - This leaves two unused addresses hanging with each network able to support $2^5 - 2 = 30$ addresses for the devices in the organisation. Let us assume that the marketing department alone has about 45 members of staff, admin has about 6, production has 25 and accounting has 12.
    - You will notice that leaving 30 usable addresses in each subnet has become quite unreasonable.
    - This form of subnetting also referred to classful addressing presents a wasteful IP addressing scheme.

Network Layer

- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)
    - VLSM is the process of “subnetting a subnet” and using different subnet masks for different networks in your IP plan.
    - Variable Length Subnet Masks allow you a much tighter control over your addressing scheme.
    - By using VLSM you can adjust the number of subnets and number of addresses depending on the specific needs of your network.
    - The benefits of VLSM include:
      - Allows efficient use of address space
      - Allows the use of multiple subnet mask lengths
      - Breaks up an address block into smaller custom blocks
      - Allows for route summarization
      - Provides more flexibility in network design
      - Supports hierarchical enterprise networks

Network Layer

- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)
    - Steps to create IPv4 address plan using VLSM:
      1. Determine how many bits (h) will be needed to satisfy the largest network.
      2. Pick a subnet (n) for the largest network to use.
      3. Pick the next largest network to work with.
      4. Pick the third largest network to work with.
      5. Determine network numbers for serial links.

Network Layer

- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)
    - Steps to create IPv4 address plan using VLSM:

i. Determine how many bits will be needed to satisfy the largest network $(2^5 - 2 \geq \text{number of devices})$.

ii. Pick a subnet for the largest network to use.

iii. Pick the next largest network to work with.

iv. Pick the third largest network to work with.

v. Determine network numbers for serial links.

Network Layer

- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)
    - Number of addresses required to satisfy the largest network: $= 2^h - 2$
    - Considering the example address: 192.168.1.0/24
      - The engineer would originally borrow 3 bits to satisfy its subnet requirement in the classful subnetting but no in this case.
      - The largest network (marketing department) needs 45 addresses, that is $2^6 - 2 = 62$.

Network Layer

- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)

192.168.1.0	11000000.10101000.00000001.00hhhhhh
255.255.255.192	11111111.11111111.11111111.11000000

This scheme changes the /24 prefix into /26

  - This results in the following addresses:

Not to be assigned to any device or interface on the network $2^n - 2$

192.168.1.0	11000000.10101000.00000001.00hhhhhh
255.255.255.192	11111111.11111111.11111111.11000000
192.168.1.64	11000000.10101000.00000001.01hhhhhh
255.255.255.192	11111111.11111111.11111111.11000000
192.168.1.128	11000000.10101000.00000001.10hhhhhh
255.255.255.192	11111111.11111111.11111111.11000000
192.168.1.192	11000000.10101000.00000001.11hhhhhh
255.255.255.192	11111111.11111111.11111111.11000000

Subnets that cans be used to create new networks with varied prefixes.

Network Layer

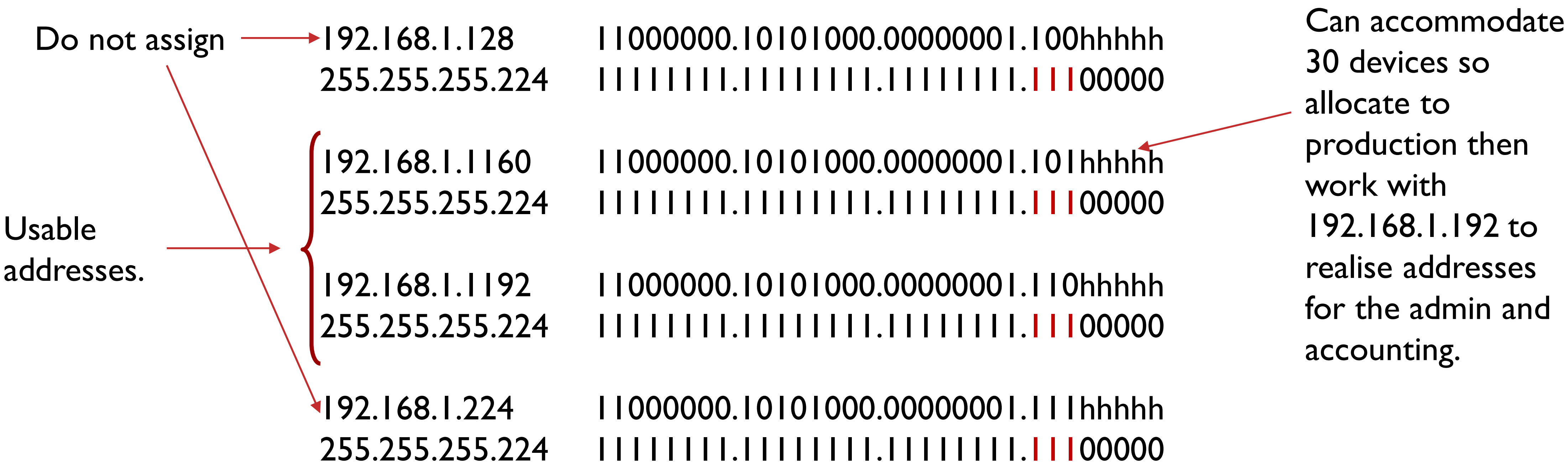
- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)
    - Assign 192.168.1.64/26 to the marketing department.
    - The next step is to identify the second largest network which in this case is production so we need h bits such that $2^5 - 2 \geq 27$.
    - So, break 192.168.1.128/26 into new networks.

```
192.168.1.128      11000000.10101000.00000001.100hhhhh
255.255.255.224    11111111.11111111.11111111.11100000
```

    - Now we have a /27 network to further address.

Network Layer

- IPv4 Addressing
  - Variable-Length Subnet Mask (VLSM)
    - The resulting addresses working with 192.168.1.128/27 are:



Do not assign

Usable addresses.

192.168.1.128	11000000.10101000.00000001.100hhhhh
255.255.255.224	11111111.11111111.11111111.11100000
192.168.1.1160	11000000.10101000.00000001.101hhhhh
255.255.255.224	11111111.11111111.11111111.11100000
192.168.1.1192	11000000.10101000.00000001.110hhhhh
255.255.255.224	11111111.11111111.11111111.11100000
192.168.1.224	11000000.10101000.00000001.111hhhhh
255.255.255.224	11111111.11111111.11111111.11100000

Can accommodate 30 devices so allocate to production then work with 192.168.1.192 to realise addresses for the admin and accounting.

Network Layer

- IPv4 Addressing
  - Private and Public Address
    - The rapid growth of the Internet resulted in a shortage of available IPv4 addresses.
    - In response, a specific subset of the IPv4 address space was designated as private, to temporarily alleviate this problem.
    - This gave rise to the of ***public*** and ***private*** addresses.

Network Layer

- IPv4 Addressing
  - Private and Public Address
    - ***Public Address***
      - A public address can be routed on the Internet.
      - Hosts that must be Internet-accessible must be configured with (or reachable by) public addresses.
      - Allocation of public addresses is governed by the Internet Assigned Numbers Authority (IANA).
    - ***Private Address***
      - A private address is intended for internal use within a home or organization, and can be freely used by anyone.
      - However, private addresses can never be routed on the Internet.
      - In fact, Internet routers are configured to immediately drop traffic with private addresses.

Network Layer

- IPv4 Addressing
  - Private and Public Address
    - ***Private Address***
      - Three private address ranges were defined in RFC 1918, one for each IPv4 class:
      - Class A - 10.x.x.x /8
      - Class B - 172.16.x.x /12
      - Class C - 192.168.x.x /24

Network Layer

- IPv6

Network Layer

- IPv6 Header Format

<table>
<tr><td>Version
(4 bits)</td><td>Traffic Class
(8 bits)</td><td colspan="3">Flow Label
(20 bits)</td></tr>
<tr><td colspan="3">Payload Length
(16 bits)</td><td>Next Header
(8 bits)</td><td>Hop Limit
(8 bits)</td></tr>
<tr><td colspan="5">Source Address
(128 bits)</td></tr>
<tr><td colspan="5">Destination Address
(128 bits)</td></tr>
</table>

Network Layer

- IPv6 Addressing
  - IPv6 address is 128bits long.

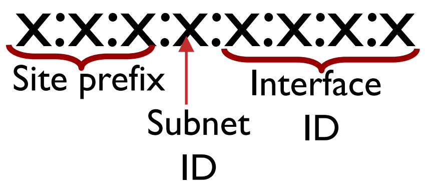
  - This allows 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,455 addresses available to connect devices to the internet.

  - In IPv6
    - The address is represented by eight hexadecimal values each of 16 bits separated by a colon: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (x = 4bits hexadecimal number).

    - It can also be represented as x:x:x:x:x:x:x:x (x = 16bits hexadecimal number)
    - The 16 bit number is converted to a 4 digit hexadecimal number

  - Example of an IPv6 address is: ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

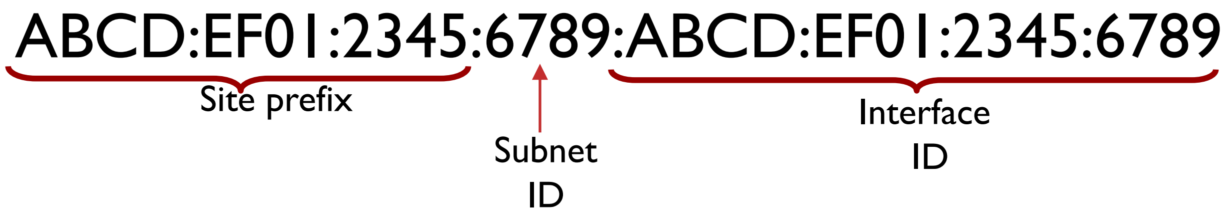
Network Layer

- IPv6 Addressing Structure
  - Addressing Structure
    - Like in IPv4 where you have the network side and the host side, IPv6 is also divided to different parts.
    - 
      x:x:x:x:x:x:x:x

      - **Site prefix**: The first 48-bit field of IPv6 describes the public topology that is usually allocated to your site by an ISP or Regional Internet Registry (RIR).
      - **Subnet ID**: The next16-bit field is the subnet ID, which either you or another administrator allocate for your site. The subnet ID describes the private topology, also known as the site topology, because it is internal to your site.
      - **Interface ID**: The rightmost 64 bits contain the interface ID, also referred to as a token. The interface ID is either automatically configured from the interface's MAC address or manually configured in EUI-64 format.

Network Layer

- IPv6 Addressing Structure
  - Addressing Structure
    - ABCD:EF01:2345:6789:ABCD:EF01:2345:6789



Site prefix

Subnet ID

Interface ID

Network Layer

Note that this field is a 16 bits field. E.g.,: 0000 0000 0000 0000

- IPv6 Addressing
  - Given: ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

So, when it is expanded and each hex value is converted, you get this.

  - ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

Match A with the corresponding hex value

  - 1010 1011 1100 1101:1110 1111 0000 0001:0010 0011 0100 0101:0110 0111 1000 1001:1010 1011 1100 1101:1110 1111 0000 0001:0010 0011 0100 0101:0110 0111 1000 1001

Repeat this process for all hex values in the fields to determine your addresses.

Hexadecimal to Binary Conversion Table		
Hexadecimal	Decimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Then match with the corresponding binary value

Network Layer

- IPv6 Addressing
  - Abbreviating and expanding IPv6
    - An IPv6 address like:ABCD:EF01:2345:6789:ABCD:EF01:2345:6789 is a fully unabbreviated format of the address.
    - Supposing you have an address like: FE00:0000:0000:0001:0000:0000:0000:0056
    - Because of the many 0s, you may want to abbreviate the address to something short and easy.

Network Layer

- IPv6 Addressing
  - Abbreviating and expanding IPv6
    - To abbreviate the address, there are two simple rules to follow:
      - Inside each quartet of four hex digits, remove the leading 0s (0s on the left side of the quartet) in the three positions on the left. (Note: at this step, a quartet of 0000 will leave a single 0.)

      - Find any string of two or more consecutive quartets of all hex 0s, and replace that set of quartets with a double colon (::). The :: means “two or more quartets of all 0s.” However, you can only use :: once in a single address, because otherwise the exact IPv6 might not be clear.

Network Layer

- IPv6 Addressing
  - Abbreviating and expanding IPv6
    - Given FE00:0000:0000:0001:0000:0000:0000:0056, for example, following the first rule, the address becomes FE00:0:0:1:0:0:0:56
    - Now, following the second rule, FE00:0:0:1:0:0:0:56 can be further reduced to FE00:0:0:1::56
    - As with the case of abbreviation, add leading 0s to the respective quartets to realise the full address.

Network Layer

- IPv6 Addressing
  - IPv6 Address Prefix
    - IPv6 address prefixes can be represented much the same way that IPv4 address prefixes are written in CIDR notation.
    - An IPv6 address prefix (the network portion of the address) is represented using the following format:

      ipv6-address/prefix-length
    - The prefix-length is a decimal value indicating the number of leftmost contiguous bits of the address.
    - The prefix length identifies the prefix (that is, the network portion) of the address.
    - It is also used with unicast addresses to separate the prefix portion of the address from the
    - Interface ID.

Network Layer

- IPv6 Addressing
  - IPv6 Address Prefix
    - Supposing we have been assigned an example IPv6 address: 2001:db8:cafe::/48
    - 2001:db80:cafe:0000:0000:0000:0000:0000

      /48 – meaning 48 leftmost bit representing the network portion of the address like in IPv4

    - 0010 0000 0000 0001:1101 1011 1000 0000:1100 1010 1111 1110:0000 0000 0000 0000:0000 0000 0000 0000:0000 0000 0000 0000:0000 0000 0000 0000:0000 0000 0000 0000

Network Layer

- IPv6 Addressing
  - IPv6 Address Prefix
    - There are many possible prefixes achievable in IPv6. examples include: /32, /48, /52, /56, /60, and /64.
    - In these examples, all the prefixes fall on a *nibble boundary*, a multiple of 4 bits.
    - Prefix lengths do not necessarily have to fall on a nibble boundary, although in most cases they do.
    - It is also important to remember that prefixes may extend to borrow bits from the interface ID portion of the address for address management.

Network Layer

- IPv6 Addressing
  - Type of IPv6 Addressing
    - IPv6 allows for three types of addressing with several variations:
    - Unicast Address
    - Anycast Address
    - Multicast Address

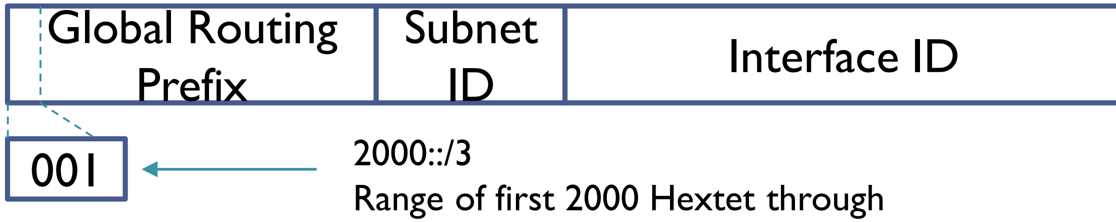
Network Layer

- IPv6 Addressing
  - Type of IPv6 Addressing
    - Unicast Address
      - A unicast address uniquely identifies an interface on an IPv6 device.
      - A packet sent to a unicast address is received by the interface that is assigned to that address
      - The type of unicast address is determined by the leftmost (high order) contiguous bits in the address, which contain the prefix.
      - Unicast addresses include:
        - Global Address
        - Link Local Address
        - Unspecified Address
        - Loopback Address

Network Layer

- IPv6 Addressing
  - Type of IPv6 Addressing
    - Unicast Address
      - Global Address
        - Global unicast addresses (GUAs), also known as aggregatable global unicast addresses, are globally routable and reachable in the IPv6 Internet.
        - The current global unicast address assignment from IANA begins with binary value 001, or the prefix 2000::/3.
        - This results in a range of global unicast addresses range of 2000::/3 through 3fff::/16.

Network Layer



2000::/3
Range of first 2000 Hextet through

- IPv6 Addressing
  - Type of IPv6 Addressing
    - Unicast Address
      - Global Address
      - The structure of the global unicast address is made up of:
        - Global Routing Prefix
          - The global routing prefix is the prefix or network portion of the address assigned by the provider, such as an ISP, to a customer or site.
          - This is a site's prefix or network address, as seen by the provider (that is, the ISP).
        - Subnet ID
        - Inteface ID
          - The Interface ID uniquely identifies the interface on the subnet. As shown earlier, the 64-bit Interface ID allows 18,446,744,073,709,551,616 addresses for each subnet.
          - The term Interface ID is used rather than Host ID because, a single host can have multiple interfaces, each having one or more IPv6 addresses.

Global Unicast Address (Hexadecimal)	Range of First Hextet	Range of First Hextet in Binary
2000::/3	2000 to 3fff	0010 0000 0000 0000 0011 1111 1111 1111

Network Layer

- IPv6 Addressing
  - Type of IPv6 Addressing
    - Unicast Address
      - Link Local Address
        - Link-local addresses (LLA) are unicast addresses that are confined to a single link.
        - “Link” here refers to a network segment or subnet. Therefore, link-local addresses are local only to a particular link or subnet and not routable off the link.
        - Link-local addresses use the fe80::/10 prefix resulting in a range of addresses from fe80::/10 to febf::/10

Network Layer

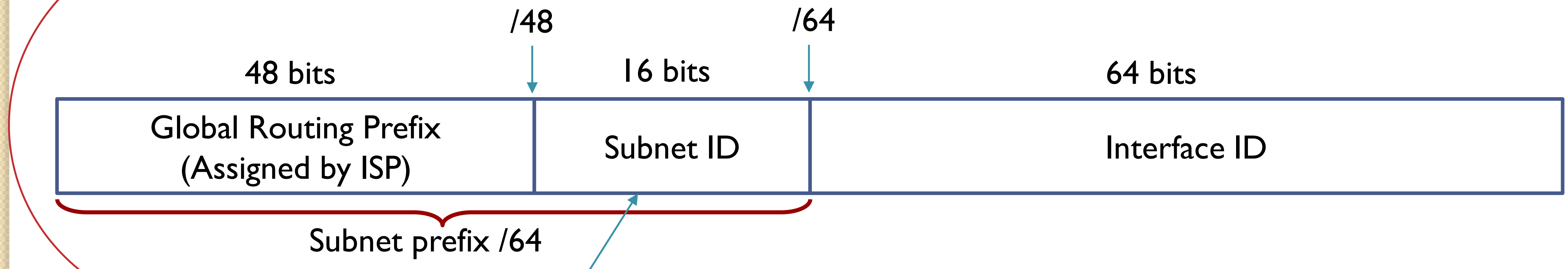
- IPv6 Addressing
  - Type of IPv6 Addressing
    - Unicast Address
      - Unspecified Address
        - An unspecified unicast address is an all-0s address.
        - An unspecified unicast address is used as a source address to indicate the absence of an address.
        - It cannot be assigned to an interface.
      - Loopback Address
        - A loopback address is another type of unicast address.
        - An IPv6 loopback address is represented as ::1, that is, an all-0s address except for the last bit, which is set to 1.
        - It is equivalent to the IPv4 address block 127.0.0.0/8 or the most commonly used 127.0.0.1 loopback address.

Network Layer

- IPv6 Addressing
  - Subnetting
    - IPv6 subnetting is quite simple and straightforward compared to IPv4 subnetting.
    - Subnetting however like in IPv4's VLSM depends on the subnet prefix.
    - A common IPv6 site prefix is /48, assigned by the provider—usually an ISP but can also be an RIR.
    - This creates a 16-bit Subnet ID, allowing 216, or 65,536, subnets. Remember that the all-0s and all-1s subnets are valid subnets.

Network Layer

- IPv6 Addressing
  - Subnetting
    - Given 2001:db8:cafe::/48



/48

/64

48 bits

16 bits

64 bits

Global Routing Prefix (Assigned by ISP)

Subnet ID

Interface ID

Subnet prefix /64

- 2001:db80:cafe:0000:0000:0000:0000:0000

Network Layer

- IPv6 Addressing
  - Subnetting

Global Routing Prefix	Subnet ID	New Address Format
2001:db8:cafe:	0001	2001:db8:cafe:1::/64
2001:db8:cafe:	0002	2001:db8:cafe:2::/64
2001:db8:cafe:	0003	2001:db8:cafe:3::/64
2001:db8:cafe:	0004	2001:db8:cafe:4::/64
2001:db8:cafe:	0005	2001:db8:cafe:5::/64
…	…	…
2001:db8:cafe:	000f	2001:db8:cafe:f::/64

Network Layer

- IPv6 Addressing
  - Multicast Address
    - A multicast address is used to send a single packet or, more likely, a single stream of packets to multiple devices simultaneously.
    - This is much more efficient than duplicating a stream of packets as a separate unicast transmission for each destination.
    - Multicast can be a better option than broadcast when the recipients are only a subset of all the devices on a subnet.
    - An IPv6 multicast address has the prefix ff00::/8, which defines a group of devices known as a multicast group.
    - A packet sent to a multicast group always has a unicast source address.
    - A multicast address can only be a destination address and can never be a source address.

Network Layer

- IPv6 Addressing
  - Anycast Address
    - An IPv6 anycast address is an address that can be assigned to more than one interface (typically different devices).
    - In other words, multiple devices can have the same anycast address.
    - A packet sent to an anycast address is routed to the "nearest" interface having that address.
    - There is no special prefix for an IPv6 anycast address.
    - An IPv6 anycast address uses the same address range as global unicast addresses.
    - Each participating device is configured to have the same anycast address.

Questions!