**Essentials of Networking Spring 2018 Study Guide by Shay Walker**

Be able to name and describe the 7 layers of the OSI networking model.

1. Physical

* The physical method of moving data between computers, so the cabling and central box are part of the physical layer
* The physical method that is used to communicate data, such a copper cabling, coax, hubs, switches, (etc)

1. Data Link

* Any device that deals with a MAC address is part of the Data Link Layer (NICs)
* The reliable electric connectivity of devices that use the MAC address OUI and NIC to address the destination of data for the wanted device

1. Network

* Containers called packets get created and addressed so they can go form one network to another. (TCP/IP)
* The data router, or controls where the data is sent using the logical address or the IP address of another device. Also involves packets or frames that allow for data checking (FCS)

1. Transport

* The assembler and disassembler of software. The Transport layer also initializes requests for packets that were not received in good order.
* Breaks the data up so that it can be sent over a network more efficiently and effectively, therefore no bottlenecking or wire hogging.

1. Session

* Handles all sessions for a system. The session layer initiates sessions, accepts incoming sessions, and opens and closes existing sessions.
* Controls the two way communication and can end or accept sessions

1. Presentation

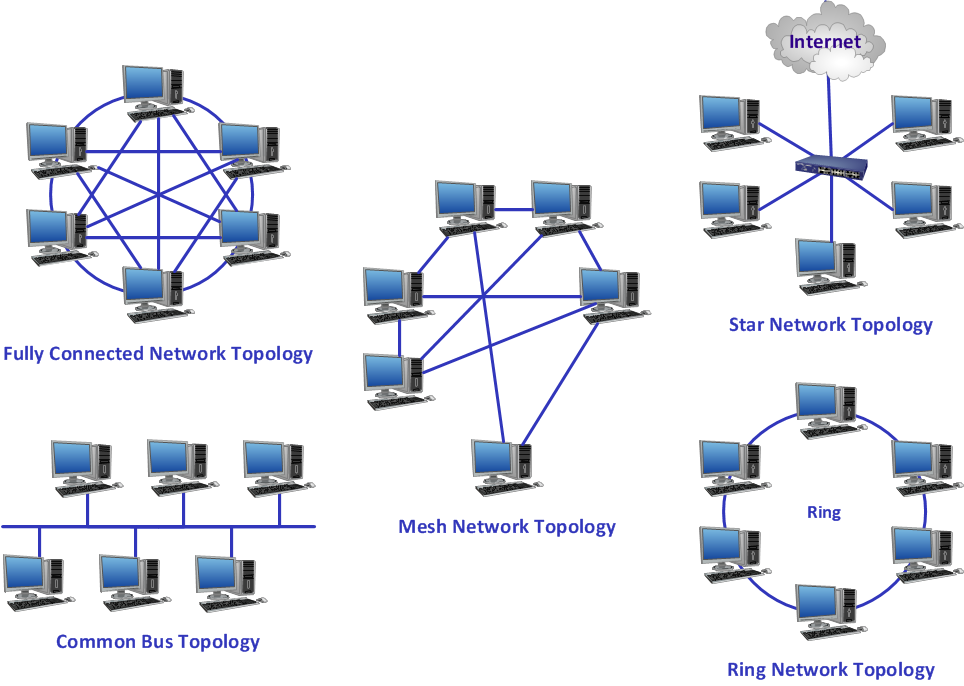
-translates data from lower layers into a format usable by the application layer and vice versa

- this layer breaks down the data into forms that the desired application can use in the next level, it can also decrypt and encrypt data here

1. Application

* Refers to the code built into all operating systems that enables network-aware applications. (Application Programming Interfaces)
* Uses what is handed to it by the presentation layer, to then allow the application the user desires or is being called can function properly

**Understand the differences between the 8 network topologies.**



Bus Topology – terminators at each end, to prevent reflection of the signals

Ring Topology – signals move in one direction, if one break in the circuit then the data flow stops completely

Star Topology- used a central connection box for all the computers on the network, this offers fault tolerance, unlike Bus and Ring

Star-Ring Topology-Ring inside central box

Star-Bus Topology- Bus inside central box

Mesh Topology - Connects every computer to every other computer via two or more routes. Partial Mesh or Fully Meshed.

Point to Multipoint - Like a Star but with an intelligent device or computer at the center directing the connections

Point- to- Point – Two computers connected directly together

**Be able to describe the essential functions of core network devices: hub, switch, router, firewall.**

Hub – an electronic device that sits at the center of a star topology network, providing a common point for the connection of network devices. In a 10BaseT Ethernet network, the Hub contains the electronic equivalent of a properly terminated bus cable. Hubs are rare today and have been replaced by switches.

* A hub repeats data to all devices on a network simultaneously

Switch – A Layer 2 Data Link multiport device that filters and forwards frames based on MAC addresses.

* Implements Spanning Tree Protocol

Router – connects each of the subnets through logical addressing. Routers use the IP address, not he MAC address to forward data. This enables networks to connect across data lines that do not use Ethernet, like the telephone network.

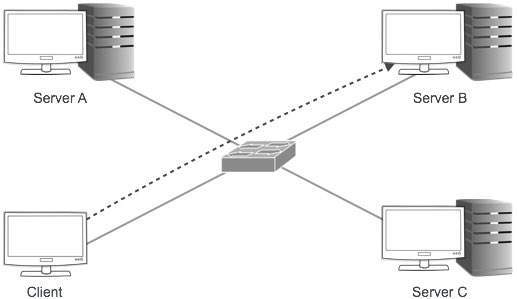
Firewall – a device that restricts traffic between a local network and the Internet

**Know how IPv4 and IPv6 addressing works, the definition of a subnet, and key network IDs for each.**

IPv4 supports three different type of addressing modes:

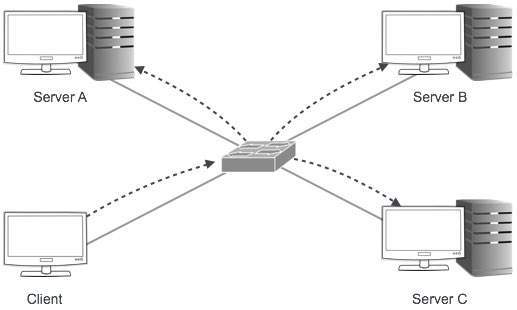
## **Unicast Addressing Mode:**

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here client sends data to the targeted server:



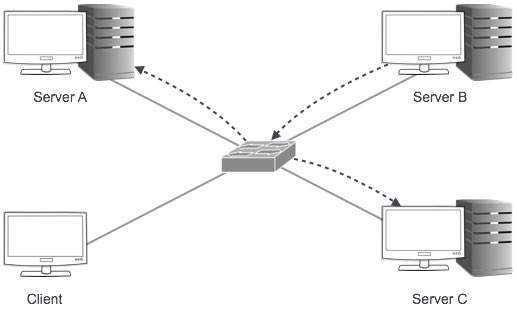
## **Broadcast Addressing Mode:**

In this mode the packet is addressed to all hosts in a network segment. The Destination Address field contains special broadcast address i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here client sends packet, which is entertained by all the Servers:



## **Multicast Addressing Mode:**

This mode is a mix of previous two modes, i.e. the packet sent is neither destined to a single host nor all the host on the segment. In this packet, the Destination Address contains special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which is entertained by more than one Servers. Every network has one IP address reserved for network number which represents the network and one IP address reserved for Broadcast Address, which represents all the host in that network.

## **Hierarchical Addressing Scheme**

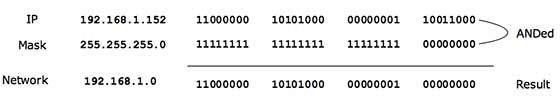
IPv4 uses hierarchical addressing scheme. An IP address which is 32-bits in length, is divided into two or three parts as depicted:



A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

## **Subnet Mask**

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish the both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address 192.168.1.152 and the Subnet Mask is 255.255.255.0 then



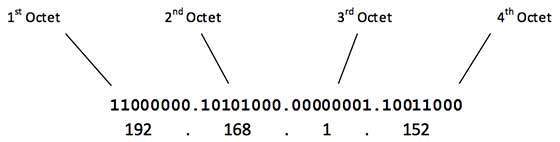
This way Subnet Mast helps extract Network ID and Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

# **IPv4 - Address Classes**

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situation as per the requirement of hosts per network. Broadly, IPv4 Addressing system is divided into 5 classes of IP Addresses. All the 5 classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers - responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



Number of networks and number of hosts per class can be derived by this formula:



When calculating hosts IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

## **Class A Address**

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

Class A Addresses

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (27-2) and 16777214 hosts (224-2).

Class A IP address format thus, is **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

## **Class B Address**

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

Class B Addresses

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses.

Class B IP address format is, **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

## **Class C Address**

The first octet of Class C IP address has its first 3 bits set to 110, that is

Class C Addresses

Class C IP addresses range from 192.0.0.x to 192.255.255.x. The default subnet mask for Class B is 255.255.255.x.

Class C gives 2097152 (221) Network addresses and 254 (28-2) Host addresses.

Class C IP address format is **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

## **Class D Address**

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of

Class D Addresses

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that's why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

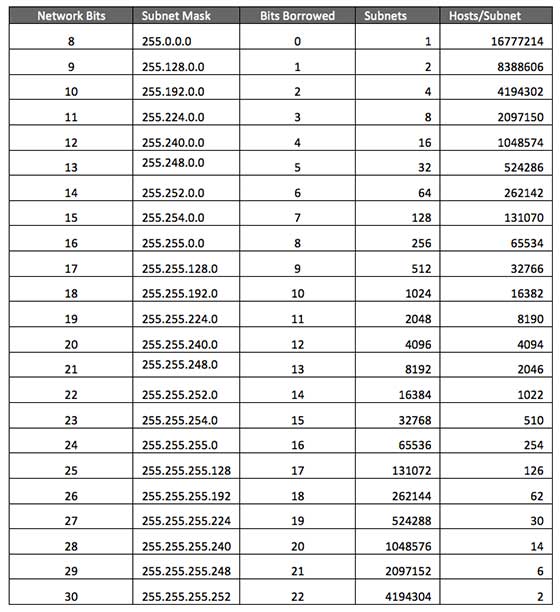
## **Class E Address**

This IP Class is reserved for experimental purposes only like for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

# **IPv4 - Subnetting (CIDR)**

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP addresses can be used to have smaller sub-networks which provides better network management capabilities.

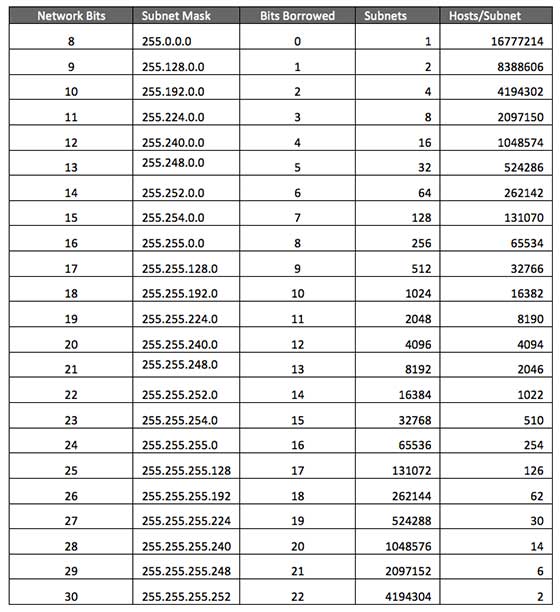


## **Class A Subnets**

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (21=2) with (223-2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets:



In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, Sub-netting cannot be implemented by using more than 30 bits as Network Bits which provides less than two hosts per subnet.

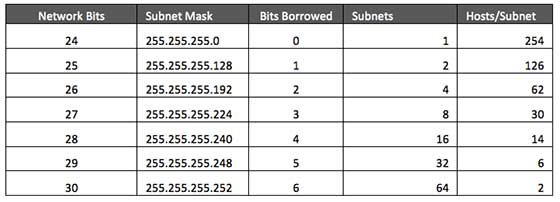
## **Class B Subnets**

By Default, using Classful Networking, 14 bits are used as Network bits providing (214) 16384 Networks and (216-1) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting:



## **Class C Subnets**

Class C IP addresses normally assigned to a very small size network because it only can have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address:



# **IPv4 - Variable Length Subnet Masking (VLSM)**

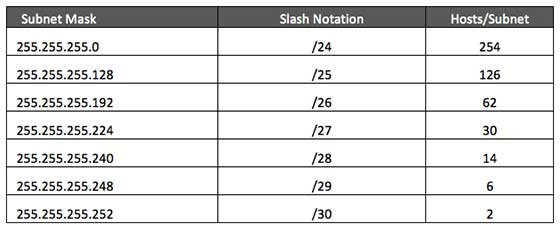
Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. He is having three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

## **Step - 1**

Make a list of Subnets possible.



## **Step - 2**

Sort the requirements of IPs in descending order (Highest to Lowest).

* Sales 100
* Purchase 50
* Accounts 25
* Management 5

## **Step - 3**

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of Sales Department. The subnet Mask used for this subnet has 10000000 as the last octet.

## **Step - 4**

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all Purchase department's PCs. The subnet mask used has 11000000 in the last octet.

## **Step - 5**

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

## **Step - 6**

Allocate next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of subnet mask will contain 11111000.

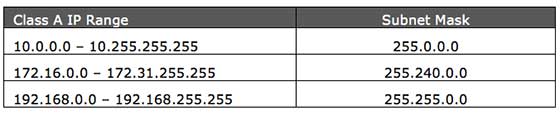
By using VLSM, the administrator can subnet the IP subnet such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, still left with plenty of IP addresses which was not possible if he has used CIDR.

# **IPv4 - Reserved Addresses**

There are few Reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside Local Area Network.

## **Private IP Addresses**

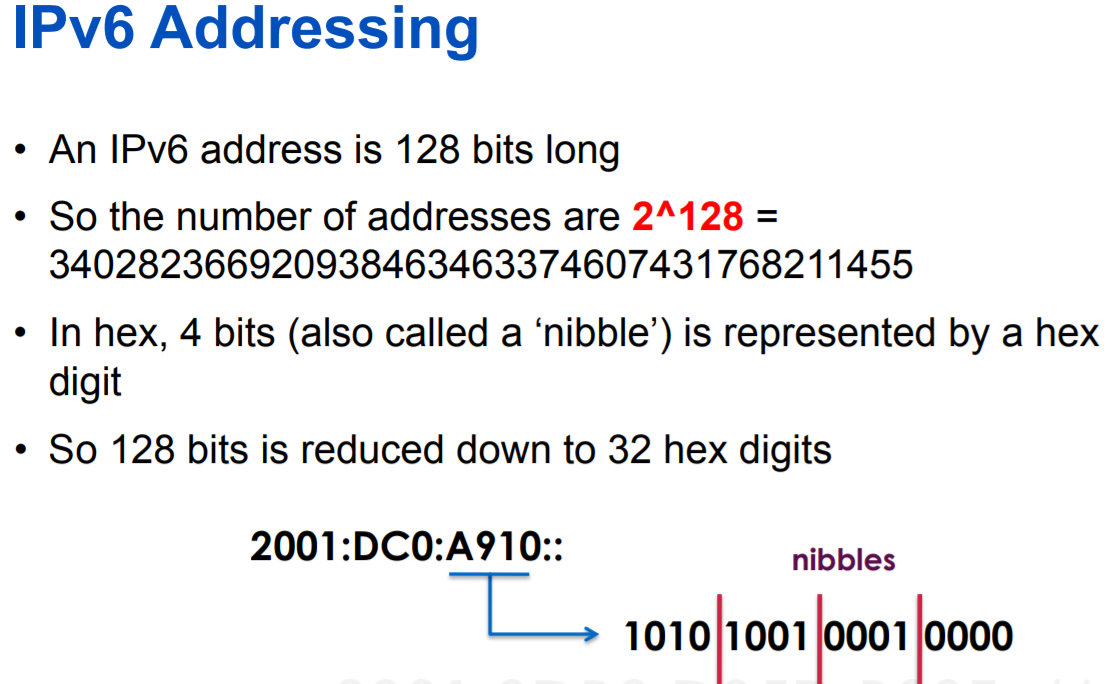
Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on Internet so packets containing these private addresses are dropped by the Routers.

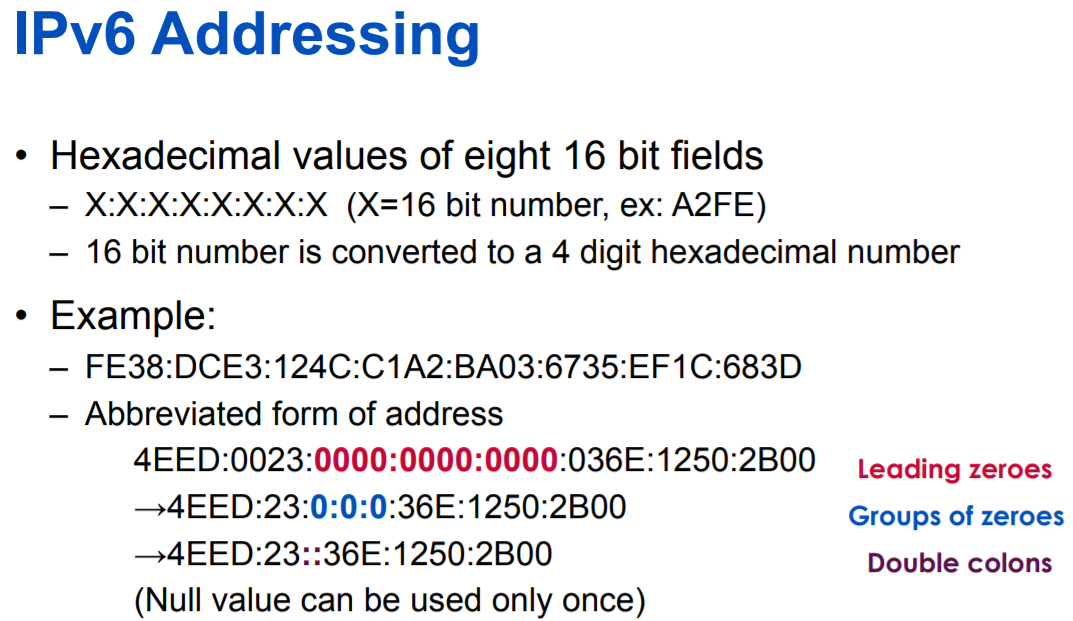


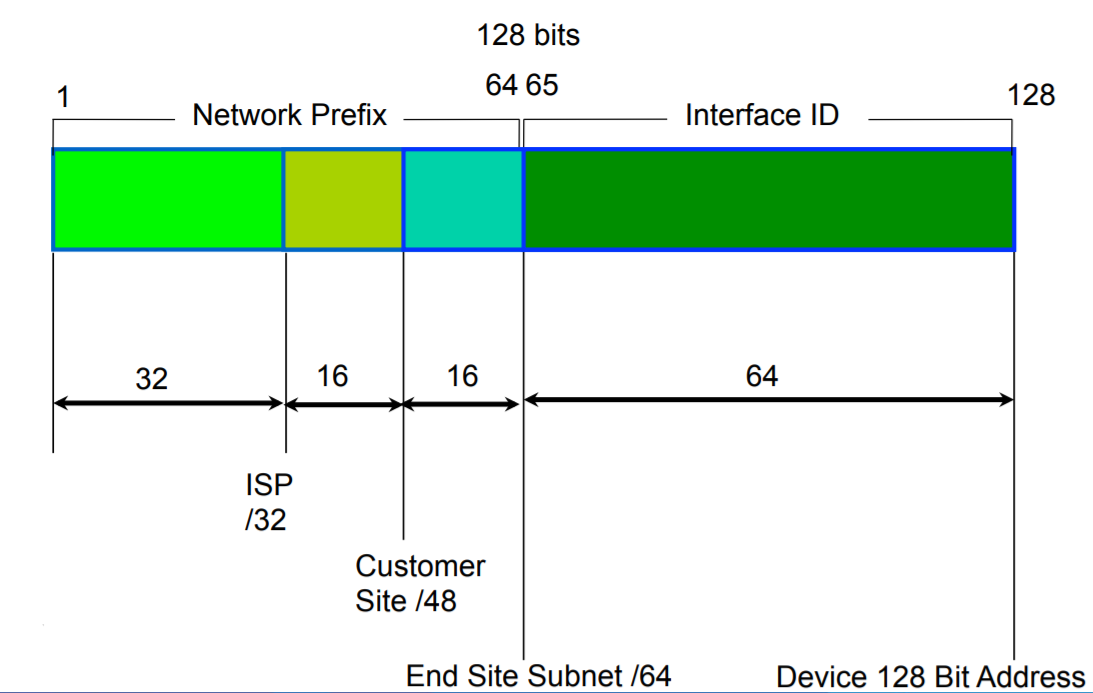
In order to communicate with outside world, Internet, these IP addresses must have to be translated to some public IP addresses using NAT process or Web Proxy server can be used.

The sole purpose to create separate range of private addresses is to control assignment of already-limited IPv4 address pool. By using private address range within LAN, the requirement of IPv4 addresses has globally decreased significantly. It has also helped delaying the IPv4 address exhaustion.

IP class, while using private address range, can be chosen as per the size and requirement of the organization. Larger organization may choose class A private IP address range where smaller may opt for class C. These IP addresses can be further sub-netted be assigned to departments within an organization.







Subnetting

In most cases a subnet calculator will not be required, since IPv6 using hex (hexadecimal) – and so long as the prefix length is a multiple of 4, it makes it quite easy.  For example (this is also where the table “IPv6 Subnet Reference IP Address” comes in a lot of handy above):

2402:9400:1234:1234::/64  
2402:9400:1234:123X::/60  
2402:9400:1234:12XX::/56  
2402:9400:1234:1XXX::/52  
2402:9400:1234:XXXX::/48  
2402:9400:123X:XXXX::/44  
2402:9400:12XX:XXXX::/40

/48 allocations are usually provided to business, who require additional VLANs or may require the range to be split up.  Using a /48 allocation would allow them to do so.

2402:9400:10::/48  
2402:9400:11::/48  
2402:9400:12::/48  
2402:9400:13::/48  
2402:9400:14::/48

Be able to explain the difference between a site to site and remote access VPN.

Site-to-site VPNs connect entire networks to each other -- for example, connecting a branch office network to a company headquarters network. In a site-to-site VPN, hosts do not have VPN client software; they send and receive normal TCP/IP traffic through a VPN gateway. The VPN gateway is responsible for encapsulating and encrypting outbound traffic, sending it through a VPN tunnel over the Internet, to a peer VPN gateway at the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet towards the target host inside its private network.

Remote access VPNs connect individual hosts to private networks -- for example, travelers and teleworkers who need to access their company's network securely over the Internet. In a remote access VPN, every host must have VPN client software (more on this in a minute). Whenever the host tries to send any traffic, the VPN client software encapsulates and encrypts that traffic before sending it over the Internet to the VPN gateway at the edge of the target network. Upon receipt, that VPN gateway behaves as described above for site-to-site VPNs. If the target host inside the private network returns a response, the VPN gateway performs the reverse process to send an encrypted response back to the VPN client over the Internet.

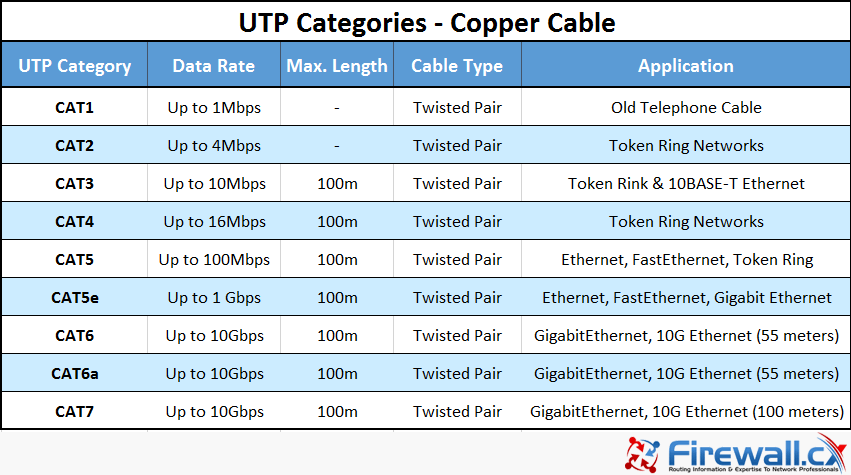
Site to site VPN – directly connect two separate LANs permanently. It is slow but inexpensive, compared to a dedicated high-speed connection between two faraway LANs. This kind of connection enables two separate LANs to function as a single network, sharing files and services as if in the same building. This is called site to site VPN.

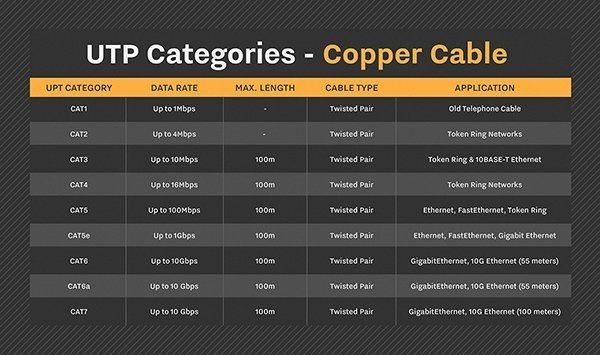
Remote access VPN - A remote-access VPN allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers.

Remote access – tunnel through firewall that is encrypted (signed certificate)

Site to site – Firewall to Firewall, password/certificate based, requires handshaking then a tunnel, subnets are needed and must be different, all must have a public IP address.

**Identify the limitations (distance / bandwidth) of different types of network cabling, Cat3 and newer.**





**Be able to explain the essential functions of DHCP in IPv4 and IPv6 networks.**

Ipv4

Dynamic Host Configuration Protocol – automatically assigns and IP address whenever a computer connects to the network.

* You first must configure the computer to use DHCP, it then becomes a DHCP Client.
* When the client boots up it will send a special DHCP Discover packet using the broadcast address.
* One system to the LAN must be running DHCP server software, designed to respond with a DHCP offer, which it then offers an IP address and subnet mask from the previously configured range of address that the server has available.

Ipv6

* Only assigns the host part of the addresses(Stateless)
* Catalogs activity and stores names of all sites/services on the network like active directory and printers.

Tunneling Protocols:

6 to 4- that enables Ipv6 traffic to use the Ipv4 Internet without having to se up explicit tunnels (generally used to connect two routers) (starts with 2002)

6 in 4 – one of the most popular, it can go through NAT

Teredo- built into Microsoft windows, starts with 2001,

Miredo – open source version of teredo

ISATAP – router to router, adds the ipv4 address to an ipv6 prefix to create a nonstandard address

4 to 6 (Ipv6 cannot use NAT) encapsulates Ipv6 traffic into an Ipv4 tunnel to et to an Ipv6- capable router

Following is a list of the differences between DHCP for IPv6 and DHCPv6.

* *DHCPv6 uses DHCP Unique Identifiers (DUIDs) (*[*RFC 6355*](http://tools.ietf.org/html/rfc6355)*) whereas DHCP for IPv4 uses MAC addresses to identify the client.*
* *Their message type names are different, but perform many of the same functions (*[*DHCP message types*](http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml)*,*[*DHCPv6 message types*](http://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml)*).*
* *Obviously, DHCP for IPv4 messages are transmitted over IPv4 packets and DHCPv6 is transmitted over IPv6 packets.*
* *DHCPv6 uses ICMPv6 Router Advertisement (RA) and IPv6 multicast messages and DHCP uses broadcast IPv4 messages on the LAN.*
* *DHCPv6 uses link-local IPv6 addresses when communicating between client and relay/server (*[*RFC 6939*](https://tools.ietf.org/html/rfc6939)*), and DHCP for IPv4 uses unsolicited broadcasts.*
* *DHCP for IPv4 and DHCPv6 UDP port numbers are different. DHCP servers and relay agents listen on UDP port 67 and clients listen on UDP port 68, DHCPv6 clients listen on UDP port 546, DHCPv6 servers and relay agents listen on UDP port 547.*
* *DHCPv6 servers offer randomized interface identifiers (helps limit attacker reconnaissance), DHCP offers the next IPv4 address from the scope/pool.*
* *DHCPv4 can be configured on a router, stateful*[*DHCPv6 is not typically available on router*](https://community.infoblox.com/blogs/2014/09/15/still-using-dhcp-your-routers-you-can%E2%80%99t-do-ipv6)*s.*
* *DHCP for IPv4 can provide the default gateway IP address to the client, whereas DHCPv6 does not have this option; the IPv6 node learns about its first-hop router from the ICMPv6 RA message (*[*Pending draft on this subject*](https://tools.ietf.org/html/draft-ietf-mif-dhcpv6-route-option-05)*).*
* *DHCP for IPv4 scopes are susceptible to exhaustion; DHCPv6 scopes are typically /64s with over 18 quintillion addresses so pool exhaustion is impossible.*

Be able to explain how the PKI chain of trust makes the internet more secure.

### **Elements of PKI**

A typical PKI consists of hardware, software, policies and [standards](https://whatis.techtarget.com/definition/standard) to manage the creation, administration, distribution and revocation of keys and [digital certificates](https://searchsecurity.techtarget.com/definition/digital-certificate). Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the [public key](https://searchsecurity.techtarget.com/definition/public-key) contained in the certificate.

A typical PKI includes the following key elements:

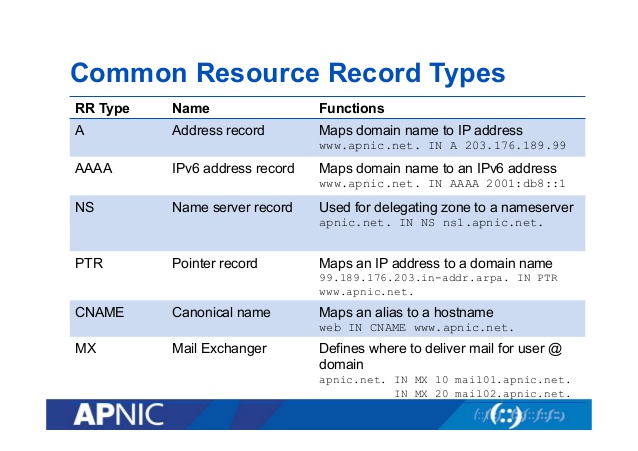
* A trusted party, called a [certificate authority (CA)](https://searchsecurity.techtarget.com/definition/certificate-authority), acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities
* A [registration authority](https://searchsecurity.techtarget.com/definition/registration-authority), often called a subordinate CA, certified by a root CA to issue certificates for specific uses permitted by the root
* A certificate database, which stores certificate requests and issues and revokes certificates
* A certificate store, which resides on a local computer as a place to store issued certificates and [private keys](https://searchsecurity.techtarget.com/definition/private-key)

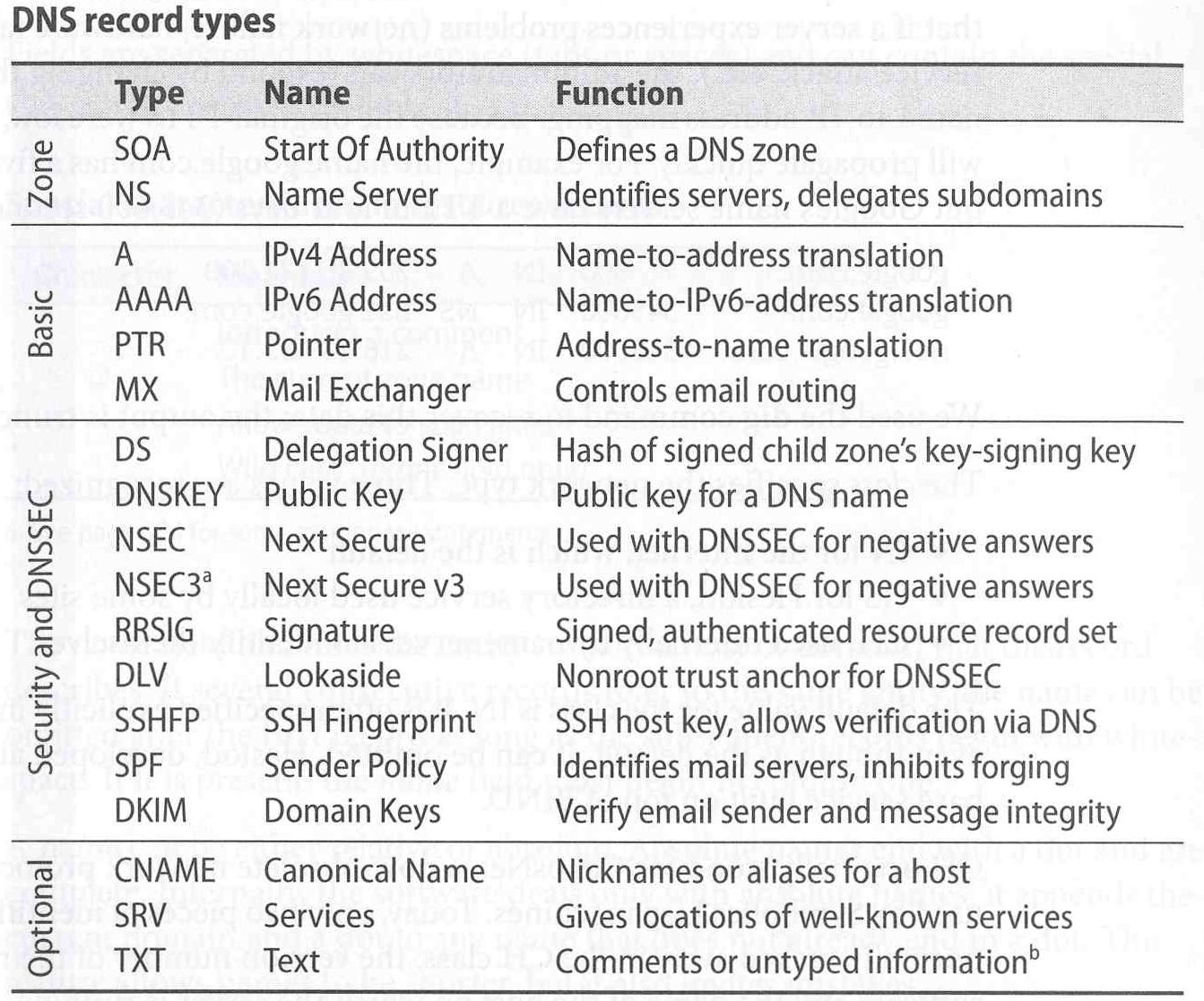
A CA issues digital certificates to entities and individuals after verifying their identity. It signs these certificates using its private key; its public key is made available to all interested parties in a self-signed CA certificate. CAs use this trusted root certificate to create a "chain of trust" -- many root certificates are embedded in Web browsers so they have built-in trust of those CAs. Web servers, email clients, smartphones and many other types of hardware and software also support PKI and contain trusted root certificates from the major CAs.

Along with an entity’s or individual’s public key, digital certificates contain information about the [algorithm](https://whatis.techtarget.com/definition/algorithm) used to create the signature, the person or entity identified, the digital signature of the CA that verified the subject data and issued the certificate, the purpose of the public key encryption, signature and certificate signing, as well as a date range during which the certificate can be considered valid.

A public key infrastructure (PKI) allows users of the Internet and other public networks to engage in secure communication, data exchange and money exchange. This is done through public and private cryptographic key pairs provided by a certificate authority.

**Describe the meaning of the different types of DNS records.**





Be able to recognize well known TCP or UDP port numbers, and the service provided on that port.

FTP- Data Port – 20 (Normal FTP – 21) (TCP)

FTPS- 20/21 (TCP)

SSH- 22 (TCP)

SSHS

DNS – 53 (Both)

DNSS – 53 (Both)

HTTP – 80 (TCP)

HTTPS- 443 (TCP)

LDAP – 389 (UDP)

LDAPS- 636 (TCP)