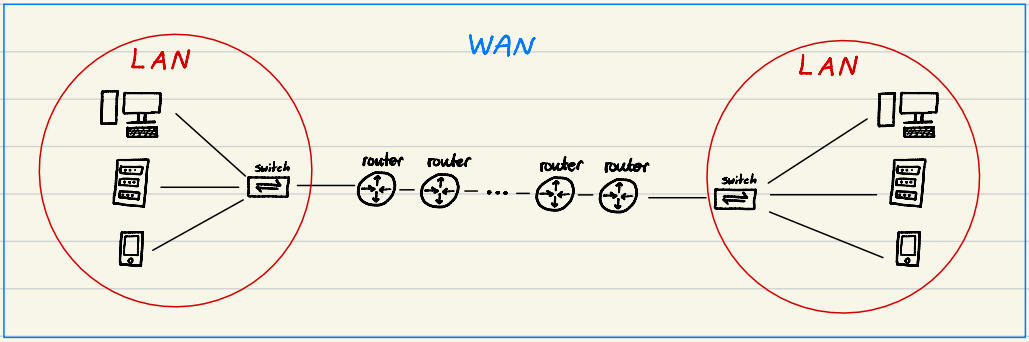
Intro to Networking

* Local Area Network (LAN): connected devices that are in one physical location.
* Wide Area Network (WAN): connected devices that are in different physical locations.



* OSI Model: a layered representation of how devices communicate.

Sender Reciever

layer	Name	Includes	Device
7	Application		
6	presentation		
5	Session		
4	Transport	TCP/UDP, Port	
3	Network	IP Adress	Routers
2	Data-Link	MAC Adress	Switches
1	Physical		Wires / cables

* TCP/IP stack : the stack (model) that is actually used in networking.

layer	name	uses
4	Application	Data
3	Transport	Segment
2	Internet	Packet
1	Network Access	Frame

} Protocol Data Unit (PDU)

note: Engineers reference the OSI model since it breaks down the layers into specific sections.

OSI Model Breakdown

Upper 3 Layers of the OSI model:

note: developers handle these layers not network engineers.

* Layer 7 (Application): provides network services to the applications of the user.
  - It differs from other layers in that it doesn't provide services to any other layer.
  - It establishes the availability of intended communication partners.
  - It synchronizes and establishes agreement on procedures for error recovery and control of data integrity.
* Layer 6 (presentation): ensures that the information sent at layer 7 of one system is readable by the other.
  - It can translate among multiple data formats.
* Layer 5 (session): establishes, manages and terminates sessions between two hosts.
  - It also synchronizes dialog between layer 6 of two hosts and manages their data exchange.
  - It also offers efficient data transfer, CoS and exception reporting of upper layer problems.

Lower 4 Layers of the OSI model:

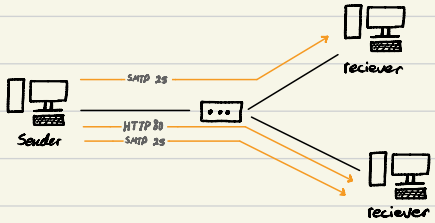
* Layer 4 (transport): defines the services to segment, transfer and reassemble data for individual communications.
  - It determines whether TCP or UDP is used and the port number.
  - It breaks down large files into smaller segments that are less likely to incure transmission problems.
* Layer 3 (network): provides connectivity and path selection between two hosts and may be on seperate networks.
  - It manages connectivity of hosts by providing logical addressing (IP address).
* Layer 2 (data-link): defines how data is formatted for transmission and how access to physical media is controlled.
  - It includes error detection and correction to ensure a reliable delivery of the data.
  - It uses the layer 2 address (MAC address).
* Layer 1 (Physical): concerns literally the physical components of the network (cables).
  - It defines the specs needed for activating, maintaining and deactivating the physical link between end devices.
  - It enables bit transmission between end devices.

Lower 4 Layers in Depth

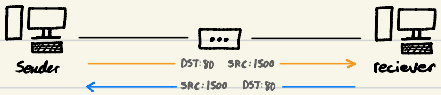
Layer 4 (Transport):

* The transport layer provides transparent transfer of data between hosts and is responsible for end-to-end error recovery and flow control.
  → Flow control is the process of adjusting the flow of data from the sender to ensure that the receiver can handle all of it.

* Session Multiplexing: the process where the host is able to support multiple sessions simultaneously and manage the individual traffic streams over a single link.



* The layer 4 destination port number is used to identify the upper layer protocol.
* The sender also adds a source port number to the layer 4 header.
* The combination of source and destination port number can be used to track sessions.



* Protocols :

1- TCP : once a connection is established, data can be sent bidirectionally.

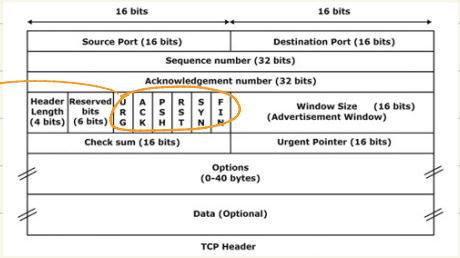
→ carries out sequencing to ensure segments are processed in the correct order.

→ is reliable but slower than UDP.

→ perform a three-way handshake : sender —Syn→ / ←Syn/Ack— / —Ack→ reciever (if parts of data is missing it will be resent.)

→ Performs flow control.

TCP header :



2- UDP: once connected it sends data to one side (no handshake).

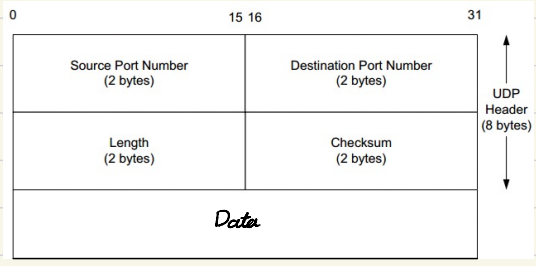
→ does not carry out sequencing.

→ is fast but not reliable

→ doesn't perform flow control.

→ if data recovery is required, its up to the upper layers to provide it.

UDP header :



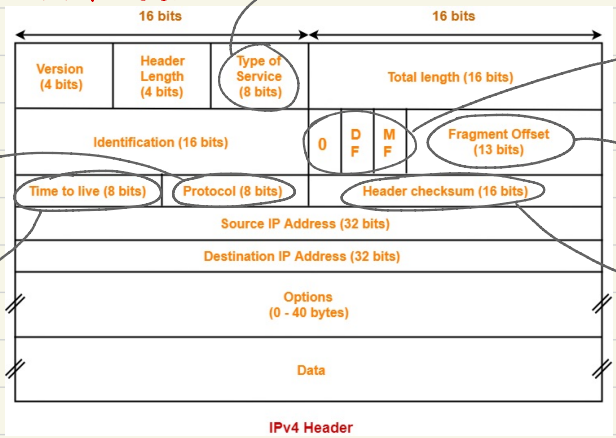
TCP is used when you don't mind slower data transmission as long as it's not missing any parts.

UDP is used when you need fast transmission and you can afford to lose some parts of the data.

Layer 3 (Network):

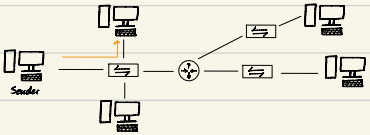
* The network layer is responsible for routing packets to their destination and for Quality of Service.
* IP (Internet Protocol) is the best known Layer 3 protocol.
* IP is a connectionless protocol with no acknowledgement at layer 3.
* the network designer uses IP adressing to partition the overall network into smaller "subnets".
  → this improves performance and security and makes troubleshooting easier.

IPv4 header:

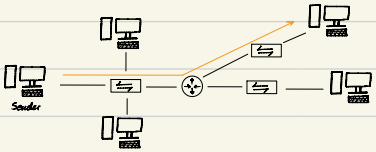


* There are three main IP traffic types:

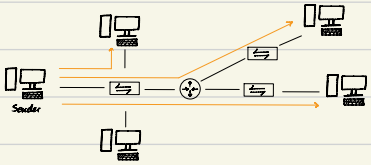
1- Unicast: to a single destination host.



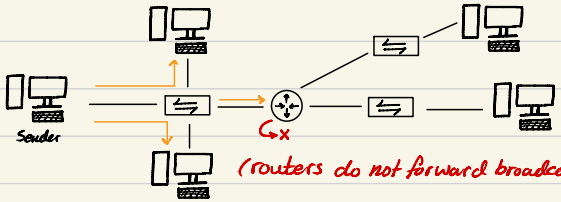
Or



→ Unicast to multiple hosts takes up high bandwidth & is slower



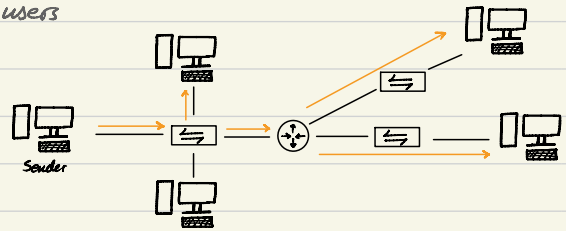
2- Broadcast: to all hosts on the subnet.



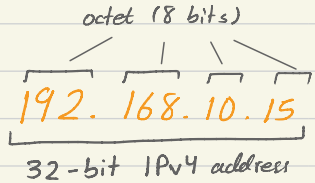
(routers do not forward broadcast traffic)

3- Multicast: to multiple interested hosts.

→ one copy is sent to multiple users (unlike unicast to multiple hosts)



* IPv4 address:
  - → 32 bits long
  - → written as 4 "octets"
  - → Eeach octet is 8 bits long



The IP address is usually set manually on servers, printers and network devices such as routers and switches. It is usually assigned automatically through the Dynamic Host Configuration Protocol (DHCP) on desktop computers.

* Each octet has a value ranging from 0 to 255.

IPv4 (Decimal)		IPv4 (Binary)
0 . 0 . 0 . 0	=	00000000.00000000.00000000.00000000
192.168. 10 . 15	=	11000000 . 10101000 . 00001010 . 00001111
255.255.255.255	=	11111111 . 11111111 . 11111111 . 11111111

* a host can send traffic directly to another host on the same subnet via switches.
* for a host to send traffic to another subnet, it must be forwarded via routers.
* The host needs to understand if the destination is on the same or different subnet.
  - → this can be done using a Subnet mask.
* The subnet mask is also 32 bits long.
  - → it can be written in a dotted decimal or slash notation.

* How the subnet mask is compaired with the IP acddress:

example:

decimal
- IPv4: 192.168.10.15
- subnet mask: 255.255.255.0

convert ↓

binary
- IPv4: 11000000 . 10101000 . 00001010 . 00001111
- subnet mask: 11111111 . 11111111 . 11111111 . 00000000

in the subnet mask:

1 → Part of the network address (fixed)

0 → host address (variable)

network portion | host portion

11000000 . 10101000 . 00001010 . 00001111

∴

11111111 . 11111111 . 11111111 . 00000000

If the two IP adresses' network portion match → they are on the same network.

* The subnet mask is alwasy a block of 1s followed by a block of 0s
* The host portion should be unique for each host on the subnet.

* Slash notation:

255.0.0.0 → <IP>/8

255.255.0.0 → <IP>/16

255.255.255.0 → <IP>/24

* IP adresses classes :

When IPv4 was created, designers didn't realise how big the internet was going to get.
So, they didn't create a big enough address.
Therefore, IPv6 was created with a much bigger address space.

- Class A : 1.0.0.0/8 to 126.255.255.255/8 (large Networks)
  → The first bit is always set to 0.
  ∴ this allows for 126 networks and 16,777,214 hosts per network.

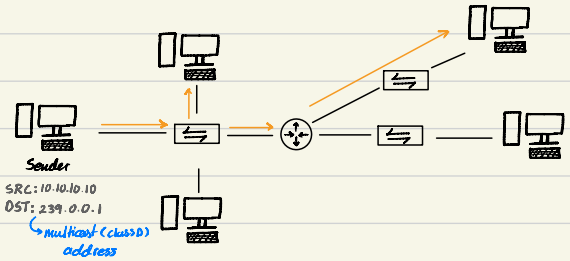
Reserved address	Reason
0.0.0.0/8	signifies "this network"
0.xxx.xxx.xxx	not valid host addresses
127.0.0.0/8	loopback address (for testing local computer)
127.xxx.xxx.xxx	not valid host adresses

∴ this wipes out 33,554,428 addresses from the global address pool.

- Class B : 128.0.0.0/16 to 191.255.255.255/16 (Medium to larger networks)
  → first two bits are 10 always.
  ∴ this allows for 16,384 networks and 65,534 hosts per network.

- Class C : 192.0.0.0/24 to 223.255.255.255/24 (small networks)
  → first three bits are always 110
  ∴ this allows for 2,097,152 networks and 254 hosts per network.

- **Class D:** 224.0.0.0 to 239.255.255.255 (for IP Multicast addresses)
  - → first four bits are always 1110
  - → these addresses are not allocated to hosts
  - → there is no default subnet mask.



- **Class E:** 240.0.0.0 to 255.255.255.255 (experimental / reserved for future use)
  - → first four bits are always 1111
  - → 255.255.255.255 is the broadcast address for "this network".
  - → there is no default subnet mask.

*IP address classes recap:

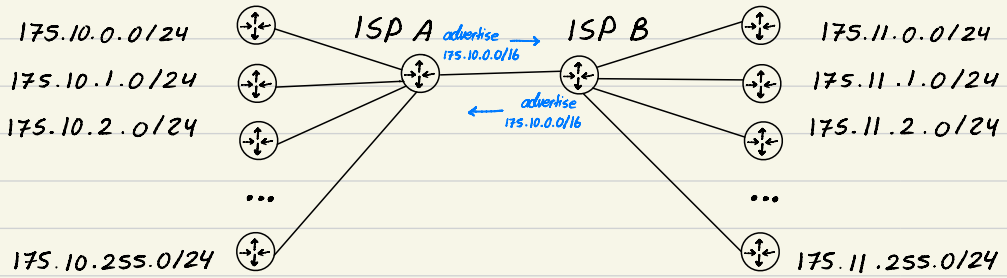
Class	first octet	default subnet mask	
		slash	decimal
A	1 - 126	/8	255.0.0.0
B	128 - 191	/16	255.255.0.0
C	192 - 223	/24	255.255.255.255
D	224 - 239	none	none
E	240 - 225	none	none

A problem with classful address was that if a company had more than 254 hosts they would need to be assigned to class B. This could waste a huge amount of the global address space since class C takes up to 254 hosts and class B takes up to 65,534 hosts.

→ Classless Inter-Domain Routing (CIDR) fixes this problem.

* **CIDR:** removed the fixed /8, /16, /24 requirements for the address classes, and allowed them to be split ("Subnetted") into smaller networks.
  → the company can allocate address range which matches their needs so they don't waste address. For example: 175.10.10.0 /20.
  → this way an ISP can give a limitted number of IPs to a company and save the rest for others.

* **Route Summerization:** a benifit of CIDR is that aggregate blocks of networks can be advertised on the internet.



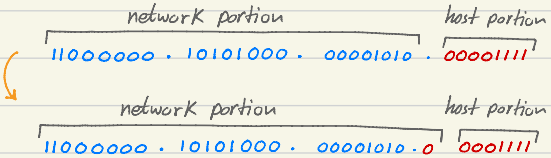
→ this way ISP A does not know about all 256/24 networks reachable on ISP B. Only the single 175.11.0.0/16 summary route.
→ this reduces the size of ISP A's routing table and saves memory.
→ if an individual link in ISP B goes down, it has no impact on ISP A. The single summary rout does not change.

Subnetting:

For companies with multiple departments on different offices.

Instead of purchasing seperate address range for the different departments, purchase one range and subnet it into smaller portions.

→ to do that, we would borrow bits from the host portion of the IP and add them to the network portion.



the more bits borrowed, the more subnets we will have of that size but less hosts.

* Calculating the number of subnets: $2^{\text{subnet bits}}$
* Calculating the number of hosts: $2^{\text{host bits}} - 2$ → network address & broadcast address

example 1:

if a class C network uses a /28 subnet mask:

We have borrowed 4 bits (from the original /24) → Class C subnet mask

∴ number of subnets = 2^4 = 16 subnets

We have 4 bits left for hosts

∴ number of hosts = $2^4 - 2$ = 14 hosts

example 2:

if a class B network uses a /28 subnet mask:

We have borrowed 12 bits (from the original /16) → Class B subnet mask

∴ number of subnets = 2^{12} = 4096 subnets

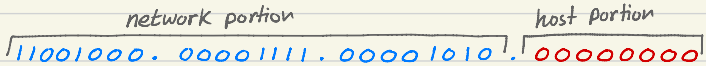
We have 4 bits left for hosts

∴ number of hosts = $2^4 - 2$ = 14 hosts

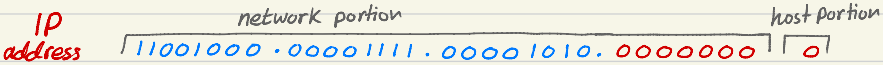
* Hosts on different subnets communicate with each other using a router. (as if they are on different networks)

* Subnetting Class C networks:

→ lets say we have been allocated Class C 200.15.10.0/24

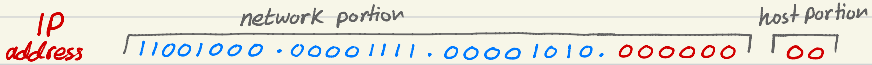


→ C/31 subnet (255.255.255.254)



this leaves one bit for the host address with a possible value of 0 or 1.
it borrows 7 bits for the network address.
∴ number of subnets = 2^7 = 128 & number of hosts = 2 (didn't subtract 2 (/31 is an exception))

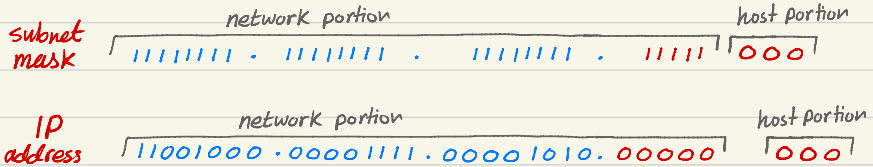
→ C/30 subnet (255.255.255.252)



this leaves two bits for the host address with 2^2 possible values
it borrows 6 bits for the network address.
∴ number of subnets = 2^6 = 64 & number of hosts = $2^2 - 2 = 2$

* In the CCNA exam, use /30 when a subnet supports 2 hosts, unless told to use /31 *

→ C/29 subnet (255.255.255.252)



this leaves 3 bits for the host address with 2^3 possible values
it borrows 5 bits for the network address.
∴ number of subnets = $2^5 = 32$ & number of hosts = $2^3 - 2 = 6$

→ C/28 (255.255.255.240)
16 networks, 14 hosts each

→ C/27 (255.255.255.224)
8 networks, 30 hosts each

→ C/26 (255.255.255.192)
4 networks, 62 hosts each

→ C/25 (255.255.255.128)
2 networks, 126 hosts each

→ C/24 (255.255.255.0) default C class network
1 network, 254 hosts each

* Variable Length Subnet Mask (VLSM):

→ Early routing protocols supported fixed length subnet masking (FLSM), all subnets had to be the same size.

→ Modern routing protocols support variable length subnet masking (VLSM), this allows us to size subnets differently according to how many hosts they have.

* Subnetting practice questions:

Q1) What are network, broadcast, and valid host addresses for the IP: 198.22.45.173/26

network address: 198.22.45.?, last octet: 173 = 1 0 1 0 1 1 0 1 (network: 1 0 | host: 1 0 1 1 0 1), 10000000 = 128

(128 64 32 16 8 4 2 1)

∴ network address: 198.22.45.128

broadcast address: (host portion all 1s) last octet 1 0 1 1 1 1 1 1 (network: 1 0 | host: 1 1 1 1 1 1), 10111111 = 191

∴ broadcast address: 198.22.45.191

Valid host addresses: from the network (excluded) to the broadcast (excluded) address

∴ Valid host addresses: 198.22.45.129 to 198.22.45.190

Q2) What is the subnet mask in dotted decimal notation?

in the last octet: 11000000 (since it borrows 2 bits from the host) = 192 in decimal

∴ the subnet mask is 255.255.255.192

* Subnetting considerations:

1- How many locations do we have in the network?

2- How many hosts are in each location?

3- What are the IP addressing requirements for each location?

4- What size is appropriate for each subnet?

* Subnet design tips:

1- Find the largest segment and allocate a suitable subnet size for it.

2- Allocate this subnet at the start of the address space.

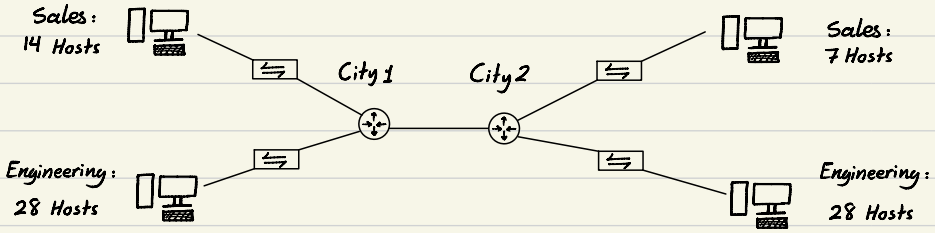
3- Continue going down the list.

Note: in the real world, you want a scalable size (allocate spare subnets for future growth).

in the CCNA exam, do exactly what the question asks (don't worry about best practice).

Subnetting Example

allocated: class C network 200.15.10.0/24



note: router interfaces also needs IP addresses.

note: point to point links (between routers) also needs IP addresses.

network | host

11001000.00001111.00001010.00000000

1- Calculate the optimal subnet mask for the engineering departments:

if we make it /27 (borrow 3 bits from host) → $2^5 - 2 = 30$ hosts

City 1 Engineering subnet — network: 11001000.00001111.00001010.000 | host: 00000

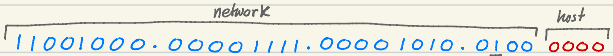
- → network address: 200.15.10.0/27 — ...000 00000
- → broadcast address: 200.15.10.31 — ...000 11111
- → hosts addresses: 200.15.10.1 to 200.15.10.30 — ...00000001 to ...00011110

City 2 Engineering subnet — network: 11001000.00001111.00001010.001 | host: 00000

- → network address: 200.15.10.32/27 — ...001 00000
- → broadcast address: 200.15.10.63 — ...001 11111
- → hosts addresses: 200.15.10.33 to 200.15.10.62 — ...00100001 to ...00111110

2 - Calculate the optimal subnet mask for City 1's Sales department:

if we make it /28 (borrow 4 bits from host) → $2^4 - 2 = 14$ hosts



City 1 Sales subnet

- → network address: 200.15.10.64 — ... .0100 0000
- → broadcast address: 200.15.10.79 — ... .0100 1111
- → hosts addresses: 200.15.10.65 to 200.15.10.78 — ... .01000001 to ... .01001110

3 - Calculate the optimal subnet mask for City 2's Sales department:

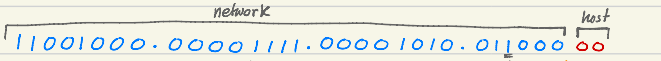
if we make it /29 (borrow 5 bits from host) → $2^3 - 2 = 7$ hosts

City 2 Sales subnet

- → network address: 200.15.10.80 — ... .01010 000
- → broadcast address: 200.15.10.95 — ... .01010 111
- → hosts addresses: 200.15.10.81 to 200.15.10.94 — ... .01010001 to ... .01010110

4 - Calculate the optimal subnet mask for point to point links (City 1 & City 2 routers):

if we make it /30 it will support 2 hosts

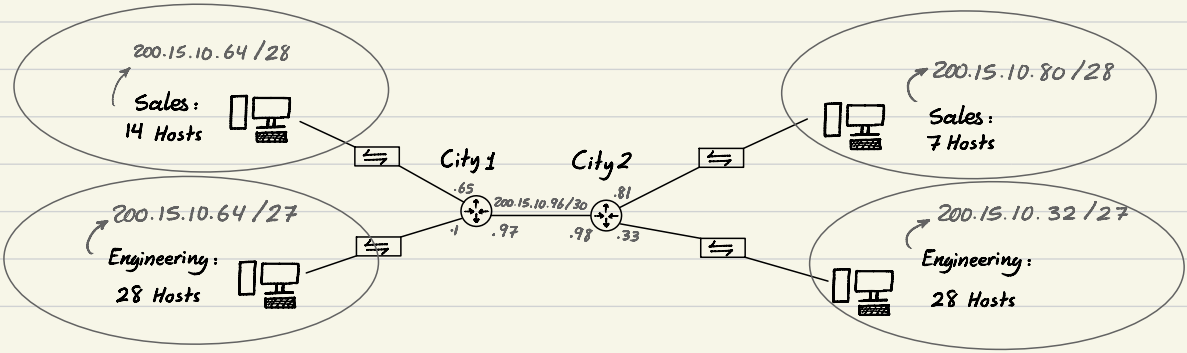


Point to Point subnet

- → network address: 200.15.10.96/30 — ... .011000 00
- → broadcast address: 200.15.10.99 — ... .011000 11
- → hosts addresses: 200.15.10.97 to 200.15.10.98 — ... .01100001 to ... .01100010

Solution:

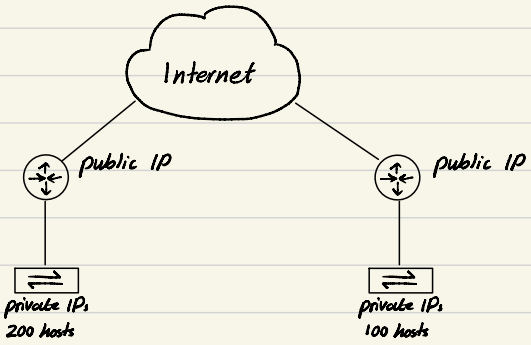
class C network 200.15.10.0/24



* **Private IP addresses (RFC 1918):** not directly connected to the internet.
  → hosts on different network can have the same private addresses.

* **IPv4 global address space problem:**
  → designers of IPv4 did not expect the explosive growth of its use.
  → 4.3 billion addresses seemed to be more than enough to them at that time.
  → to solve this, IPv6 was developed where it has 128 bit instead of 32.
  → there is no seamless migration path from IPv4 to IPv6.
  → NAT (Network Access Translation) was implemented as a temporary solution.

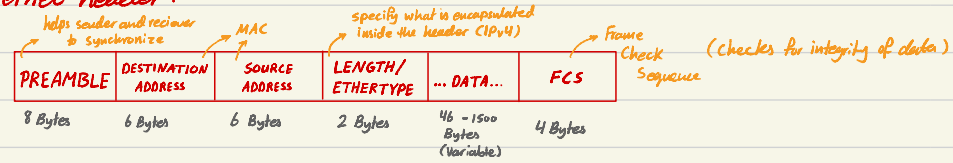
* **NAT:** (current solution)
  → An organization can use private addresses on their inside network and can access the internet by translating them to their outside public IP address.
  → Many hosts on the inside can share one public IP address.



Layer 2 (Data-Link):

* Layer 2 encodes and decodes frames into bits to be ready to be put on the physical wire.
* Error detection and correction for the physical layer can be provided here.
* Ethernet is the medium used on LANs.

* Ethernet header:



* MAC address: 48-bit Hexadecimal address used by Ethernet
  - → The first 24 bits is the OUI (Organizationally Unique Identifier) which uniquely identifies the manufacturer.
  - → The last 24 bits is vendor assigned
  - → The burned in MAC address on every NIC port in the world is globally unique.

Layer 1 (Physical):

* Layer 1 conveys the bit stream at the electrical and mechanical level.
* Ethernet LAN connections can be carried over coaxial cable (no longer used), twisted copper cable, fiber cable or wireless.

Copper:

* Copper UTP cables are commonly used to connect computers to switches.
* Straight-through: connect an end device (PC to switch)
* Crossover: connects devices together (PC to PC)
* Modern switches support auto MDI-X where the receive and transmit signals are reconfigured automatically.

Fiber:

* Fiber optic cables can be used to support longer distances.
* Single mode: supports higher bandwidth and longer distances but is more expensive.
* Multi mode: supports lower bandwidth and shorter distances and is less expensive.

* PoE (Power over Ethernet): can be used to transmit power through the Ethernet port.