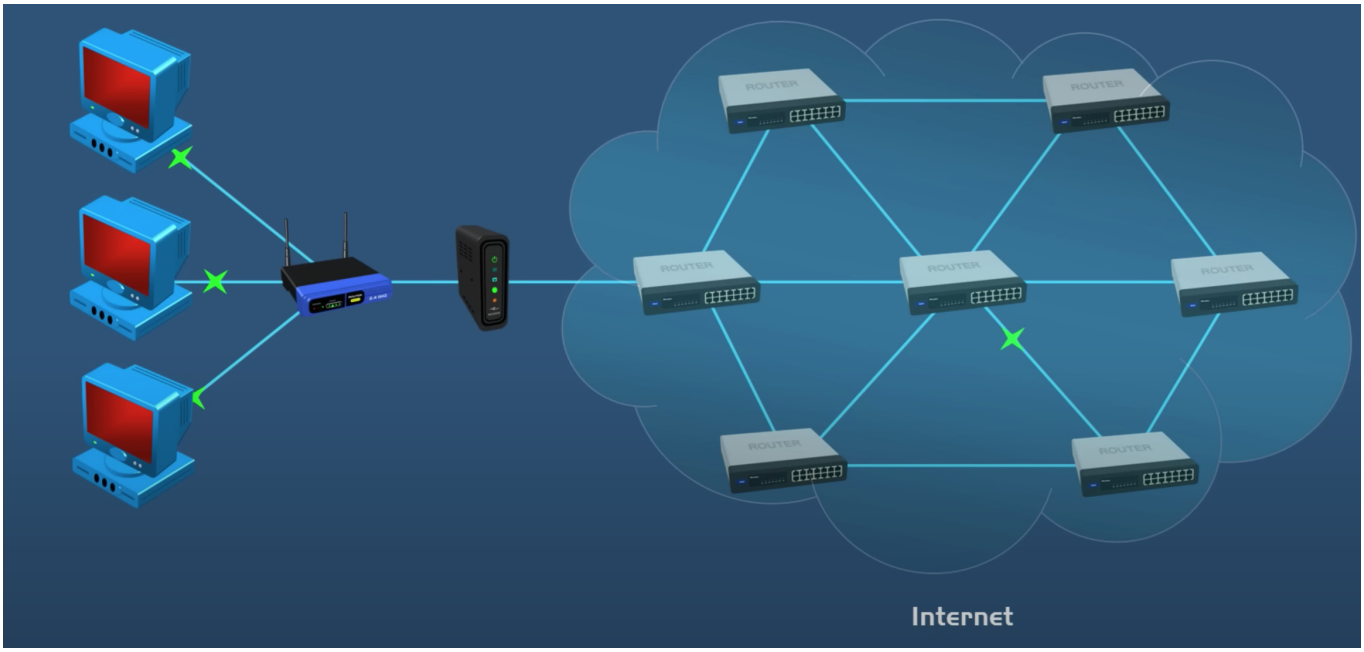
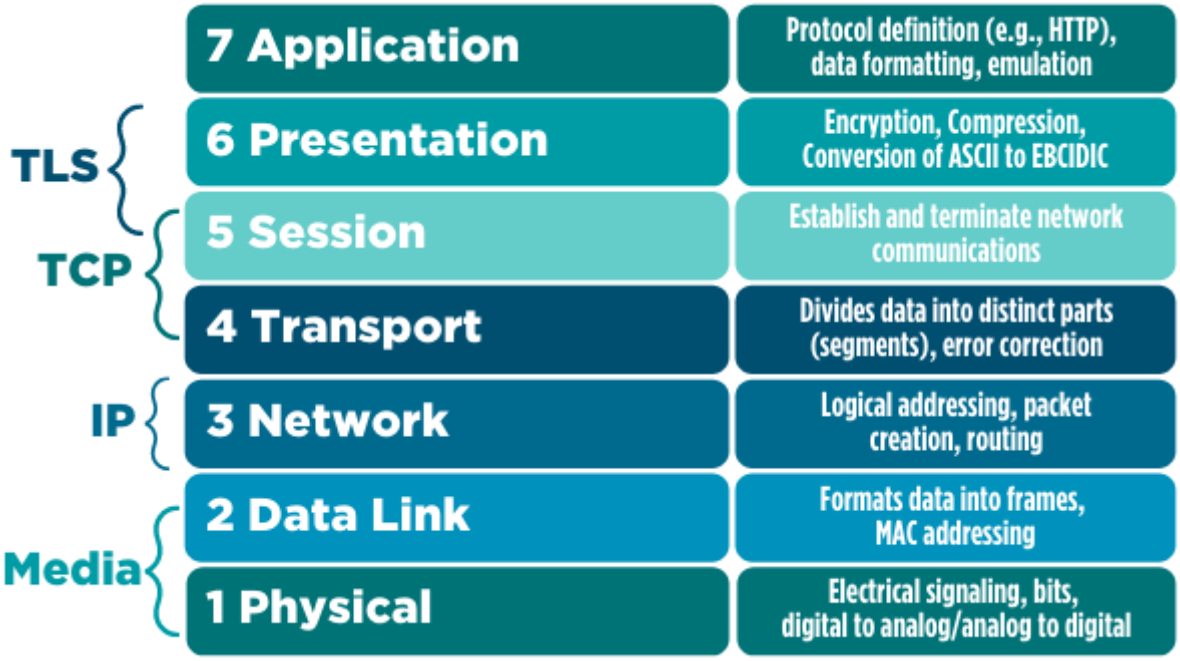


OSI Model

Open Systems Interconnection
that standardizes and defines how different computer systems can communicate with each other over a network. It provides a logical structure and a common language for understanding and designing network protocols and systems. Overall, the OSI model provides a structured approach to network communication by dividing the process into distinct layers, each handling specific tasks.

1. Physical Layer: The physical layer deals with the physical aspects of network communication, such as transmitting and receiving raw data over the physical medium (wires, cables, radio waves, etc.).
2. Data Link Layer: The data link layer handles the reliable transfer of data frames between directly connected devices. It provides error detection, flow control, and access control to the physical medium.
3. Network Layer: The network layer is responsible for addressing, routing, and forwarding data packets across multiple networks. It determines the best path for data transmission and manages logical network addressing.
4. Transport Layer: The transport layer ensures the reliable and efficient delivery of data between two hosts. It manages end-to-end communication, segments and reassembles data, and handles error detection and correction.
5. Session Layer: The session layer establishes, manages, and terminates communication sessions between applications on different hosts. It sets up connections, coordinates data exchange, and provides synchronization and recovery mechanisms.
6. Presentation Layer: The presentation layer handles data representation and formatting. It ensures that data from different systems can be interpreted correctly by converting it into a compatible format.
7. Application Layer: The application layer contains the protocols and services that directly interact with end-user applications. It provides a communication interface for various applications, such as web

browsers, email clients, file transfer, and more.



Modem vs Router

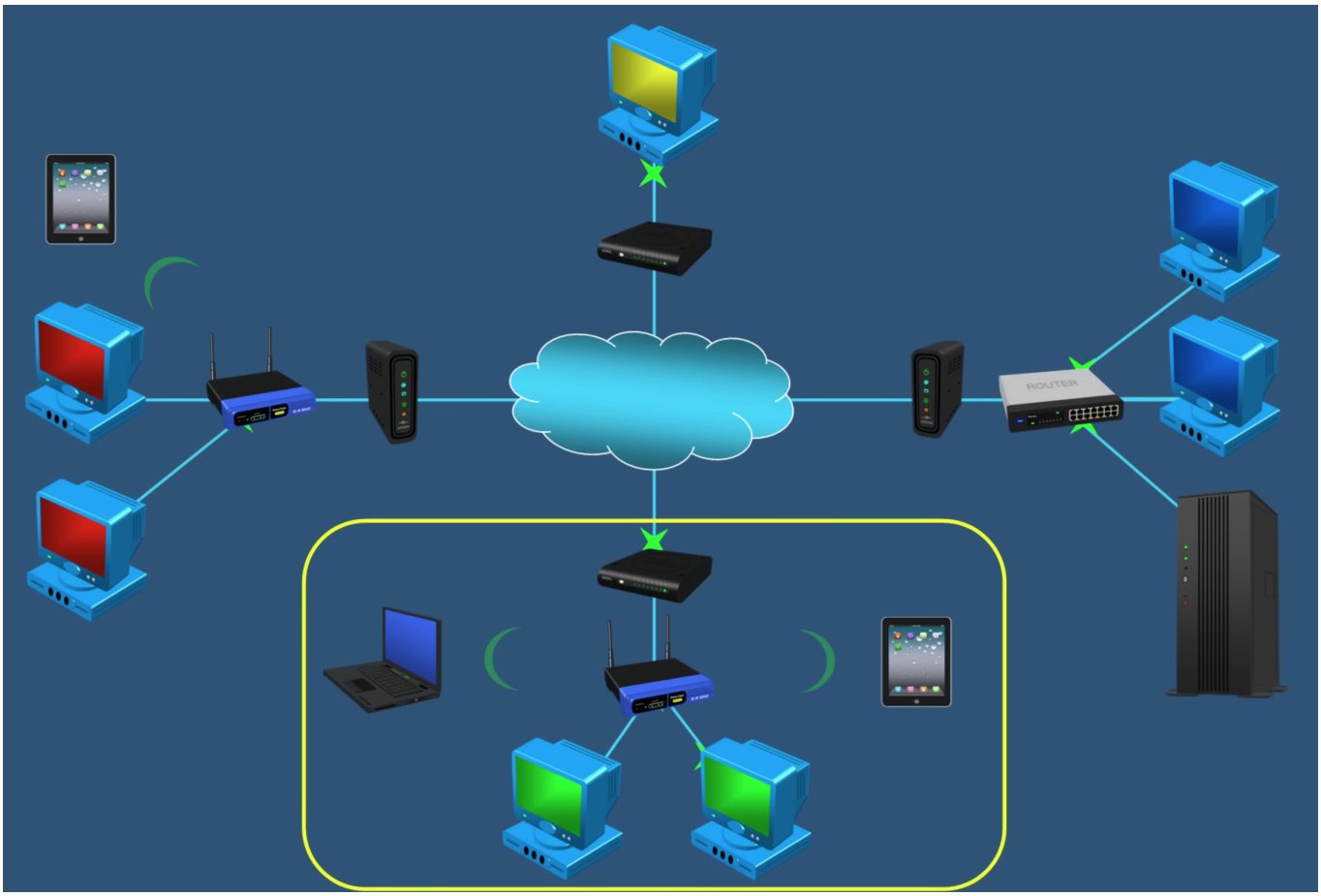
modem: modulator / demodulator

A modem, short for modulator-demodulator, is a device that enables communication between a computer or network and an Internet service provider (ISP) or a telephone line. It converts digital signals from a computer or network into analog signals that can be transmitted over telephone lines, cable lines, fiber optic lines, or wireless networks. Similarly, it also converts analog signals received from the network into digital signals that computers can understand.

two types of modems: Cable modems (connecting with coaxial cables) & DSL modems (connecting with phone line)
a lot of times we use a modem+router combination device:

router

A router is a networking device that connects **multiple networks** together and directs network traffic between them.
Technically, you don't need a router if you only want one of your devices to access the internet.
A router operates at the network layer (Layer 3) of the OSI model and is responsible for forwarding data packets across networks based on their destination IP addresses. there can be different networks with different router/modem combinations/types:



what is the difference between hub, switch and router?

hub

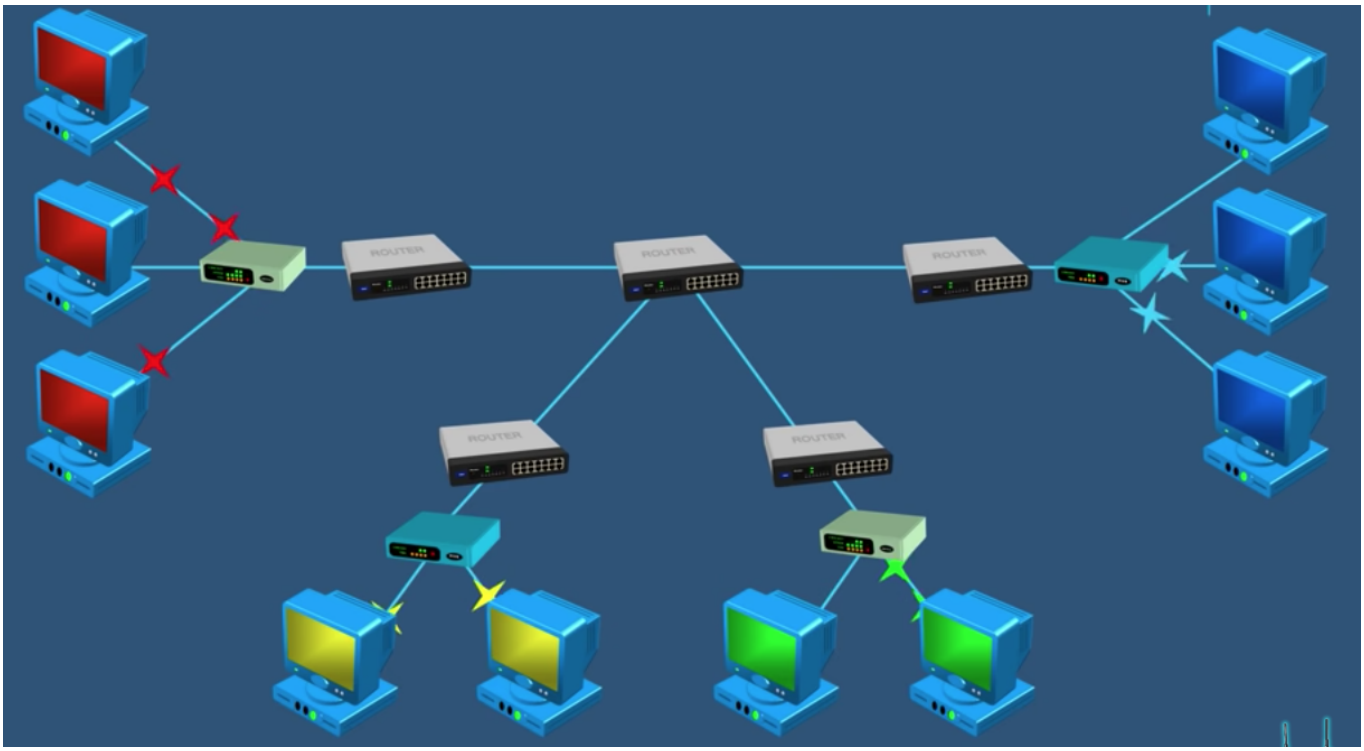
A hub is a simple networking device that connects multiple devices in a network. It has multiple ports that accepts ethernet connection from other network devices. It operates at the physical layer (Layer 1) of the OSI model and is primarily responsible for broadcasting incoming data packets to all connected devices. However, it lacks the intelligence and advanced features of more modern networking devices like switches and routers. Like a data sharing drive in a company.

switch

A switch is a networking device that connects multiple devices within a local area network (LAN). It operates at the data link layer (Layer 2) of the OSI model and is responsible for efficiently forwarding data packets between devices within the same network. Unlike a hub, a switch intelligently directs traffic only to the intended recipient rather than broadcasting it to all connected devices.

router

it routes (forwards) data from one network to another based on their IP addresses. nether hub nor switch is capable of connecting to other networks and they only function in a local area network (they cannot read IP addresses.)
a router only accepts to send and receive data packets that are for the specific IP addresses.



Wireless access point (WAP) vs WiFi router

WAP

A WAP (Wireless Access Point) is a networking device that enables wireless communication between devices and a wired network. It acts as a central hub for wireless devices, and connects the devices in different points through a single router to the internet. WAP itself is not a router. (used by companies mostly to cover the area for wifi access)

difference?

But Wifi routers are routers and if a company uses multiple wifi routers to cover the access to wifi, it would be hard to configure such network, because every router should be configured independently, there would be multiple subnetting.

TCP

Transmission Control Protocol is one of the core protocols of the Internet protocol suite, commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of data packets over a network, such as the Internet.

TCP operates at the *transport layer* of the TCP/IP model and is responsible for breaking data into smaller units called packets and reassembling them at the destination. It ensures that data sent from one device (sender) reaches the intended device (receiver) accurately and in the correct order.

IP

The IP protocol operates at the network layer (Layer 3) of the OSI model and is responsible for addressing, routing, and fragmenting data packets. It enables devices to communicate with each other across different

networks, regardless of the underlying physical network technology.

IP address

An IP address, short for Internet Protocol address, is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two primary functions: identifying the host or network interface and providing the location of the device in the network.

IP addresses are essential for facilitating communication between devices on the internet. They enable data packets to be sent and received across networks by specifying the source and destination of the information.
IP

An IP address has two parts; one part identifies the *host* such as a computer or other device, and the other part identifies the *network it belongs to*. TCP/IP uses a subnet mask to separate them.

IPv4

32 bit numeric address, (4 Octets)

- produces over 4 B unique addresses
- computers understand IP addresses only binary numbers

IPv6

128 bit hexadecimal address

- produces over 340 undecilion addresses (340 X 10^36)

Public IP address

when you order internet service from ISP, they are going to assign your modem or your router a public IP address. This public IP address is registered on the internet, its what gives you the access to the world wide web. So if you dont have public IP address, you cannot access the internet.
Public IP addresses are unique.

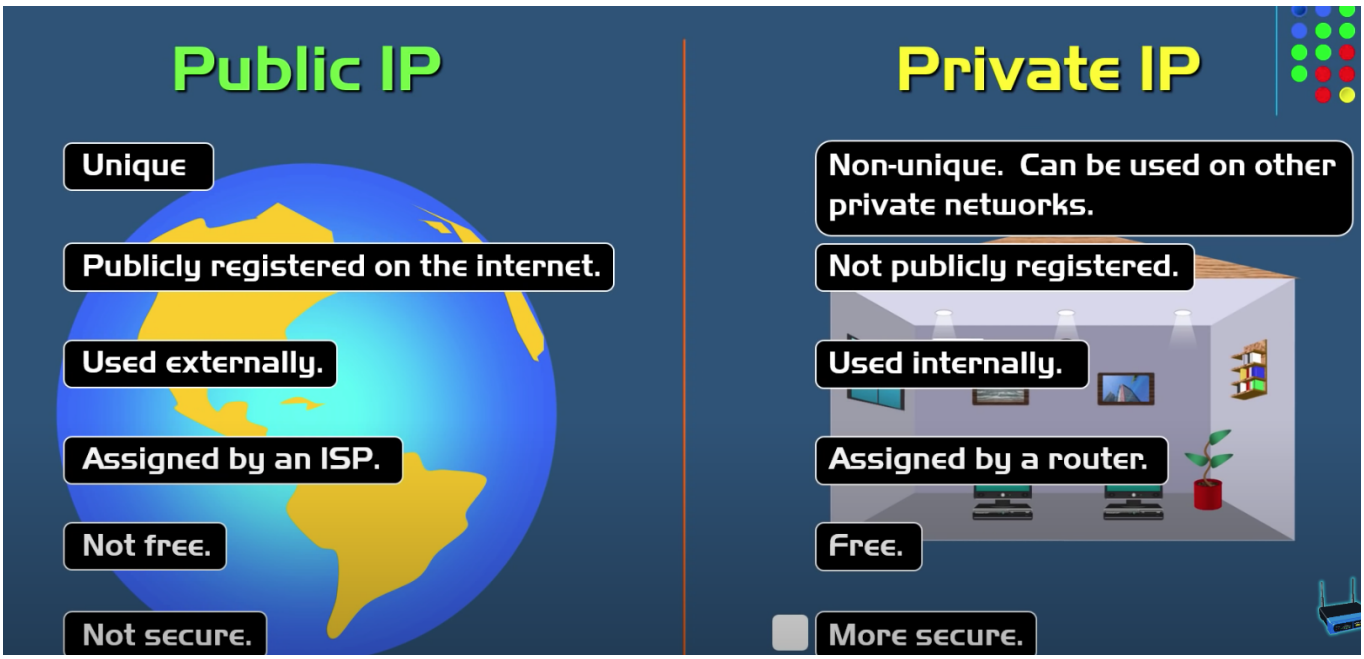
Private IP addresses

Private IP addresses are not publicly registered on the internet. so you cant access the internet via a private IP. if your device has a private IP address and you want to connect to the internet, your private IP needs to be converted into a public IP address before you can access internet. and this is because private IP addresses are only used internally. and a service that is inside your router called DHCP assigns your internal devices a private IP address. NAT (network address translation) is a service that translates a set of IP addresses to another set of IP addresses.

Private IP addresses have three different classes:

CLASS	IP ADDRESS RANGE	DEFAULT SUBNET MASK
A	10.0.0.0 – 10.255.255.255	255 . 0 . 0 . 0
B	172.16.0.0 – 172.31.255.255	255 . 255 . 0 . 0
C	192.168.0.0 – 192.168.255.255	255 . 255 . 255 . 0

the difference between public and private:



special IP addresses

The following special address-ranges are reserved for Private Networks:
`10.0.0.0 – 10.255.255.255`
`172.16.0.0 – 172.31.255.255`
`192.168.0.0 – 192.168.255.255`

The following address-range is reserved for so called loopback addresses:
`127.0.0.0 – 127.255.255.255`

There is some more special ip-ranges, but for this project, you only need to remember those above.

DNS

domain name system
resolves names (domain names) to numbers(IP addresses)

Subnet Mask

A subnet mask is a 32-bit number used in conjunction with an IP address to divide an IP network into subnetworks or subnets. It is used to determine the network and host portions of an IP address, allowing for proper routing of data packets within a network.

When a device wants to send data to another device, it performs a logical AND operation between the IP address and the subnet mask. This operation reveals the network portion of the IP address. By comparing the network portion of the source and destination IP addresses, the device can determine if the destination is on the same local network or if it needs to be routed to another network.

Subnet masks allow for efficient network management by partitioning IP networks into smaller subnets. This segmentation provides better organization, improved security, and more efficient routing within a larger network infrastructure.

what is network IP address?

The network IP is significant for various purposes, such as routing. When devices communicate with each other, they compare the network portion of their IP addresses to determine if they are on the same network or if routing to another network is required. The network IP helps define the boundaries of a network and serves as a reference point for routing decisions.

It's worth noting that the network IP address, represented by the network portion of the IP address, is typically reserved and not assigned to any specific device. It is used to identify the network as a whole and differentiate it from other networks in the same IP address space.

CIDR Notation (/24)

The mask can also be represented with the Classless Inter-Domain Routing (CIDR). This form represents the mask as a slash "/", followed by the number of bits that serve as the network address.

Therefore, the mask in the example above of `255.255.255.128`, is equivalent to a mask of `/25` using the CIDR notation, since 25 bits out of 32 bits represent the network address.

Subnetting

taking one network and dividing it into smaller subnetworks.
Subnetting is the process of dividing a larger network into smaller, more manageable subnetworks called subnets. It involves partitioning a network's IP address space to create separate segments, each with its own unique network address. Subnetting provides several benefits, including improved network performance, efficient resource allocation, and enhanced network security.
for example taking a /24 network and dividing it to two /25 network

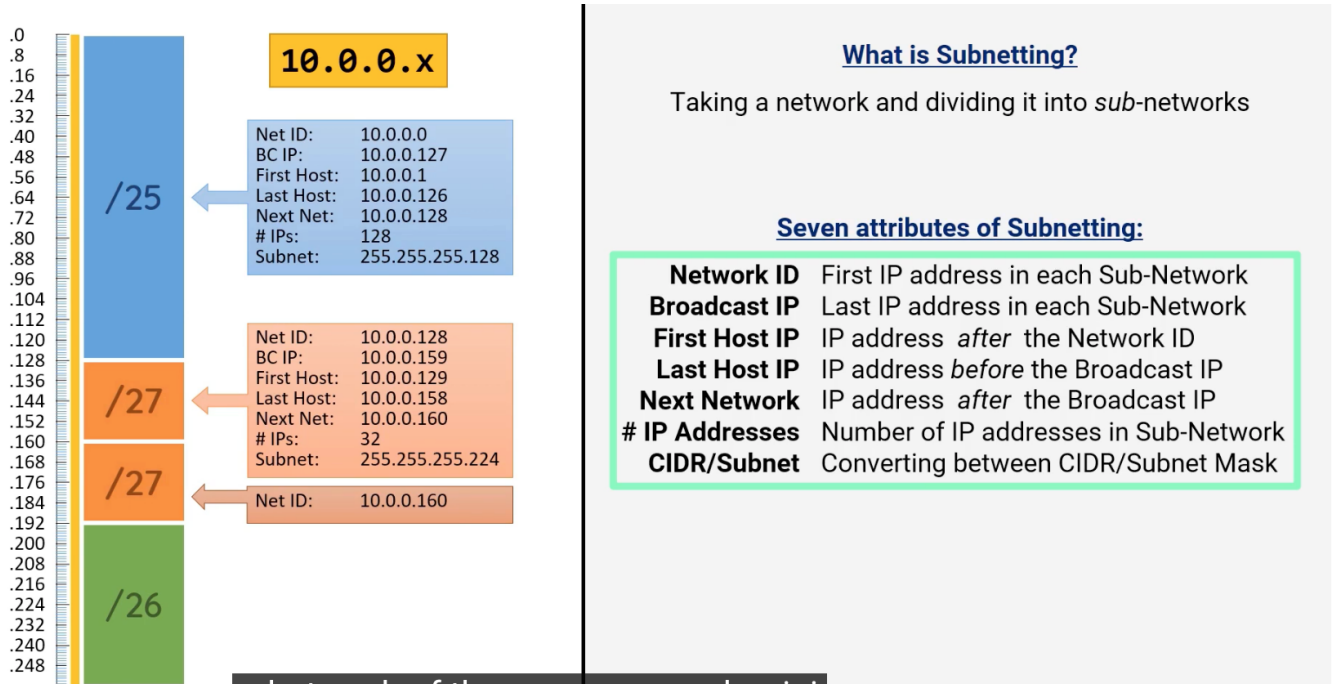
attributes of each subnet:

- network IP : first IP address in each sub network (cant be assigned to a host)
- broadcast IP : last IP address in each sub network (cant be assigned to a host)
- first host IP : IP address immediately after network ID
- last host IP : IP address immediately before broadcast IP
- next network : IP address after broadcast IP
- IP addresses : number of IP addresses in the subnet

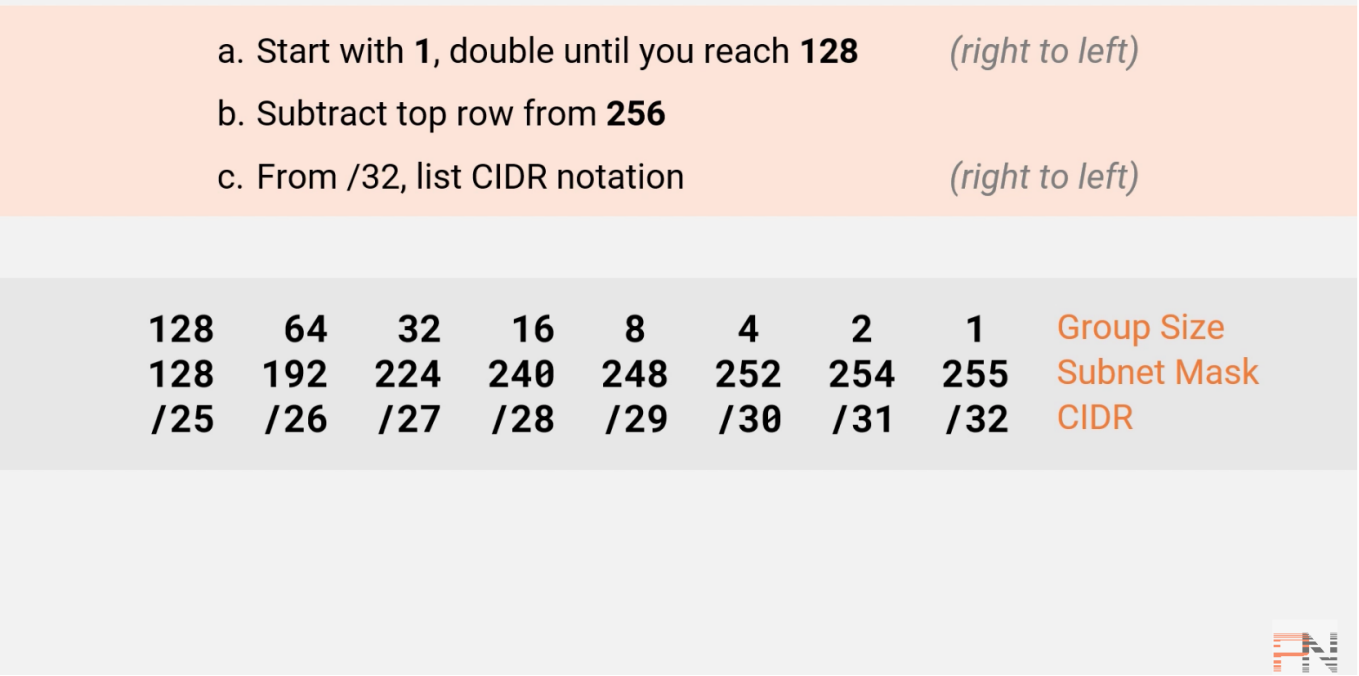
- CIDR/subnet mask

formula

all the one bits in the mask = IP address of network
2 ^ (number of zeroes of the mask) - 2 = number of host IPs



cheatsheet for subnetting



does the subnet mask of router and switch have to be the same?

No, the subnet mask of a router and a switch does not have to be the same. The subnet mask is a configuration parameter that determines the network and host portions of an IP address. While routers and

switches are both networking devices, they serve different purposes and operate at different layers of the network stack.

Routers primarily operate at the network layer (Layer 3) and are responsible for forwarding packets between different networks. They connect multiple networks together and facilitate the exchange of data between them. Routers use IP addresses and subnet masks to determine the network boundaries and make routing decisions.

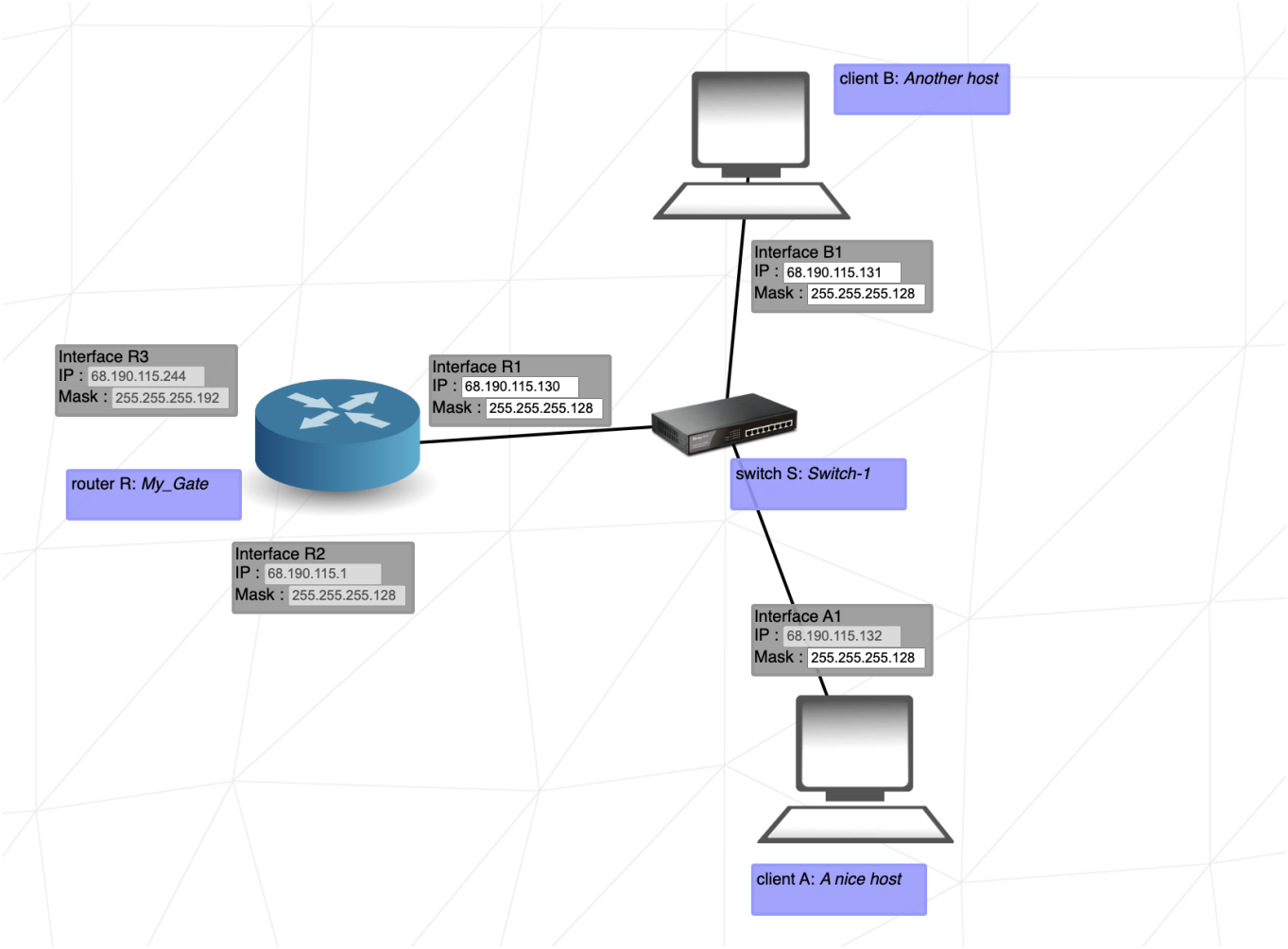
Switches, on the other hand, operate at the data link layer (Layer 2) and are responsible for facilitating communication between devices within a local network. They use MAC addresses to forward data packets within the same network segment. Switches do not typically perform routing functions and do not require subnet masks for their basic operation.

That said, both routers and switches can have IP addresses assigned to their management interfaces. These IP addresses allow administrators to access and configure the devices remotely. When assigning IP addresses to router or switch interfaces, it is recommended to use IP addresses that are within the same subnet to ensure they can communicate with each other.

While the subnet mask on the router and switch management interfaces can be the same for ease of management and communication, it is not a strict requirement. Each device can have its own unique subnet mask depending on the specific network configuration and requirements. The important consideration is that the IP addresses and subnet masks are properly configured to allow for connectivity and proper routing between the devices and networks they are connected to.

level 4

in this example, we wanna chose an interface that both hosts can connect.



by comparing IP of A1 we se it is not feasible for hostA to be part of subnets of interface R2 and R3, because R2 covers the IP ranges from 0 - 127 and R3 covers the IP ranges from 193 - 255, but our hostA's IP is 132 which is not fitting in any of these ranges.
so we need to cover the other remaining range in the R1: from 128 to 192 IP addresses should be covered here.
we will chose the wider mask, so that it allows for more IPs: 255.255.255.128
I guess the other mask in this case would be fine too.

and then we have our mask, we just assign some valid IPs in the range!

routing table

A routing table is a data structure maintained by a router or network device that contains information about the available routes in a computer network. It serves as a key component of the routing process, helping routers determine the best path for forwarding network traffic to its destination.

The routing table consists of a list of network destinations (IP addresses or network prefixes) and the corresponding next hop or outgoing interface for each destination. It provides the router with the necessary information to make forwarding decisions based on the destination IP address of incoming packets.

A routing table is a data table stored in a router or a network host that lists the routes to particular network destinations. In NetPractice, the routing table consists of 2 elements:

- **Destination**: The destination specifies a network address on which a host is the end target of the packets. The route of `default` or `0.0.0.0/0`, is the route that takes effect when no other route is available for an IP destination address. The default route will use the next-hop address to send the packets on their way without giving a specific destination. The default route will match any network.
- **Next hop**: The next hop refers to the next closest router a packet can go through. It is the IP address of the next router on the packet's way. Every single router maintains its routing table with a next hop address.

When a router receives a packet, it consults its routing table to determine the best route for forwarding the packet based on the destination IP address. The router matches the destination IP address with entries in the routing table and uses the associated next hop or outgoing interface to forward the packet accordingly.

level 5: how A and B communicate?

???

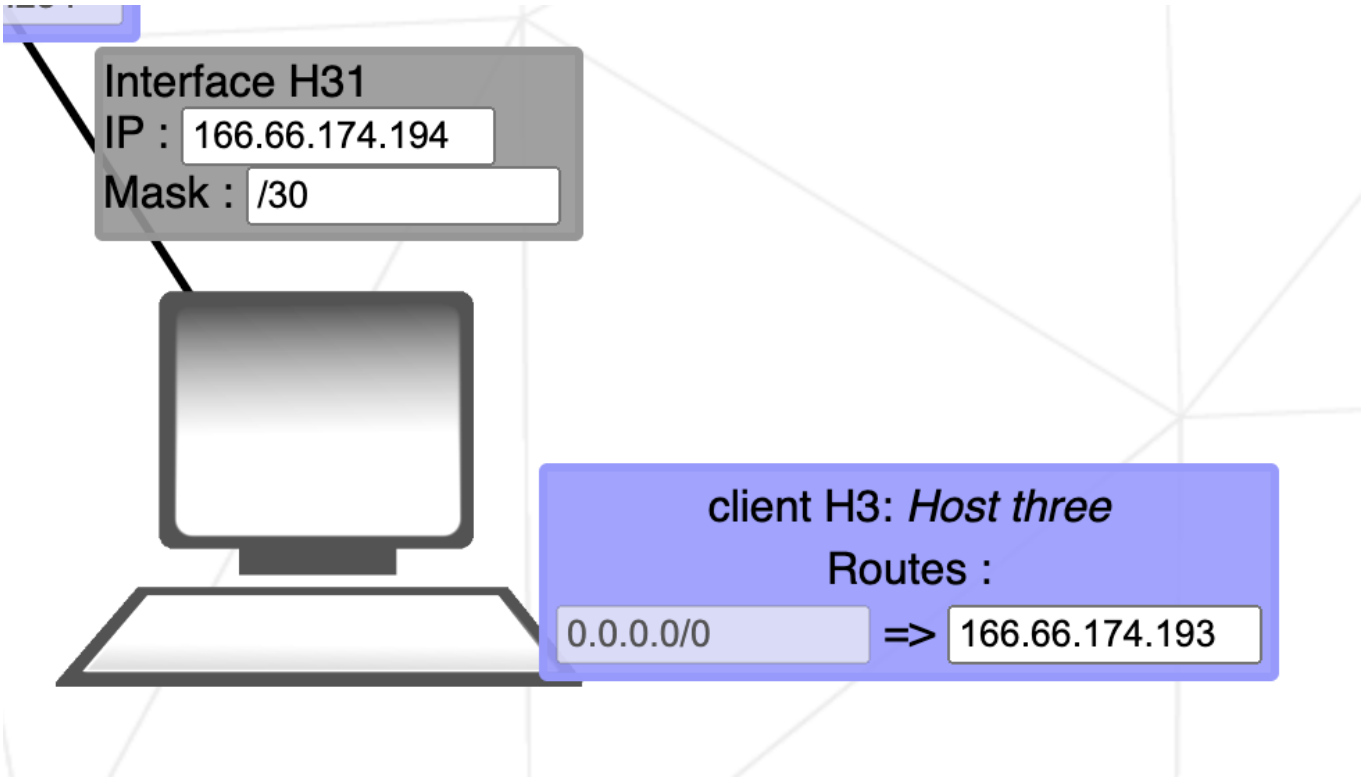
- what does the blue box do? apparently it is a routing table. so does it mean that the interface that has the blue box is a router and can rout packets?

All 4 of the Possible /26 Networks for 111.198.14.*

Network Address	Usable Host Range	Broadcast Address:
111.198.14.0	111.198.14.1 - 111.198.14.62	111.198.14.63
111.198.14.64	111.198.14.65 - 111.198.14.126	111.198.14.127
111.198.14.128	111.198.14.129 - 111.198.14.190	111.198.14.191
111.198.14.192	111.198.14.193 - 111.198.14.254	111.198.14.255

قوانین:
نتورک آدرس همیشه از هوست آدرس کوچیک تره. یعنی هوست از نتورک به بالا رو شامل می شه.
اگه ماسک ۲۶ داشته باشیم، یعنی می تونیم چهارتا سابنت درست کنیم.

در کل به دنبال چی هستیم ؟

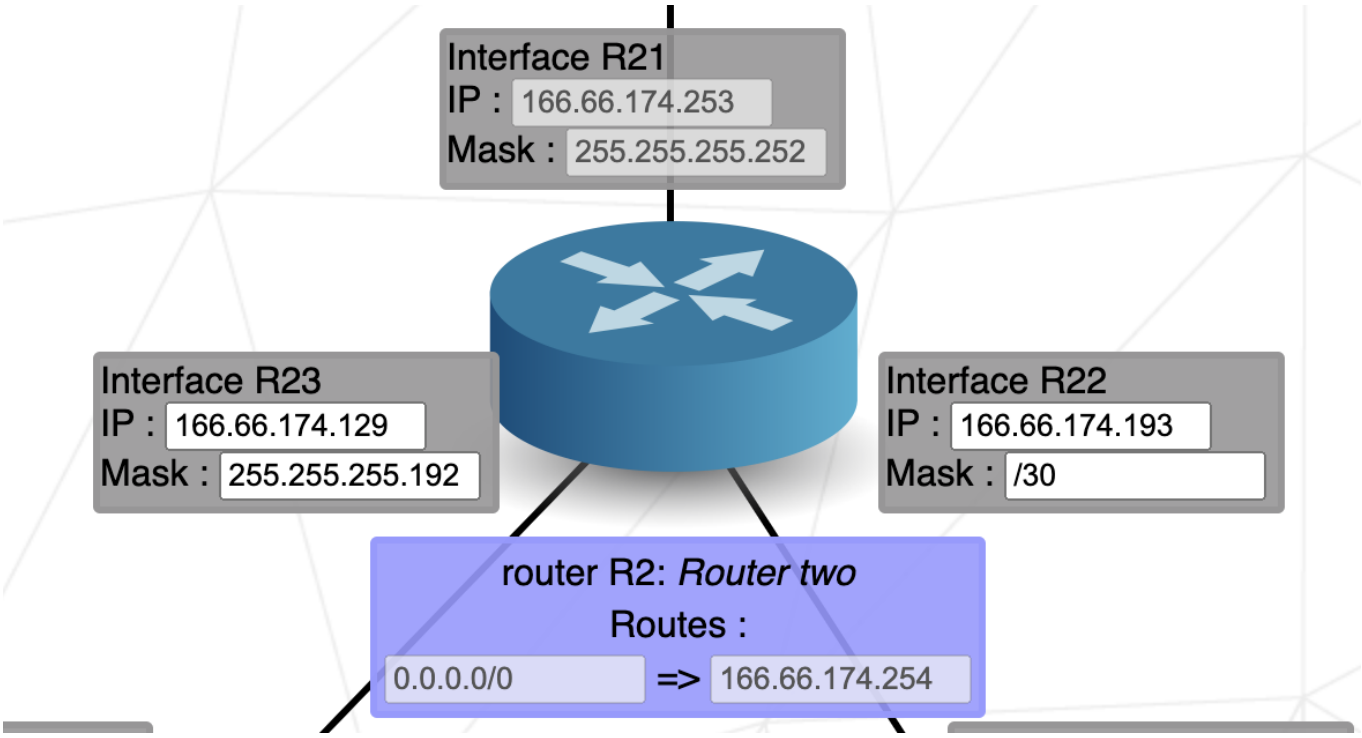


وقتی که مقصد یا همین عدد سمت چپ در destination. اینجا ما واحد هایی داریم که در خواست بهشون میدیم با یه آی پی، به نام آی پی مقصد یا جدول روتینگ با اینترفیسی تطابق نداشته باشه، هر ماشین یا روتر به جدول روتینگش نگاه می کنه تا ببینه چی رو کجا بفرسته. اگه درخواست مقصد عینا مشابه یک اینترفیس متصل به ماشین باشه اصلا این جدول چک نمی شه.

مثلا اینجا این می گی هر چی درخواست ای پی مقصد بود و یوزر هرکجا تو (چه تو نتورک چه تو اینترنت، هر ای پی ای) ارایه داد که توی مسیر اینترفیس های متصل به ماشین نبود، بیا ببرش به :

next hop: 166.66.174.193

و اصولا نکست هاب همون مسیر روتر متصل هست. یعنی از طریق این جدول اون پکت داده سوق داده می شه به روتر بعدی.

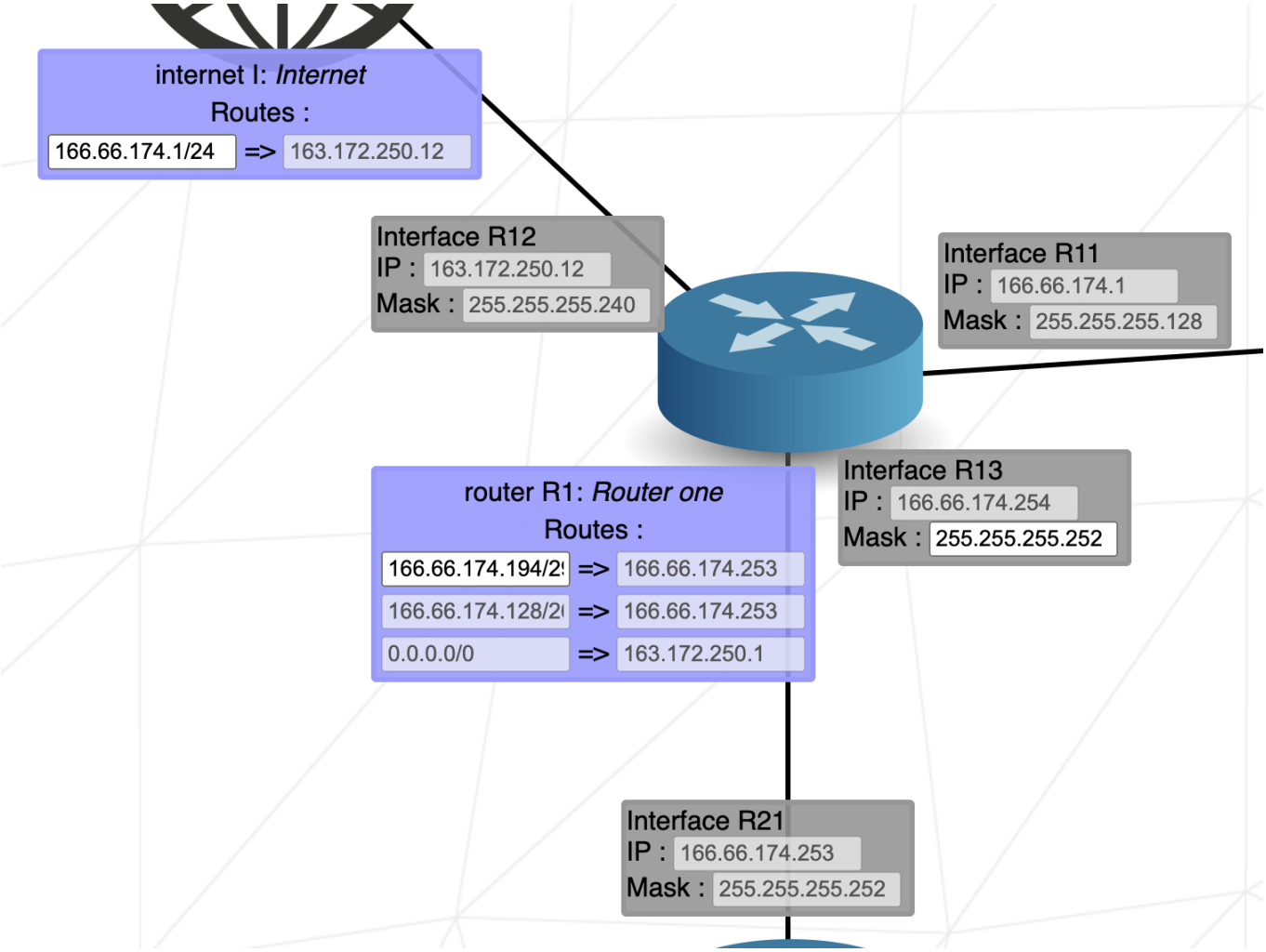


حالا این روتر چند تا مسیر بهش وصله. از کجا بدونه چی رو بفرسته کجا؟

.توی جدول روتینگش نگاه می کنه و از روی آی پی مقصد می فهمه هر چی رو کجا بفرسته

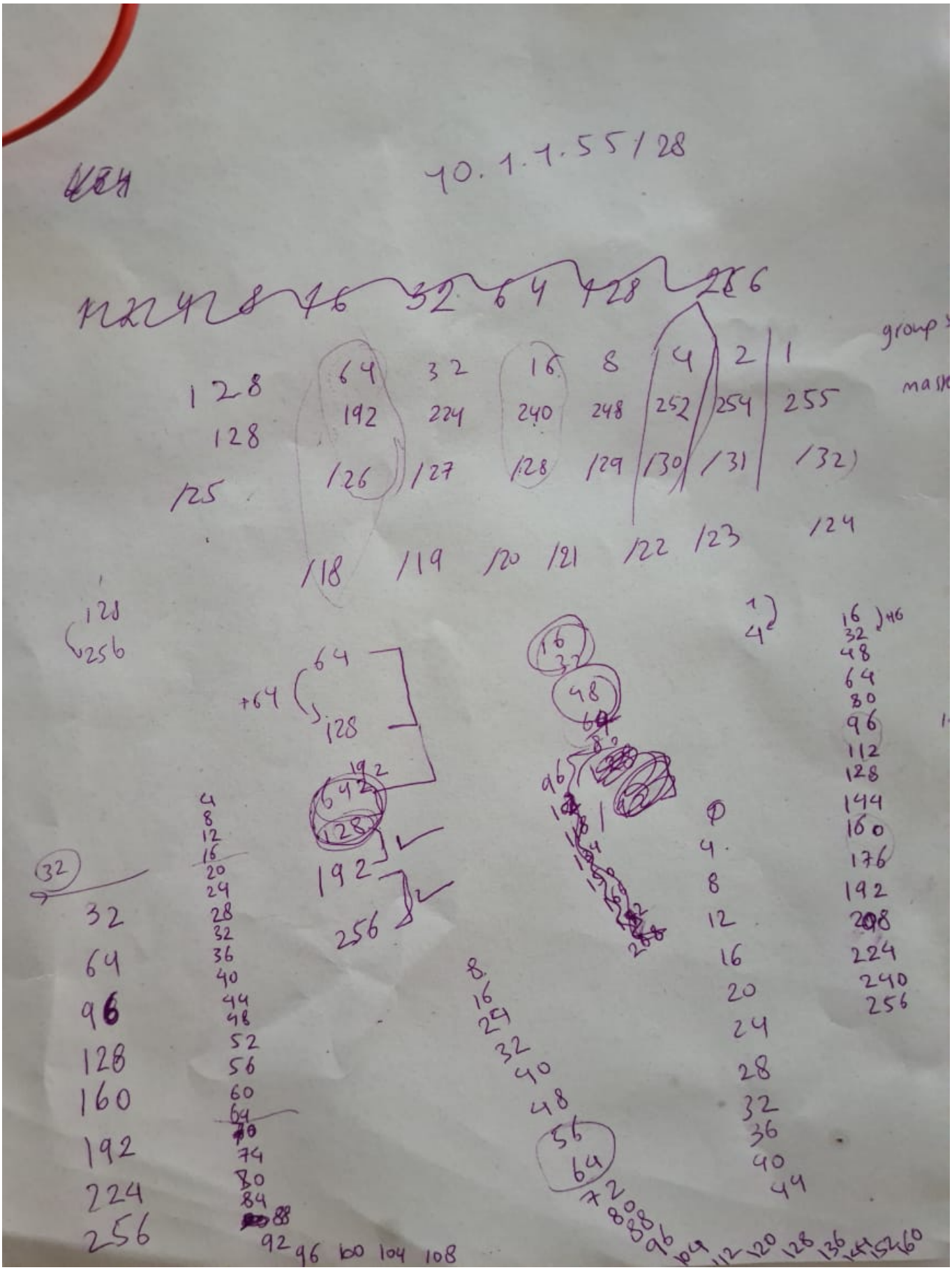
مثلا اینجا حالت دیفالت، یعنی هرررر چی آی پی مقصد داشتی، بنداز روی خط 166.66.174.254

این خط چی رو نشون میده؟ مسیر اینترفیس های روتر، هرکدوم چک می کنن که ببینن کدومشون مسیرشون به این ای پی بازه. اون خودش میفرسته .روی اون آی پی



اینجا هم همینه. هر روتری پاکت هایی که بهش می رسه رو اختصاص می ده به مسیر خاصی، هر پاکت می گه که مقصدش کجاست. توی جدول روتینگ مشخص می شه مقصد ایکس روی کدوم خط باید بیفته.
حالا مثلا حالت دیفالت همه چی اینه که بره رو اینترنت. پس ما می بینیم که دیفالت روی مسیر 163.172.250.1 قرار داره. مسیر اون و تمام ساب نت هاش منظورمونه دیگه که 163.172.250.12 هم شاملش می شه با توجه به ماسکش. پس حالت دیفالت همه چی می ره رو اینترنت.

اما مسیر برگشت چی؟اگه یه یوزری از اینترنت بخواد به یه پی سی با ایپی خاصی پاکت بفرسته چی؟
اون موقه ما به اینترنت می گیم که اگه ای پی با فلان مقصد برات اومد، بفرست روی فلان روتر.


10.1.1.55/28
group
mask