4 : Network Layer

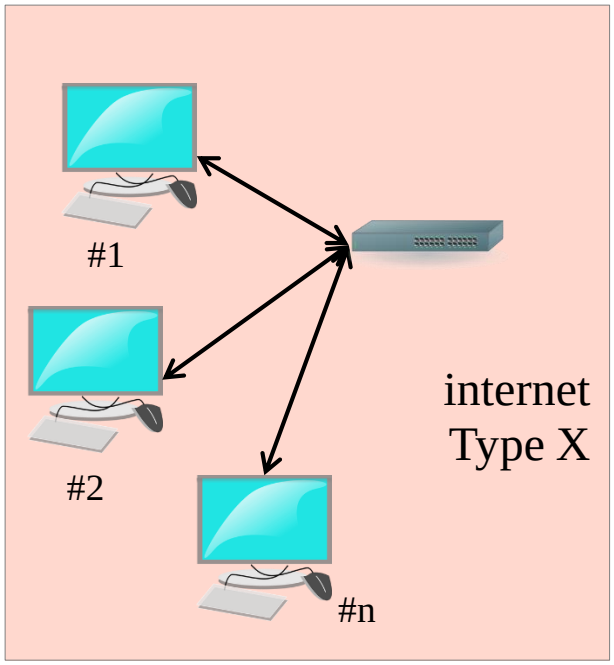
IT 4506 – Computer Networks

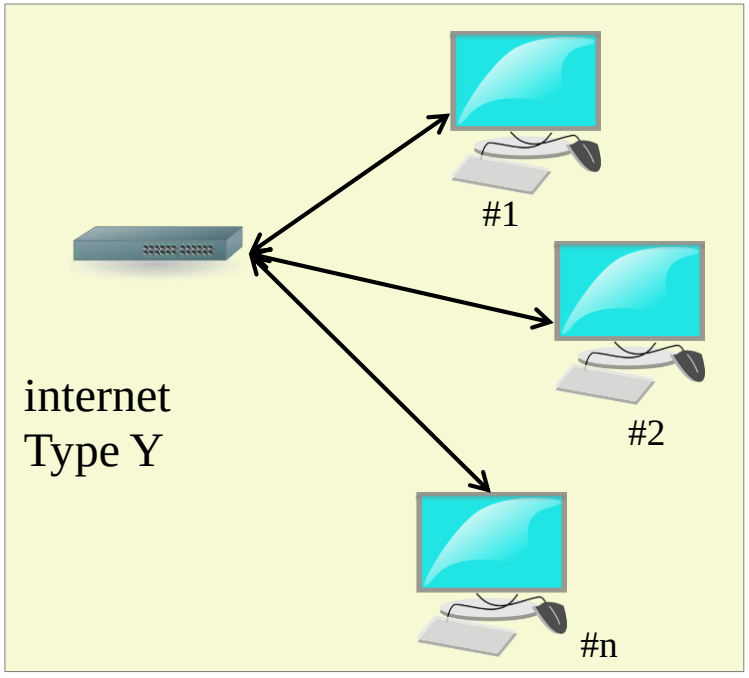
Level II - Semester 4

4.1 internetworking [Ref 01: Section 5.5]

Internet vs internet

4.1 internetworking





4.1 internetworking

How Networks Differ?

Item	Some Possibilities
Service offered	Connectionless versus connection oriented
Addressing	Different sizes, flat or hierarchical
Broadcasting	Present or absent (also multicast)
Packet size	Every network has its own maximum
Ordering	Ordered and unordered delivery
Quality of service	Present or absent; many different kinds
Reliability	Different levels of loss
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, packet, byte, or not at all

4.1 internetworking

How Networks Can be Connected?

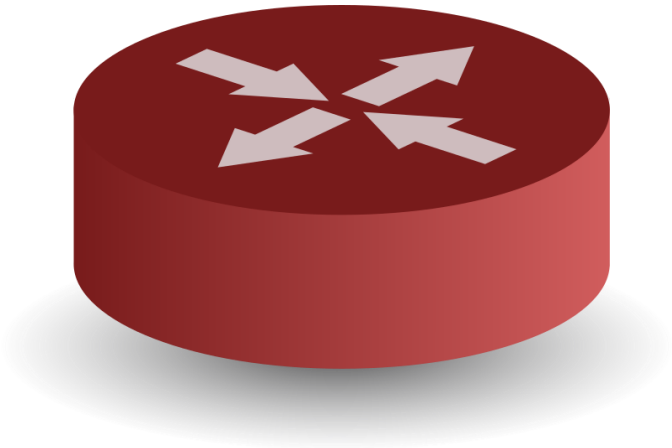
Two ways to solve it:

1. build devices that translate or convert packets from each kind of network into packets for each other network – Not scalable
2. adding a layer of indirection and building a common layer on top of the different networks

4.1 internetworking

Interconnection devices operate at Network Layer?

Routers



4.1 internetworking

A layer of indirection – e.g. IP

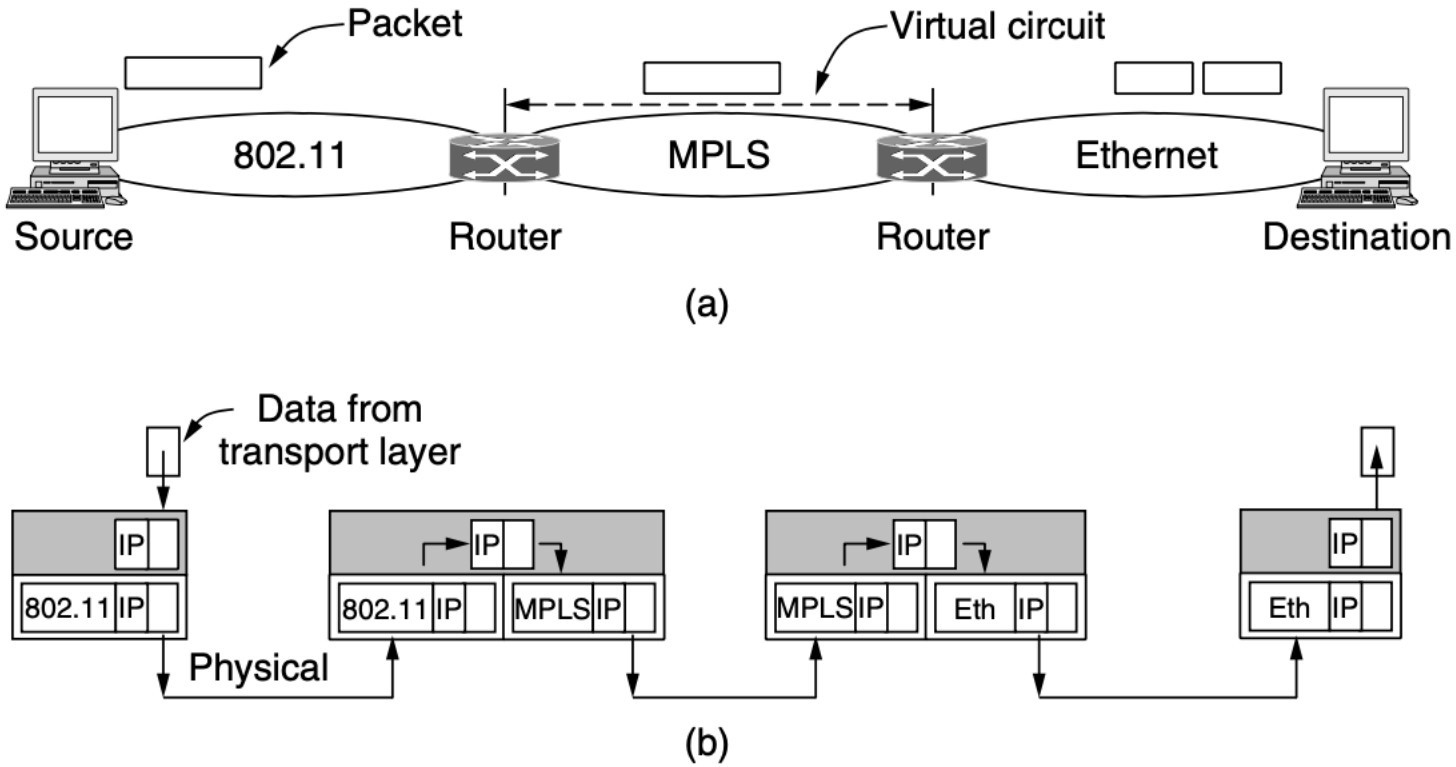


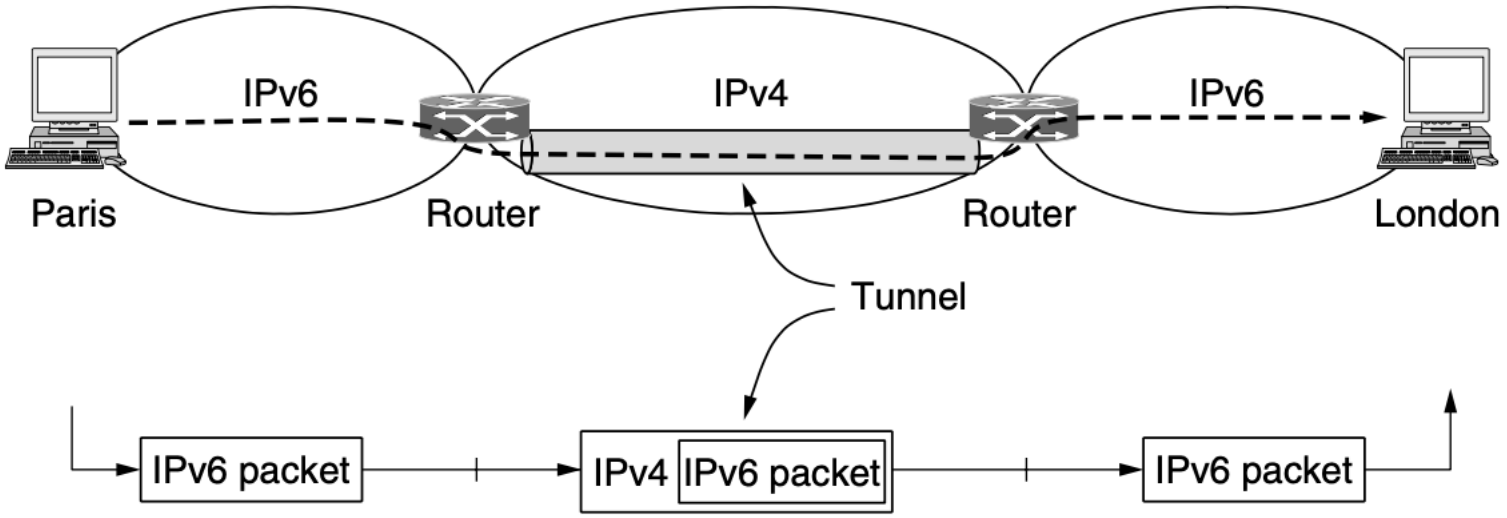
Figure 5-39. (a) A packet crossing different networks. (b) Network and link layer protocol processing.

4.1 internetworking

How to connect two IPv6 networks over a IPv4 network?

- IPv6 addresses are 128 bits long
- IPv4 addresses are 32 bits long, so the protocol does not support the size of the address.
- How we solve this problem?

4.1 internetworking
Tunnelling



4.1 internetworking

Internetwork routing

- Different networks run on different protocols
- Different network operators may have different interest on how they treat traffic
- Different territories may force conditions on network traffic

4.1 internetworking
Internetwork routing

- Solution: Using two levels of routing algorithms
  - Intradomain
  - Interdomain
- In the Internet, the interdomain protocol is called BGP (Border Gateway Protocol)

- This makes each and every network connected to the Internet an Autonomous System.
  - Example: ISP Network

4.1 internetworking
Limitations of interdomain networks

- Maximum packet size that can be transferred over the network due to:
  - Hardware
  - Operating Systems
  - Protocols
  - Compliance with international standards
  - Desire to reduce error
  - etc.

4.1 internetworking
Limitations of interdomain networks

- Solution: Get to know the Path MTU (Maximum Transmission Unit)
  - Not effective to find all the MTUs of all the paths on the Internet before transmitting a packet
- Solution: Fragment the packets
  - Transparent fragmentation
    - Overhead on intermediary Routers/ Network nodes
  - Non-transparent fragmentation
    - Higher network overhead might occur
    - IP works this way.

4.1 internetworking
Limitations of interdomain networks

- Solution: Get rid of fragmentation
  - Path MTU Discovery
  - The strategy is used in modern Internet

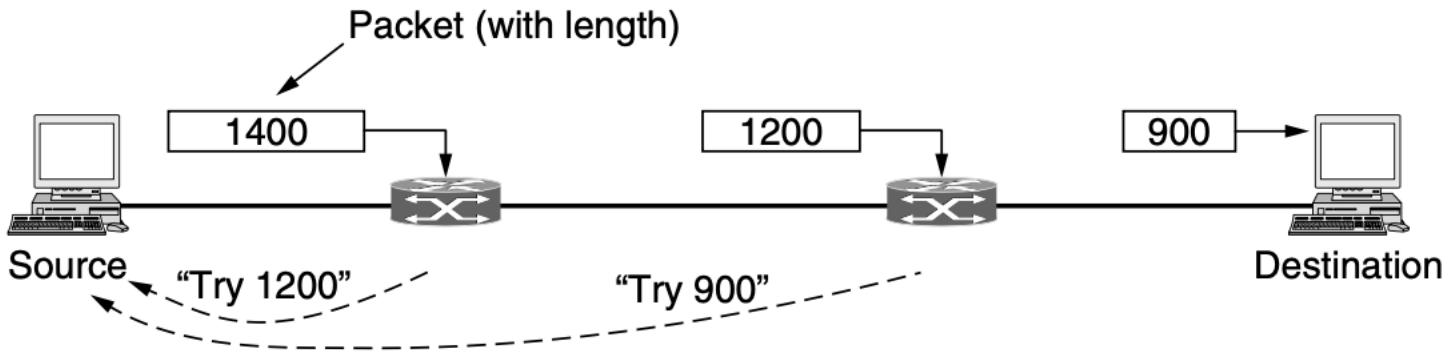


Figure 5-44. Path MTU discovery.

4.2 The network layer in the Internet

Principles of designing network protocols

[**Ref 01: Section 5.6**]

1. Make sure it works
2. Keep it simple
3. Make clear choices
4. Exploit modularity
5. Expect heterogeneity
6. Avoid static options and parameters
7. Look for a good design; it need not be perfect
8. Be strict when sending and tolerant when receiving
9. Think about scalability
10. Consider performance and cost

4.2.1 IP version 4

IP version 4 header fields

[**Ref 01: Section 5.6.1**]

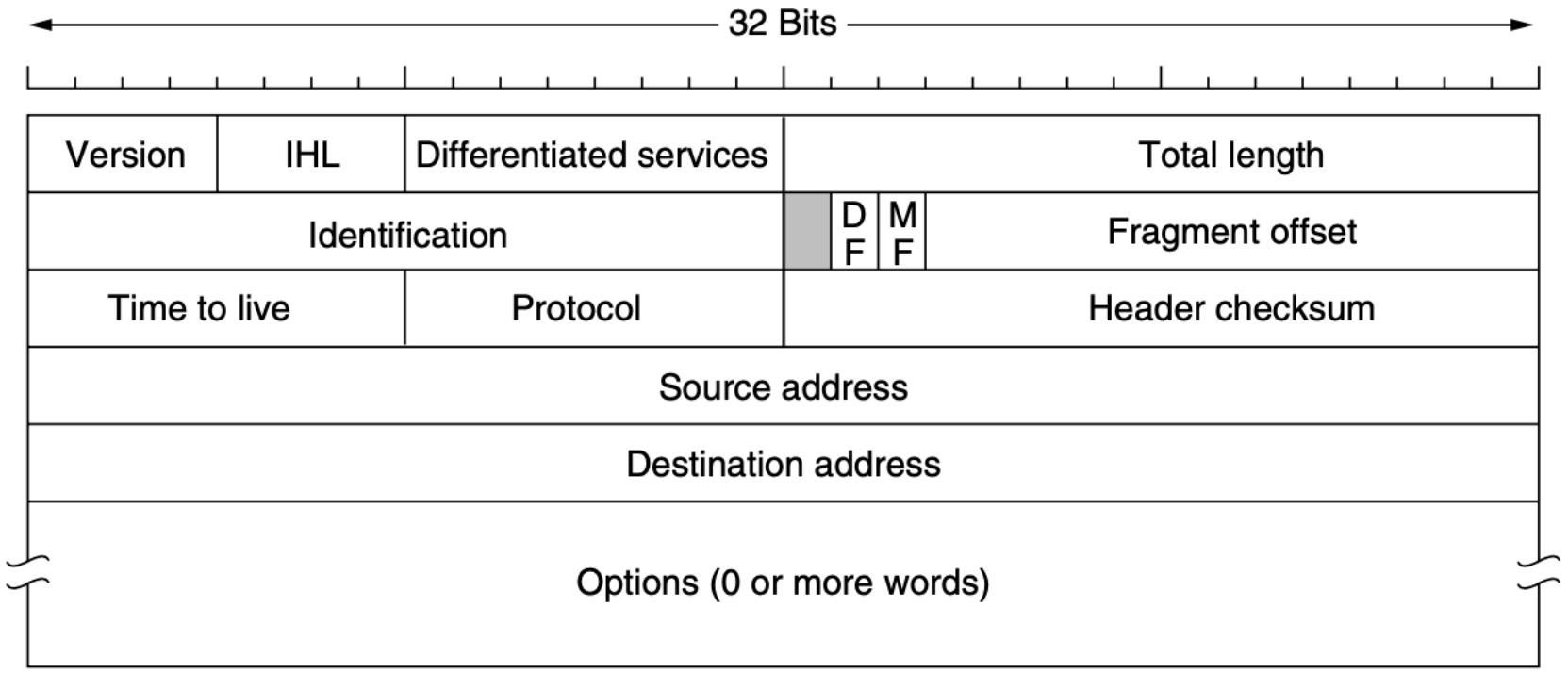


Figure 5-46. The IPv4 (Internet Protocol) header.

4.2.1 IP version 4

IP version 4 header - Options

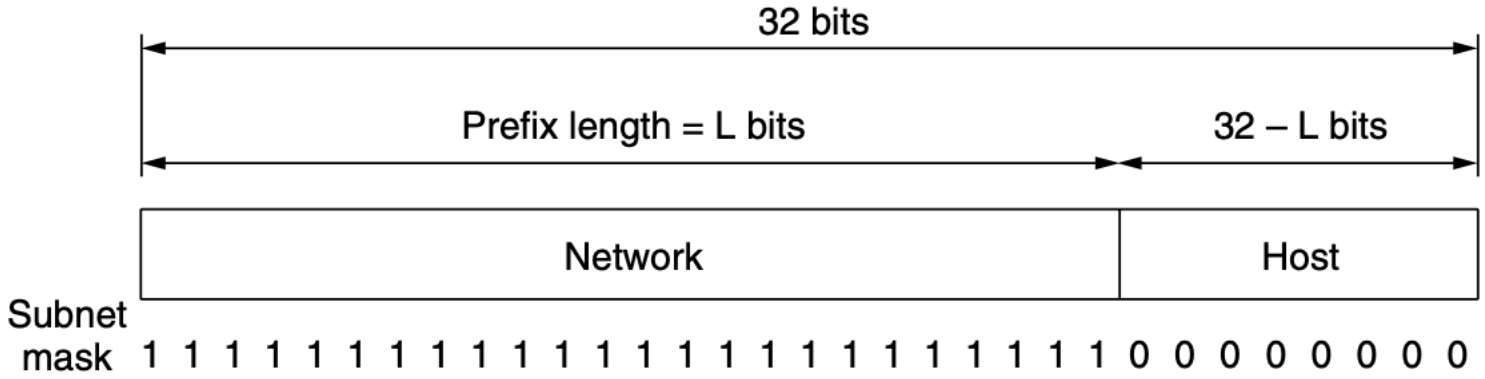
Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

4.2.1 IP version 4

4.2.1.1. Prefixes

[**Ref 01: Section 5.6.2**]

Each 32-bit address is comprised of a variable-length network portion in the top bits and a host portion in the bottom bits.



The network portion has the same value for all hosts on a single network with contiguous block of IP address space. This block is called **Prefix**

4.2.1 IP version 4

4.2.1.1. Prefixes

IP addresses are written in dotted decimal notation.
E.g. 128.208.2.151

If the prefix contains 2^8 Addresses, then the network address is written as 128.208.2.0/24 where 24 represents the number of bits representing the network potion.

Since the prefix length cannot be inferred from the IP address alone, routing protocols must carry the prefixes to routers.

128.208.2.0/24: When written out this way, it is called a **subnet mask in CIDR notation**.

4.2.1 IP version 4

4.2.1.2. Subnets

[**Ref 01: Section 5.6.3**]

routing by prefix requires all the hosts in a network to have the same network number
This property can cause problems as networks grow.

Let's assume the initial prefix is /16. The network already has provision to over 60,000 hosts but would not be able to use them.

The solution is to allow the block of addresses to be split into several parts for internal use as multiple networks, while still acting like a single network to the outside world - **subnetting**

4.2.1 IP version 4

4.2.1.2. Subnets

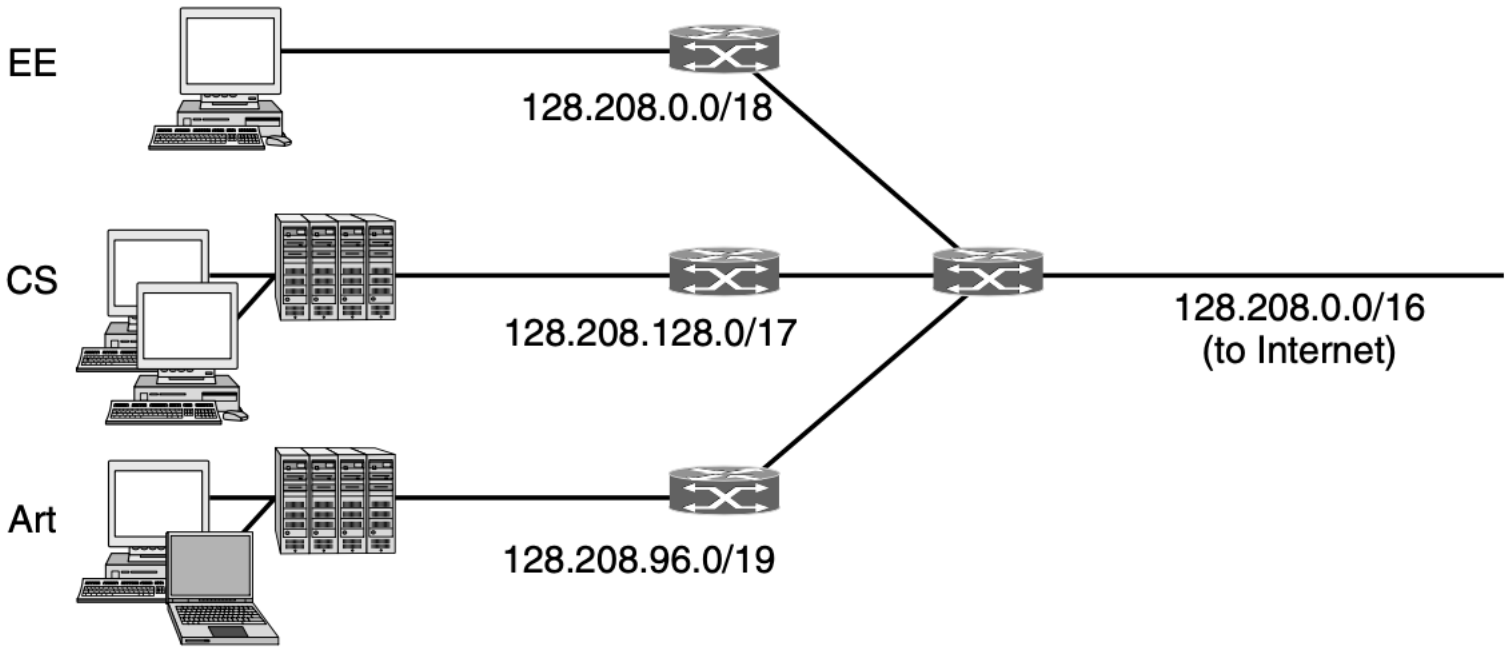
Example: Assume a university has a /16 IP block. Let's say it has three departments: Computer science, Electrical Engineering, and Art. The subnetting could be done as follows.

Computer Science:	10000000	11010000	1|xxxxxxx	xxxxxxxx
Electrical Eng.:	10000000	11010000	00|xxxxxx	xxxxxxxx
Art:	10000000	11010000	011|xxxxx	xxxxxxxx

Here, the vertical bar (|) shows the boundary between the subnet number and the host portion.

4.2.1 IP version 4

4.2.1.2. Subnets



4.2.1 IP version 4

4.2.1.3. Classless InterDomain Routing (CIDR)

Internet routers must know which way to go to get to every network and no one really knows how many networks are connected to the Internet. It is a very large number

This could make a very large routing table in each router

Additionally, routers exchange information and with large routing tables, this would be a difficult job to process.

For example, routers could know multiple networks in a particular path using a single entry instead of multiple entries.

4.2.1 IP version 4

4.2.1.3. Classless InterDomain Routing (CIDR)

The process of combining multiple small prefixes into a large prefix is called **route aggregation**.

As a result, IP addresses are contained in prefixes of varying sizes.

This design also works with subnetting and called **CIDR (Classless InterDomain Routing)**.

Additionally, CIDR design allows to utilize IP addresses more efficiently. You will understand this further when we discuss Classful addressing.

4.2.1 IP version 4

4.2.1.3. Classless InterDomain Routing (CIDR)

Assume that block of 8192 IP addresses is available starting at 194.24.0.0. Suppose that Cambridge, Edinburgh, and Oxford need 2048, 1024, and 4096 IP blocks respectively. Following is a way of assigning IP addresses for each university.

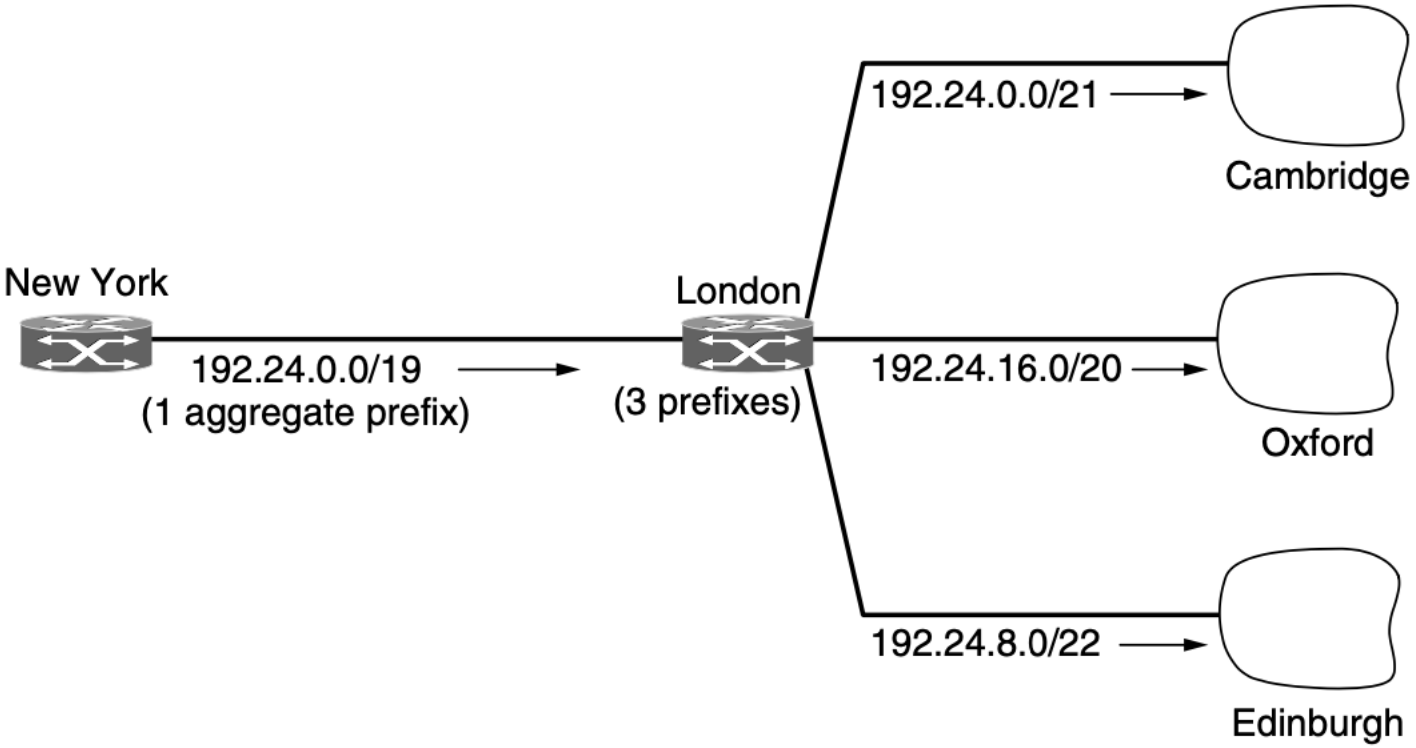
Try to understand what an (Available) block is there at the middle.

University	First address	Last address	How many	Prefix
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12.0/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

4.2.1 IP version 4

4.2.1.3. Classless InterDomain Routing (CIDR)

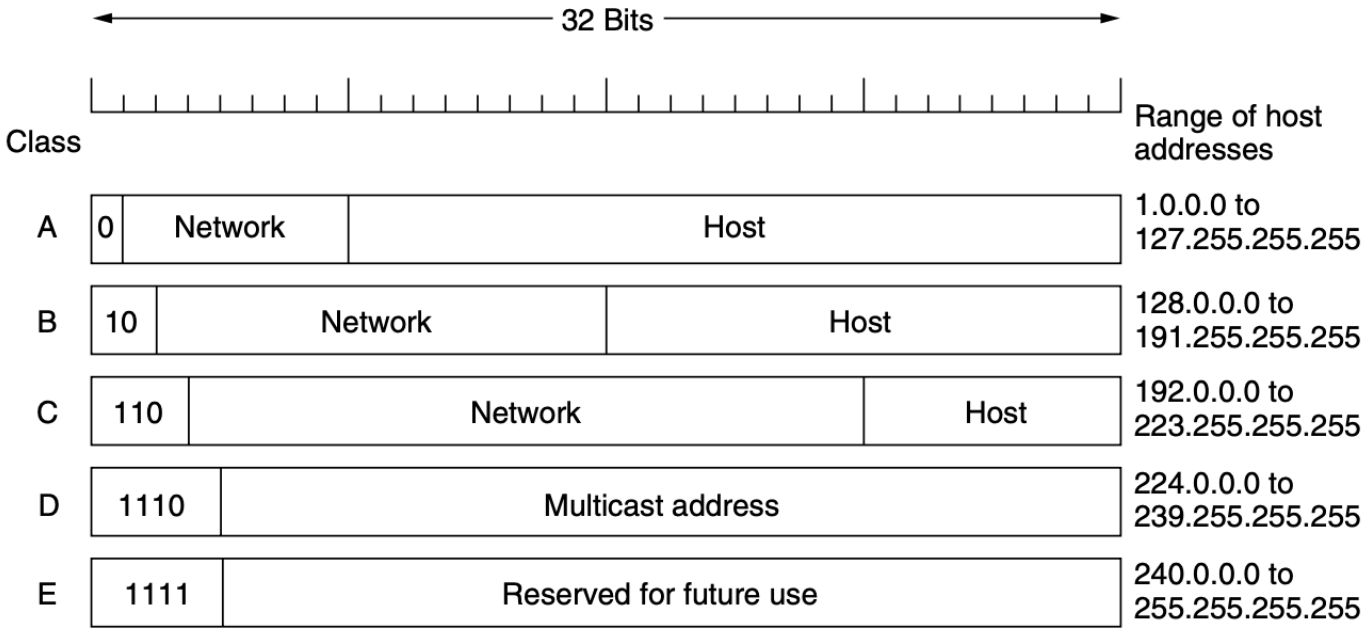
Now let us look at these three universities from the point of view of a distant router in New York



4.2.1 IP version 4

4.2.1.4. Classful and Special Addressing

Before 1993, IP addresses were divided into the five categories



Over 2 billion addresses exist, but organizing the address space by classes wastes millions of them. Today, the bits that indicate whether an IP address belongs to class A, B, or C network are no longer used.

4.2.1 IP version 4

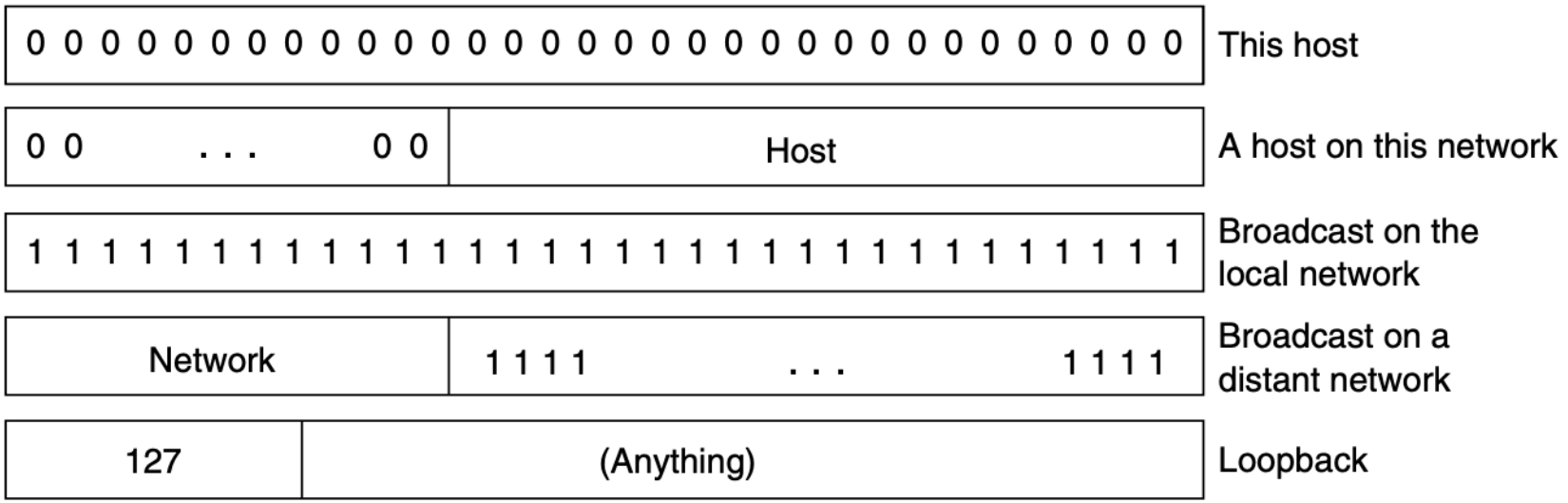
4.2.1.4. Classful and Special Addressing

Class D addresses continue to be used in the Internet for multicast

- There are also several other addresses that have special meanings
  - The IP address 0.0.0.0, the lowest address, means this host
  - The address consisting of all 1s, or 255.255.255.255, the highest address, is used to mean all hosts on the indicated network.
  - Finally, all addresses of the form 127.*xx.yy.zz* are reserved for loopback testing

4.2.1 IP version 4

4.2.1.4. Classful and Special Addressing



4.2.1 IP version 4

4.2.1.5. Network Address Translation (NAT)

The problem of running out of IP addresses is not a theoretical one, It is happening right here and right now.

The long-term solution is for the whole Internet to migrate to IPv6, which has 128-bit addresses.

The quick fix that is widely used today came in the form of **NAT (Network Address Translation)**

4.2.1 IP version 4

4.2.1.5. Network Address Translation (NAT)

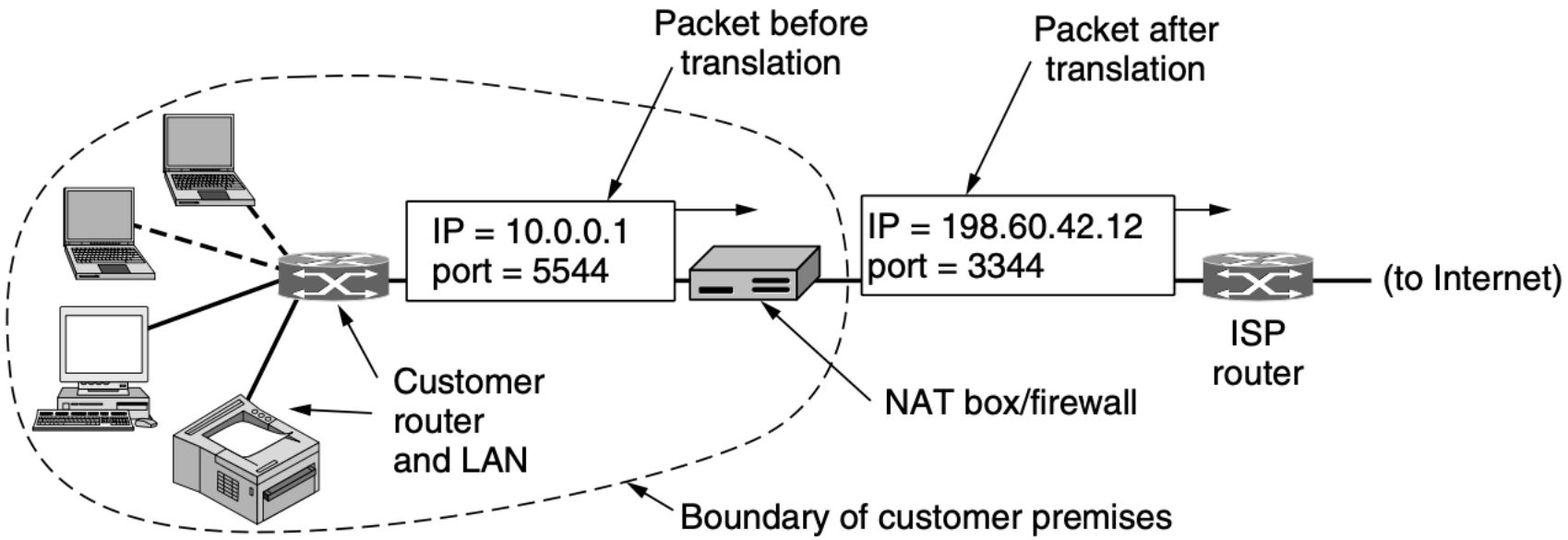
The basic idea behind NAT is for the ISP to assign each home or business a single IP address (or at most, a small number of them) for Internet traffic.

Within the customer network, every computer gets a unique IP address, which is used for routing intramural traffic.

Just before a packet exits the customer network and goes to the ISP, an address translation from the unique internal IP address to the shared public IP address takes place.

4.2.1 IP version 4

4.2.1.5. Network Address Translation (NAT)



Private IP addresses: The only rule is that no packets containing these addresses may appear on the Internet. The three reserved ranges are:

10.0.0.0	– 10.255.255.255/8	(16,777,216 hosts)
172.16.0.0	– 172.31.255.255/12	(1,048,576 hosts)
192.168.0.0	– 192.168.255.255/16	(65,536 hosts)

4.2.1 IP version 4

4.2.1.5. Network Address Translation (NAT)

Complications of NAT:

- NAT breaks the end-to-end connectivity model of the Internet
- NAT changes the Internet from a connectionless network to a peculiar kind of connection-oriented network as NAT device has to maintain the information of the connections passing it.
- NAT violates the most fundamental rule of protocol layering
- If the Internet is introduced with new transport layer protocol, application fails.
- Special precaution should be taken to make applications using multiple TCP/IP connections or UDP ports