Computer Network I

Reti di Calcolatori I

Università di Napoli Federico II – Scuola Politecnica e delle Scienze di Base
Corso di Laurea in Informatica

Riccardo Caccavale

(riccardo.caccavale@unina.it)

Università degli Studi di Napoli Federico II

DIETI

UNINA

Network Layer

Internet Protocol (IP)

- The **Internet Protocol (IP)** is the network-layer protocol used to ensure host-to-host delivery. There are 2 versions of IP currently in use:
  - **IP version 4 (IPv4)** which is the most used and the most common.
  - **IP version 6 (IPv6)** which is the newer version, proposed to replace IPv4.

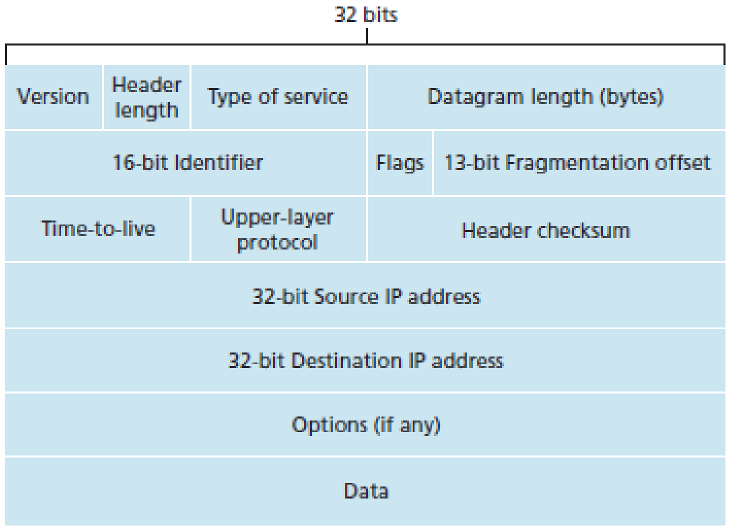
- The **most important functionality** provided by the IP is **to identify hosts** on a network (IP addressing).

- The **IP addressing** is the process of assigning IP addresses to devices. Addressing is **crucial** for network functionalities and is quite **complex** in Internet (there are millions or billions of hosts to be addressed).

Network Layer

Internet Protocol: Datagram

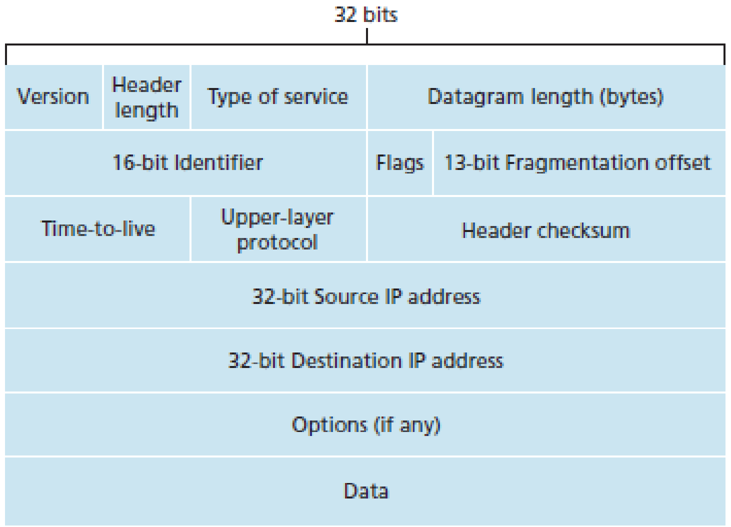
- Internet’s network-layer packet called **datagram** (as UDP). The key fields in the IPv4 datagram are:
  - **Version number** (4 bits) specify **the IP version** (e.g., v4 or v6) of the datagram (formats depends on versions).
  - **Header length** (4 bits) **dimension of the header** (not fixed, options are of variable size), used to know where the payload starts (no options means 20 bytes header).
  - **Type of service** (TOS, 8 bits) identifies specific **proprieties** of the datagram (e.g., real-time/non-real-time). Such types are **defined by network administrators** of routers.
  - **Datagram length** (16 bits) length in **bytes of the datagram** (header + data). Datagrams are rarely larger than 1500 bytes (out of 65535 max).
  - **Identifier** (16 bits) a progressive number that uniquely identifies a datagram (used in fragmentation).
  - **Flags and fragmentation offset** (3+13 bits) proprieties and offset of the fragment (used in fragmentation).
  - **Time-to-live** (TTL, 8 bits) ensure that datagrams do **not circulate forever in the network**. This field is decremented by one each time the datagram is processed by a router. If the TTL field reaches 0, a router must drop that datagram.



Network Layer

Internet Protocol: Datagram

- **Upper-layer Protocol** (8 bits) indicating the **transport-layer protocol** to which the payload (data filed) of this IP datagram should be passed (e.g., 6 for TCP, 17 for UDP).
  - Complete list of protocols available from IANA website: https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
- **Header checksum** (16 bits) for error detection. Here checksum is calculated as 1s complement of the 2 bytes-wise sum of the header. **Routers check this value** and **erroneous datagrams are typically discarded**.
  - Note that the checksum must be **recomputed and stored again at each router** due to the TTL and options fields that can change.
- **Source and destination IP addresses** (32+32 bits).
- **Options** (not fixed) allow an IP header to be extended (**additional functionalities**). Option field provide a certain degree of complexity (unknown size), it is not present in IPv6.
- **Data** (not fixed) contains the **actual message (payload)** typically in the form of a TCP/UDP transport-layer segment.



Network Layer

Internet Protocol: Fragmentation

- The first problem with IP datagrams is that they can be **fragmented at the link level**. Some link-layer protocols carries datagrams of **different dimensions**.
  - Example: Ethernet frames can carry up to 1500 bytes of data.

- IP datagrams are eventually encapsulated into link-layer frames to be transported from node to node. The maximum amount of data (i.e., the maximum frame length) that a link-layer frame can carry is the **maximum transmission unit** (MTU).

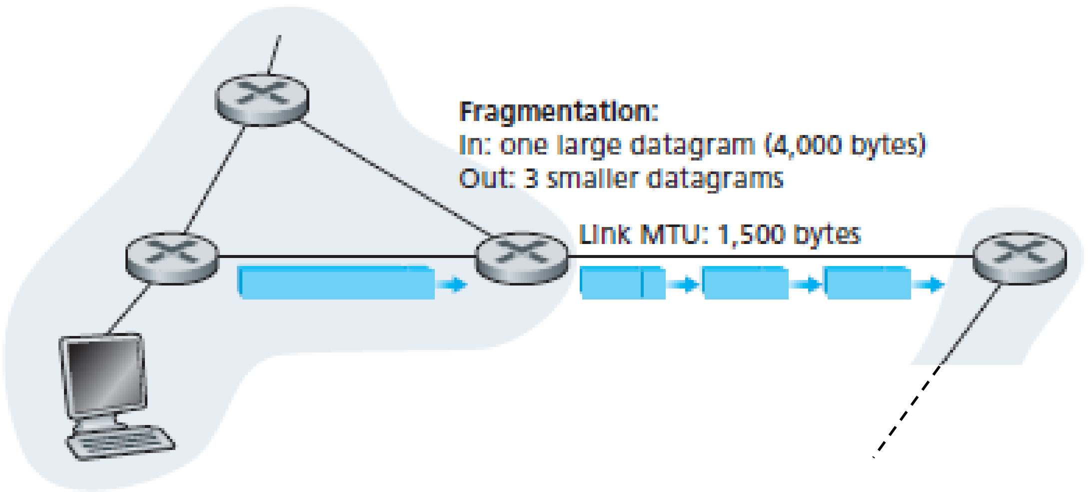
- A router that interconnects 2 links having different MTUs **may receive an IP datagram from input link that does not fit the output link**.

- The **router has to divide the payload** of the IP datagram into two or more smaller IP datagrams (fragments). **Fragments are then encapsulated into link-layer frames** and forwarded over the outgoing link.

Network Layer

Internet Protocol: Fragmentation

- When a router **fragments a datagram**:
  - It **copies the same identifier, source address, and destination address** into the newer fragments.
  - It sets the **fragment offset** field of all fragments **to progressive numbers**.
  - It sets the **flag of the last fragment to 1** (to signal that the fragments are over).



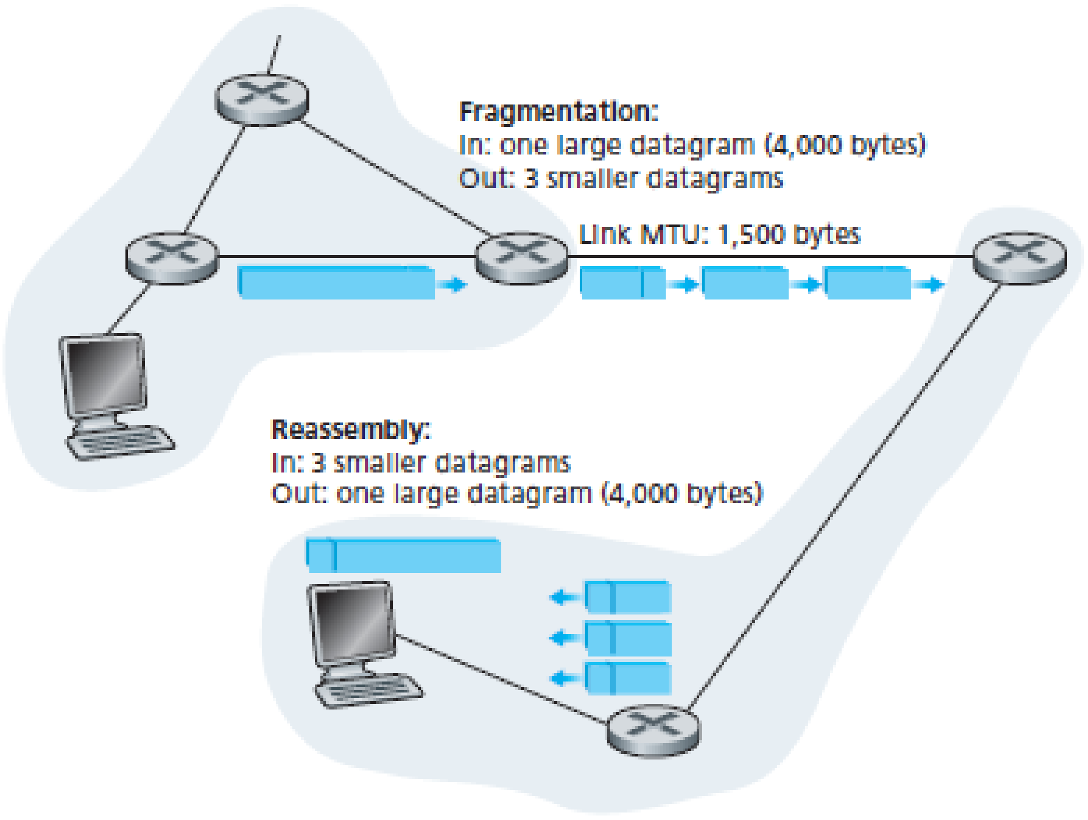
- Clearly, **fragments need to be reassembled** before they reach the transport layer at the destination since both TCP and UDP are expecting to receive complete segments from the network layer…

Network Layer

Internet Protocol: Fragmentation

- The designers of IPv4 felt that **reassembling datagrams in the routers** would introduce significant complication into the protocol and **put a damper on router performance**.

- In IPv4 datagram **reassembly is then performed into the end systems**:
  - If multiple datagrams having **same addresses and identifier** are received, it means that the original datagram has been fragmented.
  - The host has to **recreate the original datagram** from the fragments.



Network Layer

Internet Protocol: Addressing

- IP addresses are typically written in so-called **dotted-decimal notation**, in which each byte of the address is written in its decimal form and is separated by a period (dot) from other bytes in the address.

- For example:

	Dotted-decimal	Binary
IP address	193.32.216.9	11000001 00100000 11011000 00001001

- Each device in the global Internet must have (somehow) an **IP address that is globally unique**.

- Since each **IP address is 32 bits (4 bytes) long** (equivalently, 4 bytes), there are a total of **2^{32} (around 4 billion) possible IP addresses**.

Network Layer

Internet Protocol: Addressing

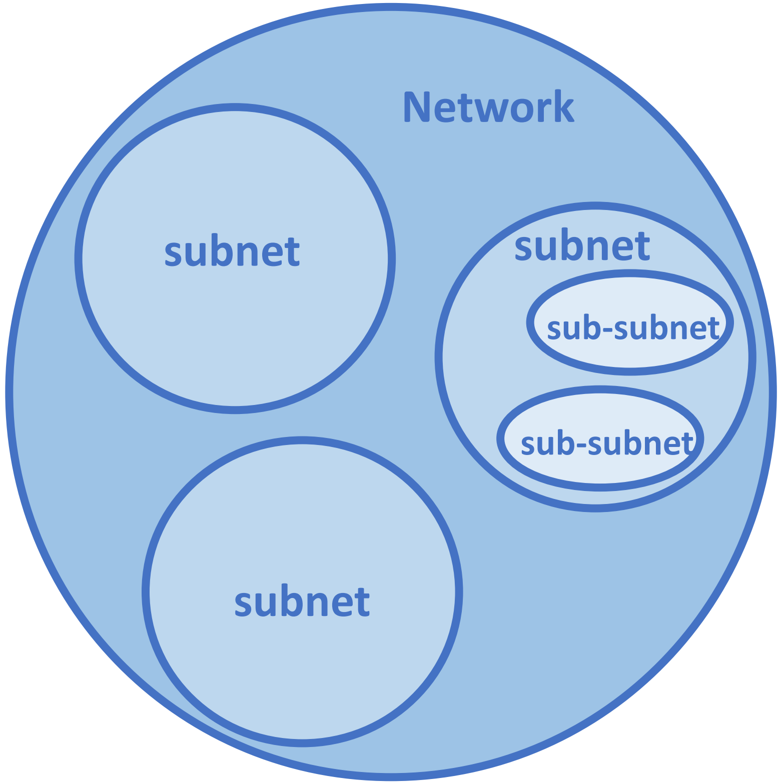
- Hosts and, in general, **network devices are connected through links** (wired or wireless).
- A host typically has only a single link into the network, while a network device (e.g., a router) **may have multiple links**.
- The boundary between the host and the physical link is called **interface**.
- Because every host and router is capable of sending and receiving IP datagrams, IP requires **each interface to have its own IP address**.
- Thus, an **IP address is technically associated to the interface**, rather than the host or router containing that interface.

Network Layer

Internet Protocol: Addressing

- Assigning IP addresses to different interfaces is **not trivial**. It would be **unwise to randomly assign IP** addresses for several reasons, for example:
  - As IPs give no indication about locations, **we wouldn't know where to find hosts**.
  - We would need for **huge forwarding tables** inside routers.

- The network addressing resembles the one of *standard telephony*: **networks are hierarchically divided into sub-networks** (or **subnets**) having different prefixes.



- An IP address is then divided in **two parts**:
  - The **first portion** (leftmost) identifies the subnet to which the node is connected.
  - The **second portion** (rightmost) identifies the single interface.

- The **number of bits belonging to each portion is not fixed**.

Network Layer

Internet Protocol: Addressing

- Specifically, to distinguish the subnet-part from the interface-part, an IP address is associated to a **subnet mask** that specifies which bit of the address belongs to the subnet-part.

- For example:

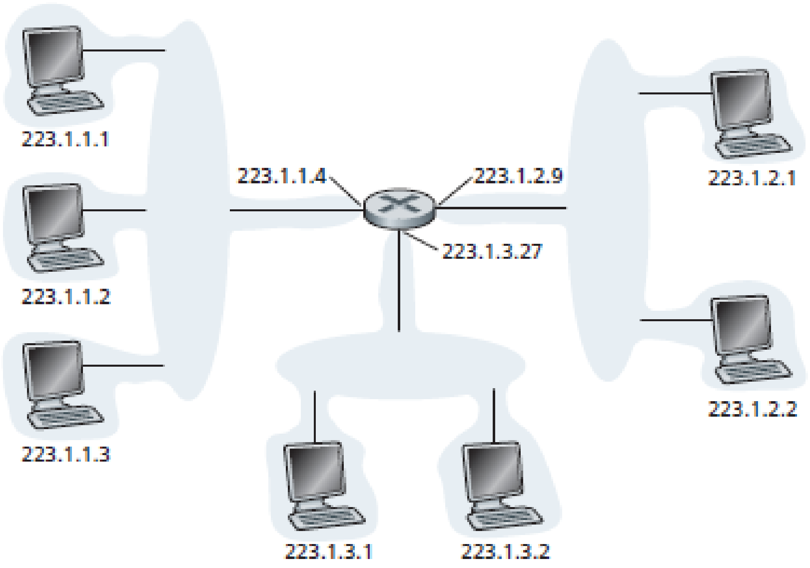
	Dotted-decimal	Binary
IP address	193.32.216.9	11000001 00100000 11011000 00001001
Subnet Mask	255.255.255.0	11111111 11111111 11111111 00000000

- Another common way to represent the masks is the ***slashed notation***, for instance 193.32.216.0/24 represents the IP of the subnet, where the /24 indicates that the leftmost 24 bits of the address are dedicated to the subnet.

Network Layer
Internet Protocol: Addressing

- In this example, one router (with three interfaces) is used to interconnect seven hosts. Hosts are divided in 3 **subnets** (left, right, down) each one linked to one interface of the router.

- Each subnet is associated to a specific address, for instance the **left subnet** has address 223.1.1.0/24, so all interface in this network have IP addresses in the form 223.1.1.XXX:
  - 223.1.1.1 (host),
  - 223.1.1.2 (host),
  - 223.1.1.3 (host),
  - 223.1.1.4 (router).

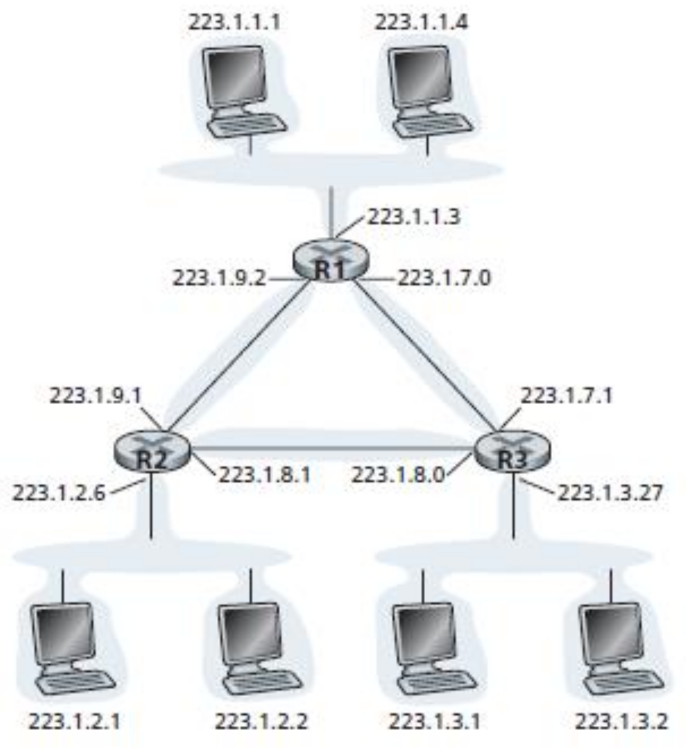


- The other two subnets have 223.1.2.0/24 and 223.1.3.0/24 addresses.

Network Layer

Internet Protocol: Addressing

- In this example **there are 3 routers** that are interconnected by a direct (point-to-point) link. Each router has **3 interfaces**, one for each **point-to-point link** and one for the **broadcast link** that directly connects the router to a pair of hosts.
- There is a total of 6 subnets:
  - 223.1.1.0/24 (R1-hosts),
  - 223.1.2.0/24 (R2-hosts),
  - 223.1.3.0/24 (R3-hosts),
  - 223.1.9.0/24 (R1-R2),
  - 223.1.8.0/24 (R2-R3),
  - 223.1.7.0/24 (R3-R1).
- In this case routers are like gates (**gateways**) connecting different networks: if we could detach the interfaces from each router, we would have 6 isolated networks.
- Typically, **medium/large organizations** (such as a companies or academic institutions) have multiple interconnected subnets.



Network Layer
Ifconfig

- On Linux machines we can check our own address by using the *ifconfig* command (the equivalent on windows machines is *ipconfig*).

- Ifconfig (Interface configuration) provides the **list of all network interfaces** of the machine **along with their network configuration** (addresses, masks, etc.).
  - There are also modern commands to do so like ip.

- Usage:
  - To get the configuration:
    - $ ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:0F:20:CF:8B:42
          inet addr:217.149.127.10  Bcast:217.149.127.63  Mask:255.255.255.192
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2472694671 errors:1 dropped:0 overruns:0 frame:0
          TX packets:44641779 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1761467179 (1679.8 Mb)  TX bytes:2870928587 (2737.9 Mb)
          Interrupt:28
```

Ifconfig output example (Wikipedia)

Network Layer

Internet Protocol: Internet Addressing

- The idea of **breaking large networks into smaller ones is particularly important** on Internet where billions of devices (not to mention interfaces) must be connected.

- On Internet, IP **addresses must be carefully assigned** to avoid some issues:
  - The **forwarding tables** of routers may become very large.
  - We could have different interfaces with the **same address**.
  - We cloud **run out of addresses**.

- The approach is to divide Internet addresses by **providing subnets for the organizations** (such as ISPs, companies, institutions, etc.). There are 2 ways:
  - **Classful addressing** (older, no more used in practice).
  - **Classless addressing** (current).

Network Layer

Internet Protocol: Classful Addressing

- In **classful addressing** Internet addresses were divided into classes depending on a specific division:

	Format	Example	IPs per network
Class A	a.b.c.d/8	10.X.X.X	> 16 million
Class B	a.b.c.d/16	10.10.X.X	65535
Class C	a.b.c.d/24	10.10.10.X	254

- For example, if your organization needed 300 IPs, **you would have assigned a class B address** (e.g., 241.115.0.0) along with all IPs within it.
- There is a clear problem with this approach, since **only 300 IPs are needed, the additional 65335 IPs are wasted!**

Network Layer
Internet Protocol: Classless Addressing

- The modern approach is more flexible and is called **Classless InterDomain Routing** (**CIDR**, pronounced cider). Here, an organization could have assigned network addresses of any form:

a.b.c.d/X

- Now if you need 300 IPs you could have assigned a.b.c.d/23 (e.g., 241.115.2.0/23) which **provides 512 IPs and only 212 wasted ones**.

- In "CIDRized" addresses:
  - The network-part of the address is called **prefix.**
  - The set of IPs reserved to the organization is called **block**.

- Note: **it is possible for blocks to overlap**, in this case the length (X) of the prefix can be used to discriminate different blocks.
  - Example: the IP 10.10.10.15/16 is not in the same block of 10.10.10.14/24.

Network Layer

Internet Protocol: Classless Addressing

- There is also the possibility **to create inner subnets** (i.e., subnets inside an organization) within a CIDR block.

- For example, the **CIDR block 241.115.0.0/16 can be decomposed** into additional subnets:
  - 241.115.1.0/24 (subnet 1),
  - 241.115.2.0/24 (subnet 2),
  - 241.115.3.0/24 (subnet 3),
  - etc.

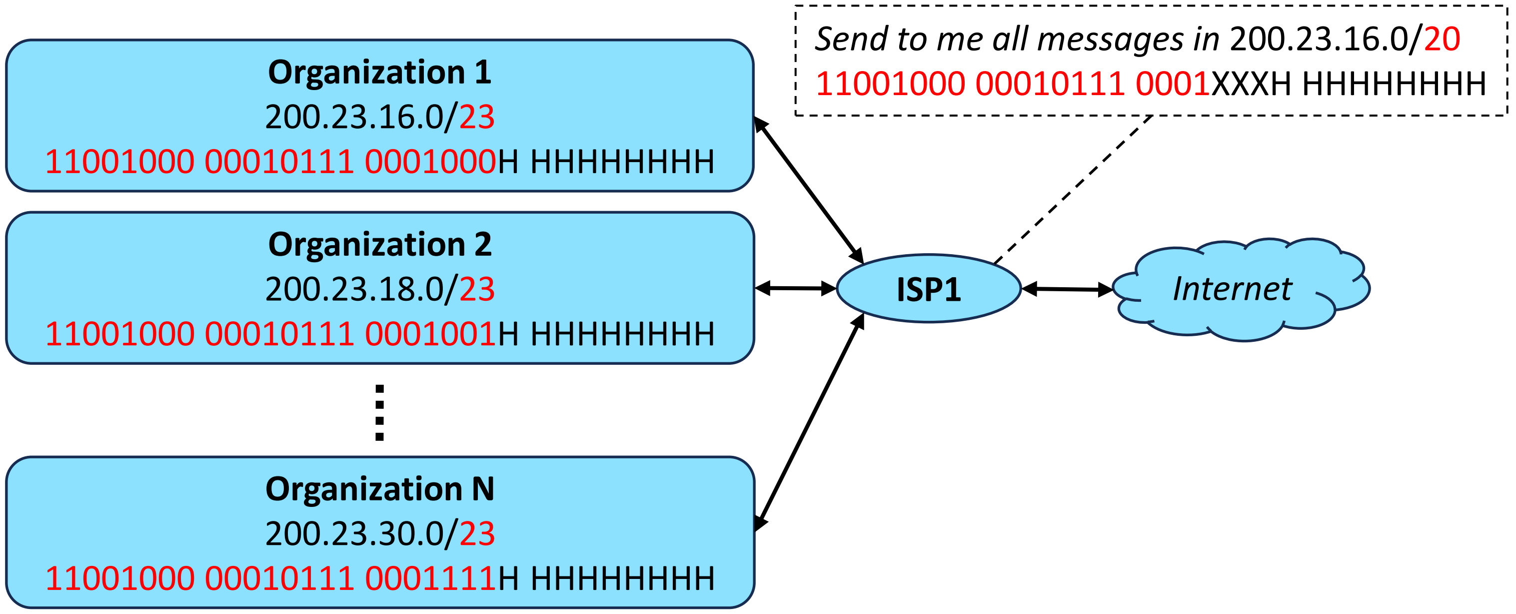
- From a binary standpoint:

$$\overbrace{\overbrace{11110001\ 01110011}^{\text{Prefix}}\ SSSSSSSS}^{\text{Subnet}}\ \overbrace{HHHHHHHH}^{\text{Host}}$$

Network Layer

Internet Protocol: Address Aggregation

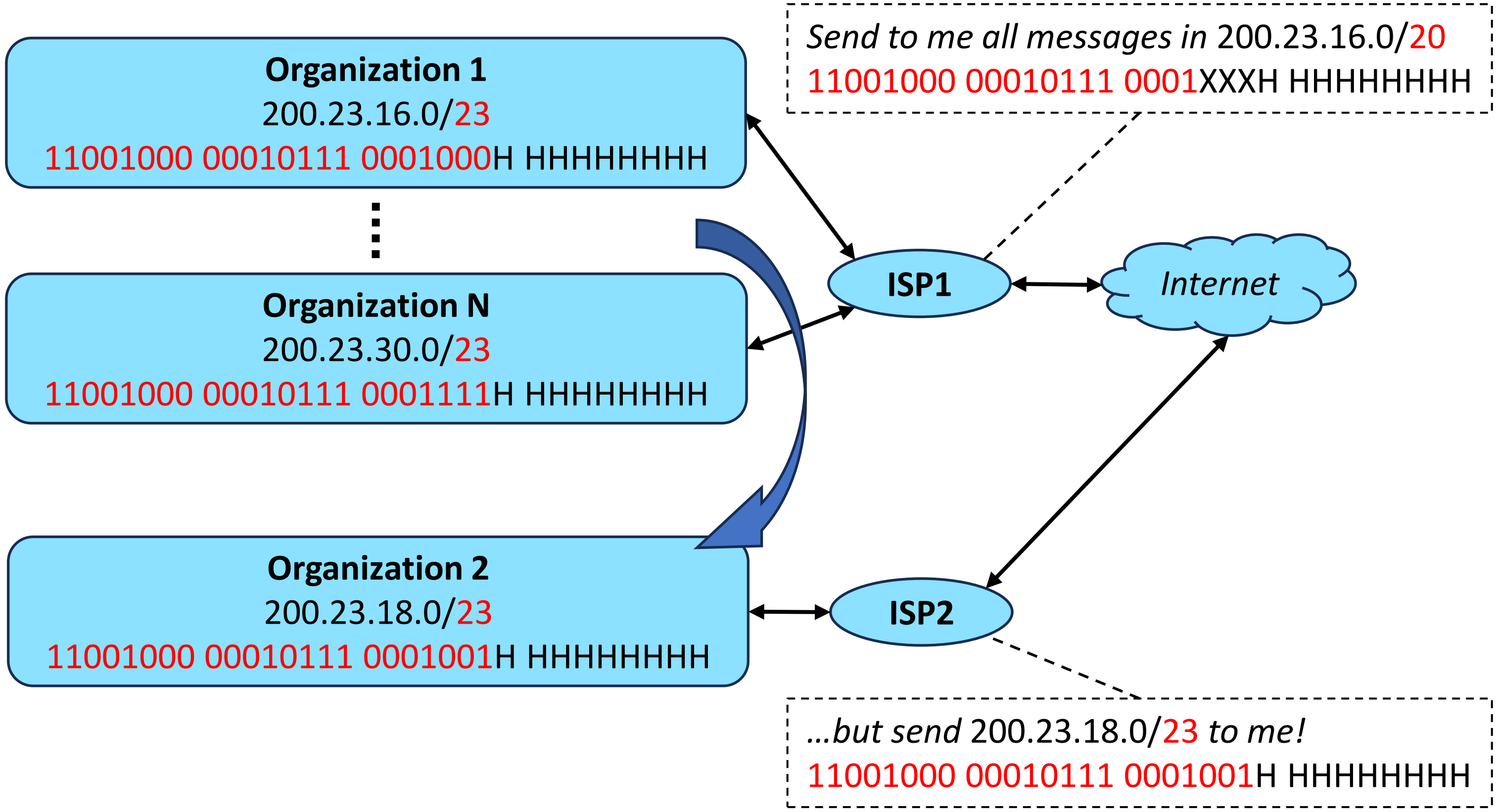
- The prefix-based addressing is very useful for devices that connect different prefixes.
- It is possible for a router to just remember (i.e., save into forwarding table) the prefixes.
- When a message with a specific prefix is received, it is forwarded to a more specific router, and so on.
- This approach is called **address aggregation** (or route summarization).



Network Layer

Internet Protocol: Address Aggregation

- The prefix-based addressing is very useful for devices that connect different prefixes.
- It is possible for a router to just remember (i.e., save into forwarding table) the prefixes.
- When a message with a specific prefix is received, it is forwarded to a more specific router, and so on.
- This approach is called **address aggregation** (or route summarization).



It is more effective as long as blocks are **clustered**!

Network Layer

Internet Protocol: Obtaining a Block

- In order **to obtain a block of IP addresses** for use within an organization's subnet there are 2 ways:
  1. You can **contact an ISP**, which would provide addresses from a larger block of addresses that had already been allocated.
     - For example, **the ISP may itself have been allocated the address block** 200.23.16.0/20, that can be further separated into sub-blocks of variable size depending on the ISP policy.
  2. You can ask to the **Internet Corporation for Assigned Names and Numbers (ICANN)**, which is a no-profit global authority that has the responsibility to manage the IP address space (e.g., allocating address blocks to ISPs, etc.). **ICANN also manages the DNS root servers**, by assigning domain names and resolving domain name disputes.
     - Link: https://www.icann.org/