Networks: General Introduction + IPv_4 addressing

Ali Benzerbadj

University of Ain Temouchent Belhadj Bouchaïb (UAT-BB)

21 février 2025

Plan

Plan

Plan

Plan

Plan

Module Objective

Module Objective

- Provide students with essential concepts for a thorough understanding of networks.
- The students should be able to explain what a network is, its components, how computers can communicate with each other, describe various types of media, different types of topologies, as well as a detailed study on the five layers of the Internet model.

Module Objective (2)

Module Objective

- Enable the students to understand the operation, plan the installation, and use a computer network.
- Familiarize the students with various layers of implementing a computer network.
- Initiate the students to the main communication protocols and message routing.

Module Objective (3)

Module Objective

- Familiarize the student with the key components of a computer network.
- Enable the student to use the basic services of a network within a program.

Program (Course)

Module Objective

1. Chapter I : Introduction to Networks
2. Chapter II : Physical Layer
3. Chapter III : Data Link Layer
4. Chapter IV : Network Layer
5. Chapter V : Transport Layer
6. Chapter VI : Application Layer

Program (Practical Work)

Module Objective

1. Practical Work 1 : Basic Configuration of a Network
2. Practical Work 2 : Network Programming (Socket)
3. Practical Work 3 : Routing
4. Practical Work 4 : Protocol Analyzer

References

References

- "Computer Networks", Andrew S. Tanenbaum, David J. Wetherall, 5th Ed., Prentice Hall, 2011
- "Réseaux", Guy Pujolle, édition 2014, Eyrolles
- "Les réseaux, Principes fondamentaux", Pierre Rolin et al., Ed. Lavoisier/Hermes

Tools Used

Tools Used

- Operating System : Linux recommended (I am using Ubuntu 22.04.3 LTS)
- Network Simulator : Packet Tracer 8.1 Cisco / GNS3
- Network Packet Analyzer : *Wireshark*
  - http ://www.wireshark.org/

Introduction to Computer Networks

What is a Computer Network ?

- A computer network consists of a set of computers, servers, peripherals, and other electronic devices that share resources and communicate with each other.
- The main goal of a computer network is to facilitate the transfer of information and the sharing of resources, whether locally within a company, on a university campus, or across the global boundaries of the Internet.

Layered Models

OSI and TCP/IP Models

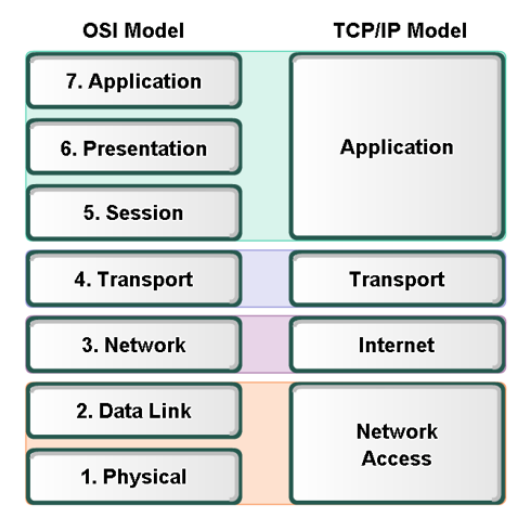


Figure 1 – OSI vs TCP/IP

Layered Models

OSI Model

- The OSI model (Open Systems Interconnection) consists of **7 distinct layers**.
- The model was created in 1978 by the International Organization for Standardization (ISO).
- Each of these layers operates with a number of protocols.

Layered Models

OSI Model

- The lower layers of the OSI model deal with the transportation of information, while the upper layers correspond to their processing.
- Each layer defines functionalities that are implemented by a protocol associated with the layer.
- Each layer provides a service to the layer above it.
- In other words, each layer utilizes the underlying layer to perform its function

Layered Models

OSI Model

To remember the 7 layers of the OSI model, from bottom to top and top to bottom, you can recall the following two sentences in English :

- **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way, which stands for : "Please Do Not Throw Sausage Pizza Away," where P represents *physical*, D *data link*, N *network*, T *transport*, S *session*, P *presentation*, and A *application*.

Layered Models

OSI Model

- **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing, which means : "All People Seem To Need Data Processing," where A represents *application*, P *presentation*, S *session*, T *transport*, N *network*, D *data link*, and P *physical*.

Layered Models

TCP/IP Model

- The TCP [a]/IP [b] model was created in the 1970s by the United States Department of Defense, specifically by the Defense Advanced Research Projects Agency (DARPA) [c].
- For this reason, it is also referred to by another name, namely the DoD [d] Model.
- The model in question consists of only **4 layers.**"

---

a. Transmission Control Protocol
b. Internet Protocol
c. Defense Advanced Research Projects Agency
d. Department of Defense

IPv_4 Addressing

IPv_4 Addressing

- An IPv_4 address, also known as a *logical* address, is an identification number consisting of 4 bytes, assigned permanently or temporarily to each network interface using the IPv_4 protocol.
- The IPv_4 address is assigned either manually by the local network administrator or automatically through the DHCP protocol. If a component has multiple interfaces, each of these interfaces has a specific IPv_4 address.
- IPv_4 addresses are generally written in dotted-decimal form, i.e., 4 integers from 0 to 255 separated by dots.

IPv_4 Addressing

Example

- The IPv_4 address 10.0.0.1 is in dotted-decimal form.
- The IPv_4 address 10.0.0.1 is represented in binary as : 00001010.00000000.00000000.00000001

IPv_4 Addressing

IPv_4 Addressing

The sequence of 4 Bytes in an IPv_4 address is divided into two parts :

- Net-ID : denotes the address of a network (*Network IDentifier*)
- Host-ID : denotes the address of a host machine (*Host IDentifier*) on the network specified by Net-ID.

IPv_4 Addressing

IPv_4 Classes

- IPv_4 addresses are divided into 5 classes.
- The lengths of the Net-ID and Host-ID fields vary, depending on the class of the IPv_4 address.

IPv_4 Addressing

IPv_4 Classes

- It is worth noting that this class-based distribution became **obsolete** later due to the **shortage** of IPv_4 addresses resulting from the rapid growth of internet usage.
- The **class-based addressing system** was replaced by **Classless Inter-Domain Routing** (CIDR[a]) in the mid-1990s.

a. Classless Inter-Domain Routing

IPv_4 Addressing

IPv_4 Classes

1. Class A (large networks) : These are addresses where the most significant bit is set to 0. The Net-ID is encoded in the first byte, and the remaining three octets represent the Host-ID.
   - **Range : from 1.0.0.0 to 126.255.255.255**.

   Remark : I deliberately excluded networks 0.0.0.0 and 127.0.0.0, where addresses represent the **absence of an IP address or the default route**, and the network of addresses known as **loopback addresses**, respectively.

IPv_4 Addressing

IPv_4 Classes

2. Class B (medium-sized networks) : These are addresses where the two most significant bits are 10. The Net-ID is encoded in 2 bytes, and the Host-ID in the remaining two bytes.
   - **Range : de 128.0.0.0 à 191.255.255.255**.

IPv_4 Addressing

IPv_4 Classes

3. Class C (Small networks) : These are addresses where the three most significant bits are 110. The Net-ID is encoded in the first 3 bytes, and the Host-ID in the last byte.
   - **Range : de 192.0.0.0 à 223.255.255.255**.

IPv_4 Addressing

IPv_4 Classes

4. Class D (Multicast[a]) : These are addresses where the 4 most significant bits are 1110. The remaining 28 bits in this case identify a multicast group. Addresses belonging to this class are used for sending multicast messages. For example, the address 224.0.0.9 is used by the Routing Information Protocol version 2 (RIPv2).
   - **Range : de 224.0.0.0 à 239.255.255.255**.

a. Multicast addressing is used to address a group of hosts simultaneously

IPv_4 Addressing

IPv_4 Classes

5. Class E (Reserved Class) : These are addresses where the 4 most significant bits are 1111. This class is reserved for future use.
   - **Range : de 240.0.0.0 à 247.255.255.255**.

IPv_4 Addressing

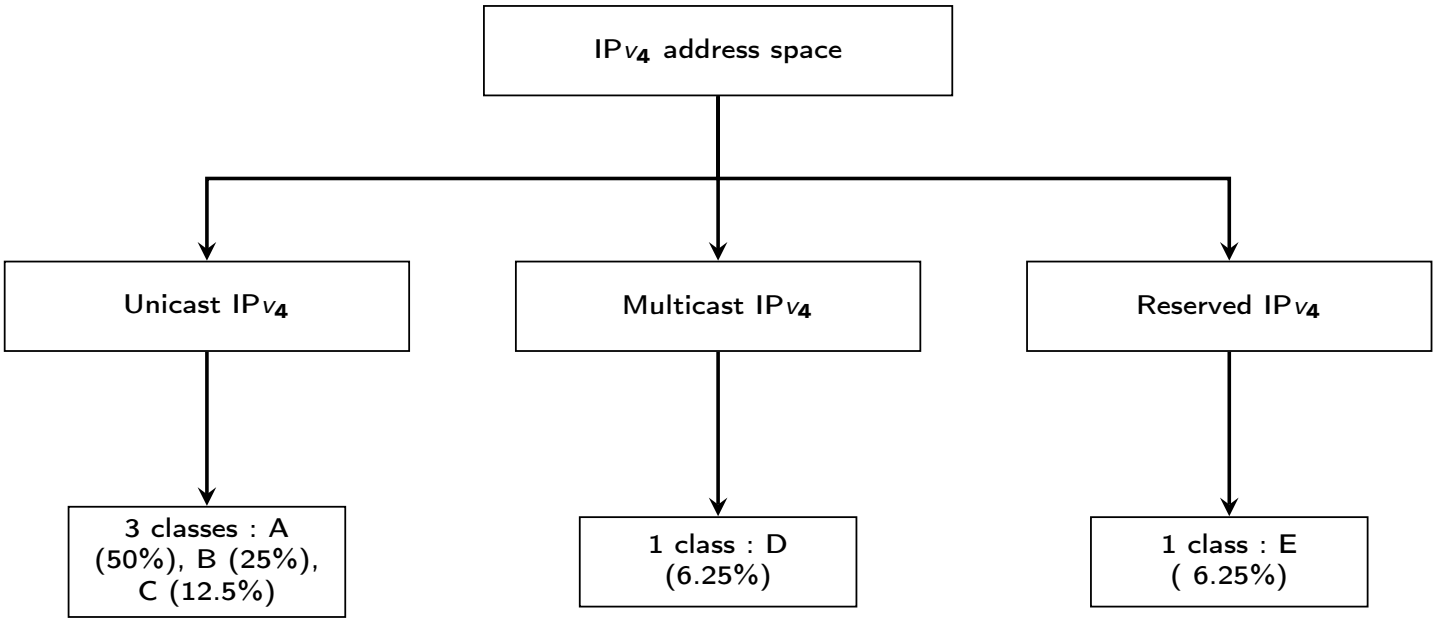


Figure 2 – Distribution of IPv_4 classes by communication type.

IPv_4 Addressing

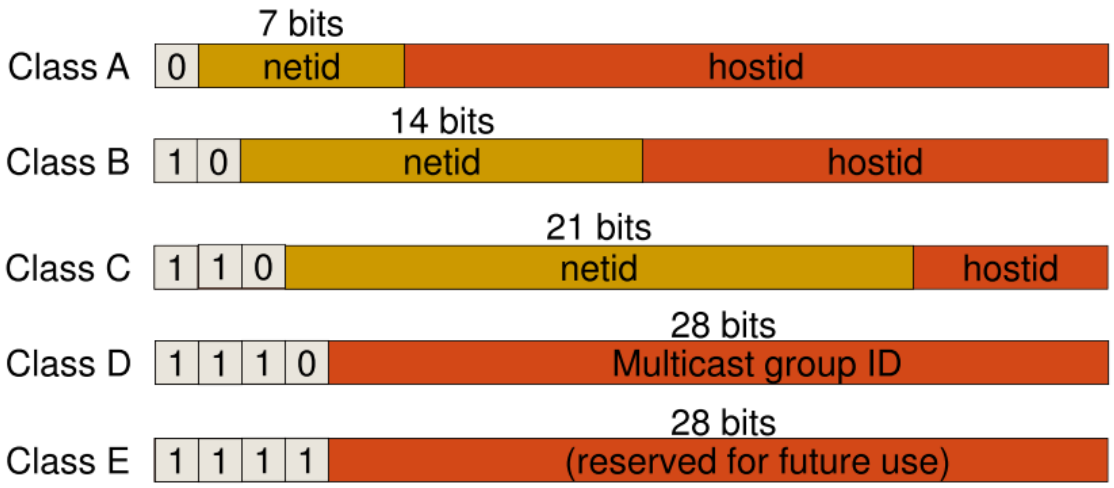


Figure 3 – Most Significant Bit Method for classifying IPv_4 addresses [1].

IPv_4 Addressing

Most significant bit method to classify IPv_4 addresses

1. **If the first bit is 0**, the address is **Class A**. There are 7 bits to identify the network and 24 bits to identify the host. Therefore :
   - 127 networks (from 1 to 127)
   - (2^{24} - 2) = 16 777 214 different hosts per network.
2. **If the first two bits are 10**, the address is **Class B**. There are 14 bits to identify the network and 16 bits to identify the host. Therefore :
   - 2^{14} = 16 384 networks (from 128.0 to 191.255)
   - (2^{16} - 2) = 65 534 different hosts per network.

IPv_4 Addressing

Most significant bit method to classify IPv_4 addresses

3. **If the first three bits are 110**, the address is **Class C**. There are 21 bits to identify the network and 8 bits to identify the host. Therefore :
   - 2^{21} = 2 097 152 networks (from 192.0.0 to 223.255.255)
   - (2^8 - 2) = 254 hosts per network.

IPv_4 Addressing

Most significant bit method to classify IPv_4 addresses

4. **If the first four bits of the address are 1110**, it is a special addressing class, **Class D**. This class is intended for "multicast" or "multipoint" communication (RFC 1112).
5. **If the first four bits of the address are 1111**, it is an experimental class, **Class E**. Class E addresses are reserved for future use.

Table 1 – Distribution into classes of the IPv4 address space.

Class	Most Signif. bit of the 1^{st} byte	Decimal range of the 1^{st} byte	Net. and Host address	Default subnet mask	N#	H# per network
A	0	1-126	N.H.H.H	255.0.0.0	126	16 777 214 (2^{24}-2)
B	10	128-191	N.N.H.H	255.255.0.0	16.384	65 534 (2^{16}-2)
C	110	192-223	N.N.N.H	255.255.255.0	2.097.152	254 (2^{8}-2)
D	1110	224-239	Intended for "multicast" or "multipoint"			.
E	1111	240-247	Reserved for future use			

IPv_4 Addressing

Reserved addresses

Certain IP addresses are reserved for specific purposes :

- The range of addresses for **APIPA** [a] is from 169.254.0.1 to 169.254.255.254. This range is used when a network interface configured as a DHCP client does not receive a response from a DHCP server. The initial purpose is to allow hosts in networks without a DHCP server to communicate with each other. It is important to note that APIPA addresses are only used in case of issues.

a. Automatic Private IPv4 Addressing

IPv_4 Addressing

Reserved addresses

- The network **127.0.0.0** is reserved for loopback testing, with the IP address 127.0.0.1 being the "localhost" address, i.e., the loopback address of your machine :
- **0.0.0.0** : Value indicating either the absence of an IPv4 address or the default route.

IPv_4 Addressing

Reserved addresses

- **255.255.255.255** : limited broadcast address. In this type of broadcast, the router on the local area network (LAN) does not forward the broadcast packet to any of its other connected network segments. Thus, the broadcast is limited within the LAN.

IPv_4 Addressing

Reserved addresses

- **The broadcast address associated with a network that corresponds to a host part of the address where all bits are set to 1**. This is called directed or targeted broadcast, where the broadcast is sent from one network to another network as a unicast IPv4 datagram packet. When the directed broadcast packet sent as unicast from one network reaches the destination network, it will be broadcast on the destination network.

IPv_4 Addressing

Private and Public IPv_4 addresses

Private addressing can be freely used by any administrator or user within their local network. In contrast, public addressing is subject to declaration and registration restrictions with a specialized organization, namely IANA [a]. This is what ISPs [b] do by acquiring a range of IPv4 addresses for their subscribers.

---

a. Internet Assigned Numbers Authority

b. Internet Service Provider : a company that provides access to the Internet.

IPv_4 Addressing

Private IPv_4 addresses

Private IPv4 addresses (RFC [a] 1918) are not routable to the Internet. Table 2 illustrates the different ranges of private IPv4 addresses.

a. Request For Comments

Table 2 – Ranges of private IPv_4 addresses.

Class	Range of private IPv_4 addresses
A	de 10.0.0.0 à 10.255.255.255 (One class A Network)
B	de 172.16.0.0 à 172.31.255.255 (16 class B Networks)
C	de 192.168.0.0 à 192.168.255.255 (255 classe C Networks)

IPv_4 Addressing

Public IPv_4 addresses

Unlike private IPv_4 addresses, public IPv_4 addresses are not used in a local network but only on the internet. Table 3 illustrates the different ranges of public IPv4 addresses. It is important to note that a public IPv4 address is an address that is globally unique.

Table 3 – Ranges of public IPv_4 addresses.

Class	Range of public IPv_4 addresses
A	1.0.0.0 - 9.255.255.255 11.0.0.0 - 126-255.255.255
B	128.0.0.0 - 169.253.255.255 169.255.0.0 à 172.15.255.255 172.32.0.0 - 191-255.255.255
C	192.0.0.0- 192.167.255.255 à 192.169.0.0 - 223-255.255.255

IPv_4 Addressing

Subnet Mask

- The subnet mask is a sequence of four bytes with bits corresponding to the Net-Id set to 1 and those of the Host-Id set to 0.
- By performing a bitwise "logical and" between an IPv_4 address and the associated mask, we obtain the network address to which it belongs.
- The pair (IPv4 address, mask) can be represented in CIDR notation as the IPv_4 address followed by a forward slash "/" and the number of bits set to 1 in the binary representation of the subnet mask.

IPv_4 Addressing

Subnet Mask

- The subnet mask associated with the address 192.168.1.1 is 255.255.255.0 since it is an IPv4 address of class C.
- In CIDR notation, the pair (IPv_4 address, mask) will be indicated as follows : 192.168.1.1/24.
- A bitwise "logical and" between 192.168.1.1 and 255.255.255.0 gives the network address 192.168.1.0 to which the IPv_4 address belongs.

IPv_4 Addressing

Subnet Mask

In IP addressing, both "subnet mask" and "network mask" are commonly used terminologies to refer to the same concept, which defines the boundary between the network prefix and the host identifier within an IP address.

IPv_4 Addressing

Subnet Mask

Classful addressing allows giving a single mask for all subnetworks, meaning all subnetworks will have the same number of hosts, which is not always optimal and leads to wastage at both the host address and subnetwork levels.

IPv_4 Addressing

CIDR

- *CIDR* stands for Classless Inter-Domain Routing (RFC**1518** and **1519**).
- It was proposed starting from 1994.

IPv_4 Addressing

CIDR

- It is a classless approach where an address is no longer implicitly considered to belong to one of the three classes A, B, or C.
- In CIDR, every IPv_4 address is explicitly associated with a mask that defines the prefix characterizing the network to which this address corresponds.
- Network addresses are therefore always used with their prefix, which can be of arbitrary size (e.g., /10, /17, /21).

IPv_4 Addressing

CIDR

CIDR is currently the most widely used system for managing and allocating IPv4 addresses. It was designed to replace class-based addressing. Its objectives are :

IPv_4 Addressing

CIDR

- CIDR allows networks to be divided into subnets of any size, making better use of address space and reducing wastage.
- CIDR, also known as supernetting, simplifies routing by aggregating IP addresses into larger blocks, which reduces the size of routing tables and improves the efficiency of routing on the internet.

IPv_4 Addressing

CIDR

We would like to remind in conclusion that :

- IPv4 addresses using CIDR addressing are called *classless* addresses.
- IPv4 addresses *classfull* designate addresses that use classful addressing.

IPv_4 Addressing

Subnetting

We will address subnetting through the following example : Let's consider the network address 134.214.0.0/16. We want to divide it into 4 subnetworks. For each subnetwork, we want to determine the subnet mask, subnet address, and broadcast address.

IPv_4 Addressing

Subnetting

First, let's recall :

- To obtain the network address, all bits of the Host-Id are set to 0.
- To obtain the broadcast address, all bits of the Host-Id are set to 1.

IPv_4 Addressing

Subnetting

Solution :

1. We want to divide the initial network into 4 subnetworks :
   - Knowing that $4 \leq 2^2$, the mask for each subnetwork is obtained by adding 2 bits set to 1 to the initial mask.
   - Note that these two bits are borrowed from the Host-Id part.

IPv_4 Addressing

Subnetting

- The initial mask is 255.255.0.0 (16 bits set to 1 followed by 16 bits set to 0).
- The new mask is : 255.255.192.0 (16 + 2 = 18 bits set to 1 (/18 in CIDR notation) followed by 14 bits set to 0).
- The Host-Id part, initially consisting of 16 bits (considering the given address belongs to class B), is now reduced to 14 bits after borrowing 2 bits to create 4 subnetworks from the initial network, which is 134.214.0.0/16.

IPv_4 Addressing

Subnetting

2. We will now determine the address of each subnetwork. To do this, we set all bits of the Host-Id to 0 :
   - 134.214.(00000000).0, so @(subnetwork 1) is 134.214.0.0/18
   - 134.214.(01000000).0, so @(subnetwork 2) is 134.214.64.0/18
   - 134.214.(10000000).0, so @(subnetwork 3) is 134.214.128.0/18
   - 134.214.(11000000).0, so @(subnetwork 4) is 134.214.192.0/18

IPv_4 Addressing

Subnetting

3. To obtain the broadcast addresses for each subnetwork, we set all bits of the Host-Id to 1 :
   - 134.214.(00111111).255, so @(broadcast of subnetwork 1) is 134.214.63.255/18
   - 134.214.(01111111).255, so @(broadcast of subnetwork 2) is 134.214.127.255/18
   - 134.214.(10111111).255, so @(broadcast of subnetwork 3) is 134.214.191.255/18
   - 134.214.(11111111).255, so @(broadcast of subnetwork 4) is 134.214.255.255/18

IPv_4 Addressing

Subnetting (Exercise)

Let's consider a class B network that has a subnet mask of 255.255.248.0.

1. How many bits were taken from the Host-Id part to create subnetworks ?
2. Deduce the number of possible subnetworks.
3. How many bits remain in the Host-Id part ?
4. Deduce the number of possible hosts for each subnetwork.

IPv_4 Addressing

Supernetting

Supernetting (also known as route summarization, route aggregation, or route summarization) allows aggregating IPv_4 addresses into a single address, reducing the size of routing tables and network traffic (fewer route advertisements by dynamic routing protocols, saving bandwidth).

IPv_4 Addressing

Supernetting

It should be noted that before proceeding with route aggregation, the following rules must be verified :

1. All networks must be contiguous.
2. The block size of each network must be the same (i.e., all networks must have the same size), and the total size of the supernet must be in the form of 2^n.

IPv_4 Addressing

Supernetting

2. The first network identifier (Net-ID) must be exactly divisible by the total size of the supernet. Note that the first network identifier means the smallest identifier.

IPv_4 Addressing

Supernetting/Example

- 200.1.0.0 / 24 (255.255.255.0)
- 200.1.1.0 / 24 (255.255.255.0)
- 200.1.2.0 / 24 (255.255.255.0)
- 200.1.3.0 / 24 (255.255.255.0)

IPv_4 Addressing

Supernetting/Example

First, we will verify if the 3 rules mentioned above are met :

1. Are the 4 networks contiguous ? $\rightarrow$ Yes : (200.1.0.0, 200.1.1.0, 200.1.2.0, 200.1.3.0). Indeed, the range of the first network is from 200.1.0.0 to 200.1.0.255. If you add 1 to the last IP address of the first network, i.e., 200.1.0.255 + 0.0.0.1, you get the next network identifier which is 200.1.1.0. By performing the same operation, you can verify that all networks are contiguous.

IPv_4 Addressing

Supernetting/Example

2. Are the 4 networks of the same size ? $\rightarrow$ Yes : The block size of each network is 2^8 (Host-ID=8 bits). Is the total size of the supernet in the form of 2^n ? $\rightarrow$ Yes : We have 4 blocks, i.e., $4 * 2^8 = 2^2 * 2^8 = 2^{10}$.

IPv_4 Addressing

Supernetting/Example

3. Is the first network identifier exactly divisible by the total size of the supernet ? $\rightarrow$ Yes :
   - The total size of the supernet is $4 * 2^8 = 2^2 * 2^8 = 2^{10}$ IPv4 addresses.
   - The first network identifier, which is 200.1.0.0/24, is indeed divisible by 2^{10} the last 10 bits are equal to 00.00000000, which proves that this identifier is divisible by 2^{10} because these last 10 bits represent the remainder of the division of this first network identifier by 2^{10}.

Supernetting/Remark

When a binary number is divided by 2^n, the last n bits represent the remainder of this division. Therefore, to prove that the first IPv_4 address is exactly divisible by the size of the supernet, we can check the last n bits if they are 0 or not.

Supernetting

To determine the supernet mask, we look at the common bits :

- 200.1.0.0 / 24 → 11001000.00000001.00000000.00000000
- 200.1.1.0 / 24 → 11001000.00000001.00000001.00000000
- 200.1.2.0 / 24 → 11001000.00000001.00000010.00000000
- 200.1.3.0 / 24 → 11001000.00000001.00000011.00000000

Supernetting

By counting the common bits (bits in blue), we can conclude that the supernet mask is /22.
Concerning the Net-Id, it is obtained by setting to 0 all the non-common bits, then we read the resulting addresses.
Typically, we would choose the lowest or the first address in the sequence :

Supernetting

- 200.1.0.0 / 24 → 11001000.00000001.00000000.00000000
- 200.1.1.0 / 24 → 11001000.00000001.00000000.00000000
- 200.1.2.0 / 24 → 11001000.00000001.00000000.00000000
- 200.1.3.0 / 24 → 11001000.00000001.00000000.00000000

Supernetting

- Therefore, the Net-Id is 200.1.0.0 and the aggregated route is : 200.1.0.0/22
- Remember that the number of 1s in the supernet mask is always less than the number of 1s in the original mask.

Supernetting

1. you can obtain the network ID of the aggregated route by taking the common bits from the given IP addresses and set the remaining bits to 0. Typically, you would choose the lowest or the first address in the sequence
2. you can determine the network ID of the aggregated route by taking the smallest identifier among the given IP addresses
3. you can obtain the network ID of the aggregated route by performing a bitwise logical AND operation between the given IP addresses

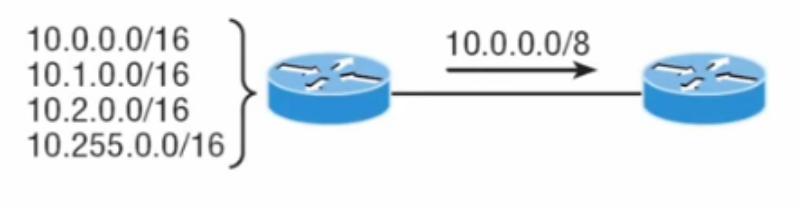


Figure 4 – Route agregation :Example 1 (Note : Invalid example : The networks must be adjacent in binary representation

Supernetting

The issues faced by the router in Example 1 :

1. **The Summarization Might Include Unwanted Networks :**
   If you try to summarize these subnets under a common prefix (e.g., 10.0.0.0/14 (If we consider the aggregation of only the first three networks) or 10.0.0.0/8 (If we consider the aggregation of all four networks)), you may end up including other networks that do not exist in your original list. This can cause the router to send packets to networks that do not belong to the intended range.

Supernetting

The issues faced by the router in Example 1 :

2. **Possible Traffic Blackholing :**
   If the router believes that a summarized route covers 10.0.0.0/14, but there is no actual device in 10.0.0.0/16 or 10.0.3.0/16, traffic to those networks might be dropped.
3. **Inefficient Routing and Wrong Forwarding :**
   If a packet for 10.0.4.0/16 arrives, and your router has summarized 10.1.0.0/16 - 10.3.0.0/16, the router might send it to the wrong next-hop because 10.0.4.0/16 was not explicitly excluded.

Supernetting

The issues faced by the router in Example 1 :

4. **Summarization Is Not Valid for Routing Protocols :**
   Dynamic routing protocols like OSPF [a], EIGRP [b], and BGP [c] typically do not summarize non-contiguous networks. You would need manual route filtering to avoid including unintended networks.

---

a. Open Shortest Path First
b. Enhanced Interior Gateway Routing Protocol
c. Border Gateway Protocol

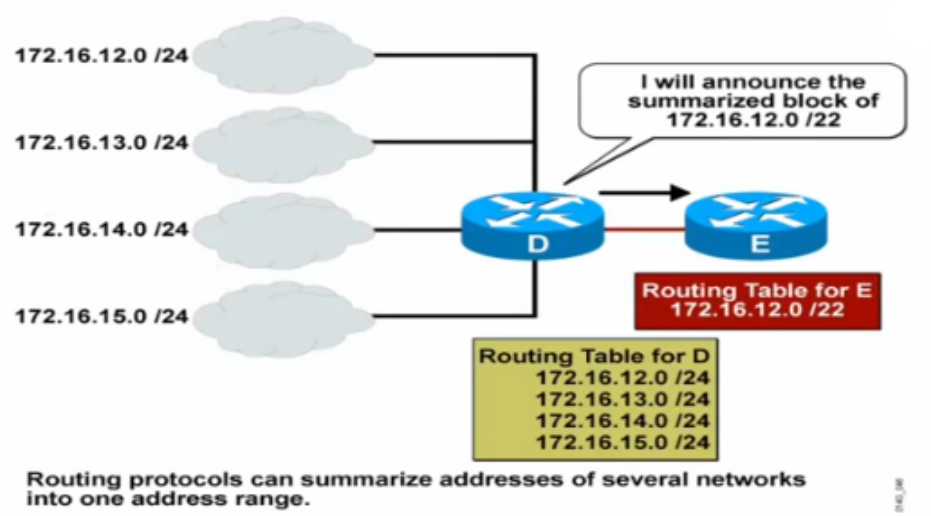


Figure 5 – Route Agregation :Example 2

Supernetting/Remark

- Number of subnets in the supernet = $2^{(\text{Number of 1s in the default mask - Number of 1s in the supernet mask})}$
- Number of IPv4 addresses in the supernet = $2^{(\text{Number of 0s in the supernet mask})}$

Supernetting/Exercise

Find the aggregated route for the following networks :

- 200.1.2.0/25
- 200.1.2.128/26
- 200.1.2.192/26

Supernetting

To find the addresses aggregated within a given route, you can use the following method :

- Determine the range of IP addresses that fall within the aggregated route. Calculate the network and broadcast addresses for the given route.
- Identify all the specific subnets that are encompassed by the aggregated route.

Supernetting

For example, if you have the aggregated route 172.16.12.0/22, you can find the specific subnets encompassed by this route by calculating the range of IP addresses, the network and broadcast addresses, and the specific subnets within this range. Using the route 172.16.12.0/22 as an example, the range of IP addresses within this route is from 172.16.12.0 to 172.16.15.255. The network address is 172.16.12.0, and the broadcast address is 172.16.15.255. The specific subnets within this aggregated route are 172.16.12.0/24, 172.16.13.0/24, 172.16.14.0/24, and 172.16.15.0/24

IPv_4 Addressing

VLSM

We first want to recall that to address the shortage of IPv_4 addresses, several solutions have been considered. VLSM (Variable Length Subnet Mask) is one of them :

IPv_4 Addressing

VLSM

1. Subnetting in 1985
2. Classless Inter-Domain Routing (CIDR) (RFCs 1517, 1518, 1519, and 1520) in 1993
3. Variable Length Subnet Mask (VLSM) (RFC 1009) in 1987
4. Network Address Translation (NAT)
5. Ultimate solution : IPv_6 (128 bits)

IPv_4 Addressing

VLSM

- In the 1990s, the internet was rapidly expanding, and the demand for IPv_4 addresses was growing exponentially.
- The protocols used at that time were called *classful* (like RIP v1 and IGRP), meaning they used the default masks of the address classes (255.0.0.0 for class A, 255.255.0.0 for class B, and 255.255.255.0 for class C).

IPv_4 Addressing

VLSM

- There was significant IPv_4 address waste, and a shortage of class B addresses was looming. In *classful* addressing, the number of networks and hosts is fixed, with the subnet mask itself being fixed.

IPv_4 Addressing

VLSM

VLSM is a technique that allows the creation of subnetworks with variable sizes, enabling a more efficient use of IP address space.

IPv_4 Addressing

VLSM

- We talk about VLSM when a network is divided into subnetworks of different sizes, which allows for better utilization of available addresses.

IPv_4 Addressing

VLSM

- Some dynamic protocols, such as BGP [a], OSPF [b], IS-IS [c], EIGRP [d] and RIPv2 [e], support VLSM because they always indicate a network mask associated with an advertised route.

---

a. Border Gateway Protocol
b. Open Shortest Path First
c. Intermediate system to Intermediate System
d. Enhanced Interior Gateway Routing Protocol
e. Routing Information Protocol Version 2

IPv_4 Addressing

VLSM

- Protocols like RIPv1 [a], IGRP [b] do not support VLSM.

---

a. Routing Information Protocol Version 2
b. Interior Gateway Routing Protocol), and EGP (Exterior Gateway Protocol

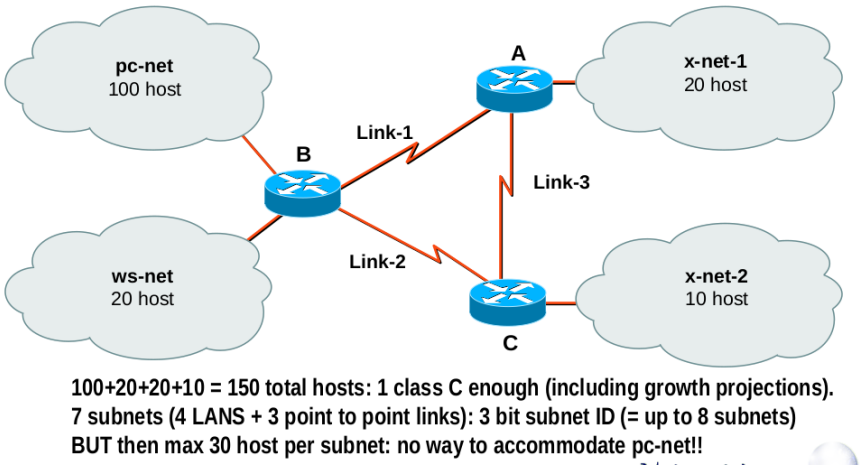


Figure 6 – Typical problem

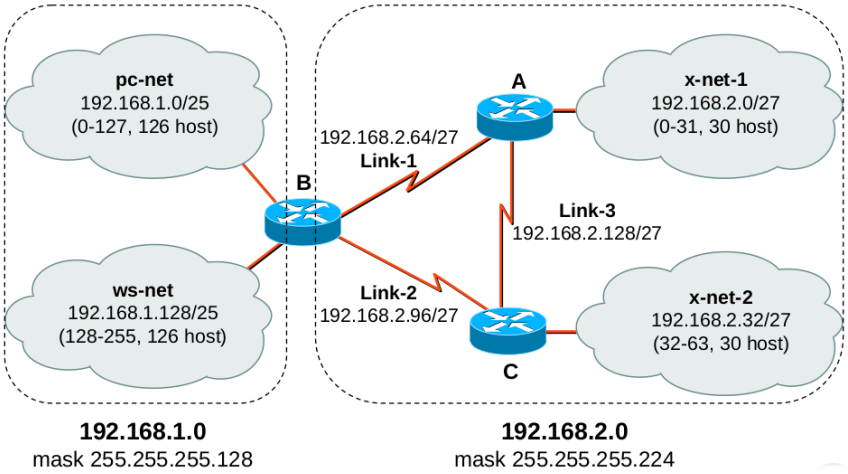


Figure 7 – Solution without VLSM, the problem requires 2 class C addresses.

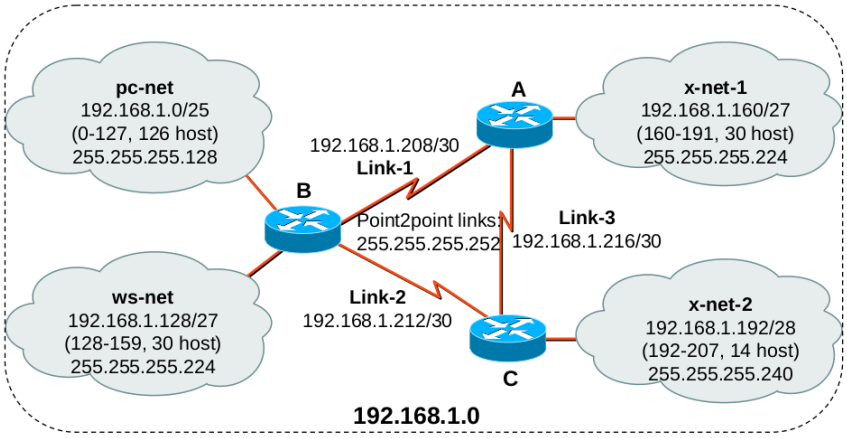


Figure 8 – Solution to the problem using VLSM : 1 class C address is sufficient

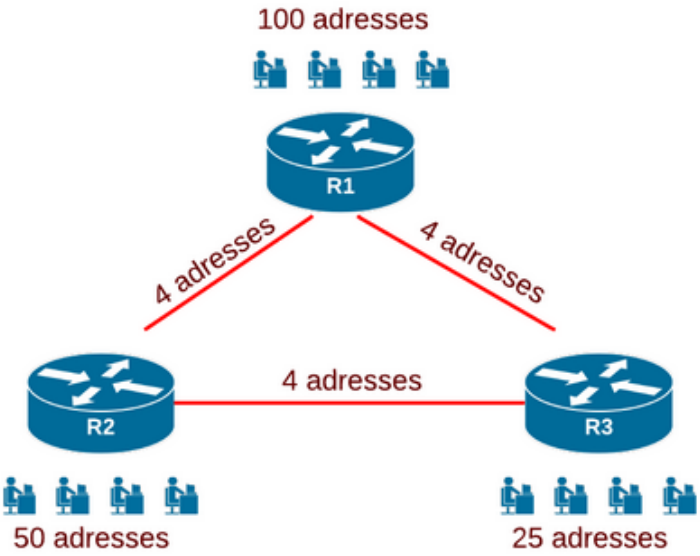
IPv_4 Addressing

VLSM

Let's consider the IPv4 network address : 195.167.46.0/24. We want to divide this network into three subnetworks :

- LAN de R1 100 PCs,
- LAN de R2 50 PCs,
- LAN de R3 25 PCs.

VLSM


100 adresses
R1
4 adresses
4 adresses
R2
4 adresses
R3
50 adresses
25 adresses

IPv_4 Addressing

VLSM

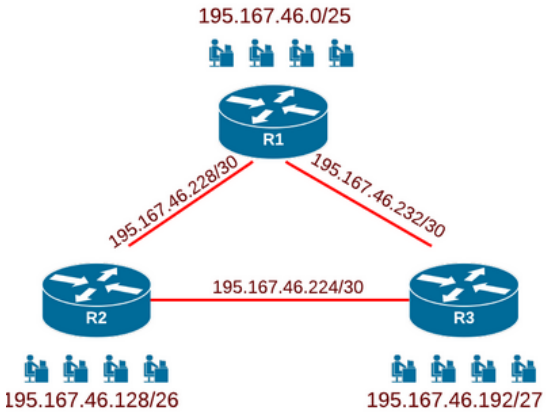
So, we have a block of 256 addresses (/24). Here, we propose to divide it as follows :

IPv_4 Addressing

VLSM

- A /25 block of 128 addresses for R1's LAN
  ($2^7 - 2 >= 100\,;\, 126 + 2$)
- A /26 block of 64 addresses for R2's LAN
  ($2^6 - 2 >= 50\,;\, 62 + 2$)
- A /27 block of 32 addresses for R3's LAN
  ($2^5 - 2 >= 50\,;\, 30 + 2$)
- For the remainder, we will take three /30 blocks of 4 addresses each to address the point-to-point connections.

IPv_4 Addressing



IPv_4 Addressing

Subnet	Nbr. of hosts	Subnet Addr.	Range	Broadcast addr.
LAN R1	100	195.167.46.0/25	195.167.46.1/25 → 195.167.46.126/25	195.167.46.127/25
LAN R2	50	195.167.46.128/26	195.167.46.129/26 → 195.167.46.190/26	195.167.46.191/26
LAN R3	25	195.167.46.192/27	195.167.46.193/27 → 195.167.46.222/27	195.167.46.223/27
R2-R3	4	195.167.46.224/30	195.167.46.225/30 → 195.167.46.226/30	195.167.46.227/30
R1-R2	4	195.167.46.228/30	195.167.46.229/30 → 195.167.46.230/30	195.167.46.231/30
R1-R3	4	195.167.46.232/30	195.167.46.233/30 → 195.167.46.234/30	195.167.46.235/30

 M. A. PERALDI-FRATI. La couche réseau : adresse ip. https://www.i3s.unice.fr/~map/Cours/LPSILADMIN/C3_Reseau_IP_CIDR_LPSIL.pdf, visité le 20.09.2022.