- Classful IPv4 addressing.
- IPv4 static routeing
- Practical exercises
- Support on Project 1 progress

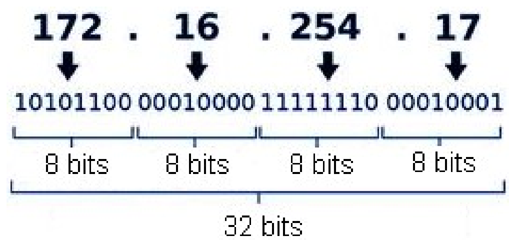
# 1. Classful IPv4 addressing

- An IPv4 address is a 32-bits number, for the sake of human handling, it is represented as four sets of eight bits (octets). Each octet is represented as a decimal number and octets are separated by a dot. This is called **dot-decimal representation**.

- The image shows an IPv4 address (172.16.254.17) representation.

- Each octet can have a value from zero $(00000000)_2$ up to 255 $(11111111)_2$.

- An IPv4 address is meant to uniquely identify a node, there shouldn´t be two nodes using the same address.




- To make routeing easier, nodes connected to the same LAN are grouped into networks, each network is also identified by a unique address.

- In fact, an IPv4 node address (32-bits) identifies both the node and the network the node belongs to.

- Nodes belonging to the same IPv4 network can communicate directly with each other's, for that to be possible they must also be connected to the same LAN (same broadcast domain).

- If two nodes belong to different IPv4 networks they are not able to communicate directly, even if they were connected to the same LAN (same broadcast domain).

- If two nodes belong to different IPv4 networks they may yet communicate by using routers.

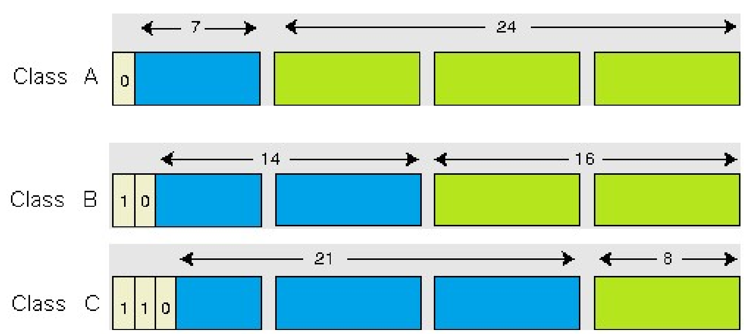
## 1.1. Classful IPv4 addresses and network masks

An IPv4 node address (32-bits) has two parts, the most significant bits are the network address (they uniquely identify the IPv4 network) and the remaining bits are used to identify the node within the network, the full 32-bits uniquely identify the node.

The number of more significant bits used to identify the network is called network prefix and it's not the same for every network. The network mask represents the network prefix by expressing in dot-decimal an IPv4 address where network bits have value 1 and node bits have value 0.

Classful addressing uses only three possible network prefixes: 8-bits, 16-bits, and 24-bits, correspondingly class A, B, and C networks. Therefore, corresponding network masks are 255.0.0.0, 255.255.0.0 and 255.255.255.0.

For classful addresses, the first most significant bits identify the class, and thus the network prefix and mask.



The image above represents the three classes of classful IPv4 addresses, blue bits are used to identify the network, and green bits are used to identify nodes within the network.

Given an IPv4 node address, we can determine the network address it belongs to by zeroing all bits beyond the network prefix, this is also equivalent to perform a bit-by-bit and operation with the network mask

Within every IPv4 network, two addresses are reserved, the address with all node bits having the zero value and the address with all node bits having the one value. The first represents the network´s address and the second the network's broadcast address. The number of different available networks and the maximum number of nodes each network can hold depend on the prefix/mask:

| First bits | Values for left octet | Class | Network mask | Available networks | Maximum valid nodes on each network |
|---|---|---|---|---|---|
| 0…. | 0 – 127 | A | 255.0.0.0 | $2^7 = 128$ | $(2^{24} - 2) = 16777214$ |
| 10… | 128 – 191 | B | 255.255.0.0 | $2^{14} = 16384$ | $(2^{16} - 2) = 65534$ |
| 110… | 192 – 223 | C | 255.255.255.0 | $2^{21} = 2097150$ | $(2^8 - 2) = 254$ |

Left octet values above 223 are reserved for special purposes like multicast.

## 2. IPv4 static routeing

IPv4 intermediate nodes operate at network layer transferring IPv4 packets between different networks, they are usually called routers or gateways.

IPv4 routers are connected to several local networks and make use of these local networks to forward IPv4 packets to other neighbour routers known as next-hops. Routers must know which networks are available behind each neighbour router, this knowledge is provided by the routeing table.

This is an example of a routeing table:

| **Destination** | | ***Next hop*** |
|---|---|---|
| **Network Address** | **Network Mask** | |
| 10.0.0.0 | 255.0.0.0 | 190.20.5.8 |
| 195.20.30.0 | 255.255.255 | 130.0.0.1 |
| 0.0.0.0 | 0.0.0.0 | 190.20.5.10 |

Each router only handles a single step (hop) in the path a packet has to follow to go from source to destination. A single bad routeing table, in a router along the path, will make the destination unreachable.

For every packet the router processes, the packet's destination address is matched with each entry at the routeing table, the idea is checking if the address belongs to the network in the table entry, if so, the packet is forwarded to the table´s entry next-hop, and the router mission is accomplished.

On the example above the last table's entry is called the default-route and the corresponding next-hop is called default-gateway. Due to the network and mask values used, the default-route matches any IPv4 address, it's therefore used to represent all remote networks that are unknown to a router.

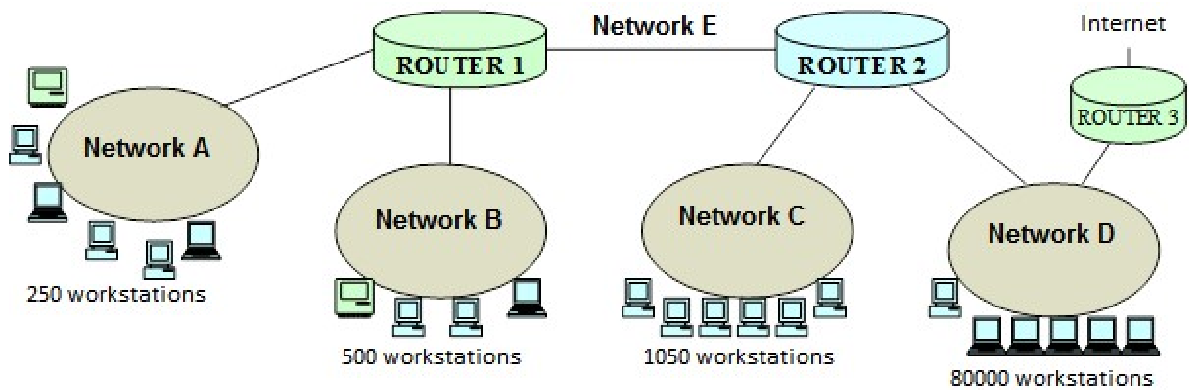
Defining a default-route in all routers is always required if the infrastructure has an internet connection, this is because it´s impossible to add all networks of the internet to a routeing table.

## 3. Practical exercises

**3.1. Given the following classful IPv4 node addresses, determine the IPv4 network address it belongs to, the first valid node address on that network and the broadcast address on that network.**

| | | | |
|---|---|---|---|
| a) | 195.34.56.30 | b) | 120.10.50.3 |
| c) | 170.17.23.8 | d) | 190.0.0.8 |

**3.2. See the following diagram representing several IPv4 networks interconnected by routers.**




a) Assign a classful network address to each network (A; B; C; D and E). For each network, the address must capable of supporting the specified number of nodes, and also, addresses wasting should be avoided as far as possible.

b) Accordingly, set the IPv4 node addresses of each router's interface.

c) Define each router's routeing table.

## 4. Support on Project 1 progress

### 4.1. Network outlets

The sprint one submission deadline is approaching (structured cabling). Once each room's area was estimated, the number of required outlets for each has been established.

Concerning network outlets for indoors wireless access-points, walls, slabs, and columns disturb the signal propagation, each access-point reach is always less than about 30 meters. To maximise coverage and avoid signal propagation to outdoors, access-points should be placed in floors central locations.

For a fair coverage of an area by a set of access-points, they ought to be closer than 50 meters from each other. As far as possible, access-points in adjacent floors ought to have different positions to avoid cells overlapping, later Wi-Fi channels will be assigned to each access-point reinforcing this cell overlapping issue.

Each individual outlet must be pinpointed in floor blueprints.

### 4.2. Cross-connects, cable pathways and cables

Having all outlets locations fixed, the next step it's deciding where to place each cross-connect. Several previously studied standards and guidelines, apply here.

Concerning horizontal cabling subsystems, remember no outlet can distance more than 80 meters from the horizontal cross-connect in a straight line, also cable length cannot be above 90 meters. If required consolidation points may be created.

Cable pathways outlining comes next. As far as possible, the maximum number of cables ought to share the same pathway, or at least part of it.

Now, each cable length can be calculated. A recheck on horizontal cabling lengths is prudent for the longer cables. Furthermore, all cable types can now be established. For lengths above 90 meters, the only available option is the optical fibre, all the same, backbones, in general, should use optical fibre. Backbone redundant connections must not be forgotten.

### 4.3. Patch-panels and telecommunication enclosures

Every cable entering a cross-connect is wired up to a patch panel. Being that the number of cables and cable types entering each cross-connect is now known, consistently, the number and type of required patch panels in each cross-connect can be settled.

The number of required connections at each cross-point must then be matched with patch-panel manufacturers' data, the vertical space occupied in the telecommunication enclosures is specified in U rack units. Typical 24 ports CAT6 copper patch panels take 1U and 48 ports CAT6 copper patch panels do occupy 2U on the telecommunications enclosure. Current optical fibre patch-panels have similar densities to copper patch-panels, older models are more modest: as low as four optical fibre connections for 1U.

Enforcing the previously suggested oversizing strategies, we can infer the telecommunications enclosures size by multiplying by four the amount of space required by housed patch-panels, and round it up to the next commercially available size.

### 4.4. Inventories

In fact, the structured cabling hardware inventory is mostly done, it's just an accounting mater to establish total numbers for network outlets, each type of patch-panel, and telecommunication enclosures. One key element yet missing from the inventory are cables themselves.

Building the cable inventory over the pathways blueprint can be a fairly significant effort, previously discussed simplification can be used.

Patch cords are not regarded as structured cabling hardware, but they are ultimately required. Copper and optical fibre patch-cords are commercially available ranging from 0.5 meters up to 5 meters long. Inside telecommunications enclosures 0.5 meters models are most appropriate to connect patch-panels to active hardware.