Xarxes i Protocols

Miquel Rodríguez Juvany

2n Trimestre

Índex

[1. Network Components 4](#_Toc134179466)

[1.1 Host Roles 4](#_Toc134179467)

[1.2 End Devices 4](#_Toc134179468)

[1.3 Intermediary Network Devices 4](#_Toc134179469)

[1.4 Network Media 5](#_Toc134179470)

[2. Network Representations and Topologies 6](#_Toc134179471)

[2.1 Network Representations 6](#_Toc134179472)

[2.2 Topology Diagrams 6](#_Toc134179473)

[3. Common Types of Networks 7](#_Toc134179474)

[3.1 Networks of Many Sizes 7](#_Toc134179475)

[3.2 LANs and WANs 7](#_Toc134179476)

[3.3 The Internet 7](#_Toc134179477)

[4. Internet Connections 8](#_Toc134179478)

[4.1 Internet Access Technologies 8](#_Toc134179479)

[4.2 The Converging Network 8](#_Toc134179480)

[5. Reliable Networks 9](#_Toc134179481)

[5.1 Network Architecture 9](#_Toc134179482)

[5.2 Fault Tolerance 9](#_Toc134179483)

[5.3 Scalability 9](#_Toc134179484)

[2. Protocols and Models 10](#_Toc134179485)

[2.1 The Rules 10](#_Toc134179486)

[2.1.1 Communications Fundamentals 10](#_Toc134179487)

[2.1.2 Communications Protocols 10](#_Toc134179488)

[2.1.3 Rule Establishment (Cont.) 10](#_Toc134179489)

[2.1.4 Network Protocol Requirements 10](#_Toc134179490)

[2.1.5 Message Encoding 11](#_Toc134179491)

[2.1.6 Message Formatting and Encapsulation 11](#_Toc134179492)

[2.1.7 Message Size 11](#_Toc134179493)

[2.1.8 Message Timing 11](#_Toc134179494)

[2.1.9 Message Delivery Options 12](#_Toc134179495)

[2.1.10 A Note About the Node Icon 12](#_Toc134179496)

[2.2 Protocols 13](#_Toc134179497)

[2.2.1 Network Protocol Overview 13](#_Toc134179498)

[2.2.2 Network Protocol Functions 13](#_Toc134179499)

[2.2.3 Protocol Interaction 13](#_Toc134179500)

[2.3 Protocol Suites 14](#_Toc134179501)

[2.3.1 Network Protocol Suites 14](#_Toc134179502)

[2.3.2 Evolution of Protocol Suites 14](#_Toc134179503)

[2.3.3 TCP / IP Protocol Example 14](#_Toc134179504)

[2.3.4 TCP / IP Protocol Suite 15](#_Toc134179505)

[2.3.5 TCP / IP Communication Process 15](#_Toc134179506)

[2.4 Standards Organizations 16](#_Toc134179507)

[2.4.1 Internet Standards 16](#_Toc134179508)

[2.5 Reference Models 16](#_Toc134179509)

[2.5.1 The benefits of Using a Layered Model 16](#_Toc134179510)

[2.5.2 The OSI Reference Model 17](#_Toc134179511)

[2.5.3 The TCP/IP Reference Model 17](#_Toc134179512)

[2.5.4 OSI and TCP/IP Model Comparison 18](#_Toc134179513)

[2.6 Data Encapsulation 18](#_Toc134179514)

[2.6.1 Segmenting Messages 18](#_Toc134179515)

[2.6.2 Sequencing 18](#_Toc134179516)

[2.6.3 Protocol Data Units 19](#_Toc134179517)

[2.6.4 Encapsulation Example 19](#_Toc134179518)

[2.6.5 De-encapsulation Example 20](#_Toc134179519)

[2.7 Data Access 20](#_Toc134179520)

[2.7.1 Addresses 20](#_Toc134179521)

[2.7.2 Layer 3 Logical Address 21](#_Toc134179522)

[2.7.3 Devices on the Same Network 21](#_Toc134179523)

[2.7.4 Role of the Data Link Layer Addresses: Same IP Network 22](#_Toc134179524)

[2.7.5 Devices on a Remote Network 22](#_Toc134179525)

[2.7.6 Role of the Network Layer Addresses 22](#_Toc134179526)

[2.7.7 Role of the Data Link Layer Addresses: Different IP Networks 23](#_Toc134179527)

[2.7.8 Data Link Addresses 24](#_Toc134179528)

[3. IP Protocol (I) 26](#_Toc134179529)

[3.1 IP – The Internet Protocol 26](#_Toc134179530)

[3.1.1 IP Protocol. Concepts 26](#_Toc134179531)

[3.1.2 IP Service 27](#_Toc134179532)

# 1. Network Components

## 1.1 Host Roles

Every computer on a network is called a host or end device.

Servers are computers that provide information to end devices:

* Email servers: An email server runs an email server software. Clients use client software to access email.
* Web servers: A web server runs a web server software. Clients use browser software to access web pages.
* File servers: A file server stores corporate and user files. The client devices access these files.

Clients are computers that send requests to the servers to retrieve information:

* Web page from a web server.
* Email from an email server.

## 1.2 End Devices

An end device is where a message originates from or where it is received. Data originates with an end device, flows through the network, and arrives at an end device.

Diagrama

Descripción generada automáticamente

## 1.3 Intermediary Network Devices

An intermediary device interconnects end devices. Examples include switches, wireless access points, routers, and firewalls.

Management of data as it flows through a network is also the role of an intermediary device, including:

* Regenerate and retransmit data signals.
* Maintain information about what pathways exist in the network.
* Notify other devices of errors and communication failures.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

## 1.4 Network Media

Communication across a network is carried through a medium which allows a message to travel from source to destination.

Media types and its descriptions:

* **Metal wires within cables**: Uses electrical impulses.
* **Glass or plastic fibres within cables (fibre-optic cable)**: Uses pulses of light.
* **Wireless transmission**: Uses modulation of specific frequencies of electromagnetic waves.

# 2. Network Representations and Topologies

## 2.1 Network Representations

Network diagrams, often called topology diagrams, use symbols to represent devices within the network.

Important terms to know include:

* Network Interface Card (NIC)
* Physical Port
* Interface

**Note**: Often, the terms port and interface are used interchangeably.

## 2.2 Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cables installation.

Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.

# 3. Common Types of Networks

## 3.1 Networks of Many Sizes

Small Home Networks – connect a few computers to each other and the Internet.

Small Office / Home Office – enables computer within a home or remote office to connect to a corporate network.

Medium to Large Networks – many locations with hundreds of thousands of interconnected computers.

World Wide Networks – connects hundreds of millions of computers world-wide – such as the Internet.

## 3.2 LANs and WANs

Network infrastructures vary greatly in terms of:

* Size of the covered area
* Number of connected users
* Number and types of available services
* Area of responsibility

Two most common types of networks:

* Local Area Network (LAN)
* Wide Area Network (WAN)

A LAN is a network infrastructure that spans a small geographical area.

* Interconnects end devices in a limited area.
* Administered by a single organization or individual.
* Provides high-speed bandwidth to internal devices.

A WAN is a network infrastructure that spans a wide geographical area.

* Interconnects LANs over wide geographical areas.
* Typically administered by one or more service providers.
* Typically provides slower speed links between LANs.

## 3.3 The Internet

The Internet is a worldwide collection of interconnected LANs and WANs.

* LANs are connected to each other using WANs.
* WANs may use copper wires, fibre optic cables, and wireless transmissions.

The Internet is not owned by any individual or group. IETF, ICANN or AIB were groups developed to help maintain structures on the Internet.

# 4. Internet Connections

## 4.1 Internet Access Technologies

There are many ways to connect users and organizations to the Internet:

Popular services for home users and small offices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

Organizations need faster connections to support IP phones, video conferencing and data centre storage.

Business-class interconnections are usually provided by **service providers (SP)** and may include business DSL, leased lines, and Metro Ethernet.

## 4.2 The Converging Network

Before converged networks, an organization would have been separately cabled for telephone, video, and data. Each of these networks would use different technologies to carry the signal.

Each of these technologies would use a different set of rules and standards.

**Converged data networks** carry multiple services on one link including:

* Data
* Voice
* Video

Converged networks can deliver data, voice, and video over the same network infrastructure. The network infrastructure uses the same set of rules and standards.

# 5. Reliable Networks

## 5.1 Network Architecture

Network Architecture refers to the technologies that supports the infrastructure that moved data across the network.

There are four basic characteristics that are underlying architectures need to address to meet user expectations:

* Fault Tolerance
* Scalability
* Quality of Service (QoS)
* Security

## 5.2 Fault Tolerance

A fault tolerant network limits the impact of a failure by limiting the number of affected devices. Multiple paths are required for fault tolerance.

Reliable networks provide redundancy by implementing a packet switched network:

* Packet switching splits traffic into packet that are router over a network.
* Each packet could theoretically take a different path to the destination.

This is not possible with circuit-switched networks which establish dedicated circuits.

## 5.3 Scalability

A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.

Network designers follow accepted standards and protocols in order to make the networks scalable.

# 2. Protocols and Models

## 2.1 The Rules

### 2.1.1 Communications Fundamentals

Networks can vary in size and complexity. It is not enough to have a connection. Devices must agree on “how” to communicate.

There are three elements to any communication:

* There will be a source (sender).
* There will be a destination (receiver).
* There will be a channel (media) that provides for the path of communications to occur.

### 2.1.2 Communications Protocols

All communications are governed by protocols. Protocols are the rules that communications will follow. These rules will vary depending on the protocol.

### 2.1.3 Rule Establishment (Cont.)

Protocols must account for the following requirements:

* An identified sender and receiver.
* Common language and grammar.
* Speed and timing of delivery.
* Confirmation or acknowledgement requirements.

### 2.1.4 Network Protocol Requirements

Common computer protocols must be in agreement and include the following requirements:

* Message encoding
* Message formatting and encapsulation
* Message size
* Message timing
* Message delivery options

### 2.1.5 Message Encoding

Encoding is the process of converting information into another acceptable form for transmission.

Decoding reverses this process to interpret the information.

### 2.1.6 Message Formatting and Encapsulation

When a message is sent, it must use a specific format or structure.

Message formats depend on the type of message and the cannel that is used to deliver the message.

### 2.1.7 Message Size

Encoding between hosts must be in an appropriate format for the medium.

* Messages sent across the network are converted to bits.
* The bits are encoded into a pattern of light, sound, or electrical impulses.
* The destination host must decode the signals to interpret the message.

### 2.1.8 Message Timing

Message timing includes the following:

* **Flow Control** – Manages the rate of data transmission and defines how much information can be sent and the speed at which it can be delivered.
* **Response Timeout** – Manages how long a device waits when it does not hear a reply from the destination.
* **Access Method** – Determines when someone can send a message.
  + There may be various rules governing issues like “collisions”. This is when more than one device sends traffic at the same time and the messages become corrupt.
  + Some protocols are proactive and attempt to prevent collisions; other protocols are reactive and establish a recovery method after the collision occurs.

### 2.1.9 Message Delivery Options

Message delivery may one of the following methods:

* **Unicast** – one to one communication.
* **Multicast** – one to many, typically not all.
* **Broadcast** – one to all.

**Note**: Broadcast are used in IPv4 networks, but are not an option for IPv6. Later we will also see “Anycast” as an additional delivery option for IPv6.

### 2.1.10 A Note About the Node Icon

Documents may use the node icon, typically a circle, to represent all devices.

The figure illustrates the use of the node icon for delivery options.

Gráfico, Gráfico de dispersión

Descripción generada automáticamente

Unicast: De un a un.

Multicast: Movistar+, Netflix…

Broadcast: Televisió, radio…

Control de flux: Gestiona la velocitat d’extrem a extrem.(equip origen – equip destí)

Control de congestió: Igual que l’anterior però amb dispositius intermitjos.

## 2.2 Protocols

### 2.2.1 Network Protocol Overview

Network protocols define a common set of rules.

Protocol Type and Description:

* **Network Communications**: enable two or more devices to communicate over one or more networks.
* **Network Security**: secure data to prove authentication, data integrity, and data encryption.
* **Routing**: enables routers to exchange route information, compare path information, and select best path.
* **Service Discovery**: used for the automatic detection of devices or services.

### 2.2.2 Network Protocol Functions

Devices use agreed-upon protocols to communicate.

Protocols may have one or more functions.

Function and Description:

* **Addressing**: Identifies sender and receiver.
* **Reliability**: Provides guaranteed delivery.
* **Flow Control**: Ensures data flows at an efficient rate.
* **Sequencing**: Uniquely labels each transmitted segment of data.
* **Error Detection**: Determines if data became corrupted during transmission.
* **Application Interface**: Process-to-process communications between network applications.

### 2.2.3 Protocol Interaction

Networks require the use of several protocols.

Each protocol has its own function and format.

Protocol and Function:

* **Hypertext Transfer Protocol**: Governs the way a web server and web client interact. Defines content and format.
* **Transmission Control Protocol** **(TCP)**: Manages the individual conversations. Provides guaranteed delivery. Manages flow control.
* **Internet Protocol (IP)**: Delivers messages globally from the sender to the receiver.
* **Ethernet**: Delivers messages from one NIC to another NIC on the same Ethernet Local Area Network (LAN).

## 2.3 Protocol Suites

### 2.3.1 Network Protocol Suites

Protocols must be able to work with other protocols.

Protocol suite:

* A group of inter-related protocols necessary to perform a communication function.
* Sets of rules that work together to help solve a problem.

The protocols are viewed in terms of layers:

* Higher Layers.
* Lower Layers – concerned with moving data and provide services to upper layers.

### 2.3.2 Evolution of Protocol Suites

There are several protocol suites.

* **Internet Protocol Suite or TCP/IP**: The most common protocol suite and maintained by the Internet Engineering Task Force (IETF).
* **Open Systems Interconnection (OSI) protocols**: Developed by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU).
* **AppleTalk**: Proprietary suite release by Apple Inc.
* **Novell NetWare**: Proprietary suite developed by Novell Inc.

### 2.3.3 TCP / IP Protocol Example

Diagrama

Descripción generada automáticamente con confianza media

TCP/IP protocols operate at the application, transport and internet layers.

The most common network access layer LAN protocols are Ethernet and WLAN (Wireless LAN).

### 2.3.4 TCP / IP Protocol Suite

TCP/IP is the protocol suite used by the Internet and includes many protocols.

TCP /IP is:

* An open standard protocol suite that is freely available to the public and can be used by any vendor.
* A standards-based protocol suite that is endorsed by the networking industry and approved by a standards organization to ensure interoperability.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

### 2.3.5 TCP / IP Communication Process

1. A web server encapsulating and sending a web page to a client.
2. A client de-encapsulating the web page for the web browser.

Gráfico, Gráfico de cajas y bigotes

Descripción generada automáticamente

## 2.4 Standards Organizations

### 2.4.1 Internet Standards

* **Internet Society (ISOC)**: Promotes the open development and evolution of Internet.
* **Internet Architecture Board (IAB)**: Responsible for management and development of Internet standards.
* **Internet Engineering Task Force (IETF)**: Develops, updates, and maintains Internet and TCP/IP technologies.
* **Internet Research Task Force (IRTF)**: Focused on long-term research related to Internet and TCP/IP protocols.

Standards organizations involved with the development and support of TCP/IP:

* **Internet Corporation for Assigned Names and Numbers (ICANN)**: Coordinates IP address allocation, the management of domain names, and assignment of other information.
* **Internet Assigned Numbers Authority (IANA)**: Oversees and manages IP address allocation, domain name management, and protocol identifiers for ICANN.

## 2.5 Reference Models

### 2.5.1 The benefits of Using a Layered Model

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamenteComplex concepts such as how a network operates can be difficult to explain and understand. For this reason, a layered model is used.

Two layered models describe network operations:

* Open System Interconnection (OSI) Reference Model
* TCP/IP Reference Model

These are the benefits of using a layered model:

* Assist in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below.
* Foster competition because products from different vendors can work together.
* Prevent technology or capability changes in one layer from affecting other layers above and below.
* Provide a common language to describe networking functions and capabilities.

### 2.5.2 The OSI Reference Model

Tabla

Descripción generada automáticamente

### 2.5.3 The TCP/IP Reference Model

Aplicación

Descripción generada automáticamente con confianza baja

### 2.5.4 OSI and TCP/IP Model Comparison

Gráfico

Descripción generada automáticamenteThe OSI model divides the network access layer and the application layer of the TCP/IP model into multiple layers.

The TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium.

OSI layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

## 2.6 Data Encapsulation

### 2.6.1 Segmenting Messages

Gráfico, Diagrama

Descripción generada automáticamenteSegmenting is the process of breaking up messages into smaller units.

Multiplexing is the process of taking multiple streams of segmented data and interleaving them together.

Segmenting messages has two primary benefits:

* **Increases speed** – Large amounts of data can be sent over the network without typing up a communications link.
* **Increases efficiency** – Only segments which fail to reach the destination need to be retransmitted, not the entire data stream.

### 2.6.2 Sequencing

Diagrama

Descripción generada automáticamenteSequencing messages if the process of numbering the segments so that the message may be reassembled at the destination.

TCP is responsible for sequencing the individual segments.

### 2.6.3 Protocol Data Units

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamenteEncapsulation is the process where protocols add their information to the data.

* At each stage of the process, a PDU has a different name to reflect its new functions.
* There is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite.
* PDUs passing down the stack are as follows:
  + Data (Data Stream)
  + Segment
  + Packet
  + Frame
  + Bits (Bit Stream)

Diagrama

Descripción generada automáticamente

### 2.6.4 Encapsulation Example

Interfaz de usuario gráfica

Descripción generada automáticamenteEncapsulation is a top down process.

The level above does its process and then passes it down to the next level of the model. This process is repeated by each layer until it is sent out as a bit stream.

### 2.6.5 De-encapsulation Example

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente con confianza mediaData is re-encapsulated as it moves up the stack.

When a layer completes its process, that layer strips off its header and passes it up to the next level to be processed. This is repeated at each layer until it is a data stream that the application can process.

1. Received as Bits (Bit Stream)
2. Frame
3. Packet
4. Segment
5. Data (Data Stream)

## 2.7 Data Access

### 2.7.1 Addresses

Both the data link and network layers use addressing to deliver data from source to destination.

**Network layers source and destination addresses** – Responsible for delivering the IP packet from original source to the final destination.

**Data link layer source and destination addresses** – Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.

Diagrama

Descripción generada automáticamente

### 2.7.2 Layer 3 Logical Address

The IP packet contains two IP addresses:

* **Source IP address** – The IP address of the sending device, original source of the packet.
* **Destination IP address** – The IP address of the receiving device, final destination of the packet.

These addresses may be on the same link or remote.

Diagrama

Descripción generada automáticamente

All IP address contains two parts:

* **Network portion (IPv4)**
  + The left-most part of the address indicates the network group which the IP address is a member.
  + Each LAN or WAN will have the same network portion.
* **Host portion (IPv4)**
  + The remaining port of the address identifies a specific device within the group.
  + This portion is unique for each device on the network.

### 2.7.3 Devices on the Same Network

Diagrama

Descripción generada automáticamenteWhen devices are on the same network the source and destination ill have the same number in network portion of the address.

* PC1 – 192.168.1.110
* FTP Server – 192.168.1.9

### 2.7.4 Role of the Data Link Layer Addresses: Same IP Network

Diagrama

Descripción generada automáticamenteWhen devices are on the same Ethernet network the data link frame will use the actual MAC address of the destination NIC.

MAC addresses are physically embedded into the Ethernet NIC and are local addressing.

* The Source MAC address will be that of the originator on the link.
* The Destination MAC address will always be on the same link as the source, even if the ultimate destination is remote.

### 2.7.5 Devices on a Remote Network

Diagrama

Descripción generada automáticamenteWhat happens when the actual (ultimate) destination is not on the same LAN and is remote?

What happens when PC1 tries to reach the Web Server?

Does this impact the network and data link layers?

### 2.7.6 Role of the Network Layer Addresses

When the source and destination have a different network portion, this means they are on different networks.

* Diagrama

  Descripción generada automáticamentePC1 – 192.168.1
* Web Server – 172.16.1

### 2.7.7 Role of the Data Link Layer Addresses: Different IP Networks

When the final destination is remote, Layer 3 will provide Layer 2 with the local default gateway IP address, also knows as the router address.

* The default gateway (DGW) is the router interface IP address that is part of this LAN and will be the “door” or “gateway” to all other remote locations.
* All devices on the LAN must be told about this address or their traffic will be confined to the LAN only.
* Once Layer 2 on PC1 forwards to the default gateway (Router), the router then can start the routing process of getting the information to actual destination.

Diagrama

Descripción generada automáticamente

The data link addressing is local addressing so it will have a source and destination for each link.

The MAC addressing for the first segment is:

* Source – AA-AA-AA-AA-AA-AA (PC1) sends the frame.
* Destination – 11-11-11-11-11-11 (R1 – Default Gateway MAC) receives the frame.

Diagrama

Descripción generada automáticamente

### 2.7.8 Data Link Addresses

Since data link addressing is local addressing, it will have a source and destination for each segment or hop of the journey to the destination.

The MAC addressing for the first segment is:

* Source – (PC1 NIC) sends frame.
* Destination – (First router – DGW interface) receives frame.

Diagrama

Descripción generada automáticamente

The MAC addressing for the second hop is:

* Source – (First Router – Exit interface) sends frame
* Destination – (Second router) receives frame.

Diagrama

Descripción generada automáticamente

The MAC addressing for the last segment is:

* Source – (Second Router – exit interface) sends frame.
* Destination – (Web server NIC) receives frame.

Diagrama

Descripción generada automáticamente

Notice that the packet is not modified, but the frame is changed, therefore the L3 IP addressing does not change from segment to segment like the L2 MAC addressing.

The L3 addressing remains the same since it is global and the ultimate destination is still the Web Server.

Diagrama

Descripción generada automáticamente con confianza media

# 3. IP Protocol (I)

## 3.1 IP – The Internet Protocol

Diagrama

Descripción generada automáticamente

### 3.1.1 IP Protocol. Concepts

IP (Internet Protocol) is a Network Layer Protocol.

IP’s current version is Version 4 (IPv4). It is specified in RFC 891.

IP is the highest layer protocol which is implemented at both routers and hosts.

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

### 3.1.2 IP Service