

Erasmus Plus Programme – KA2 Strategic Partnerships for higher education



IO1: Industrial Cyber Security Training Course for Technicians in Industry 4.0

English Version

Project № 2018-1-ES01-KA203-050493



This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein



Co-funded by the
Erasmus+ Programme
of the European Union



MODULE 1

Industrial Systems - Components and Characteristics

1.1 Components of an Industrial Control System

Description

1.1 Components of an Industrial Control System

Table of contents

1. Definition of an Industrial Control System

2. Structure

- 2.1. Field level (level 0)
- 2.2. Direct Control (level 1)
- 2.3. Plant Supervisory (level 2)
- 2.4. Production Control (level 3)
- 2.5. Production Scheduling (level 4)

Industrial Control System (ICS) is a general term that encompasses several types of control systems, networks and associated instrumentation used for industrial process control. As it is shown in Figure 1.1, process control is implemented using loops in which the value of a measured process variable (PV) is automatically adjusted to equal the value of a desired set-point (SP). It includes the process sensor, the controller function, and the final control element (FCE) which are required for automatic control.

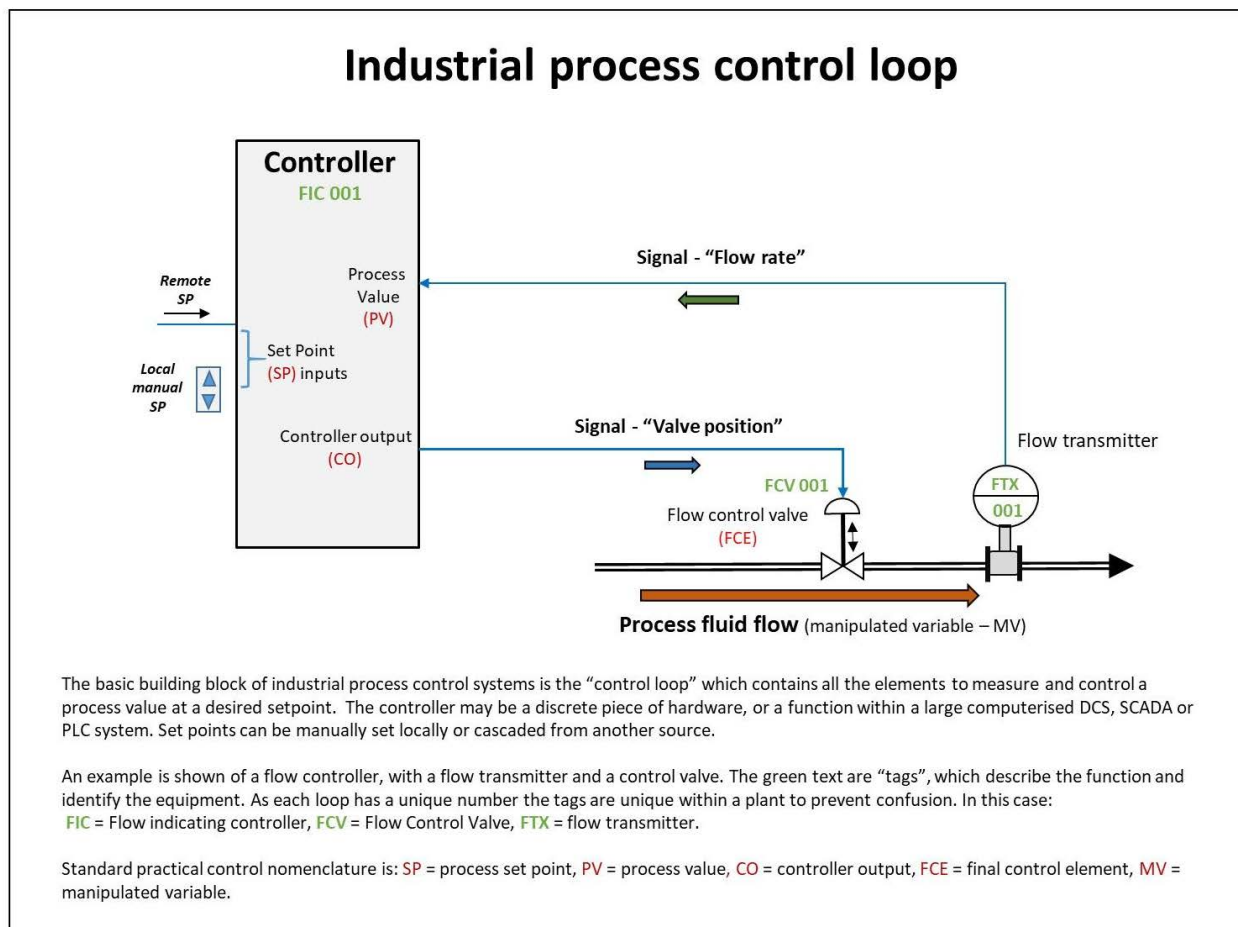


Figure 1.1- Industrial process control loop (source: Wikipedia)

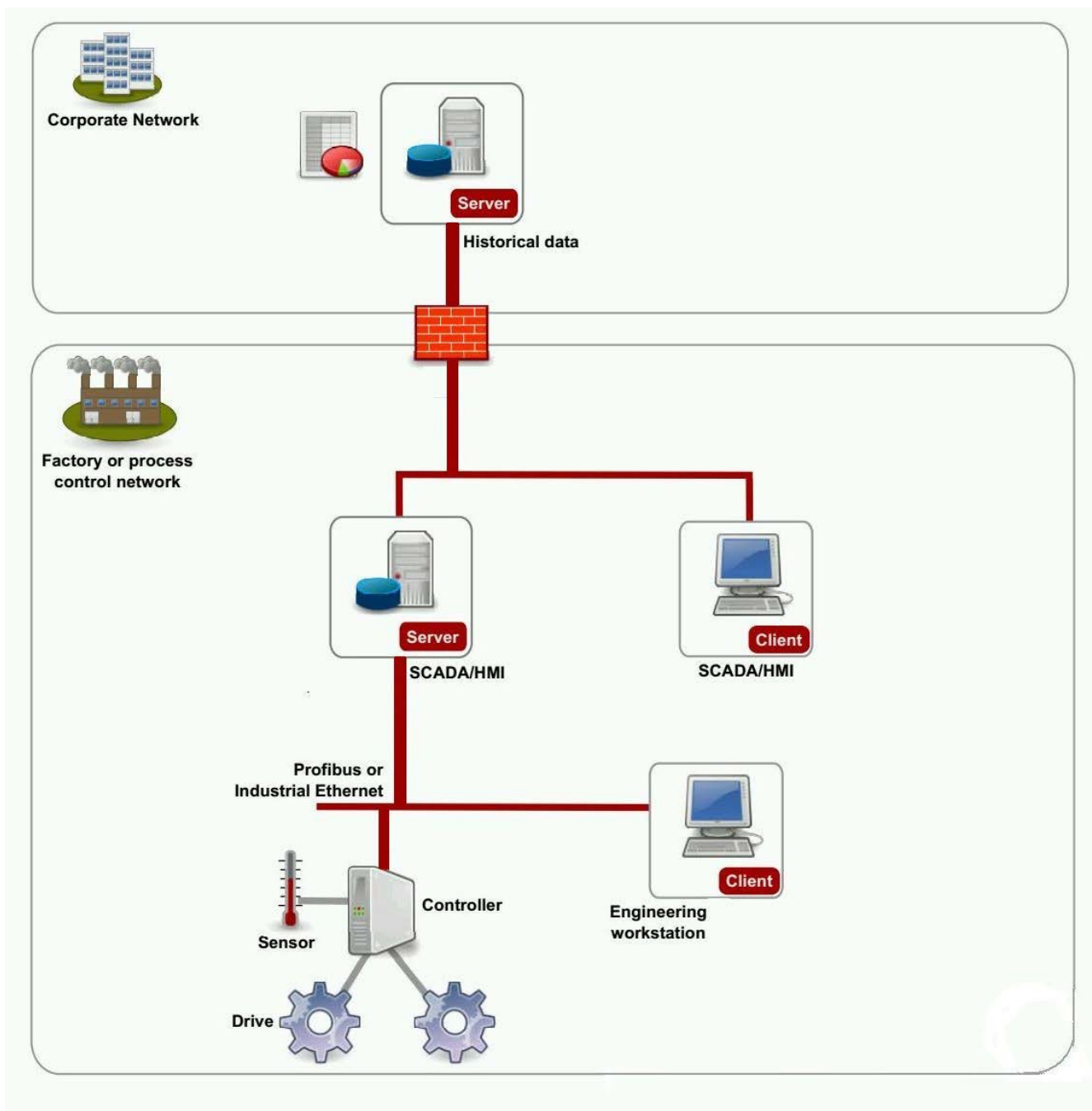
Such systems can range from a few modular panel-mounted controllers to large interconnected and interactive distributed control systems with many thousands of field connections. All systems receive data received from remote sensors measuring process variables, compare these with desired set points and derive command functions which are used to control a process through the final control elements, such as control valves.

There are several types of ICSs, the most common of which are **Supervisory Control and Data Acquisition (SCADA)** systems, and **Distributed Control Systems (DCS)**. In practice, large SCADA systems have grown to become very similar to distributed control systems in function, but using multiple means of interfacing with the plant.

As it is shown in Figure 1.2, ICS's are integrated in the industrial companies as the next diagram shows. The management staff use data from the manufacturing plant and take decisions based on them, resulting on plans that are transferred to the production level and must be carried out using resources controlled by the ICS.

Figure 1.2 - ICS integration in a company (source: Open Security Archive)

A specific case of ICS is the **safety instrumented system (SIS)** which consists of an engineered set of hardware and software controls that are especially used on **critical process systems** such as the ones used in **refineries, chemical and nuclear** facilities to provide protection such as open/close a critical valve in order to reduce dangerous gas overpressure or liquid high temperature.



Safety instrumented systems are composed of the same types of control elements (including sensors, logic solvers, actuators and other control equipment) as a Basic Process Control System (BPCS). However, all of the control elements in an SIS are dedicated solely to the proper functioning of the SIS. **Support** systems, such as power, instrument air, and communications, are generally required for SIS operation. The support systems should be designed to provide the required **integrity and reliability**.

ICS's are typically divided in **5 levels**, shown in Figure 1.3. Each level has its own functionality and must communicate with the other levels in order to carry out the planned actions.

Data acquisition begins at the level1 **RTU** or **PLC** and includes instrumentation readings and equipment status reports that are communicated to level 2 SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the **HMI** (Human Machine Interface) can make supervisory decisions to adjust or override normal RTU or PLC controls. Data may also be fed to a historian, often built on a commodity database management system, to allow trending and other analytical auditing.

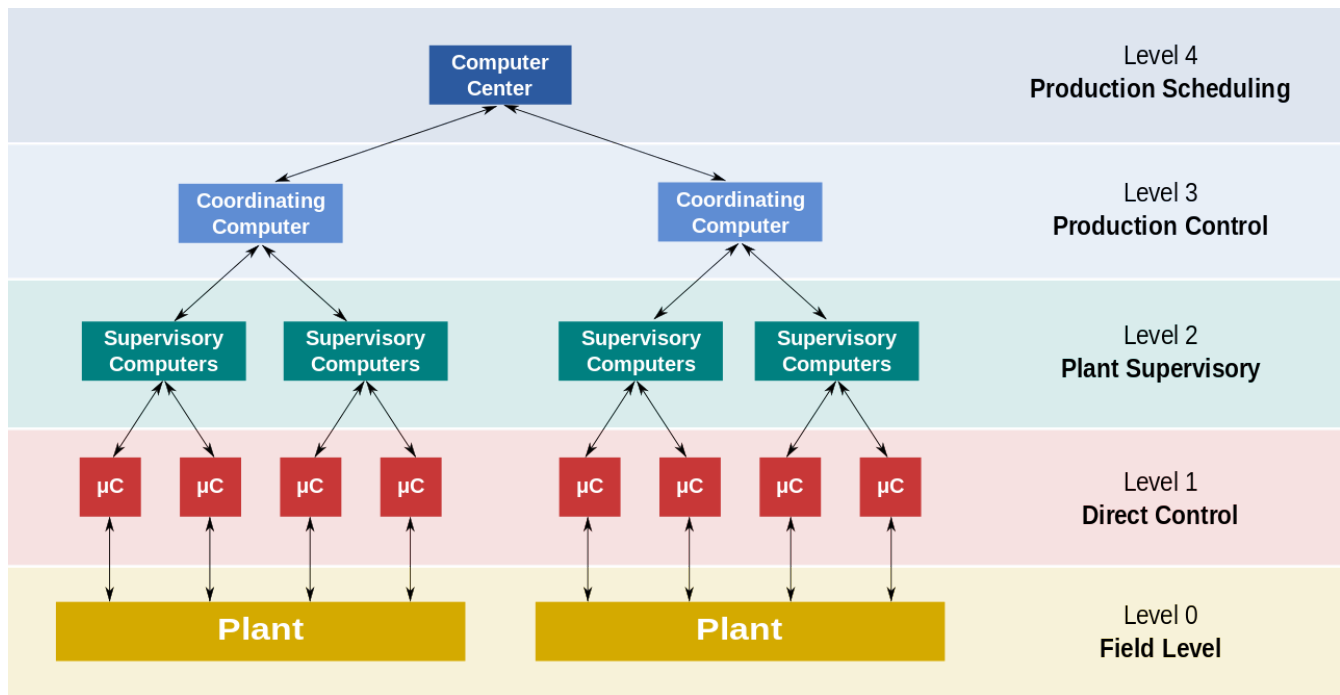


Figure 1.3 - ICS levels (source: Wikipedia)

This level contains the field devices such as **sensors** and final control elements or **actuators**.

In the broadest definition, a sensor is a device, module, or subsystem whose purpose is to detect events or changes in its environment and send the information to other electronics, frequently a computer processor. A sensor is always used with other electronics.

Sensors (Figure 1.4 shows an IR sensor) are used in everyday objects such as touch-sensitive buttons (tactile sensor) and in industrial processes to measure different magnitudes (pressure, position, temperature...).

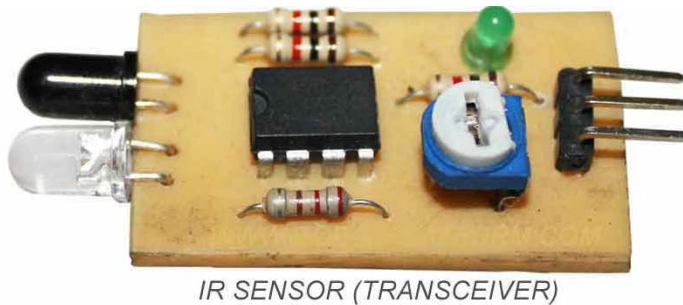


Figure 1.4- IR sensor (source: Wikipedia)

An actuator (Figure 1.5 shows an hydraulic valve) is a component of a machine that is responsible for moving and controlling a mechanism or system, for example by opening a valve. In simple terms, it is a "mover".

An actuator requires a control signal and a source of energy. The control signal is relatively low energy and may be electric voltage or current, pneumatic or hydraulic pressure, or even human power. When it receives a control signal, an actuator responds by converting the signal's energy into mechanical motion.



Figure 1.5- Hydraulic valve (source: Wikipedia)

This level contains the industrialised input/output (I/O) modules, and their associated distributed electronic processors. It contains the programmable logic controllers (PLCs) or remote terminal units (RTUs).

A **programmable logic controller (PLC)** is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis.

A PLC (Figure 1.6) is an example of a "hard" real-time system since output results must be produced in response to input conditions within a limited time, otherwise unintended operation will result.

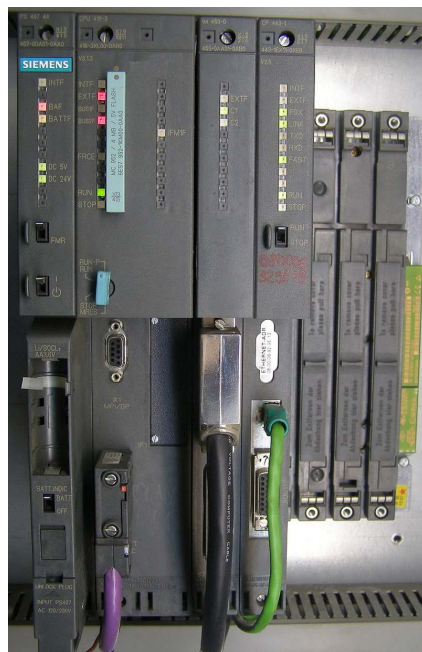


Figure 1.6- Programmable Logic Controller ([source: Wikipedia](#))

Figure 1.7 shows a **remote terminal unit (RTU)**, which is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects. Other terms that may be used for RTU are remote telemetry unit and remote telecontrol unit.



Figure 1.7- Remote Terminal Unit ([source: Wikipedia](#))

This level contains the **supervisory computers**, which collate information from processor nodes on the system, and provide the operator control screens.

Level 2 contains the **SCADA** software and computing platform. The SCADA software exists only at this supervisory level as control actions are performed automatically by Level 1 RTUs or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow.

The SCADA also enables **alarm** conditions, such as loss of flow or high temperature, to be displayed and recorded. A **feedback control loop** is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop.

The **human-machine interface (HMI)** (Figure 1.8 shows a typical HMI touch panel) is the operator window of the supervisory system. It presents plant information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the plant being controlled, and alarm and event logging pages. The HMI is linked to the SCADA supervisory computer to provide live data to drive the mimic diagrams, alarm displays and trending graphs. In many installations the HMI is the graphical user interface for the operator, collects all data from external devices, creates reports, performs alarming, sends notifications, etc.

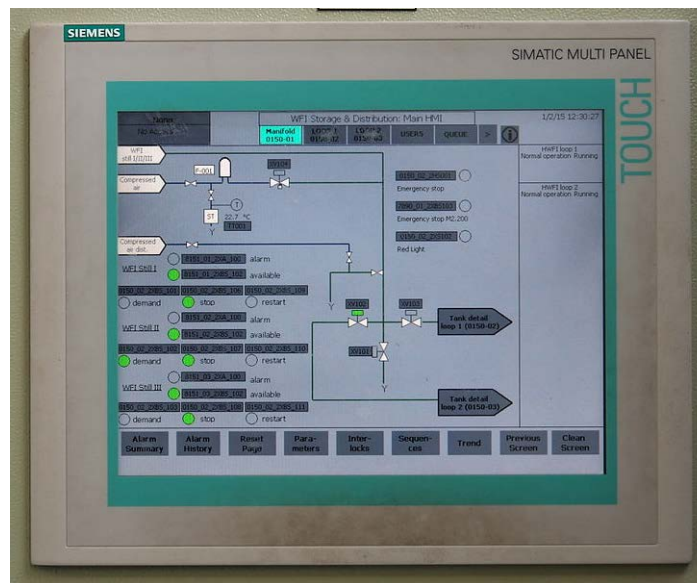


Figure 1.8- HMI Touch Panel (source: Wikimedia)

The core of the SCADA system is the **Supervisory Workstation**, gathering data on the process and sending control commands to the field connected devices. It refers to the computer and software responsible for communicating with the field connection controllers, which are RTUs and PLCs, and includes the HMI software running on operator workstations.

In smaller SCADA systems, the supervisory computer may be composed of a single PC, in which case the HMI is a part of this computer. In larger SCADA systems, the master station may include several HMIs hosted on client computers, multiple servers for data acquisition, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual-redundant or hot-standby formation providing continuous control and monitoring in the event of a server malfunction or breakdown.

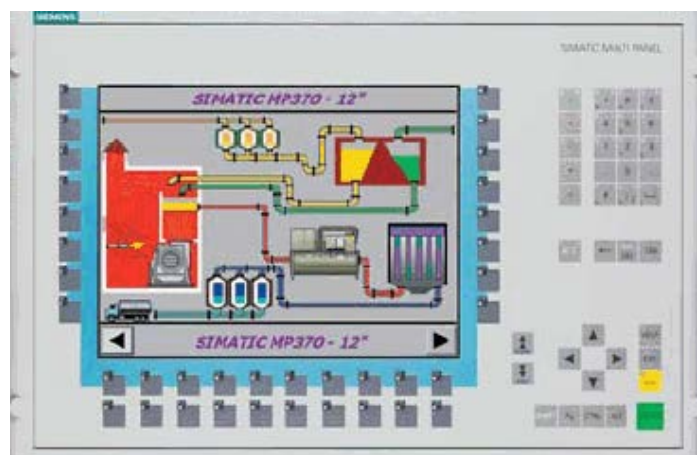


Figure 1.9- SCADA display ([source: Wikimedia](#))

Levels 3 and 4 are not strictly process control in the traditional sense, but are where production control and scheduling takes place.

This level does not directly control the process, but is concerned with **monitoring production and targets**. It contains MES, CMMS and WMS systems

Manufacturing execution systems (MES) are computerized systems used in manufacturing, to track and document the transformation of raw materials to finished goods. MES provides information that helps manufacturing decision makers understand how current conditions on the plant floor can be optimized to improve production output. MES works in real time to enable the control of multiple elements of the production process. The Figure 1.10 shows the different parts of a MES system.

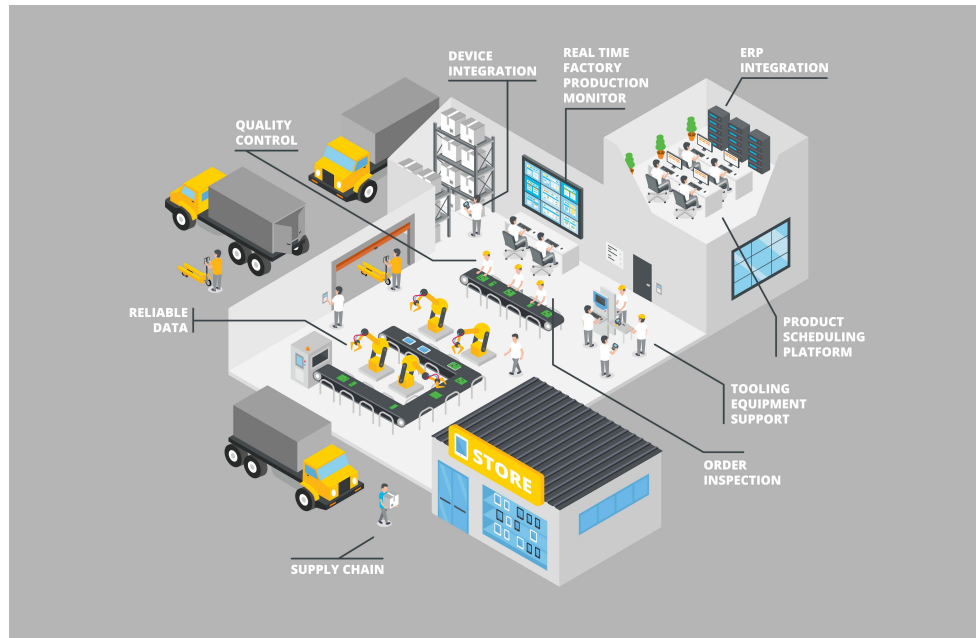


Figure 1.10- Company organization for MES management (source: Wikimedia)

Warehouse management system (WMS) is a software application, designed to support and optimize warehouse functionality and distribution center management. These systems facilitate management in their daily planning, organizing, staffing, directing, and controlling the utilization of available resources, to move and store materials into, within, and out of a warehouse, while supporting staff in the performance of material movement and storage in and around a warehouse.

Computerized maintenance management system (CMMS), is a software package that maintains a computer database of information about an organization's maintenance operations. This information is intended to help maintenance workers do their jobs more effectively (for example, determining which machines require maintenance and which storerooms contain the spare parts they need) and to help management make informed decisions (for example, calculating the cost of machine breakdown repair versus preventive maintenance for each machine, possibly leading to better allocation of resources).

This level contains ERP systems and its main function is to provide information and decision support to management staff.

Enterprise resource planning (ERP) is usually referred to as a category of business management software -- typically a suite of integrated applications--that an organization can use to collect, store, manage, and interpret data in real-time from these many business activities. It provides an integrated and continuously updated view of core business processes using common databases maintained by a database management system.

ERP systems track business resources--cash, raw materials, production capacity--and the status of business commitments: orders, purchase orders, and payroll. The applications that make up the system share data across various departments (manufacturing, purchasing, sales, accounting, etc.) that provide the data.

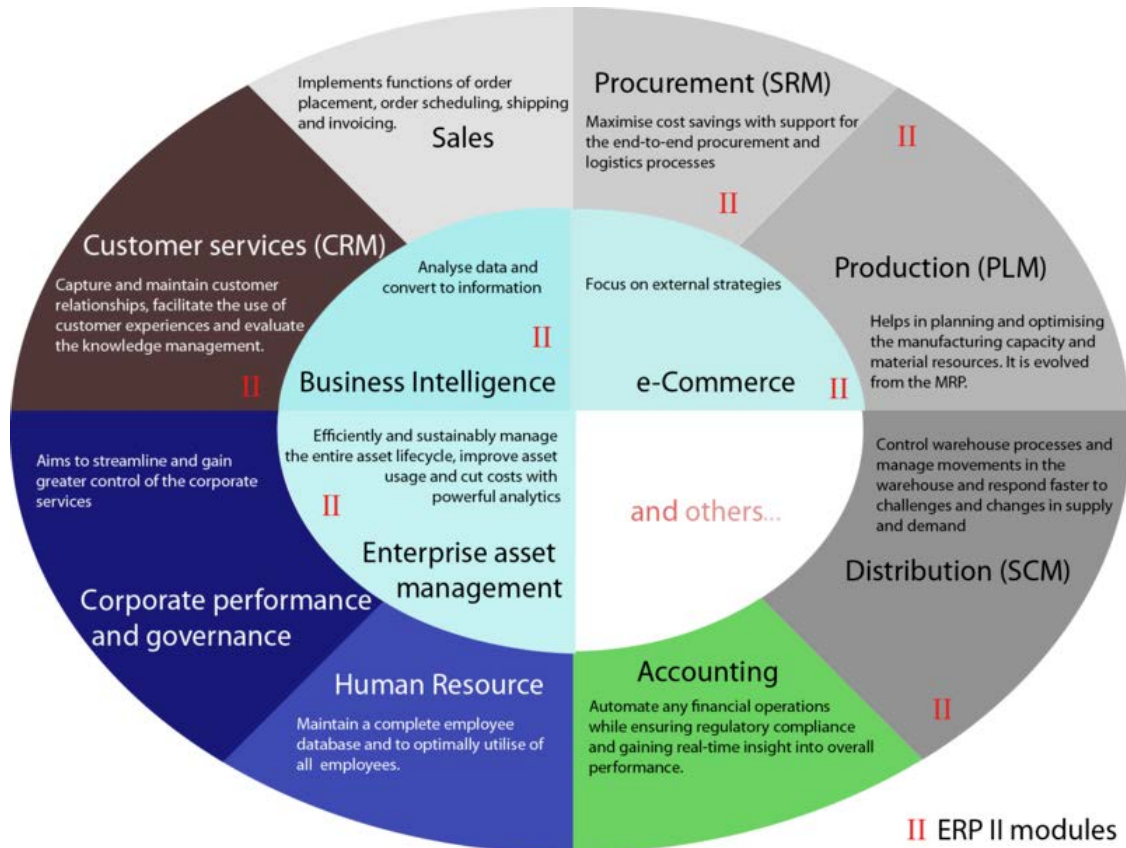


Figure 1.11- ERP modules according to company structure ([source: Wikipedia](https://en.wikipedia.org/wiki/Enterprise_resource_planning))

1.2 Network design and architecture

Description

Design and architecture of networks

Table of contents

1. OSI Levels

2. Data encapsulation

3. Physical topologies

3.1. Bus topology

3.2. Star topology

3.3. Ring topology

3.4. Cellular topology

4. Network performance

5. Computer networks

6. Network protocols

6.1. Serial standards: RS232, RS485

6.2. Ethernet

6.3. TCP/IP

7. Network segmentation

7.1. Switches and VLAN's

7.2. Routers and IP subnetting

7.3. Firewalls

8. Remote access

8.1. Telnet and SSH

8.2. Remote desktop

8.3. VPN

1. OSI Levels

On the previous chapter it has been stated that Industrial Control Systems (Figure 1.12) are composed of interconnected devices that share and transfer information between them. In this chapter we are going to study what are the most common network structures and which are their characteristics.

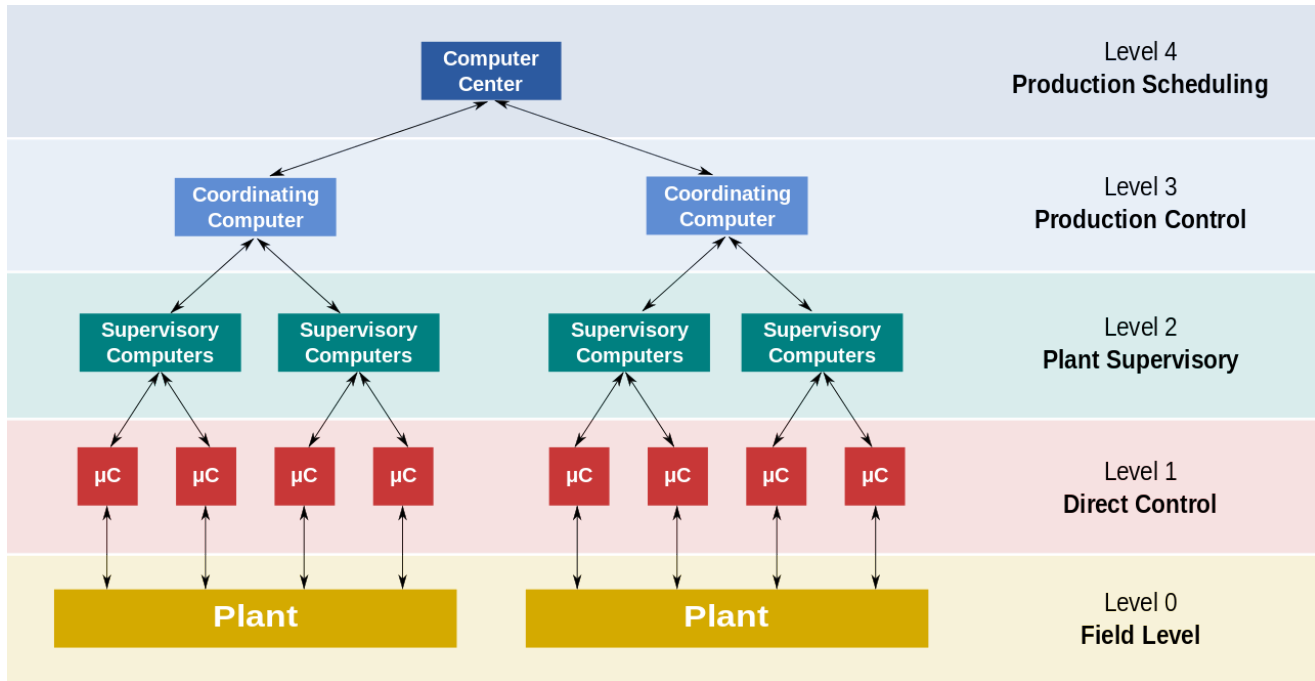


Figure 1.12- ICS levels (source: Wikipedia)

In that purpose, we will begin studying the **Open Systems Interconnection model (OSI model)**, which is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.

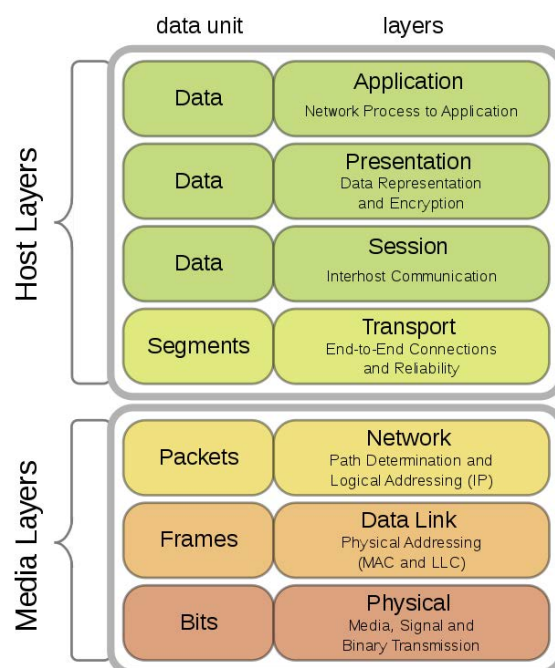


Figure 1.13- OSI levels (source: Wikipedia)

The **physical layer** is responsible for the transmission and reception of unstructured raw data between a device and a physical transmission medium.

It converts the digital bits into electrical, radio, or optical signals. Layer specifications define characteristics such as voltage levels, the timing of voltage changes, physical data rates, maximum transmission distances, modulation scheme, channel access method and physical connectors.

The **data link layer** provides node-to-node data transfer. It is divided in two sublayers:

- Medium access control (**MAC**) layer - responsible for controlling how devices in a network gain access to a medium and permission to transmit data.
- Logical link control (**LLC**) layer - responsible for identifying and encapsulating network layer protocols, and controls error checking and frame synchronization.

The protocols **802.3 Ethernet** and **802.11 Wi-Fi**, operate at the data link layer.

The **network layer** is responsible of **transferring** data sequences (called **packets**) from one node to another connected in "**different networks**".

This nodes are identified by a layer 3 address, which typically are **IP address**.

Routers are responsible to transfer the packets to their destination nodes by finding their way through the different networks.

The **transport layer** is responsible of **transferring** data sequences (called **segments**) from a source to a destination host, while maintaining the **quality of service**.

Protocols such as **TCP** and **UDP** work in this level. **Ports** defined in this level are the entry points to server's public services.

The **session layer** controls the **dialogues** (also known as connections or sessions) between computers (between local and remote applications).

The **presentation layer** enables communication between systems with different **syntax** and semantics (for example **ASCII** and EBCDIC codes, **MPEG** video compression or XML data structure).

The **application layer** interacts with **software applications** that implement a communicating component. Such application programs (for example **FTP** server/clients, internet browsers...) fall outside the scope of the OSI model.

Well known Layer 7 protocols are **HTTP**, **Modbus**.

2. Data encapsulation

In computer networking, **encapsulation** is a method of designing modular communication protocols in which each layer builds a protocol data unit (PDU) by adding a header (and sometimes trailer) containing control information to the PDU from the layer above.

The physical layer is responsible for physical transmission of the data, link encapsulation allows local area networking, Internet Protocol (IP) provides global addressing of individual computers, and Transmission Control Protocol (TCP) selects the process or application, i.e. the port which specifies the service such as a Web or TFTP server.

For example, in the Internet protocol suite, the contents of a web page are encapsulated with an HTTP header, then by a TCP header, an IP header, and, finally, by a frame header and trailer. The frame is forwarded to the destination node as a stream of bits, where it is decapsulated (or de-encapsulated) into the respective PDUs and interpreted at each layer by the receiving node.

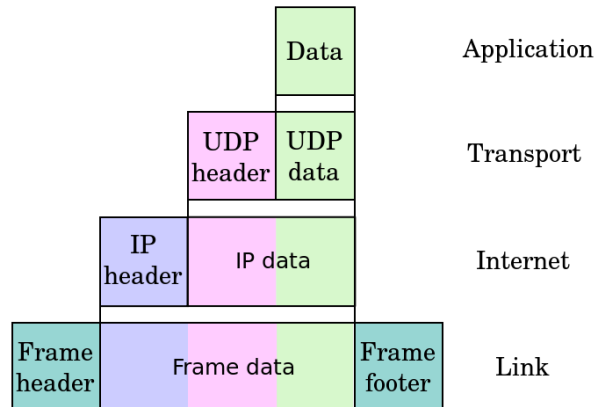


Figure 1.14- Data encapsulation ([source: Wikipedia](https://en.wikipedia.org/wiki/Data_encapsulation))

3. Physical topologies

Network topology is the arrangement of the elements (links, nodes, etc.) of a communication network.

Physical topology is the placement of the various components of a network (e.g., device location and cable installation), while logical topology illustrates how data flows within a network. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two different networks, yet their topologies may be identical.

A network's physical topology is a particular concern of the physical layer of the OSI model.

3.1. Bus topology

In the bus topology workstations are directly connected to a common linear half-duplex link with some medium such as twisted pair or coaxial cable, and they receive all traffic generated by each station. They need a terminating resistor at the end of the line, which eliminate signal bounces.

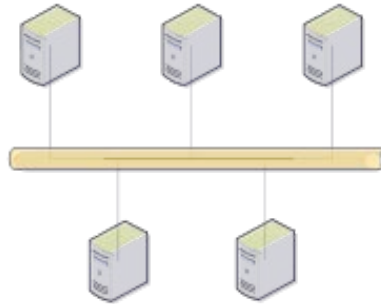


Figure 1.15- Bustopology (source: [Wikipedia](#))

3.2. Star topology

In a star network, every host is connected to a central hub (usually a switch), which retransmits messages from sending stations to receiving ones. This is one of the most common computer network topologies.

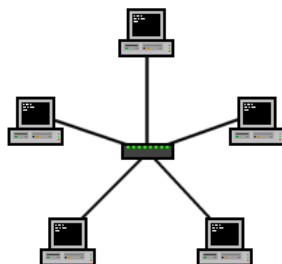


Figure 1.16- Star topology ([source: Wikipedia](#))

3.3. Ring topology

A ring network is a network topology in which each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node. Data travels from node to node, with each node along the way handling every packet.

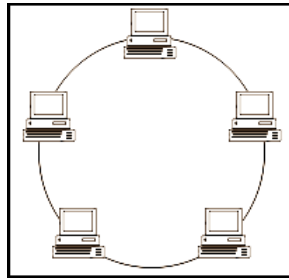


Figure 1.17- Ring topology (source: [Wikimedia](#))

3.4. Cellular topology

A cellular network is a communication network where the last link is wireless. The network is distributed over areas called cells, each served by at least one access-point. These nodes provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content.

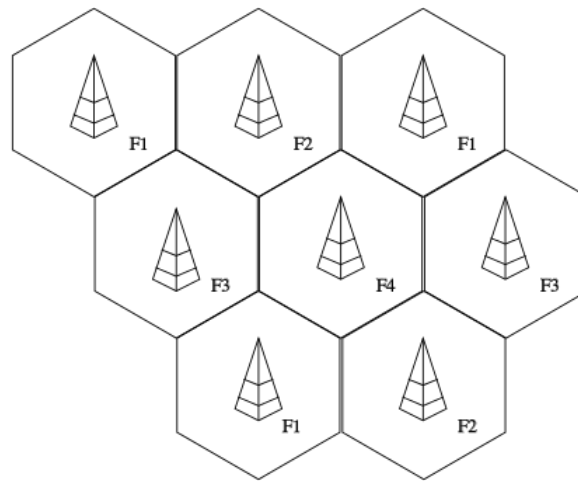


Figure 1.18- Cellular topology (source: [Wikipedia](#))

4. Network performance

Bandwidth and latency (Figure 1.19) are two of the most relevant characteristics in a digital network.

Latency is expressed in a time unit, usually milliseconds (ms). Latency is the amount of time it takes for data to travel from one point to another. It is dependent on the physical distance that data must travel through cords, networks and the like to reach its destination

Bandwidth is expressed in bits per second (bps). It refers to the amount of data that can be transferred during one second. Obviously, the wider the pipe, the more bits can be transferred per second. And if your bandwidth is congested, your latency (delay) is increased.

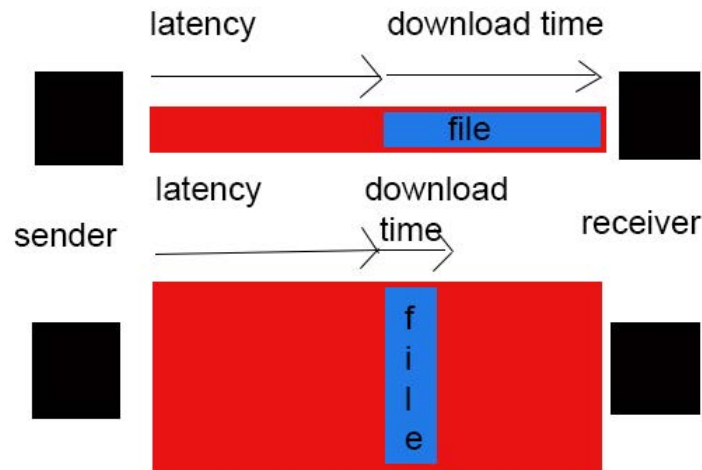


Figure 1.19- Transmission latency and bandwidth (source: [Wikipedia](#))

In digital transmission, the **bit error rate (BER)** is the number of bit errors per unit time. The **bit error ratio** (also **BER**) is the number of bit errors divided by the total number of transferred bits during a studied time interval. Bit error ratio is a unitless performance measure, often expressed as a percentage.

Received bits of a data stream over a communication channel could be altered due to noise, interference, distortion or bit synchronization error. Signal To Noise Ratio (SNR) parameter indicates the proportion of the non desired signal related to the information transmitting signal. As Figure 1.20 shows, the higher SNR (better signal) the lower BER (less errors during transmission).

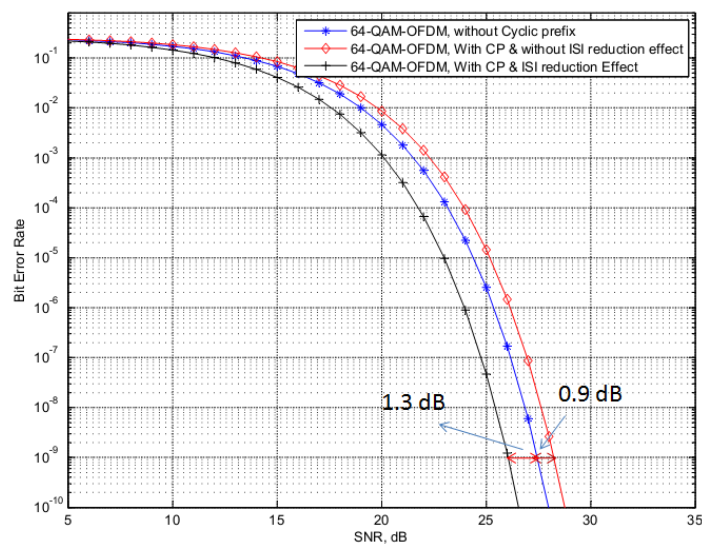


Figure 1.20- SNR vs BER (source: [Wikipedia](#))

5. Computer networks

A **local area network (LAN)** is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

Ethernet and Wi-Fi are the two most common technologies in use for local area networks.

100BASE-T and **structured cabling** are the basis of most commercial LANs today. While optical fiber cable is common for links between network switches, use of fiber to the desktop is rare.

In a **wireless LAN**, users have unrestricted movement within the coverage area. Wireless networks have become popular in residences and small businesses, because of their ease of installation. Most wireless LANs use Wi-Fi as it is built into smartphones, tablet computers and laptops. Guests are often offered Internet access via a hotspot service.

Simple LANs generally consist of cabling and one or more switches. A switch can be connected to a router, cable modem, or ADSL modem for Internet access.

A LAN can include a wide variety of other network devices such as **firewalls**, load balancers, and network intrusion detection. Advanced LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and their ability to segregate traffic with **VLANs**.

At the higher network layers, protocols such as NetBEUI, IPX/SPX, AppleTalk and others were once common, but the Internet Protocol Suite (**TCP/IP**) has prevailed as a standard of choice.

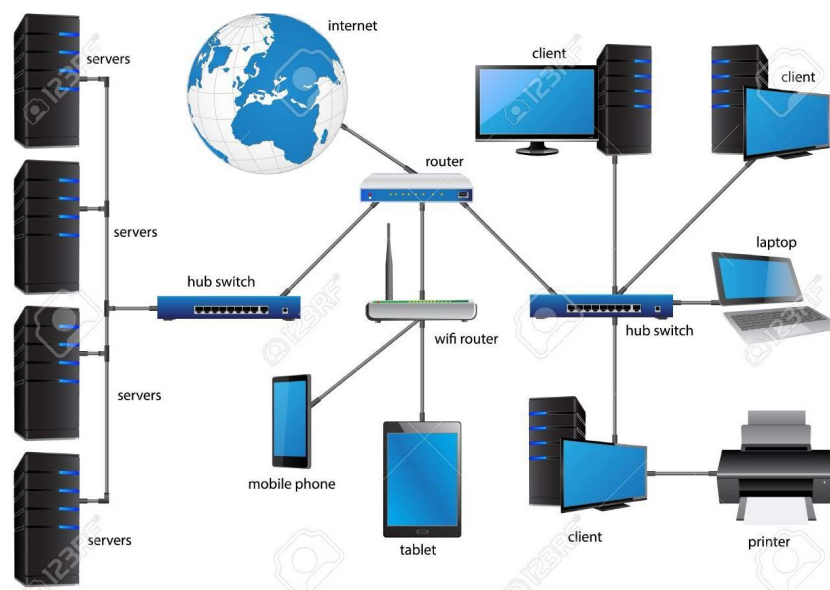


Figure 1.21- LAN network structure (source: [Wikimedia](#))

LAN networks can maintain connections with other LAN networks via leased lines, leased services, or across the Internet using **virtual private network (VPN)** technologies. Depending on how the connections are established and secured, and the distance involved, such linked LAN networks may also be classified as a metropolitan area network (MAN) or a wide area network (WAN).

A **wide area network (WAN)** is a telecommunications network that extends over a large geographical distance for the primary purpose of computer networking. Wide area networks are often established with leased telecommunication circuits.

Business, education and government entities use wide area networks to relay data to staff, students, clients, buyers, and suppliers from various locations across the world. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet may be considered a WAN.

Many WANs are built for one particular organization and are private, for example connecting the different offices of a company to its headquarters. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet.

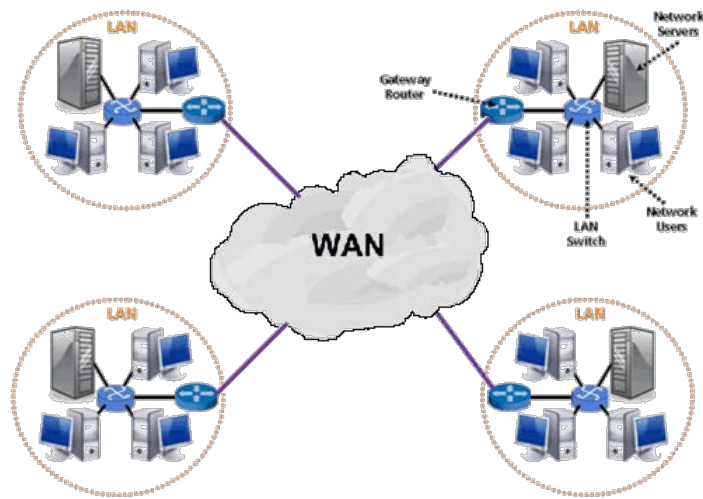


Figure 1.22- WAN network (source: [Wikimedia](#))

Many technologies are available for wide area network links, such as circuit-switched telephone lines, radio wave transmission, and optical fiber.

6. Network protocols

The standardized method by which nodes are allowed to transmit information to the bus or network wiring is called a **protocol**. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.

Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together are known as a protocol suite.

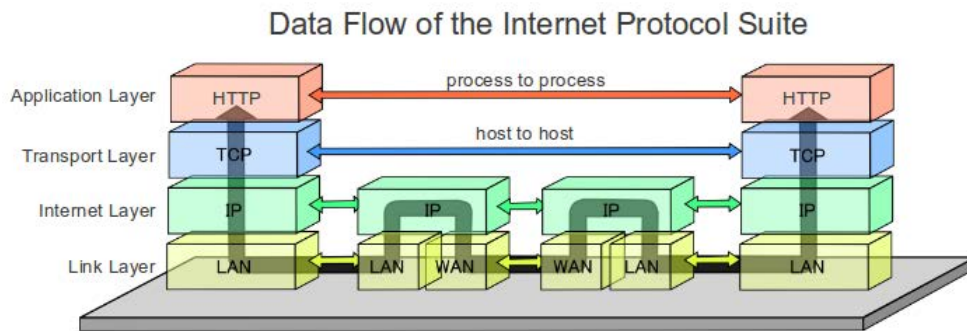


Figure 1.23- TCP/IP protocol suite (source: [Wikimedia](#))

6.1. Serial standards: RS232, RS485

In data transmission, **serial communication** is the process of sending data one bit at a time, sequentially, over a communication channel or computer bus. They are very common in the industrial networks due to their simplicity, and RS-232 and RS-485 are some of most spread serial communication protocols. These protocols correspond to physical layer of the OSI model.

RS-232 refers to a standard for serial communication transmission of data. It formally defines signals connecting between a **DTE** (data terminal equipment) such as a computer terminal, and a **DCE** (data circuit-terminating equipment or data communication equipment), such as a modem. Thus, it can not be considered a networking protocol but a point-to-point communication protocol.

The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pinout of connectors. The RS-232 standard had been commonly used in computer **serial ports**.

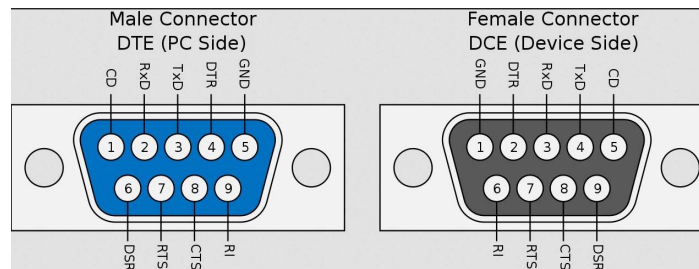


Figure 1.24- RS-232 connection pin layout (source: [Wikimedia](#))

RS-232, when compared to later interfaces such as RS-485 and Ethernet, has lower features. In modern personal computers, USB has displaced RS-232 from most of its peripheral interface roles. But thanks to their simplicity, RS-232 interfaces are still used--particularly in industrial machines where a short-range, point-to-point, low-speed wired data connection is fully adequate.

RS-485 is a standard defining the electrical characteristics of drivers and receivers for use in serial communications systems.

Digital communications networks implementing the standard can be used effectively over long distances and in electrically noisy environments.

Multiple receivers may be connected to such a network in a linear, multidrop bus. These characteristics make RS-485 useful in industrial control systems and similar applications.

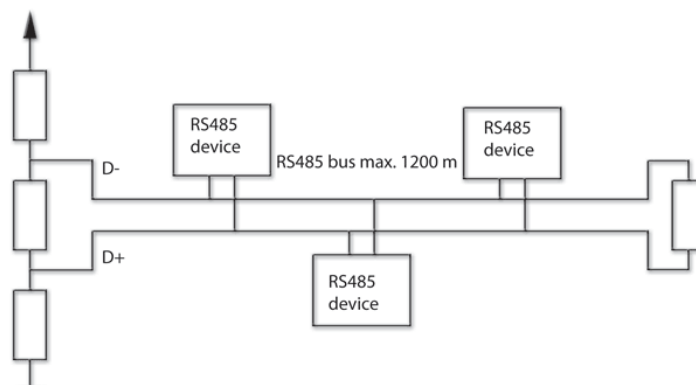


Figure 1.25- RS-485 network structure (source: [Wikimedia](#))

Personal computers may need network converters (usually RS232 to RS485 or USB to RS485) to connect to a RS485 network.

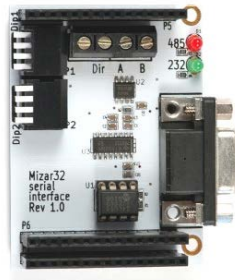


Figure 1.26- RS-485/RS-232 converter (source: [Wikimedia](#))

6.2. Ethernet

Ethernet is a family of computer networking technologies commonly used in local area networks (LAN). The newer Ethernet variants use twisted pair (**UTP cables and RJ45 connectors**) and fiber optic or twisted pair cable links in conjunction with **switches**. The Ethernet standards comprise several wiring and signaling variants of the OSI **physical layer** in use with Ethernet.



Figure 1.28- Ethernet cable (UTP+RJ45) (source: [Wikimedia](#))

The most common physical topology for Ethernet networks is **star** topology based on switches.

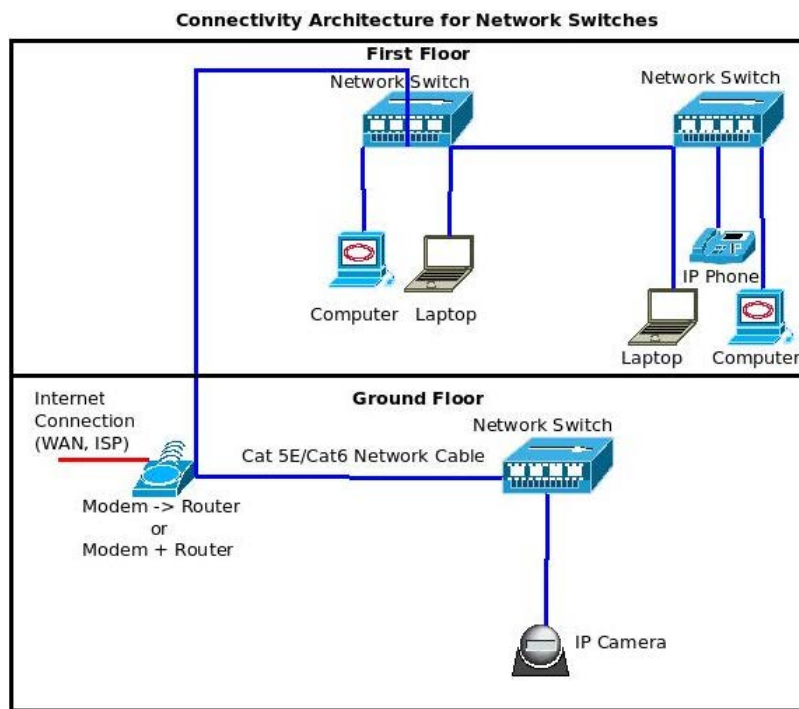


Figure 1.29- Ethernet network star topology (source: [Wikipedia](#))

ICS's in industry are often based on the Ethernet protocol, which facilitates sharing information between OT devices and IT workstations. Industrial switches are used to connect OT equipment such as PLC's, HMI and monitors (Figure 1.30)

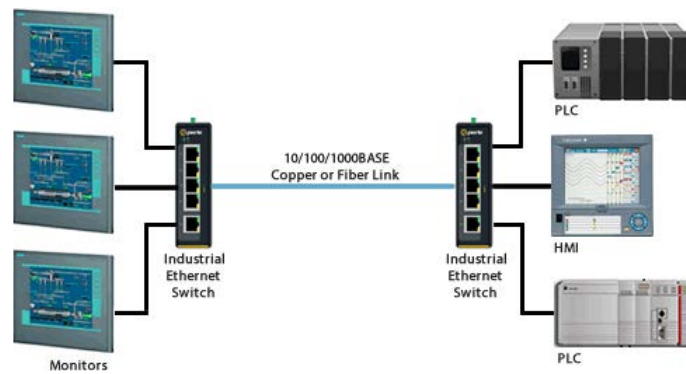
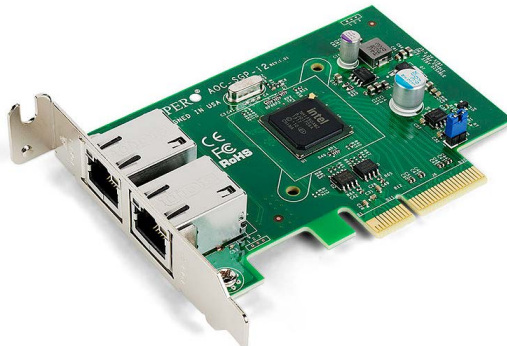
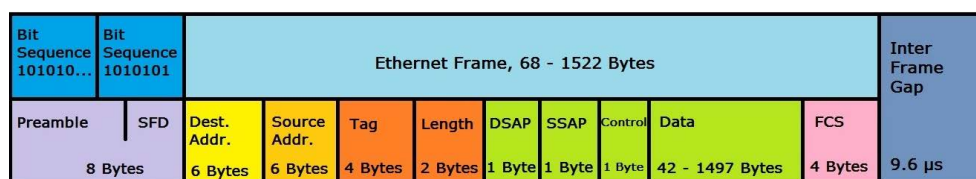


Figure 1.30- Industrial Ethernet network structure

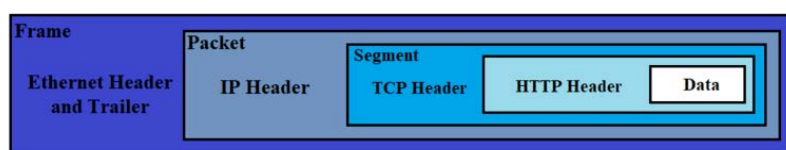
Each of the nodes (computers, PLC's...) connected to an Ethernet network need a special card (**Network Interface Controller, NIC**) which provides the physical interface and the logical procedure (**CSMA/CD**) needed to access and exchange information through that network.

Figure 1.31- Ethernet NIC (source: [Wikipedia](#))

Systems communicating over Ethernet divide a stream of data into shorter pieces called **frames**. Each frame contains source and destination addresses (48 bit **MAC address**), and error-checking data so that damaged frames can be detected and discarded. As per the OSI model, Ethernet provides services included in the **data link layer**

Figure 1.31- Ethernet frame (source: [Wikipedia](#))

The Internet Protocol (IP) is commonly carried over Ethernet and so it is considered one of the key technologies that make up the Internet.

Figure 1.32- IP packet encapsulated in Ethernet frame (source: [Wikimedia](#))

6.3. TCP/IP

The **Internet protocol suite** is the conceptual model and set of communications protocols used in the Internet and similar computer networks. It is commonly known as **TCP/IP** because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet protocol (IP). Figure 1.33 compares the OSI model with the TCP/IP implementation, in which application layer protocols (FTP...) use the transport services provided by the TCP/IP protocols.

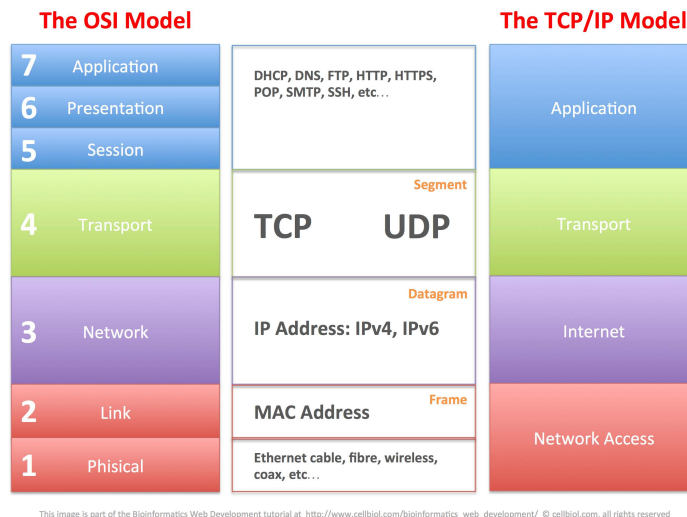


Figure 1.33- Communication protocol stack (source: blog.pythian.com)

TCP/IP provides **end-to-end** data communication specifying how data should be packetized, addressed, transmitted, routed, and received. This functionality is organized into **four abstraction layers**. From lowest to highest, the layers are the **link layer** (based usually on Ethernet), containing communication methods for data that remains within a single network segment (link); the **internet layer** (based on IP protocol), providing internetworking between independent networks; the **transport layer** (based on TCP protocol), handling host-to-host communication; and the **application layer** (protocols such as HTTP and FTP are defined in this layer), providing process-to-process data exchange for applications.

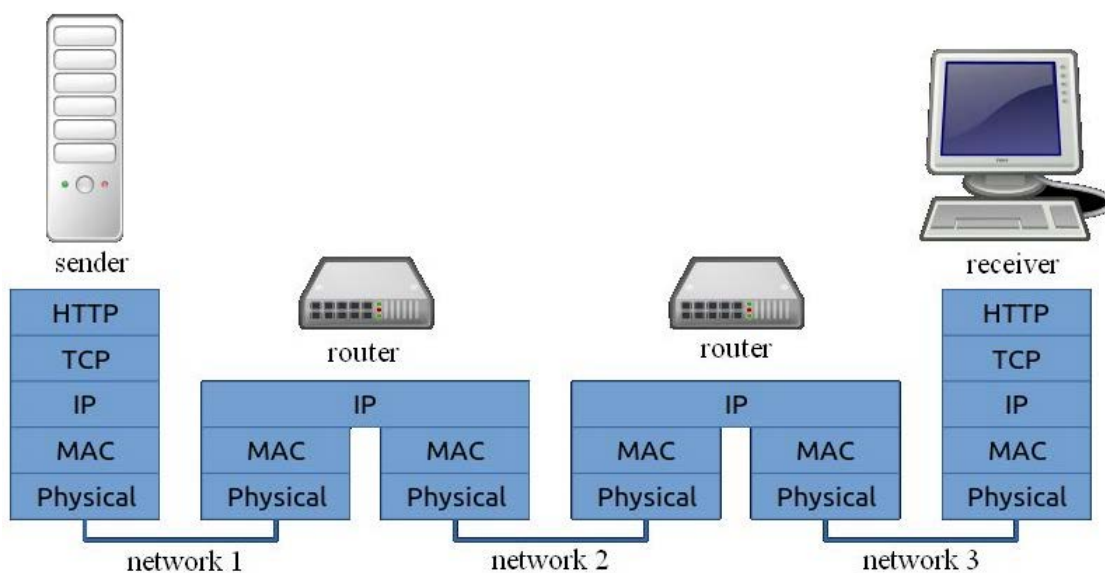


Figure 1.34- TCP/IP connection structure (source: [Wikimedia](https://commons.wikimedia.org/wiki/File:TCP_IP_Connection_Structure.png))

A **router** is a networking device that forwards data packets between computer networks. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node.



Figure 1.35- IP packet routing (source: <http://routinglab.blogspot.com>)

Routing is based on **IP addresses assigned to nodes**. IP (v4) addresses may be represented in any notation expressing a 32-bit integer value. They are most often written in the dot-decimal notation, which consists of four octets of the address expressed individually in decimal numbers and separated by periods.

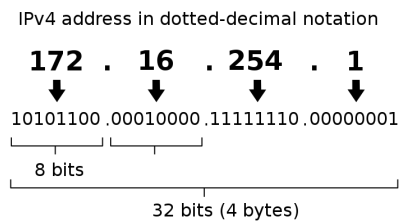


Figure 1.36- IP address structure (source: [Wikimedia](https://www.wikimedia.org/))

Information is sent from a transmitting node to a receiving one in form of IP packets, which include the source and destination IP addresses.

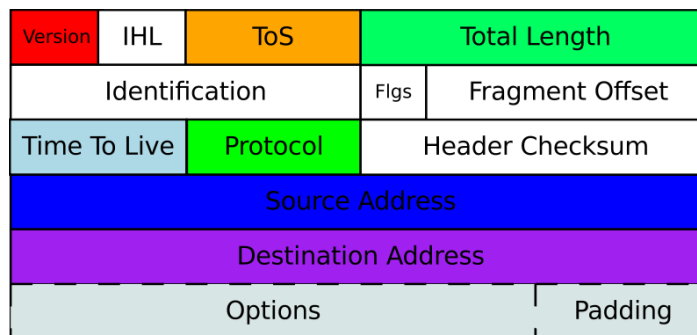


Figure 1.37- IP packet structure (source: [Wikimedia](https://www.wikimedia.org/))

7. Network segmentation

Network segmentation in computer networking is the act or practice of splitting a computer network into subnetworks as it is shown in Figure 1.38, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.

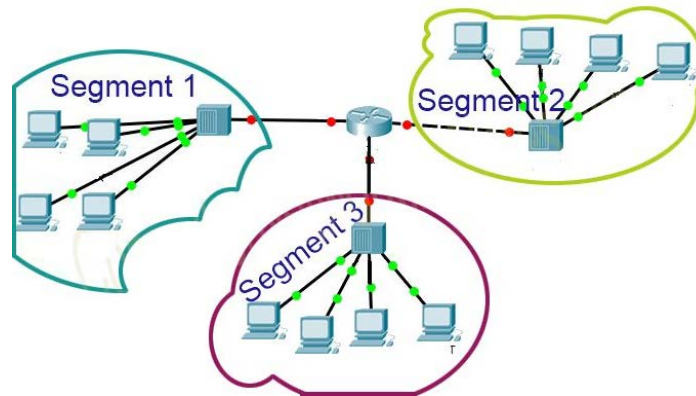


Figure 1.38- Network segmentation

Improved performance is achieved, because on a segmented network there are fewer hosts per subnetwork, thus minimizing local traffic and reducing congestion.

Improved security is achieved due to the following reasons:

- Broadcasts will be contained to local network. Internal network structure will not be visible from outside.
- There is a reduced attack surface available. Common attack vectors can be partially alleviated by proper network segmentation as they only work on the local network.
- By creating network segments containing only the resources specific to the consumers that you authorise access to, you are creating an environment of least privilege.

Visitor access control is achieved implementing VLANs to segregate the network

7.1. Switches and VLAN's

A **virtual LAN (VLAN)** is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

To subdivide a network into VLANs network equipment (usually switches) must be configured by software assigning a group of ports to each VLAN.

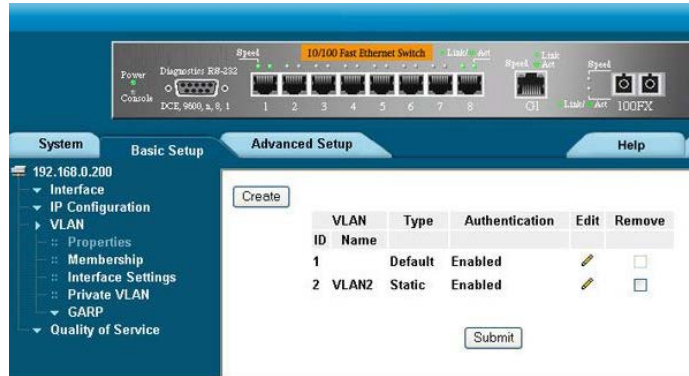


Figure 1.39- VLAN configuration screen

Once ports are assigned to each VLAN, data can't be exchanged between nodes (computers, PLC...) connected to different VLAN ports.

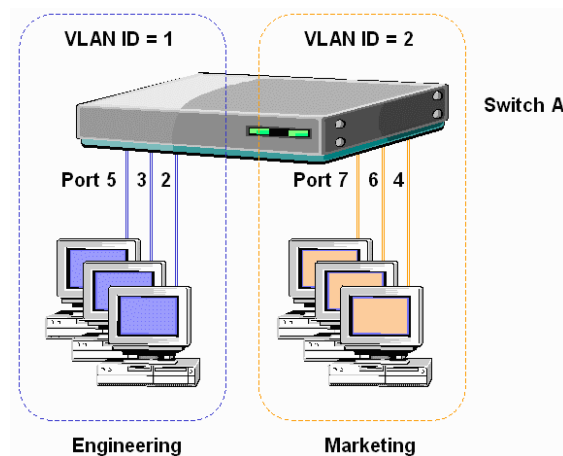


Figure 1.40- VLAN segmentation in a switch (source: <http://photos1.blogger.com/blogger/6124/4181/320/vlan-fig1.png>)

VLANs work by applying **tags** (this method is developed under the 802.1Q standard) to layer-2 frames, creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks.

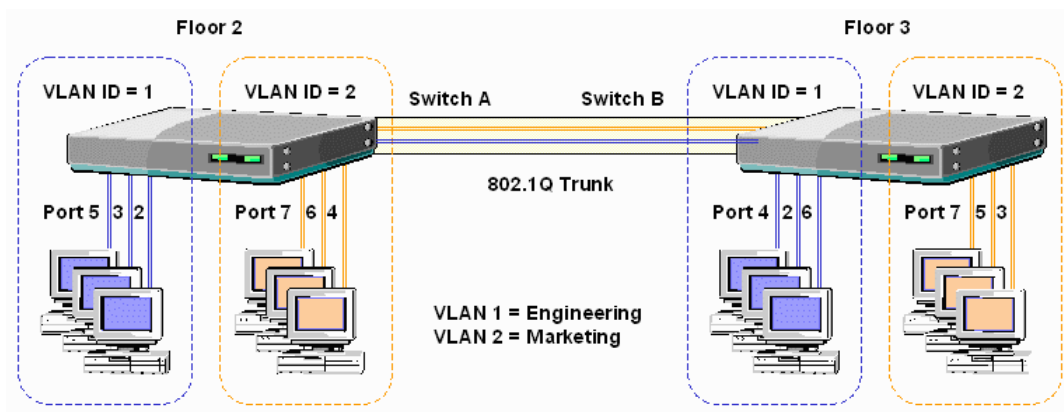


Figure 1.41- VLAN tagging (source: [Wikimedia](#))

VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch.

7.2. Routers and IP subnetting

In technical terms, a **router** is a Layer 3 network gateway device, meaning that it contacts two or more networks and that the router operates at the network layer of the OSI model. Figure 1.42 shows how three routers interconnect different LAN networks (they are identified by 150.10.0.0, 160.10.0.0 and 170.10.0.0 network addresses).

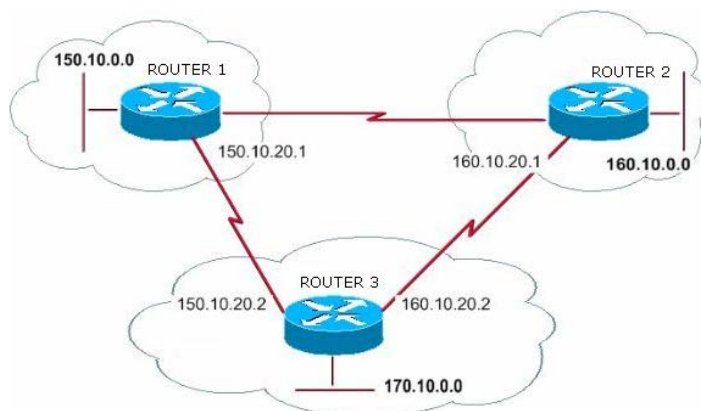


Figure 1.42- Router interconnecting different LAN networks.

To route the information from a source to a destination node it requires an addressing system, which usually is the one based on the IPv4 addresses.

An IP address is divided into two fields, the **network identifier** (used by routers to find the destination network on the internet) and the **host identifier** (an identifier for a specific host) (Figure 1.43).

The number of bits dedicated to each field is defined by the **mask** applied to an IP address, using logical "1" bits for the network part of the address and "0" for the host part. The number of bits allocated to the network part is used for the identification of the IP address of the corresponding network (e.g. in host address 192.168.1.110/**24** the first 24 bits are allocated for network addressing, so 192.168.1.0/**24** is the IP address of the network the host belongs).

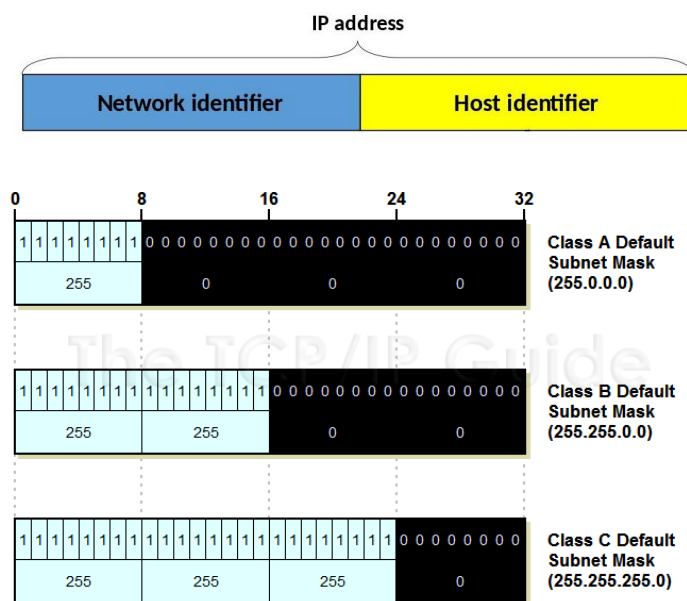


Figure 1.43- IP address class vs IP mask

A **subnetwork** or **subnet** is a logical subdivision (Figure 1.44) of an IP network. The practice of dividing a network into two or more

networks is called **subnetting**.

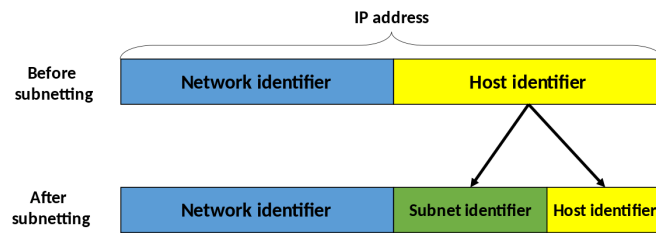


Figure 1.44- IP subnet identifier (source: [Wikipedia](#))

Some bits from the host identifier field are allocated (modifying the IP network mask to add more "1" bits allocated for the subnet field) to create a **subnet identifier**. Computers that belong to the same subnet are addressed with an identical subnet identifier in their IP addresses.

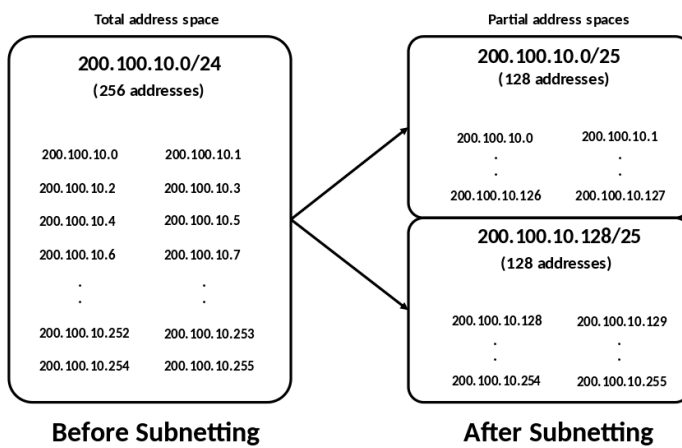


Figure 1.45- IP subnetting segmentation (source: [Wikimedia](#))

Computers located in different IP subnets need a router to communicate between them, so subnetting is a valid method to segmentate a network into isolated parts.

7.3. Firewalls

A **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

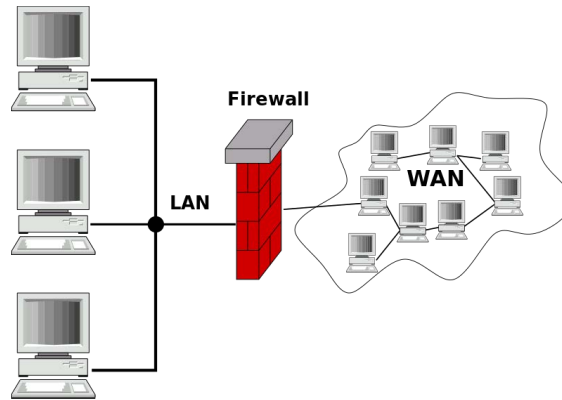


Figure 1.46- Firewall based protection (source: [Wikipedia](#))

Firewall filters packets transferred between computers. When a packet does not match **filtering rules**, the firewall rejects the packet, else it is allowed to pass. Packets may be filtered by source and destination network addresses, protocol, source and destination port numbers.

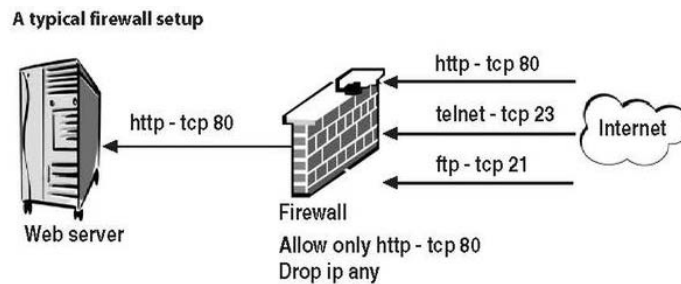


Figure 1.47- Firewall filtering rules (source: [Wikimedia](#))

DMZ or **demilitarized zone** is a subnetwork that contains an organization's external-facing services to a larger network such as the Internet. The purpose of a DMZ is to add a layer of security to an organization's LAN: an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.

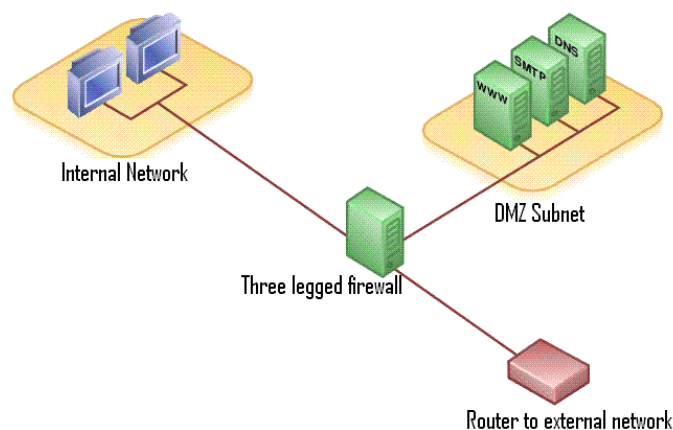


Figure 1.48- Firewall based DMZ (source: [Wikimedia](#))

8. Remote access

A **remote access services (RAS)** is any combination of hardware and software which allows a connection between a client to a host computer, known as a remote access server.

Many manufacturers help desks use this service for **technical troubleshooting of their customers' problems**. Various professional first-party, third-party, open source, and freeware **remote desktop** applications are available.

8.1. Telnet and SSH

Telnet and SSH (Secure Shell) are two network protocols used to connect to **remote servers** in order to facilitate some sort of communications. They enable network administrators to remotely access and manage a device working with a **terminal** emulator.

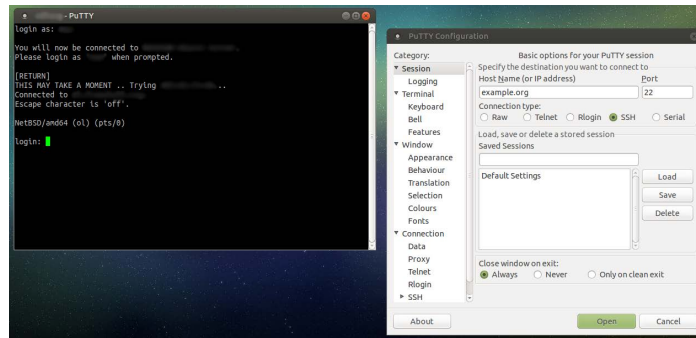


Figure 1.50- Putty based remote terminal

The main difference between Telnet and SSH is that SSH provides security mechanisms (encrypts exchanged data using public key **cryptography**) that protect the users establishing a secure connection between two remote hosts over the Internet, while Telnet has not security measures as user/password data are unencrypted.

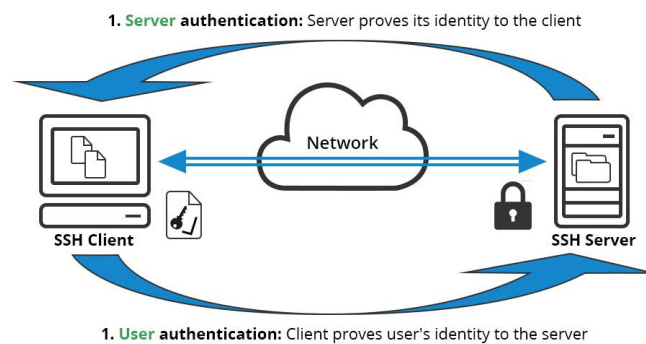


Figure 1.51- SSH based encrypted connection

8.2. Remote desktop

Remote desktop refers to a software that allows a personal computer's desktop environment to be run remotely on one system while being displayed on a separate client device. Taking over a desktop remotely is a form of remote administration.



Figure 1.52- Remote desktop control (source: <http://www.itarian.com>)

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software (built in many operative systems) for this purpose, while the other computer must run RDP server (built only in Windows OS) software.

Microsoft currently refers to their official RDP client software as Remote Desktop Connection, formerly "Terminal Services Client".

Unupdated RDP is nowadays one of the main entry points for **ransomware**. It is very important to keep Windows updated in order to avoid this type of attacks. There are a few options to secure it. [Follow the link for further information](#)

Virtual Network Computing (VNC) is an open-source graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits over a network the keyboard and mouse events from one computer to another, relaying the graphical-screen updates back in the other direction.

Multiple clients may connect to a VNC server at the same time. Popular uses for this technology include remote technical support and accessing files on one's work computer from one's home computer, or vice versa.

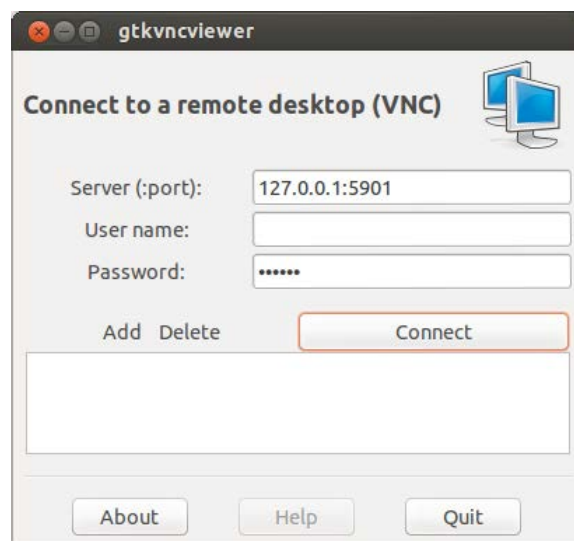


Figure 1.53- Remote desktop connection login (source: [flickr VNC](#))

TeamViewer is proprietary software for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers. Once installed in a computer, it allows remote connections to users with permission.

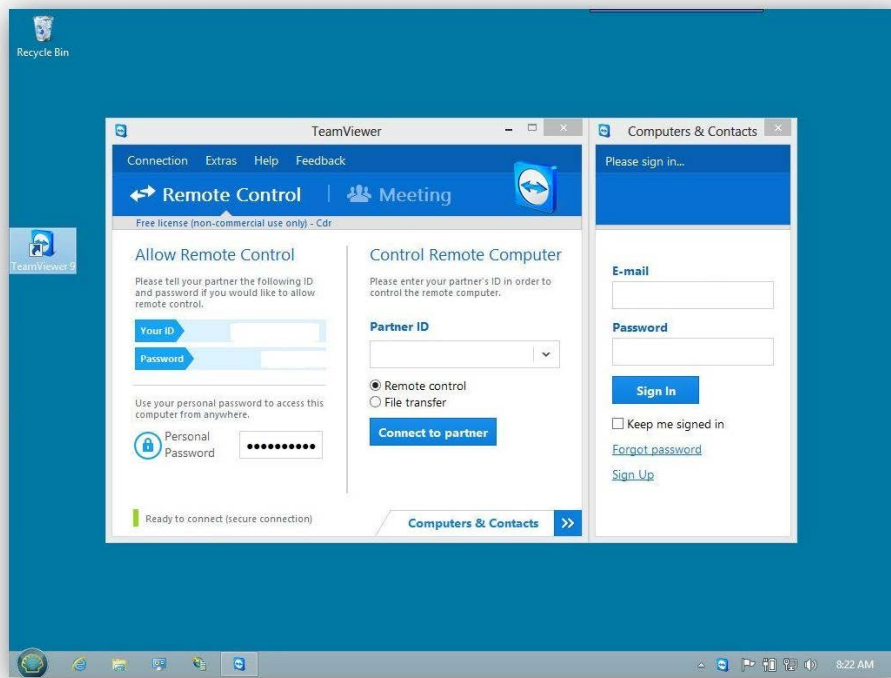


Figure 1.54- Teamviewer remote connection configuration

8.3. VPN

A **virtual private network (VPN)** extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

To ensure security, the private network connection is established using an **encrypted** layered **tunneling** protocol and VPN users use authentication methods, including passwords or certificates.

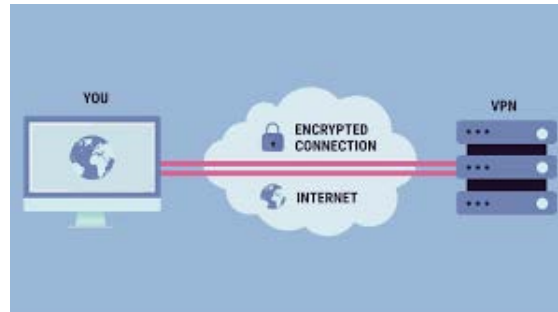


Figure 1.55- VPN connection (source: <http://hardzone.es>)

1.3 Industrial Network Protocols

Description

Industrial Network Protocols

Table of contents

1. Fieldbus Protocols

1.1. Modbus

1.2. Profibus

1.3. Industrial Ethernet.

2. OPC protocol

Fieldbus is the name of a family of industrial computer network protocols used for real-time distributed control.

In an Industrial Control System there is usually a Human Machine Interface (HMI) at the top of the hierarchy, linked to a middle layer of programmable logic controllers (PLC) via a non-time-critical communications system (e.g. Ethernet). At the bottom of the control system is the fieldbus that links the PLCs (Layer 1) to the components that actually do the work (Layer 0), such as sensors, actuators, electric motors, console lights, switches, valves and contactors.

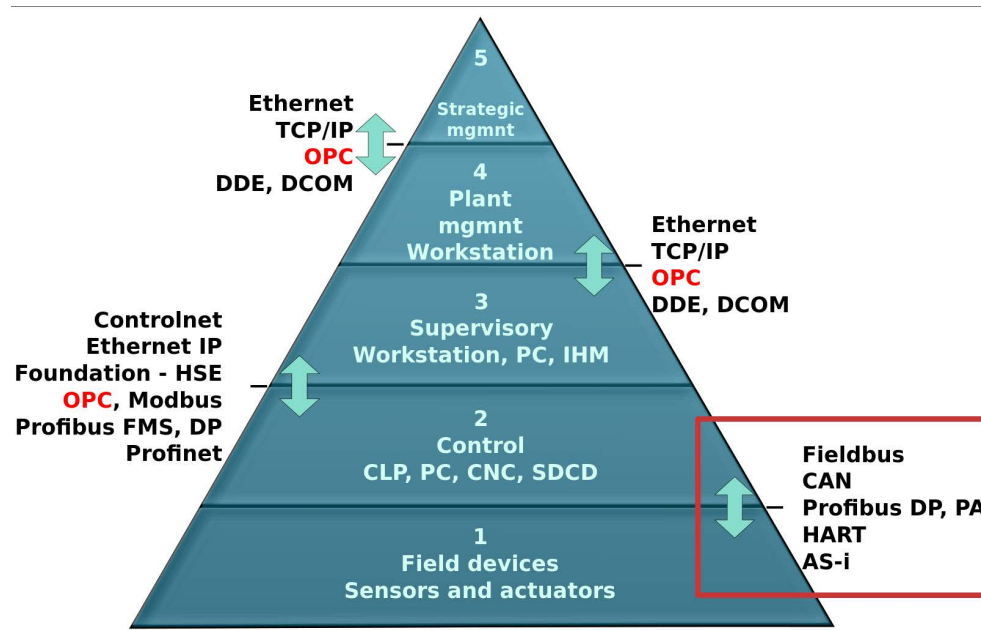


Figure 1.56- Fieldbus level scheme (source: [Wikimedia](#))

Fieldbus is an industrial network system for **real-time** distributed control and is the equivalent of the current LAN-type connections, which require only one communication point at the controller level and allow multiple devices to be connected at the same time.

Modbus is a serial (usually implemented over RS-232 or RS-485) communications protocol used to communicate PLCs. It has become a standard communication protocol and is now a commonly available means of connecting industrial electronic devices due to the next reasons

- openly published and royalty-free,
- moves raw bits or words without placing many restrictions on vendors.

Modbus is often used to connect a supervisory computer (**master**) with a remote RTU (**slave**) in SCADA systems. It is defined as a master/slave protocol (Figure 1.57), meaning a device operating as a master will poll one or more devices operating as a slave. This means a slave device cannot volunteer information; it must wait to be asked for it. The master will write data to a slave device's registers, and read data from a slave device's registers.

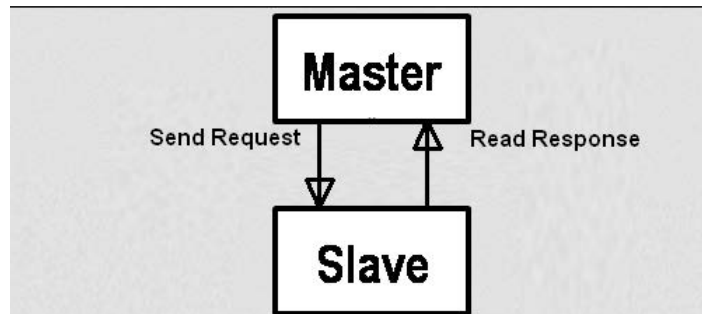


Figure 1.57- Master Slave communication process

Each exchange of data consists of a request from the master, followed by a response from the slave. As it is shown in Figure 1.58, each data packet, whether request or response, begins with the device address or slave address, followed by function code, followed by parameters defining what is being asked for or provided. The exact formats of the request and response are documented in detail in the Modbus protocol specification.

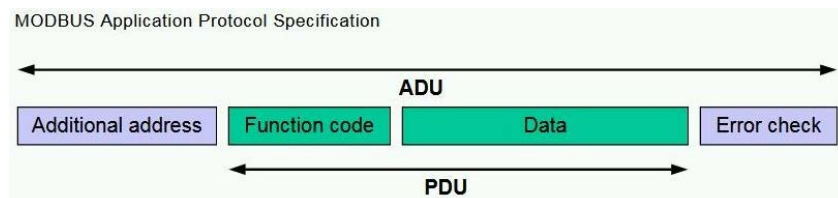


Figure 1.58- Modbus data packet structure (source: [Modbus Organization](https://www.modbus.org/))

As Figure 1.59 shows, the protocol **Modbus TCP** encapsulates Modbus RTU request and response data packets in a TCP packet transmitted over standard Ethernet networks. The address of most importance here is the IP address. The standard port for Modbus TCP is 502, but port number can often be reassigned if desired.

Checksum and error handling are handled by Ethernet in the case of Modbus TCP.

The TCP version of Modbus follows the OSI Network Reference Model. Modbus TCP defines the presentation and application layers in the OSI model.

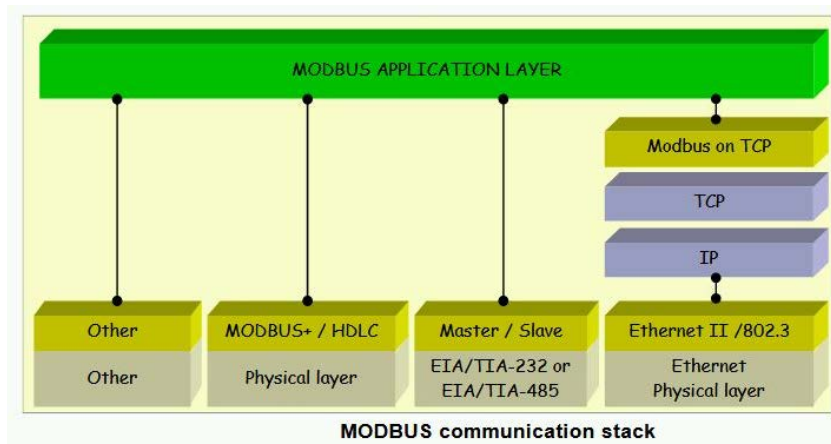


Figure 1.59- Modbus protocol stack (source: [Modbus Organization](#))

Modbus TCP runs on Ethernet (data link and physical layer), and Modbus RTU is a serial level protocol (physical layer). To communicate both networks a **gateway** (Figure 1.60) is needed to convert one protocol to the other adding or removing a 6-byte header which allows routing in Modbus TCP.

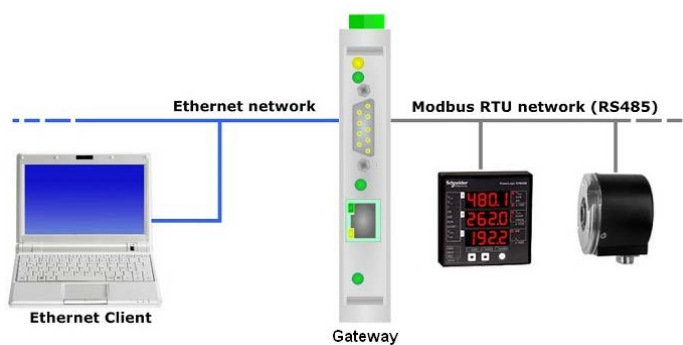


Figure 1.60- TCP-RTU communication gateway

Modbus TCP is the common protocol that connects the rest of the Modbus options through gateways.

Profibus (Process Field Bus) is a standard for fieldbus communication in automation technology. It should not be confused with the Profinet standard for Industrial Ethernet.

There are two variations of Profibus in use today (Figure 1.62); the most commonly used is Profibus DP:

- **PROFIBUS DP** (Decentralised Peripherals) is used to operate sensors and actuators via a centralised controller in a production automatized system.
- **PROFIBUS PA** (Process Automation) is used to monitor measuring equipment in process automation applications. This variant is designed for use in explosion/hazardous areas ([Ex-zone](#) 0 and 1). The Physical Layer conforms to IEC 61158-2, which allows power to be delivered over the bus to field instruments, while limiting current flows so that explosive conditions are not created, even if a malfunction occurs.

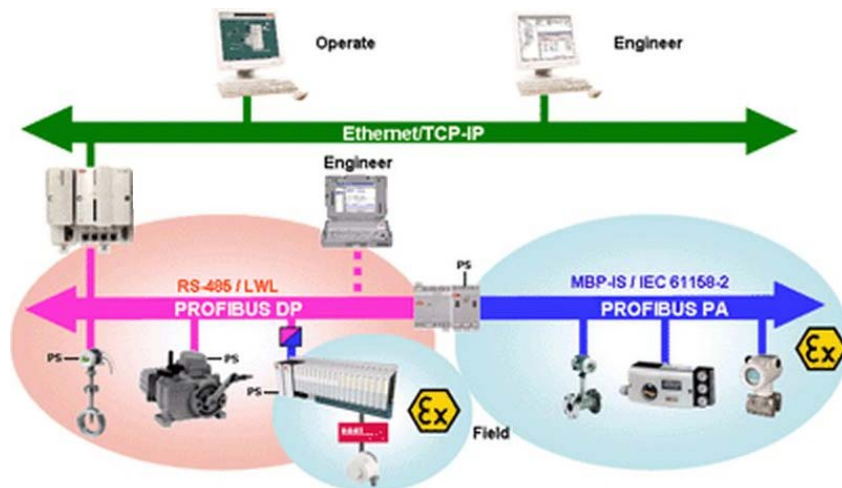


Figure 1.62- Profibus DP/PA

Profibus is developed on the OSI Layer 1,2 and 7 (Figure 1.63):

OSI-Layer	PROFIBUS		
7 Application	DPV0	DPV1	DPV2
6 Presentation			
5 Session			
4 Transport	--		
3 Network			
2 Data Link	FDL		
1 Physical	EIA-485	Optical	MBP

Figure 1.63- OSI model-Profibus levels comparison

Layer 1:

Three different methods are specified for the bit-transmission layer:

- With electrical transmission pursuant to EIA-485. Bit rates from 9.6 kbit/s to 12 Mbit/s can be used. The cable length between two repeaters is limited from 100 to 1200 m, depending on the bit rate used. This transmission method is primarily used with PROFIBUS DP.

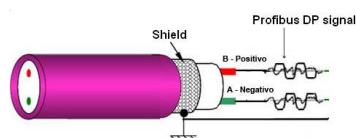


Figure 1.64 - Profibus RS-485 cable

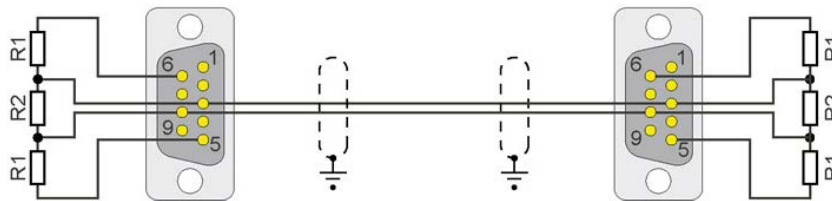
- With optical transmission via fiber optics, star, bus and ring topologies are used. The distance between the repeaters can be up to 15 km. Optic fiber-RS485 converters are needed (Figure 1.65)



Figure 1.65- Optic fiber-RS485 converter

- With MBP (Manchester Bus Powered) transmission technology, data and field bus power are fed through the same cable. This technology is used in Profibus PA.

In Profibus networks usually 9 pin Sub-D type connectors are used.

Figure 1.67- Profibus RS485 9 pin D type connector (source: [Wikimedia](#))

Layer 2:

The data link layer is called **FDL** (Field bus Data Link) and works with a hybrid access method that combines token passing with a master-slave method. In a PROFIBUS DP network, the controllers or process control systems are the **masters** and the sensors and actuators are the **slaves**. (Figure 1.68)

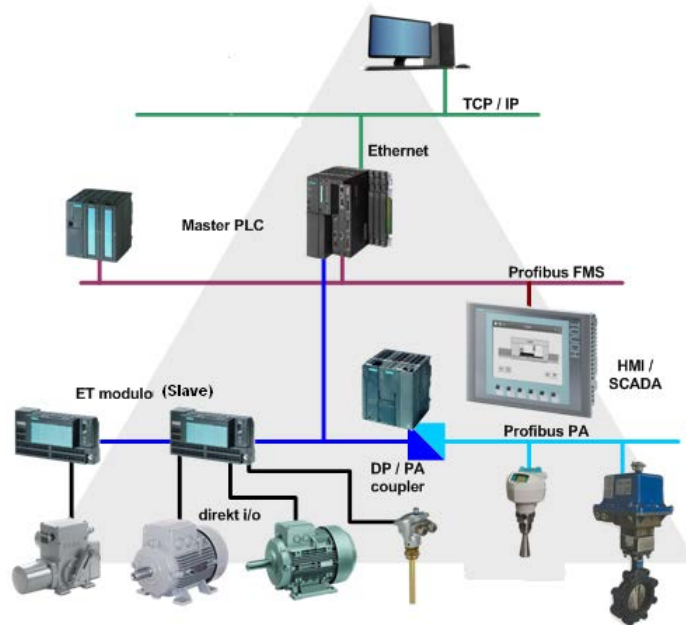


Figure 1.68- Profibus master-slave architecture (source: [Wikimedia](#))

Profibus can be connected to other fieldbus networks using the needed gateway (Figure 1.69).

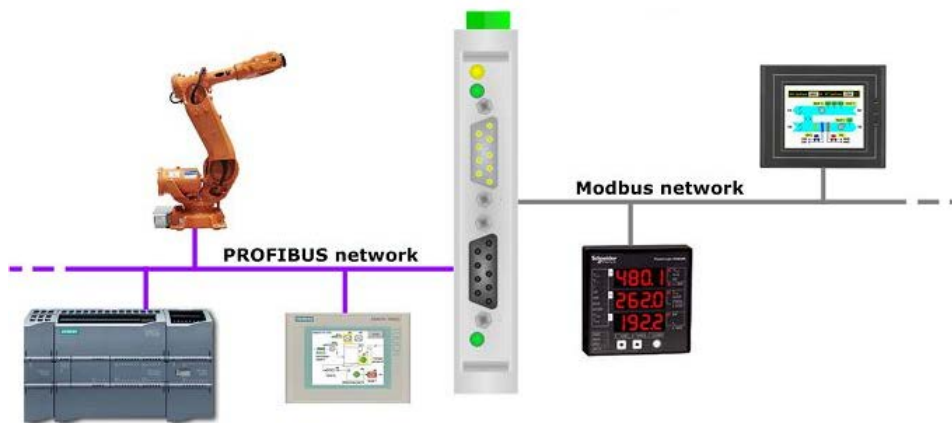


Figure 1.69- Profibus and Modbus interconnection via gateway

Industrial Ethernet uses the standards developed for Ethernet and implements them for manufacturing network communications (Figure 1.70). Modifying the data-link layer (Media Access Control) Industrial Ethernet provides **determinism** and **real-time** control (low latency), which is not critical working in an Information Technology environment but necessary in Operation Technology (industrial automation).

In addition, it must provide **interoperability** of higher levels of the OSI model and **security** from intrusions from outside the plant and from unauthorized use within the plant.

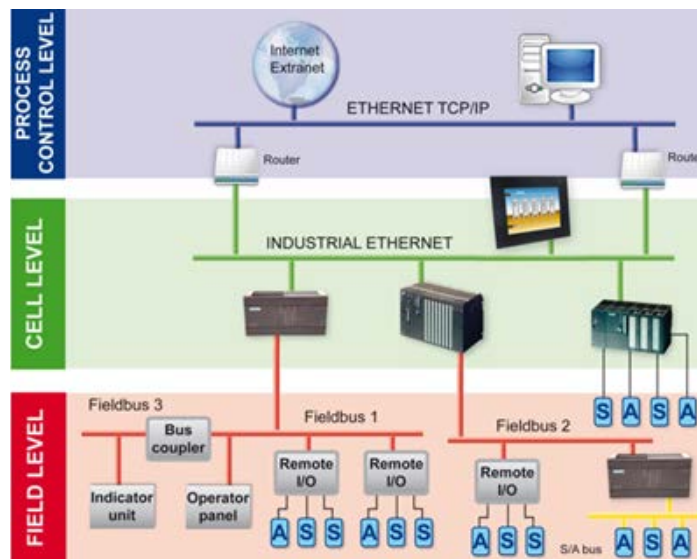


Figure 1.70 Industrial Ethernet network architecture (source: [Industrial Ethernet Book](#))

Industrial Ethernet equipment is designed for **harsh environments**, so it needs special features such as rugged connectors and extended temperature switches needed in an industrial environment. Components used in plant process areas must be designed to work in of temperature extremes, humidity, and vibration that exceed the ranges for IT equipment.

The use of fiber-optic (**SFP** ports) Ethernet reduces the problems of electrical noise and provides electrical isolation.



Figure 1.71- Industrial Ethernet switch (source: [Wikipedia](#))

Profinet is the open Industrial Ethernet standard of the International Profibus association and one of the most commonly used communication standards in automation networks.

Profinet allows compatibility with Ethernet communications (more typical of IT environments), but it must be taken on account the difference in speed that an Ethernet communication has in a corporate network versus the real-time performance required by an industrial network.

The use of the Profinet can provide the following advantages:

- Improves scalability in infrastructures.
- Makes it easier to access field devices from other networks.
- Execution of maintenance tasks from anywhere through secure connections (VPN) for remote maintenance.

The PROFINET protocol consists basically of three devices (Figure 1.72).

- **IO Controller:** Master, where the control program is executed
- **IO Device:** Remote field device that maintains communication with a controller
- **IO Supervisor:** programmable graphics device where the network analysis is made.

There is no kind of hierarchy between these devices, which means every IO has the same importance in a PROFINET network.

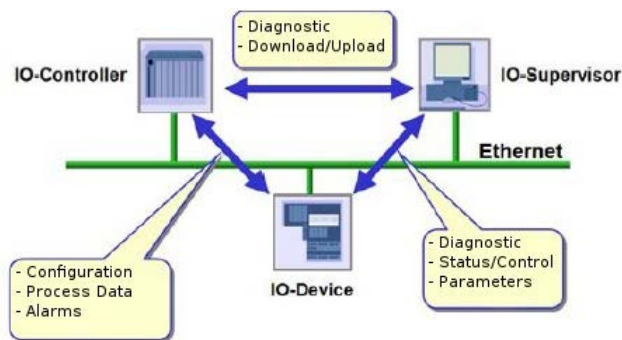


Figure 1.72- Profinet device types (source: www.semanticscholar.org)

Profinet incorporates different **profiles** through a specific interpretation for each case of the transmitted data, modifying OSI level 7 (application). There are 3 Profinet versions:

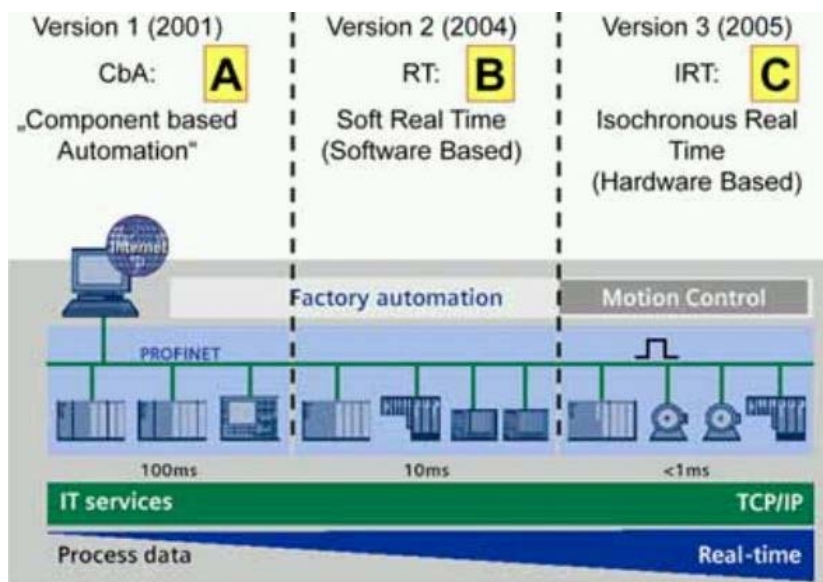
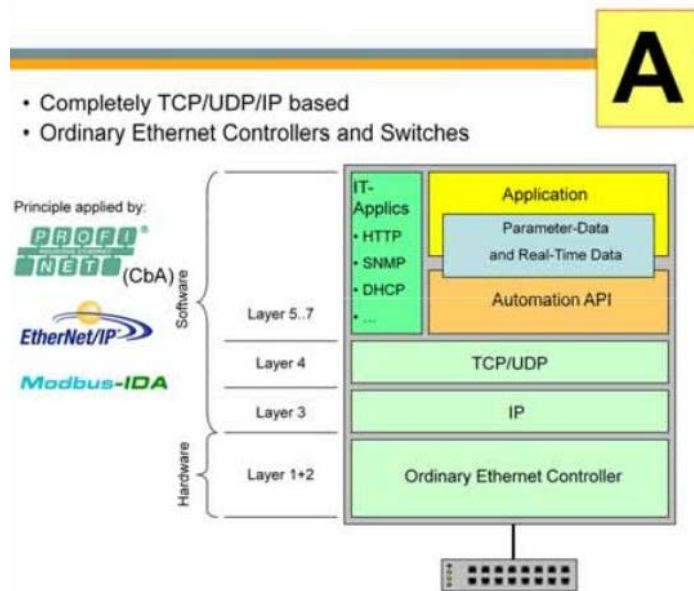


Figure 1.73- Profinet profiles (source: www.semanticscholar.org)

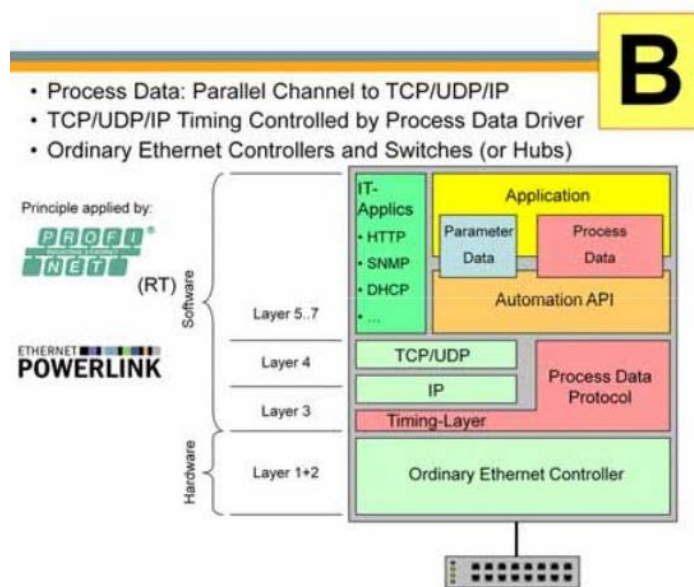
- Version 1 (Class A): **Component Based Automation (CBA)**

Its typical cycle time is 100ms, and is used for parametrization, not used for process data communication. it is not supported anymore by Profibus.

Figure 1.74- Profinet CBA architecture (source: www.ethercat.org)

- Version 2 (Class B): **Real-Time (RT)**

Its typical cycle time is 10ms, similar to Profibus, and it is used for process data communication.

Figure 1.75- Profinet RT architecture (source: www.ethercat.org)

- Version 3 (Class C) : **Isochronous Real Time (IRT)**

Its typical cycle time is 1 ms. The difference to real-time communication is essentially the high degree of determinism, so that the start of a network cycle is maintained with high precision.

C

- Process Data: Parallel Channel to TCP/UDP/IP
- TCP/UDP/IP Timing Controlled by Process Data Driver
- Special Realtime Ethernet Controllers or Switches

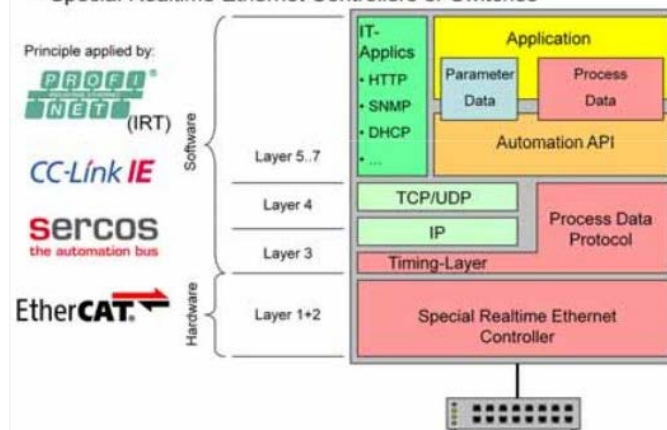


Figure 1.76- Profinet IRT architecture (source: www.ethercat.org)

OPC (Open Platform Communications) is the interoperability standard for the secure and reliable exchange of data in the industrial automation, it is platform independent and ensures the seamless flow of information among devices from multiple vendors.

These specifications define the interface between **clients and servers**, as well as servers and servers, including access to real-time data, monitoring of alarms and events, access to historical data and other applications.

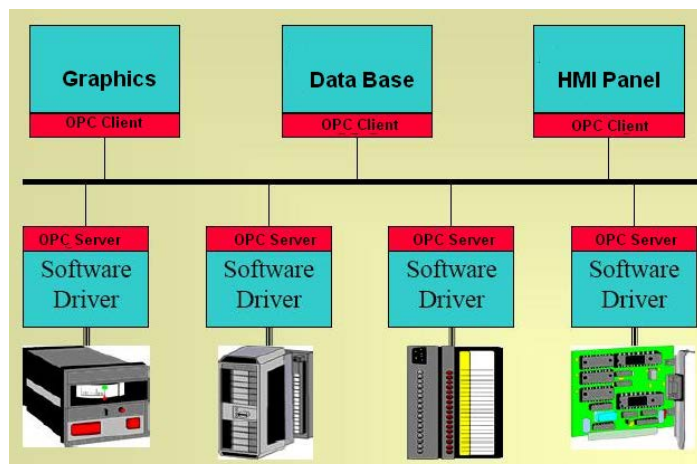


Figure 1.77- OPC server/client architecture (source: [Wikipedia](https://en.wikipedia.org/wiki/OPC))

OPC is designed to provide a **common bridge** for software applications and process control hardware to access field data from plant floor devices (Figure 1.78).

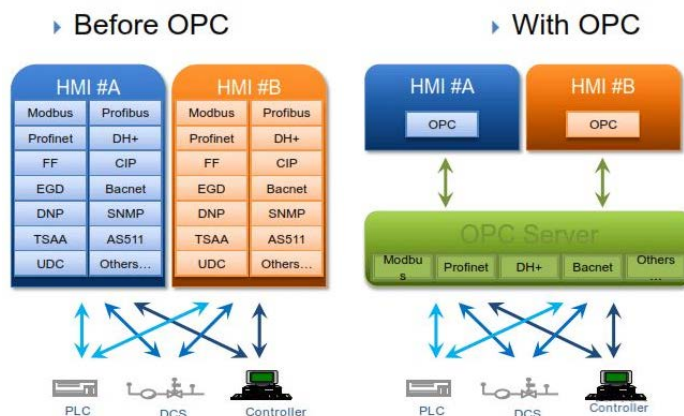


Figure 1.78- OPC architecture (source: www.theautomization.com)

An OPC Server for one hardware device provides the same methods for an OPC Client to access its data. Once a hardware manufacturer had developed their **OPC Server** for the new hardware device their work was done to allow any 'top end' to access their device, and once the SCADA producer had developed their **OPC Client** their work was done to allow access to any hardware with an OPC compliant server.

The **OPC Unified Architecture (UA)** is a platform independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework.

Innovative technologies and methodologies such as new transport protocols, security algorithms, encoding standards, or application-services can be incorporated into OPC UA while maintaining backwards compatibility.

Task 1. Computer Settings

On this first task you will learn how to set up your computer's network.

Open a command interface window (Launch>command). The following window will open:



Remember how to open it because you might need it later.

Type "ipconfig" (without quotation marks) and press Enter button. The command will return your computer's network set up data. Fill in the following table with the answer:

IP address	
Subnet mask	
Default gateway (router)	

Type "ipconfig /?" to see command options.

Type "ipconfig /all" and it will return advanced settings. This information can also be seen by launching winipcfg (Home/launch/winipcfg). Fill in the table.

Windows IP settings	
Host name	
Main DNS suffix	
Enabled routing	
Ethernet adapter	
Physical address	
Enabled DHCP	

Fill in the table with the data of your left and right colleagues (if you are last on the row, ask another colleague). Compare similar and different values.

Colleague on the left

Windows IP settings	
Host name	
Main DNS suffix	
Enabled routing	
Ethernet adapter	
Physical address	
Enabled DHCP	
IP address	
Subnet mask	
Default gateway (router)	
DNS server	

Colleague on the right

Windows IP settings	
Host name	
Main DNS suffix	
Enabled routing	
Ethernet adapter	
Physical address	
Enabled DHCP	
IP address	
Subnet mask	
Default gateway (router)	
DNS server	

Task 2. IP Addressing

On the Internet, computers are identified by their IP address (Internet Protocol). The IP is composed of 4 numbers, separated by 3 dots. Each of the 4 numbers has a value between 0 and 255 (i.e. 192.168.2.3, or 158.42.4.2).

There is also another type of identification, using domain names (i.e. www.google.com). Thanks to a protocol named DNS, the computer knows what IP address matches to that name, in this case IP address 216.58.201.164.

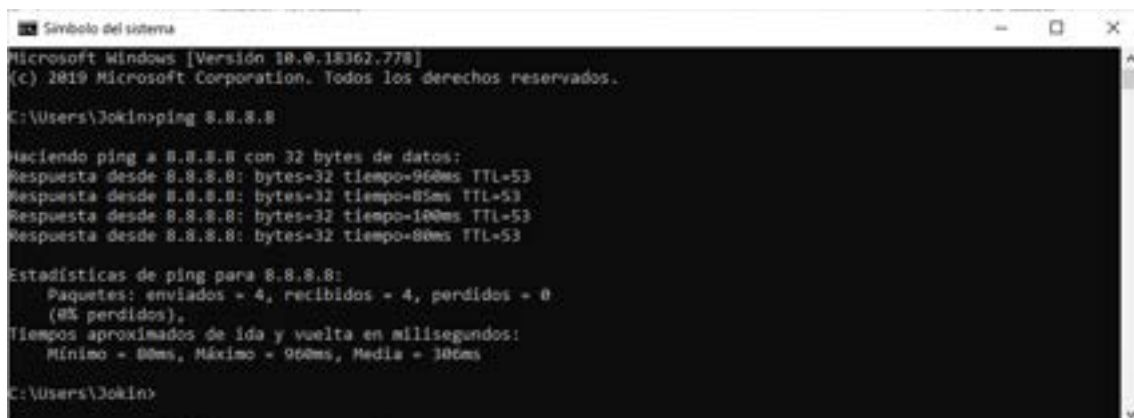
Open a command interface window (Launch>command). The following window will open:



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.18362.778]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Jokin>
```

Launch command “ping 8.8.8.8” and see if the result is similar to this one:



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.18362.778]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Jokin>ping 8.8.8.8

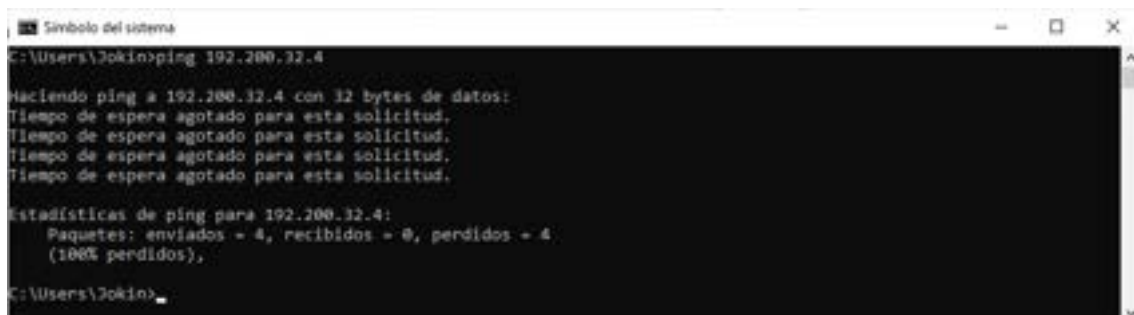
Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=960ms TTL=53
Respuesta desde 8.8.8.8: bytes=32 tiempo=85ms TTL=53
Respuesta desde 8.8.8.8: bytes=32 tiempo=180ms TTL=53
Respuesta desde 8.8.8.8: bytes=32 tiempo=88ms TTL=53

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 88ms, Máximo = 960ms, Media = 106ms

C:\Users\Jokin>
```

“Time” response parameter shows the amount of time (usually milliseconds) an ICMP packet needs (this corresponds to *ping* command) to reach destination (in this case the computer with the IP address 8.8.8.8) and return to the sender (our computer).

If there isn’t connectivity between the sender and the destination, the error message will be similar to this one:



```
Símbolo del sistema
C:\Users\Jokin>ping 192.200.32.4

Haciendo ping a 192.200.32.4 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.200.32.4:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\Jokin>
```

See what happens when launching “ping dns.google” command. *Dns google* should be translated to its equivalent IP address. Which is that IP?

```
Símbolo del sistema

C:\Users\Jokin>ping dns.google

Haciendo ping a dns.google [8.8.4.4] con 32 bytes de datos:
Respuesta desde 8.8.4.4: bytes=32 tiempo=69ms TTL=53
Respuesta desde 8.8.4.4: bytes=32 tiempo=70ms TTL=53
Respuesta desde 8.8.4.4: bytes=32 tiempo=72ms TTL=53
Respuesta desde 8.8.4.4: bytes=32 tiempo=73ms TTL=53

Estadísticas de ping para 8.8.4.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 69ms, Máximo = 73ms, Media = 71ms

C:\Users\Jokin>
```

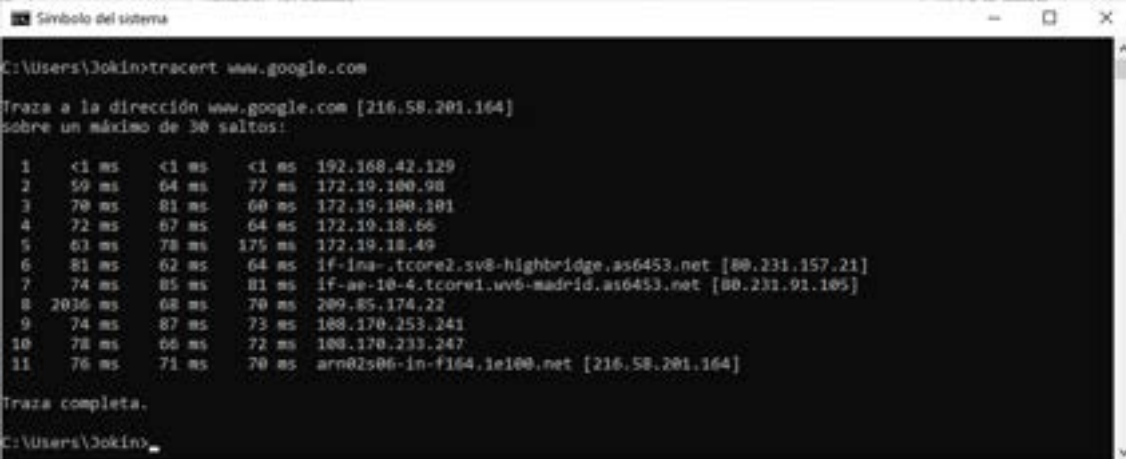
Now launch “ping www.google.com”. Which is the IP?

Task 3. Tracert Command

Internet is made of a lot of networks, linked together by communication devices called routers. When information is sent through the internet, data goes through every router until it reaches destination. Every time a network is changed through a router, we say that data has jumped.

The tracert command (it comes from *trace route*) can be used to know what devices data has gone through to reach destination. This command works like the ping command. In a command interface window, we need to launch tracert followed by the IP address or domain name from which we need the information. If we ask for a domain, it also gives the information of the IP address.

For example, if we need to know how to reach Google web server, we need to launch “tracert www.google.com”:



```
Símbolo del sistema
C:\Users\Jokin>tracert www.google.com

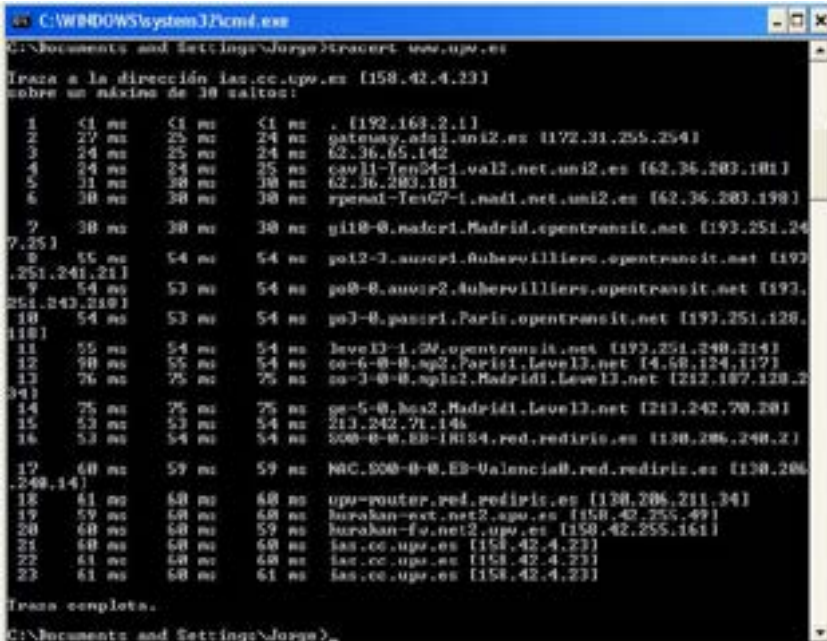
Traza a la dirección www.google.com [216.58.201.164]
sobre un máximo de 30 saltos:

  1  <1 ms    <1 ms    <1 ms  192.168.42.129
  2  59 ms    64 ms    77 ms  172.19.100.98
  3  79 ms    81 ms    60 ms  172.19.100.101
  4  72 ms    67 ms    64 ms  172.19.18.66
  5  63 ms    78 ms    175 ms 172.19.18.49
  6  81 ms    62 ms    64 ms  1f-1ea-.tcore2.sv8-highbridge.as6453.net [80.231.157.21]
  7  74 ms    85 ms    81 ms  1f-ae-10-4.tcore1.uv6-mad18.as6453.net [80.231.91.105]
  8 2036 ms   68 ms    70 ms  209.85.174.22
  9  74 ms    87 ms    73 ms  188.170.253.241
 10  78 ms    66 ms    72 ms  188.170.233.247
 11  76 ms    71 ms    70 ms  arr02s06-in-f164.1e100.net [216.58.201.164]

Traza completa.
C:\Users\Jokin>
```

The answer shows the IP addresses of the routers the response request has gone through until it has reached destination, and also their response time.

By using the tracert command we may find some curiosities, such as it doesn't always follow the shortest path to reach destination. In the following example you can see that to reach the UPV server (which is located in Valencia) from Bilbao, it has gone through various routers in Paris.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Jorge>tracert www.upv.es

Traza a la dirección las.cc.upv.es [158.42.4.231]
sobre un máximo de 30 saltos:

  1  <1 ms    <1 ms    <1 ms  . [192.168.2.1]
  2  27 ms    25 ms    24 ms  gateway.adsl.uni2.es [172.31.255.254]
  3  24 ms    25 ms    24 ms  62.36.65.142
  4  24 ms    24 ms    25 ms  cav11-1en04-1.val2.net.uni2.es [62.36.203.101]
  5  31 ms    28 ms    30 ms  62.36.203.101
  6  30 ms    28 ms    30 ms  rpenal-1en07-1.nad1.net.uni2.es [62.36.203.190]
  7  38 ms    38 ms    38 ms  g118-0.nadcr1.Madrid.opentransit.net [193.251.24
7.25]
  8  55 ms    54 ms    54 ms  po12-3.auxcp1.Buherovilliers.opentransit.net [193
.251.241.211]
  9  54 ms    53 ms    54 ms  po8-0.auxr2.Buherovilliers.opentransit.net [193.
251.242.210]
 10  54 ms    53 ms    54 ms  po7-0.pasr1.Paris.opentransit.net [193.251.128.
110]
 11  55 ms    54 ms    54 ms  leve13-1.0v.opentransit.net [193.251.240.214]
 12  90 ms    54 ms    54 ms  eo-6-0-0.sp2.Paris1.Level3.net [4.58.124.117]
 13  76 ms    75 ms    75 ms  eo-3-0-0.spl2.Madrid1.Level3.net [212.107.120.2
34]
 14  75 ms    75 ms    75 ms  eo-5-0.hca2.Madrid1.Level3.net [212.242.70.201]
 15  52 ms    53 ms    54 ms  212.242.71.146
 16  53 ms    54 ms    54 ms  000-0-0.EB-1N184.red.rediris.es [130.206.240.2]
 17  60 ms    59 ms    59 ms  NAC.000-0-0.EB-Valencia8.red.rediris.es [130.206
.240.14]
 18  61 ms    60 ms    60 ms  upv-router.red.rediris.es [130.206.211.34]
 19  59 ms    60 ms    60 ms  buraban-est.net2.upv.es [158.42.255.49]
 20  60 ms    60 ms    59 ms  buraban-fw.net2.upv.es [158.42.255.161]
 21  60 ms    60 ms    60 ms  las.cc.upv.es [158.42.4.231]
 22  61 ms    60 ms    60 ms  las.cc.upv.es [158.42.4.231]
 23  61 ms    60 ms    61 ms  las.cc.upv.es [158.42.4.231]

Traza completa.
C:\Documents and Settings\Jorge>
```

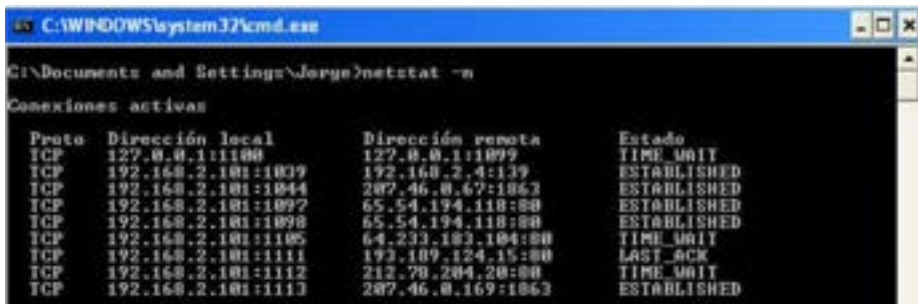
Fill in the following table with the results of using the tracert command with the following domains:

Name	Number of "jumps"
www.elpais.com	
www.upv.es	
www.marca.com	
Sntp.correo.yahoo.es	
www.google.com	

Task 4. Netstat Command

The netstat command shows the connections that are open between various computers, for example, when you connect to a website or download the email.

Launch the “netstat -n” command and see what connections are currently open in your computer:

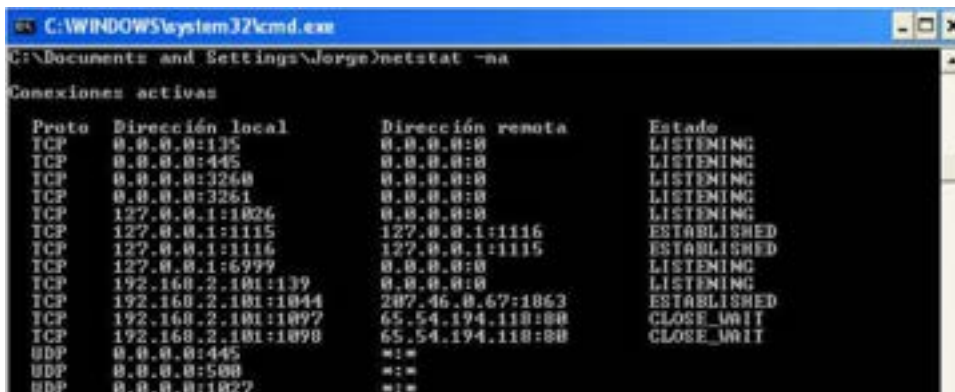


```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Jorge>netstat -n
Conexiones activas
Proto  Dirección local      Dirección remota      Estado
TCP    127.0.0.1:1100        127.0.0.1:11099      TIME_WAIT
TCP    192.168.2.101:1039    192.168.2.4:139      ESTABLISHED
TCP    192.168.2.101:1044    207.46.0.67:1063     ESTABLISHED
TCP    192.168.2.101:1097    65.54.194.118:80     ESTABLISHED
TCP    192.168.2.101:1098    65.54.194.118:80     ESTABLISHED
TCP    192.168.2.101:1105    64.233.103.104:80    TIME_WAIT
TCP    192.168.2.101:1111    193.109.124.15:80    LAST_ACK
TCP    192.168.2.101:1112    212.78.204.20:80     TIME_WAIT
TCP    192.168.2.101:1113    207.46.0.169:1063    ESTABLISHED
```

In the answer of the Netstat command, both local and remote addresses are indicated by the IP or computer name, followed by two dots and the port number. The port is one number that indicates the application or protocol that is being used.

For example, port 80 is from protocol http, for websites; or 1863 is the Messenger port (disused messaging application).

Another option for the netstat command is -a. This shows what ports you have currently open in your computer. These are applications that are listening as servers in your computer, and they would allow other people to connect to your computer (for example, if you have a shared folder). These can be identified because the state shows *listening*.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Jorge>netstat -na
Conexiones activas
Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135          0.0.0.0:0             LISTENING
TCP    0.0.0.0:445          0.0.0.0:0             LISTENING
TCP    0.0.0.0:3260         0.0.0.0:0             LISTENING
TCP    0.0.0.0:3261         0.0.0.0:0             LISTENING
TCP    127.0.0.1:1026       0.0.0.0:0             LISTENING
TCP    127.0.0.1:1115       127.0.0.1:1116       ESTABLISHED
TCP    127.0.0.1:1116       127.0.0.1:1115       ESTABLISHED
TCP    127.0.0.1:6999       0.0.0.0:0             LISTENING
TCP    192.168.2.101:139    0.0.0.0:0             LISTENING
TCP    192.168.2.101:1044    207.46.0.67:1063     ESTABLISHED
TCP    192.168.2.101:1097    65.54.194.118:80     CLOSE_WAIT
TCP    192.168.2.101:1098    65.54.194.118:80     CLOSE_WAIT
UDP    0.0.0.0:445          *:*
UDP    0.0.0.0:500          *:*
UDP    0.0.0.0:1027        *:*
```

Launch netstat -na in your command line. How many connections are there? Which are their IP addresses and ports?

Task 5. How to connect through SSH / Telnet to a router for advanced settings with PuTTY

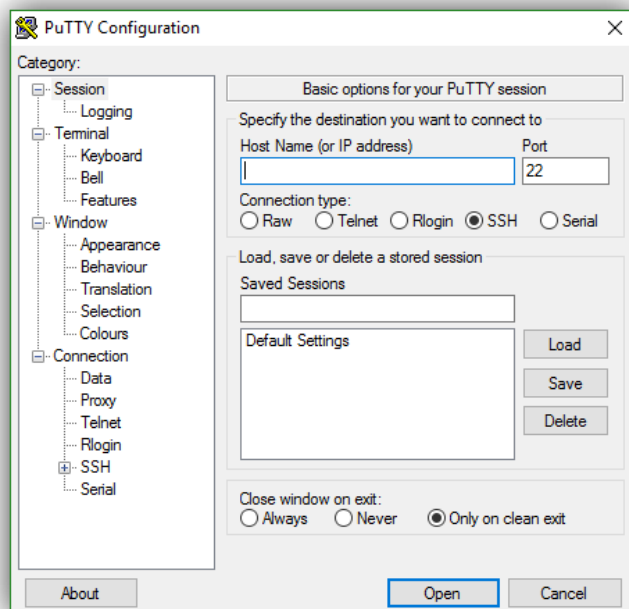
Nowadays, practically all the routers in the market have a web interface from which we can make all kinds of settings: change username/password, Wi-Fi settings, open ports and so on. This interface has been mainly created for home users, who have a lack of advanced knowledge, and apart from being user-friendly, it only shows the main and most used options of the routers, so most of the functions are hidden and with no access, not at least through this interface.

Practically every router has a Telnet server that allows us to communicate with the router from the command line, which is ideal for expert users with advanced knowledge. It allows us to control almost every possible inside setting from the router, in case we need to access them. The most advanced routers have SSH protocol support, which allows us to connect in a similar way as we do through Telnet, but encrypting all the connections.

Although Windows can enable a Telnet and SSH client in the system, there are some third-party applications that are easier to use, such as PuTTY, that will allow us to manage all these connections in a correct way.

PuTTY is a free application, portable and with an open code, which has been developed to ease the connections through the SSH/Telnet protocols from Windows. Let's see how we can connect remotely to a router by using these protocols.

First, we need to download the latest version of PuTTY [from their main website](#). It is portable and it doesn't need installation, so once you have downloaded it, you only need to run it. A window similar to this one will open:



First, we need to introduce the IP address of our router. It usually is 192.168.1.1 or 192.168.0.1, depending on the model and settings.

Right below the blank to introduce the IP, we find "**Connection type**", in which we need to specify the protocol we are going to use. The most common ones, as we said, are SSH and Telnet. If our router connects through the serial port, PuTTY will also allow us to set a connection with the serial port in order to set it up through the commands.

After introducing the IP and selecting the connection protocol, press “Open” and the programme will connect to the router.

If the connection is allowed and has been set up, PuTTY will show the following window:



Last, we need to log in with our username and password to start controlling the device.

It might occur that the username and password of Telnet / SSH do not correspond to those of the web interface, especially in the routers of the operators.



Co-funded by the
Erasmus+ Programme
of the European Union



MODULE 2

Security concepts in industrial environments, Integration of IT/OT

2.1 Security in Critical infrastructures

Description

2.1 Security in Critical infrastructures

Table of contents

- 1. Plant security**
- 2. Plant security (continue)**
- 3. Network and System security**

Plant security ensures that the buildings engaged in the manufacturing progress are well protected against prohibited access. Some countermeasures taken can be:

Ø Fences

It is common in plant installations to be surrounded by a fence (Figure 2.1)

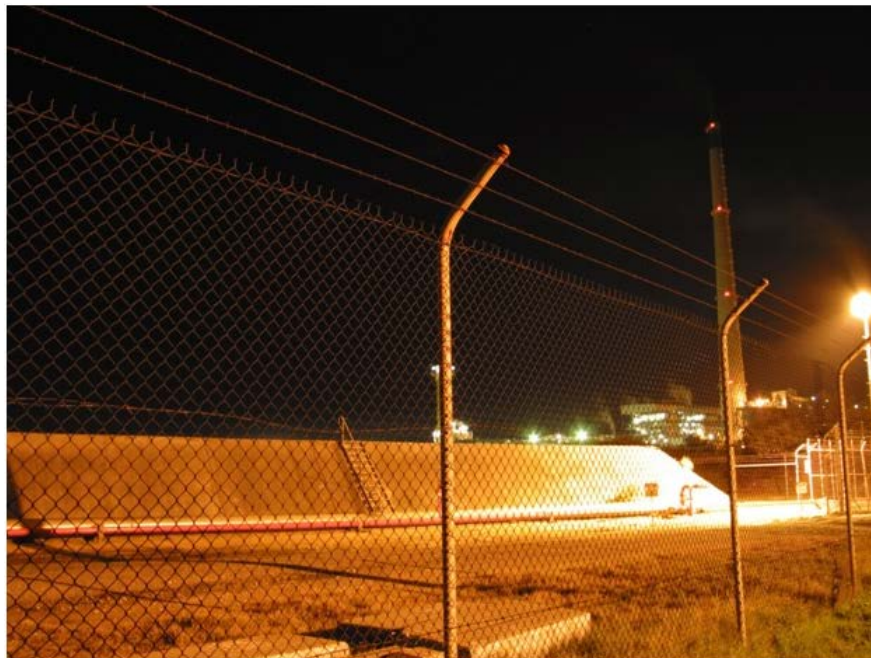


Figure 2.1 Industrial area with a fence [source](#)

Typically, a plant fence establishes boundaries of the plant property, but its main use is to provide a first security measure against possible intruders. Although a fence by itself does not prevent an intruder, if used in conjunction with other security measures it can be a good safety solution. Nowadays, fences are getting 'smart'. This means that sensors spread along the fence can identify if an intruder has entered the prohibited area. This new generation of fences can be connected in a network.

G

G Guards.

Th The presence of guards mainly depends on the type and size of the installed business. Depending on the law they might be armed as well. Usually there is an outpost at the main gate of the factory and the guards allow or not the entrance of the personnel and the visitors as well. Part of their duties could be the patrol of the plant especially when the factory is closed.

Turnstiles.

A turnstile (Figure 2.2) may be present at the main gate of the factory. It prevents visitors of the plant to enter the facility without control and also delays intruders. Latest implementations give network capabilities to turnstiles.



Figure 2.2: A turnstile - By Fabtron - Own work, CC BY-SA 4.0 [source](#)

∅

Ø CCTV cameras

CCTV stands for closed circuit television. Security cameras (Figure 2.3) are placed around the outer perimeter of the plant - usually in vaults upon the outer fence- to record any activity 24/7. Security cams are also placed in the building, the main entrance and in many cases in working areas also. In large installations (with a large number of security cameras) there is a control room, where authorized and trained personnel monitors the cameras to detect delinquent behavior. All data captured from the cams are stored into hard discs in a digital video recorder (DVR) or a network video recorder (NVR). In the latter case the installation technicians and the monitoring personnel must be very careful because the NVR can be easily a target of a cyberattack.



Figure 2.3 Security cams

Biometric readers

They are placed outside of doors, main gates etc. Typical biometric data used for identifying a person includes: fingerprints, eye iris and the shape of the face. Since all the pre-mentioned biometric characteristics are unique for each person, biometric readers are supposed to provide a very good security level. However, there is a risk that the biometric readers be compromised as well, especially when connected in a network. Biometric readers can also be used in conjunction with a RFID card or a password for better security (Figure 2.4). Latest biometric readers have network capabilities, therefore the risk of becoming target of a cyber-attack is relatively high.



Figure 2.4 A biometric reader - [Source](#)

Ø

Access Controls

These security systems are used to provide access to authorized personnel or visitors. They are programmable and can define different access rights according to the security plan of the industry. Different employees can have different access rights regarding the areas they can visit, the visiting times, etc. Like all the pre-mentioned methods access controls have network capabilities also. RFID readers, smart magnetic cards or even biometric readers can be used.

Network security

- Concerns both hardware and software
- Focuses into a variety of threats
- Prevents unauthorized access to networks
- Supervises network access

Common types of network security are:

- Internet security software (antivirus, anti-malware, ransomware protection, etc.)
- Application security
- Data loss avoidance
- Email security
- Firewalls – Network segmentation - Virtual Private Network (VPN)
- Web security
- Wireless security
- Access control

System's integrity concerns all the measures/policies taken to protect automation systems and components against unauthorized access (physical or remote). Some of the measures could be:

- Antivirus and white listing software
- Maintenance and update processes
- User authentication for plant or machine operators
- Integrated access protection mechanisms in automation components

2.2. OT/IT Integration

Description

2.2. OT/IT Integration

Table of contents

- 1. OT/IT Integration**
- 2. Advantages**
- 3. Disadvantages**
- 4. Computer security updating policy**
- 5. PLCs security updating policy**

1. OT/IT Integration

Operational Technology (OT) in any industrial environment is defined as the hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Basically, OT is the utilization of PCs to monitor or change the physical condition of a system.

Operational technology examples:

- SCADA
- PLCs
- Scientific equipment
- DCS

Information Technology (IT) mention to anything identified with registering innovation to computing technology, PC equipment, software programming, hardware and systems administration. Software programming incorporates all the PC programs - codes and guidelines - inside a PC. PCs don't work without programming. Computer hardware, mention to in this situation, alludes to the physical segments of a PC. The (screen), mouse, and motherboard, and there are other devices where they are hardware devices.

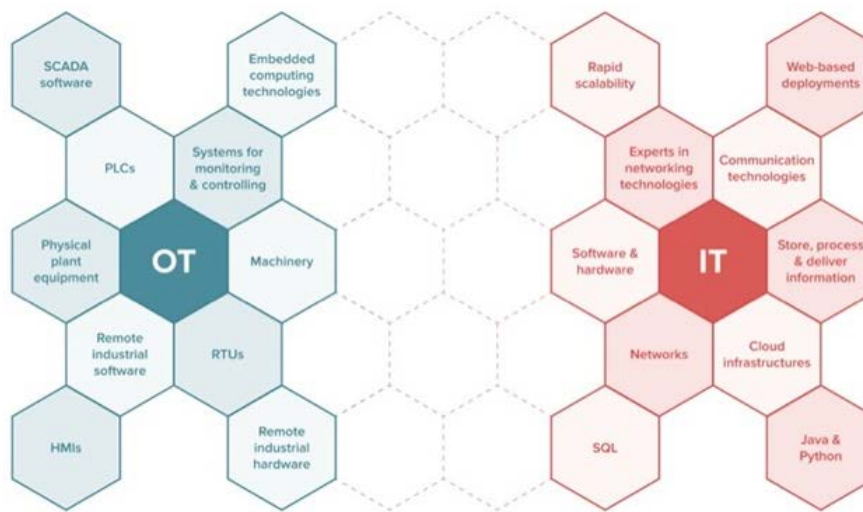


Figure 2.5 operational technology (OT) and information technology (IT) [source](#)

It may come to your mind that IT is System communications, hardware, software that store, process, and convey data to all parts of an organization. IT experts are intimate and spent significant time in the progress. For example, cloud foundations, web applications and programming technologies (Python, SQL, java, c++) etc.

OT includes devices, physical gear and equipment, hardware and remote industrial software. OT experts center around systems utilized for monitoring and control. They are utilized to PLC's, Human Machine Interfaces (HMI's), embedded computing technologies, Remote Terminal Units (RTU's), Supervisory Control and Data Acquisition (SCADA) frameworks.

SCADA systems gather information from various procedures on the plant floor. The individuals who work in OT must make sense of how to incorporate every one of the systems to cooperate together. Since most OT innovations are proprietary, numerous SCADA arrangements can be hard to integrate.

PROFINET (OT network) and Ethernet (IT network) are two widespread protocols that can be interconnected (more information can be found in [Module 1](#)). The only problem when these two protocols are interconnected is that it may reduce the [availability](#).

For more information on security countermeasures, visit: <https://www.iso.org/isoiec-27001-information-security.html>

2. Advantages

OT/IT integration has several advantages:

Increases Production and Saves Time

Information technology has assisted the business process to make them incredibly cost effective money making machines. This thusly expands efficiency which at last offers ascend to profits that implies better pay and less tiresome working conditions.

Improves Communication

Information Communication Technology (ICT) tools such as email, video conferencing, cellphones, laptops and so forth allow direct communication within a business. This permits more connectivity all through interior and outside structures.

Improves Data Storage, File Management, and Data Reporting/ Analysis

Businesses use cloud services facilitating businesses to store and backup data to reinforcement business information. Additionally, it saves times and makes transfer and access to the data easier from anywhere at anytime remotely. Services such Dropbox, entrepreneurs can get their information at anytime they want. Also, databases today take into account better analysis of a lot of data advancing better and more informed decision making with an effect on development.

Reduce Costs of Operation

Communication technology and social technology have made business advancement and the release of products affordable. Numerous independent companies have discovered approaches to utilize social technology to raise their brand congition and get more customers at a negligible expense. Elements like cost play a decisive role in the advancement and development of a business. Along these lines, utilizing information technology data innovation to chop down operational costs, will bring about business development.

Improves Business Competitive

A Business use of technology is to gain competitive advantages. Business who advance and embrace innovation to stay productive and improve their process. Commonly have high trustness of their customer's rates as they can reliably meet and serve the desires for their customers.

3. Disadvantages

However, OT/IT integration has also disadvantages:

Implementation Costs

Small companies sometimes have basic precision technology and try to maintain this technology to be cost efficient; due to this lack of investment they lose their customers, which become clients of other companies in their industry while having the funds and resources.

Removal work

As it is known, the growth of technologies has replaced human positions in several jobs.

Security Breaches

Since businesses store their information on remote cloud servers which can be accessed online with a username and secret password, it is possible to lose that information or to have any vulnerability due to bugs or hackers

4. Computer security updating policy

To guarantee security and stability, it's important to have well-documented practices for installing **software updates**. The table below offering rules for backups, administer updating process and a planning time for the updates.

From the policy: Maintaining a standard timetable of updates- - just as applying basic fixes as vulnerabilities are found is vital to keeping up the integrity of corporate security. With the coming of such threats as ransomware, the performing ordinary security and platform updates and creating backups, is important to guarantee that business processes can be waged smoothly. An example of the security measures that should be taken to adequately protect a computer is shown in Table 1

Table 1: Computer Security Policy

Weekly Updates

Payload: Security patches and updates to standard applications installed on the computer.

Schedule: Every Thursday(or some other day) starting at 8PM.

Power State: Computer must be turned on in order to receive updates.

Login State: Computer will attempt to install updates regardless of whether anyone is logged onto the computer or not. **SAVE YOUR WORK AS THE COMPUTER WILL REBOOT REGARDLESS OF ANY OPEN APPLICATIONS AND/OR UNSAVED WORK.**

Failover: If the computer is not powered on during the scheduled update, application updates will be applied the next time the computer is turned on.

Backup: Backup important files twice a month

IF a User IS Logged In

Overview: The computer will attempt to install updates, prompting the user with flexible installation and reboot options to accommodate user work schedule. Updates will be applied and the computer will be rebooted given a lack of response to prompts.

Snoozing Timeout: If the update is not snoozed within 30 minutes, updates will automatically begin installing.

Reboot Snoozing: If an update is applied which requires a reboot, the user may snooze the reboot up to seven (7) times before the computer will automatically reboot in order to complete the installation. Snoozing lasts 30 minutes before the user is re-prompted.

Reboot Timeout: If the reboot is not snoozed within 30 minutes, the computer will re-prompt in 120 minutes (ie. another snooze). After the seven (7) snoozes noted above, the user will be forced to reboot the computer.

Reboot Frequency: If an update is applied which requires a reboot, the computer will reboot once.

Performance Impact: Application updates vary in number and size at any given time. Impact to computer performance is generally negligible with a possible reboot after installation.

IF NO User Is Logged In

Overview: The computer will install updates and automatically reboot if necessary.

Reboot Frequency: If an update is applied which requires a reboot, the computer will reboot once.

5. PLCs security updating policy

PLCs are as important in control system networks as they would be in any other network environment. It is essential that they are managed with the highest priority. Any access, maintenance, upgrade, test, modification, downtime of PLCs need to be accounted for and these policies need to be enforced.

Basic policy principles

- **Correcting default passwords**

Change all default passwords. Factory-set default passwords being left unchanged is one of the most common password mistakes that organizations make.

- **Ensuring only certified individuals are in the control system's environment**

For security issues only people who have access to the business control system must be there.

- **Limiting access to thumb drives and securing access**

Users must often be informed about the usage of the devices and new technologies, or if something changes in the future.

- **Upgrading firmware to the last version**

A common operating system update/firmware update is a security update, which is issued to protect your computer/system against vulnerabilities that might be exploited by hackers and viruses.



Figure 2.6 PLC [source](#)



Figure 2.7 PLC [source](#)

2.3 Attacks on Industrial Systems

Description

2.3 Attacks on Industrial Systems

Table of contents

1. DoS/DDos Attacks

- 1.1. Types of DDoS Attacks
- 1.2. Volume-Based Attacks
- 1.3. Protocol Attacks
- 1.4. Application Layer Attacks
- 1.5. Example of SYN flood attack
- 1.6. Example of HTTP flood attack
- 1.7. Example of DNS amplification attack
- 1.8. DDoS prevention
- 1.9. DoS activity
- 1.10. Dos summary

2. Man-in-the-Middle (MitM) attack

- 2.1. Simplification of the ARP protocol
- 2.2. ARP Network traffic
- 2.3. ARP Spoofing
- 2.4. Example scenario
- 2.5. HTTPS to the rescue... ?
- 2.6. Forcing HTTP communication

3. Dictionary and phishing attacks**4. SQLInjection attack**

- 4.1. How Do SQL Injection Attacks Work?
- 4.2. How Can SQL Injection Attacks Be Prevented?

5. Modbus attack

- 5.1. Countermeasures

DOS is the acronym of **D**enial of **S**ervice. Is a type of attack which takes place on a computer or network, preventing system resources from being accessible to users. Turns off the site(web-server) you are targeting. To achieve this goal it creates many service requests at the same time that the server hosting the site cannot satisfy the server failing to respond to all the requests. So, as long as there is a DoS attack, regular website traffic will be either slow or inactive.

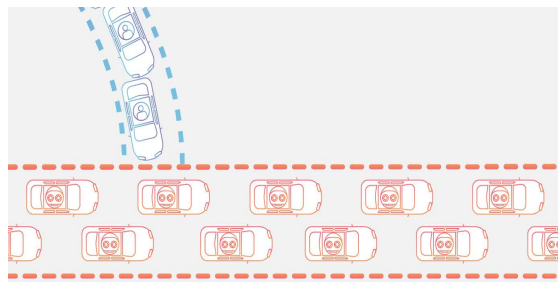


Figure 2.8 Dos attack traffic [source](#)

Cutting off some business from the web can conduct to huge loss of business or money. The web-internet and computer networks feed a great deal of organizations. Some organizations, for example, ecommerce, payment services, altogether rely upon the internet to work together as business.

There are two types of attacks:

- **DoS**- this type of attack is performed by a single host
- **Distributed DoS(DDoS)**- is accomplished by sending a large number of unnecessary requests to the system or network resource from many different sources..

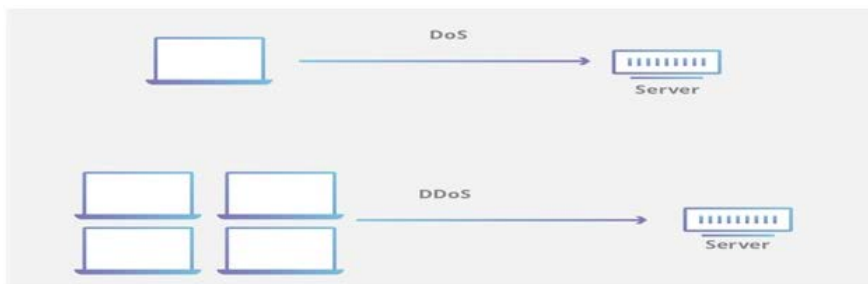


Figure 2.9 Types of Dos attacks [source](#)

Operation of a DDoS attack

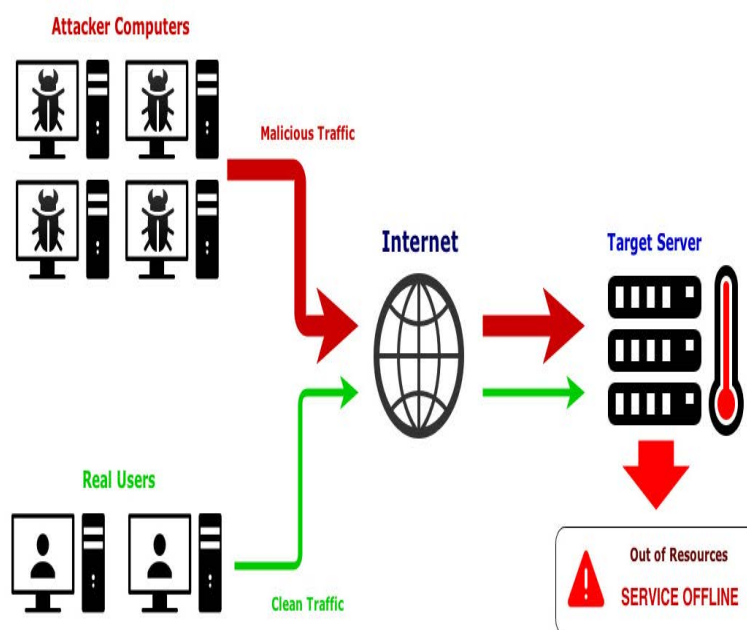


Figure 2.10 Understanding DDos attacks [source](#)

There are three types of DDoS attacks:

- Volume-based Attacks
- Protocol Attacks
- Application Layer Attacks

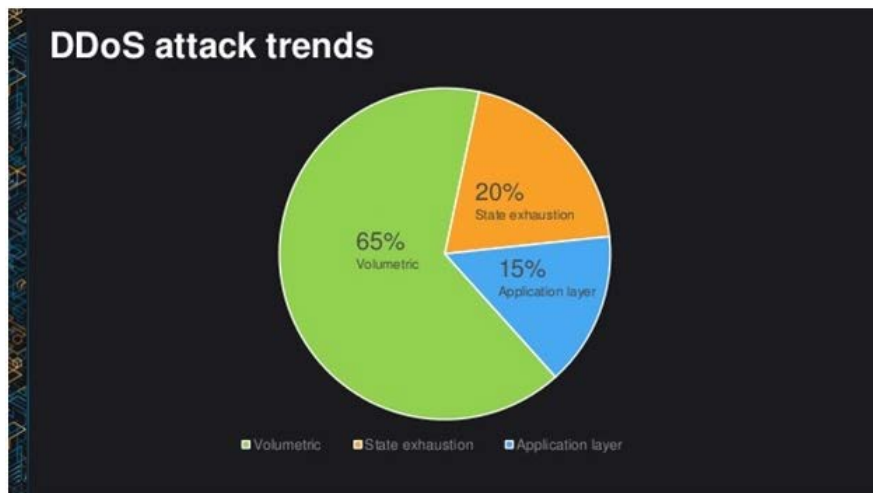


Figure 2.11 DDoS attacks trends [source](#)

Volume-based attacks as their name implies, these attacks are based on volume. There are likewise called **Layer 3 and 4 Attacks**. The attacker uses very basic tactics and most of the available resources are earned in this "game". If they manage to overload and exceed the available resources, they win. For most site owners, it is easy to run out of resources. The attack magnitude is measured in **Bits per Second (bps)**.

Volume Based Attacks

- >UDP floods
- >ICMP floods
- >Other spoofed-packet floods



Figure 2.12 Volume Based Attacks [source](#)

Some floods are:

- **UDP Flood** – A UDP flood attack involves sending a very large number of UDP packets to a computer's random ports, more especially port number 53. The attacking computer will first have to determine if any of its services are listening on that port and if it is not responding must reply with an ICMP Destination Unreachable packet. Therefore, the influx of a large number of UDP packets into the attacking computer forces him to respond with an equally large number of ICMP packets, which ultimately prevents other ordinary users from using his PC services. Specialized firewalls can be used to filter out or block malicious UDP packets.
- **ICMP Flood** – The attacker sends ICMP Echo Request flooding packets to a remote host/user. In order for this attack to succeed, the attacker must have more bandwidth than the victim. If the victim responds with an ICMP Echo Reply packet to each ping packet (ICMP Echo Request), then it consumes all of its bandwidth and consequently the services it offers are no longer available to its users. A tactic to deal is: Instead of rejecting all ping packets, the number of packets that the firewall receives is logged, and if that number is found to exceed a predefined limit, then the firewall starts to reject them.
- **HTTP Flood** – HTTP flood attack is a type of denial of service attack in which the attacker manipulates the HTTP and POST protocols in order to attack a webserver or application.

Protocol attacks this type of attack is targeted at protocol level. This category includes Synflood, Ping of Death, DNS flood and more. The attack magnitude is measured in **Packets per Second**.

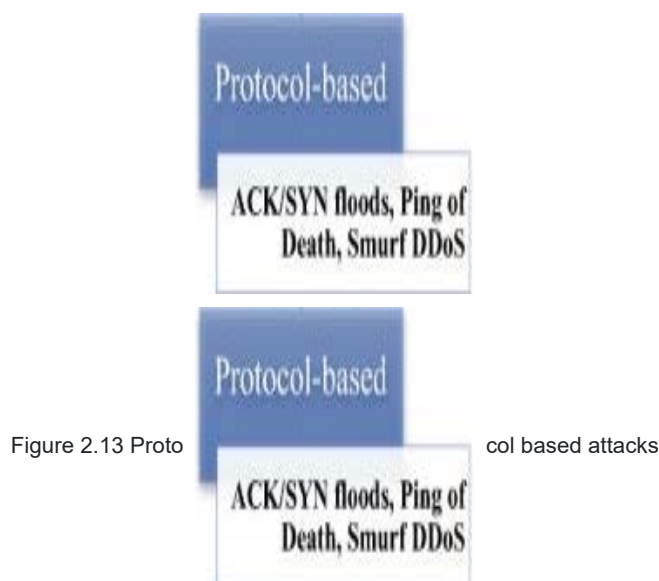


Figure 2.13 Proto

col based attacks

- **DNS Flood** – The attacker arranges to send a large number of DNS requests to the target, which is apparently a DNS server. The result is the victim receiving so many DNS requests at the same time that it is unable to handle them and therefore ends up it is drop down due to overloads mainly on its memory and CPU.
- **SYN Flood** – The attacker sends multiple SYN requests to one victim. The victim computer allocates a place in its tables for each request that arrives and sends a SYN + ACK response packet. If the attacker does not respond, or if he has hidden his real ip address, the position in the table will remain reserved until the waiting time expires. If the intruder sends thousands of SYN requests, the victim's computer table positions will be filled and the legitimate connections will not be able to pass.

The most effective way to deal with this risk is to record the number of connections each client has started and to forbid the creation of new connections when that number exceeds a predefined limit. However, if the attacker in each new SYN request gives a different sender IP address, the above method does not work.

- **Ping of Death** – A ping packet is normally 64 bytes (or 84 bytes if the header that adds the IP protocol is added). Many types of computers cannot handle ping packets that are larger than 65535 bytes, which is the maximum permitted by IP protocol. As a result, the Ping Of Death attack involves the continuous sending of large ping packets to a computer until the system crash.

In order to counter this attack, it is important to check if packets are valid when assembling the IP packets. This way it is possible to reject IP packets that are larger than allowed and thus avoid the risk of this type of attack.

Application layer attacks this type of attack targets vulnerabilities in software such as Windows, Apache, OpenBSD, etc., to execute the attack and crash the server. The attack magnitude is measured in **Requests per Second**.

- **Application Attack** – also called Layer 7 Attack, is one of the most popular types of attacks targeted at specific application-level vulnerabilities. All that is needed is a small modification to the code and a small tweak to start sending information to hackers. It is extremely hard to recognize Layer 7 assaults since they take after genuine site traffic.
- **Slowloris** – is used to launch the server and carry out a DDoS attack. It sends huge numbers of HTTP requests to the target (webserver). Target keeps all connections open and so there is overflow of concurrent connection.
- **Zero-day DDoS Attacks** – are new type of attacks that exploit vulnerabilities for which no patch has yet been released. Most common example is (exploiting vulnerabilities) on the linux machines.

A **SYN Flood attack** in which the attacker sends multiple SYN (Synchronization) requests to the victim with a spoofed IP address. The TCP protocol requires the following three steps to connect between two computers:

- Sender sends SYN (Synchronize) packet
- The recipient responds with a SYN-ACK (Synchronize Acknowledge) packet
- The sender sends a recent ACK packet and the connection is considered successful.

The attacker sends multiple SYN requests and does not send ACK so the process continues, with the goal of wasting significant computing resources and unable to serve other users.

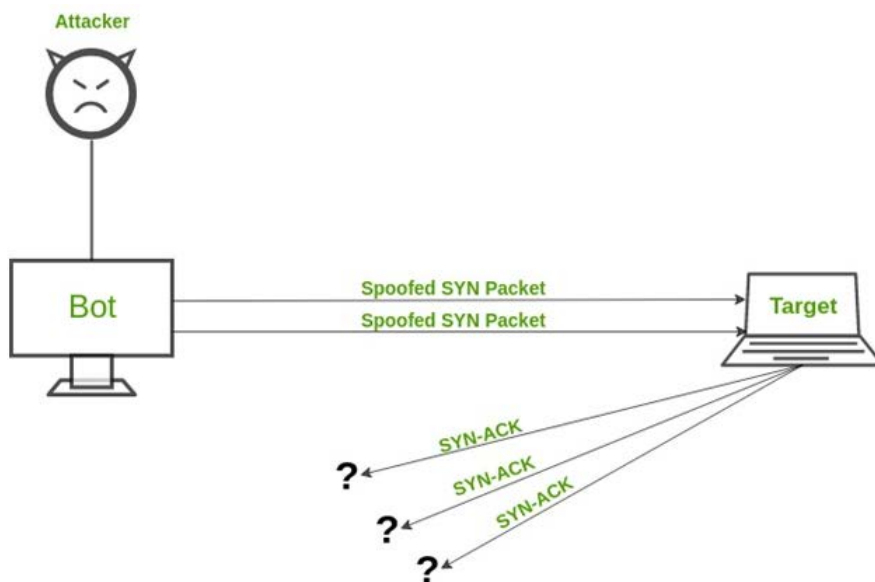


Figure 2.14 Syn flood attack [source](#)

In **HTTP Flood attack** sends multiple HTTP GET or POST requests to attack a web server or application. The attack forces the server or application to devote the maximum resources possible in response to each request.

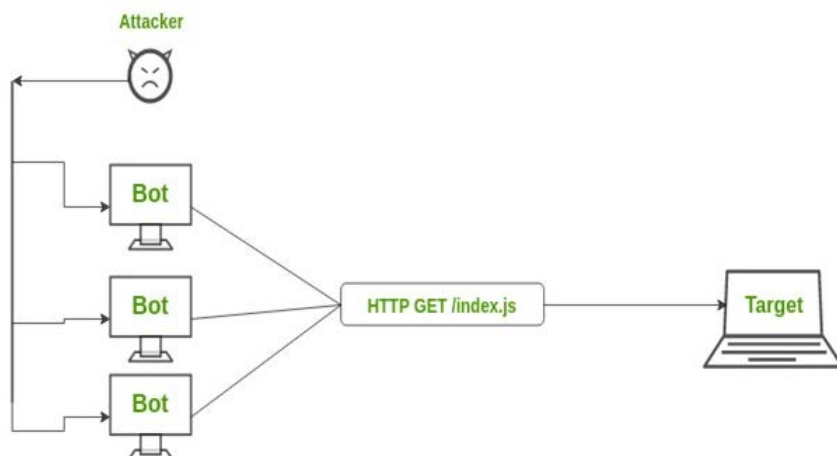


Figure 2.15 Http flood attack [source](#)

These attacks are very popular today and are noted in Layer 3 / 4. They use widely available DNS servers from different parts of the globe to flood your server with DNS response traffic. The server is overloaded with a confusion of responses and has difficulty operating as its resources are reduced, resulting in it not being able to respond properly to normal DNS traffic.

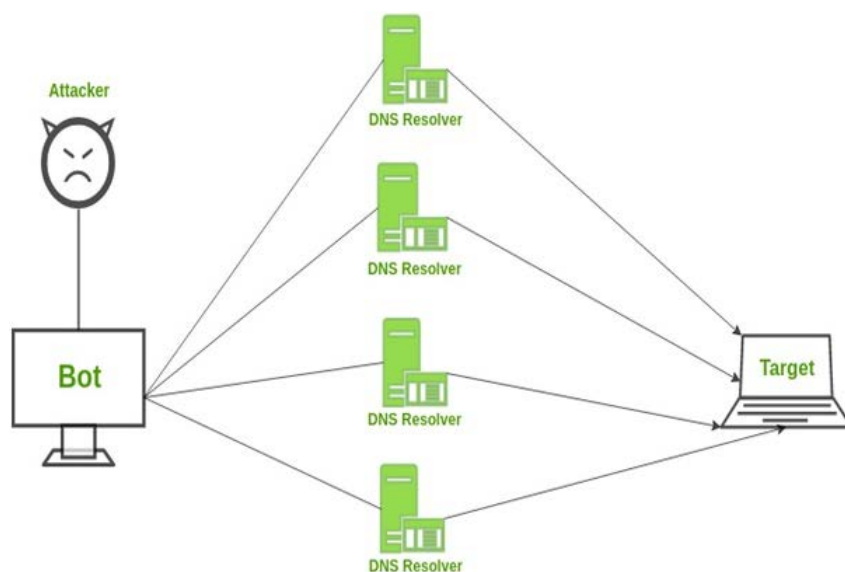


Figure 2.16 DNS flood attack [source](#)

Preventing DDoS attacks **is more difficult than** DoS attacks in light of the fact that the traffic originates from numerous ip addresses (sources) .A portion of the relief systems that can be utilized are:

Some techniques that can be used are:

1. **Blackhole routing**

In blackhole routing, the network traffic is directed to a 'black hole'. In this, both the malicious traffic and non-malicious traffic gets lost in the black hole. This countermeasure is useful when the server is experiencing DDoS attack and all the traffic is diverted for the upkeep of the network.

2. **Rate limiting**

Rate limiting involves controlling the rate of traffic that is sent or received by a network interface. It is efficient in reducing the pace of web scrapers as well as brute-force login efforts. But, just rate limiting is unlikely to prevent compound DDoS attacks.

3. **Blacklisting / whitelisting**

Blacklisting is the mechanism of blocking the IP addresses, URLs, domains names etc. mentioned in the list and allowing traffic from all other sources. On the other hand, whitelisting refers to a mechanism of allowing all the IP addresses, URLs, domain names etc. mentioned in the list and denying all other sources the access to the resources of the network.

An organization can embrace the accompanying strategy to ensure itself against Denial of Service assaults.

- SYN flooding attacks exploit bugs in the operation system(windows,linux,etc..) **Installing security patches** can help decrease the odds of such attacks
- **Intrusion detection systems(IDS)** can be used to monitoring illegal activities
- **Routers** can be configured through Access Control List to restrict the access in the network and drop unlawful traffic.
- **Firewalls** can be utilized to stop a DoS attack by hindering all traffic originating from an attack by recognizing his IP.



Figure 2.17 Dos mitigations [source](#)

Activity:

Suppose we use windows and we have two computers in the same network. DOS attacks are illegal on systems/networks that you are not authorized. This is the reason you should arrangement your own system to do so.

Simply open the windows command prompt(cmd)

We have a victim and we flooding this ip address with 65000 packets.

```

Administrator: C:\Windows\system32\cmd.exe - ping 10.128.131.108 -t -l 65500
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128

```

Figure 2.18 Dos flooding

Attacking on a single host has little effect on the target. To be more effective it needs more computers (DDoS attack).

The attack is often used in web servers, routers etc.

you can check if that attack has effects on the victim. Just open the task manager and click on the networking tab.

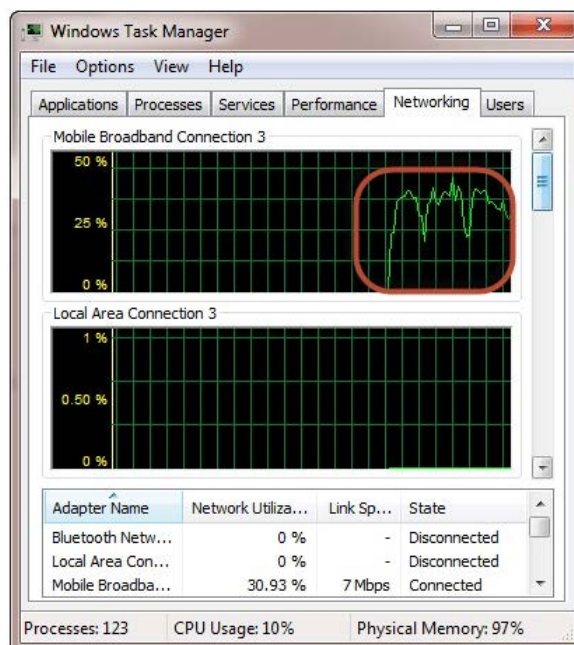


Figure 2.19 Checking network

As we can see the network activity has increased when the attack was successful.

- A DOS attack aim is to deny real clients access to a resource, for example, in a system, server and so forth.
- There are two types of attacks, **DOS** and **DDoS**.
- A DOS attack can be carried out using HTTP flood, DNS flood, SYN flood, Application attack, buffer overflow. etc.
- Updates for operating systems, firewalls, monitoring systems such as IDS (Intrusion detection system) and router/switch configurations, can be used to protect against dos attacks.

A **Man-in-the-Middle (MITM) attack** occurs when a communication between two systems is intercepted by an outside entity. This can happen with in any network or any form of online communication, such as email, social media, web surfing, online banking etc.

The common goal of an attack is to steal personal information, is to gain login credentials, account details and credit card numbers or digital resource.

The ARP protocol

The way the ARP protocol works, is the reason it is open for an MITM attack. So, in order to understand the attack, a basic understanding of this protocol is required.

ARP stands for **Address Resolution Protocol**, which helps a network host make a translation from the IP-address to the MAC-address. This is required in order for data to pass from the OSI model's Network Layer (layer 3) to the Data Link layer (layer 2).

Suppose Machine A needs to transfer data to Machine B. Zooming in to the lower levels of the OSI model, it would need to pass through the Network layer, the Data Link layer and the Physical layer (layer 1). For Machine A to be able to address Machine B, Machine A would need to know the IP address of Machine B?

Information that is known in the Network layer.

The Data Link layer communicates using MAC addresses. So, a conversion needs to take place from the IP address to the MAC address of Machine B (and vice-versa on the recipient machine). This is illustrated in the image below:

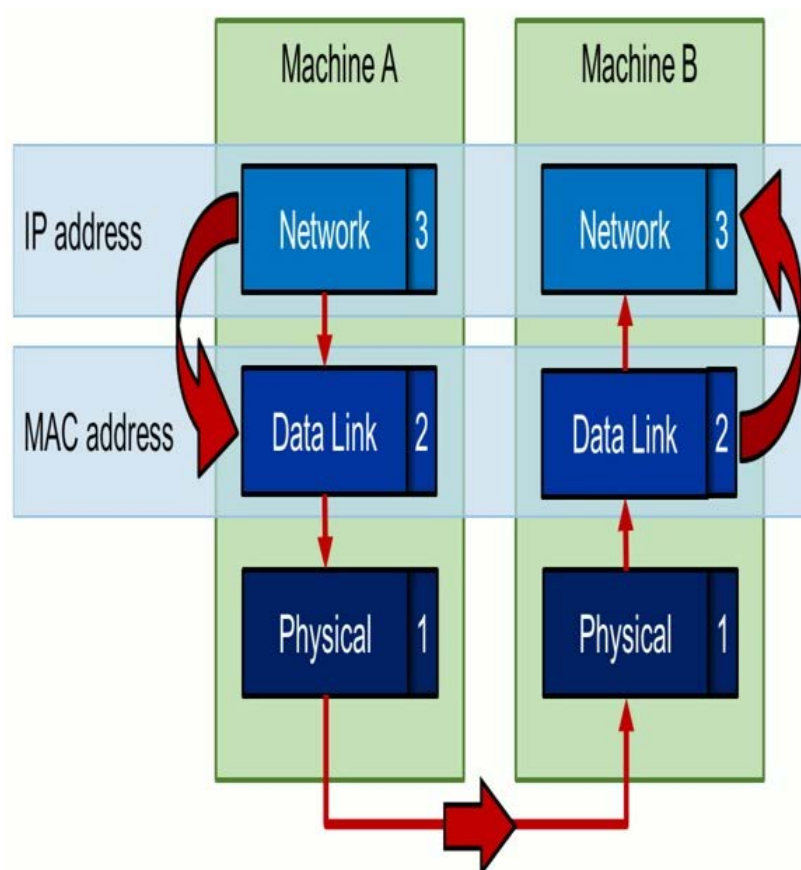


Figure 2.20 OSI model layers 1-3 [source](#)

OSI Model layers 1-3

The conversion from, or rather resolution of, the IP address into MAC address (and the other way around) is where the ARP protocol comes into play. Both machines will have an **ARP table** where the IP- and corresponding MAC-addresses of all known machines are stored. Then how does Machine A get the MAC-address corresponding to the IP Address of Machine B?

Machine A will just ask for it.

A simplification of the ARP protocol is depicted in the animation below:

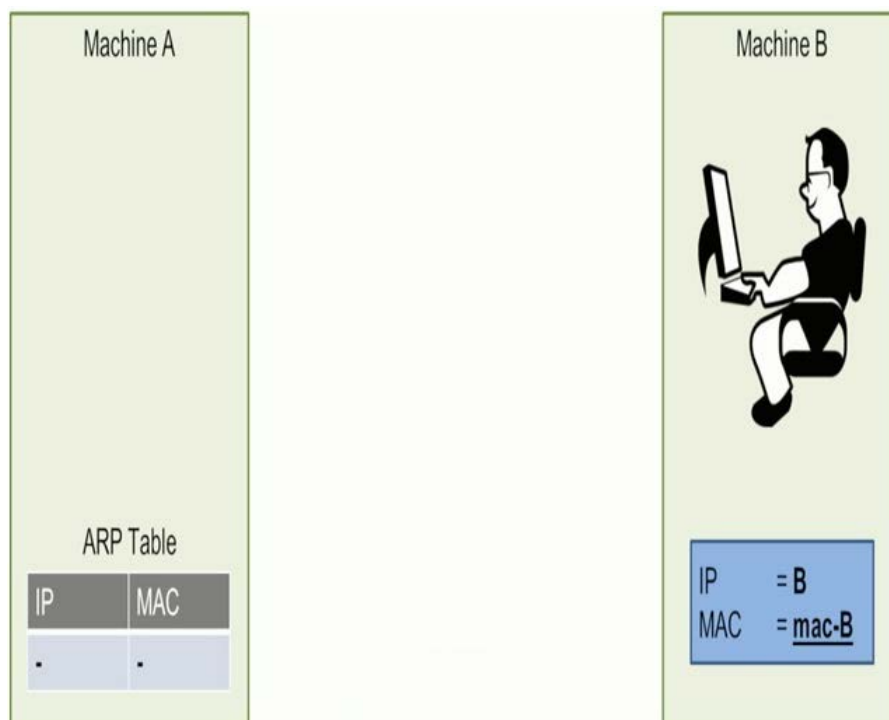


Figure 2.21 Arp protocol [source](#)

The three steps in summary

1. In the first step of the ARP protocol, Machine A sends out an **ARP request**. This is a broadcast to the network with the question "Who has the MAC-address for the IP-address of Machine B?".
2. Machine B has this knowledge and sends an **ARP response** stating "MAC-address B is the MAC-address of Machine B".
3. Machine A receives the ARP response and writes (or updates) the entry in his **ARP table**.

The last step is exactly where the problem with this protocol lies. However, before we dive into its issues, we'll take a look at the ARP packets being transmitted over the network.

The image below displays a part of a network capture made with [Wireshark](#).

No.	Time	Source	Destination	Protocol	Length	Info
7	4.2908...	00:0c:29:13:56:e7	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.1.2? Tell 192.168.1.130
8	4.2908...	00:50:56:ea:01:e7	00:0c:29:13:56:e7	ARP	60	192.168.1.2 is at 00:50:56:ea:01:e7


```

▶ Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: Vmware_13:56:e7 (00:0c:29:13:56:e7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Vmware_13:56:e7 (00:0c:29:13:56:e7)
  Sender IP address: 192.168.1.130
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.2

```

Figure 2.22 ARP network captured traffic [source](#)

We can obviously observe two packets with numbers 7 and 8.

- The first Packet (7) contains the **ARP request** from a computer with source MAC address 00:0c:29:13:56:e7 and with destination MAC address ff:ff:ff:ff:ff:ff, which means a broadcast message. So, the logical is "Who has 192.168.1.2? Tell 192.168.1.130".
- The second Packet (8) is the **ARP response** from a computer with MAC address 00:50:56:ea:01:e7 and with destination MAC address of the original packet 7. Wireshark knows that the ip "192.168.1.2 has mac address 00:50:56:ea:01:e7", which is actually the same MAC-address of the source of this message.

The fact that Machine A updates its ARP table with the info from an ARP response **without any question about the validity of this information**, opens the door for ARP spoofing (also known as **ARP poisoning**).

An attacker might send a malicious ARP response, without any preceding request, containing his own MAC address and the IP address of another machine. The machine to which the response was directed will update its ARP table unquestioningly.

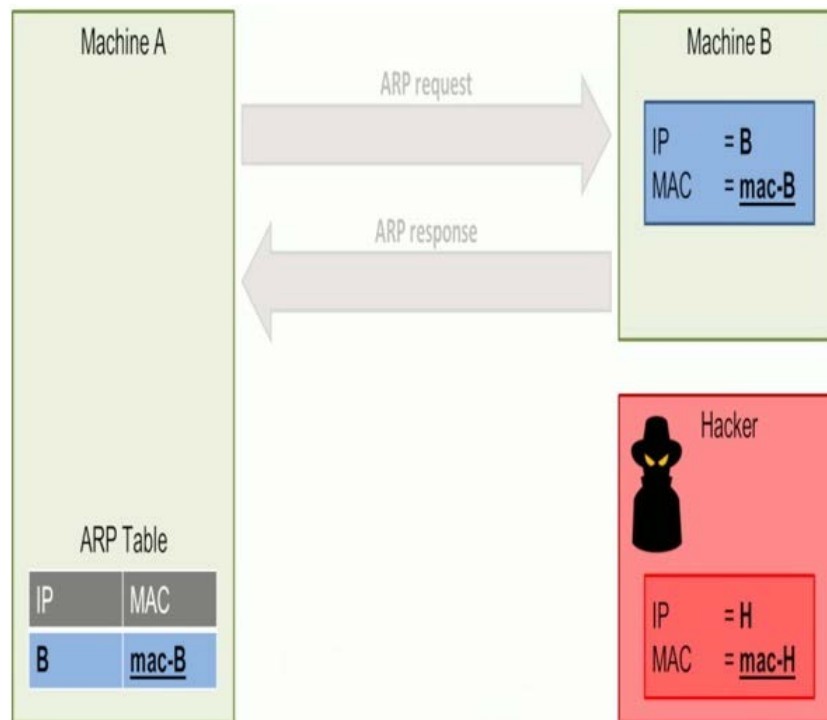


Figure 2.23 Arp spoofing [source](#)

The image above depicts the same scenario as before. However, a hacker has now joined Machine A and B on the network. The hacker has done his work in the reconnaissance and scanning phases, knows Machine A and B exist in the network and what IP addresses they have.

In this example, the hacker himself has IP-address H and MAC-address mac-H. He sends his malicious ARP response directed at Machine A with the message "mac-H is the MAC-address of IP-address B". Machine A updates its ARP table and IP-address B is now linked to MAC-address H.

From now on, every time Machine A wants to send a message to Machine B, it will translate the IP address of Machine B into MAC-address H and be sent to the hacker instead of Machine B.

Man-in-the-middle

We've seen how an attacker can make a machine send its data to him instead of the intended destination by sending a malicious ARP.

Suppose we have the following scenario:

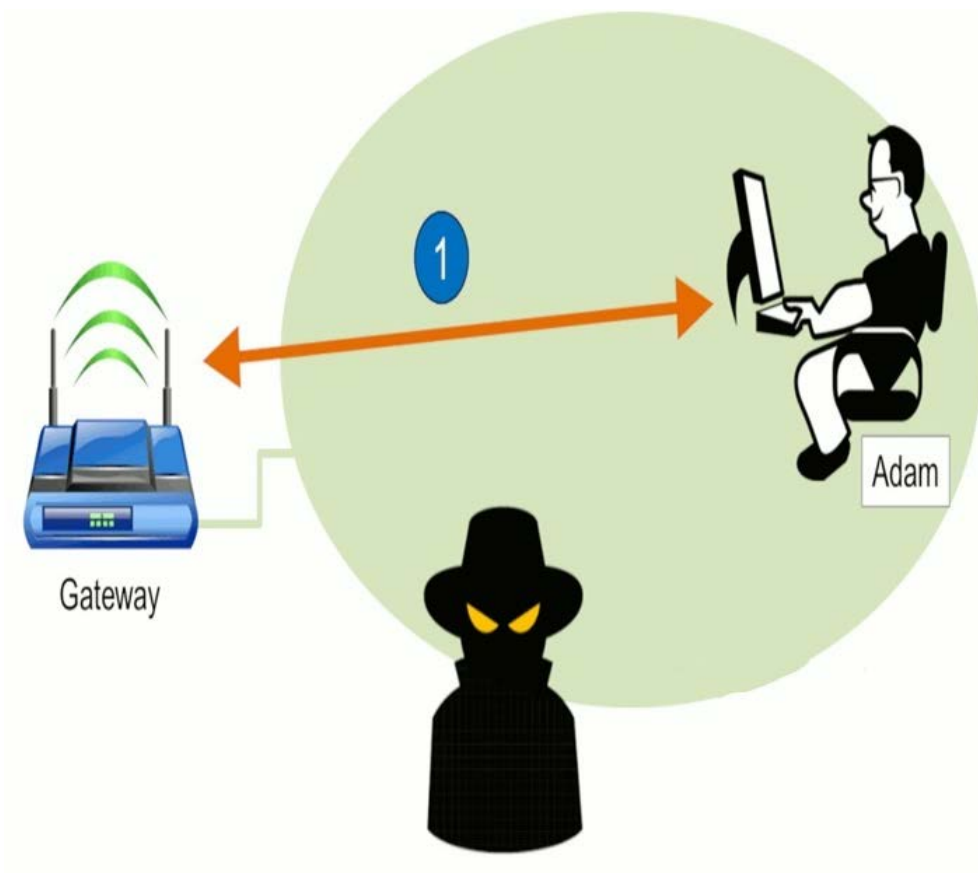


Figure 2.24 Arp spoofing scenario [source](#)

We gave A Gateway, a hacker and Adam.

1. In the first step Adam connected in the network. In this progression, the attacker will do scanning on the network to discover who else is available and what IP-and MAC-addresses he has.
2. Then the hacker sends a malicious ARP response to both(Gateway and Adam). Basically, the hacker tells the Gateway that he is Adam and simultaneously tells Adam that he is the Gateway.
3. Both Gateway and Adam will update their ARP tables with their new information. From then on, these nodes will start to send their data to the hacker instead of each other. ARP spoof completed!

The attacker will need to take some measures before he can properly start intercepting data.

Consider the scenario of the previous sub-chapter where the hacker is in between the Gateway and Adam. The hacker would be able to see all traffic of both parties. For example, if Adam browses to a website, the hacker may see all data sent to and received from the websites he's contacting.

What about **HTTPS**? That's HTTP over **TLS** (or HTTP over SSL). It would mean that all data over the line would be encrypted right? True, and real-time decryption still is not even remotely feasible. So, the hacker would not be able to see the encrypted contents of HTTPS-traffic.

The solution: **force the victim to communicate via HTTP**, which is unencrypted plain text, instead of HTTPS.

Before I explain how this can be done, let's take a look at how an HTTPS-session is setup when you browse to www.google.com (for example):

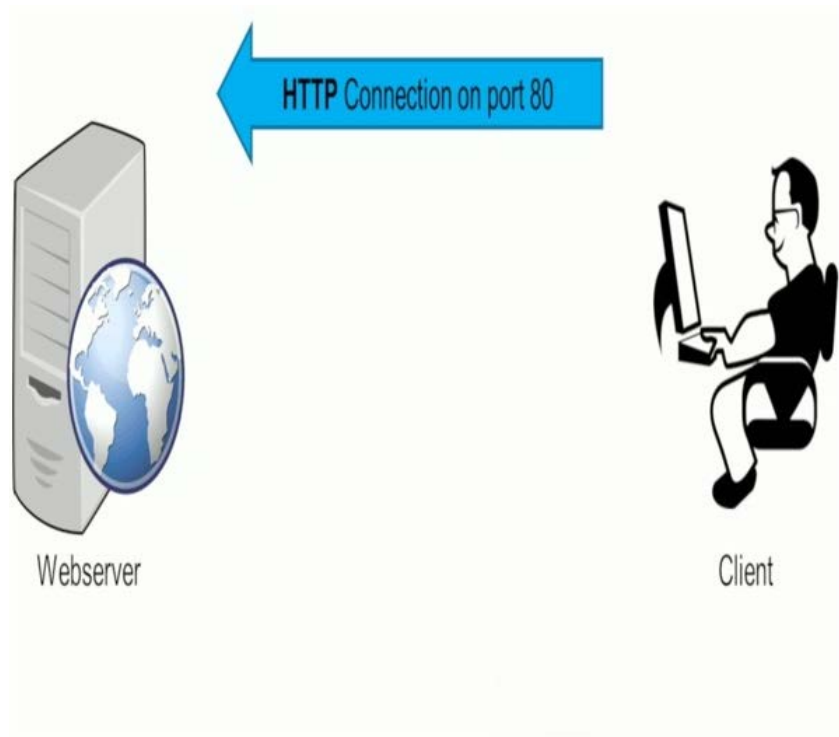


Figure 2.25 An HTTPS session [source](#)

Typing www.google.com in a web browser's address bar will have the browser make an HTTP-connection (on port 80) to www.google.com. Since google.com will only allow HTTPS-connections, the site will request the user to make an HTTPS-connection instead then the client using HTTPS on port 443 reconnect back. In the last step google sends the certificate.

Consider the scenario where a hacker is somewhere in between the communication of web server and the client. The hacker would be able to read the contents of the web traffic until the moment the client sets up the HTTPS-connection. After this all data will be encrypted and no longer readable by the hacker. Earlier we stated that this might be circumvented by forcing the client to keep communicating via HTTP. SSLStrip is the tool we will use to achieve this.

[SSLStrip](#), created by Moxie Marlinspike, will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links. Let's take a look at the HTTPS session setup when the hacker uses SSLStrip in between the client and the web server.

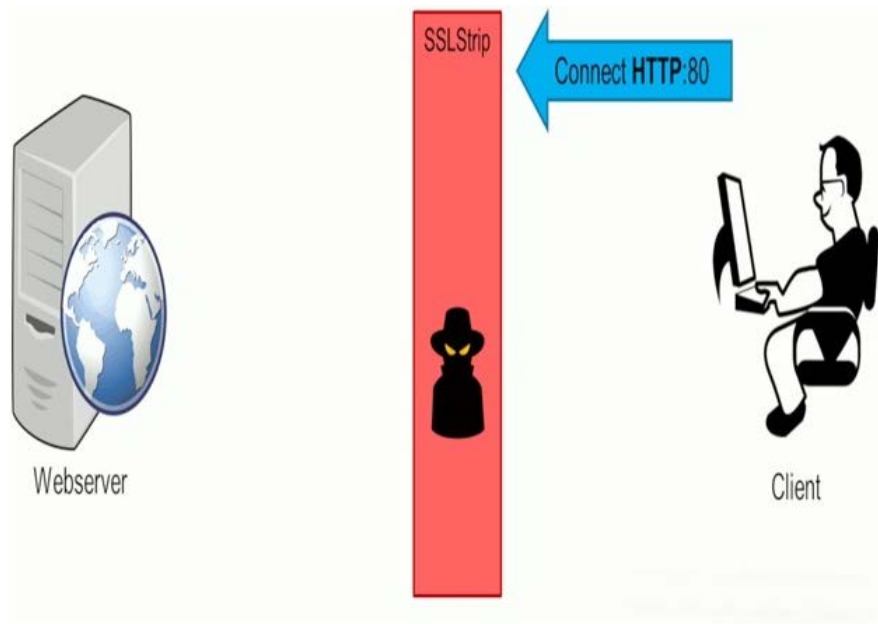


Figure 2.26: SSLStrip [source](#)

Like before, the client types www.google.com in the web browser, which will attempt to setup an HTTP connection with the website. Now with SSL Strip in the middle, this connection is forwarded to the intended destination. However, instead of the entire HTTPS-redirect-dance to be performed on the client's side, SSL Strip takes care of this on the hacker's machine. After the HTTPS-connection was setup, SSL Strip will return an **HTTP-OK** to the client. The client's browser thinks this is acceptable since it never saw the HTTPS-redirect and will continue to communicate via HTTP; a format the hacker can read effortlessly.

HTTP strict transport Security

Having HTTP strict transport security ([HSTS](#)) enabled for your website will inform the browser to always communicate using HTTPS. It does this via a special HSTS response header. Simply put, the browser maintains a list of websites from which it received this header. For these websites, the browser will immediately make an HTTPS-connection regardless of how the user attempted to connect. Typing www.google.com will not result in the HTTP-HTTPS-redirect-dance, but immediately call www.google.com. This will prevent users from making the HTTP-connection in the first place, avoiding SSLStrip to perform this trick. That is, if your browser [supports](#) it.

The first ever visit of a client to a website may still be done via HTTP and an attacker can strip the HSTS header from the response. This is why most modern browsers have a pre-loaded list of HSTS sites. More on prevention in the final chapter.

A **dictionary attack** is a password attack that attempts to determine a password by trying words from a predefined list, or dictionary, of likely passwords

A dictionary attack is the simplest and fastest password cracking attack. Use a file containing common words, phrases, or passwords that may have been used by someone as a password. Hackers have access to databases that have 100,000 (or more) top passwords or they can create and find larger files. The attack hashing on these passwords and compares the hash with the password it wants to crack. This is a faster method than others.

```
Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-04 07:24:27
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password" - 2 of 12 [child 1]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_1" - 5 of 12 [child 4]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password" - 6 of 12 [child 5]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_2" - 8 of 12 [child 7]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_2" - 12 of 12 [child 11]
[ ] [ ] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-09-04 07:24:36
david@lab:~$
```

Figure 2.27: A dictionary attack

Phishing

Phishing is an example of social engineering approach used to obtain sensitive user information (personal identifying data) typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information. that will be used to deceive systems. Phishing attempts most often begin with an email attempting to obtain sensitive information through some user interaction, such as clicking on a malicious link or downloading an infected attachment.

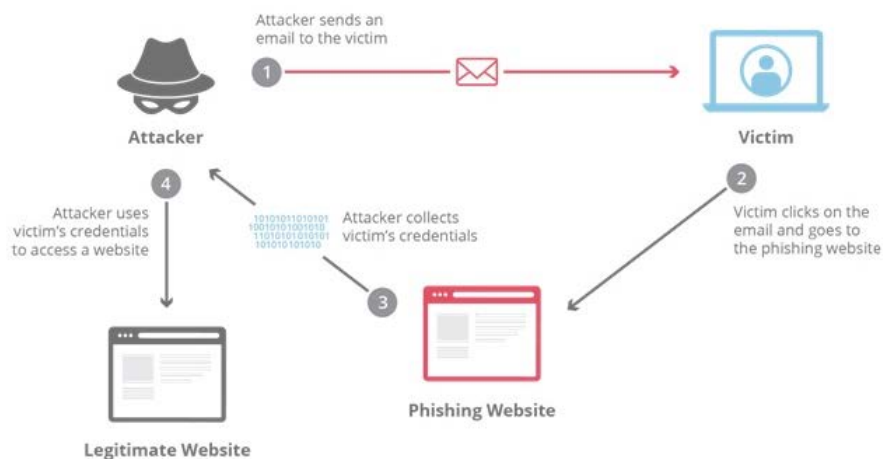


Figure 2.28 phishing attack [source](#)

In order to counter phishing attacks, organizations and companies must provide employees with ways to identify these attacks and countermeasures these attacks. The most common of phishing attacks are emails, virus attachment files, and virus links that lead to viruses and drop off connection bandwidth. Attackers are constantly updated about new attacks, so you need to provide the knowledge in the employees to avoid such attacks.

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as **MySQL, Oracle, SQL Server, or others**. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can **modify** or **delete** this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

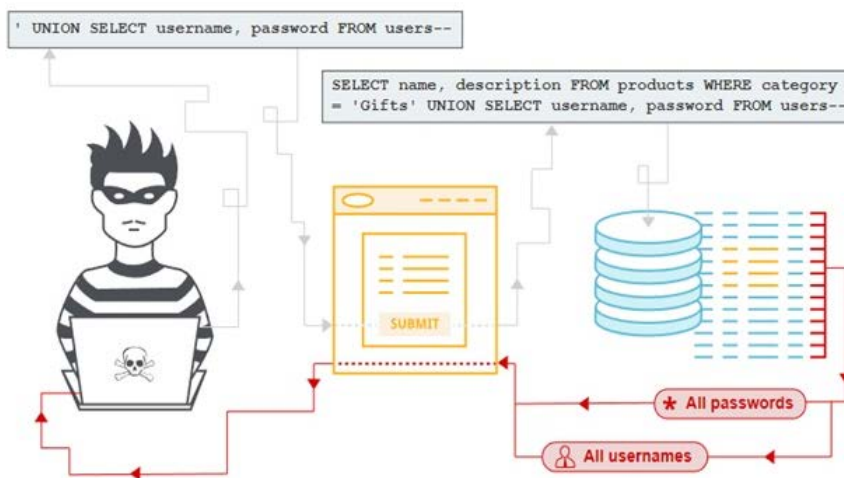


Figure 2.29 SQL injection [source](#)

Database-specific factors

Some core features of the SQL language are implemented in the same way across popular database platforms, and so many ways of detecting and exploiting SQL injection vulnerabilities work identically on different types of database.

However, there are also many differences between common databases. These mean that some techniques for detecting and exploiting SQL injection work differently on different platforms

What Can SQL Injection Attacks Do?

There are a lot of things an attacker can do when exploiting an SQL injection on a vulnerable website. By leveraging an SQL injection vulnerability, given the right circumstances, an attacker can do the following things:

- Bypass a web application's authorization mechanisms and extract sensitive information
- Easily control application behavior that's based on data in the database
- Inject further malicious code to be executed when users access the application
- Add, modify, and delete data, corrupting the database, and making the application or unusable
- Enumerate the authentication details of a user registered on a website and use the data in attacks on other sites.



Figure 2.30 Sql injection attacks [source](#)

The following things might result from SQL injection:

- Hacking other person's account.
- Stealing and copying website's or system's sensitive data.
- Changing system's sensitive data.
- Deleting system's sensitive data.
- The user could log in to the application as another user, even as an administrator.
- The user could view private information belonging to other users e.g. details of other users' profiles, their transaction details etc.
- The user could change application configuration information and the data of the other users.
- The user could modify the structure of the database even delete tables in the application database.
- The user could take control of the database server and execute commands on it at will.



Figure 2.31 SQL prevention [source](#)

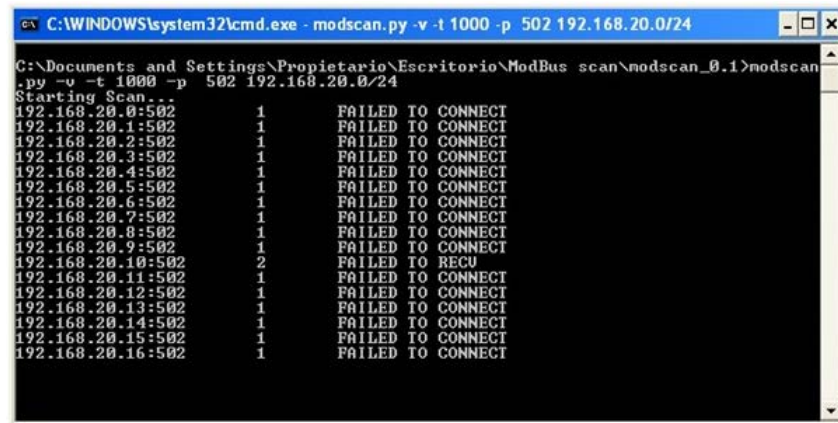
There are several ways to deal with SQL injection attacks so you are better prepared and avoid the potential damage you may suffer. Some ways are:

- Discover SQL injection vulnerabilities with the various techniques available for this attack
- Repair SQL injection vulnerabilities by utilizing parameterized queries. The database will always treat them as data rather than part of a SQL command.
- Remediate SQL injection vulnerabilities by using escape characters so that special characters are ignored.
- Mitigate the impact of SQL injection vulnerabilities by enforcing least privilege on the database, this way each software component of an application can access and affect only the resources it needs.
- Use a **Web Application Firewall (WAF)** for web applications that access databases. This can help identify SQL injection attempts and sometimes help prevent SQL injection attempts from reaching the application as well.

Modbus is a very widespread industrial communications protocol with a publicly available specification, based on a master/slave architecture. There are currently no extensive restrictions on the time at which data blocks can be managed in an industrial system; implementing this would be straightforward, and would require little development. There are currently two implementations: Modbus series (with ASCII and RTU operating modes) and Modbus/TCP.

Protocol weaknesses

In Modbus, the slave elements' operation mode consists of always responding to the packets they receive. The [Modscan](#) tool takes advantage of this feature, directing TCP requests (therefore only available for Modbus/TCP implementations) to the standard Modbus port, 502, and thereby discovering the slaves connected to the network, as can be seen in the image below.

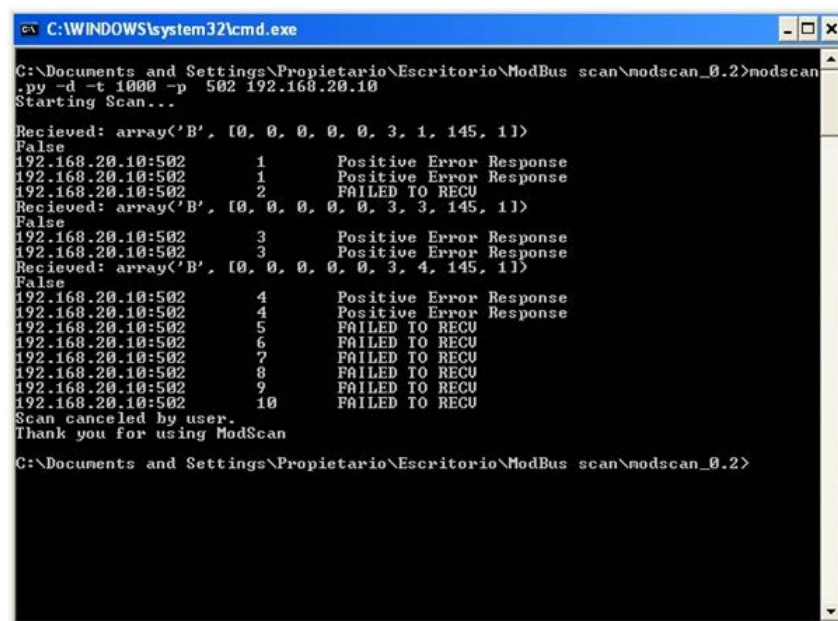


```

C:\WINDOWS\system32\cmd.exe - modscan.py -v -t 1000 -p 502 192.168.20.0/24
C:\Documents and Settings\Propietario\Escritorio\ModBus scan\nodscan_0.1>modscan
.py -v -t 1000 -p 502 192.168.20.0/24
Starting Scan...
192.168.20.0:502 1 FAILED TO CONNECT
192.168.20.1:502 1 FAILED TO CONNECT
192.168.20.2:502 1 FAILED TO CONNECT
192.168.20.3:502 1 FAILED TO CONNECT
192.168.20.4:502 1 FAILED TO CONNECT
192.168.20.5:502 1 FAILED TO CONNECT
192.168.20.6:502 1 FAILED TO CONNECT
192.168.20.7:502 1 FAILED TO CONNECT
192.168.20.8:502 1 FAILED TO CONNECT
192.168.20.9:502 1 FAILED TO CONNECT
192.168.20.10:502 2 FAILED TO RECU
192.168.20.11:502 1 FAILED TO CONNECT
192.168.20.12:502 1 FAILED TO CONNECT
192.168.20.13:502 1 FAILED TO CONNECT
192.168.20.14:502 1 FAILED TO CONNECT
192.168.20.15:502 1 FAILED TO CONNECT
192.168.20.16:502 1 FAILED TO CONNECT

```

Figure 2.32 Discovering the Modbus slaves' IPs with Modscan



```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Propietario\Escritorio\ModBus scan\nodscan_0.2>modscan
.py -d -t 1000 -p 502 192.168.20.10
Starting Scan...
Received: array('B', [0, 0, 0, 0, 0, 3, 1, 145, 1])
False
192.168.20.10:502 1 Positive Error Response
192.168.20.10:502 1 Positive Error Response
192.168.20.10:502 2 FAILED TO RECU
Received: array('B', [0, 0, 0, 0, 0, 3, 3, 145, 1])
False
192.168.20.10:502 3 Positive Error Response
192.168.20.10:502 3 Positive Error Response
Received: array('B', [0, 0, 0, 0, 0, 3, 4, 145, 1])
False
192.168.20.10:502 4 Positive Error Response
192.168.20.10:502 4 Positive Error Response
192.168.20.10:502 5 FAILED TO RECU
192.168.20.10:502 6 FAILED TO RECU
192.168.20.10:502 7 FAILED TO RECU
192.168.20.10:502 8 FAILED TO RECU
192.168.20.10:502 9 FAILED TO RECU
192.168.20.10:502 10 FAILED TO RECU
Scan canceled by user.
Thank you for using ModScan
C:\Documents and Settings\Propietario\Escritorio\ModBus scan\nodscan_0.2>

```

Figure 2.33 Fine tuning the search for slaves and the identification of Modbus IDs

Once the slaves have been identified, it is easy to capture traffic with any tool designed for capturing network traffic. Capture analysis shows that communications are not encrypted, which means it is possible to identify and directly analyze the information given and the operation mode. The following image shows a traffic capture with an analysis of the stream.

The screenshot displays a Wireshark capture of Modbus traffic. The main pane shows a list of packets with columns for No., Time, Source, Destination, Proto., Length, and Info. Packet 16 is selected and expanded to show the following details:

- Frame 16: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
- Ethernet II, Src: vmware_f7:85:cb (00:0c:29:f7:85:cb), Dst: vmware_af:a3:89 (00:0c:29:af:a3:89)
- Internet Protocol version 4, Src: 192.168.10.20 (192.168.10.20), Dst: 192.168.10.10 (192.168.10.10)
- Transmission Control Protocol, Src Port: 502 (502), Dst Port: 1031 (1031), Seq: 88, Ack: 49, Len: 29
- Modbus/TCP
 - Function Code: Read Holding Registers (3)
 - Byte Count: 20
 - Register 0 (UINT16): 45
 - Register 1 (UINT16): 83
 - Register 2 (UINT16): 45
 - Register 3 (UINT16): 500
 - Register 4 (UINT16): 83
 - Register 5 (UINT16): 45
 - Register 6 (UINT16): 4457
 - Register 7 (UINT16): 65532
 - Register 8 (UINT16): 457
 - Register 9 (UINT16): 245

The bottom pane shows the raw packet data in hexadecimal and ASCII format:

```

0000 00 0c 29 af a3 89 00 0c 29 f7 85 cb 06 00 45 00  ..J....}....E.
0010 00 43 00 00 00 80 06 64 ff c9 a8 0a 14 c9 a8  ..A...@.....
0020 0a 0a 01 f6 04 07 62 06 39 01 f0 87 cc bd 50 18  ..A.A...P.....
0030 f9 84 07 0a 00 00 00 96 00 00 00 17 01 03 14 00  ..P.....
0040 2d 00 51 00 2d 00 f4 00 59 00 2d 18 69 7c 01  ..-...M.....
0050 c9 00 f5
  
```

Figure 2.34 Analyze traffic

Modbus' **weaknesses are rooted in its specification**, meaning that they are intrinsic to the protocol; as no changes to the specification are anticipated, it is therefore necessary to introduce additional security elements, to help mitigate its security failings.

Moving on from this option, which is the most simple, the first measure to consider is the adoption of an encryption strategy for communications. **Communications encryption** will prevent information from being analysed in transit, in case the traffic is captured.

Devices which implement this protocol are not generally able to encrypt communications, and they must therefore use external tools, which can encrypt and decrypt the information running through the Ethernet cable.

Although this solution is effective, it is **difficult in practice**, as using encryption tools brings problems of management and password distribution; in addition, information encryption and decryption must be permitted by all industrial equipment to be used to by Modbus protocol.

Therefore, in order to control the traffic between slaves and the master, **firewalls are the most popular solution**. Conventional firewalls allow for traffic control at network level, meaning that the master and slaves' addresses can be established as authorities, thereby preventing certain kinds of impersonation attacks. Application firewalls allow for inspection, including for the data section of the stream.

There is [Modbusfw](#), a module for [iptables](#) which filters traffic at the level of application layer to secure networks using the Modbus/TCP protocol. It allows for the **filtering of Modbus traffic packets**, identifying them using the slave's ID, the function code, the packet size or the reference number. In this way, it is possible to avoid writing on equipment that should only receive readings or vice versa, and to filter the use of diagnostic function codes (such as those used in certain Modbus network scan tools), etc.

Firewalls permit traffic control in different networks, but it is useful to use them in conjunction with **intrusion detection and prevention systems** (IDS/IPS) in order to detect other kinds of actions.

For the Snort IDS, and for all those based in it, there is an extension for interpreting the Modbus protocol. It is possible to define traffic control regulations for Modbus based on values that must contain different data bytes in one Modbus/TCP stream.

Using IDS/IPS systems to supervise the Modbus protocol allows the use of non-permitted functions to be recognized, as well as recognizing when data packets are sent from non-controlled IP addresses, helping, for example, to detect potential DoS attacks.

2.4 Information Society Law of Services and Electronic Commerce

Description

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

- In order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.
- The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

The official and complete law:

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>

Table of contents

1. Information Society Law of Services and Electronic Commerce

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular **electronic commerce**, in the Internal Market (Directive on electronic commerce).

Some paragraphs of the law:

- In order to ensure legal certainty and consumer confidence, this Directive lays down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.
- The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

Information Society Services Purpose of Act

(1) This Act provides the requirements for information society service providers, the organisation of supervision and liability for violation of this Act.

more information about the law

<http://unpan1.un.org/intradoc/groups/public/documents/un-kmb/unpan041622~1.htm>

E-commerce - standard EU rules

<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=LEGISSUM%3A124204>

The Electronic Commerce Directive (e-Commerce Directive 2000/31/EC), adopted in 2000, sets up an Internal Market framework for electronic commerce, which provides legal certainty for business and consumers alike.

Aim of the E-Commerce Directive

The Directive was introduced to clarify and harmonise the rules of online business throughout Europe. The aim of the Directive is to ultimately encourage greater use of e-commerce by tearing down barriers that exist across Europe and to boost consumer confidence by clarifying the rights and obligations of both consumers and businesses.

Scope of the Electronic Commerce (EC Directive) Regulations 2002

The Electronic Commerce (EC Directive) Regulations 2002 which came into force on 21st August 2002 transpose the main requirements of the E-Commerce Directive into UK law.

The Regulations apply to "information society services". "These are defined as any service normally provided for remuneration at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, at the individual request of a recipient of a service"

This includes most types of online and information services such as:

- Advertisement of goods or services online (i.e. Via internet, email, interactive television, or mobile telephone)
- Sale of goods or services on the internet or by email, irrespective of whether the goods or services are delivered electronically
- Transmitting or storing electronic content or providing access to a communications network

The official and complete law:

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>

European Union's recommendations for combating cyberattacks, the following guidelines apply:

- **ENISA study on "INDUSTRY 4.0 CYBERSECURITY: CHALLENGES & RECOMMENDATIONS, May 2019"**: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport

The appropriation of the significant level proposals proposed by ENISA aims at the improvement of Industry 4.0 cybersecurity over the European Union and at laying the foundations of the relevant forthcoming work, as well as at serving as a basis for future developments. In this short paper, ENISA pursues an holistic and extensive way to deal with the issues identified with cybersecurity in Industry 4.0, whereby difficulties and proposals are related with one of the accompanying classes: People, Processes, and Technologies.

- **This paper aims on "Cybersecurity Guidelines and Best Practices for Emergency Services, June 2018"**: <https://eena.org/wp-content/uploads/2018/11/Cybersecurity-Guidelines-and-Best-Practices-for-Emergency-Services.pdf>

This paper by EENA (European Emergency Number Association) expects to expand mindfulness among Public Safety associations about the effects identified to cyber vulnerabilities, risks, and threats and gives a few suggestions for mitigation. Cybersecurity, for the purposes of this document, refers to the technologies, processes and practices designed to protect users, networks, computers, programs and data from attack, damage or unauthorized access.

- **ISACA, "Cyber security audit"**: https://m.isaca.org/About-ISACA/advocacy/Documents/CyberSecurityAudit_mis_Eng_1017.pdf

This guide focuses on three parts, management review, risk assessments and audits of the cyber security controls. Also, includes primary security and control issues for cyber security, controls and threats for cybersecurity.

- **This ENISA study aims on "Good Practices for Security of Internet of Things in the context of Smart Manufacturing, Nov 2018"**: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport

This ENISA study aims at addressing the security and privacy challenges related to the evolution of industrial systems and services precipitated by the introduction of IoT innovations. The main objectives were to collect good practices to ensure security of IoT in the context of Industry 4.0/Smart Manufacturing, while mapping the relevant security and privacy challenges, threats, risks and attack scenarios.

- **NIST Internal Report 8228 (Draft) "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks at, Sep 2019"**: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf>

The purpose of this paper is to assist corporations better apprehend and manipulate the cybersecurity and privateness dangers associated with Internet of Things (IoT) devices during their lifecycles. Also, the text says about Cybersecurity and Privacy Risk Considerations and for challenges about Cybersecurity and Privacy Risk Mitigation for IoT Devices.

- **Department for Digital, Culture, Media & Sport "Code of Practice for Consumer IoT Security, Oct 2018"**: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

The Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home.

Practical Examples

SQL Injection

There are automated tools that you can use to check a website if it is vulnerable.

These tools include:

- **SQLMap**
- **Havij**

A demo link to practice on it.

<http://testphp.vulnweb.com/artists.php?artist=1>

The first thing we do is to put a simple quote at the end of the url.

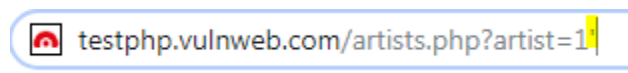


Figure 1 Checking for SQL Injection

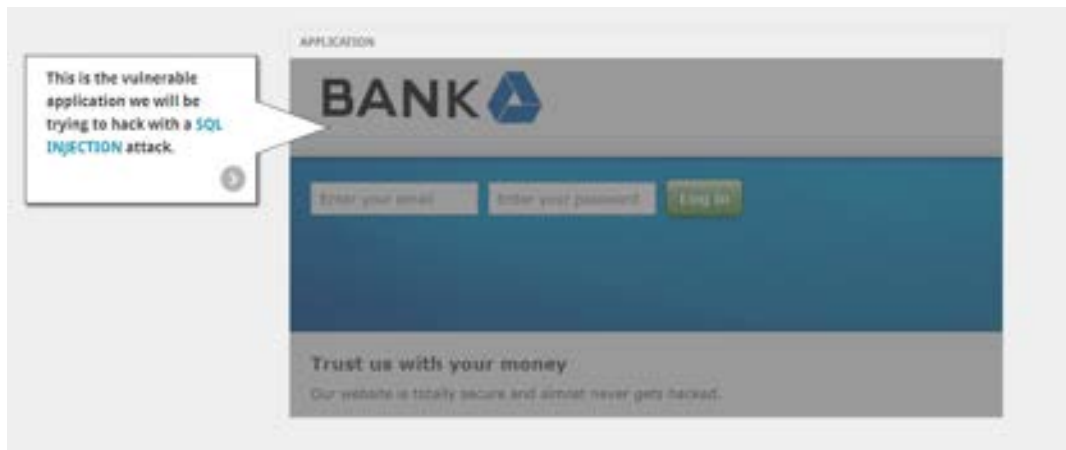
and we get the error.

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62
```

Therefore, we realize that the site is vulnerable to SQL Injection attacks.

Detailed demo to understand the attack better.

[SQL demo](#)



Dictionary attack

A dictionary attack is the simple and fast password attack.

Attackers can create their own made dictionaries with passwords or download existing ones.

Creating word list with Crunch - Kali linux

```
root@kali:~# crunch 6 8 1234567890 -o /root/numericwordlist.lst
Crunch will now generate the following amount of data: 987000000 bytes
941 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 111000000
```

Figure 2 Example

Where the first number (6) is the shortest word length and the second (8) is the longest word length and the characters are from 0-9.

What command do we need for lowercase characters a-z?

ANSWER: `crunch 6 8 abcdefghijklmnopqrstuvwxyz -o /root/loweralpha.lst`

An example of cracking sshservice(port 22)

```
C:\hydra>hydra -l root -P sshcrack.txt 192.168.1.31 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-09 14:12:
18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:0), ~7 tr
y per task
[DATA] attacking ssh://192.168.1.31:22/
[22][ssh] host: 192.168.1.31 login: root password: toor
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-09 14:12:
20
```

Figure 3 SSH cracking from windows

```
Hydra (http://www.thc.org/thc-hydra) starting at 2019-12-09 12:16:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:0), ~7 tries per task
[DATA] attacking ssh://192.168.1.31:22/
[22][ssh] host: 192.168.1.31  login: root  password: toor
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-09 12:16:55
```

Figure 4 SSH cracking from Linux

Try to do the same using a ready-made wordlist called "rockyou"! ([Rockyou download link](#))

Basic Reminders!

1) Strong passwords

Our password should be at least 12 characters long (at minimum), with the combination of the letters, numbers, and special symbols. Some letters should be uppercase and some in lowercase.

2) Unique password

You should have a unique password for different accounts. Never use the one same password for all your accounts.

3) Kaleidoscopic password

Your password should be updated at least every three months. Never reuse your old passwords.

DOS Attack

DOS Attack: A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols.

```
root@kali:~# hping3 -i u1 -S -p 80 192.168.1.2
HPING 192.168.1.2 (eth0 192.168.1.2): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.2 ttl=128 DF id=32344 sport=80 flags=SA seq=0 win=8192 rtt=28.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32345 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32346 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32347 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32348 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32349 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32350 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32351 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32352 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32354 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
len=46 ip=192.168.1.2 ttl=128 DF id=32355 sport=80 flags=SA seq=0 win=8192 rtt=0.0 ms
```

Figure 5 hping3 in action

where :i — interval wait,— u1- 1 microsecond -S — Syn packet -p — port number

We've attacked our local network

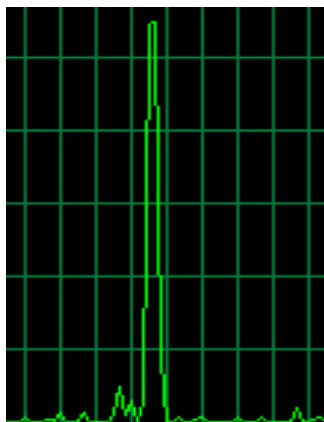


Figure 6 Network attack in practice after 15-20 second

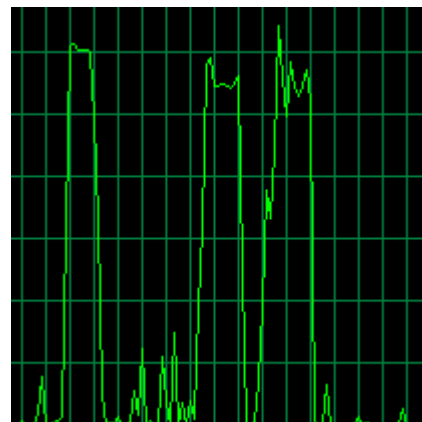


Figure 7 After 1-2 minutes

As we can see the network activity has increased significantly when the attack was successful.

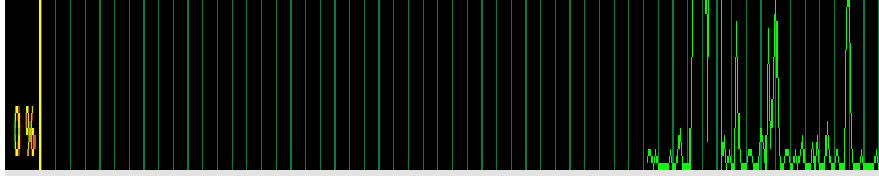


Figure 8 Normal network flow

No.	Time	Source	Destination	Protocol	Length	Info
3635...	10.305082	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5758 → 80 [SYN] Seq=0 Win=512 Len=0
3635...	10.305087	192.168.1.2	192.168.1.31	TCP	58	80 → 5758 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635...	10.305119	192.168.1.31	192.168.1.2	TCP	60	5758 → 80 [RST] Seq=1 Win=0 Len=0
3635...	10.305147	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5759 → 80 [SYN] Seq=0 Win=512 Len=0
3635...	10.305152	192.168.1.2	192.168.1.31	TCP	58	80 → 5759 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635...	10.305184	192.168.1.31	192.168.1.2	TCP	60	5759 → 80 [RST] Seq=1 Win=0 Len=0
3635...	10.305223	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5760 → 80 [SYN] Seq=0 Win=512 Len=0
3635...	10.305229	192.168.1.2	192.168.1.31	TCP	58	80 → 5760 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635...	10.305261	192.168.1.31	192.168.1.2	TCP	60	5760 → 80 [RST] Seq=1 Win=0 Len=0
3635...	10.305289	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5761 → 80 [SYN] Seq=0 Win=512 Len=0
3635...	10.305294	192.168.1.2	192.168.1.31	TCP	58	80 → 5761 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635...	10.305326	192.168.1.31	192.168.1.2	TCP	60	5761 → 80 [RST] Seq=1 Win=0 Len=0
3635...	10.305354	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5762 → 80 [SYN] Seq=0 Win=512 Len=0
3635...	10.305360	192.168.1.2	192.168.1.31	TCP	58	80 → 5762 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635...	10.305390	192.168.1.31	192.168.1.2	TCP	60	5762 → 80 [RST] Seq=1 Win=0 Len=0

Figure 9 Wireshark captured the attacked packets

It can be clearly seen that our machine is sending SYN packets(Dos attack) continuously to the target machine.

Phishing email

In general, phishing is when someone trying to stole personal information online from you in various ways. It is usually done via email and the real sender is not what it seems.

Let's look at a real example

Classic phishing email

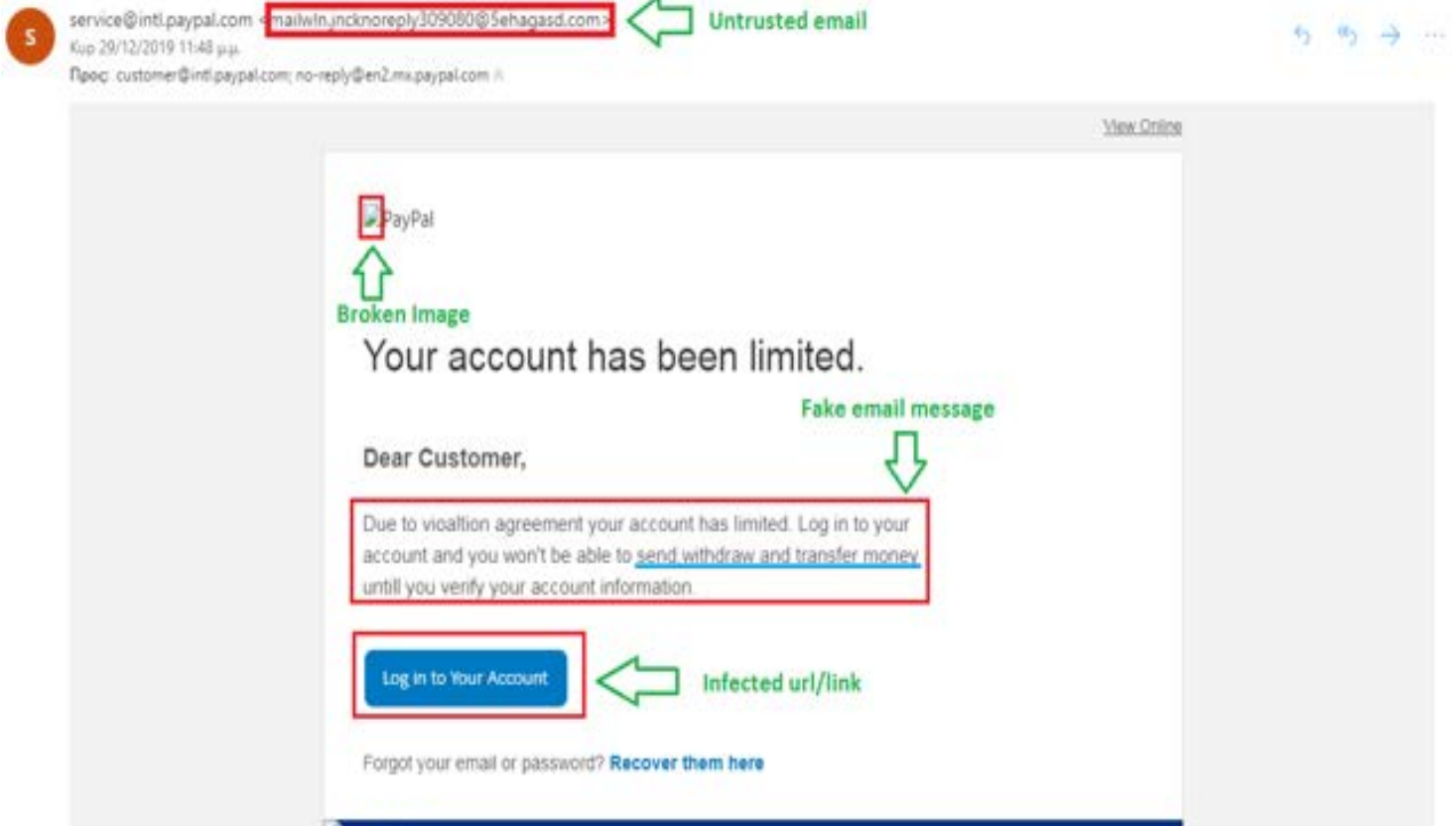


Figure 10 Fakepaypal phishing email example

There are also other categories of email phishing.

The basics are:

- Infected Attachments(.JS, .DOC, .HTML file extensions).
- Macros with Payloads in word documents.
- Social Media exploits to install malicious browser extensions.
- LinkedIn Phishing Attacks (to stole credentials of the user).

A good online demo to understand if an email is real or not(phishing) is the following:

[Phishing demo](#)



Co-funded by the
Erasmus+ Programme
of the European Union



MODULE 3

Confidentiality, integrity, and availability in industrial environments

3.1 Availability

Description

Table of contents

- 1. Business Continuity**
- 2. Degree of Availability**
- 3. Fault Tolerance**
- 4. Fault Avoidance**
- 5. Fault Detection**
- 6. Business Continuity Plan**
- 7. Risk Assessment**
- 8. Disaster Recovery**
- 9. Contingency plan**
- 10. Security policy**

Business continuity is dependent on many factors. In the field of systems administration, it is imperative to be concerned about the impact that technology infrastructure has on the business.

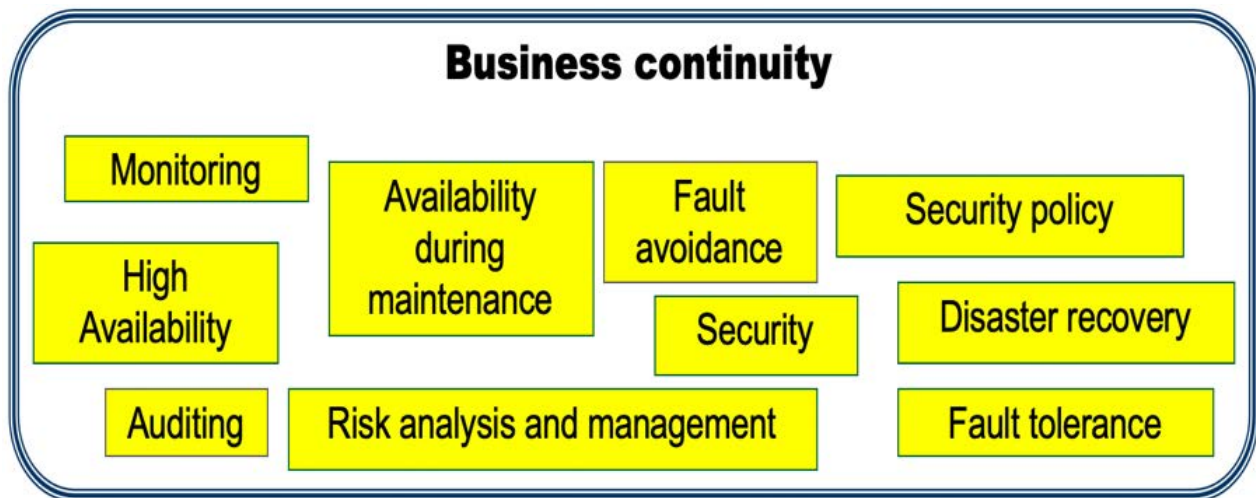


Figure 3.1. Business continuity

The technological infrastructure must ensure business continuity running without interruption within the **parameters** predicted for the business supported by this infrastructure.

It is considered a **secure system (secure technological infrastructure)** the one that is kept in operation within the expected qualitative and quantitative parameters (**SLA** - Service Level Agreement). Any deviation in these parameters is considered a failure.

These parameters involve the triad of computer security: **Confidentiality, Integrity and Availability**.

Planning a secure system that ensures business continuity involves weighing **costs** and **benefits** in order to **obtain an acceptable probability of failure**.

There are no fully secure systems to the point where there are total guarantees that a failure never occurs (0% probability of failure).

Although the probability of failure is a useful data, MTBF - Mean Time Between Failures is commonly used, which indicates the average time elapsed between failures, usually expressed in hours.

The availability of a system is the ratio between the sum of the time periods in which the system operates without fail and the total time considered (usually one year, or one month).

$$\textit{Availability} = \frac{\textit{Operation time without failures}}{\textit{Total time}}$$

Figure 3.2. Availability

Example: If a server fails 18 days in an year (more or less 5%) of the operation time (one year equals to 365 days),

Availability= (365-18)/365 = 0.95

Its availability can be defined like 95%.

Full Fault Tolerance ensures that a component failure has no impact on operating parameters.

Example: RAID1.

Redundant Array of Independent Disks (RAID) is a common example of redundancy-based fault tolerance. RAID 1 (Mirroring) which uses an array of N identical (at least 2) disks all containing the same information. It is capable of supporting simultaneous failure of N - 1 disks.

Fault tolerance is usually achieved through component redundancy. Perfect and instant replacement of the failed component is not always possible.

In this case there is a temporary degradation of the operating parameters (*Graceful Degradation*).

If this degradation is significant or prolonged, the system is renamed *Fail soft*, not *Fault Tolerant*.

A system is called *Fail safe* if the failure causes unavailability but does not compromise its integrity.

Example: UPS without generator.

Fault avoidance is intended to prevent failures from occurring. It is based on several measures of common sense:

- Use of proven quality components
- Environmental control (temperature, humidity, dust)
- Power control (stability and filtering)
- Physical access control, including communication lines
- Remote access control (firewall, authentication)
- Prevention and fire fighting
- Performing thorough testing before putting components into operation
- Simplify system administration, for example with virtualization
- Control permissions and administration privileges
- Disclosure of the Security Policy and training of users and operators
- Applying all software updates
- Guarantees of authenticity (solid authentication mechanisms)
- Monitoring (allows detection of potential points of failure)
- Control of resource utilization (limitation / reserve). Ex .: CPU; RAM; DISCO; NETWORK

No matter how careful the measures taken in the areas of **fault prevention** and **fault tolerance**, they cannot be totally eliminated, so the last resort is the **reduction of the impact of failures**.

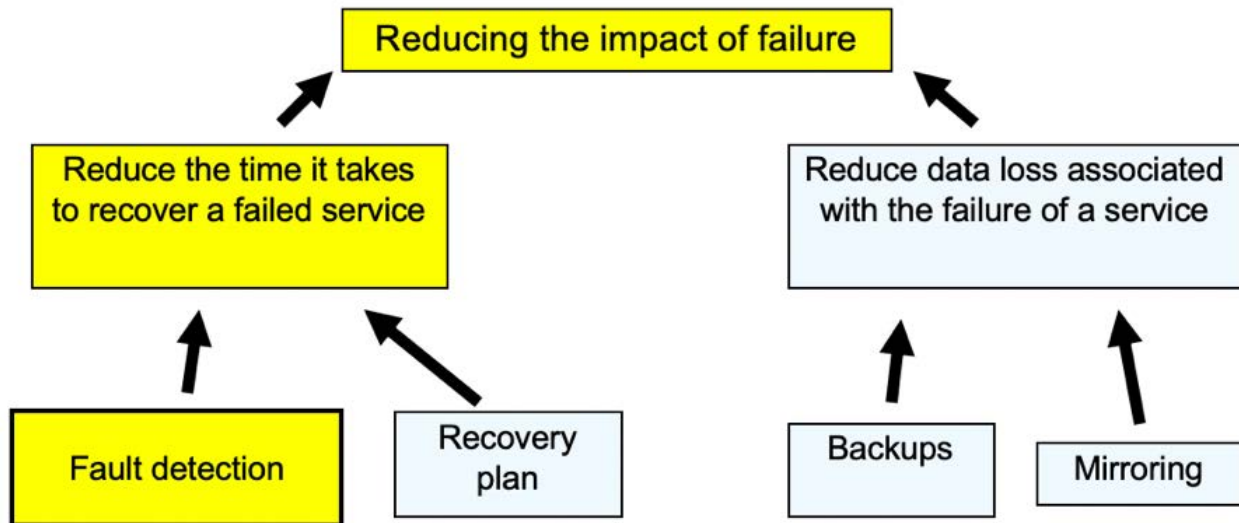


Figure 3.3. Reducing the impact of failure

For more details about mirroring see [Section 1.2 Fault Tolerance](#).

For various reasons, fault detection is directly involved in the three complementary strands of failure as can be seen in Figure 3.4.

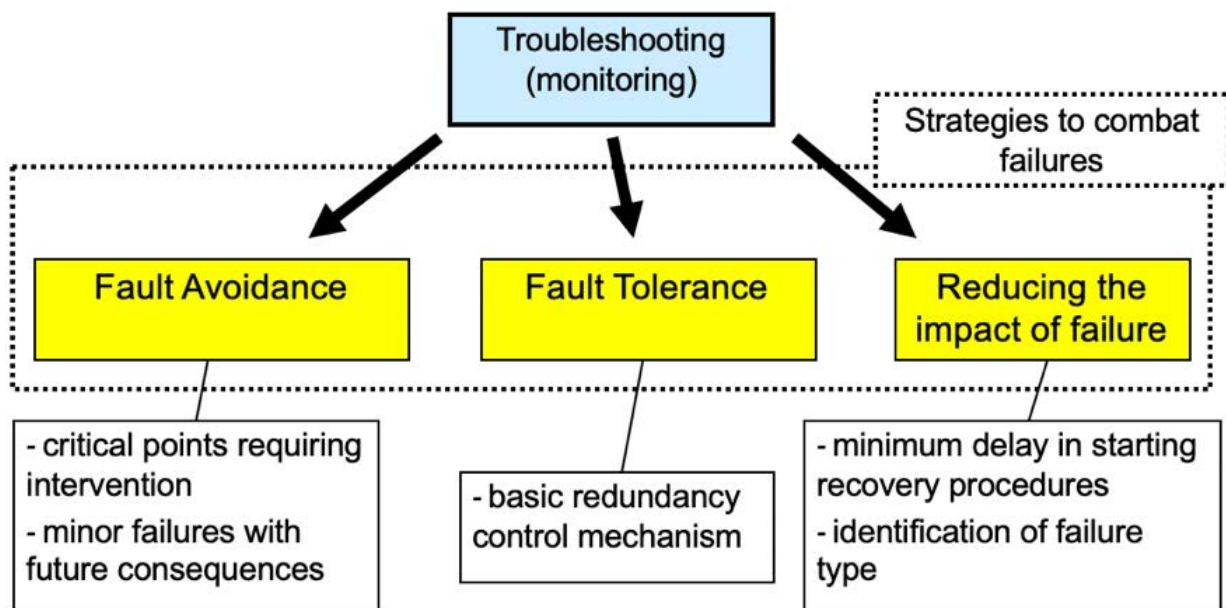


Figure 3.4. Troubleshooting

Monitoring

Detection of faults should be automated 24/7. This process consists of the periodic execution of tests on the components of the computer infrastructure:

- Service response times
- Internal devices state
- Measurements (temperatures, etc.)
- Anomalies in activity logs

- Volumes and types of network traffic
- Detection of anomalies and intruders

Once an anomaly has been detected, the monitoring system must notify the administrators as soon as possible so that the recovery process can be triggered. Typically, email is used, but it is preferable to supplement this option with a form of instant messaging.

On some systems it may be possible to define automatic recovery mechanisms for some anomalies.

The purpose of Business Continuity Plan (BCP) is to define a set of conditions and procedures aimed at ensuring the continuity of the business.

The Disaster Recovery Plan (DRP) is one of the most important elements of the BCP (sometimes confused), but the BCP is more comprehensive.

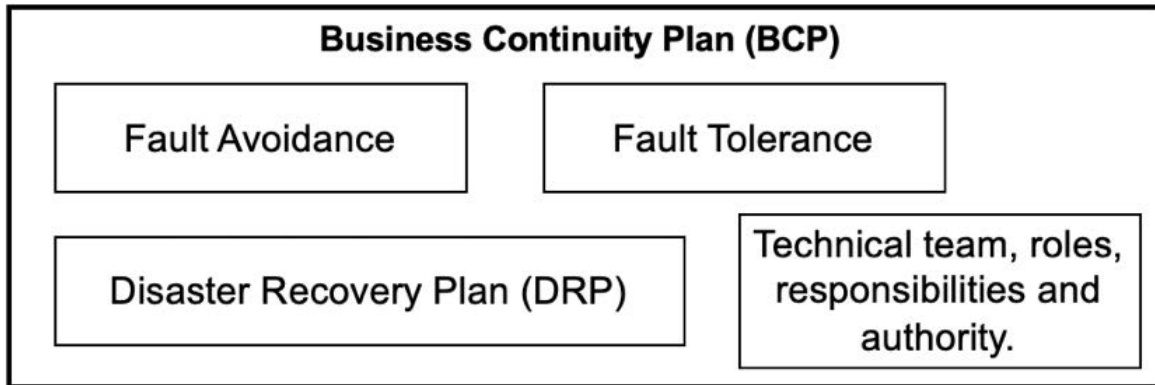


Figure 3.5. Business Continuity Plan

A business continuity plan should be composed by:

- Priorities and Responsibilities
- Main risks and minimization measures
- Suggested Strategies
- Backup Plan
- Roles and responsibilities
- Business Continuity Plan activation conditions
- Emergency recovery processes

Risk Assessment can be done using forms / surveys which, by quantifying a set of parameters, allows an abstract quantification of the risk in the domain under analysis.

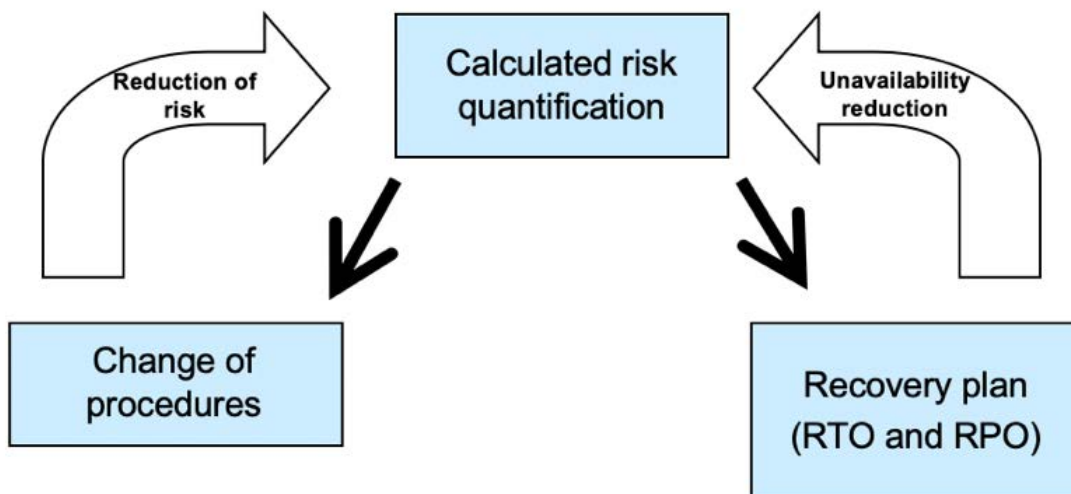


Figure 3.6. Risk assessment

Recovery Point Objective

For services where disaster data loss is permissible, Recovery Point Objective (RPO) specifies the maximum amount of data that can be lost. RPO specifies a pre-disaster operation time from which all changes made will be lost.

The time between backups can never be greater than RPO. If mirroring is used the RPO is null or very close to zero (if mirroring is synchronous, RPO is null).

Recovery Time Objective

The Recovery Time Objective (RTO) is therefore the maximum time it is assumed that the system is inoperative.

In the event of a failure, a recovery process must start (even if it is a component of a redundant system).

The term **disaster recovery** is more geared to high-impact events that include catastrophic natural disasters with almost total physical destruction.

Disaster recovery is critical to business continuity, the goal is to minimize downtime and possible data loss.

Disaster recovery is all about preparation and planning:

- Mirroring for remote location
- Regular backups stored in remote location
- Reserve hardware stored at a remote location
- Disaster scenarios and their recovery plans.

1.7.1. Disaster Recovery Plan

The purpose of DRP is to minimize downtime and loss of data in the event of a disaster.

DRP defines disaster scenarios and recovery procedures for each of them. This should also have a maximum time it is assumed that the system is inoperative.

1.7.2. Backup/Restore

The backup allows that after a disaster with loss of data or software configurations it is possible to recreate a **system with the same state as the date when the last copy was made**.

The frequency of performing backups should depend on the frequency of data changes and therefore should be appropriately tuned to each element of the infrastructure.

The exact time of backup should be adjusted to business hours. For daily copies, usually after-hours are the most appropriate.

High capacity discs are currently available at low cost, wherever possible this solution should be preferred over more traditional (very slow access) magnetic tape solutions.

These slower media are more suitable for archive copies than for backup copies.

Slow media also causes problems during the making of copies, making the operation time-consuming. Backup operations can impact system availability. Usually objects as files need to be locked to prevent changes being made to them during copying.

1.7.3. Backup/Restore plan

One way to reduce the length of copy operations is to use **incremental** copies or **differential** copies. **In any case the starting point is always a complete copy**.

An incremental copy contains the data that has been changed since the previous incremental copy (or full copy if it is the first).

A differential copy contains data that has changed since the last full copy.

- **Incremental** copies: a large number of incremental copies must be maintained; in addition to the space occupied the replacement operation becomes very time consuming.

- **Differential** copies: the volume of the differential copy is growing as changes are accumulated relative to the integral copy.

Here again the business hours must be respected, often the option is to make a full copy on Sunday and incremental or differential copies during the other days of the week (but depends on the working time in question).

A backup should never be deleted without the next backup being successfully completed. It is even desirable to keep at least one previous copy, often choosing to keep several.

The previous backup can be moved to a more economical storage medium before making a new copy.

Although the back-up can be left unmaintained in a fireproof enclosure, ideally it should be in a **separate geographic location (off-site)**.

There are some drawbacks:

- Security: it is necessary to ensure authentication and confidentiality (eg: [VPN](#)).
- Access speed: affects the time needed for the copy.
- Reliability: recovery is only possible if the network connection is operational.

The contingency plan is an important part of BCP and defines alternative methodologies to keep the business running when "normal" resources become unavailable.

In organizations highly dependent on computer systems, it can be difficult to implement.

Must define:

- What type of disaster should lead to the start of the contingency plan.
- Define the exact steps to be taken.
- Define needs in terms of personnel and materials or equipment.
- What "normal" procedures are foreseen in the contingency plan and which will be unavailable (restrictions on the operation of the business).
- How will the procedures performed during the contingency plan be integrated into the system after its recovery.

The Security Policy is a document that establishes a set of mandatory rules aiming at the protection of infrastructure and data.

It is an important element to ensure business continuity, especially in the field of fault prevention.

The Security Policy should be more abstract than a user manual, should indicate "what can not be done", "what can be done", but should not include "how to do".

For security reasons and in order to facilitate its adaptation to the evolution of the organization, it should not contain technical aspects of the implementation.

The Security Policy should be concise and easy to read and interpret; we suggest the use of the 5 Ws of journalism: **Who, What, Where, When, Why.**

The more or less restrictive nature of the Security Policy should result from a prior assessment of the potential for security risk.

It is possible to quantify a level of attack risk, through questionnaires about the organization / business and its infrastructure.

Characteristics:

- Public document, easily accessible to all users
- Mandatory reading for all users
- Identifies the various actors in the organization (users, administrators, ...)
- Clearly defines the security objectives
- Alerts users to the various threats to which the system is subject
- Stresses the importance of all without exception respecting the rules
- Justifies the reason for the imposed rules (the actors must agree)
- Identifies contacts for clarification of doubtful questions
- Defines the treatment of missing situations in the "security policy"
- It sets out the consequences of breaking rules (in an abstract way as it may conflict with legislation and / or labor agreements)
- Highlights the maintenance of activity records for audits
- Is consistent with the depth of the multi-strand approach
- It is possible to impose on the actors (it is possible to monitor compliance with the rules)

A policy must say what is allowed, prohibiting everything else. It is riskier to say what is forbidden, allowing everything else.

Policies of:

- Authentication
- Physical access
- Logical access
- Internal network usage (connecting devices to the network, ...)
- Internet use (access to websites, content control, ...)
- Passwords (rules in the definition, storage and handling)
- Use of email
- Privacy (confidentiality; activity logs and access to them)
- Management of work systems.

3.2 Data Confidentiality

Description

Table of contents

1. Data Confidentiality

2. Data Storage

2.1. External storage – Pendrives and external disks

2.2. Private Cloud (1)

2.3. Network Attached Storage

3. Data Transport

Confidentiality can be defined as guarantee that there is an appropriate level of secrecy at each processing node and that information leakage is prevented.

Confidentiality must be implemented in the whole system and not just in some parts.

Can be obtained through:

- Encryption of data stored and transmitted
- Secure communications

Can be overridden by:

- Communication monitoring
- Social engineering
- Stealing passwords

Data storage is a key part of a computer/industrial system where information needs and importance are increasing daily. Nowadays, in many cases, information is the most valuable asset of a company.

There are several media available to store data. These media differ in capacity, quality and price. In professional systems it is important to choose mediums that will ensure that information loss will not occur.

Pendrives and external disks are the cheapest media present in the market. They have some problems as result of the quality construction and because they are not very well treated/used by users.

These media can be used to store non-critic information. Nevertheless, it is advisable to have a backup in other medium.

This kind of equipment normally do not implement data security or encryption, therefore if it is lost or stolen, crucial data might become publicly available.



Figure 3.7. PenDrive

"Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams.

A cloud service has three distinct characteristics that differentiate it from traditional web hosting. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet, have accelerated interest in cloud computing.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Private cloud is a type of cloud computing that delivers similar advantages to public cloud, including scalability and self-service, but through a proprietary architecture. Unlike public clouds, which deliver services to multiple organizations, a private cloud is dedicated to the needs and goals of a single organization.

As a result, private cloud is best for businesses with dynamic or unpredictable computing needs that require direct control over their environments, typically to meet security, business governance or regulatory compliance requirements."

[1] Source: searchcloudcomputing.techtarget.com

Network Attached Storage (NAS) is a type of storage commonly used in companies because is an economical way to provide large storage space for multiple users.

The most important characteristics are:

- Quick to install and configure.
- Easy method of assuring [RAID](#) redundancy to multiple users.
- Allows you to set permissions for accessing folders and files to users.
- High utilization of storage resources.

This kind of storage has also a few drawbacks:

- Uses network resources (has at least one IP address).
- Latency and potentially data transfer issues.
- Performance affected by network availability.

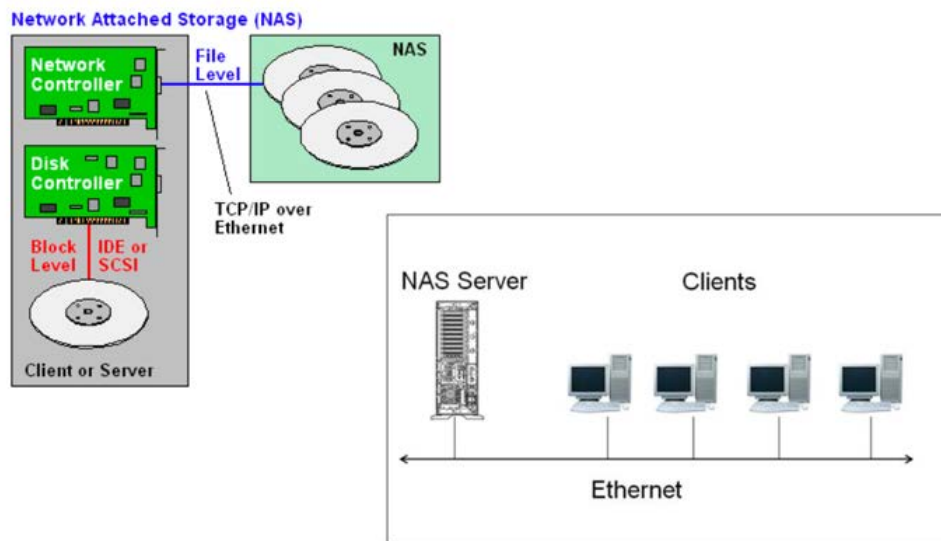


Figure 3.8. Network Attached Storage

Networks are by nature a privileged mean of conducting attacks:

- Being an information transmission means that it can be used to remotely attack systems that are safeguarded from physical access Content Delivery Network.
- Are extensive so it is very difficult to efficiently control physical access, making it even a mission impossible for wireless networks. Although physical access control does not offer guarantees, it should never be overlooked.

Authentication and encryption are two key tools for counteracting many of the attacks but may not be sufficient.

Segmentation of networks in distinct security-level zones is essential, typically three zones can be considered:

- Content Delivery Network (where lies the servers)
- Internal user network (intranet)
- External networks (Internet)

The separation between zones is ensured through the interconnection by routers that analyze and filter the information, designated by firewalls.

1.5.1. Wifi connections

In wireless networks, physical access control is totally impossible (in this kind of networks, signal is transmitted by radio waves available in the spectrum to be intercepted). Although wired local area networks currently support packet switching at level 2 (eg Ethernet), these switches do not separate broadcast domains and their operation can be compromised. From the security point of view, this type of infrastructure must always be considered equivalent to a shared transmission medium network: any packet emitted on a given node is delivered on all other nodes of the network.

In the market are available a set of algorithms that allow to implement security and encryption to the packages that circulate in WIFI networks.

The most common examples of these security algorithms are:

WEP - Wired Equivalent Privacy (1999 - 2004 standard. Possible to break. Abandoned)

WPA - WiFi Protected Access - Enhancement for WEP. Easy to break.

WPA2 - WiFi Protected Access version 2. AES Advanced Encryption Standard encryption is the most important improvement made in WPA2 over WPA.

1.5.2. Secure Data Transport - Digital signatures

A digital signature is a way to ensure authentication and/or confidentiality based on a digital certificate composed by 2 keys (one private that only the certificate owner should know and a public key that should be publicly known). This method is called asymmetric encryption because an encrypted message can only be decrypted with the other pair key.

PKI (Public Key Infrastructure)

- Used to encrypt, decrypt, and authenticate (digital signature)
- The public key is freely disclosed and can be used for encryption.
- The decryption is done with the private key (secret).
- It is not bidirectional because a key pair only allows confidentiality in a sense.

The separation between zones is ensured through the interconnection by routers that analyze and filter the information, designated by firewalls.

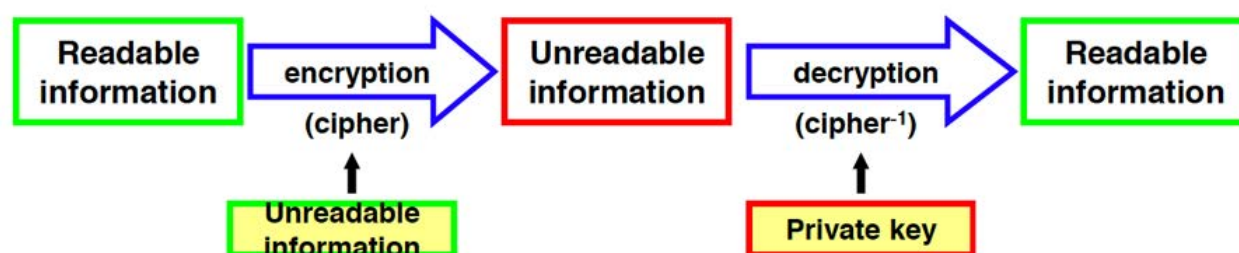


Figure 3.9. Digital Signature

A public key / private key pair only ensures one-way confidentiality, to get two-way confidentiality two key pairs are needed. The application of asymmetric encryption with the private key to a solid hash code allows to implement in a simple way all the functionalities of a digital signature, attesting:

- Integrity of content
- Author authentication
- Non-repudiation (only the author owns the private key)

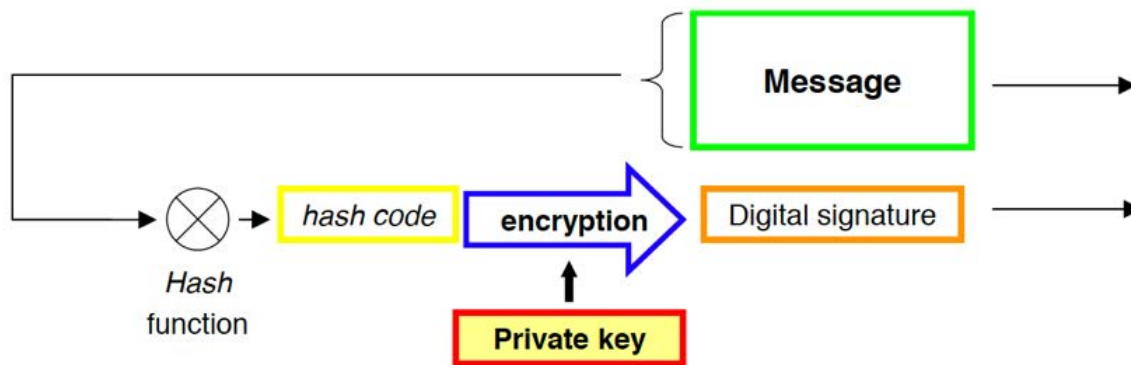


Figure 3.10. Integrity and authentication

1.5.2.1. Confidentiality with asymmetric key ciphers

The use of a public key from someone to encrypt a message allows to ensure confidentiality because the encrypted message will only be decrypted with the user's private key.

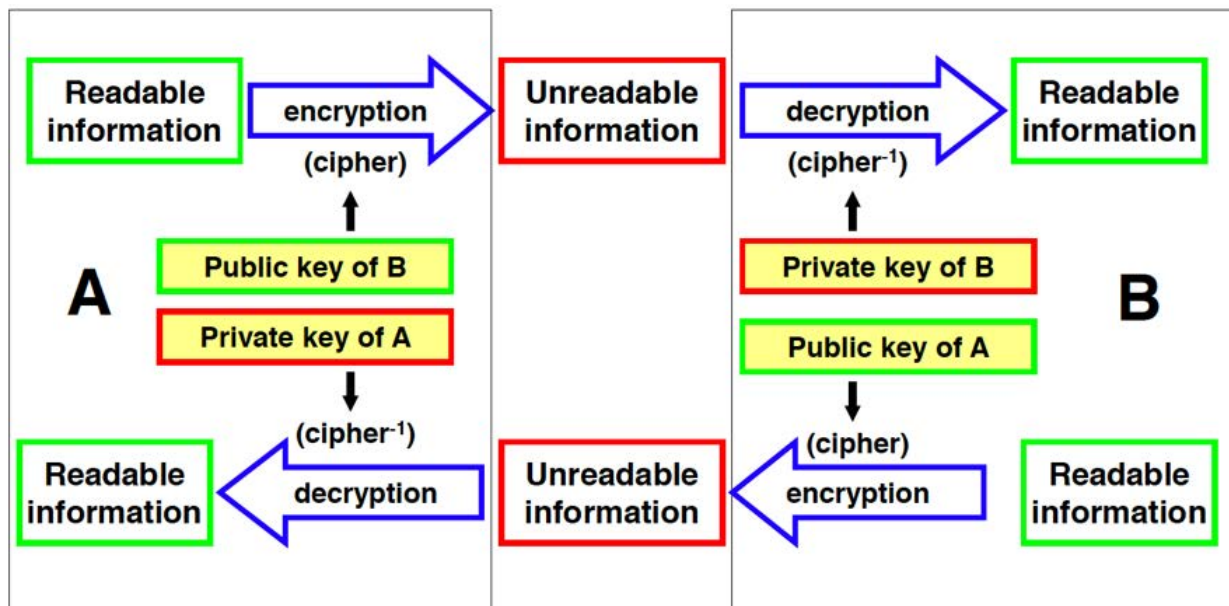


Figure 3.11. Confidentiality with asymmetric key ciphers

3.3 Data Integrity

Description

Table of contents

1. Data Integrity

1.1. Data storage

Integrity can be defined like confidence in the system's accuracy and reliability and in the unauthorized data change prevention.

It ensures that attacks and errors do not compromise the information and the system

Can be obtained through:

- good management of the capabilities of the system
- intrusion detection mechanisms
- appropriate access controls

Without guarantee of integrity a system can operate on incorrect data, without knowing it.

Data backup and storage is one of the most important measures that a company should do to protect their business.

It is important to:

- Backup data regularly (this periodicity should be evaluated in each case)
- Create backups on reliable media or in the company clouds (these clouds should have redundant backups)
- If using media for backups keep the devices in a secure, off-site location.

1.1.1. Correct backup safe place

The place where backups are located is a key part of the backup process. Because of unpredictable disasters backups should be maintained in more than one location. Companies can maintain a local backup in their installations but should have another copy in an external location (it can be a cloud or another company facilities).

1.1.2. Hash of the backed-up files

The resultant backed-up files should be hashed to guarantee that any modification was made.

This process implies the utilization of a cryptographic algorithm like MD5. The application of this type of algorithms to a file return a number/code that can be considered like an identifier. If the file is changed the result of the algorithm application will differ and it is possible to detect that some unauthorized change was made.

When a backup is made a hash code should be generated based on the application of a cryptographic algorithm. Later this hash can be used to evaluate if the file was changed.

1.1.3. Test of the backups (2)

"Imagine you're driving down the road and, suddenly, you hear an ominous sound coming from the rear of your car: thumpa-ta, thumpa-ta, thumpa-ta. As the car becomes increasingly difficult to handle, you begin to understand what has happened: You have a flat tire.

No problem. Just find a safe spot and pull the emergency spare out of the trunk. Uh-oh, the spare is flat, too.

A similar crisis faces an untold number of storage administrators every day. Due to an oversight, error or a prime storage media failure, a need suddenly arises to access a particular set of files stored on backup media. But the backup data is missing, outdated or defective. Like an unlucky driver, the storage administrator now faces a predicament that could have been easily avoided with some advance planning, in the form of testing backups.

Here's what you need to do.

- 1. Understand the seriousness of regular backup testing. Just as it's important to test a spare tire to ensure it will work when it's needed most, you need to be testing backups, said Girish Dadge, product management director for Sungard Availability Services. "Testing your backups also gives you a chance to assure yourself that your backup policies and schedules work properly," he added.*
- 2. Create a documented backup testing plan. Familiarity with a documented test plan ensures that employees have both the skills and experience necessary to successfully perform data recovery and provides confidence to the organization, observed Eamonn Fitzmaurice, worldwide data protection lead at IT services firm HPE Pointnext.*
- 3. Make testing backups a routine. To assure the validity and integrity of any backup, it's essential to carry out regular restoration tests. "It is not unusual to find organizations that have systems that are inadvertently not being protected via a backup schedule," Fitzmaurice explained. Routine and comprehensive backup testing is a strategy that can highlight anomalies so that corrective action can be taken.*
- 4. Take a holistic approach. Organizations need to understand their data layout and why they are doing backups. They then need to develop a test backup plan to meet their desired objectives.*

Every organization has different backup objectives. "For example, the banking industry needs backups for compliance, audit and legal," Dadge said. "Healthcare organizations have personal data, so they need to focus on security, retention and legal requirements." All restore and recovery testing should include data, application and system state testing, Dadge recommended.

- 5. Test frequently according to regular schedules. Ideally, a test should be conducted after every backup completes to ensure data can be successfully secured and recovered. However, this often isn't practical due to a lack of available resources or time constraints. "Each organization should, at a minimum, commit to a regular schedule of weekly and/or monthly restores of systems, applications and individual files with checks to ensure the data is valid and accessible as intended," stated Marty Puranik, CEO of Atlantic.Net, a cloud*

hosting provider. "This will also provide your organization with a realistic time frame for recovery when disaster strikes."

Not all data is created equal, a fact that should impact frequency of testing backups. "Some data is more important than others," noted Atif Malik, a director in KPMG's CIO Advisory unit. For instance, Sarbanes-Oxley Act compliance and regulator data might be considered more important than marketing data. "Controls should be in place to mitigate risks based on the importance of that data," Malik advised.

6. Take full advantage of automation. Automation should play a key role in any backup testing strategy. "Organizations should strive to automate as much of their backup testing as possible to ensure consistency and data validity and to reduce the burden on staff tasked with testing backups," Puranik suggested. "Test restoring full systems to virtual machines, applications, databases and individual files," he added.

7. Ensure that the backup test covers all bases. If the backup test doesn't actually test the entire workload being restored, it can't be considered a real test. "Many organizations will simply restore one or two files from archive and consider that a success," noted Chris Wahl, chief technologist at cloud data management provider Rubrik. "This workflow has no relationship to the reality of restoring complex applications and should be avoided when considering a real backup test."

8. Make testing backups an integral part of internal app development and deployment. Backup testing should be in the front of everyone's mind when developing and introducing new applications into the organization. "The most successful enterprise data management strategies involve knowing how and when to perform backup validation tests before allowing data to move into a production workload," Wahl explained.

9. Ensure backup accuracy. When data is recovered, storage administrators and database administrators can perform an initial "sanity check" on the data. "However, the end users of the business applications are often best positioned to highlight if the data restored is accurate and consistent," Fitzmaurice observed.

10. Have redundant backups. Never back up to only one tape or set of tapes. "If you do use tapes, replace them on a regular basis," recommended Brian Engert, senior application developer at customer software developer Soliant Consulting."

[2] Source: <https://searchdatabackup.techtarget.com/tip/Ten-important-steps-for-testing-backups>

Exercise 1. Back-up of critical information

In internet are available several backup solutions.

Some examples are:

COBIAN BACKUP (<https://www.cobiansoft.com>)

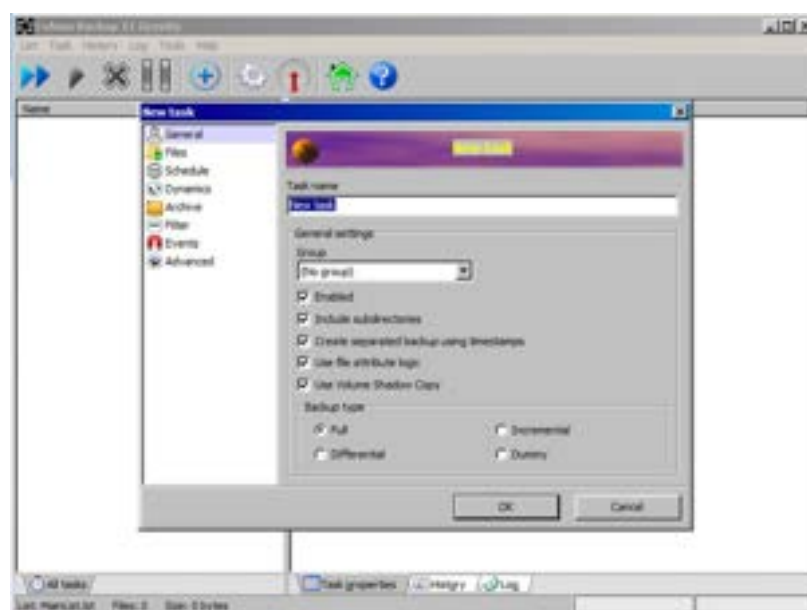
GOOGLE BACKUP AND SYNC (https://www.google.com/intl/en-GB_ALL/drive/download/backup-and-sync)

ACRONIS (<https://www.acronis.com/en-us/business/overview/>)

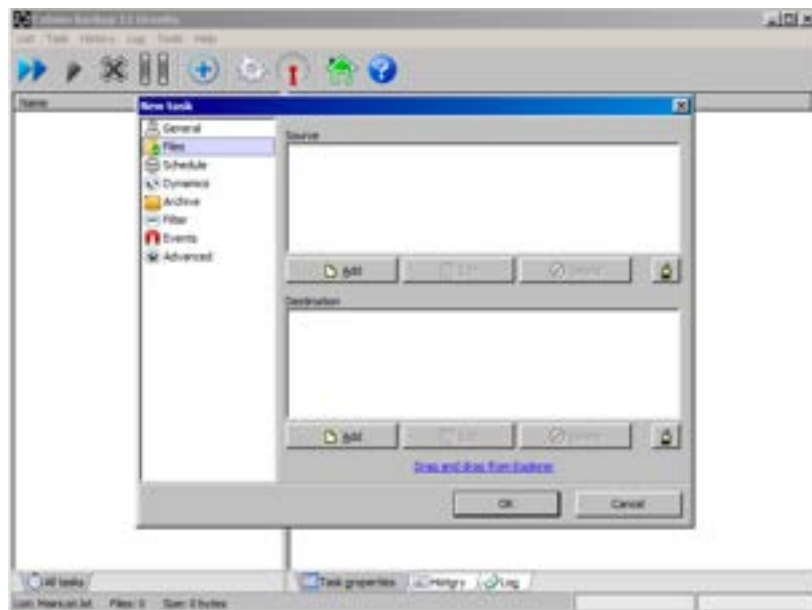
Please use one of them to create a local backup to an external location(harddrive, pendrive, sdcard, etc) and to create a remote backup to an offsite location.

Example of Cobian Backup:

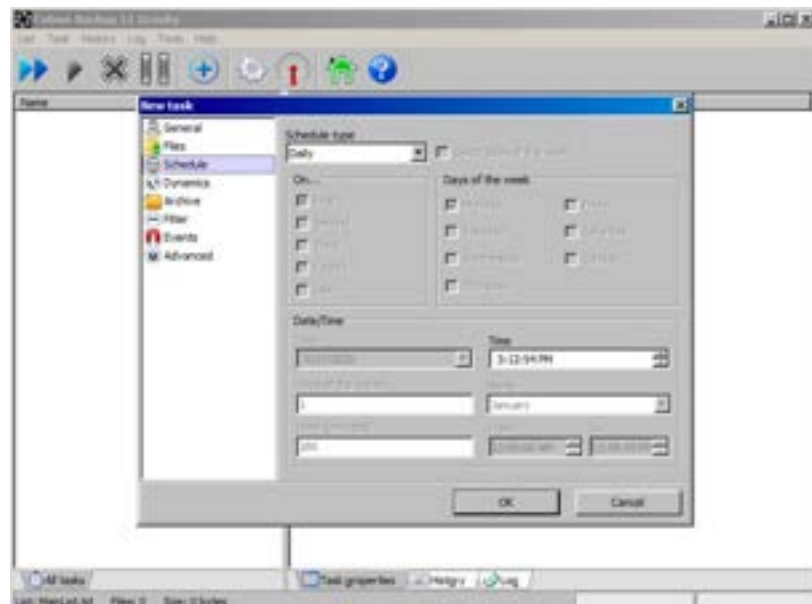
1. Download and install the software.
2. Create a new task(Task, New task) and choose the type of backup (Full, Incremental and Differential)



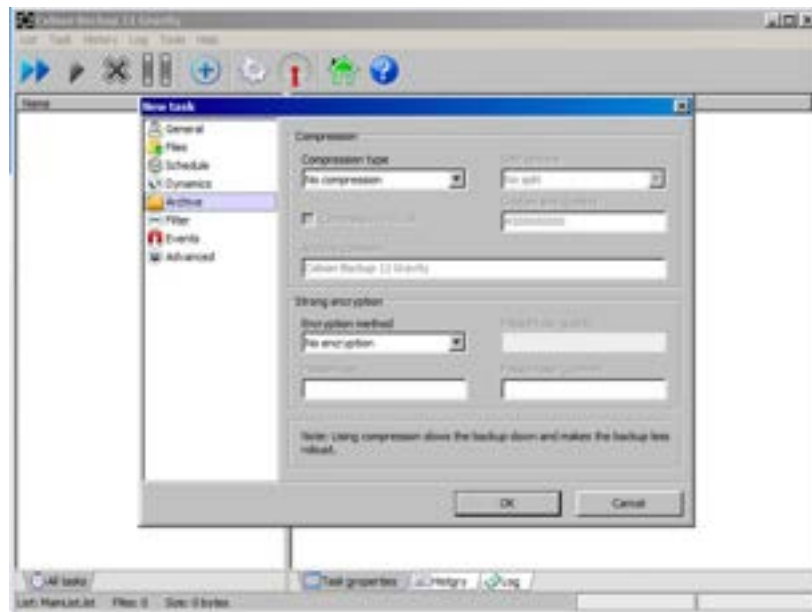
3. In the Files menu choose the files to be included in the backup and the backup destination(it can be a directory locally or in an external drive) or a remote ftp location) .



4. In the Schedule menu the backup frequency can be chosen (Normally daily, weekly or monthly)



5. In the Archive Menu, compression can be chosen if it is important to compress data before backup.



Notes

Note 1: Backups of company information must be done with knowledge and authorization of administration.

Note 2: Backups must comply with EU regulations described in **General Data Protection Regulation**. For example it is important to understand if you can backup data related with persons for locations outside EU (and in the case you need to do it what conditions you need to assure)

Exercise 2. Secure e-mail communications

In order to receive encrypted email or send digitally signed email, you must have a digital certificate.

To install your digital certificate into **Mozilla Thunderbird** to digitally sign or encrypt emails, follow these instructions:

1. Within Thunderbird, click on “Menu” and then hover over the “Options” or “Preferences” section.
2. Click on the “Account Settings” section; then click the “Security” tab.
3. Click the “View Certificates” button; then click the “Import” button.
4. Locate the backup file for your certificate and click “Open”.
5. You will be asked to enter the certificate backup password; then click “OK”. (The certificate backup password is the password you chose when exporting/backing-up the certificate.)

Configure Thunderbird with a Default Certificate

1. Within Thunderbird, click on “Menu” and then hover over the “Options” or “Preferences” section.
2. Under your “Email Account Heading” (you may need to expand it), click on “Security”.
3. Next to the box for “Use this certificate to digitally sign messages you send”, click “Select”.
4. Choose the correct digital certificate to use. Note that the email address in your email account should match the address in the certificate.

5. Next to the box for “Use this certificate to encrypt & decrypt messages sent to you”, click “Select”.
6. When composing a new email, click on the Security menu and choose Digitally Sign this Message

Further instructions about how to use digital certificates in Mozilla Thunderbird can be seen here:

https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages#w_sending-a-digitally-signed-and-or-encrypted-email

Why is it backwards? It isn't really backwards. You could give the public, encoding part to everyone you know. When someone wants to send you a secret message, they use your public key that everyone knows to encrypt it. Only your private key (that must never be shared with anyone) will allow the message to be decrypted and read. A digital certificate allows you to get, but not send, encrypted email.

Secure two-way communication is achieved by both ends having certificates and having both parties give everyone their public key. If this is done then anyone, anywhere can send an encrypted (secret) message to either of these two people. These two people have that same ability and can now send encrypted messages to each other using each other's public key.

If you have available an digital certificate from your country (in your citizen id card) or from your institution please try to use it to sign your emails and to encrypt them in order to understand the difference between these 2 approaches.