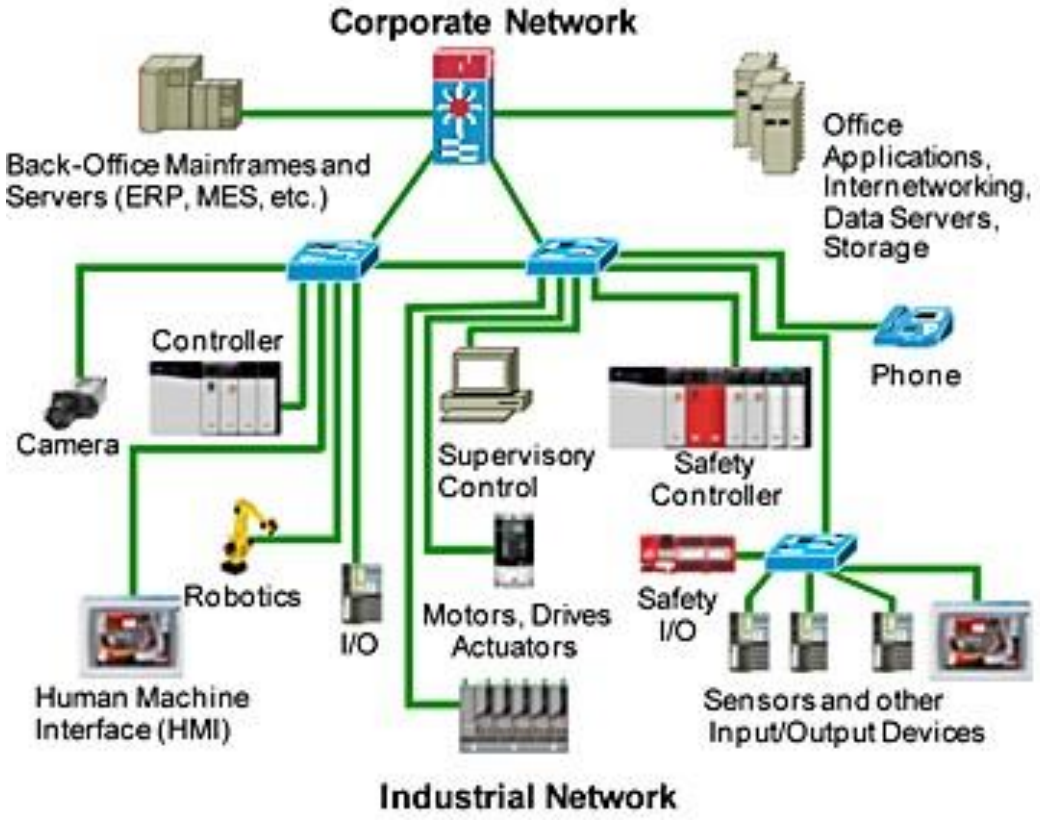
An Introduction to SCADA Fundamentals

Chapter 7

Table of Content

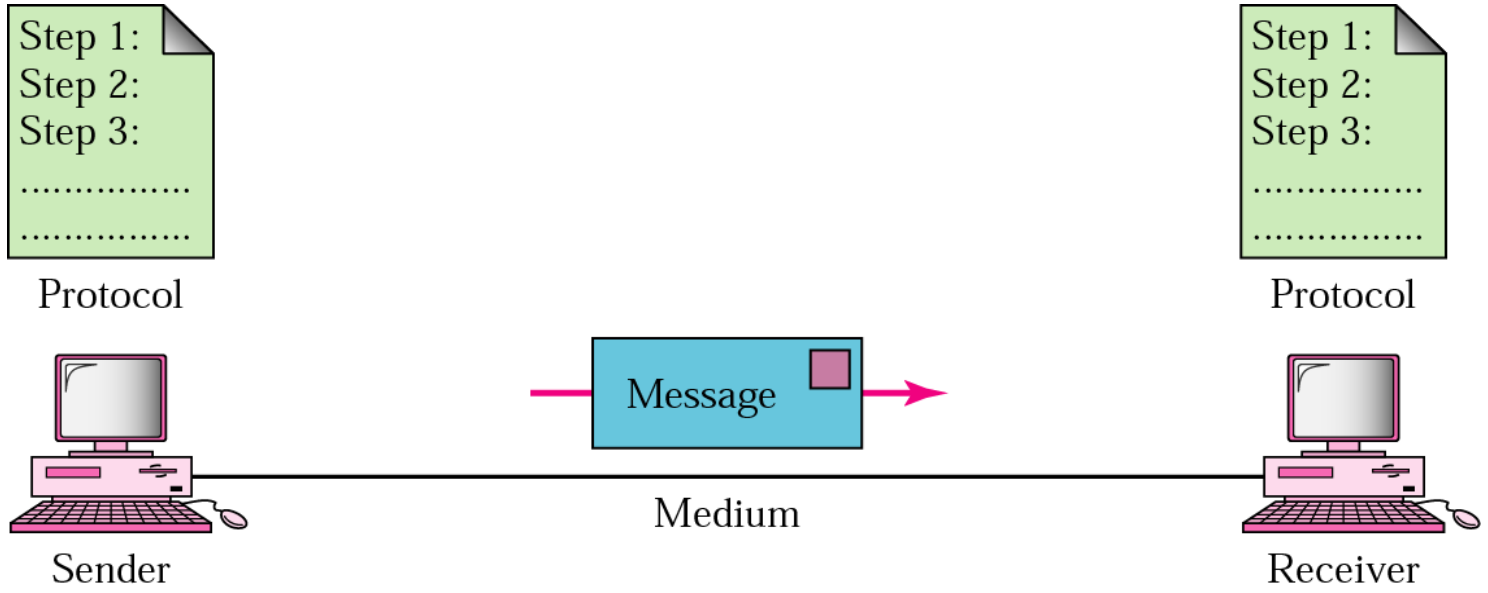
Industrial Network

- PLC (Programmable logic controller) communicate using one of several protocols, such as EtherNet/IP, Modbus, Profibus, CANopen, DeviceNet or FOUNDATION Fieldbus.
- Many Industrial Ethernet protocols use a modified MAC (Media Access Control) layer to provide low latency and determinism.
- Data communication is the transfer of data from one device to another via some form of transmission medium.
- A Network: is a set of communication devices connected by media links.
- Devices connected to the Internet are called *hosts*
- Most hosts are computers, but hosts also include routers, printers, fax machines, etc.



Network Components

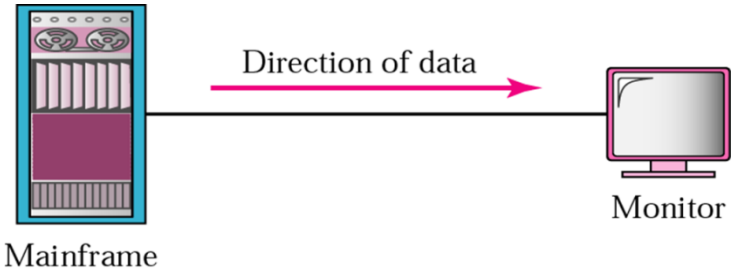
Components: message, sender, receiver, medium, and protocol.



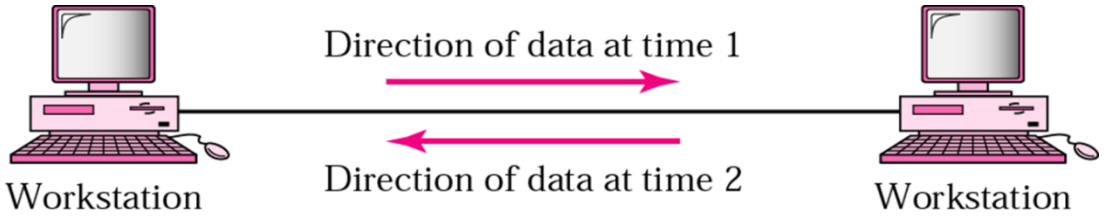
Data Flow

Data flow between two devices can occur in one of three ways:

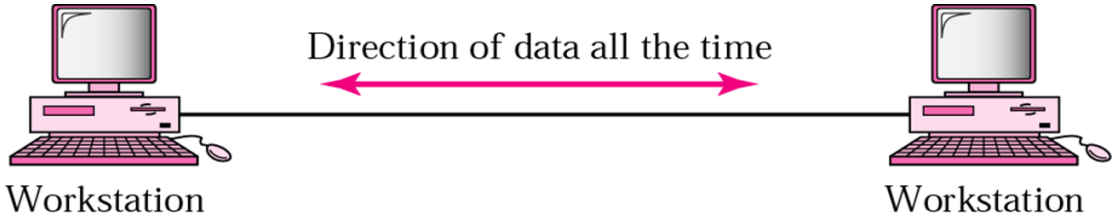
1-Simplex.



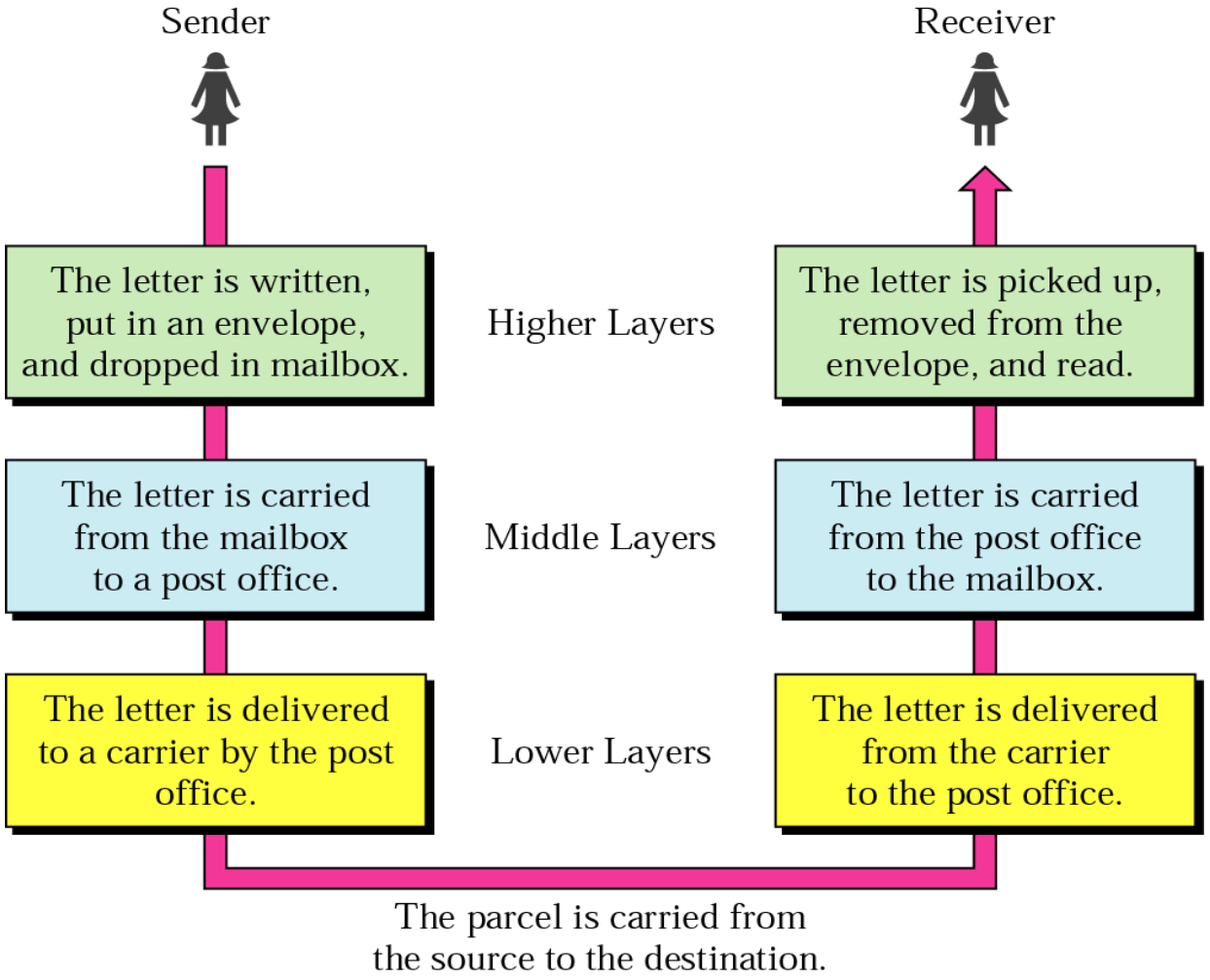
2-Half-duplex.



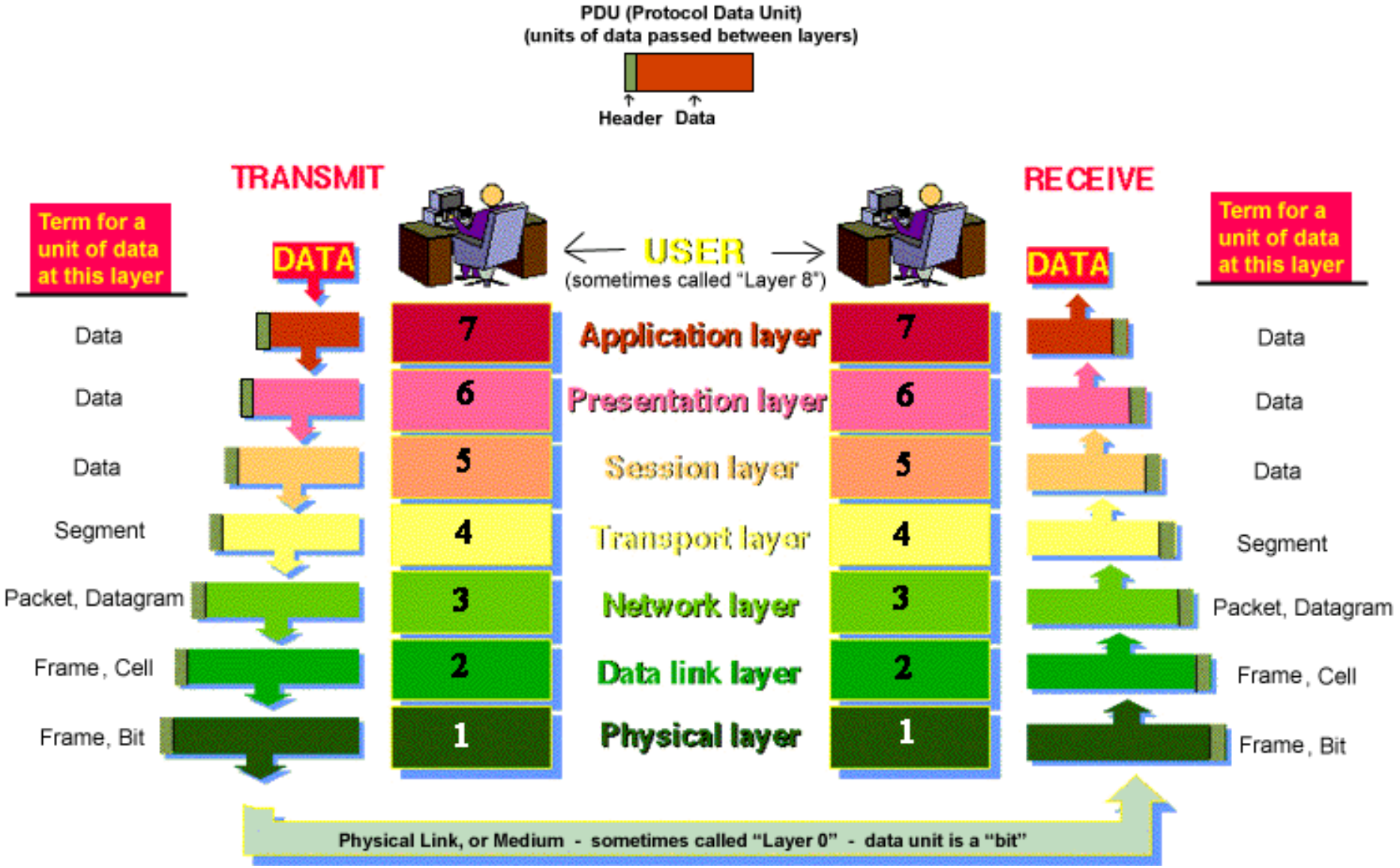
3-Full-duplex.



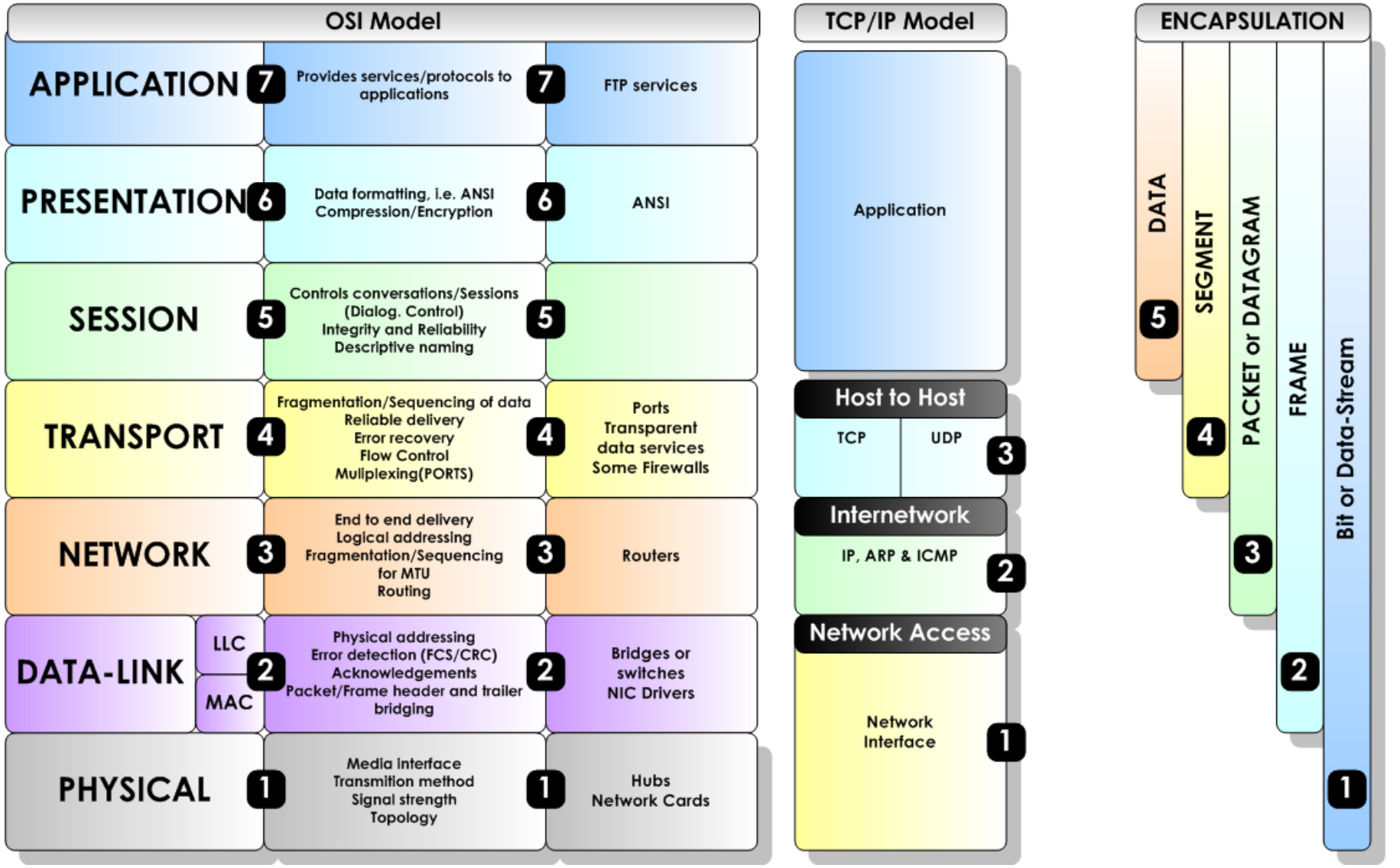
Sending a letter



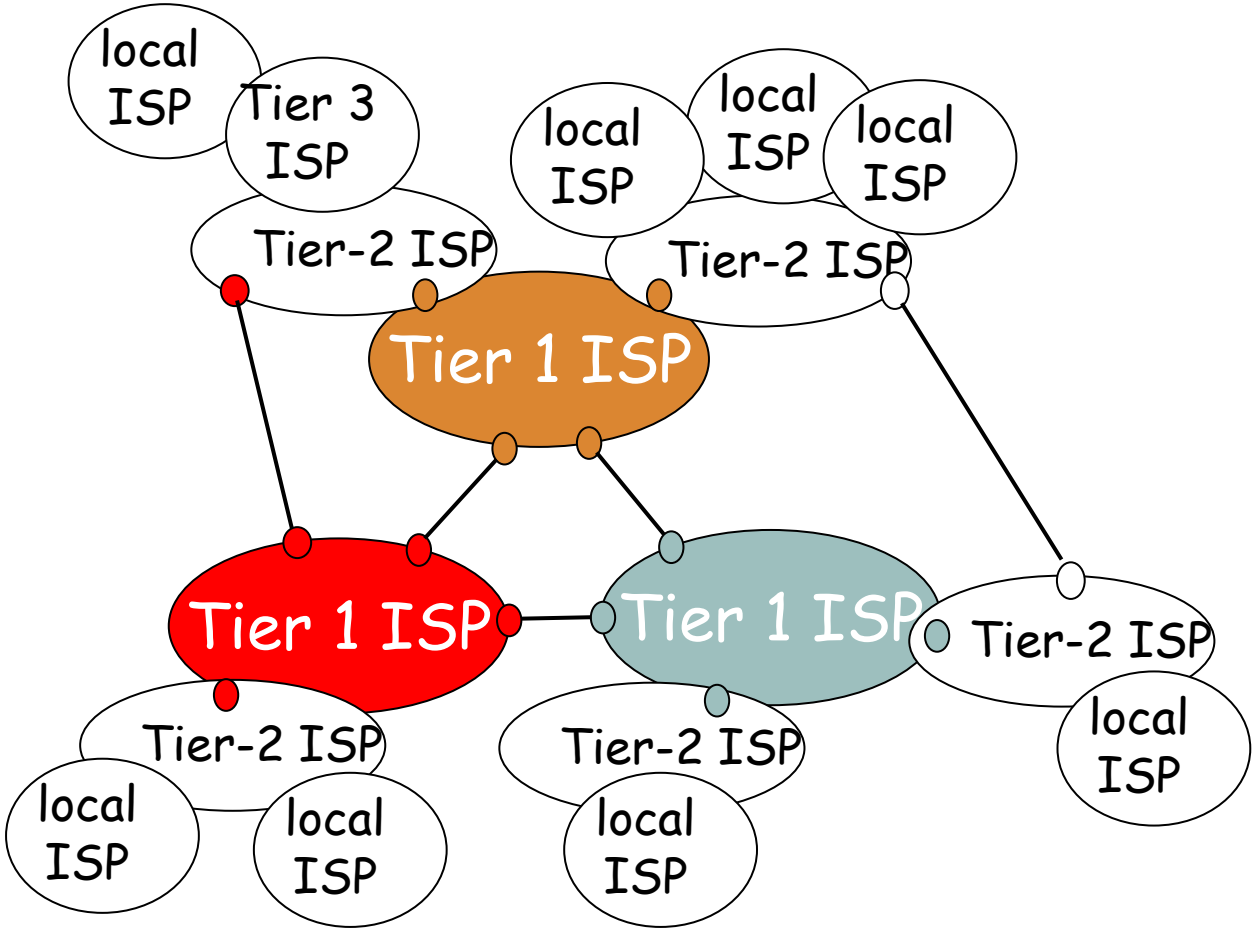
Sending a letter (Network View)

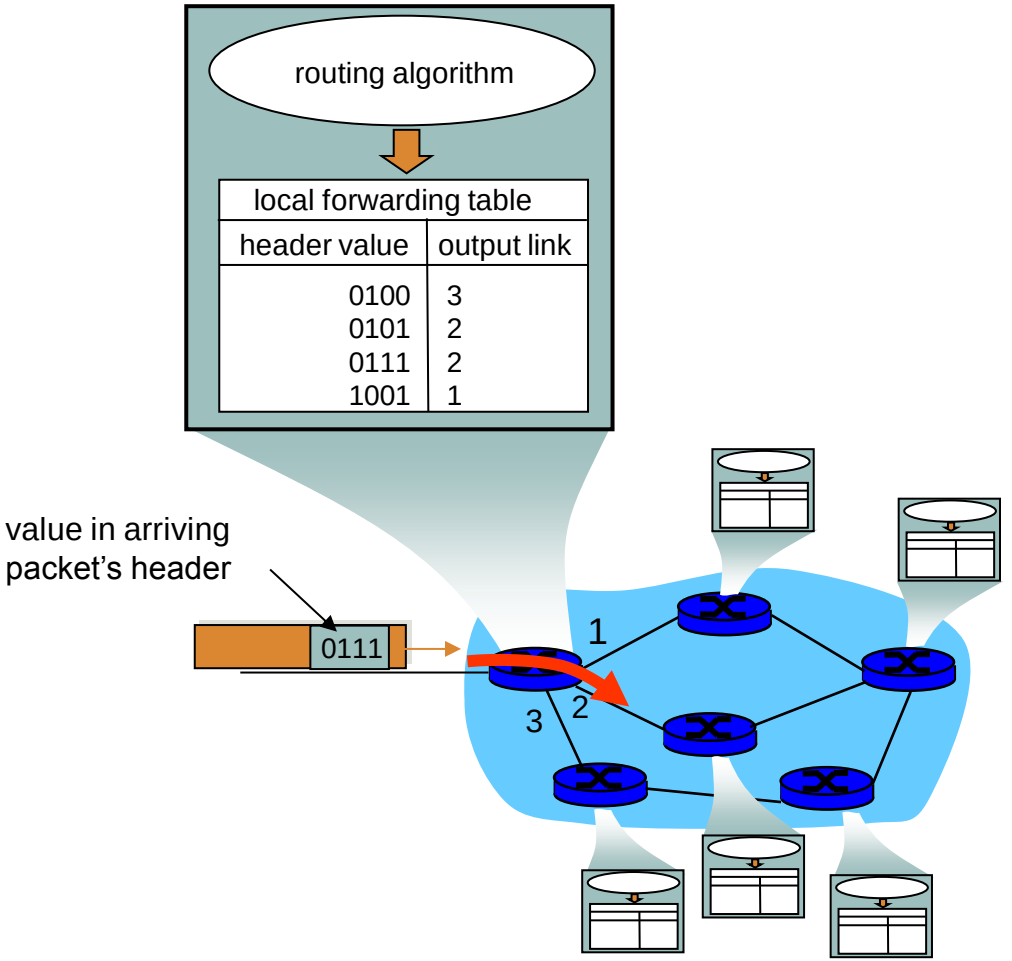


Network Layers

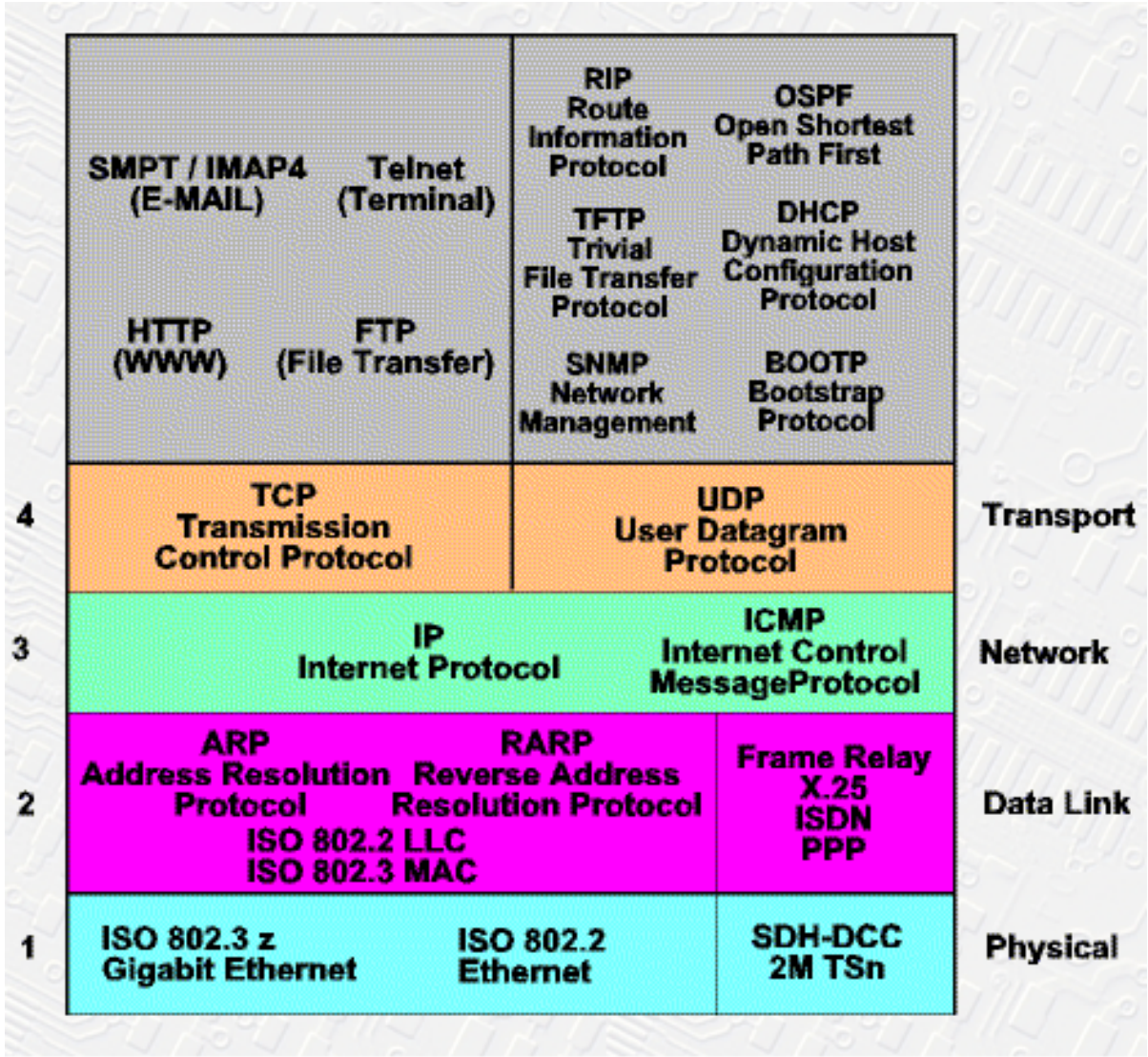


Internet structure: network of networks



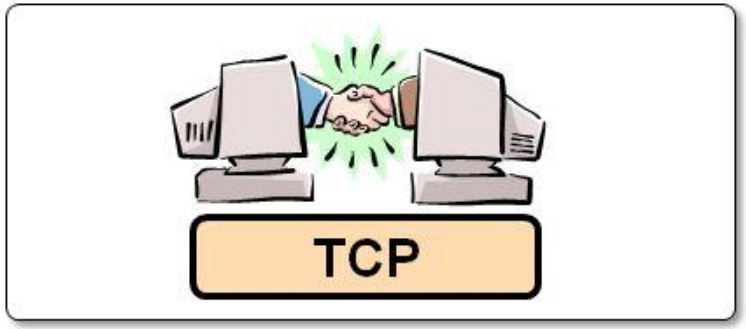


TCP/IP Major protocols

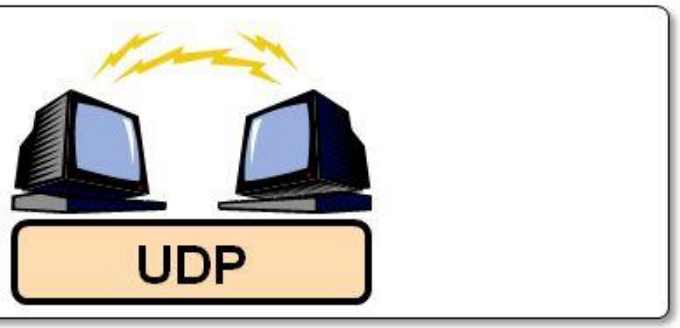


- Telnet (port 23)
- File Transfer Protocol (port 20 & 21)
- Post Office Protocol Version 3 (POP3) (port 110)
- Simple Mail Transfer Protocol (SMTP) (port 25)
- Hyper Text Transfer Protocol (HTTP) (port 80)

Transport Layer Major Protocols



- Slower but reliable transfers
- Typical applications:
  - Email
  - Web browsing



- Fast but non-guaranteed transfers ("best effort")
- Typical applications:
  - VoIP
  - Music streaming

Transmission Control Protocol (TCP)

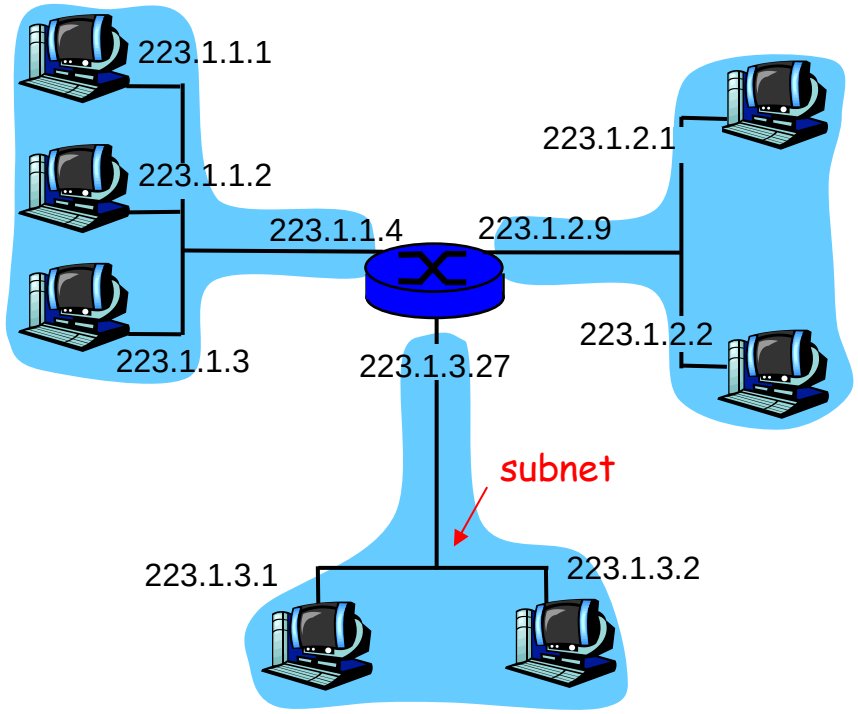
- **Layer 4 protocol that provides guaranteed delivery and ordering of packets**
- **Supports port number**
- **Contains additional information that allows it to order packets and resend them if error occurs**

User Datagram Protocol (UDP)

- **Layer 4 protocol to send packets of data**
- **Supports port number**
- **Does not guarantee delivery of packets or will arrive in the correct order**

IP Addressing

- IP address: 32-bit identifier for host, router *interface*, every host on the Internet is identified by a unique, four-byte Internet Protocol (IP4) address.
- This is written in dotted four-byte (32 bits) address format like 199.1.32.90 where each byte is an unsigned integer between 0 and 255.
- There are about four billion unique IP addresses, but they aren't very efficiently allocated.
- The solution is IPv6 which uses 128 bit addresses but it is not yet widely deployed by ISPs
- Each 32 bit IP number consists of two components:
  - The network address
    - The unique international address of the network
  - The host address
    - The unique address of a specific host in the net
- There are three classes of network address denoted class 'A', 'B' and 'C'

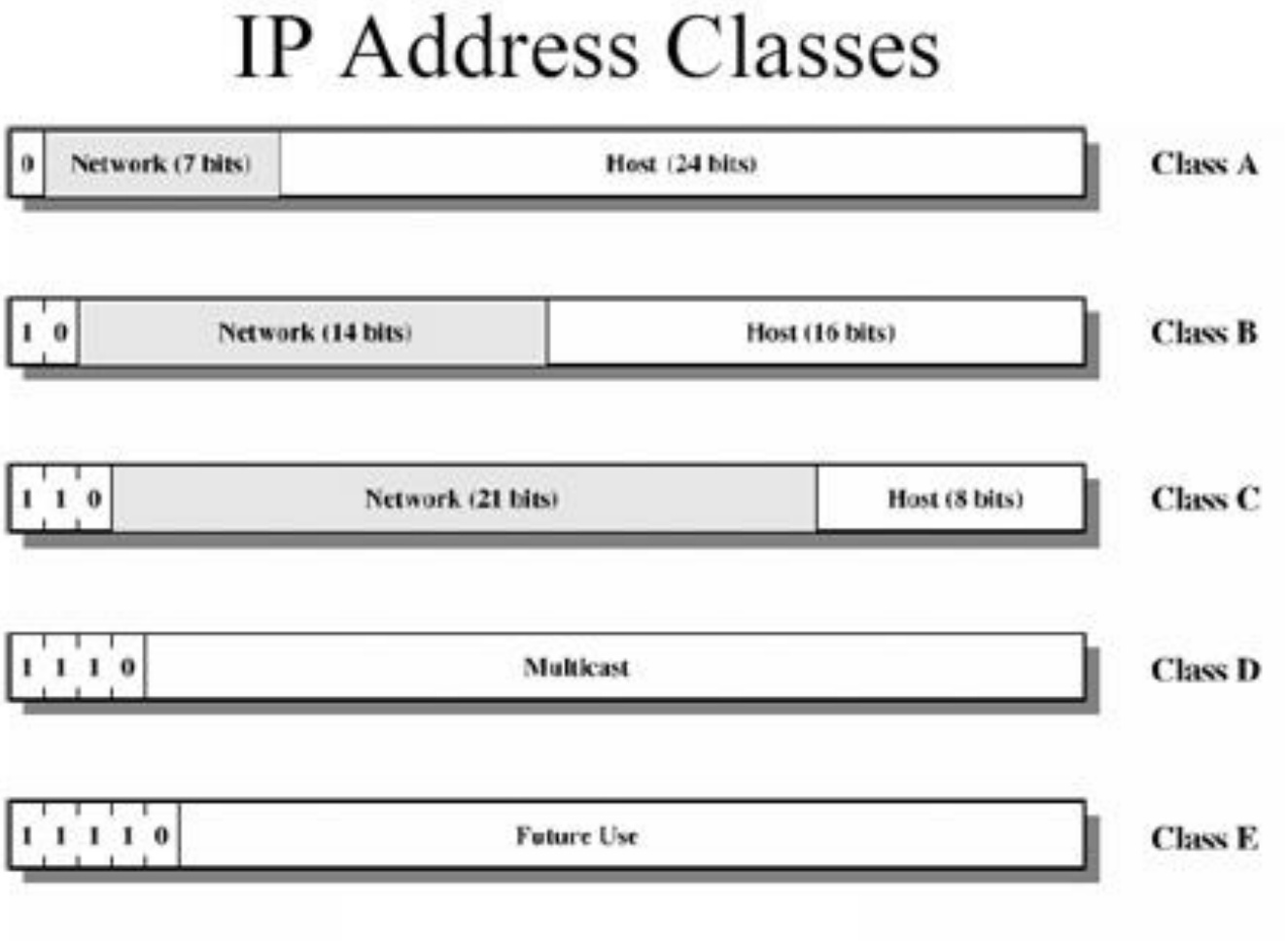


network consisting of 3 subnets

223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

IPv4 Address Classes



Private IP Addresses

Class A

10.0.0.0 to 10.255.255.255

Class B

172.16.0.0 to 172.31.255.255

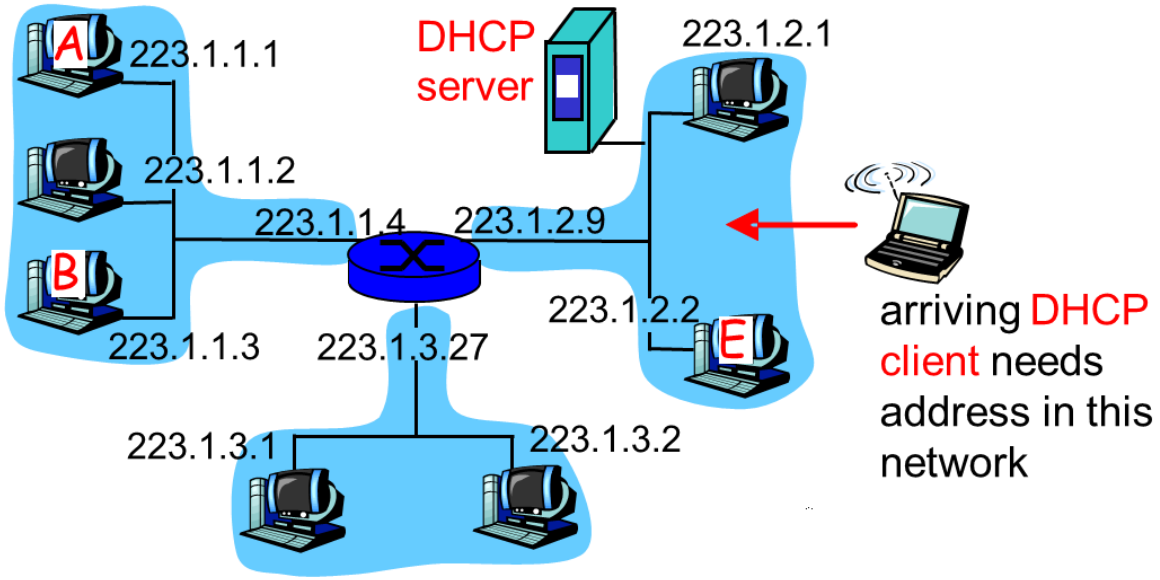
Class C

192.168.0.0 to 192.168.255.255

IP addresses: how to get one?

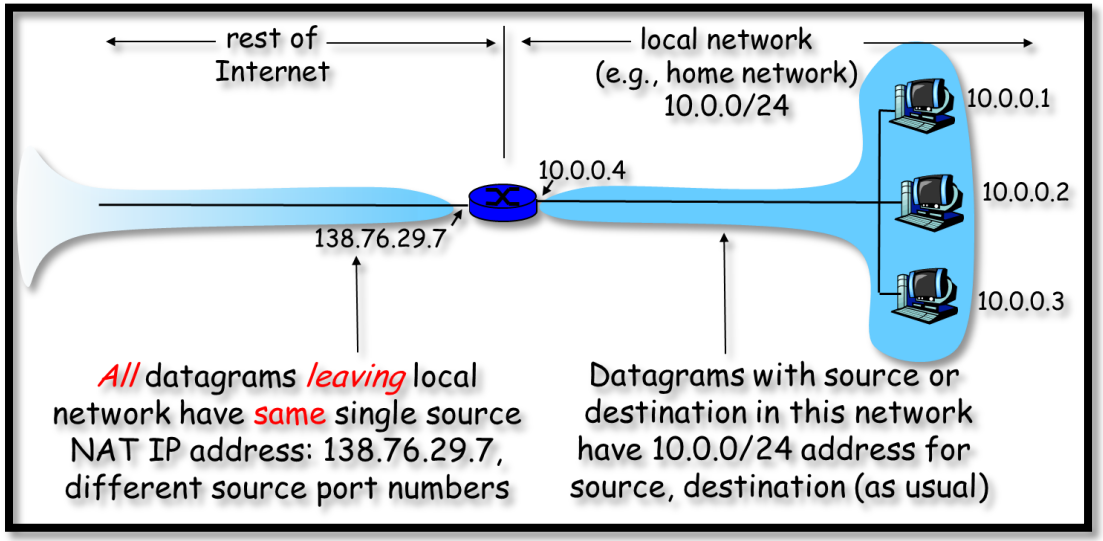
How does a *host* get IP address?

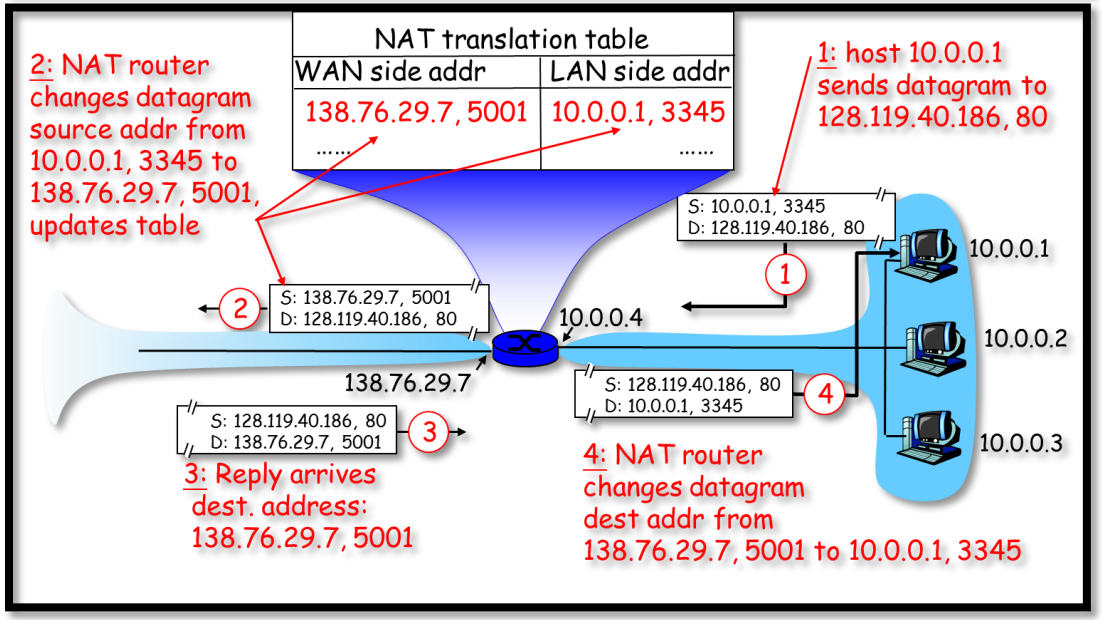
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
- Allow host to *dynamically* obtain its IP address from network server when it joins network
  - Can renew its lease on address in use
  - Allows reuse of addresses (only hold address while connected an “on”)
  - Support for mobile users who want to join network (more shortly)
- DHCP overview:
  - host broadcasts “DHCP discover” msg
  - DHCP server responds with “DHCP offer” msg
  - host requests IP address: “DHCP request” msg
  - DHCP server sends address: “DHCP ack” msg



NAT: Network Address Translation

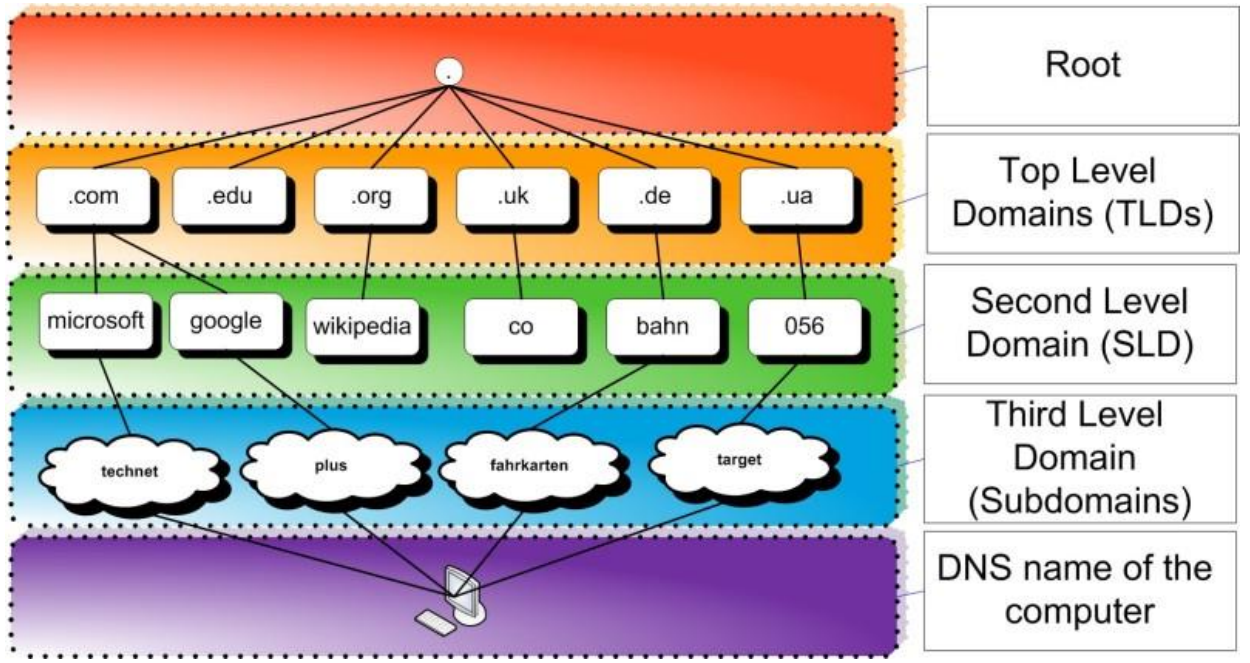
- Motivation: local network uses just one IP address as far as outside world is concerned:
  - range of addresses not needed from ISP: just one IP address for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).





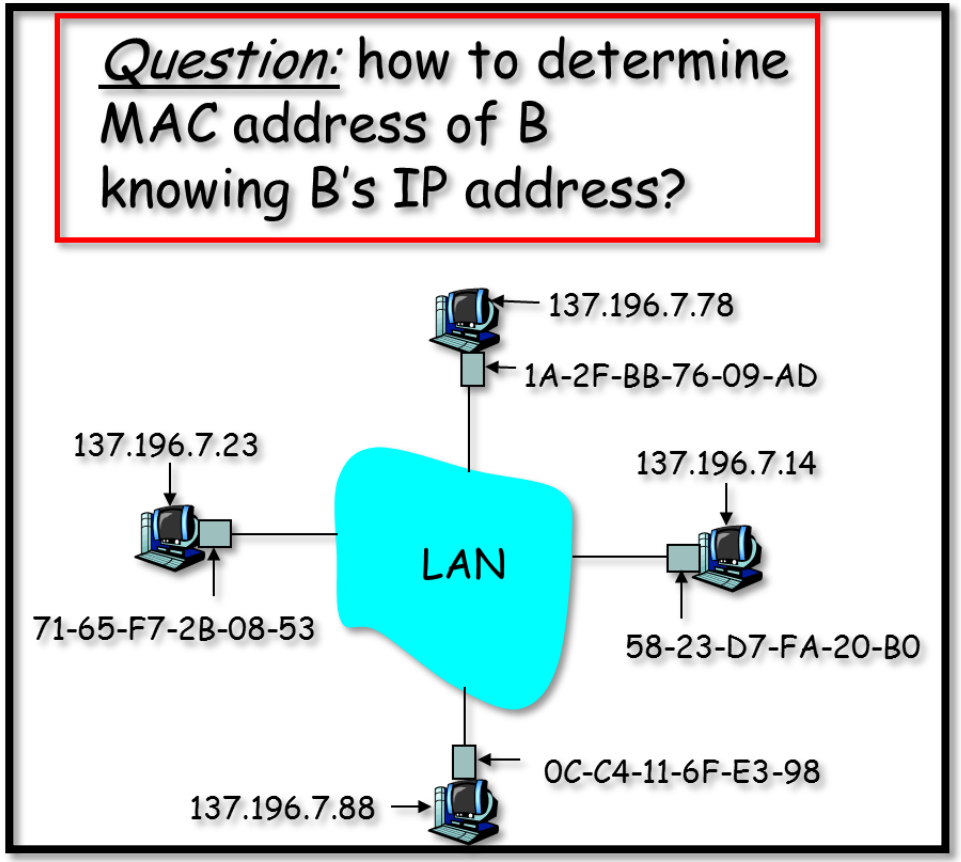
DNS: Domain Name System

- How to map between IP addresses and name ?
  - “name”, e.g., ww.yahoo.com - used by humans
  - IP address (32 bit) - used for addressing datagrams
- Distributed database implemented in hierarchy of many name servers (Why not centralize DNS?)
  - Single point of failure
  - Traffic volume
  - Maintenance
- Top-level domain (TLD) servers:
  - responsible for com, org, net, edu, etc, and all top-level country domains uk, fr, ca, jp.



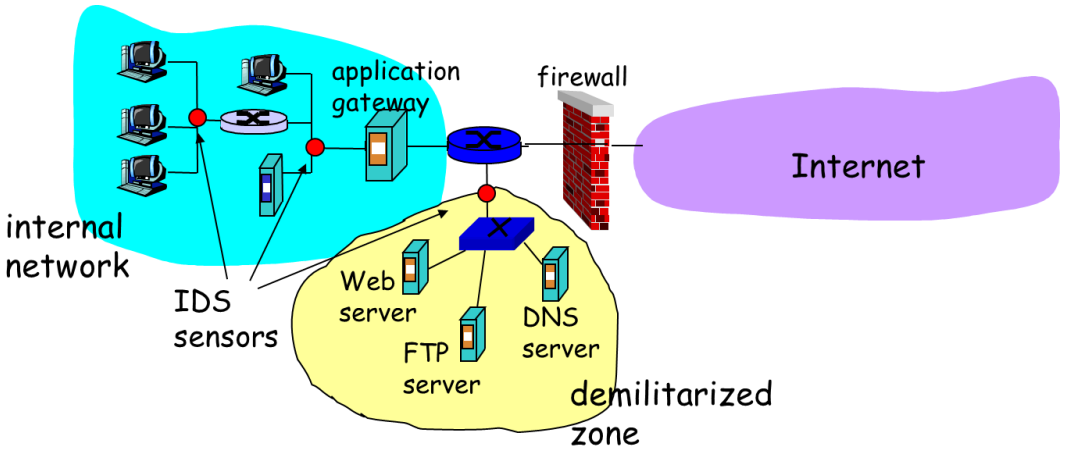
MAC Addresses and ARP

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- analogy:
  - (a) MAC address: like Social Security Number
  - (b) IP address: like postal address
- MAC flat address ➜ portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - address depends on IP subnet to which node is attached
- Each IP node (host, router) on LAN has ARP table
- ARP table: IP/MAC address mappings for some LAN nodes



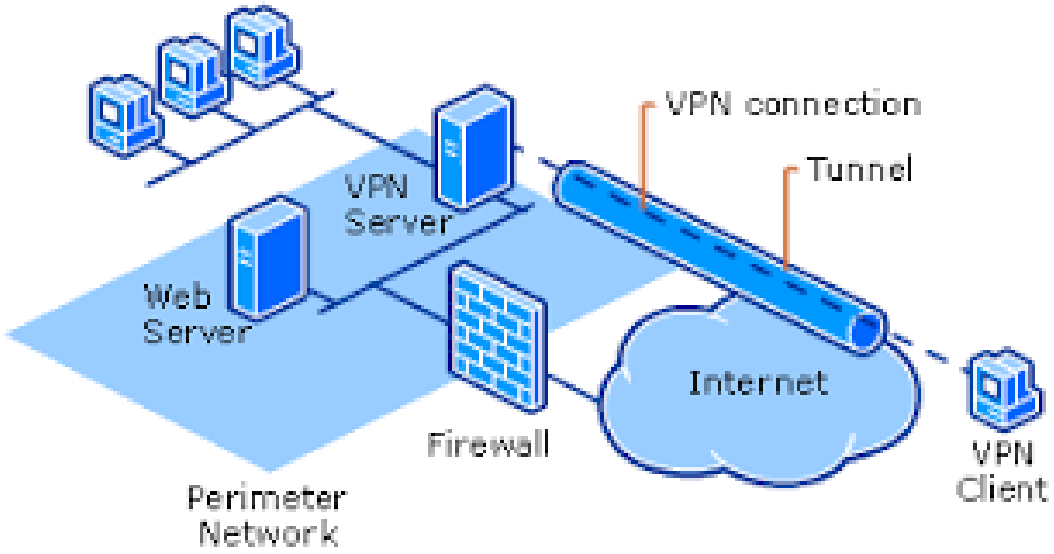
Firewalls

- Firewall: isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.
- Internal network connected to Internet via router firewall
- Router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - …
- example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - all incoming, outgoing UDP flows and telnet connections are blocked.



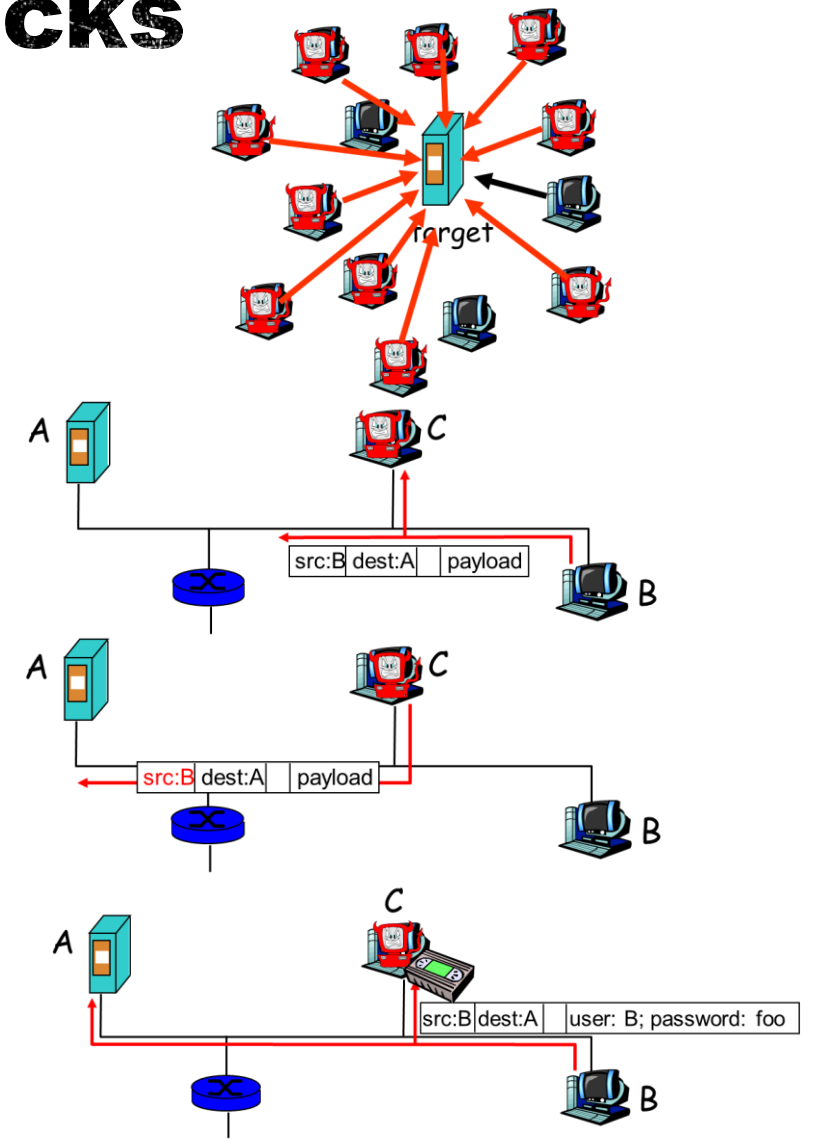
VPN (Virtual Private Network)

- 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. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network
- A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, and traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely



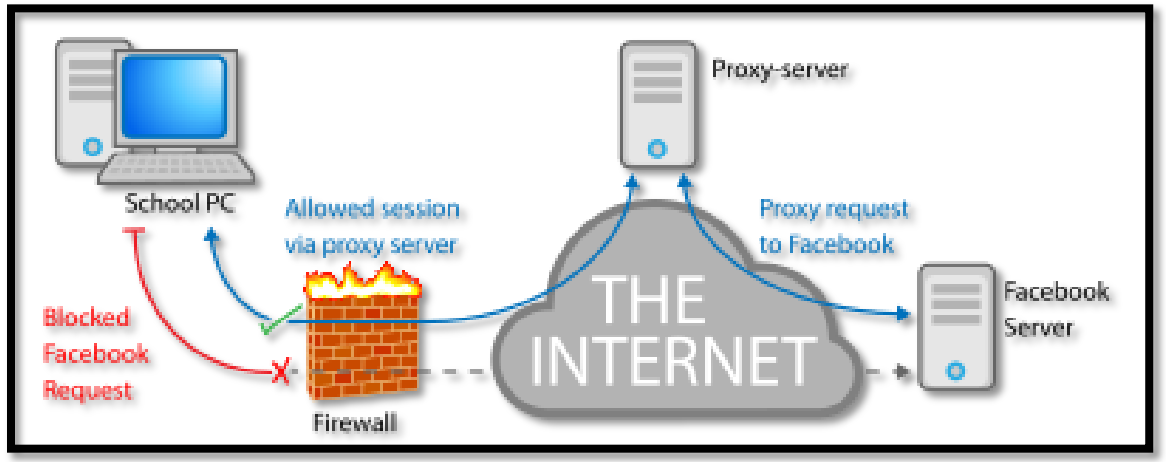
Some Network Security Attacks

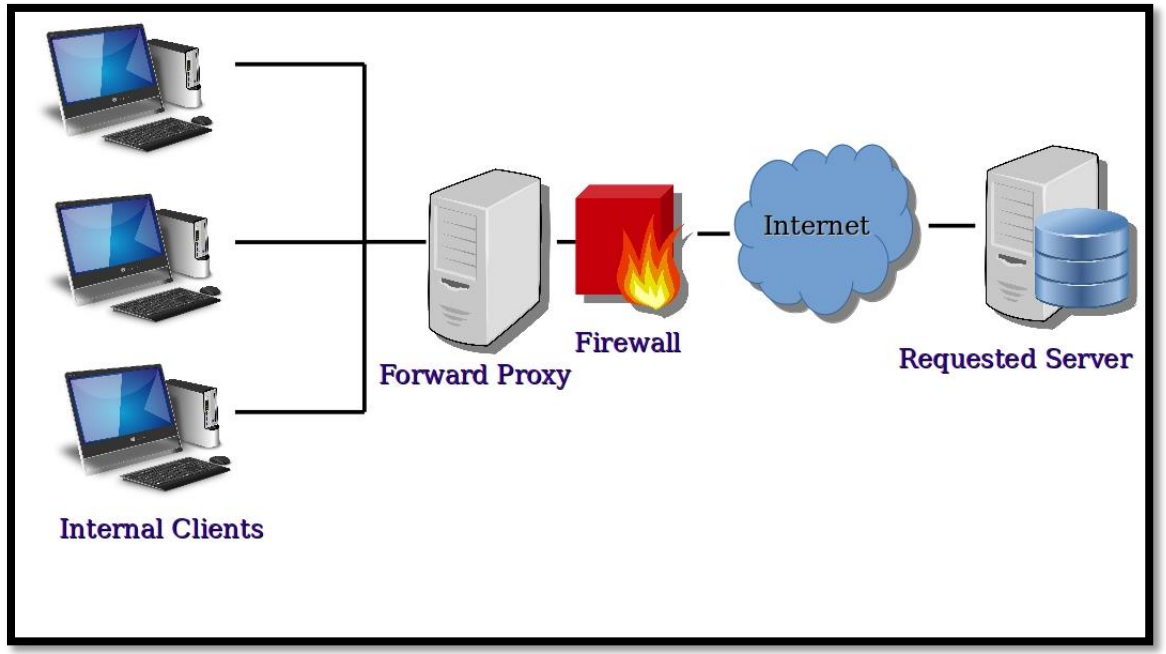
- Denial of service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with fake traffic
- Packet sniffing: broadcast media (shared Ethernet, wireless), network interface reads/records all packets (e.g., including passwords!) passing by.
- IP spoofing: send packet with false source address
- Record-and-playback: sniff sensitive info (e.g., password), and use later.



Proxy Server

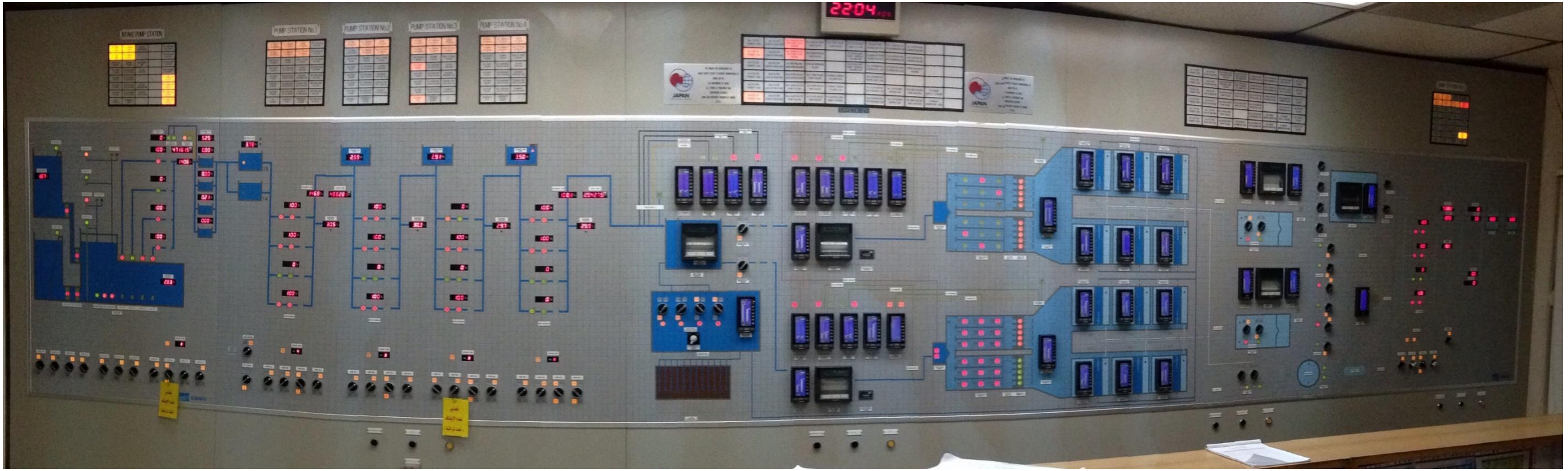
- Proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.
- Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing privacy and may be used to bypass IP address blocking.





Networking Layer Comparison

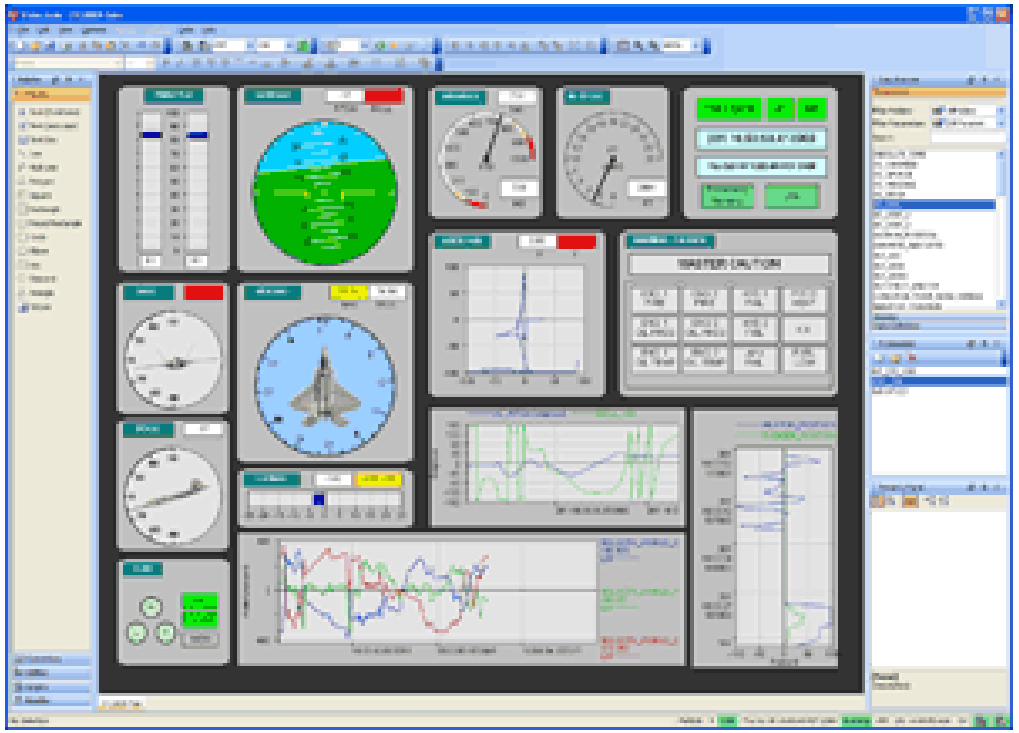
What is SCADA?



- SCADA is an acronym for Supervisory Control and Data Acquisition.
- SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.
- Application area :
  Industrial processes: chemical, power generation and distribution, …
  Nuclear processes: reactors, nuclear waste, ...

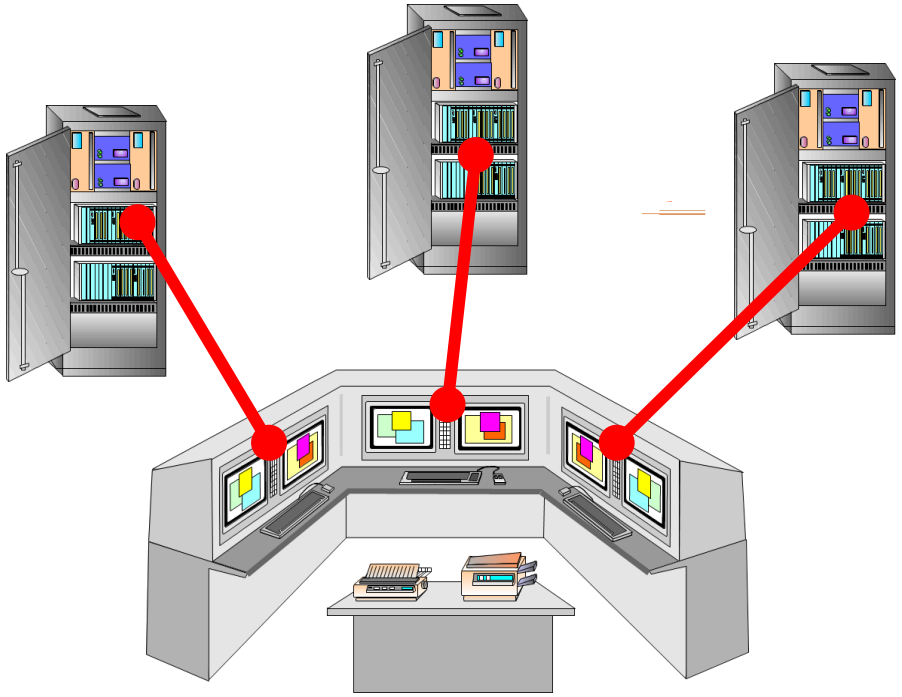
History

- Telemetry is an automated communications process by which measurements are made and other data collected at remote or inaccessible points and transmitted to receiving equipment for monitoring. The word is derived from Greek roots: tele = remote, and metron = measure
- Telemetering information over wire had its origins in the 19th century. One of the first data-transmission circuits was developed in 1845 between the Russian Tsar's Winter Palace and army headquarters.
- In 1970s SCADA systems started with aid of radio communication system



Traditional Control

- Dedicated Consoles
- Point to point communication
- No network
  - No remote access
  - No remote diagnostic

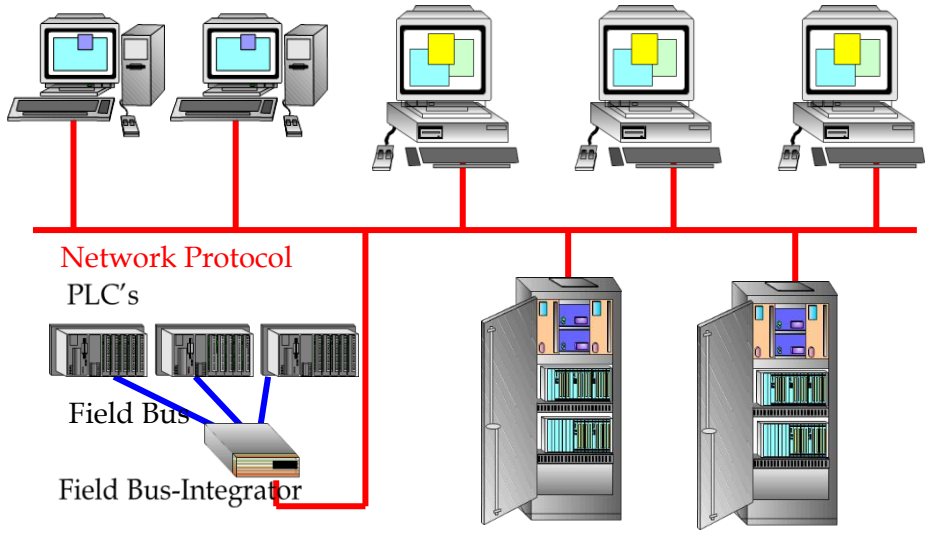


A control system is a device, or set of devices, that manages, commands, directs or regulates the behaviour of other devices or systems

Distributed Control System (DCS)

- **Distributed Control System (DCS)**

is a control system for a process or plant, wherein control elements are distributed throughout the system.



- Advantages:
  - Distributed databases
  - Distributed access
  - Distributed diagnostic
  - Display 'everything everywhere'

- Disadvantages:
  - None of the DCS systems are compatible to each other

- Difficult:
  - Integration of various field bus components

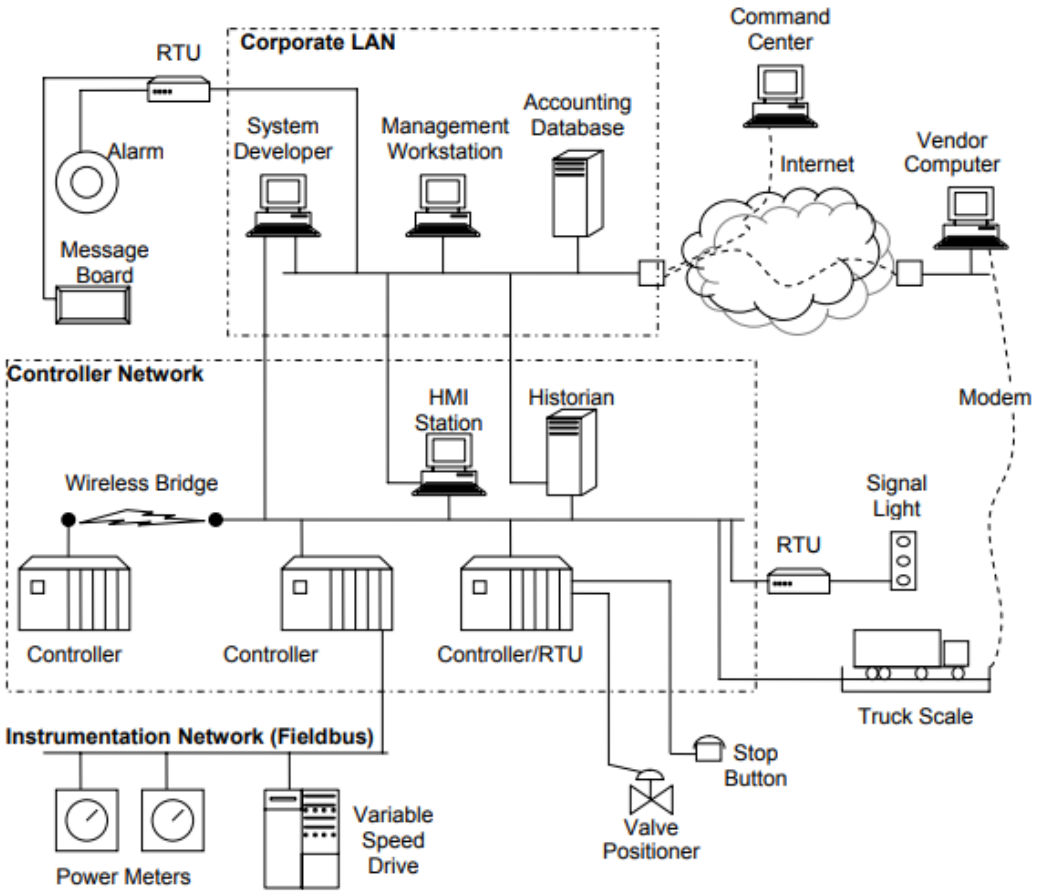
Elements of SCADA

1) Sensors and Actuators

2) Remote Terminal Units (RTUs)
   - Usually PLCs
   - Control a process
   - Data logging and alarm handling
   - Expandable

3) Communication
   - Communications system used to transfer data between:
     - sensors , actuators and control units
     - control units
     - control units and the computers
   - The Communication system can be radio, telephone, cable, satellite.
   - Encode data in protocol format
   - SECURITY: Keep data on closed LAN/WANs
     without exposing sensitive data to the open Internet.

4) Master Terminal Units (MTUs)
   - A central host computer server or servers
     (sometimes called a SCADA Centre or master station.)
   - A collection of standard and/or custom software
   - Usually Includes Human Machine Interface (HMI) software and hardware
     (sometimes called Man Machine Interface (MMI))
   - SCADA Server can be a Web server used for logging and analysing data



Selection of RTU

RTUs need to:

• communicate with all on-site equipment

• Survive an industrial environment. **Rugged construction** and ability to withstand **extremes of temperature and humidity** (it needs to be the most reliable element in your facility).

• Have **sufficient capacity** to support the equipment at a site (though should support expected growth over a reasonable period of time).

• Have a **secure, redundant power supply** for 24/7 working, support battery power and, ideally, two power inputs.

• Have **redundant communication ports** e.g. secondary serial port or internal modem to keep the RTU online even if the LAN fails (multiple communication ports easily support a LAN migration strategy)

• **H**ave **non-volatile memory (NVRAM)** for storing software and/or firmware. New firmware downloadable over LAN to keep RTU capabilities up to date without excessive site visits

• Control local systems by themselves (Intelligent control) according to programmed responses to sensor inputs

• Have a **real-time clock** to accurately date/time stamp reports

• Have a **watchdog timer** to ensure that the RTU restarts after a failure.

Selection of MTU

A SCADA master should display information in the most useful ways to human operators and intelligently regulate managed systems. It should :

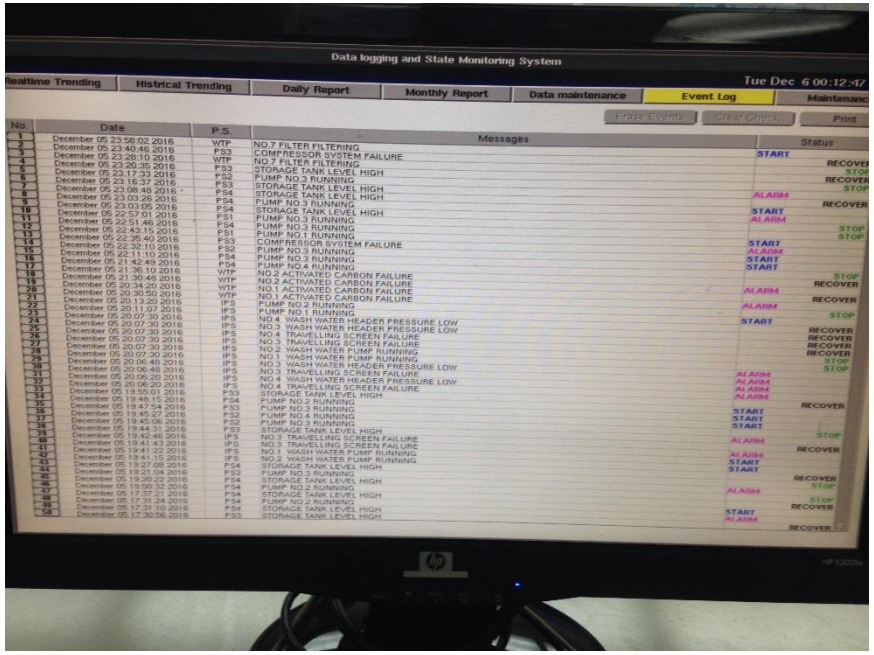
• Have flexible, programmable soft controls to respond to sensor inputs

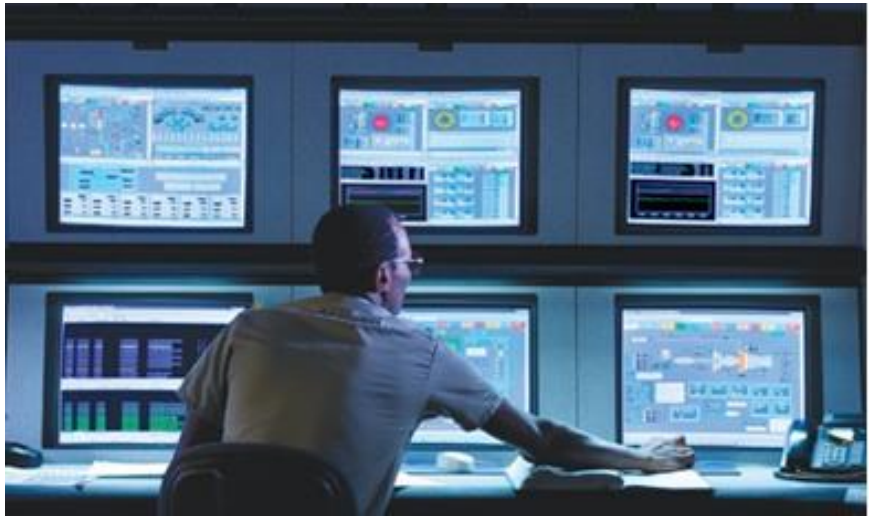
• Allow programming for soft alarms (reports of complex events that track combinations of sensor inputs and date/time statements).

• Automatically page or email directly to repair technicians and provide detailed information display in plain English, with a complete description of what activity is happening and how to manage it.

• Have tools to filter out alarms (to prevents operators from loosing confidence and stop responding even to critical alarms)

• Support multiple backup masters, in separate locations (primary SCADA master fails, a second master on the network automatically takes over, with no interruption of monitoring and control functions)

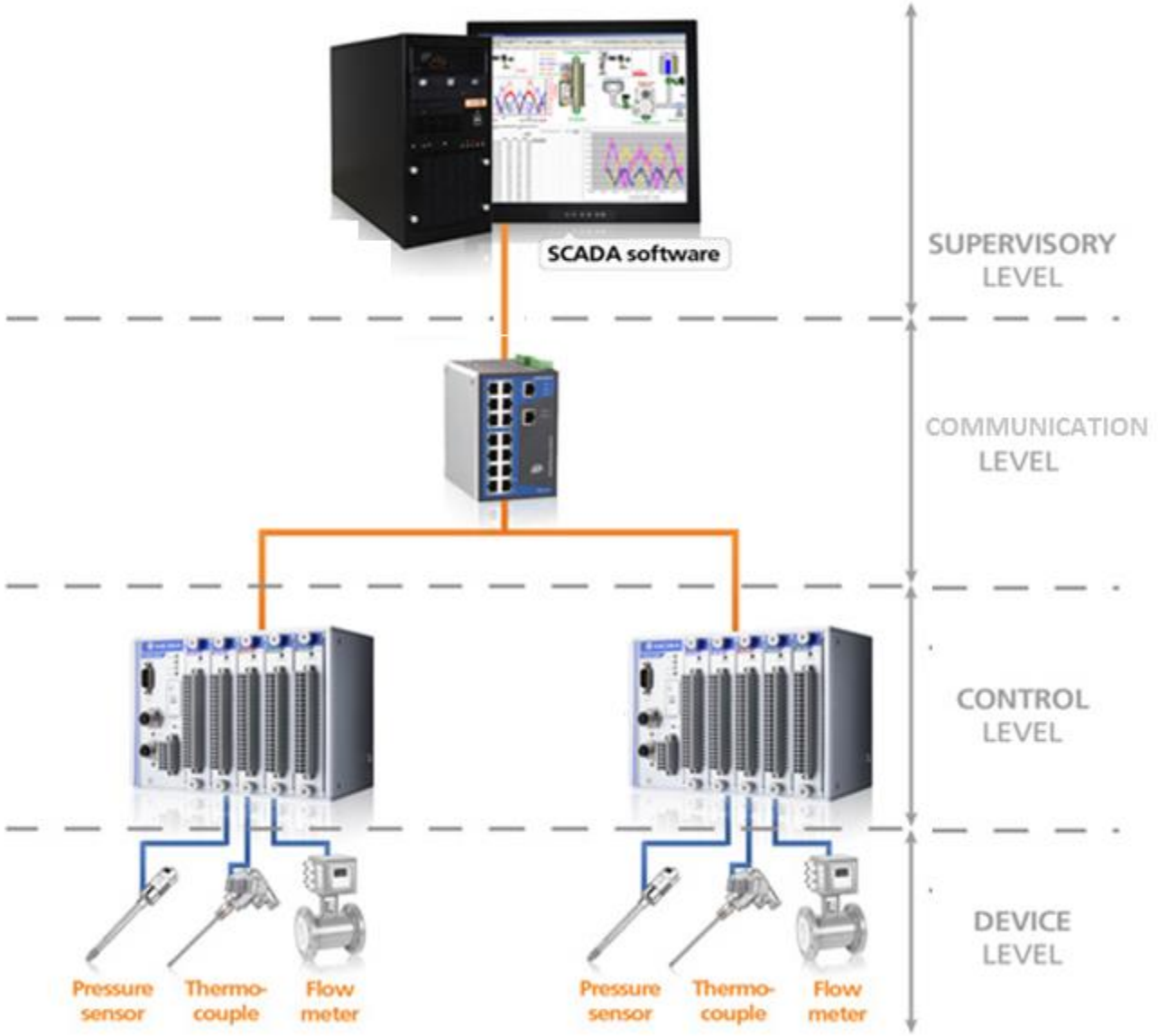




Levels of SCADA

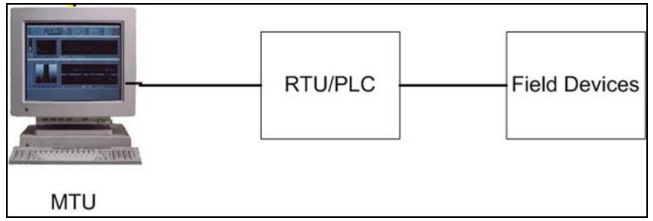
Four levels of SCADA system:

1) Level I – Device Field
   - Sensors
   - Actuators
2) Level II – Control
   - RTUs
   - PLCs
3) Level III – Communication
   - Fiber
   - Radio
   - Protocols
4) Level IV – Supervisory
   - MTU Workstations
   - Servers – Data logging
   - Virtual Private Network
   - Firewall for remote users



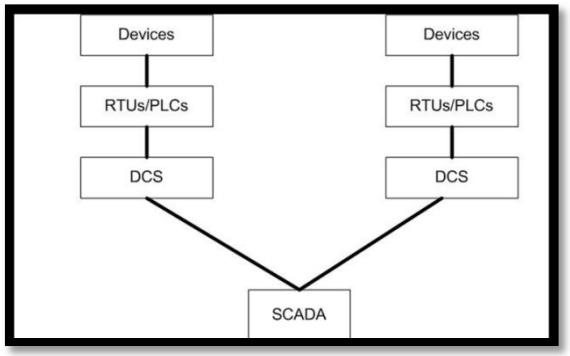
SCADA Generations

Four Generations SCADA systems:



First generation: "Monolithic"

- One machine process
- One RTU and MTU

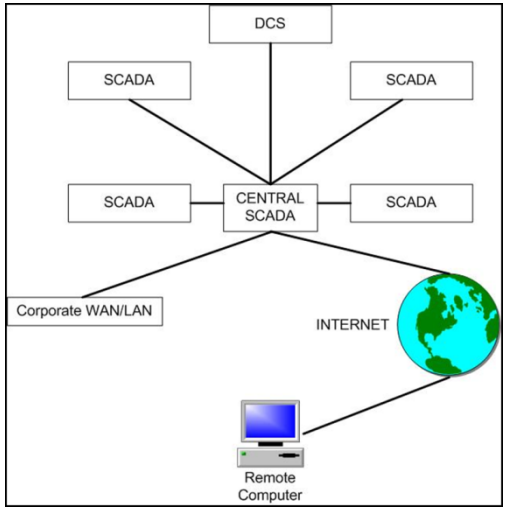


Second generation: "Distributed"

- Multiple RTUs
- DCS

Third generation: "Networked“

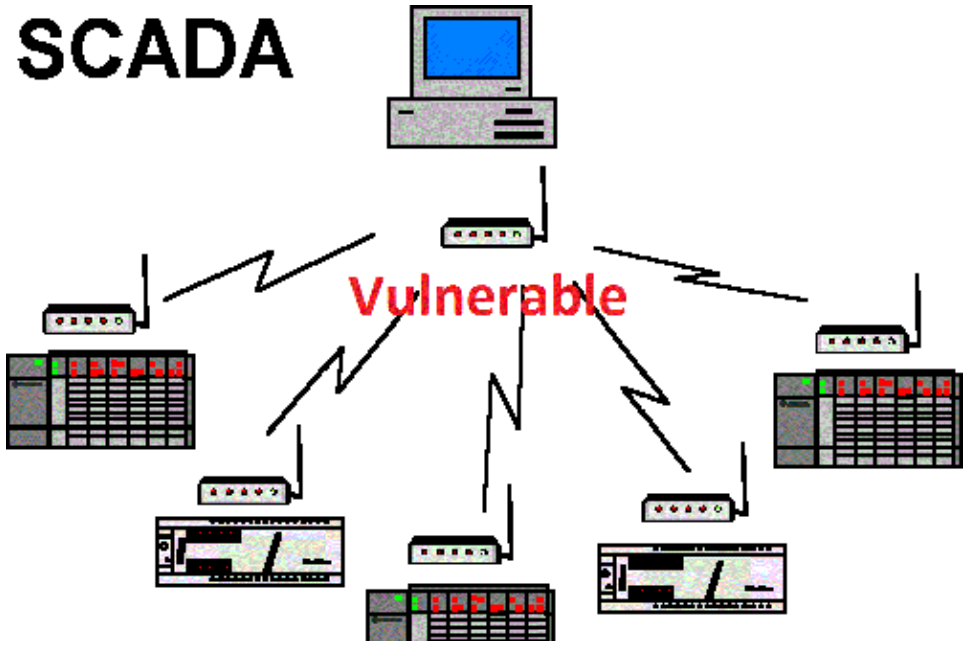
- Multiple SCADA



Fourth generation: "Internet of Things"

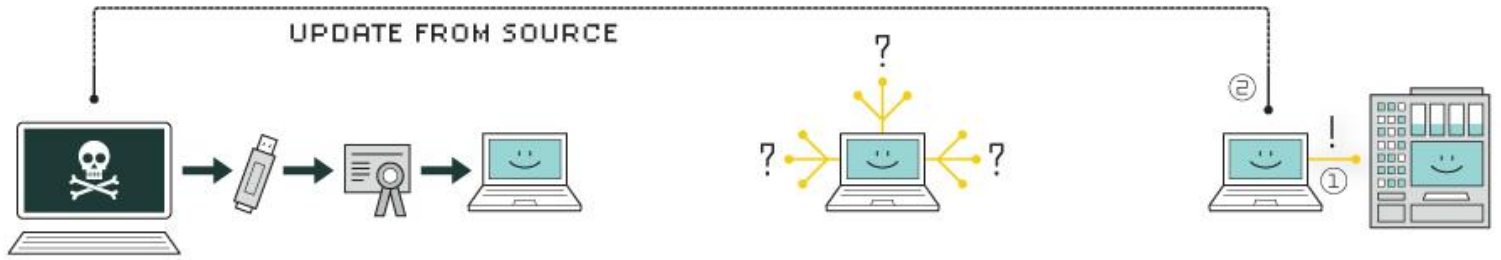
SCADA Security

Description of Attack	Type of Attack	Attack Motive	Impact to Victim
Denial of Service	System Shutdown	Wish to take down server and cause immediate shutdown situation	SCADA Server locks up and must be rebooted. When SCADA Server comes back on-line, it locks up again. Operations can no longer monitor or control process conditions, and the system will ultimately need to be shut down
Delete System Files (Low-level format on all local drives)	System Shutdown	Wish to take down server and cause immediate shutdown situation	Critical Server and SCADA files are lost and operations can no longer monitor process or control plant or facility
Take Control of SCADA System	Gain Control	Gain control of SCADA System to impact damage on industrial systems, possibly causing environmental impact, and damage corporate identity through public exposure	Highest impact, since attacker can then manually override safety systems, shut down the system, or takes control of the plant operational conditions.
Log Keystrokes, Usernames, Passwords, System Setpoints, and any Operational Information	Information Mining	Gain Information for future attacks or satisfy curiosity	Lower immediate impact, but information gained can be used for future attacks.



Stuxnet

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

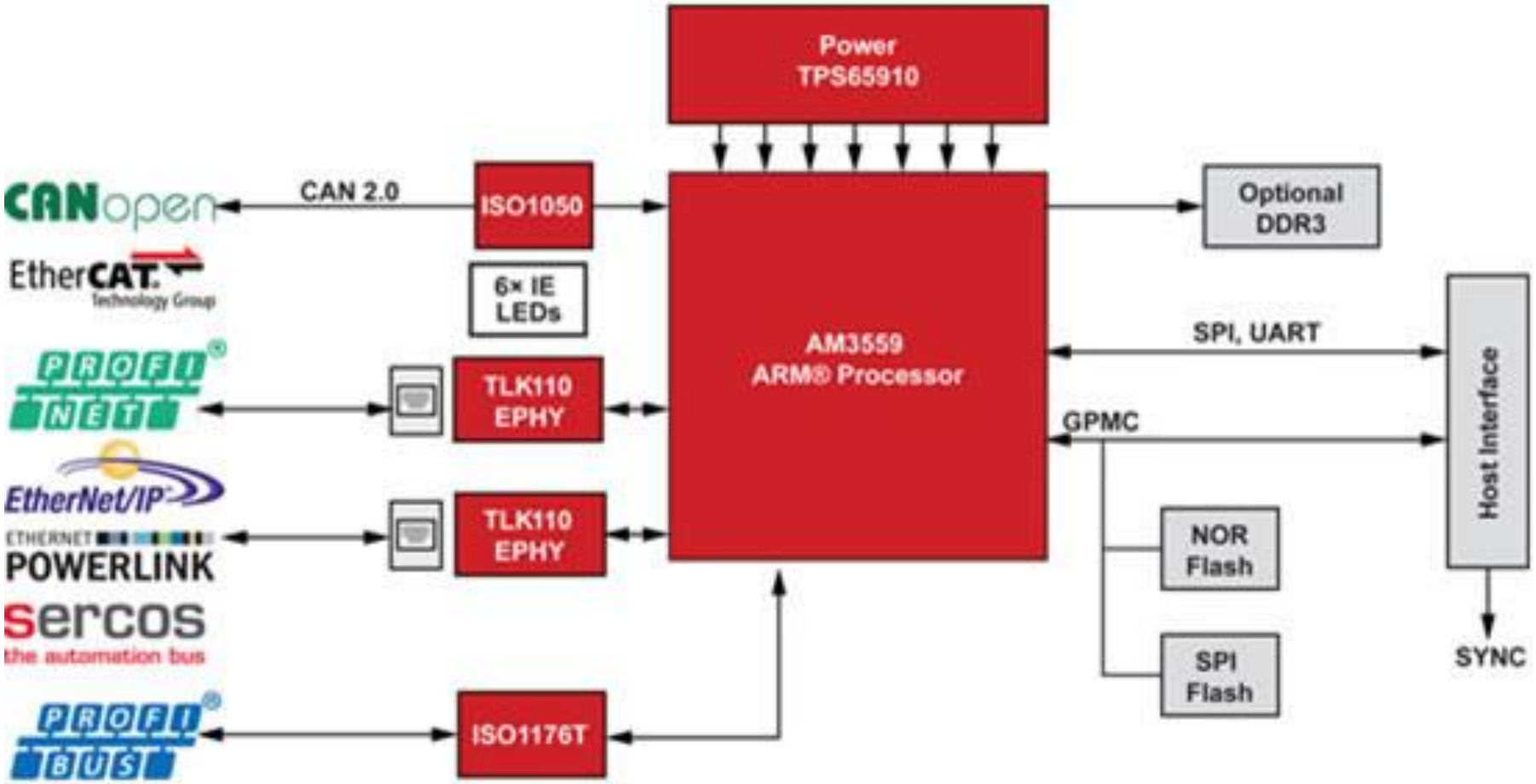
4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

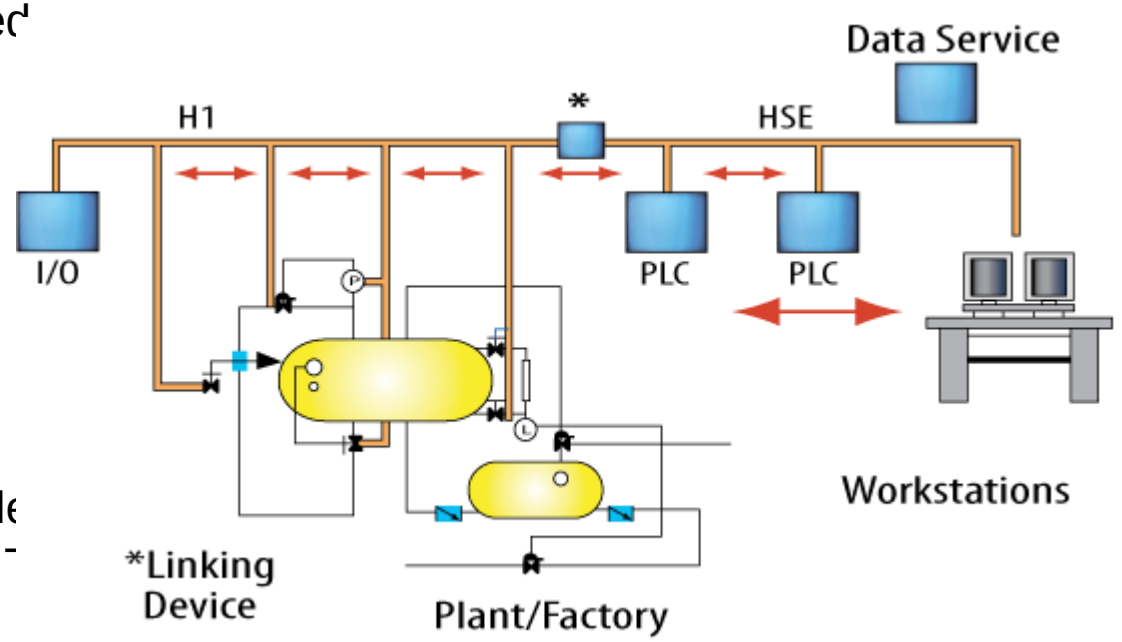
PLC Communication Protocols

- Fieldbus
- MODBUS
- Profibus
- TCP/IP



Fieldbus

- Fieldbus is the name of a family of industrial computer network protocols used for real-time distributed control, standardized as IEC 61158.
- The IEC 61158 standard has eight different protocol sets called "Types" as follows:
  - Type 1 Foundation Fieldbus H1
  - Type 2 ControlNet
  - Type 3 PROFIBUS
  - Type 4 P-Net
  - Type 5 FOUNDATION fieldbus HSE (High Speed Ethernet)
  - Type 6 SwiftNet (a protocol developed for Boeing, since withdrawn)
  - Type 7 WorldFIP
  - Type 8 Interbus
- IEC 61158 consists of the following parts, under the general title Digital data communications for measurement and control - Fieldbus for use in industrial control systems:
  - Part 1: Overview and guidance for the IEC 61158 series
  - Part 2: Physical Layer specification and service definition
  - Part 3: Data Link Service definition
  - Part 4: Data Link Protocol specification
  - Part 5: Application Layer Service definition
  - Part 6: Application Layer Protocol specification

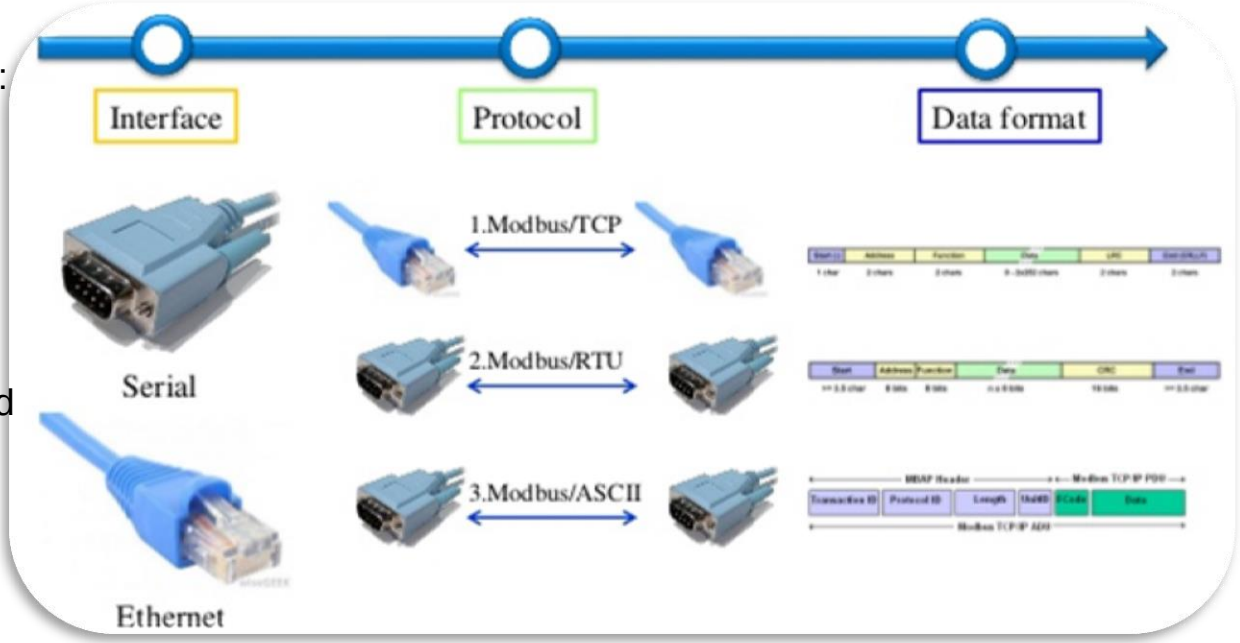


MODBUS

- Modbus is a serial communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs). Simple and robust, it has since become standard communication protocol, and it is now a commonly available means of connecting industrial electronic devices.

The main reasons for the use of Modbus in the industrial environment are:

- developed with industrial applications in mind
- openly published and royalty-free
- easy to deploy and maintain
- moves raw bits or words without placing many restrictions on vendors



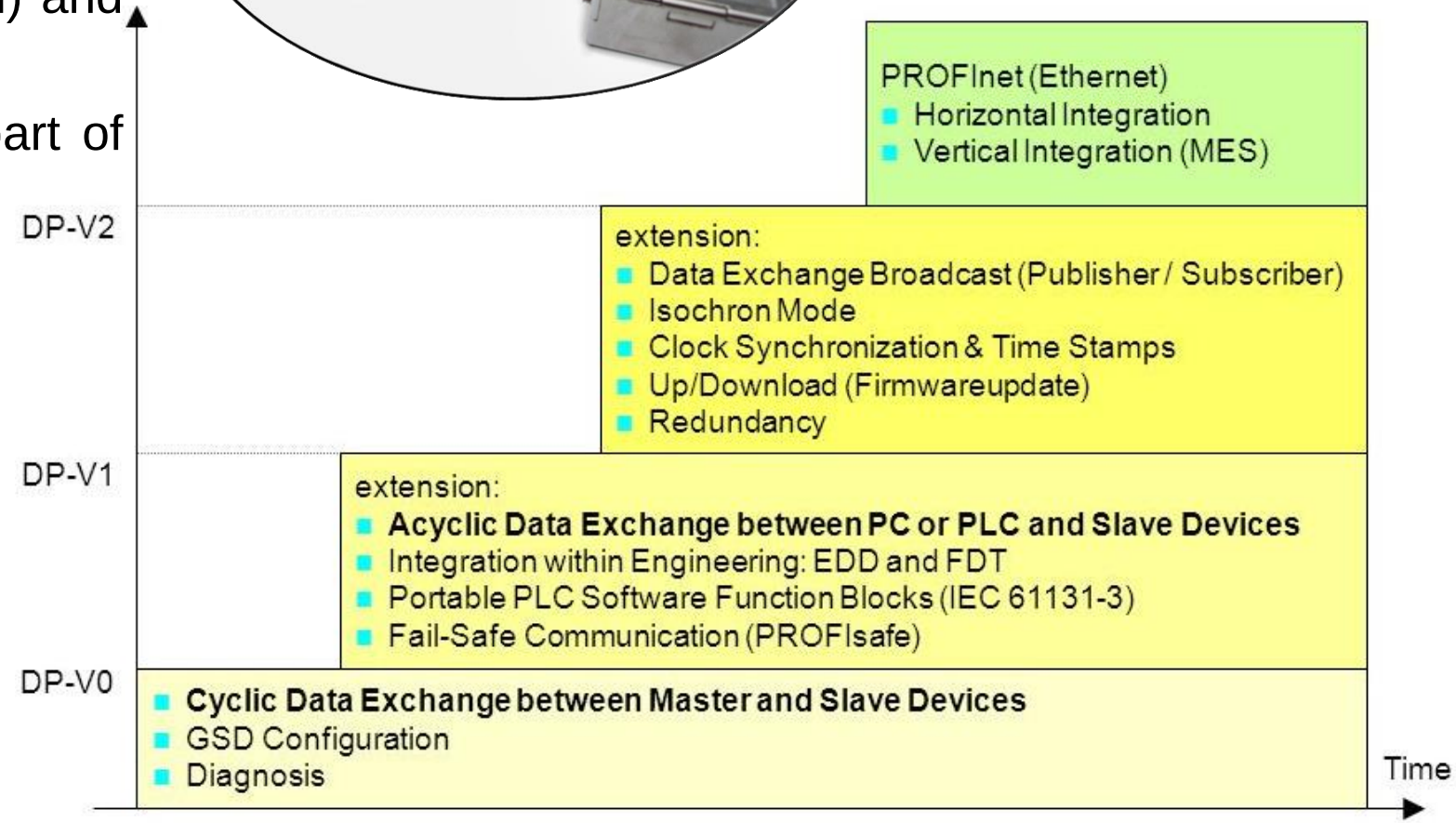
- Versions of the Modbus protocol exist for serial port and for Ethernet and other protocols that support the Internet protocol suite. There are many variants of Modbus protocols:
  - Modbus RTU — This is used in serial communication & makes use of a compact, binary representation of the data.
  - Modbus ASCII — This is used in serial communication & makes use of ASCII characters for protocol communication. Modbus
  - TCP/IP or Modbus TCP — This is a Modbus variant used for communications over TCP/IP networks, connecting over port 502.
  - Modbus over UDP — Some have experimented with using Modbus over UDP on IP networks, which removes the overheads required for TCP

Profibus

- PROFIBUS (Process Field Bus) is a standard for fieldbus communication in automation technology and was first promoted in 1989 by BMBF (German department of education and research) and then used by Siemens.
- PROFIBUS is openly published as part of IEC 61158.

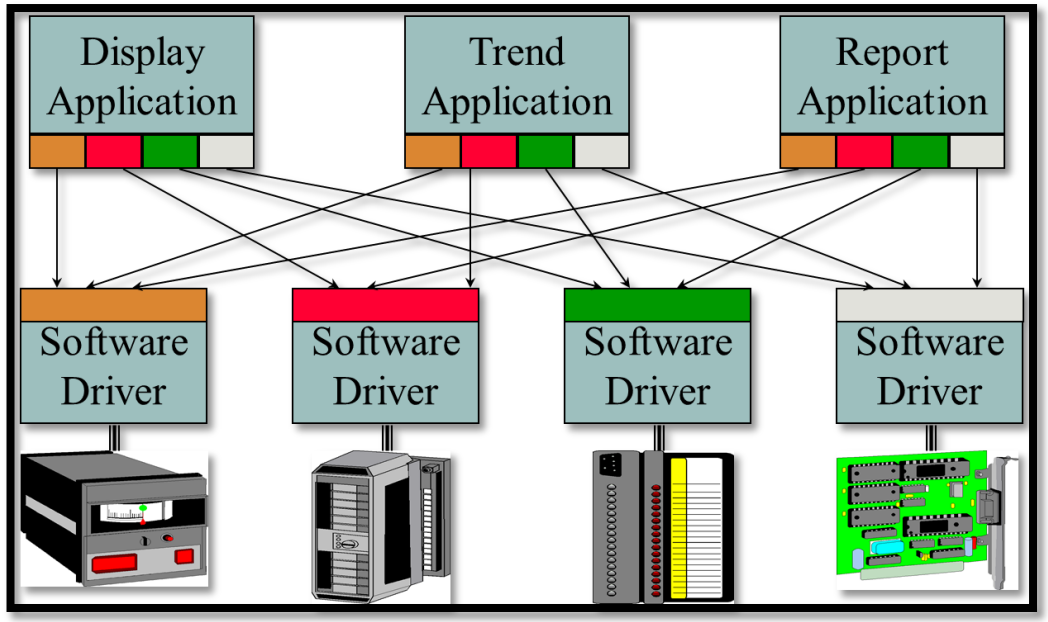
PROFIBUS Protocol (OSI reference model)

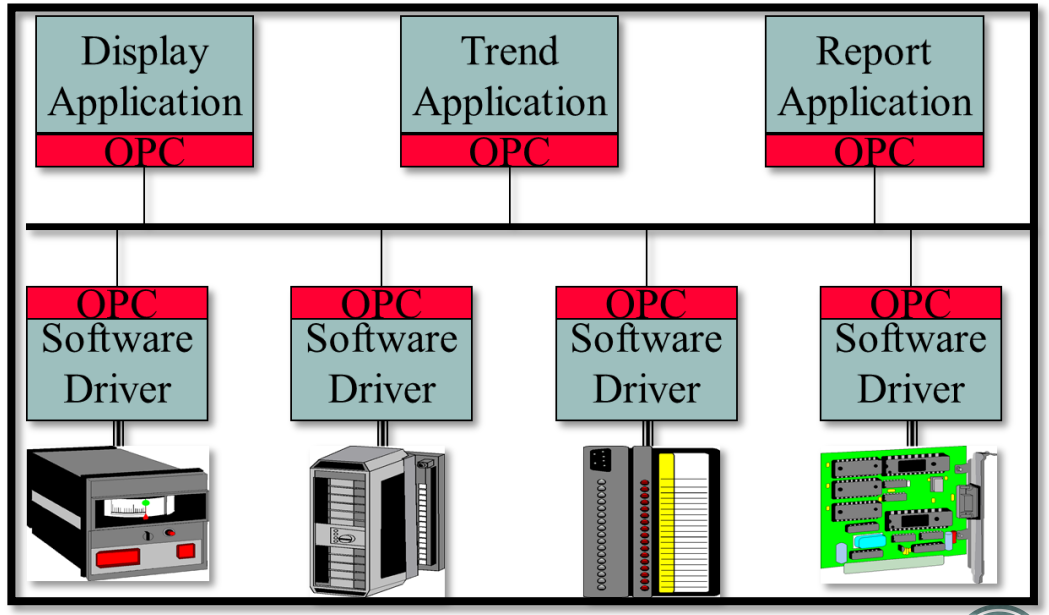
OSI-Layer		PROFIBUS			
7	Application	DPV0	DPV1	DPV2	Management
6	Presentation	--			
5	Session				
4	Transport				
3	Network				
2	Data Link	FDL			
1	Physical	EIA-485	Optical	MBP	

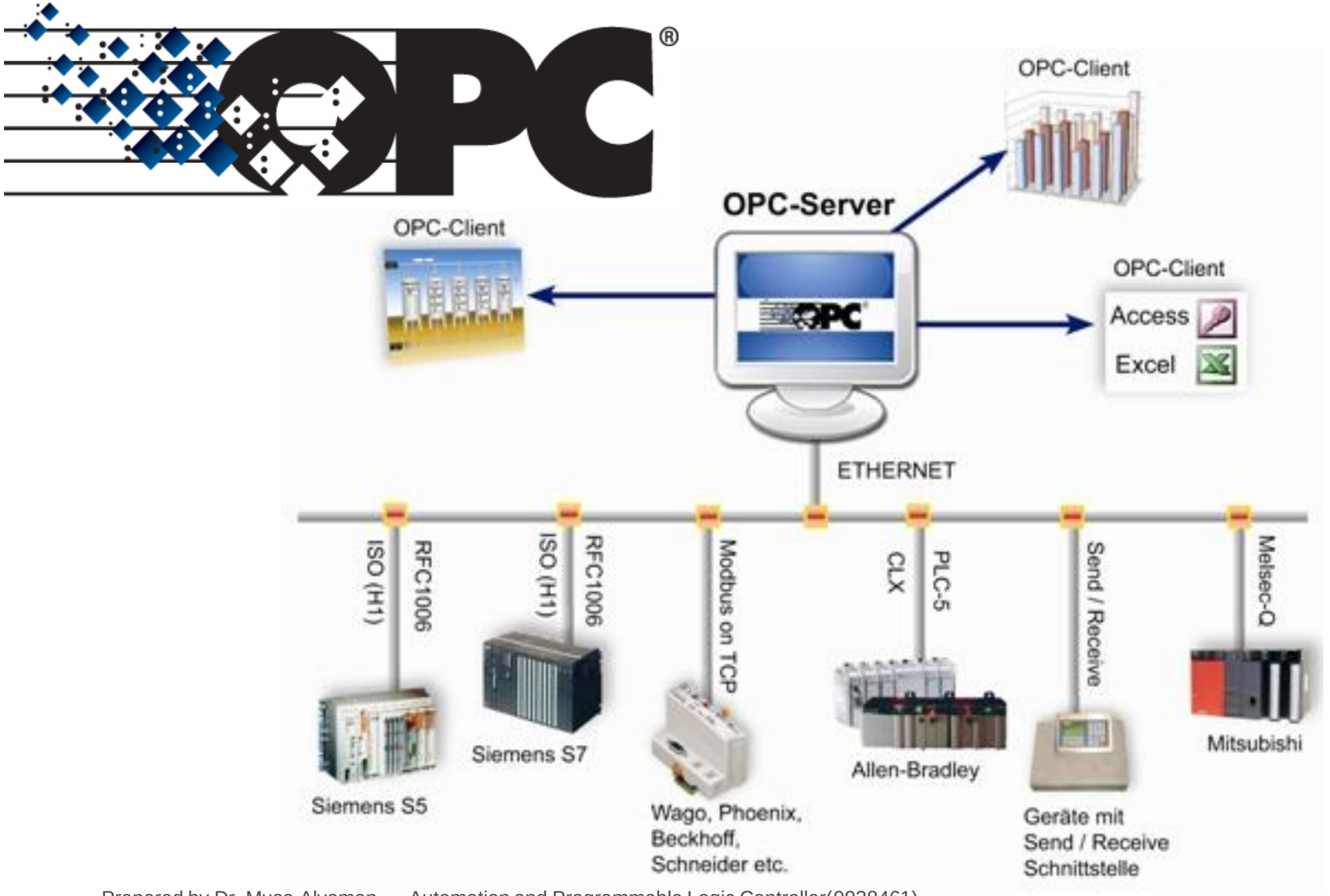


OPC

- Open Platform Communications (OPC) is a series of standards and specifications for industrial telecommunication.
- Originally the standard started in 1996 under the name OLE for Process Control (Object Linking and Embedding for Process Control).
- OPC specifies the communication of real-time plant data between control devices from different manufacturers.
- OPC Foundation changed the name to Open Platform Communications in 2011, to reflect the applications of OPC technology for applications in building automation, discrete manufacturing, process control and many others.
- The OPC Specification was based on the OLE, COM, and DCOM (Distributed Component Object Model) technologies developed by Microsoft for the Microsoft Windows operating system family.






OPC-Client
OPC-Server
OPC-Client
OPC-Client
Access
Excel
ETHERNET
ISO (H1)
RFC1006
ISO (H1)
RFC1006
Modbus on TCP
CLX
PLC-5
Send / Receive
Melsec-Q
Siemens S5
Siemens S7
Wago, Phoenix,
Beckhoff,
Schneider etc.
Allen-Bradley
Geräte mit
Send / Receive
Schnittstelle
Mitsubishi

position is July 11, 2015 at 16:00
anan-Zarqa (Jordan).
s global programs can be found at www.mcc.gov.
employer

Employment Opportunity

A wholly owned subsidiary of a leading international company is looking to recruit a highly skilled and active candidate to fill in the position of **Automation and Instrumentation Field Engineer.**

The main duties and responsibilities for this post entail:

- ✓ Responsible for support, maintenance, development and change management of PLC/SCADA system and on-line instrumentation.
- ✓ Work in a coordinated and timely manner with all the staff for support, maintenance and development for all sites where changes in PLC are done.
- ✓ Provide input to the Capital Works Program for SCADA and Telemetry assets.
- ✓ Maintain and repair on-line instrumentation.
- ✓ Maintain standards for Automation.
- ✓ Manage Risk with respect to Automation and Instrumentation.

Technical Competencies:

1. Tertiary or Post Trade Qualifications in an engineering discipline related to Automation or Instrumentation and Control Systems.
2. Experience with SCADA platforms including IP data communication system particularly Rockwell Automation would be of benefit.
3. Modern PLC programming experience with high level programming platform complying to IEC 6113-3. Experience with Rockwell RS Logix 5000 would be highly regarded.
4. Experience in the maintenance of on-line instrumentation is required.
5. A minimum of five years experience in the above.
6. Work in English and Arabic Languages.

We offer an attractive compensation package plus benefits. Interested applicants who have the right credentials are encouraged to apply. All applications will be handled in strict confidence and only those qualified will be contacted.

Please send your CV to the following address: recruit.exec.assistant@gmail.com