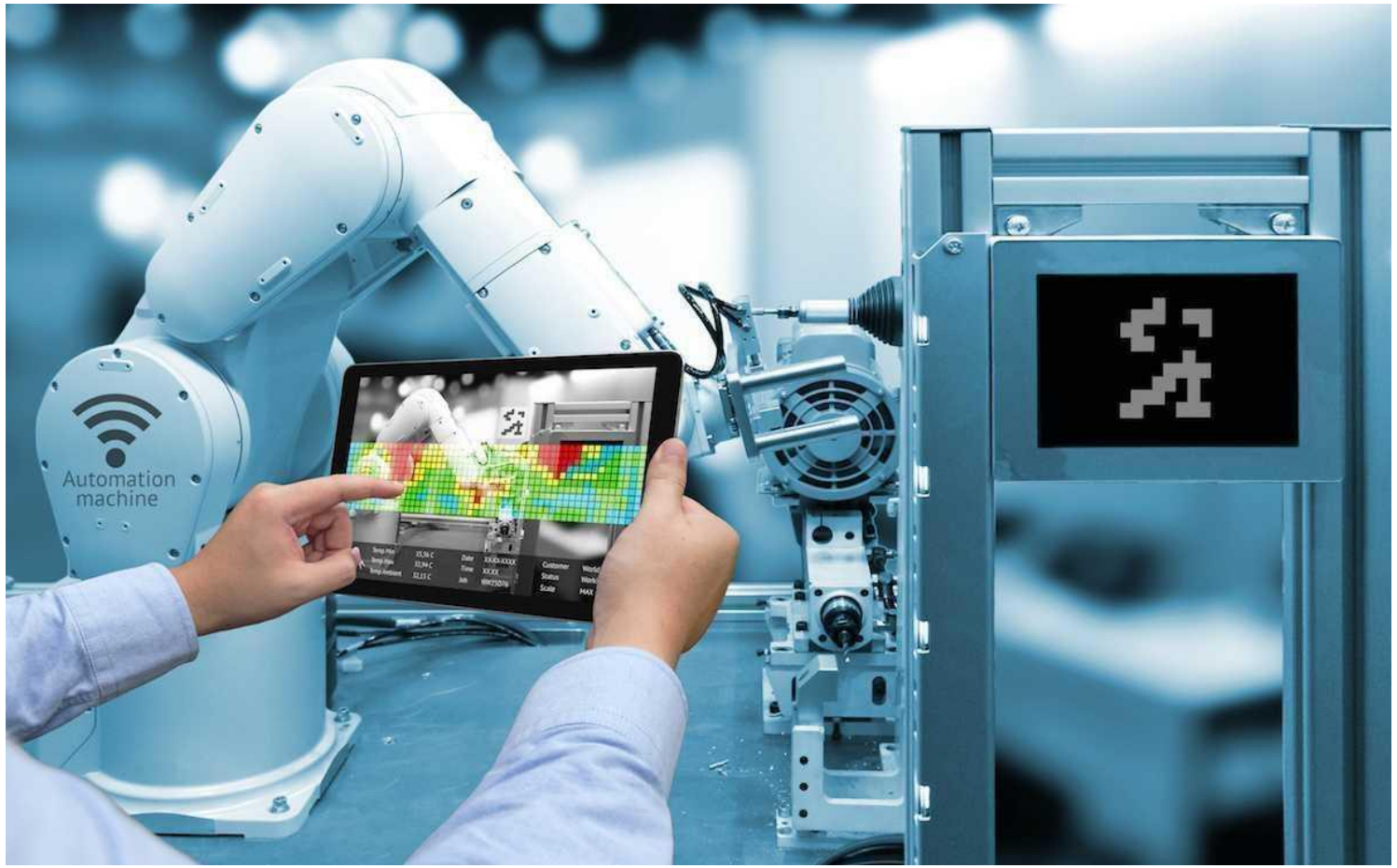
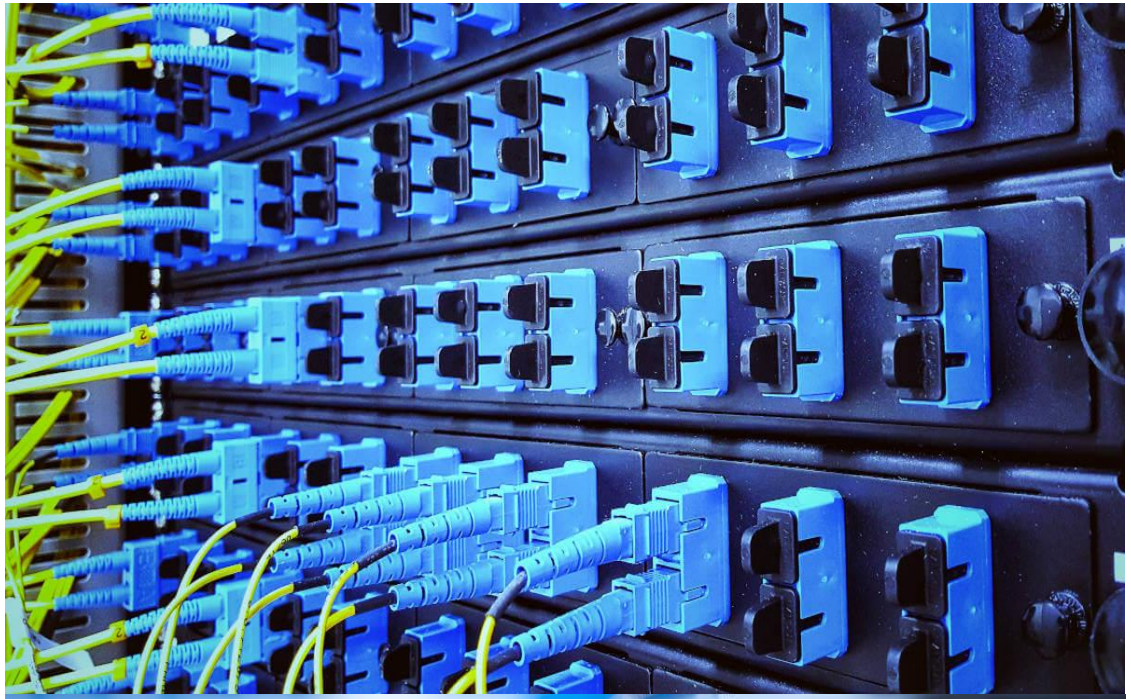
20IS709
Communication Systems For Industrial Networking

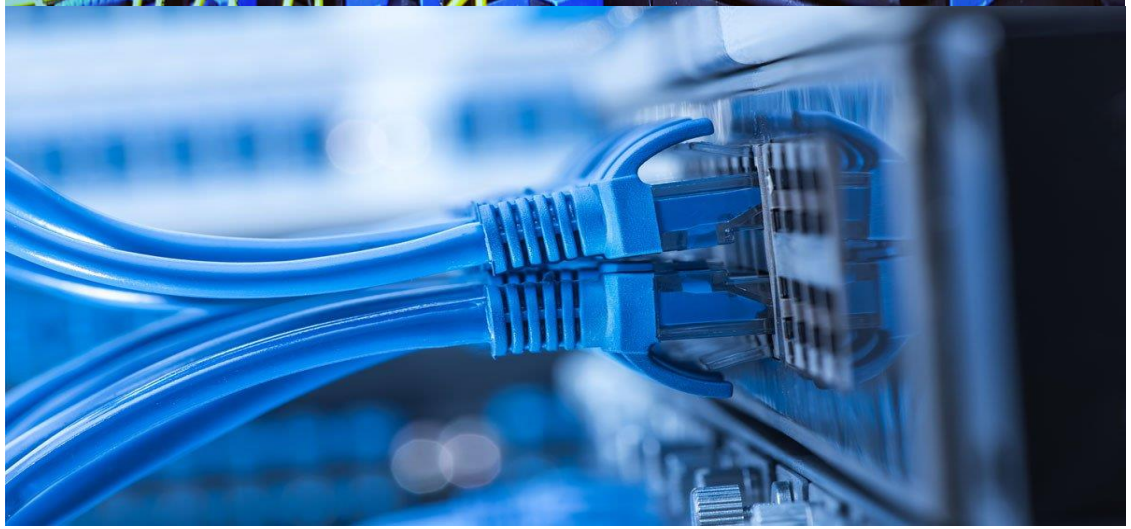


Internet Protocol

Internet Protocol

- Most Ethernet networks use Internet protocols such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) and Internet Protocol (IP).
- Provide defined and well-supported methods - flow control and flexible addressing and routing of messages.
- Messages that travel on the Internet must use IP.
- TCP and UDP are designed to work along with IP, local communications that use TCP or UDP also use IP.





Connecting to the Internet

- To communicate over the Internet, a computer must have three things:
  - an IP address that identifies the computer on the Internet
  - the ability to send and receive IP datagrams, and
  - a connection to a router that can access the Internet
- An Internet Service Provider (ISP) can provide one or more IP addresses and a connection to a router that can communicate over the Internet.
- A computer that hosts a Web page has different requirements than a computer used only to request Web page.
- Internet communications - client and server
- Web browsers are clients
- Browser's Address (such as http://www.abcd.com or http://192.168.111.1) identifies the requesting resource or the server

Technologies for Connecting

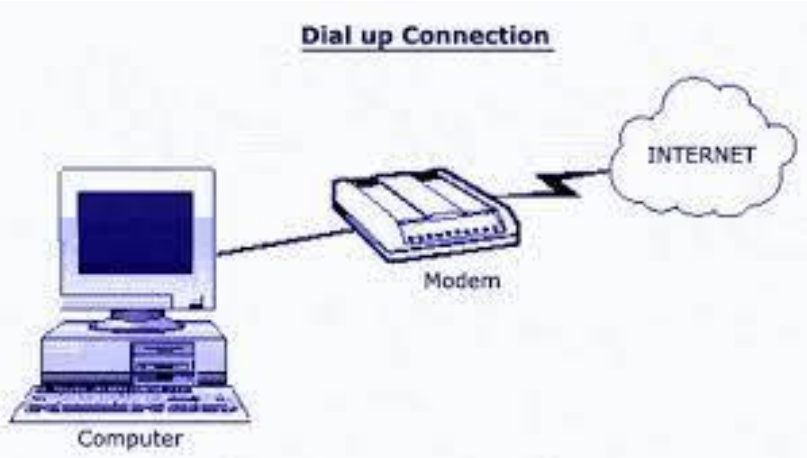
- Ways to connect to the Internet - dial-up connections on phone lines, Digital Subscriber Line (DSL), an Integrated Services Digital Network (ISDN) line, or a cable modem, Satellite connections.

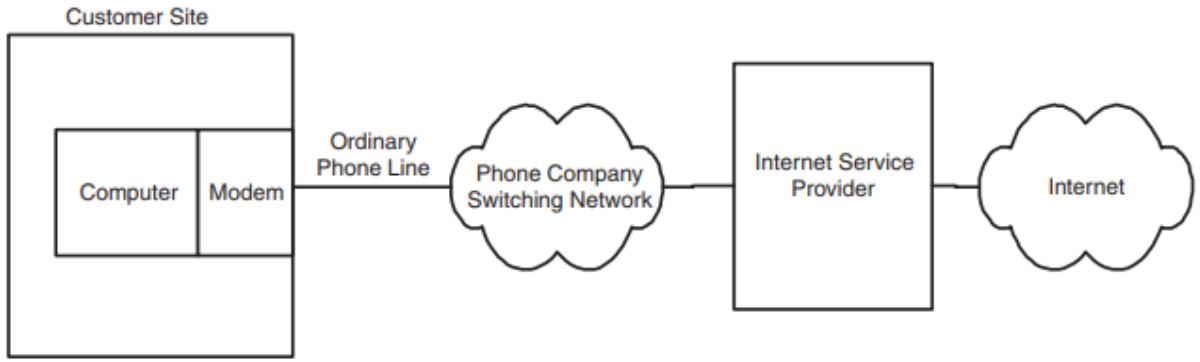
Access Type	Downstream Speed (kb/s, typical maximum)	Upstream Speed (kb/s, typical maximum)	Transmission Medium
Dial up	56	56	phone line
ADSL	1500	384	phone line
SDSL	2000	2000	phone line
BRI ISDN	128	128	phone line
PRI ISDN	1500 (23 channels)	1500 (23 channels)	phone lines
Cable modem	1500, shared	384, shared	TV cable
Satellite	500	50	wireless

Technologies for Connecting

Dail up

- Modem provides an interface between a computer that wants to access the Internet and an ordinary phone line



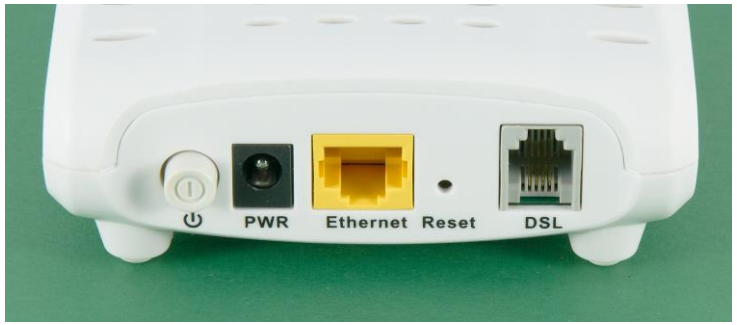


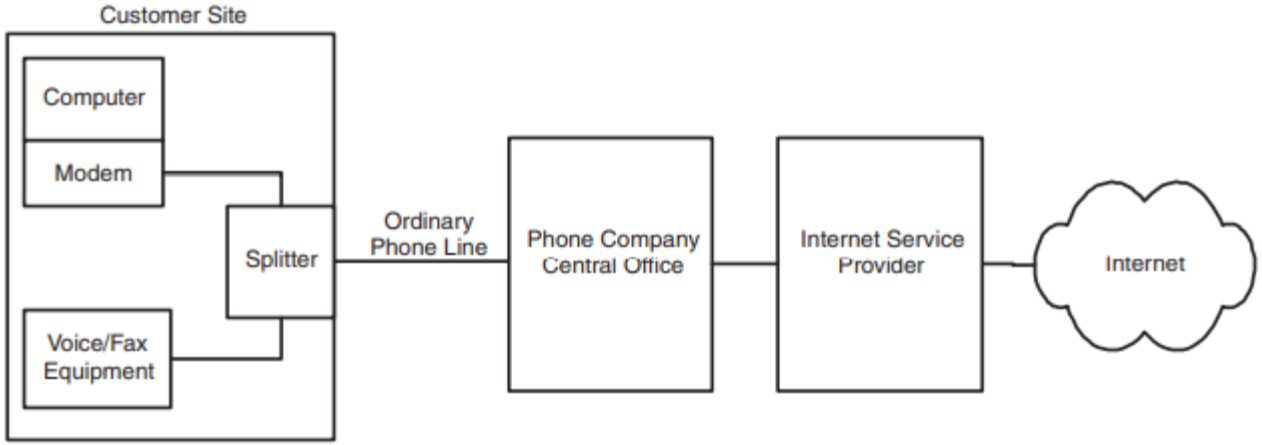
- Computer uses the Point-to-Point Protocol (PPP) to manage the modem connection and to send and receive IP datagrams over the serial link
- Maximum speed of 56 kilobits per second (kbps).
- Suitable for data loggers

Technologies for Connecting

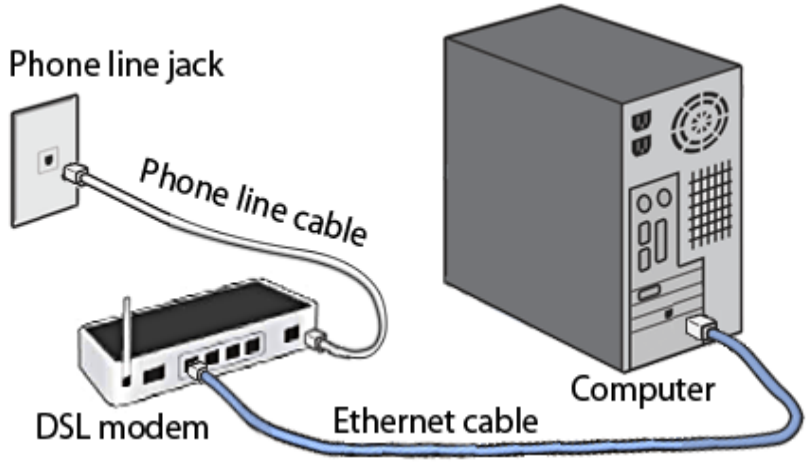
Digital Subscriber Line (DSL)

- Carry voice and Internet communications at the same time.





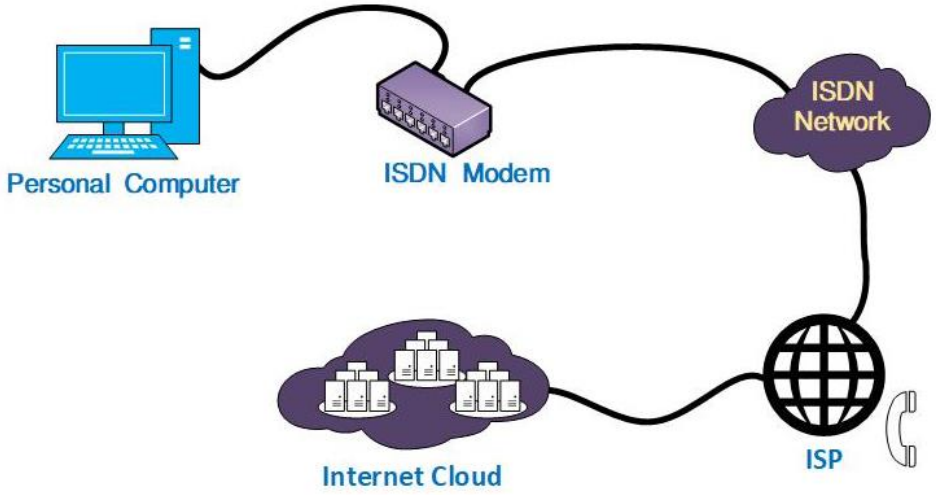
- In upstream direction, a splitter combines phone and Internet traffic on a single pair of wires.
- In downstream direction, the splitter routes the phone and Internet traffic onto the appropriate wires inside the customer's premises.
- Use Point-to-Point Protocol over Ethernet (PPPoE) - requires logging on with a user name and password
- ADSL - 1.5 Mb/s downstream (now 8 Mbps) and 384 kb/s upstream (now 448 kbps).

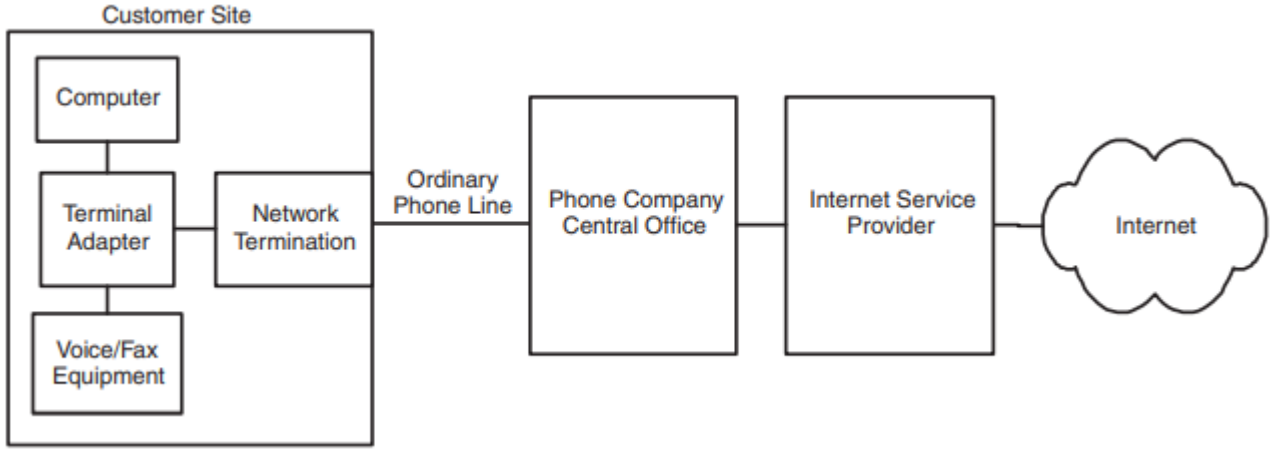


Technologies for Connecting

Integrated Services Digital Network (ISDN)

- Can use conventional phone lines
- Two channels - carry voice and data



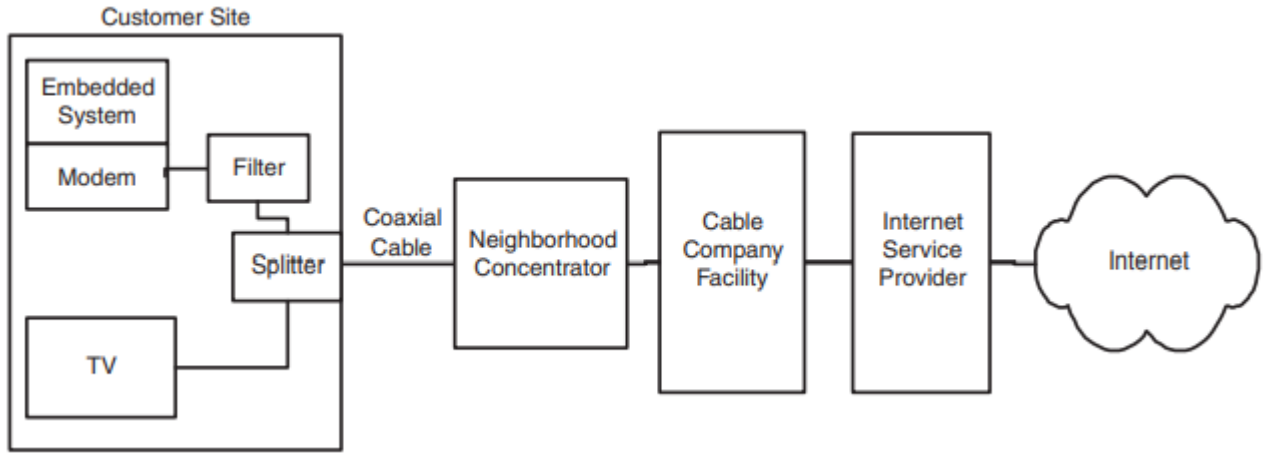


- With Basic Rate Interface (BRI) ISDN, the phone line carries two 64-kb/s “B” channels that can be combined for a single 128-kb/s connection - separate lower-speed “D” channel carries signaling information (16 kbps).
- Primary Rate Interface (PRI) ISDN has 23 channels and speeds of up to 1.544 Mb/s

Technologies for Connecting

Cable Modem

- Doesn’t use phone lines, but instead uses a connection to a cable-TV provider that offers Internet access - same cable can carry TV broadcasts and Internet traffic

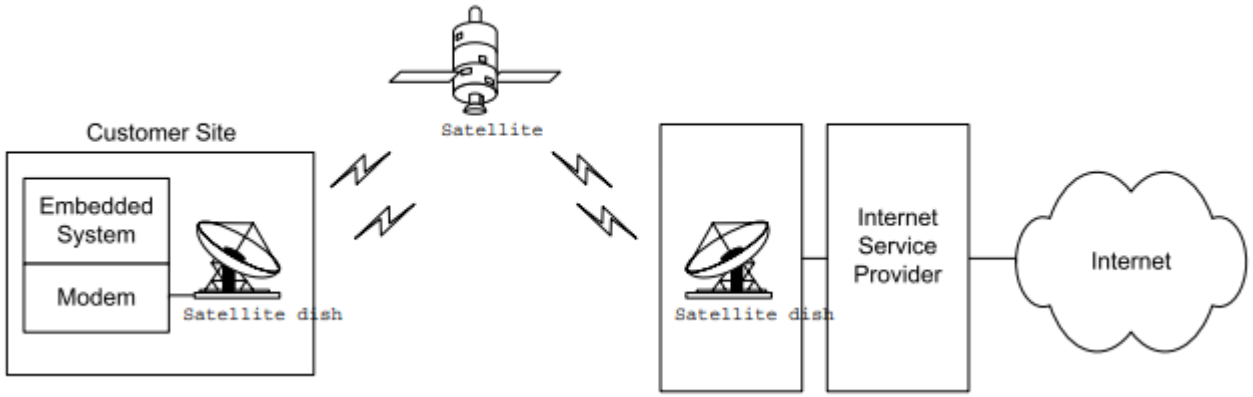


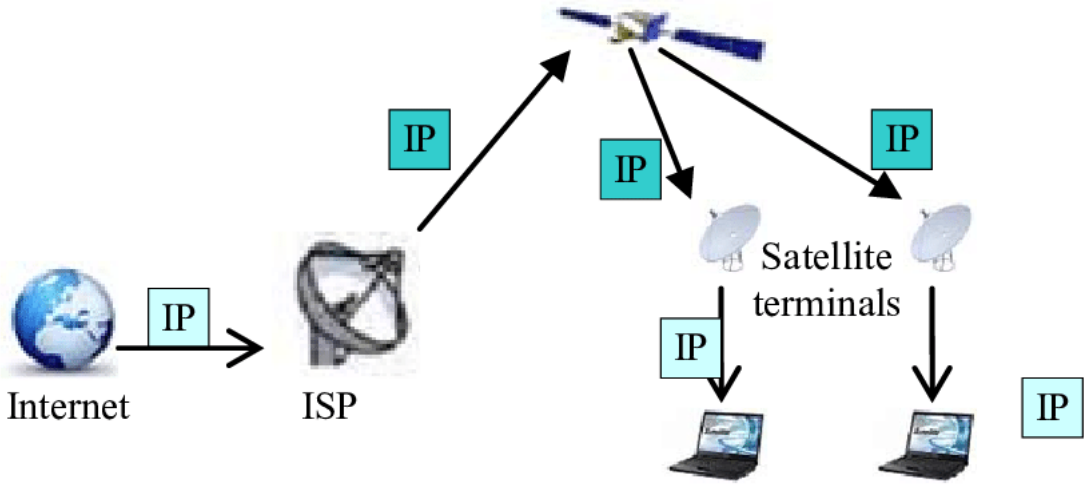
- Modem connects to a filter and splitter, then connects via coaxial cable to a neighborhood concentrator.
- Cable’s bandwidth is divided into channels - TV channel uses a 6-Mhz portion of the bandwidth. Internet traffic typically uses bandwidth above the TV channels for downstream traffic and bandwidth below the TV channels for upstream traffic.
- Network speeds for cable modems are from 256 kb/s to 1.5 Mb/s downstream (now 1–6 Mbps) and up to 384 kb/s upstream (now up to 768 kbps)

Technologies for Connecting

Satellite

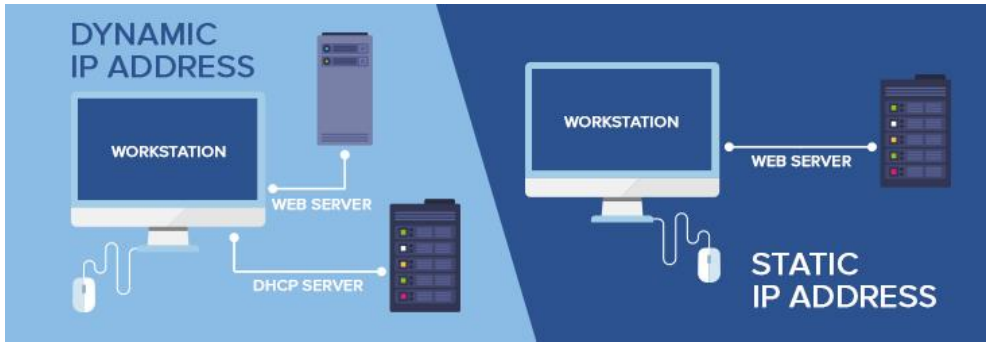
- Download speeds range between 150 to 500 kb/s, with upstream speeds of around 50 kb/s.



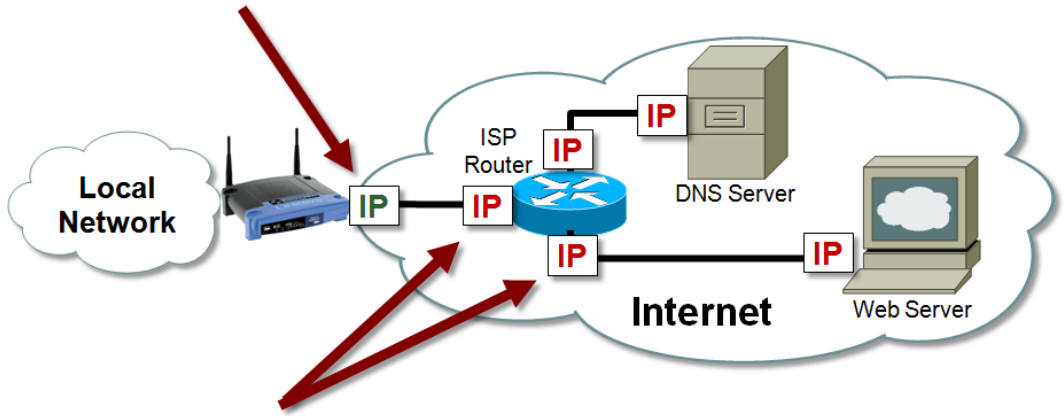


Static and Dynamic IP Addresses

- An Internet Protocol (IP) address is a unique number assigned to every device on a network.
- Internet uses DNS (Domain Name System) to enable people to use words instead of numbers for Internet addresses.
- Static IP address stays the same until explicitly changed, while a dynamic IP address can change on every boot up or network connect (DHCP server)
- Static IP addresses - when external devices or websites need to remember the IP address – eg: VPN
- When IP address changes, the DNS entry for server is automatically updated with its new IP address, so outside users can use the same domain name.



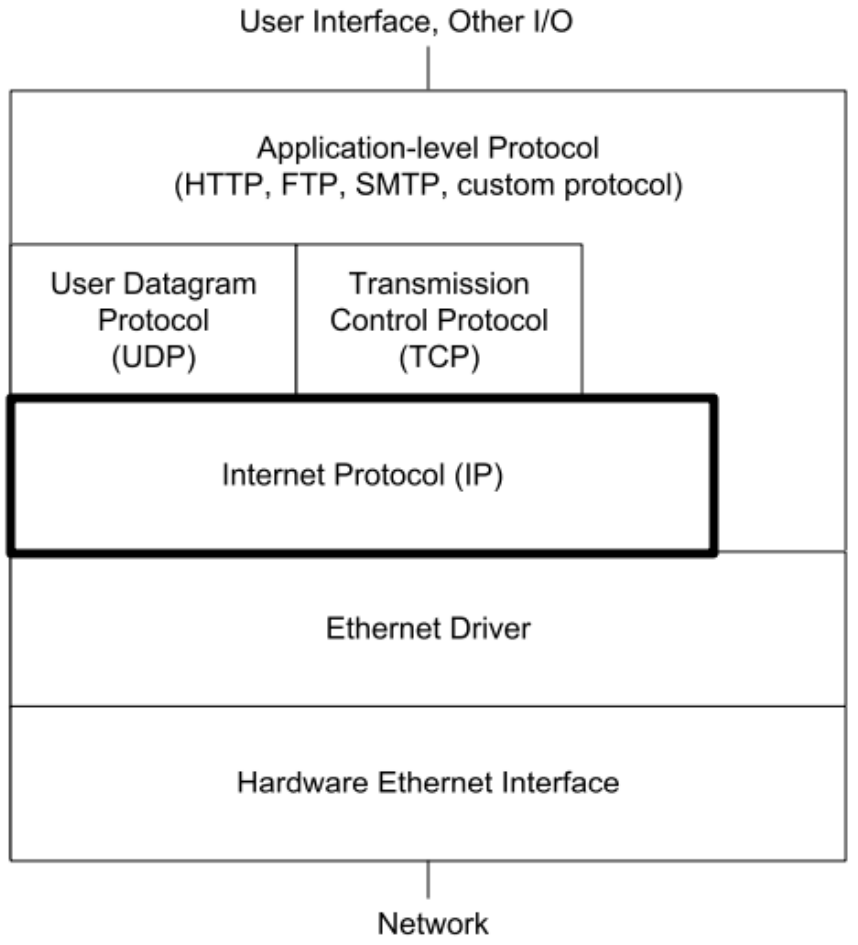
- ***Dynamic*** **IP addresses periodically change**
  - **Typically assigned to ISP customers**



- ***Static*** **IP addresses never change**

Internet Protocol (IP)

- In transmitting, the IP layer receives a message to send from a higher-level protocol layer such as TCP or UDP.
- The IP layer places the message in an IP datagram that consists of an IP header, followed by the message to send.
- The IP layer then passes the datagram to a lower layer such as an Ethernet driver, which sends the datagram on the network.
- A datagram may pass through one or more routers which examines the destination's IP address and decides where to forward the datagram.
- At the destination computer, the Ethernet layer or passes the IP datagram to the IP layer, which removes the IP header and tells what protocol layer, (TCP or UDP), should receive the datagram's message.



Internet Protocol (IP)

- Performs two major functions
  - Defines a way to specify source and destination addresses for use with any network interface and across networks that use different interfaces.
  - Enables a datagram to pass through networks of varying capabilities by defining a protocol that allows a router to fragment, a datagram into multiple, smaller datagrams and enables the destination to reassemble the original message from the fragments
- Two protocols can help in matching an IP address to a computer, or to a network interface
  - Domain Name System (DNS) protocol
  - Address Resolution Protocol (ARP) enables the sender of an IP datagram to match an Ethernet hardware address with an IP address in the local network
- IP version 4 (IPv4) - address is 32 bits – (dotted-quad format 192.168.111.1)
- IP version 6 (IPv6) - address is 128 bits.

Site	Dot-decimal	Binary
Google.com	172.217.168.238	10101100.11011001.10101000.11101110
Facebook.com	31.13.84.36	00011111.00001101.01010100.00100100

Network Address and Host Address

- Network address - same for all of the interfaces in the network - leftmost bits of the IP address
- Host address - unique to the interface within the network - rightmost bits of the IP address
- The number of bits allocated to the network address and host address depends on the network's size.
- A network with a 24-bit network address and 8-bit host addresses can have up to 254 hosts.
- A network with an 8-bit network address and 24-bits host addresses can have over 2 million hosts.
- To keep from running out of available IP addresses, network addresses should be as long as possible while still enabling every host on the Internet to have a unique host address.

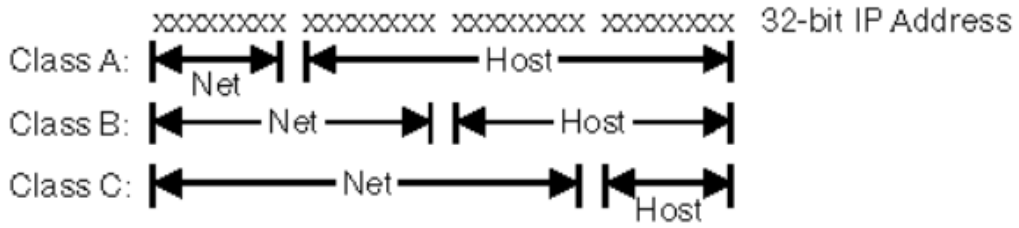
Classful Addressing

- Defines three network classes with network addresses of 8, 16, and 24 bits.
- By examining the first three bits of the IP address, a router can determine what class of network the host belongs to, and thus how many bits make up the network address
- Divided into subnetworks, or subnets.
- For each subnet, the routers in the local network store an additional 32-bit value called the subnet mask, which enables routers to determine which subnet a datagram is directed to.

Network Class	Most Significant Bit(s) in Network Address	Range of Most Significant Byte in Network Address	Number of Bytes in Network Address	Maximum Number of Networks	Number of Bytes in Host Address	Maximum Number of Hosts
A	0	1-126	1	126	3	16 million+
B	10	128-191	2	16,384	2	65,534
C	110	192-223	3	2 million+	1	254
D	1110	224-239	reserved for multicasting			
E	1111	240-255	reserved for future use			

Classful Addressing

```
00001001010000110110000100000010        32-bit address
00001001 01000011 01100001 00000010     4 octets
   9        67       97       2         dotted decimal notation (9.67.97.2)
```




```
   32-bit address           xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

   Class A                  0xxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
                 min        00000000
                 max        01111111
                 range      1 - 126    (decimal notation; 0 and 127 are reserved)

   Class B                  10xxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
                 min        10000000
                 max        10111111
                 range      128 - 191  (decimal notation)

   Class C                  110xxxxx xxxxxxxx xxxxxxxx xxxxxxxx
                 min        11000000
                 max        11011111
                 range      192 - 223  (decimal notation)

   Class D                  1110xxxx xxxxxxxx xxxxxxxx xxxxxxxx
                 min        11100000
                 max        11101111
                 range      224-239 (decimal notation)
```

Classful Addressing

- Class A network - the first byte is between 1 and 126, and the most significant bit is 0. The network address is 1 byte, leaving three bytes for the host address - up to 126 Class A networks each with 16 million hosts.

- Class B network - the first byte is between 128 and 191, and the two most significant bits are 10. The network address is 2 bytes, leaving two bytes for the host address - up to 65,534 Class B networks.

- Class C network - the first byte is between 192 and 223, and the three most significant bits are 110. The network address is 3 bytes, leaving 1 byte for the host address - up to 16,777,214 Class C networks.

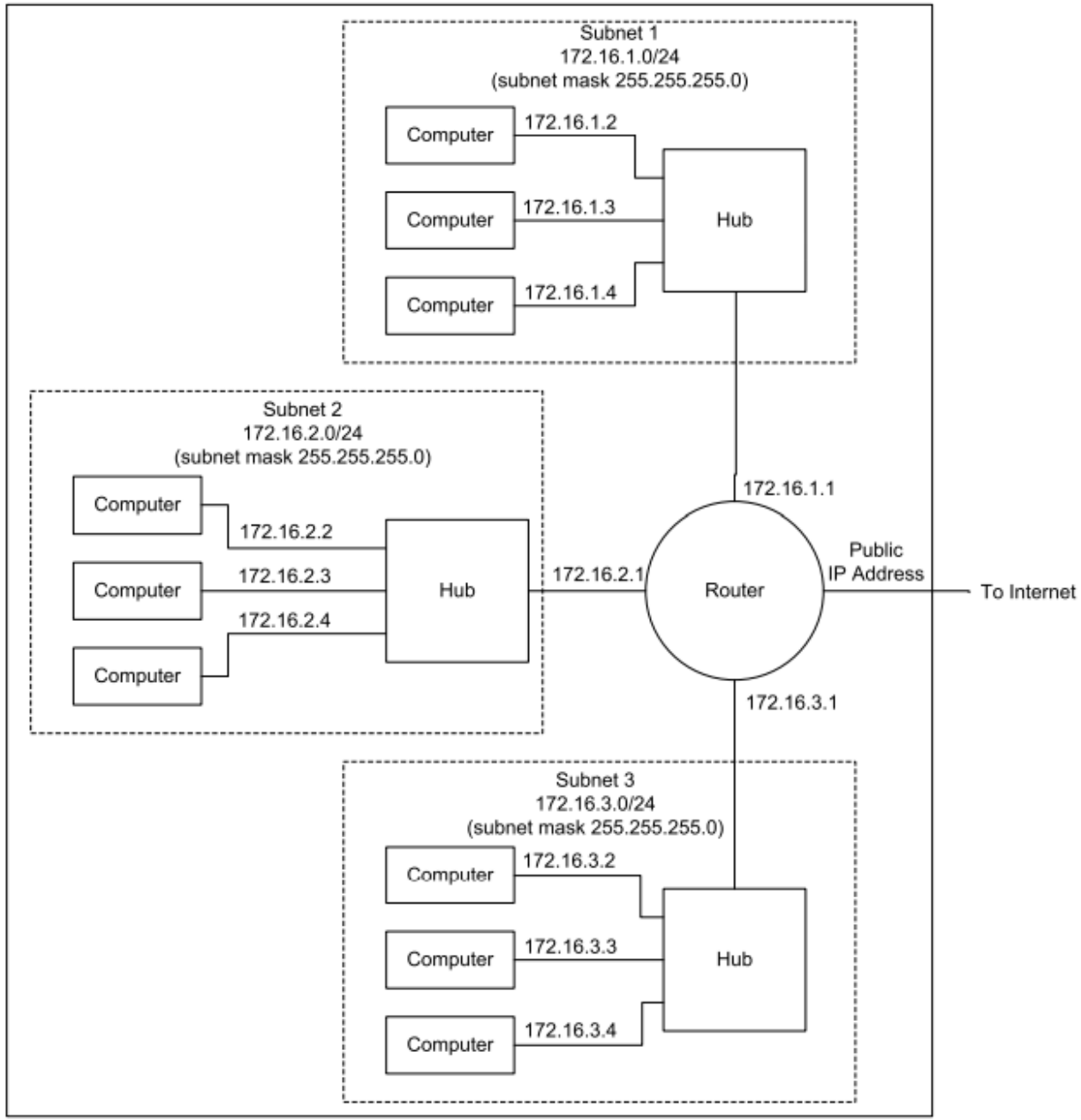
- Class D network - the first byte is between 224 and 239, and the four most significant bits are 1110.

- Class E network - the first byte is between 240 and 255, and the four most significant bits are 1111.

Subnets

- Subnetting is the process of dividing a network into groups called subnet works, or subnets.
- The hosts within a subnet are typically physically near each other and may belong to the same department or facility within an organization.
- Routers use subnet IDs to decide where to route traffic within a network.
- A large local network might use subnets for easier routing of messages.
- A public IP address obtained from an ISP is likely to be in a subnet, so even if the embedded system is in a small network, if the system connects to the Internet, the public IP address is likely to be in a subnet.
- Besides helping in routing, subnetting helps to solve the shortage of available network addresses.
- In a subnet, the host-address portion of an IP address has two parts: a subnet ID and a host ID.
- The subnet ID is the same for all hosts in the subnet, while each host ID is unique in the subnet.

Subnets



- Three Ethernet networks are subnets in a Class B network.
- A hub in each subnet connects to a router that enables the computers in the subnets to communicate with computers in other subnets and on the Internet.
- In each of the IP addresses,
  - first two bytes (172.16) are the network address,
  - the third byte is the subnet ID (1, 2, or 3), and
  - the fourth byte is the host ID.
- Determining which bits in the host address are the subnet ID requires using a 32-bit value called the subnet mask

Subnets

- To determine if a destination address is in the same subnet:
  - Perform a logical AND of the destination address and the subnet mask and compare the result to a logical AND of the host address and the subnet mask - If the values match, the destination is in the same subnet

Example 1

```
Source address =                          192.168.0.229
Source subnet mask =                      255.255.255.224
Destination address =                     192.168.0.253
Subnet mask AND Destination address =  192.168.0.224
Subnet mask AND Source address =          192.168.0.224
192.68.0.224 XOR 192.68.0.224 =           0.0.0.0
```

The values match, so the destination address and the host are in the same subnet

Example 2

```
Source address =                          10.2.1.3
Source subnet mask =                      255.255.0.0
Destination address =                     10.1.2.1
Subnet mask AND Destination address =  10.1.0.0
Subnet mask AND Source address =          10.2.0.0
10.1.0.0 XOR 10.2.0.0 =                   0.3.0.0
```

The values don't match, so the source and destination are not in the same subnet

Classless Addressing

- The network address and IP prefix are often expressed in the form:

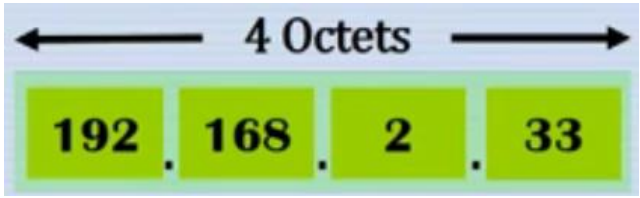
  xxx.xxx.xxx.xxx/n

  where xxx.xxx.xxx.xxx is the lowest IP address in the network and

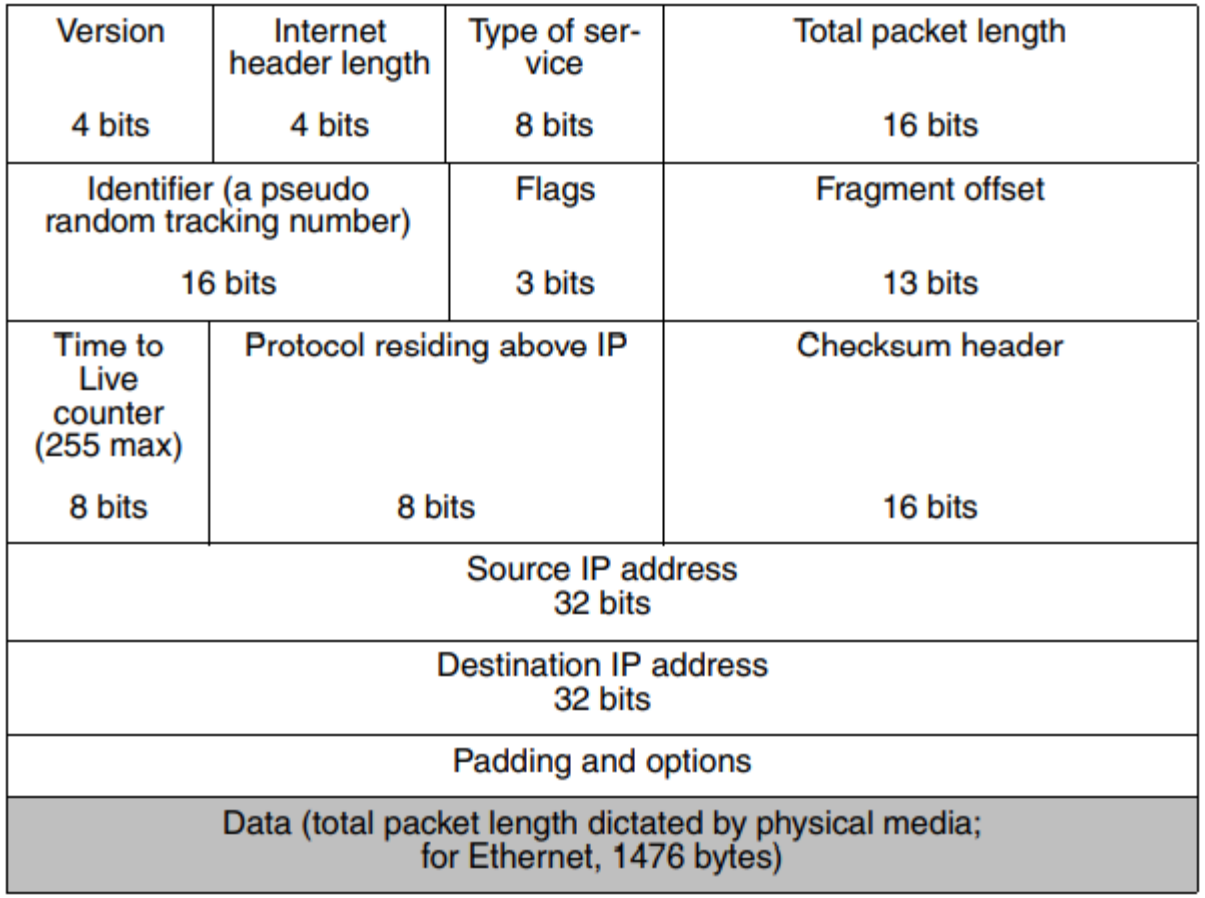
  n is the number of bits in the network-address portion of the IP address.
- For example, 192.0.2.0/24, the network address is 192.0.2 (three bytes, or 24 bits), and the final eight bits in the IP address are the host address - This notation is also called slash notation or Classless Interdomain Routing (CIDR) notation
- A network address or host address can never be all zeros or all ones - no network at 255.255.255 or 0.0.0.0
- The address 0.0.0.0 refers to the local host or network.
- Broadcast Addresses - a destination address of all ones is a broadcast to all hosts in a network or subnet. (Eg: For a network of 192.168.100.0/28, 192.168.100.255 is directed to all hosts in the network)
- HostID = 'all zeros' means 'this network'.
- HostID = 'all ones' means 'all hosts on this network'

IPv4

- A 32-bit address that uniquely and universally defines the connection of a device to the Internet.
- Each address defines one, and only one, connection to the Internet - two devices on the Internet can never have the same address at the same time.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses N bits to define an address, the address space is 2^N .
- The address space in IPv4 is 2^{32} or 4,294,967,296 (more than 4 billion) - theoretically, more than 4 billion devices could be connected to the Internet.



IPv4 Header Structure



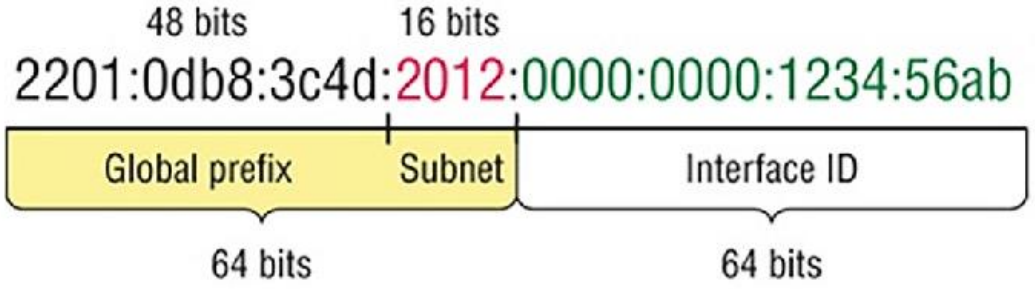
Field	Number of Bits	Description
Version	4	IP version being used
Internet Header Length	4	Total length of the header in 32-bit words
Type of Service	8	Suggestions as to the importance of minimizing delay, maximizing throughput, and maximizing reliability in routing
Total Length	16	Total length of the datagram in bytes
Identification	16	Identifier for use in reassembling fragments
Flags	3	Information used in fragmenting
Fragment Offset	13	Position of a fragment in units of 64 bits
Time to Live	8	Maximum time or number of router hops a datagram may live
Protocol	8	Protocol identifier for the data portion of the datagram
Header Checksum	16	Error-checking value for the header
Source Address	32	IP address of source
Destination Address	32	IP address of destination
Options (optional)	varies	Additional information for security, routing, identification, and/or time stamping

IPv6

- Classless addressing, Dynamic Host Configuration Protocol (DHCP), address depletion is still a long-term problem for the Internet.
- Other problems such as lack of accommodation for real-time audio and video transmission, and encryption and authentication of data for some applications, have been the motivation for IPv6.
- Address consists of 16 bytes (octets); it is 128 bits long.
- 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.

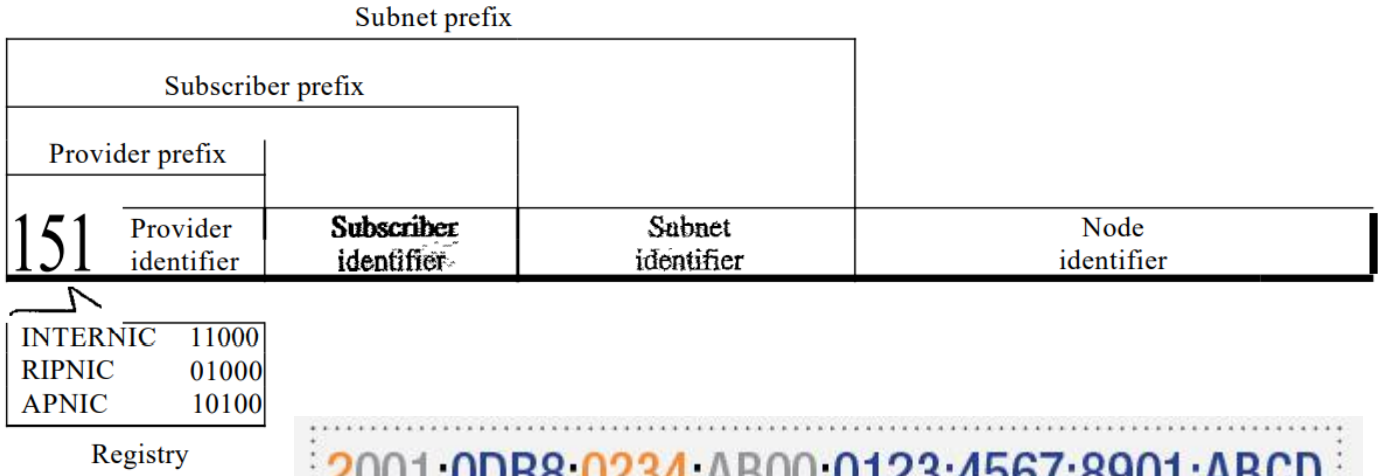
2201:0db8:3c4d:2012:0000:0000:1234:56ab

IPv6



2001:0:0:802:0:0:0:1010
equals
2001:0:0:802::1010
or
2001::802:0:0:0:1010

Gap



Registry identifier - 5-bit field indicates the agency that has registered the address

Provider identifier - variable-length field identifies the provider such as an ISP.

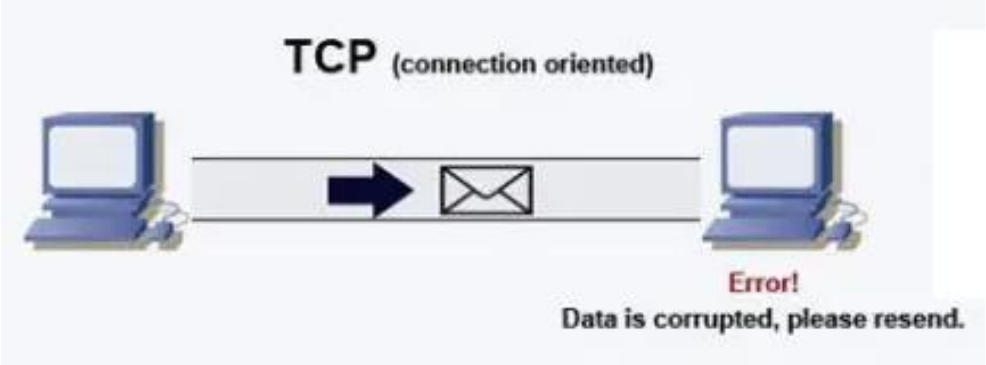
Subscriber identifier - an organization subscribes to the Internet through a provider.

Subnet identifier - Each subscriber can have many different subnetworks.

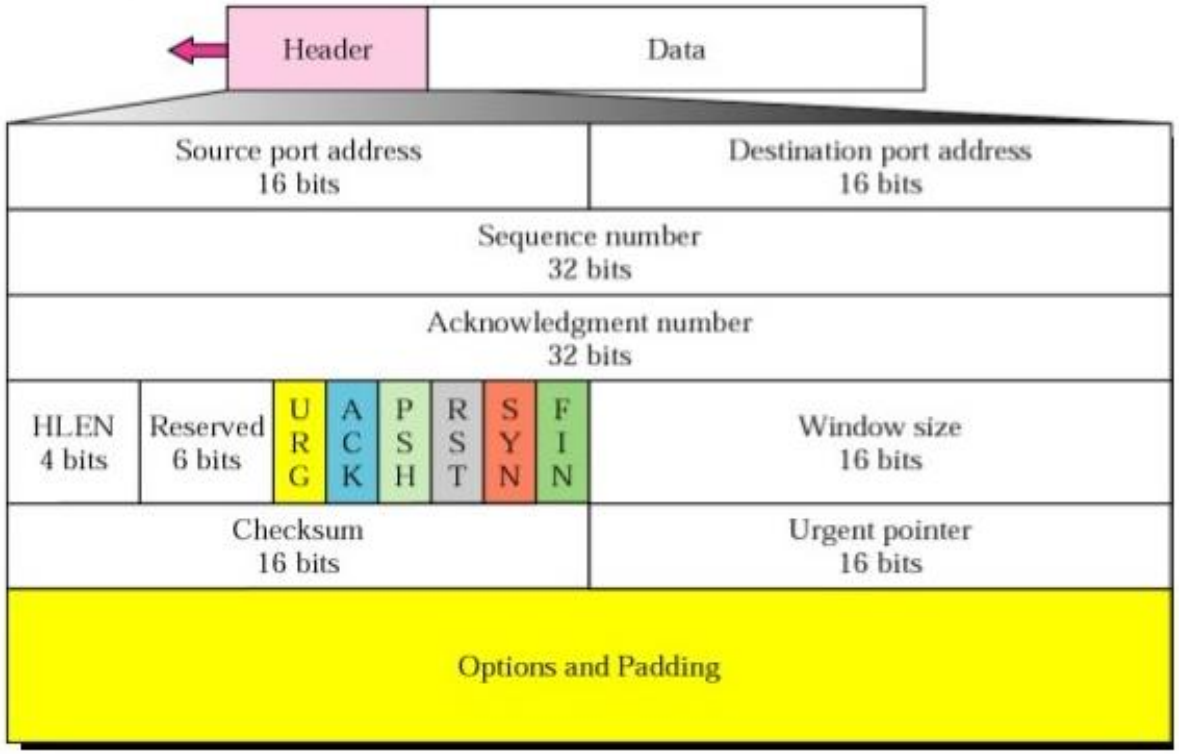
Node identifier - identity of the node connected to a subnet.

Transmission Control Protocol (TCP/IP)

- *de facto* standard world-wide for industrial and telecommunications applications - the Internet was designed around it in the first place and without it, no Internet access is possible.
- Connection-oriented protocol that offers vastly improved protection and error control.
- Heart of the TCP/IP suite - provides a very reliable method of transferring data in byte (octet) format, between applications.
- TCP/IP is not a single protocol, but an entire suite of protocols with multiple delivery mechanisms for a variety of message types.
- TCP/IP routes messages from source to destination, finding the best path through a potentially large number of transmitters and receivers.
- A packet in TCP is called a segment.
- Provides host-to-host communication.



TCP Header

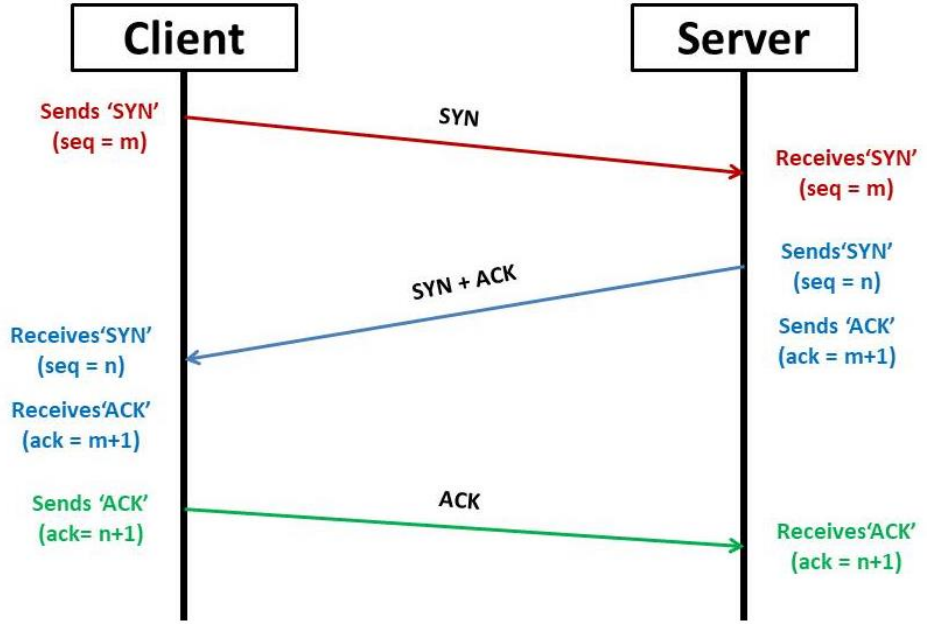


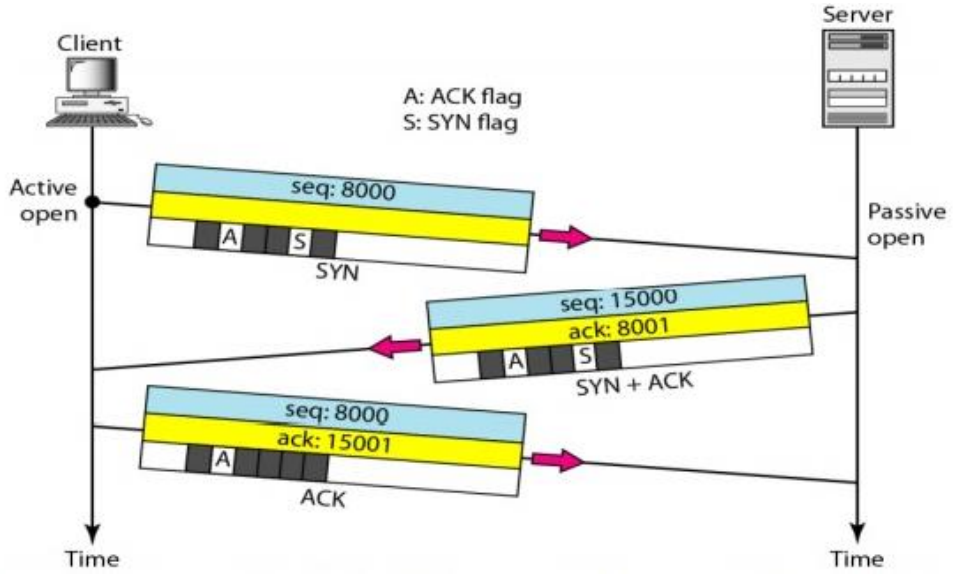
Field	Number of Bits	Description
Source Port Number	16	The port, or process, that is sending the datagram.
Destination Port Number	16	The port, or process, the datagram is directed to.
Sequence Number	32	Segment identifier.
Acknowledgment Number	32	Identifier of the last received byte.
Header Length	4	Length of TCP header in units of 32 bits.
Reserved	6	Zero.
Control Bits	6	URG: the segment is urgent ACK: the acknowledgment number is valid PSH: push the data to application right away RST: reset the connection SYN: synchronization is in progress FIN: the source has no more data to send
Window	16	The number of new bytes the source can accept.
Checksum	16	Checksum value.
Urgent Pointer	16	Sequence number of the last byte of urgent data
Options	0 or more	(optional) Can indicate the maximum segment size the source can handle.

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
13	Daytime	Returns the date and the time
20	FIP, Data	File Transfer Protocol (data connection)
21	FIP, Control	File Transfer Protocol (control connection)
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
80	HTTP	Hypertext Transfer Protocol

TCP Operation

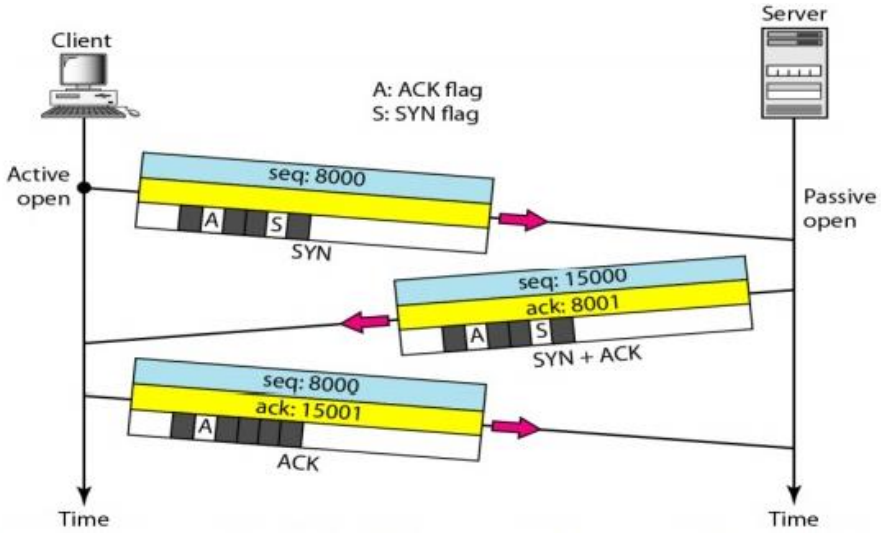
- An application program, called the client, wants to make a connection with another application program, called the server.
- The server program tells its TCP that it is ready to accept a connection - called a request for a passive open.
- A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server - issues a request for an active open.
- The client sends the first segment, a SYN segment, in which only the SYN flag is set - for synchronization of sequence numbers.
- The server sends the second segment, a SYN + ACK segment, with 2 flag bits set: SYN and ACK. A SYN segment for communication in the other direction and serves as the acknowledgment for the SYN segment.
- The client sends the third segment - an ACK segment. It acknowledges the receipt of the second segment with the ACK flag.



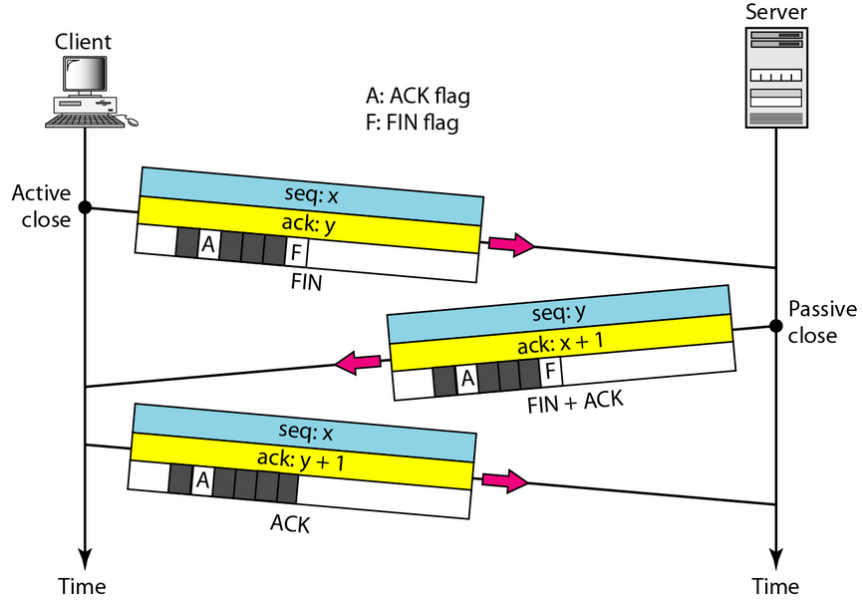


TCP Operation

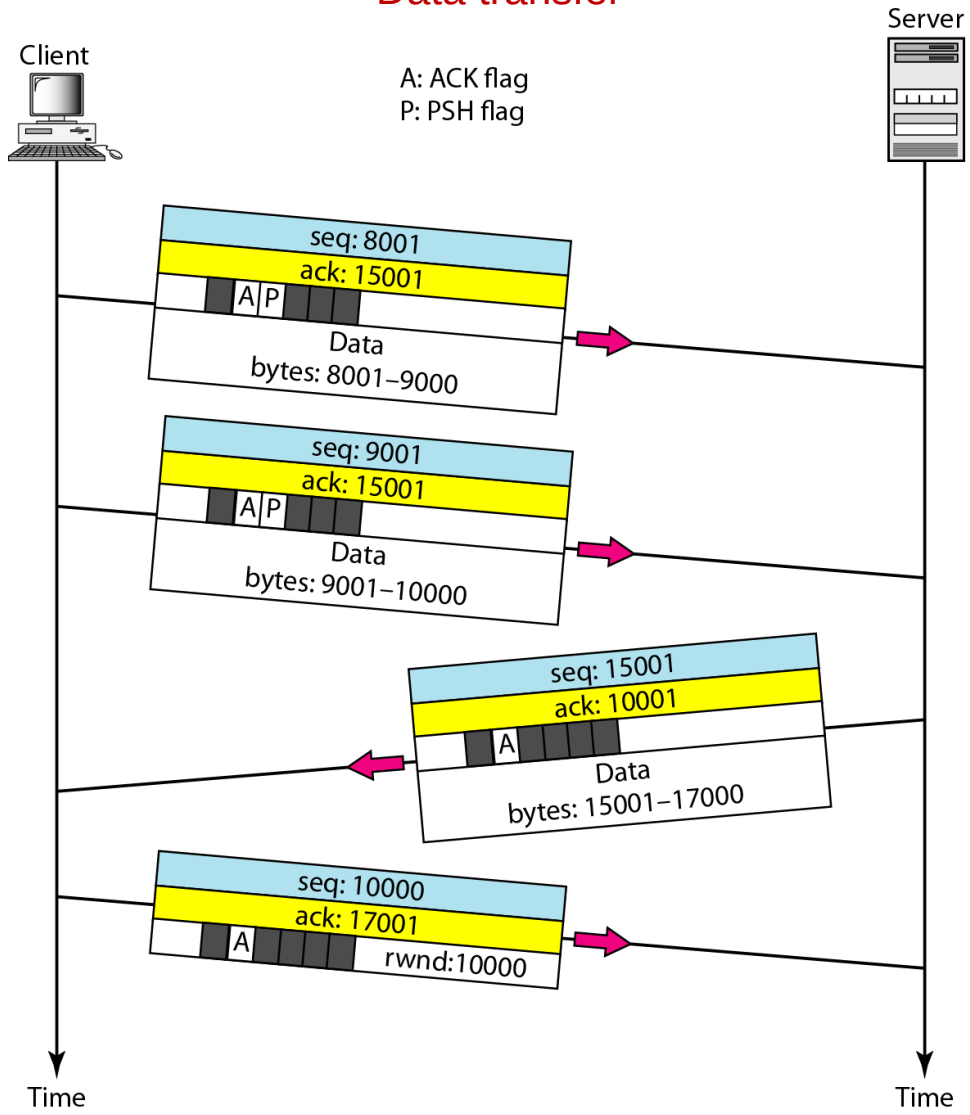
Connection establishment using three-way handshaking



Connection termination using three-way handshaking

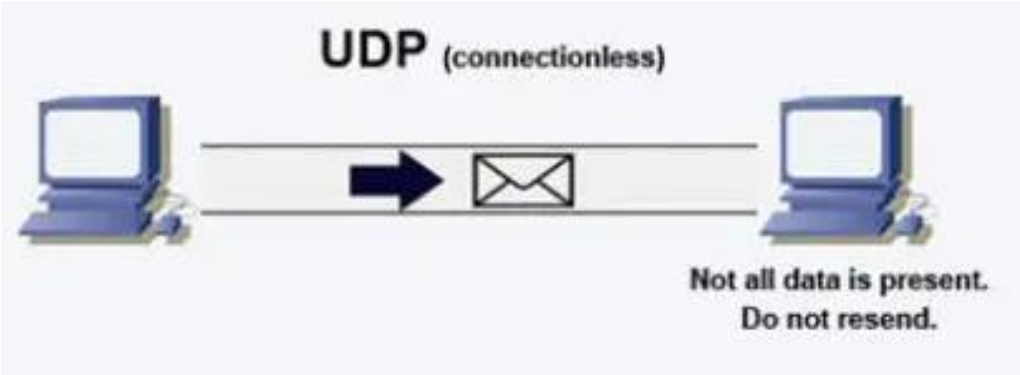


Data transfer

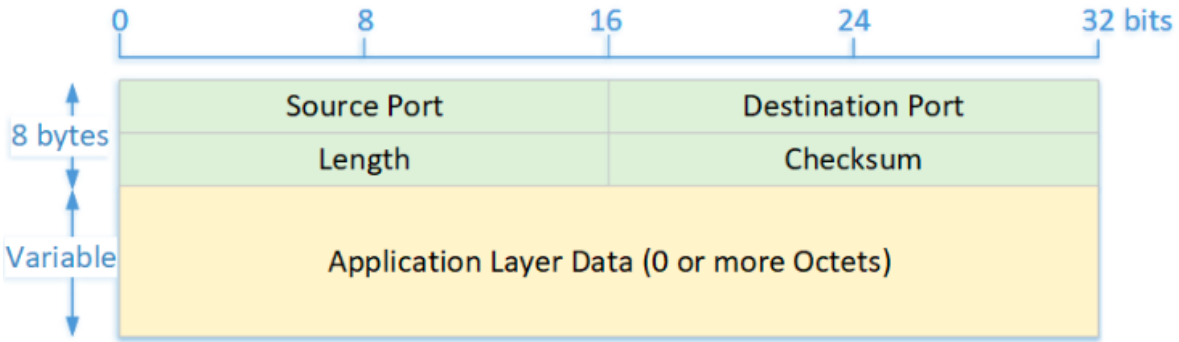


User Datagram Protocol (UDP/IP)

- A connectionless protocol - computer can send a message using UDP without first establishing that the remote computer is on the network or that the specified destination port is available to communicate.
- UDP is also called an unreliable protocol, meaning that using UDP alone, the sender doesn't know when or if the destination received a message.
- UDP is a basic protocol that adds only port addressing and optional error detecting to the message being sent - no protocol for handshaking to acknowledge received data or exchange other flow-control information
- UDP packets, called user datagrams.
- Provide process-to-process communication.



UDP Header

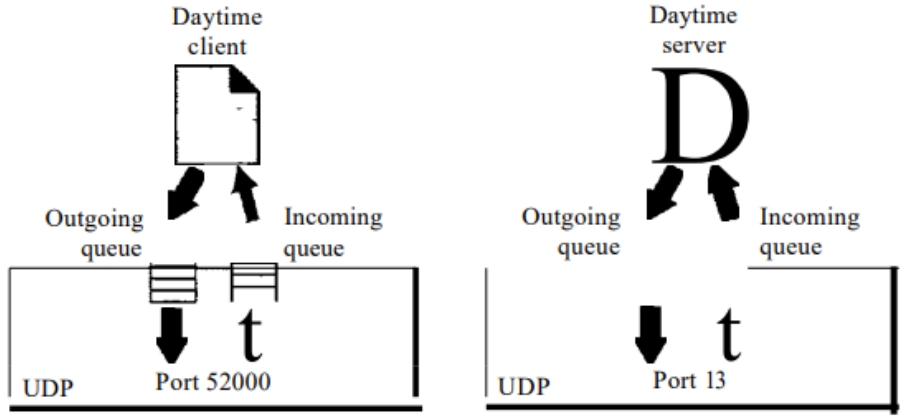


Field	Number of Bits	Description
Source Port Number	16	The port, or process, that is sending the datagram.
Destination Port Number	16	The port, or process, the datagram is directed to.
UDP Datagram Length	16	The datagram length in bytes.
UDP Checksum	16	Checksum value or zero.

- Data - UDP datagram can be up to 65,535 bytes, and the header is eight bytes, so a datagram can carry up to 65,527 bytes of data
- Shorter datagrams may be more efficient - when a large datagram travels through networks with different capabilities, the Internet Protocol may fragment the datagram, requiring the destination to reassemble the fragments.

UDP Operation

- At the client site, when a process starts, it requests a port number from the operating system.
- Create both an incoming and an outgoing queue associated with each process.
- The queues function as long as the process is running. When the process terminates, the queues are destroyed.
- The client process can send messages to the outgoing queue by using the source port number specified in the request. UDP removes the messages one by one and, after adding the UDP header, delivers them to IP.
- When a message arrives for a client, UDP checks to see if an incoming queue has been created for the port number specified in the destination port number field of the user datagram.
- If there is such a queue, UDP sends the received user datagram to the end of the queue.
- If there is no such queue, UDP discards the user datagram and sends a port unreachable message to the server.



Applications of UDP

- Lossless data transmission
- Gaming, voice and video
- Services that don't need fixed packet transmission
- Multicasting
- Fast applications

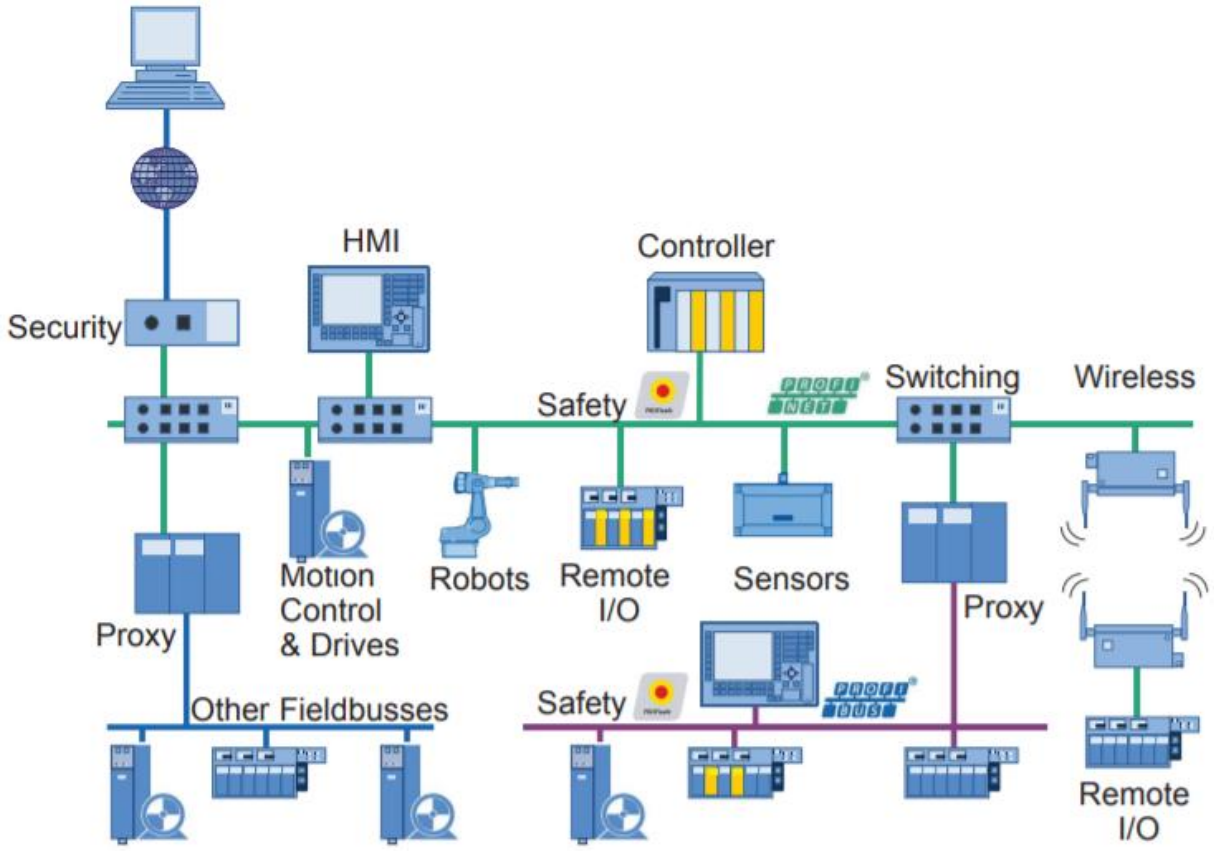
UDP	TCP
Faster as it lacks error check feature	Slower as it offers additional functionality
Unreliable	Reliable
Connectionless Protocol	Connection oriented Protocol
No order of data packets guaranteed	Proper Data segment order
No Acknowledgment	Acknowledges the data segments
No retransmission	Allows retransmission
Light overhead	Heavy Overhead

20IS709
Communication Systems For Industrial Networking

PROFINET

PROFINET

- In today's automation technology, Ethernet and information technology (IT) are increasingly used with established standards like TCP/IP and XML.
- Integrating information technology into automation opens up significantly better communication options between automation systems, extensive configuration and diagnostic possibilities, and network-wide service functionality.
- PROFINET (**Pro**cess **Fi**eld **Net**work) is the open standard for Industrial Ethernet satisfying all requirements of automation technology.
- The use of PROFINET for plant and machine manufacturers, minimizes the costs for installation, engineering, and commissioning.



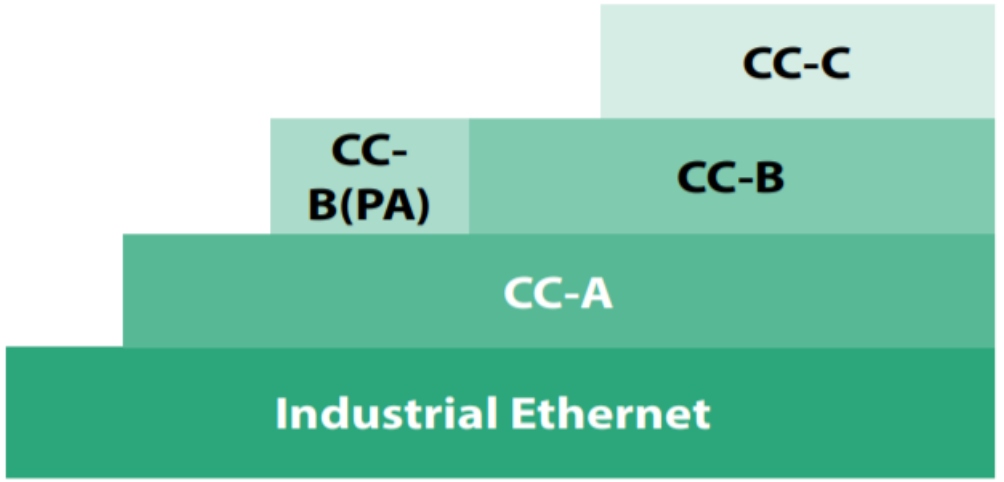
PROFINET Advantages

- Ease of use
  - Minimizes the costs for installation, engineering, commissioning and fast and efficient automation
- Flexible network topology
  - 100% Ethernet compatible according to IEEE standards and adapts to circumstances.
- Integrated diagnostics
  - Acyclic diagnostic data transmission provides important information regarding the status of devices and network.
- Integrated safety
- High availability
- Expanded system structures

Conformance classes

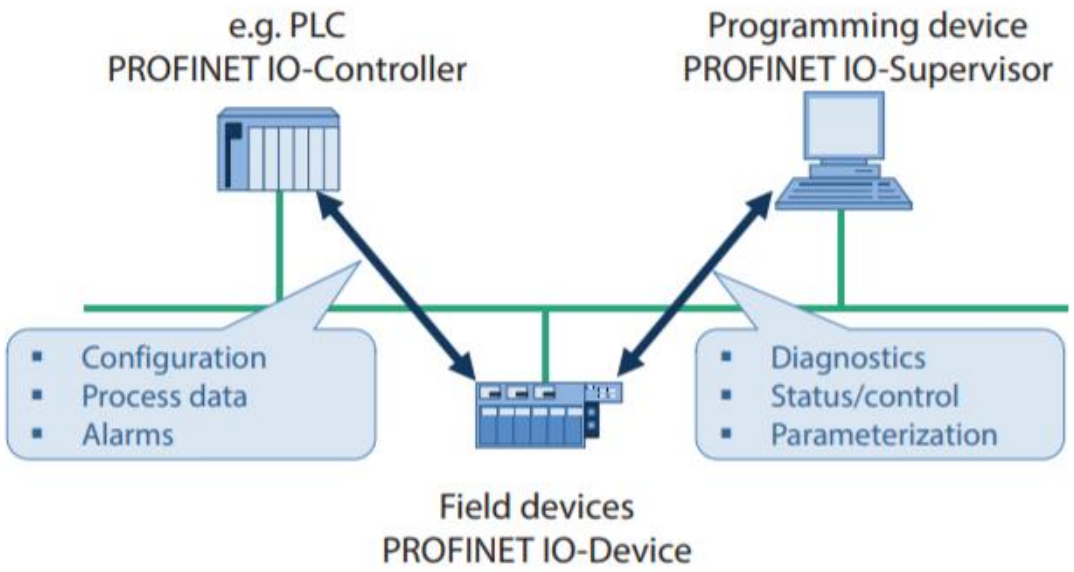
- Scope of functions supported by PROFINET IO is divided into conformance classes ("CC") - provide a practical summary of the various minimum properties.

- CC-A provides basic functions for PROFINET IO with RT communication. All IT services can be used without restriction. Typical applications are found in business automation. Wireless communication is specified for this class.
- CC-B extends the concept to include network diagnostics via IT mechanisms as well as topology information. The system redundancy function important for process automation is contained in an extended version of CC-B named CC-B(PA).
- CC-C describes the basic functions for devices with hardware-supported bandwidth reservation and synchronization and is thus the basis for isochronous real time (IRT) applications



PROFINET System Model

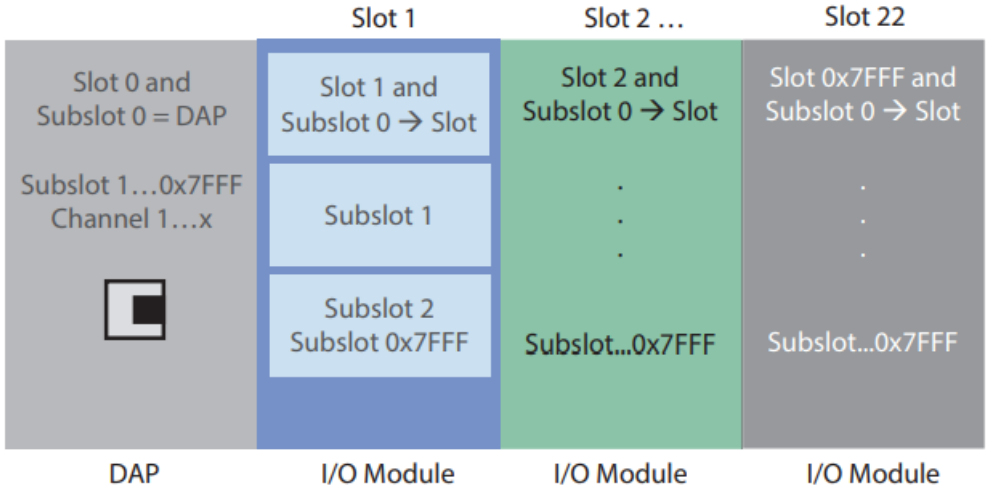
- Follows Provider/Consumer model for data exchange.
- IO controller - the programmable logic controller (PLC) on which the automation program runs.
- IO device is a distributed I/O field device that is connected to one or more IO controllers via PROFINET IO
- IO Supervisor - a Programming Device (PD), personal computer (PC), or human machine interface (HMI) device for commissioning or diagnostic purposes.
- A plant unit contains at least one IO controller and one or more IO devices. IO supervisors are usually integrated only temporarily for commissioning or troubleshooting purposes.



Device model of an IO device

- Device model describes all field devices in terms of their possible technical and functional features.
- Specified by the DAP (Device Access Point) and the defined modules for a particular device family.
- DAP is the access point for communication with the Ethernet interface and the processing program.
- A variety of I/O modules can be assigned to it in order to manage the actual process data traffic.
- The *slot* designates the place where an I/O module is inserted in a modular I/O field device.
- The configured modules containing one or more subslots for data exchange are addressed on the basis of the different slots.

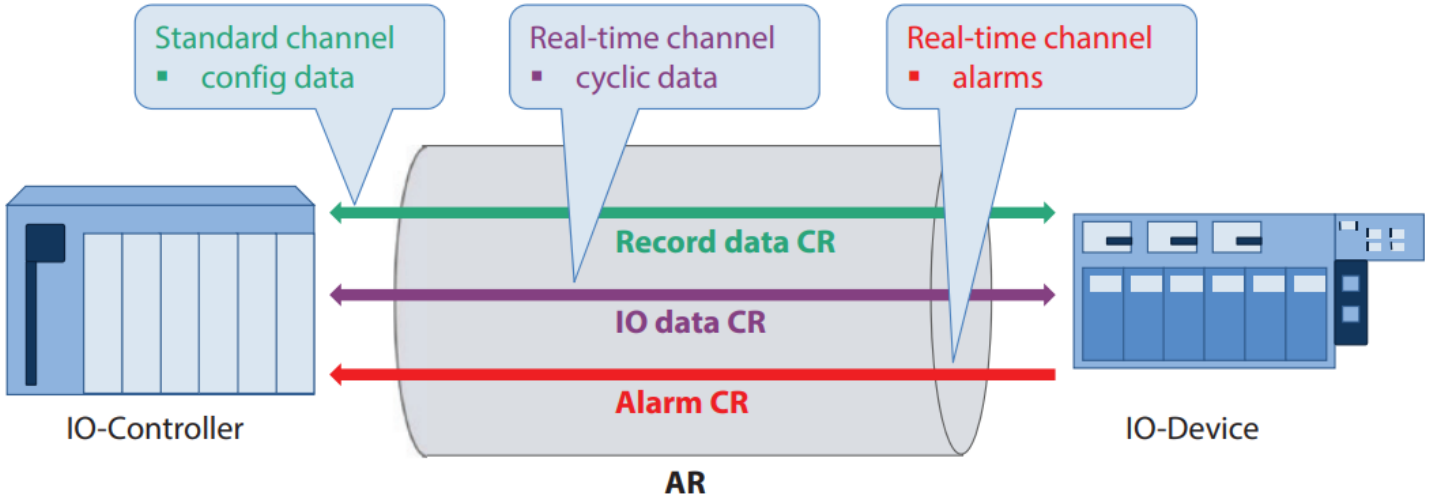
- Within a slot, the *subslots* form the actual interface to the process (inputs/outputs).
- The *index* specifies the data within a slot/subslot that can be read or written acyclically via read/write services - Certain indices are defined in the standard, and other indices can be freely defined by the manufacturer.
- For acyclic data communication via read/write services, an application can specify the data to be addressed using slot, subslot, and index.



- *API* (Application Process Identifier/Instance) is defined as an additional addressing level to avoid competing accesses in the definition of user profiles.

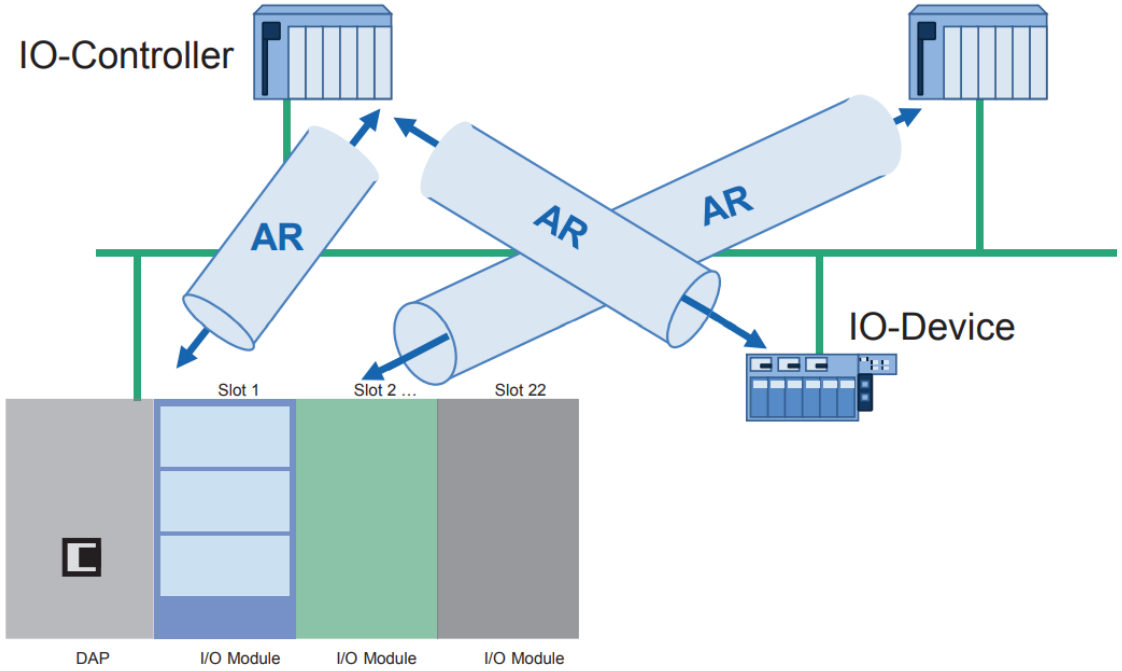
PROFINET Communication

- To establish communication between the higher-level controller and an IO device, the communication paths are set up by the IO controller during system startup based on the configuration data received from the system – specified by the data exchange.
- Every data exchange is embedded into an *AR* (Application Relation).
- Within the AR, CRs (Communication Relations) specify the data explicitly.
- All data for the device modeling, including the general communication parameters, are downloaded to the IO device.
- An IO device can have multiple ARs established from different IO controllers.
- The communication channels for cyclic data exchange (IO data CR), acyclic data exchange (record data CR), and alarms (alarm CR) are set up simultaneously

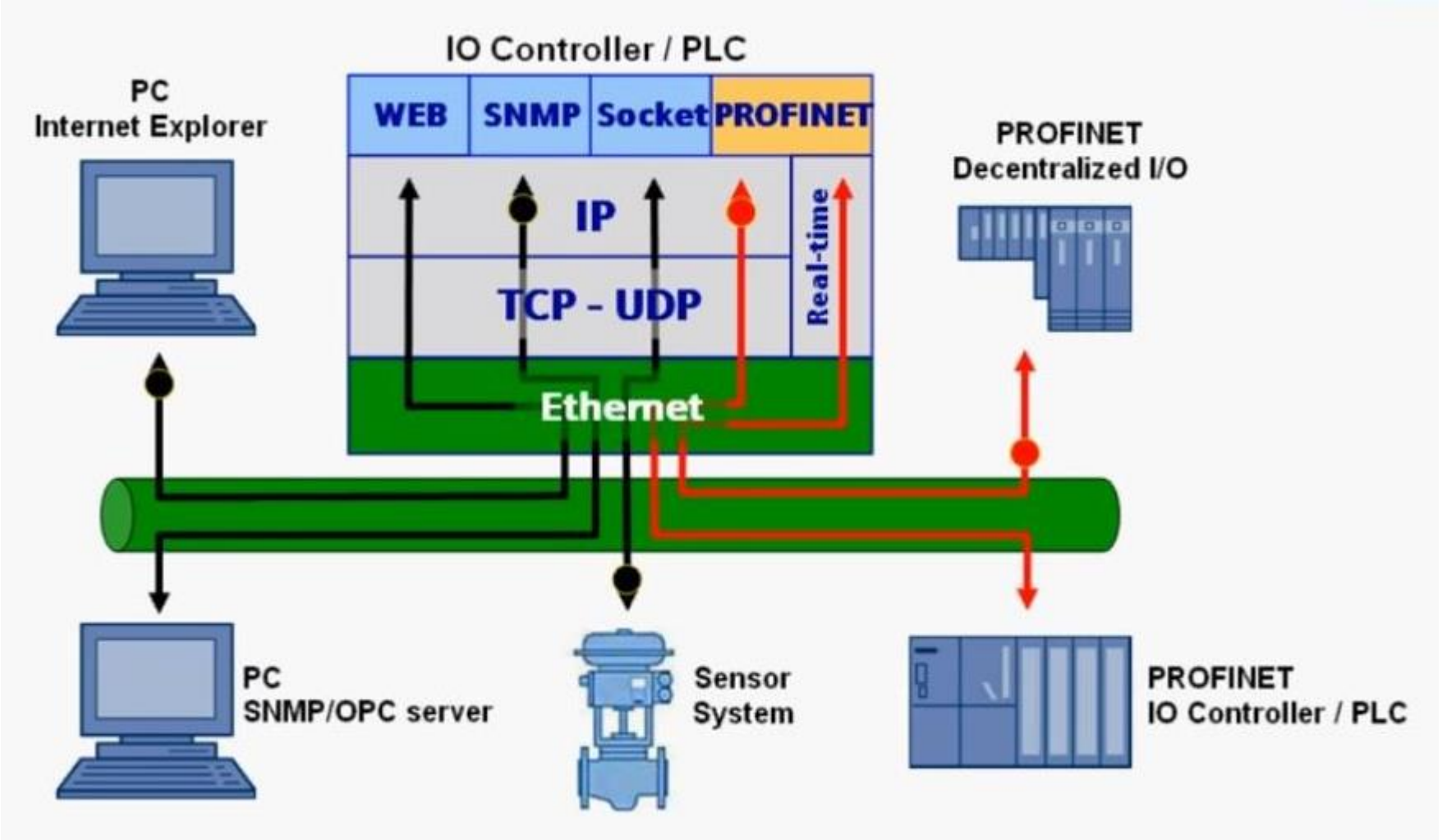


PROFINET Communication

- Multiple IO controllers can be used in a PROFINET system.
- If these IO controllers are to be able to access the same data in the IO devices, this must be specified when configuring (shared devices, shared inputs).
- An IO controller can establish one AR each with multiple IO devices.
- Within an AR, several IO CRs on different APIs can be used for data exchange - can be useful if more than one user profile is involved in the communication and different subslots are required.
- The specified APIs serve to differentiate the data communication for an IO CR



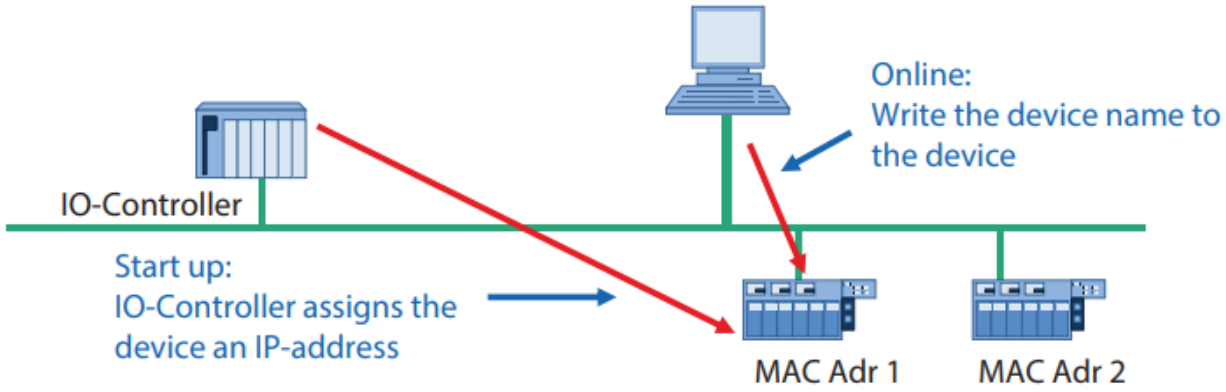
PROFINET Communication



PROFINET Addressing

- Each field device receives a symbolic name that uniquely identifies the field device within this IO system - DCP (Discovery and basic Configuration Protocol) is used for this.
- This name is assigned to the individual devices and thus to the IO device's MAC address by an engineering tool using the DCP protocol during commissioning.
- Each PROFINET device is addressed using its globally unique MAC address
- MAC address consists of a company code (bits 24 ... 47) as an OUI (Organizationally Unique Identifier) and a consecutive number (bits 0 … 23).
- With an OUI, up to 16,777,214 products of a single manufacturer can be identified.

Bit value 47 ... 24			Bit value 23 ... 0		
00	0E	CF	XX	XX	XX
Company code -> OUI			Consecutive number		



PROFINET Functions

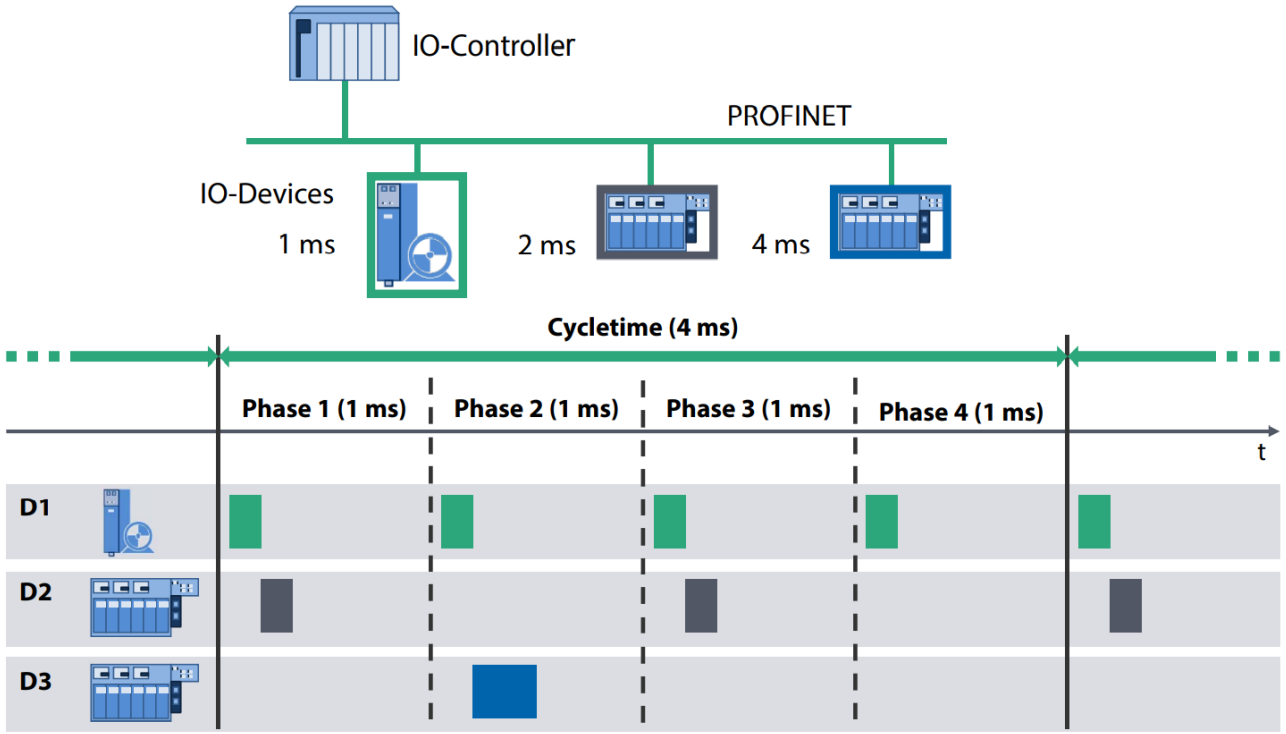
- Cyclic exchange of I/O data with real-time properties
- Acyclic data communication for reading and writing of demand-oriented data (parameters, diagnostics), including the identification & maintenance function (I&M) for reading out device information
- Flexible alarm model for signaling device and network errors with three alarm levels

Requirement	**Technical function/ solution**
Cyclic data exchange	PROFINET with RT communication
Acyclic parameter data/ Device identification (HW/ FW)	Read Record/ Write Record I&M0
Device/ network diagnos-tics (alarms)	Diagnostics and maintenance

PROFINET Functions

Cyclic data exchange

- Cyclic I/O data are transmitted via the "IO Data CR" unacknowledged as real-time data between provider and consumer in an assignable time base.
- The cycle time can be specified individually for connections to the individual devices and are thus adapted to the requirements of the application.
- Different cycle times can be selected for the input and output data, within the range of from 250 µs to 512 ms.
- During data transmission in the frame, the data of a subslot are followed by a provider status - evaluated by the consumer of the I/O data - consumer statuses for the counter direction are transmitted.
- Failure of cyclic data to arrive is monitored - If the configured data fail to arrive within the monitoring time, the consumer sends an error message to the application



PROFINET Functions

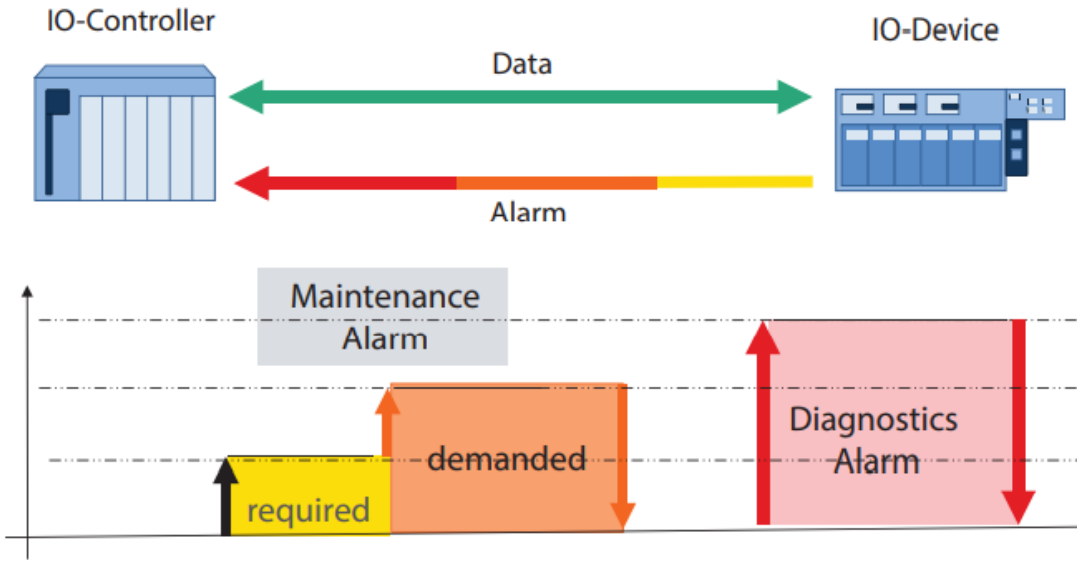
Acyclic data exchange

- Acyclic data exchange using the "Record Data CR" can be used for parameter assignment or configuration of IO devices or reading out status information.
- Accomplished with the read/write frames using standard services via TCP/IP, in which the different data records are distinguished by their index.
- In addition to the data records, the following system data records are also specially defined:
  - Diagnostic information about the network and the devices can be read out by the user from any device at any time
  - Identification and maintenance information (I&M) for explicit identification of the devices and modules and their versions - for maintenance purposes.
- I&M functions are subdivided into 5 different blocks (IM0 ... IM4) and can be addressed separately using their index - every IO device must support the IM0 function with information about hardware and firmware versions.

PROFINET Functions

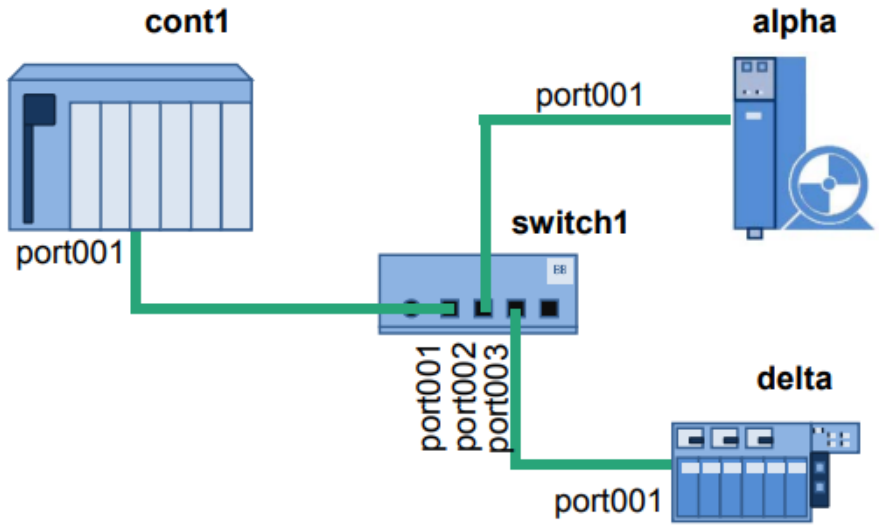
Device/network diagnostics

- A system for reliable signaling of alarms and status messages by the IO devices to the IO controller is defined for PROFINET IO.
- Alarm concept covers both system-defined events (such as removal and insertion of modules) as well as signaling of faults that were detected in the utilized controller technology (e.g., defective load voltage or wire break).
- This is based on a state model that defines "good" and "defective" status as well as the "maintenance required" and "maintenance demanded" prewarning levels.
- *Diagnostic alarms* must be used if the error or event occurs within an IO device or in conjunction with the connected components.
- *Process alarms* for messages from the process, e.g., limit temperature exceeded. In this case, the IO device may still be operable. These process alarms can be prioritized differently from the diagnostic alarms.



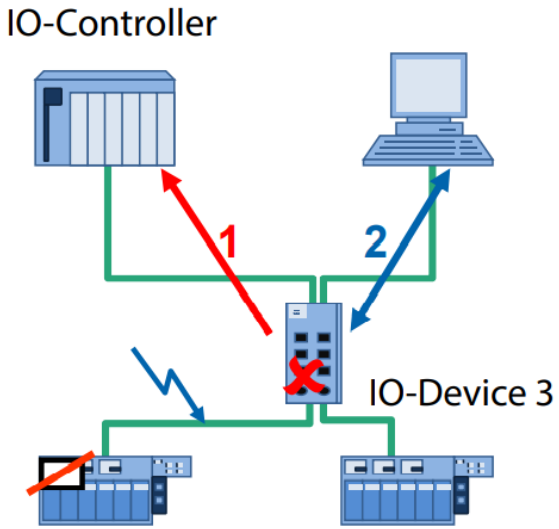
Network diagnostics and management

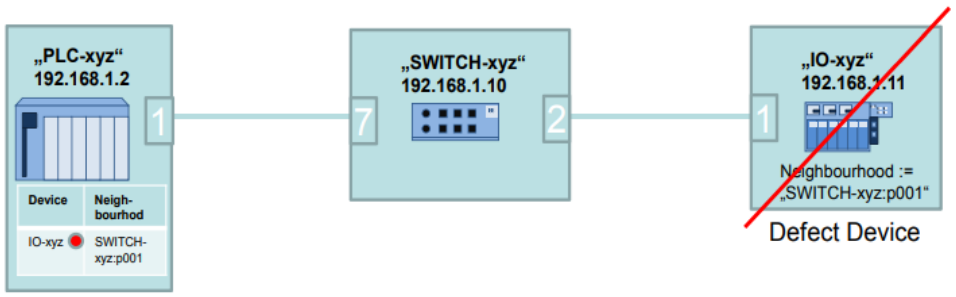
- In existing networks, Simple Network Management Protocol (SNMP) has established itself as the de facto standard for maintenance and monitoring of network components and their functions.
- In order to monitor PROFINET devices even with established management systems, implementation of SNMP is mandatory for devices of Conformance Class B and C.
- Neighborhood detection - Link Layer Discovery Protocol (LLDP) is used to exchange the available addressing information via each port allowing the respective port neighbor to be explicitly identified and the physical structure of the network to be determined.
- With this neighborhood detection, a preset/actual comparison of the topology is possible and changes of the topology during operation can be recognized immediately - which is also the basis for the automatic naming during device replacement.



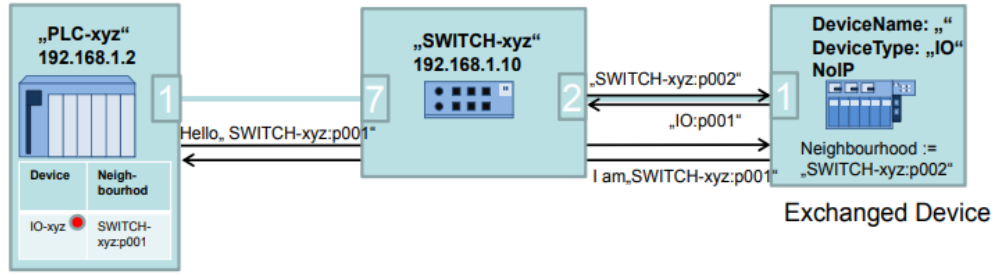
Network diagnostics and management

- If a field device fails in a known topology, it is possible to check whether the replacement device has been reconnected in the proper position.
- It is even possible to replace devices without the use of an engineering tool: When replaced, a device at a given position in the topology receives the same name and parameters as its predecessor.
- A type of switch used as PROFINET IO device can signal identified network errors of a lower-level Ethernet line and specific operating states to its IO controller by transmitting acyclic alarms using the "alarm CR" (number 1)

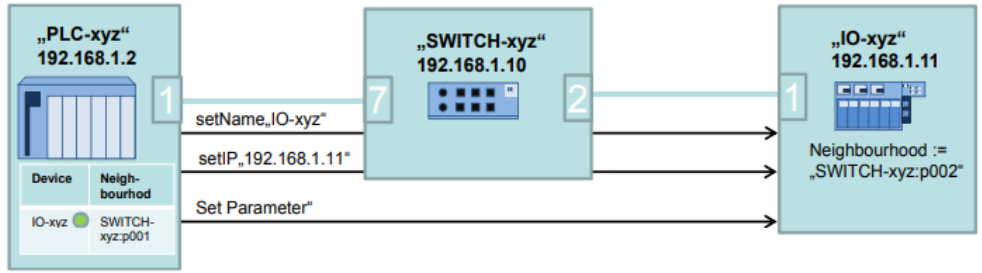




Failing of a device



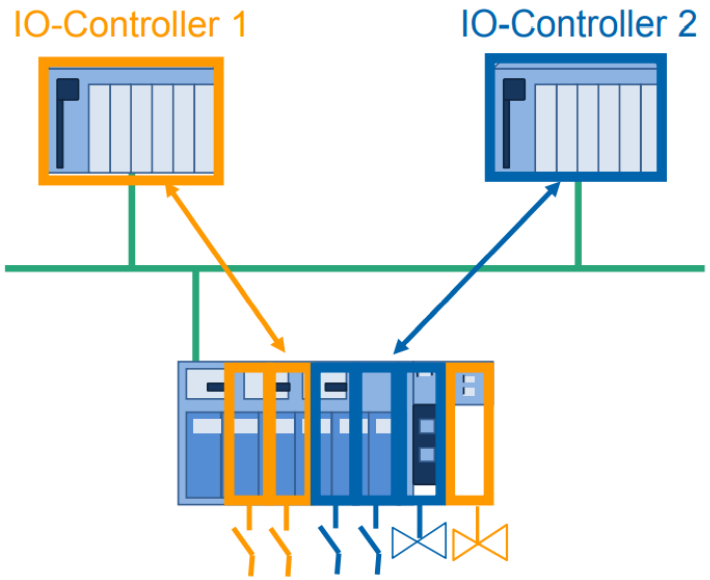
Device, which does not have a name, is implemted,
the control looks for a device with the same neighborhood



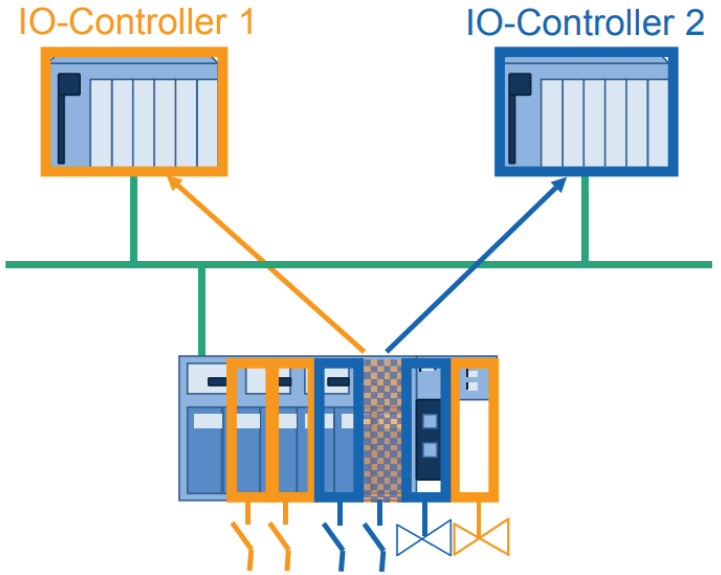
Control writes name, IP-Adress and and startup parameters on the device

Optional functions

- Shared device: Access by multiple controllers to different modules in a device

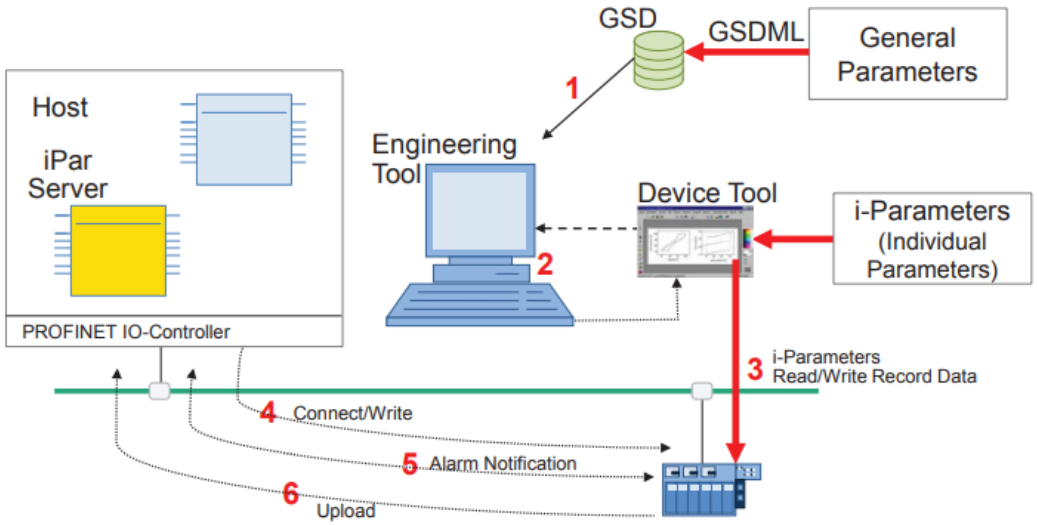


- Shared input: Multiple controllers read the same inputs on a device



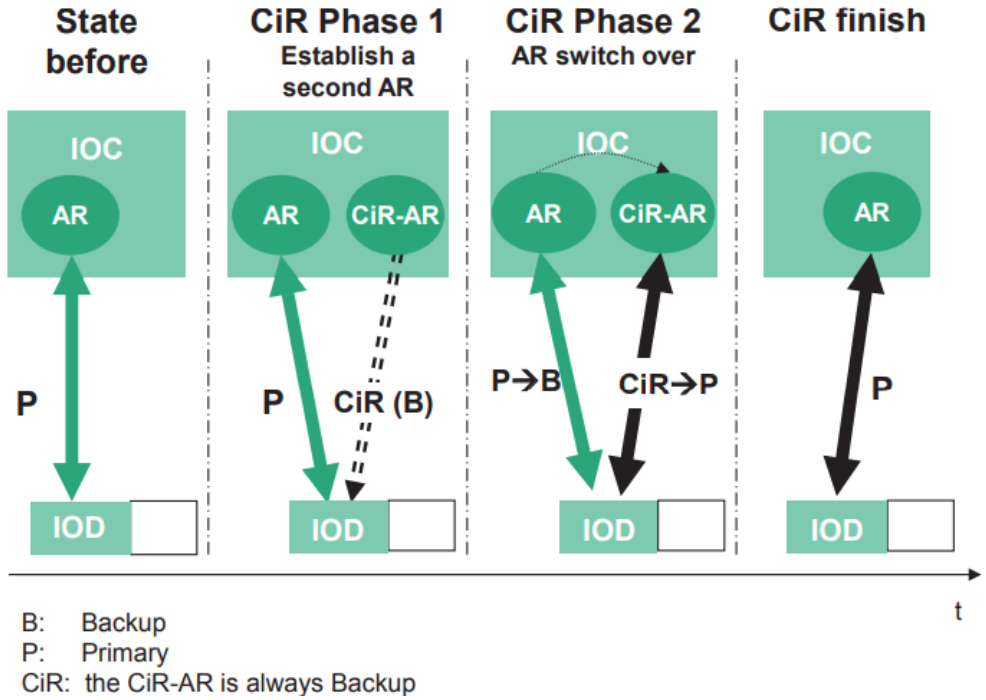
Optional functions

- A parameter server can be used to automatically reload backed-up data during device replacement



General Station Description (GSD) file is **a description of an IO device provided by the device manufacturer**

- Configuration in Run



"Configuration in Run" measures (CiR) are carried out in PROFINET without any interruption and without adversely affecting network communication - this ensures that plant repairs, modifications, or expansions can be performed without a plant shutdown in continuous production processes.

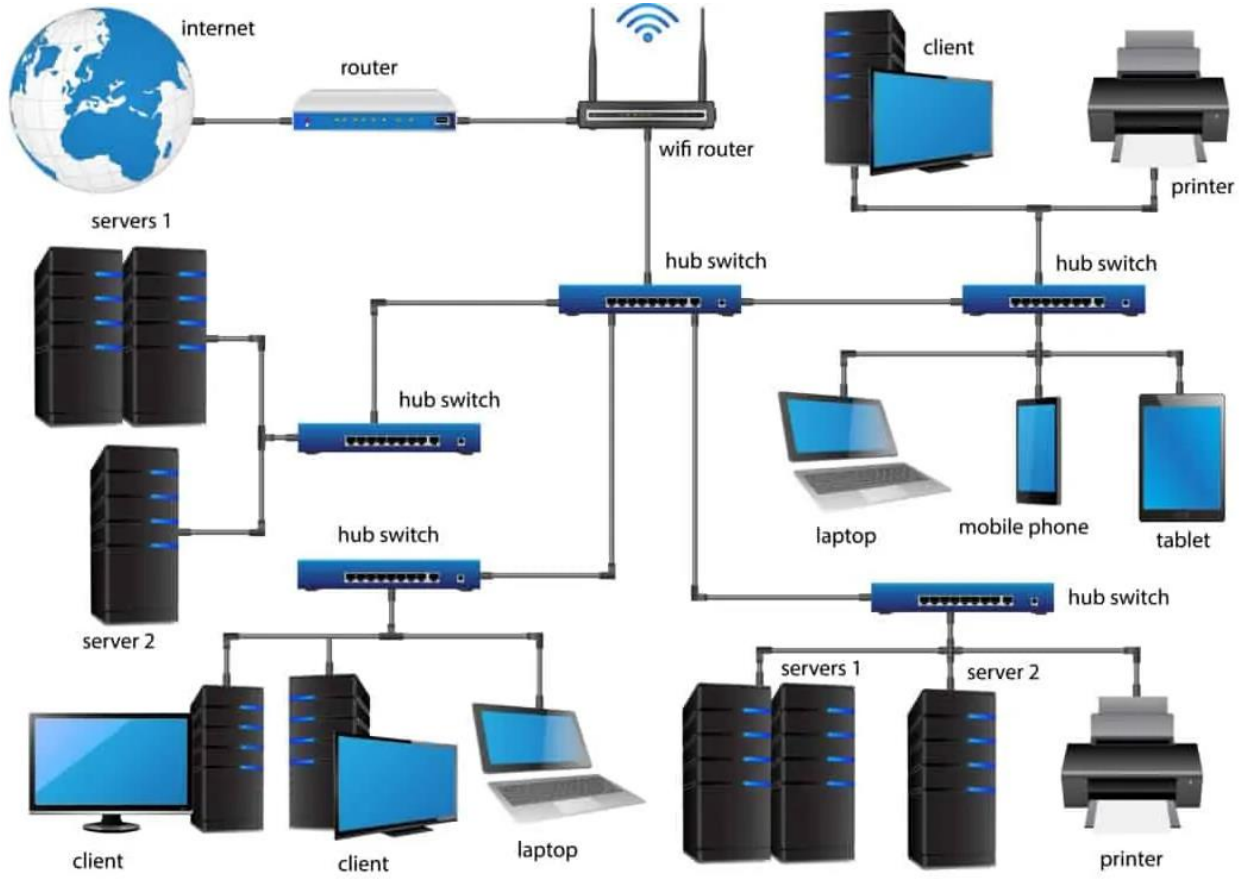
20IS709
Communication Systems For Industrial Networking

LAN System Components

Components of LAN

Three basic elements

- Hardware which is connected to form the LAN
- Software which is accessed through the LAN
- The users, who create, work with and manage the various files

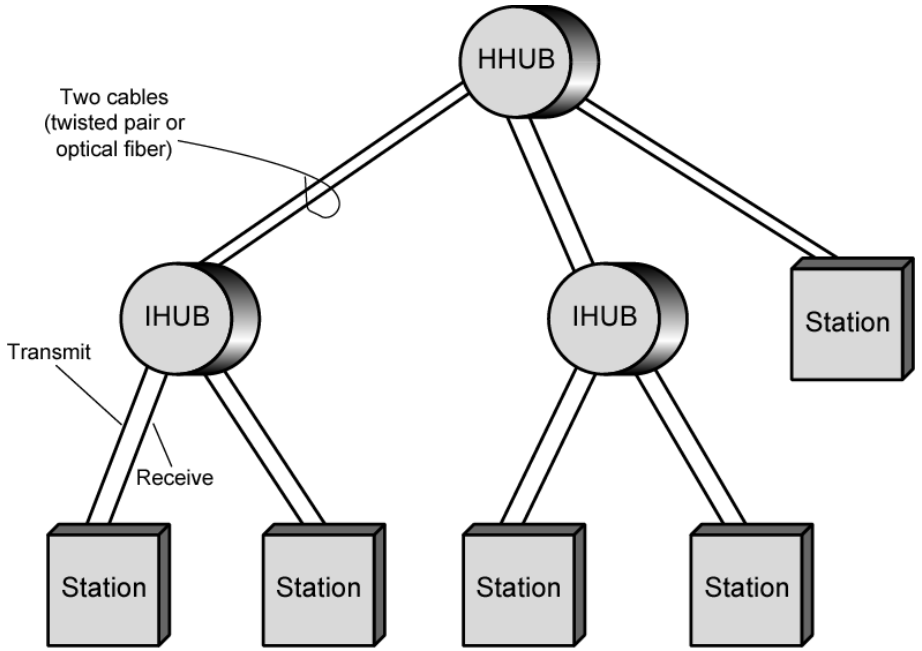


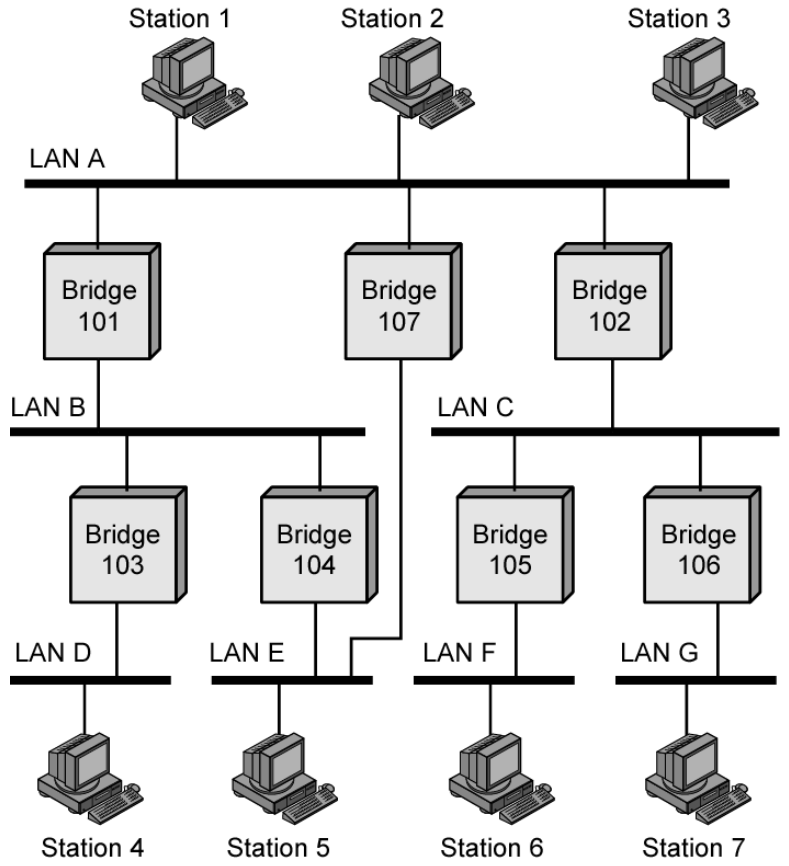
Source: https://www.itechguides.com/local-area-network/

Components of LAN

Hardware Components

- Networking Interface Card (NICs)
- Server
- Station
- Bridges
- Hub
- Switch
- Router
- Connectors



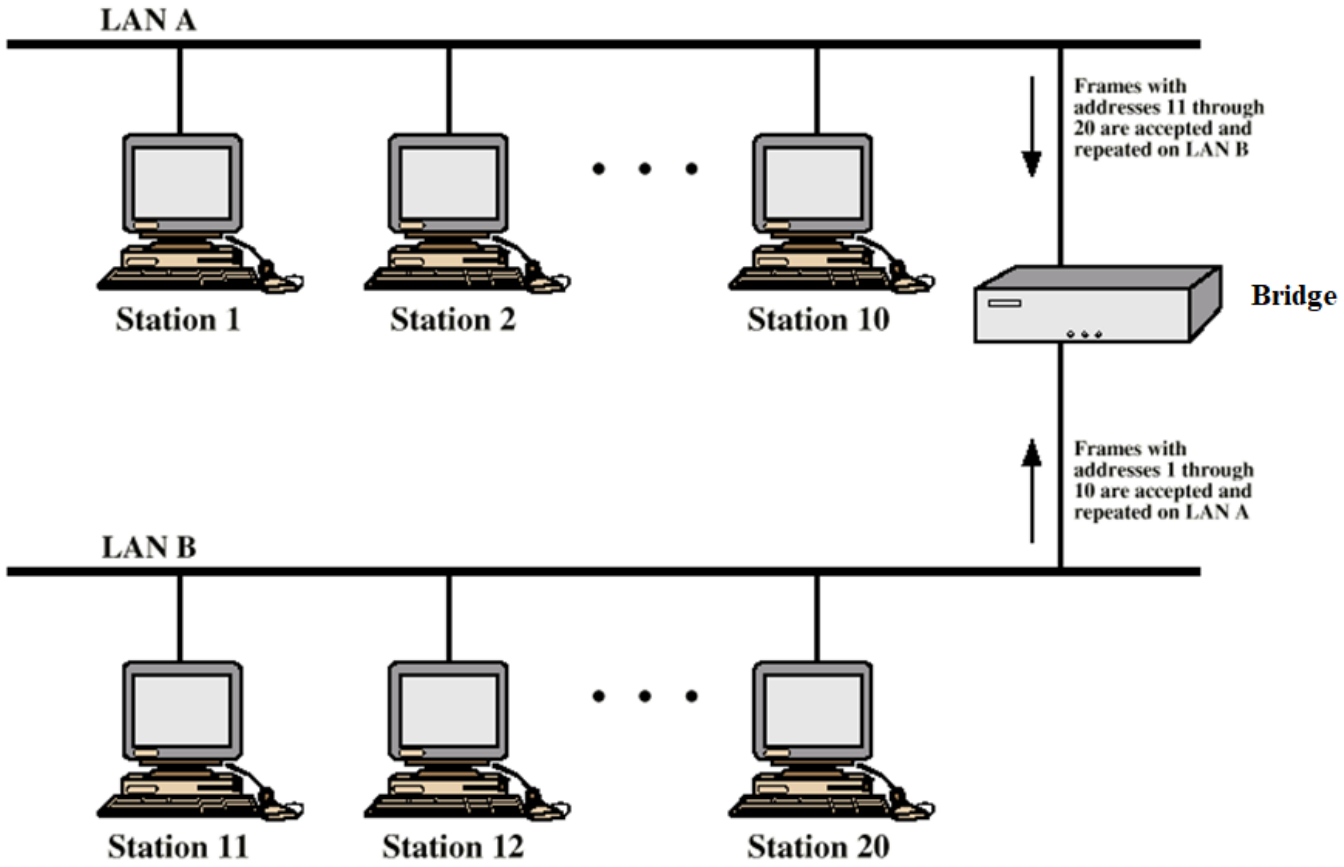


Bridges

- Ability to expand beyond single LAN to provide interconnection to other LANs/WANs
- General approaches used for this purpose: bridges and routers
- Provides a means of interconnecting similar LANs.
- The bridge is designed for use between local area networks (LANs) that use identical protocols for the physical and link layers - the amount of processing required is minimal.
- Why Bridge?
  - Reliability: connecting all data processing devices in an organization to one network may disable communication during fault - using bridges, the network can be partitioned into self-contained units.
  - Performance: A number of smaller LANs will often give improved performance if devices can be clustered so that intra-network traffic significantly exceeds inter-network traffic.
  - Security: The establishment of multiple LANs may improve security of communications.
  - Geography: Two separate LANs are needed to support devices clustered in two geographically distant locations.

Functions of a Bridge

- Read all frames transmitted on A and accept those addressed to any station on B.
- Using the medium access control protocol for B, retransmit each frame on B.
- Do the same for B-to-A traffic

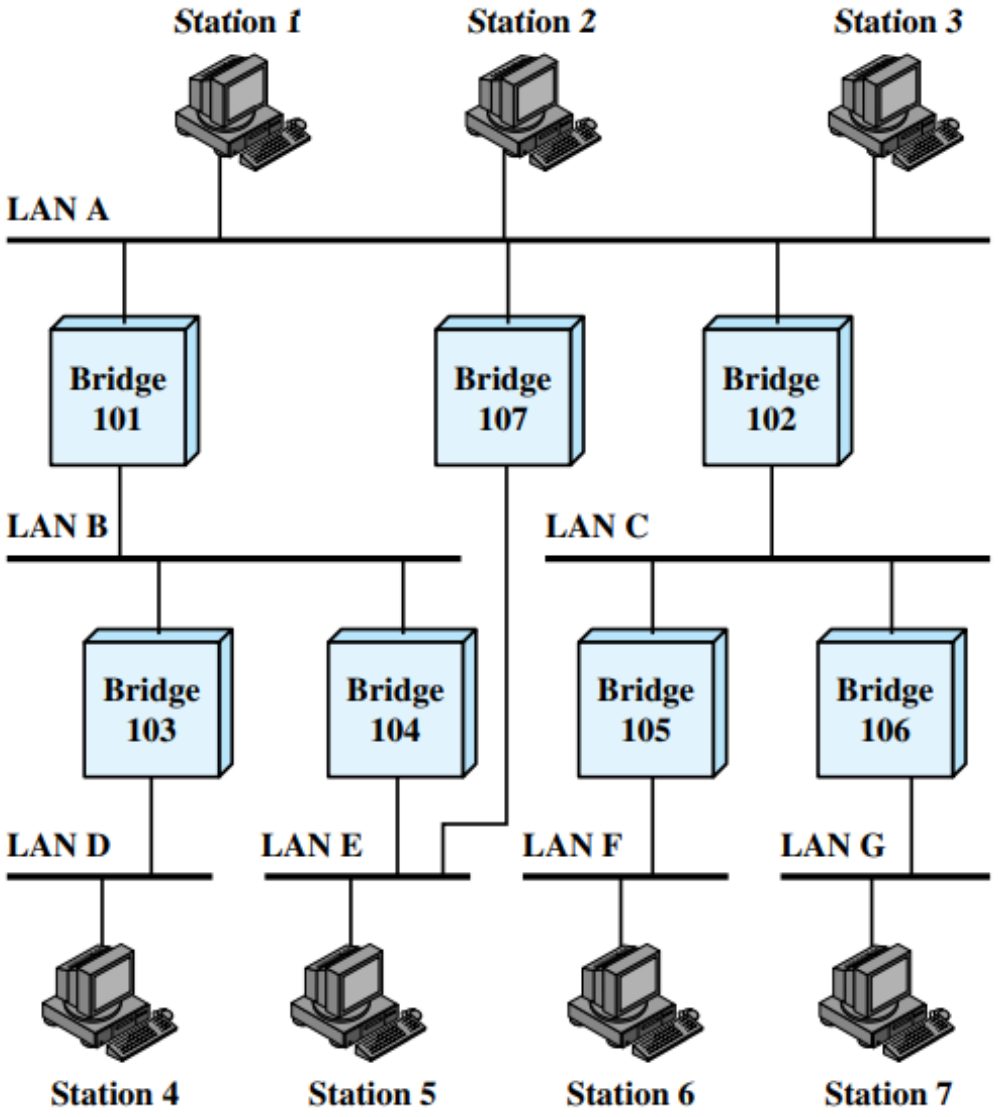


Design Aspects

- Makes no modification to the content or format of the frames it receives, nor does it encapsulate them with an additional header - each frame to be transferred is simply copied from one LAN and repeated with exactly the same bit pattern on the other LAN – use same protocol
- There may be more than two LANs interconnected by a number of bridges - a frame may have to be routed through several bridges in its journey from source to destination.
- Should contain enough buffer space to meet peak demands – frames may arrive faster than they can be retransmitted

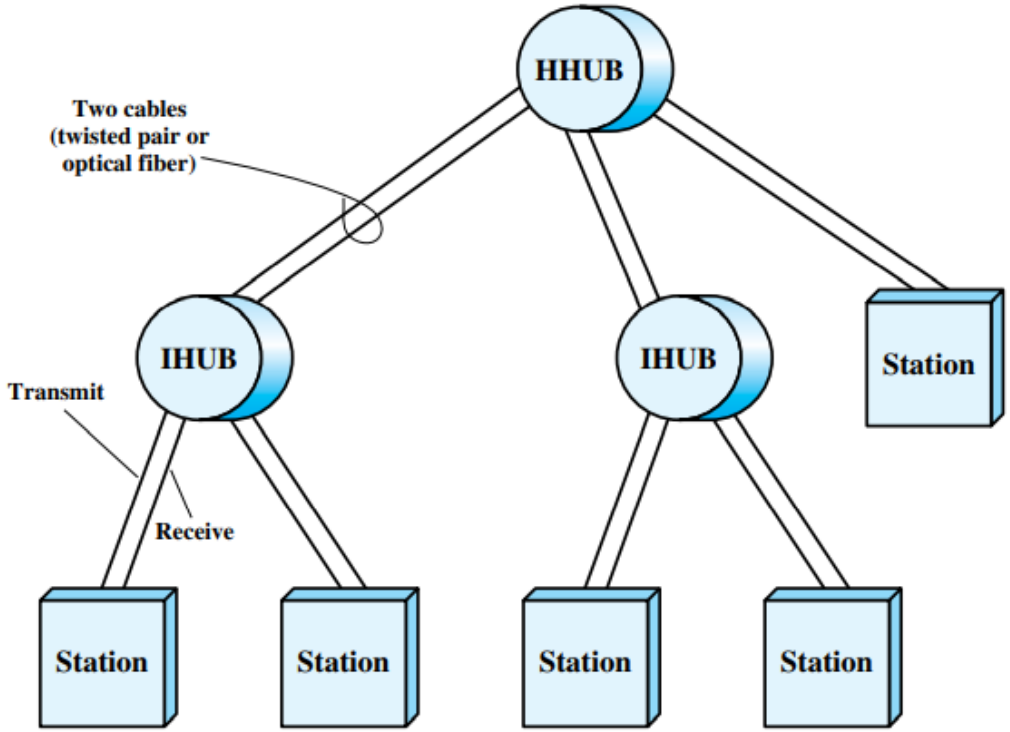
Configuration of Bridges with Alternate Routes

- Increasing number of LANs interconnected by bridges in organizations.
- As the number of LANs it becomes important to provide alternate paths between LANs via bridges for load balancing and reconfiguration in response to failure.
- Many organizations will find that static, preconfigured routing tables are inadequate and that some sort of *dynamic routing is needed*.
- When a bridge receives a frame, it must decide whether or not to forward it.
- If the bridge is attached to two or more networks, then it must decide whether or not to forward the frame and, if so, on which LAN the frame should be transmitted.



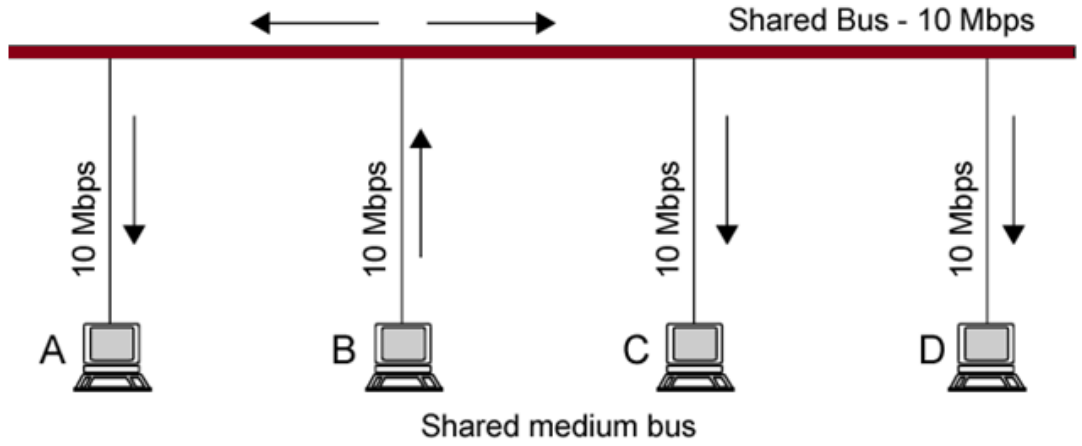
Hubs

- Active central element of star layout
- Each station connected by two lines
  - Transmit and receive
- Hub acts as a repeater - When single station transmits, hub repeats signal on outgoing line to each station
- Line consists of two unshielded twisted pairs
- Limited to about 100 m
  - Due to high data rate and poor transmission qualities of Unshielded Twisted Pair
- Optical fiber may be used - Max about 500 m
- Physically star, logically bus
- Transmission from any station received by all other stations - If two stations transmit at the same time, collision
- Multiple levels of hubs cascaded
- In two-level configuration - one header hub (HHUB) and one or more intermediate hubs (IHUB)

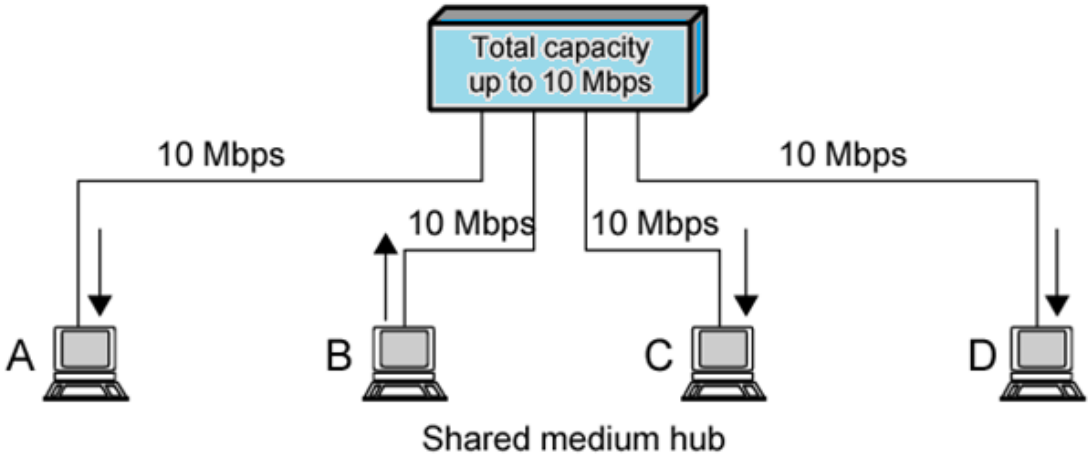


Buses and Hubs

- Bus configuration
  - All stations share capacity of bus (e.g. 10Mbps)
  - Only one station transmitting at a time



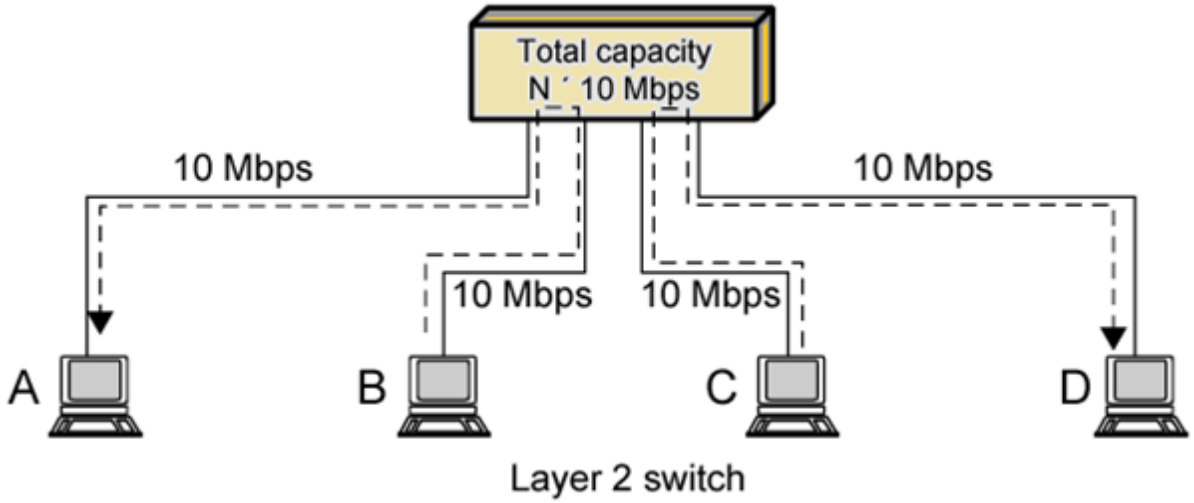
- Hub uses star wiring to attach stations to hub
  - Transmission from any station received by hub and retransmitted on all outgoing lines
  - Only one station can transmit at a time
  - Total capacity of LAN is 10 Mbps



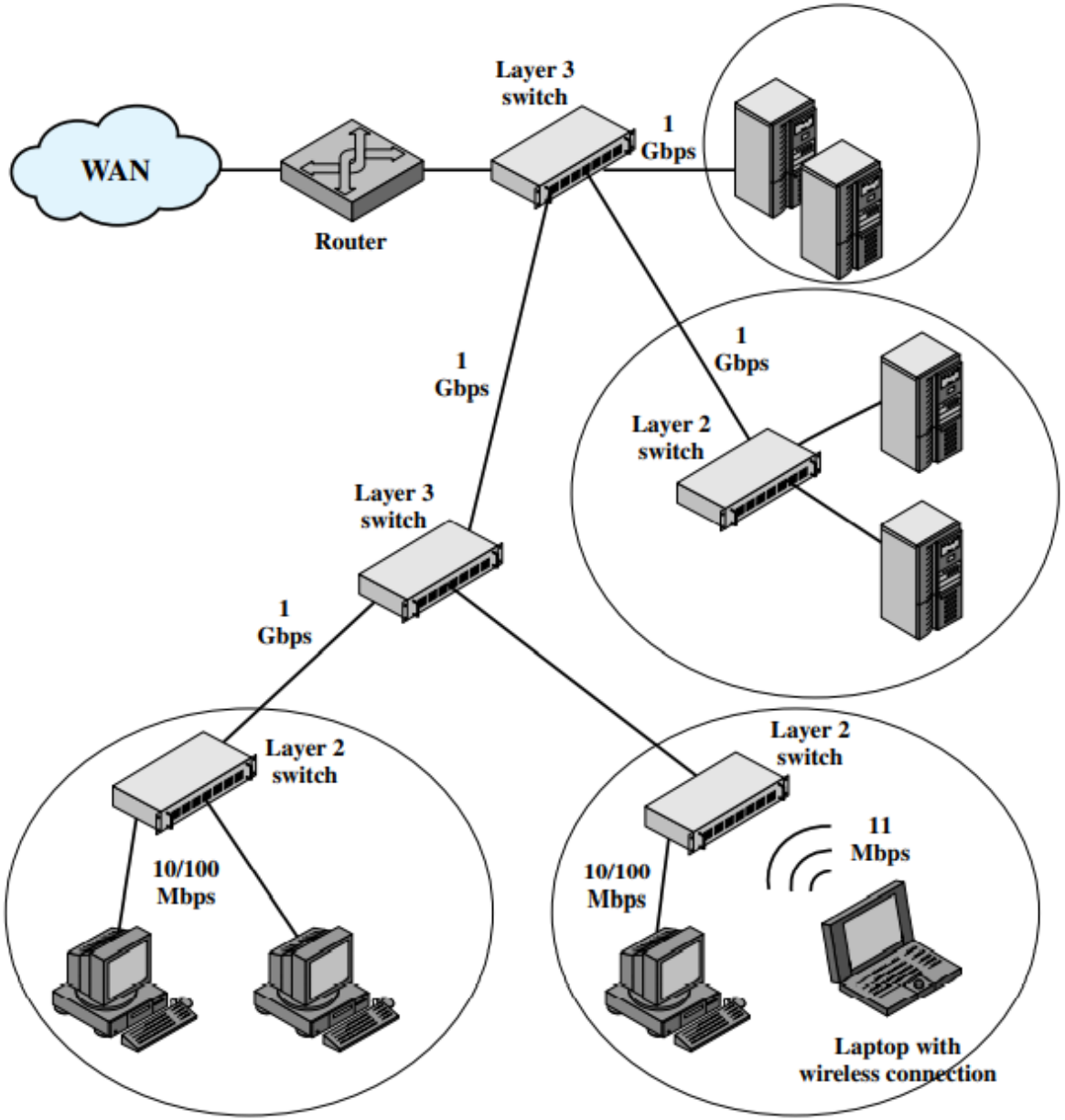
- Improve performance with layer 2 switch

Layer 2 Switches

- Central hub acts as switch
- Incoming frame from particular station switched to appropriate output line to be delivered to the intended destination
- Unused lines can switch other traffic
- More than one station transmitting at a time
- Multiplying capacity of LAN
  - Example: B is transmitting a frame to A and at the same time C is transmitting a frame to D - the current throughput on the LAN is 20 Mbps, although each individual device is limited to 10 Mbps.



Typical Large LAN Organization



References

1. David Bailey Edwin Wright, “Practical SCADA for Industry”, 1st Edition, Elsevier, 2003.
2. Perry S. Marshall, John S. Rinaldi, “Industrial Ethernet”, 2nd Edition, The Instrumentation, Systems, and Automation Society, 2004
3. Deon Reynders, Edwin Wright, “Practical TCP/IP and Ethernet Networking for Industry”, Elsevier 2003.
4. William Stallings, “Data and Computer Communications”, 8th Edition, Pearson Prentice Hall, 2007
5. Jan Axelson, “Embedded Ethernet and Internet Complete”, Lakeview Research LLC, 2003.
6. PROFINET System Description Technology and Application, Version October 2014, PROFIBUS & PROFINET International (PI)