

Chapter 4

NETWORK TECHNOLOGIES DEPLOYED IN SUPERVISORY CONTROL & DATA ACQUISITION SYSTEMS

Dr. H.K. VERMA

Distinguished Professor

Department of Electrical and Electronics Engineering

School of Engineering and Technology

SHARDA UNIVERSITY

Greater Noida, India

website: profhkverma.info

1. Introduction

As explained in Chapter 3, titled “Hardware of Supervisory Control & Data Acquisition System”, communication in a SCADA system takes place (a) between the master terminal unit (MTU) and the associated remote terminal units (RTUs) and (b) between a remote terminal unit (RTU) and the associated field devices. The MTU-RTU communication takes place via a data network, which is generally either a LAN or a WAN. On the other hand, individual analog or digital signal links are used between an RTU and the field devices associated with it. However, if any of the field devices are intelligent electronic devices (IEDs), equipped with data communication port or network connectivity, they can communicate with the RTU on a LAN created for this purpose. Thus these IEDs communicate with the MTU through an RTU to which they are networked. Alternatively, the IEDs can communicate with the MTU directly on such a LAN. Some examples of the IEDs are the intelligent digital protective relays, digital feedback controllers, sequence-of-events recorder, alarm annunciator, smart multifunction meters, smart sensors and intelligent actuators.

The LAN technologies and protocols commonly used for

- (a) MTU-RTU networking,
- (b) RTU-IED networking, or
- (c) MTU-RTU networking

are listed below under two categories of ‘wire’ and ‘wireless’ network technologies/ protocols:

1.1 Wire Network Technologies/ Protocols

- (a) EtherNet/ IEEE 802.3 (Standard Ethernet)
- (b) EtherNet/ IP (Industrial Ethernet)
- (c) RS-485
- (d) ModBus over Serial Line
- (e) ModBus over TCP/IP
- (f) Foundation FieldBus
- (g) ProfiBus
- (h) CANBus

1.2 Wireless Network Technologies/ Protocols

- (a) WiFi/ IEEE802.11
- (b) Zigbee/ IEEE802.15.4

Some of the above LAN technologies/ protocols, like EtherNet/ IEEE 802.3 (Standard Ethernet) and WiFi/ IEEE802.11, are very old and popular for business data networking and, therefore, information on them is readily available in books. This chapter describes some of the technologies/ protocols, which are either specially important or have specifically been developed for industrial control and instrumentation applications. Only the important aspects relevant to their application in SCADA are dealt with here.

2. RS-485

RS-485 (or EIA-RS-485, for the sake of completeness) is known as “Standard for Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multipoint Systems”. Recommended by EIA, it is now an industry standard.

EIA-RS485 is used in field-device level networks in distributed data acquisition, distributed control and SCADA systems. Being very simple to understand, implement and operate, it is one of the most popular wired-network protocols/ technologies used for networking of an RTU with intelligent field devices in SCADA systems. It may also be suitable for MTU-RTU networks of relatively simpler and smaller SCADA systems.

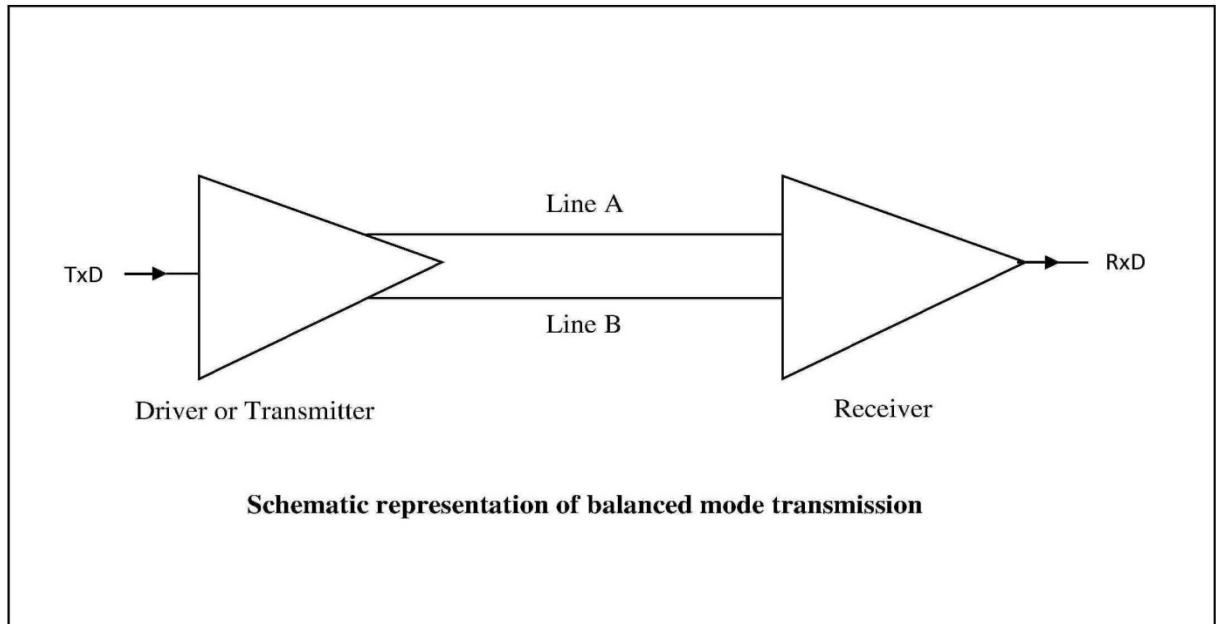
2.1 Main Features

- (i) Specifies balanced or differential mode signals for transmission
- (ii) Supports Master-Slave mode of communication
- (iii) Supports half-duplex as well as full-duplex communication
- (iv) Supports multi-point (party-line) topology
- (v) Connectors are not specified
- (vi) Allows up to 32 drivers and 32 receivers in the network
- (vii) Maximum data rate of 10 Mbps @ cable length upto 12m
- (viii) Maximum cable length of 1200m @ 100 kbps data rate.

2.2 Balanced or Differential Mode of Transmission

In this mode of transmission, illustrated in the following figure, the driver (transmitter) converts single ended (SE) input signal to a differential output signal, which is then transmitted on a pair of copper wires. Neither of the two wires is grounded. The receiver detects and translates the differential signal received by it back to a SE signal. Twisted pair is used to achieve transposition of the two wires, which ensures that the noise voltage induced by an

external signal source or closely running power lines on the two wires is nearly equal or, in other words, the differential-mode noise induced in the circuit is nearly zero.



2.3 Signal Levels

A driver conforming to the RS-485 standard provides a differential output of a minimum of ± 1.5 V across a 54-ohm load. An RS-485 conforming receiver, on the other hand, is expected to detect a differential input down to ± 200 mV. The two values provide a sufficient margin for a reliable data transmission even if there is a severe degradation of signals across the cable and the connectors. The following two factors make RS-485 network robust and suitable for long-distance networking in noisy environment:

- (a) The receiver is sensitive to differential signals only, due to which any common-mode noise induced in the two wires is rejected by it.
- (b) The minimum differential output of drivers is much higher (± 1.5 V) than the minimum differential input signal that can be detected by receivers (± 0.2 V).

2.4 Master-Slave Mode of Communication

The master-slave mode of communication, that takes place between the nodes in a RS-485 network, is defined as under:

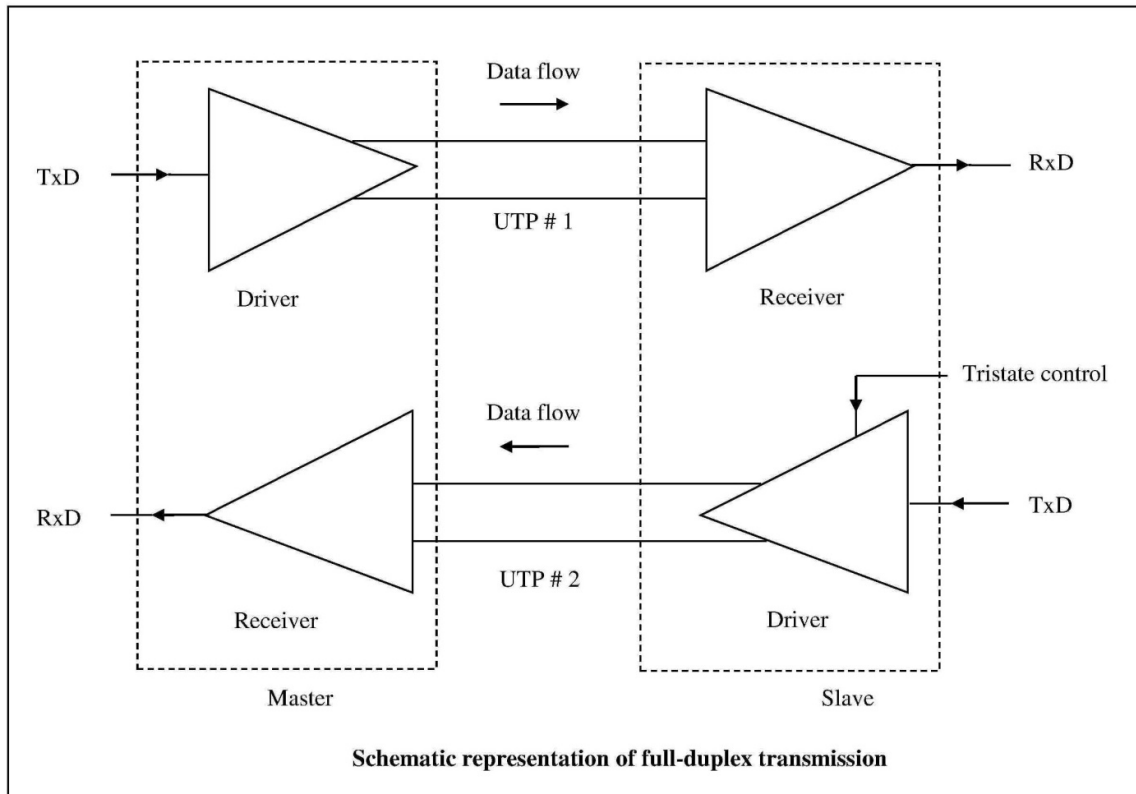
- (a) Communication is always initiated by a 'master node'
- (b) A 'slave node' transmits data (replies) only on master's request
- (c) Slave nodes never communicate with each other.

2.5 Duplex Transmission on RS-485 Network

As mentioned under “Main Features”, RS-485 supports both half-duplex and full-duplex transmissions. The two types of transmissions in RS-485 networks are described in the next two sub-sections.

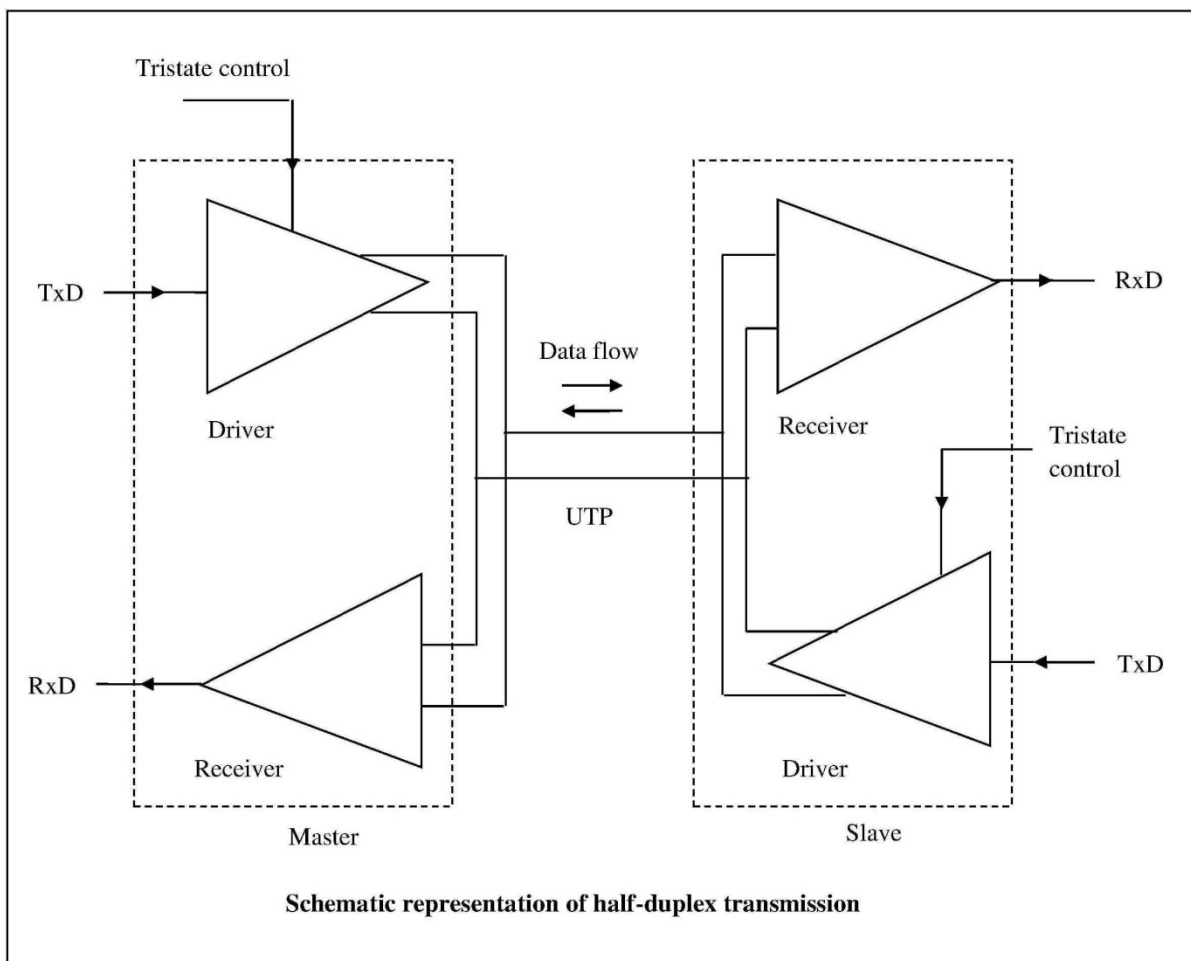
2.5.1 Full-Duplex Transmission on RS-485 Network

- (a) Two unshielded twisted pairs (UTPs) of wires are used as shown in the following diagram.
- (b) Master always initiates dialogue on one UTP.
- (c) The addressed (polled) slave responds on the other UTP.
- (d) Driver of master is always enabled, hence needs no tri-state capability.
- (e) Drivers of all slaves should have tri-state capability so that transmitter of only one slave, which has been addressed by the master, is electrically connected to respond while other slaves remain disconnected through high-Z state.



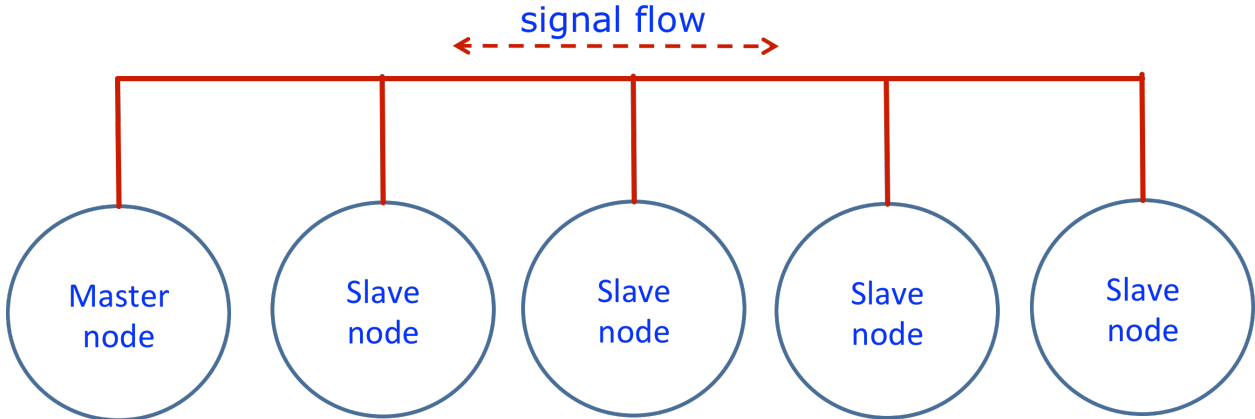
2.5.2 Half-Duplex Transmission on RS-485 Network

- (a) Only one unshielded twisted pair (UTP) of wires is used as shown in the following diagram.
- (b) Master initiates a dialogue and the addressed (polled) slave responds on the same UTP.
- (c) Drivers of all slaves as well as that of the master should have tri-state capability so that transmitter of only one slave, which has been addressed by the master, is electrically connected to respond while transmitters of other slaves and the master remain disconnected through high-Z state.



2.6 RS-485 Network Topology

The RS-485 standard supports party-line or bus topology of network. In bus topology, illustrated in the following figure, the nodes are connected to a main cable trunk via short stubs.



Basic structure of RS-485 bus

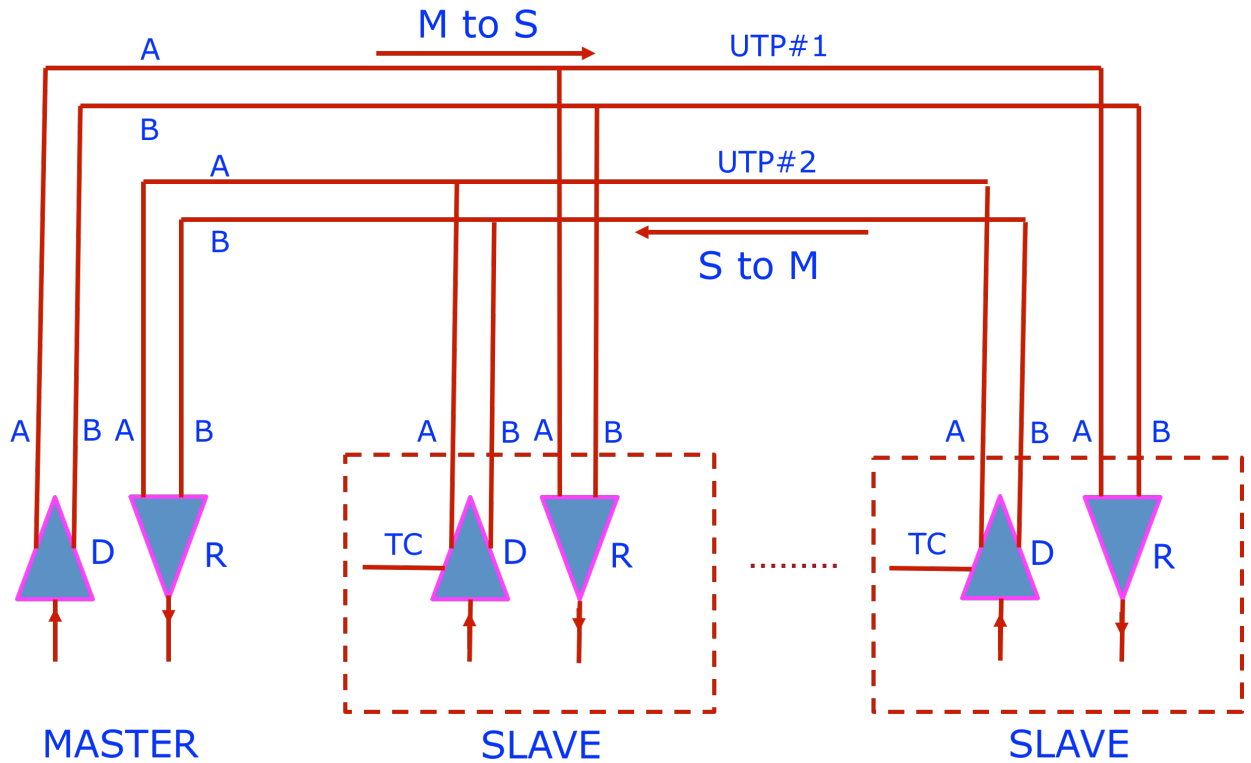
Alternatively, the nodes may be wired in a daisy-chain formation. Full-duplex and half-duplex implementations of RS-485 bus topology are now taken up separately.

2.6.1 Full-Duplex Implementation of RS-485 Bus Topology

The full-duplex implementation requires two pairs of wires, as shown in the figure below. The driver of the master and the receivers of all the slaves are connected to the upper wire-pair, which therefore provides a transmission path to the signals from the master to the slaves. The receiver of the master and the drivers of all the slaves are wired to the lower wire-pair.

As shown in the figure, the drivers of all slaves must have tri-state control (TC), so that the driver of only one slave is enabled (made active) at any time to avoid bus contention. Thus, the lower wire-pair transmits signals from the enabled slave to the master.

Use of two wire-pairs can allow simultaneous signal transmission from and to the master node, although the master-slave protocol does not need simultaneous signal transmission by the master and any slave.

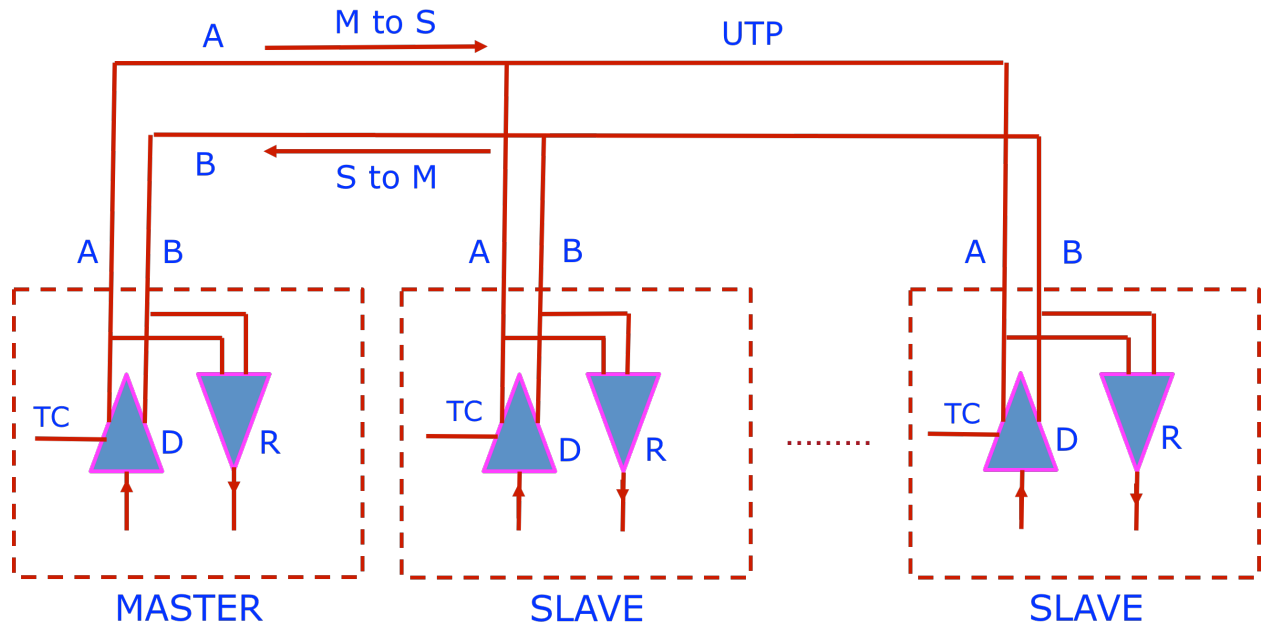


Full-duplex implementation of RS-485 bus

2.6.2 Half-Duplex Implementation of RS-485 Bus Topology

The half-duplex implementation requires a single pair of wires, as shown in the figure below. The drivers and receivers of all the nodes, master node as well as slave nodes, are connected to the same wire-pair. Signal transmission at any time, therefore, can take place in one direction only, that is, either from the driver of the master to all receivers or from the driver of a slave to all receivers.

In this case, as shown in the figure, the drivers of not only the slaves but that of the master must have tri-state control (TC). Only one driver (either that of the master or of a slave) should be enabled at any time to avoid bus contention..



Half-duplex implementation of RS-485 bus

3. ModBus over Serial-Line

It is an open serial-communication protocol, specially suitable for field-device level networks. Developed and introduced in 1979 by Modicon for use in PLCs, it is now an industry standard. At present, the ModBus has three variants or implementations:

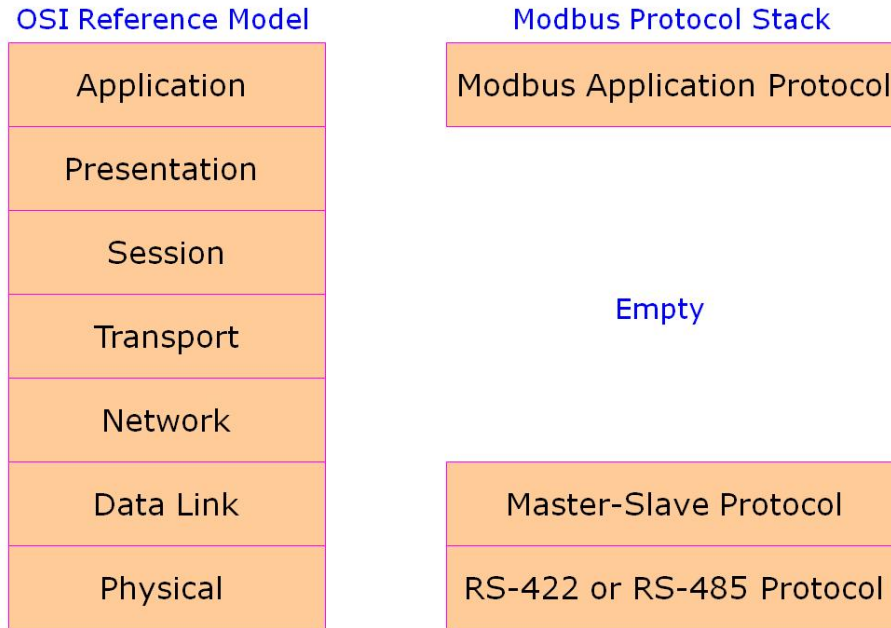
- a) ModBus over serial-line
- b) ModBus over TCP/IP
- c) ModBus Plus: ModBus over high-speed token-passing network

Only the first variant, i.e. “Modbus over serial line”, will be described here.

3.1 ModBus Protocol Stack

Protocol Stack of the “ModBus over serial-line” has only three of the seven layers of OSI Reference Model, as shown in the following figure. Other layers are not defined in this protocol.

- a) **Physical Layer:** ModBus over serial line specifies two serial line options, namely, RS-422 and RS-485, and two data transmission modes, namely, RTU and ASCII.
- b) **Data Link Layer:** The MAC protocol specified is the master-slave protocol.
- c) **Application Layer:** This layer is completely specified in ModBus.



ModBus Protocol Stack mapped to OSI Reference Model

3.2 Master-Slave Protocol

The master-slave protocol is defined as under:

- (a) Communication is always initiated by master
- (b) A slave transmits data (replies) only on master's request
- (c) Slave nodes never communicate with each other
- (d) Master node initiates only one transaction at a time
- (e) Master's request to slaves is either in "Unicast" mode or in "Broadcast" mode.

In Unicast Mode, the master addresses an individual slave and only the addressed slave replies to the master.

In Broadcast Mode, the master addresses all the slaves on the bus, all the slaves accept this "broadcast message" for "writing function" and no reply is sent to the master by any slave.

3.3 ModBus Address Space

Addresses in ModBus are 8-bit in size and thus their range is 0 to 255 (decimal). The allocation of addresses is shown in the table below:

| Address | Purpose |
|---------|--------------------------------|
| 0 | Broadcast address |
| 1-247 | Individual addresses of slaves |
| 248-255 | Reserved |

3.4 Data Transmission in RTU Mode

a) Coding System

The coding system in RTU mode uses 8-bit binary-data bytes and two hexadecimal characters per byte. Further, the hexadecimal characters used are 0-9 and A-F.

b) Bit Sequence for Transmission

The number of bits transmitted per data byte is 11. If a parity bit is transmitted, then there is one start bit and one stop bit. On the other hand, if no parity bit is transmitted, then there is one start bit and two stop bits. The two bit sequences are illustrated below:

(i) Bit Sequence for transmission, if parity is used:

| | | | |
|-----------|-----------------------------|------------|----------|
| Start Bit | 8 data bits (LSB... MSB) | Parity bit | Stop bit |
|-----------|-----------------------------|------------|----------|

(ii) Bit Sequence for transmission, if parity is not used:

| | | | |
|-----------|-----------------------------|----------|----------|
| Start Bit | 8 data bits (LSB... MSB) | Stop bit | Stop bit |
|-----------|-----------------------------|----------|----------|

c) Message Frame

The message frame in RTU mode has four fields as described in the table below:

| Field | No. of Bytes | Master-to Slave Message (Request) | Slave-to-Master Message (Response) |
|------------------|--------------|--|------------------------------------|
| 1. Address | 1 | Slave address | Slave address |
| 2. Function Code | 1 | Indicates to slave the kind of action to perform | Indicates the kind of response |
| 3. Data | 0 to 252 | Request parameters | Response parameters and values |
| 4. Error Check | 2 | Cyclic redundancy check | Cyclic redundancy check |

3.5 Data Transmission in ASCII Mode

a) Coding System

The coding system in ASCII mode uses 7-bit ASCII characters.

b) Bit Sequence for Transmission

The number of bits transmitted per ASCII character is 10. If a parity bit is transmitted, then there is one stop bit and if parity bit is not transmitted, then there are two stop bits, as illustrated in the next figure.

(i) Bit Sequence for Transmission, if Parity is used:

| | | | |
|-----------|----------------------------|------------|----------|
| Start Bit | 7 data bits (LSB...MSB) | Parity bit | Stop bit |
|-----------|----------------------------|------------|----------|

(ii) Bit Sequence for Transmission, if Parity is not used:

| | | | |
|-----------|----------------------------|----------|----------|
| Start Bit | 7 data bits (LSB...MSB) | Stop bit | Stop bit |
|-----------|----------------------------|----------|----------|

c) Message Frame

The message frame in ASCII mode has 6 fields, the details of which are given below:

| Field | No. of Characters | Master-to Slave Message (Request) | Slave-to-Master Message (Response) |
|---------------------|-------------------|--|------------------------------------|
| 1. Start Delimiter | 1 | : | : |
| 2. Address | 2 | Slave Address | Slave Address |
| 3. Function Code | 2 | Indicates to slave the kind of action to perform | Indicates the kind of response |
| 4. Data | 0 to 504 | Request parameters | Response parameters and values |
| 5. Error Check Code | 2 | LRC | LRC |
| 6. End Delimiter | 2 | Carriage return, Line feed | Carriage return, Line feed |

4. Zigbee/ IEEE-802.15.4

This section briefly describes the Zigbee wireless network technology and the IEEE Standard 802.15.4, to which the Zigbee technology complies.

4.1 Zigbee Wireless-Network Technology

Zigbee network technology addresses the needs of industrial measurement and control in the situations where wires are not feasible or acceptable. It is supported by Zigbee Alliance,

which is a consortium of more than 150 companies (end users, solution providers and manufacturers) and includes some very well-known names like Honeywell, Motorola, Phillips, Samsung and Mitsubishi.

The technology was developed to meet the special requirements of wireless sensor and actuator networks or field-device level wireless networks, which are as under:

- (a) Low bandwidth
- (b) Low latency
- (c) Long battery life
- (d) High data security

It is not attractive for business communication networks because of the low data rates supported. The main features of Zigbee wireless-network technology are listed below:

- (i) Data rates: 20, 40 and 250 kbps
- (ii) Transmitter power: 1 mw or more
- (iii) Range: 10 m or more
- (iv) Topologies supported: Star, Mesh (peer-to-peer) and Cluster tree
- (v) MAC logic: CSMA/CA
- (vi) Devices supported: Fixed, portable and moving
- (vii) Device addressing: Dynamic
- (viii) Transmission technique: DSSS
- (ix) Two ISM frequency bands are specified:

- (a) **900-MHz frequency band** with 2-MHz channel bandwidth and 20 and 40 kbps data rates
- (b) **2.4-GHz frequency band** with 5-MHz channel bandwidth and 250 kbps data rate.

4.2 IEEE-802.15.4 Standard

The IEEE 802.15.4 standard is lays down specifications for “Low-Rate Wireless Personal Area Networks (WPANs)”. The standard (or protocol) defines only the physical and media access control (MAC) layers of the 7-layer ISO model of communication system. Zigbee builds upon this standard and defines some upper layers as well.

The IEEE 802.15.4 protocol has several features that make it specially suitable for real-time data communication on the network, which include:

- (a) Collision avoidance through special data-transfer protocols
- (b) Reservation of guaranteed time slots

- (c) Integrated support for secure communications
- (d) Inclusion of power management functions in devices

The Standard specifies 2 types of devices:

(a) Full-Function Device (FFD)

- Can talk to any other device
- Can perform the job of a Network (or PAN) Coordinator (There is only one node in a network functioning as the Network Coordinator)
- Can function as a Coordinator
- Can function as an end device (terminal node)

(b) Reduced-Function Device (RFD)

- Can talk only to a Coordinator or the Network Coordinator
- Can function only as an end device (terminal node)
- Simpler in design than FFD

The Network (PAN) Coordinator has the following functions:

- a) Initiates all network communications
- b) Can communicate directly with any device
- c) Transmits beacon in the so-called beconing system for periodic data transfers.

4.3 IEEE-802.15.4 Physical Layer

The physical layer, which is the lowest layer of the OSI model, has the following functionalities:

- Data transmission and reception
- Translation of packets into over-the-air bits for transmission
- Translation of over-the-air bits on reception into packets
- Activation and deactivation of the radio transmitter
- Selection of channel frequency
- Clearing channel assessment for CSMA/CA
- Energy detection, i.e., computation of the signal power received by the node
- Link quality indication, i.e., determining the quality of the packets received by the node

4.4 IEEE-802.15.4 MAC Layer

The MAC protocol is based on the principle of collision avoidance. It uses carrier-sense multiple-access with carrier avoidance (CSMA/CA), in which collision is avoided by a node attempting to transmit on the given channel. If the channel is sensed busy before transmission by

a node, then the transmission is deferred by the node for a random interval, which reduces the probability of collisions on the channel.

The MAC protocol is flexible and supports 3 types (modes) of data transfers:

(a) Periodic Data Transfer

- Beaconing system is used to handle data
- Beacon is sent by Network Coordinator periodically
- Period can vary from 15.36 ms to 2.5 minutes approximately
- Period is a trade-off between message latency and power consumption
- Device wakes up, sends data if any, and then goes back to sleep mode
- As the devices sleep most of time, it is a power-saving mode.

(b) Intermittent Data Transfer

- Network coordinator sends message as and when data from a device is needed
- This mode uses a beaconless mechanism
- As the devices sleep most of time, this is also a power-saving mode.

(c) Guaranteed Time-slot Data Transfer

- Certain time slots are allotted to devices to transmit data without contention
- It is a low-latency data transfer mode.

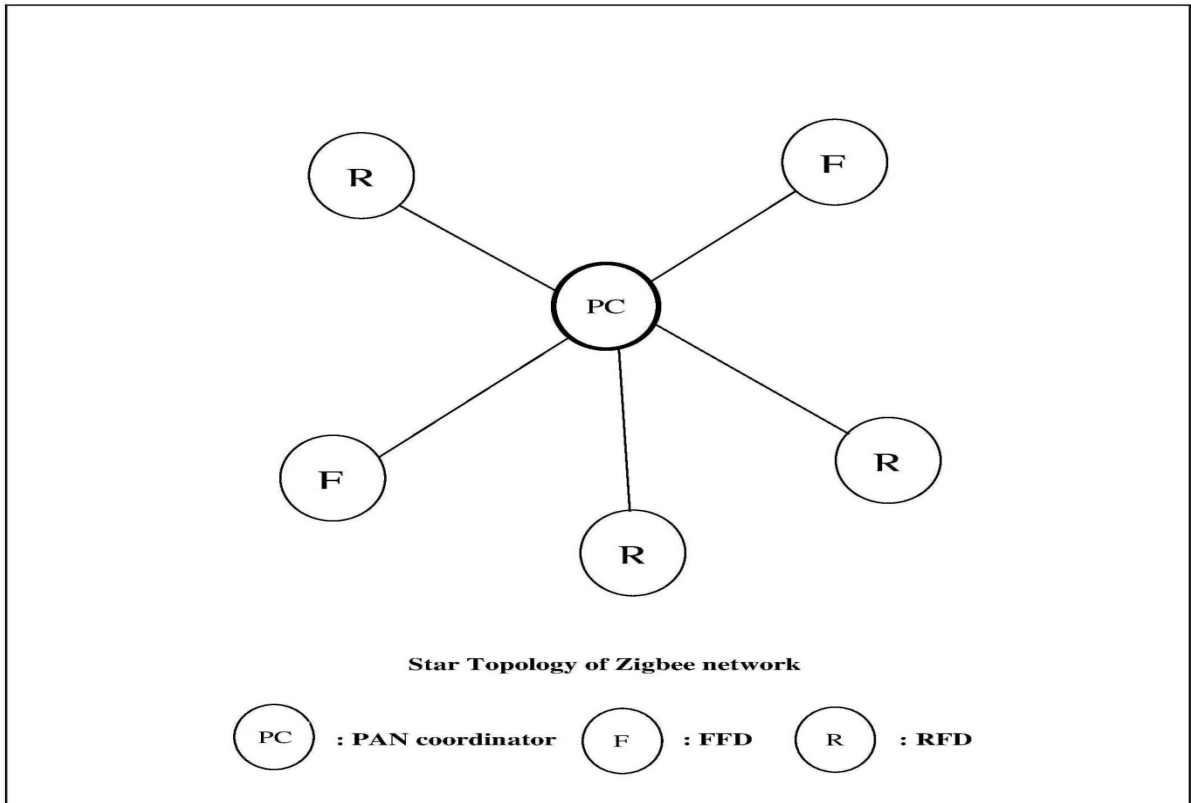
4.5 Zigbee Network Topologies

As mentioned under the main features of Zigbee, it can support three network topologies: Star topology, Mesh or peer-to-peer topology and Cluster tree topology. These are briefly described in the following paragraphs.

(a) Star Topology

In this topology, illustrated in the following figure, the PAN coordinator forms the central node to which the other nodes are connected in a star formation. The central node, therefore, has to be a full-function device (FFD) configured as PAN coordinator while each other node can be an FFD or a reduced-function device (RFD).

The advantages of star topology are its simplicity, ease of synchronization and low latency, while the disadvantage or limitation is its small scale.

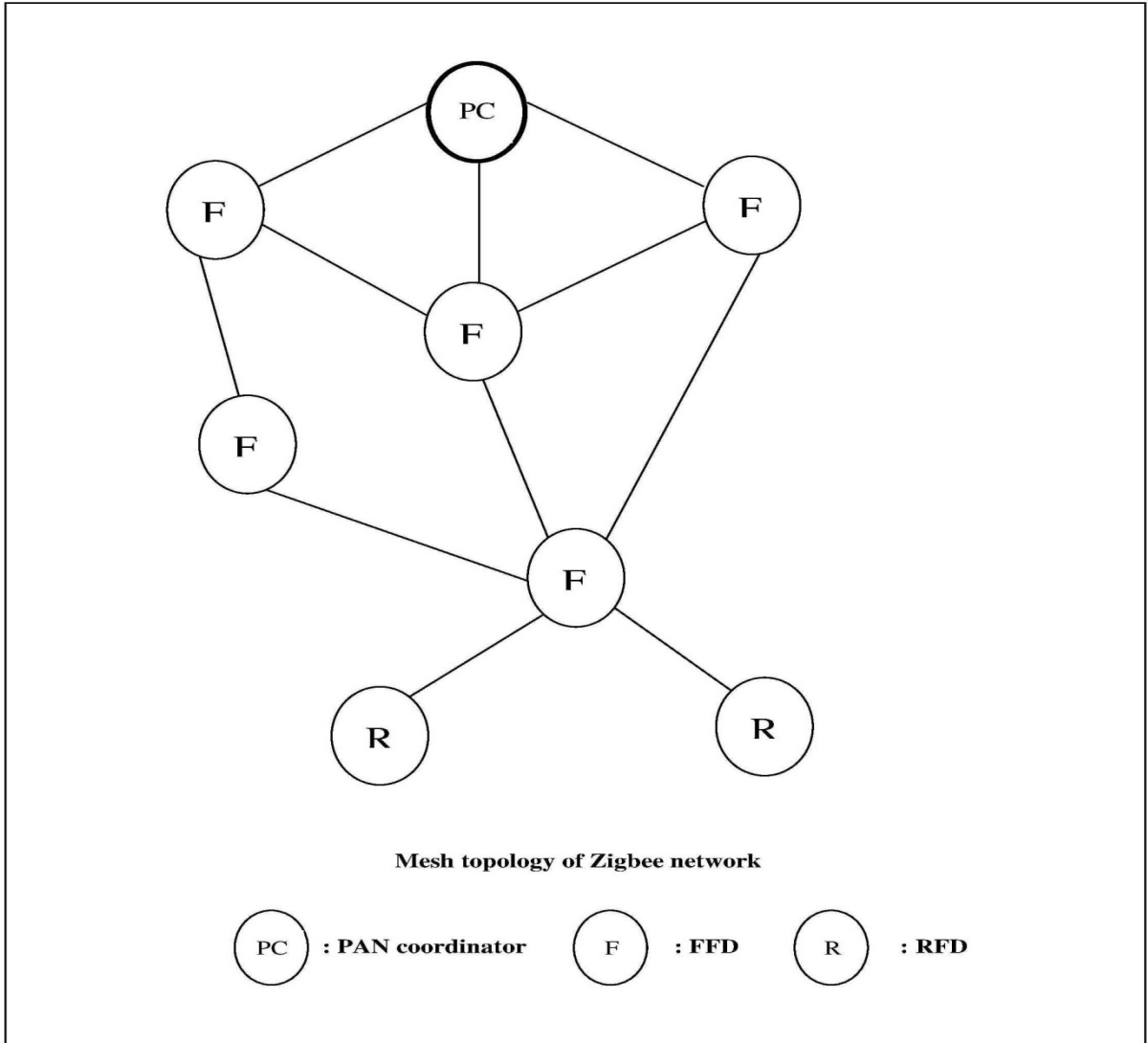


(b) Mesh or Peer-to-Peer Topology

In this topology, every node is connected to each of the other nodes. Thus each node can communicate with any other node as long as they are in the range of each other. One of the nodes is an FFD configured as PAN Coordinator. The remaining nodes in the mesh are also FFDs because of the requirement of peer-to-peer communication in the network. However, RFDs can be connected as end devices to a node in the mesh, as can be seen in the following figure.

This topology is more complex as compared to the star topology, but has several advantages:

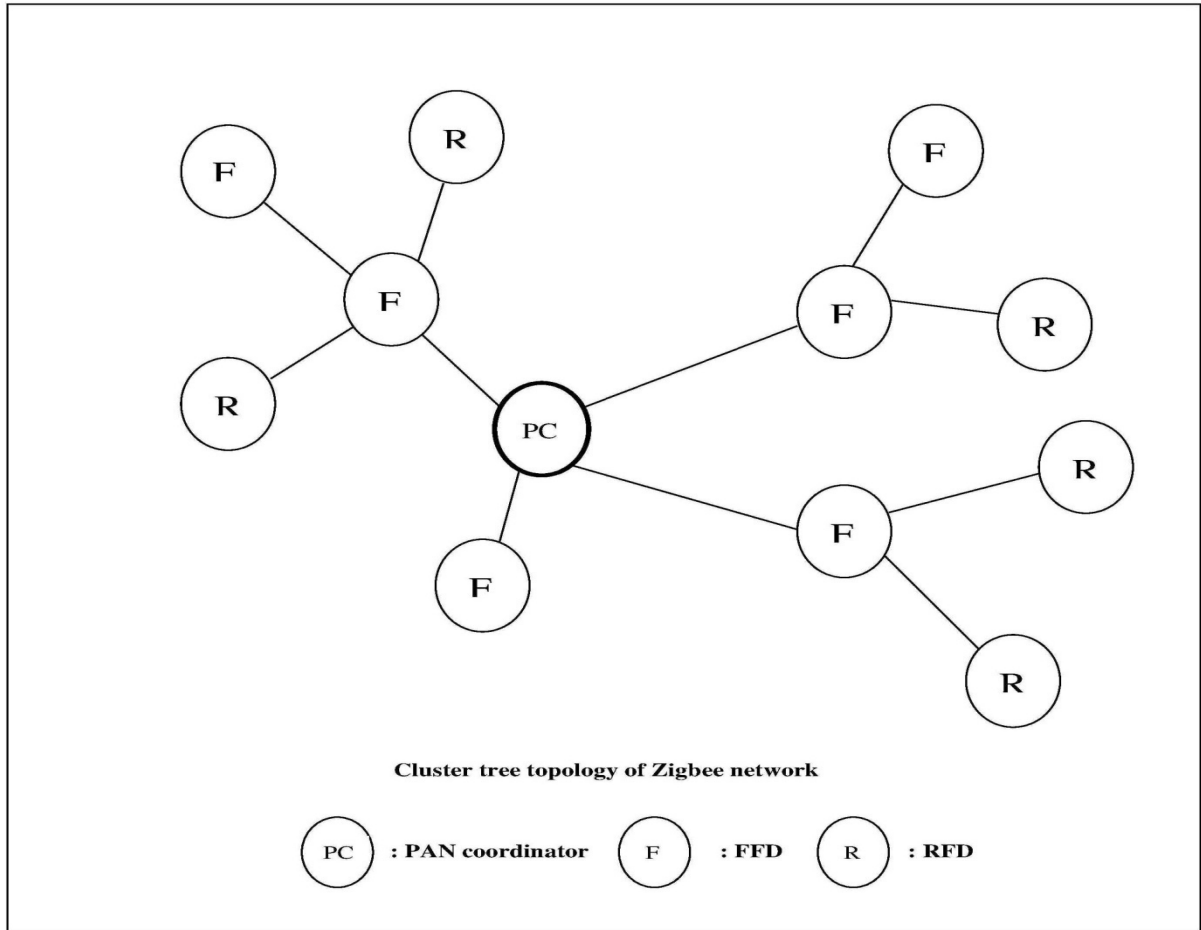
- Network is very flexible in that nodes may be easily added or removed from the network
- It is highly reliable as it provides multi-path routing and multi-hop communication
- It is easily possible to extend the range of the network because of multi-hop feature.



(c) Cluster Tree Topology

This topology is a special case of peer-to-peer topology. The PAN Coordinator acts itself as a cluster head and establishes the first cluster. It permits other devices to join or leave the network. FFDs may connect to the network as cluster heads and RFDs as end devices or leaf nodes, as shown in the following figure.

The main advantage of a cluster tree topology is that it is easily possible to extend the range of the network using multi-hop communication. The major disadvantage is that the latency may be quite long depending upon the route and number of hops involved.



4.6 Advantages and Limitations

(a) Advantages of Zigbee

Zigbee technology is preferred to WiFi technology in industrial environment because of the following advantages:

- (i) Lower cost
- (ii) Lower complexity
- (iii) Lower latency
- (iv) Lower message overhead
- (v) Lower power requirement

(b) Limitations of Zigbee

Zigbee technology is not suited to general-purpose and business-related wireless networks because of its following limitations:

- (i) Lower data rate
- (ii) Smaller range

4.7 Comparison of Zigbee with WiFi and Bluetooth Technologies

| S. No. | Feature | Zigbee | WiFi | Bluetooth |
|--------|-----------------------|----------------------------------|----------------------|---------------------|
| 1 | Data rates | 20, 40 and 240 kbps | 2, 11 and 54 Mbps | 1 Mbps |
| 2 | Range | 50-100 m | 200-500 m | 1-10 m |
| 3 | Network size | Personal area network | Local area network | Piconet |
| 4 | Topologies supported | Star and Mesh | Star | Mesh |
| 5 | ISM frequency bands | 900 MHz 2.4 GHz | 2.4 GHz & 5 GHz | 2.4 GHz |
| 6 | MAC | CSMA/CA Adhoc Peer-to-peer | CSMA Point-to-hub | Adhoc |
| 7 | Routing | Multi-hop | Single-hop | Single-hop |
| 8 | Modulation techniques | DSSS | DSSS FHSS OFDM | FHSS |
| 9 | Latency | Very low (30 ms) | High (3-5 s) | Very high (10 s) |
| 10 | Network scalability | Very high (65,000 nodes) | Good (255 nodes) | Poor (7 nodes) |
| 11 | Power consumption | Very low | High | Medium |
| 12 | Battery life | Long | Very short | Short |
| 13 | Reliability | Very high | High | High |
| 14 | Market trend | Establishing | Established | Established |

XX