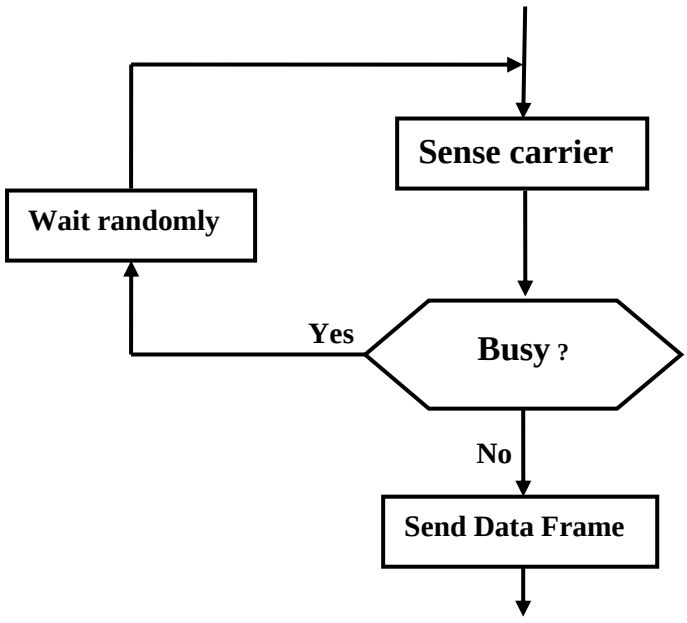
➢ Carrier Sense Multiple Accesses /Collision Detection CSMA/CD

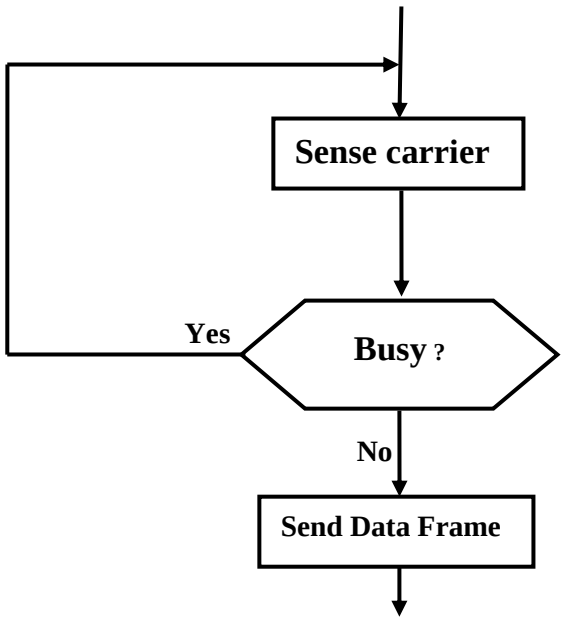
Carrier Sense:

When a station in an Ethernet network has data to transmit, it first listens to the network to see if it is in use by other stations, this is the carrier sense phase. Upon the case of the network "idle" or "busy" CSMA/CD defines what should the station do in what is called "Persistence strategy", Persistence strategies can be divided into:

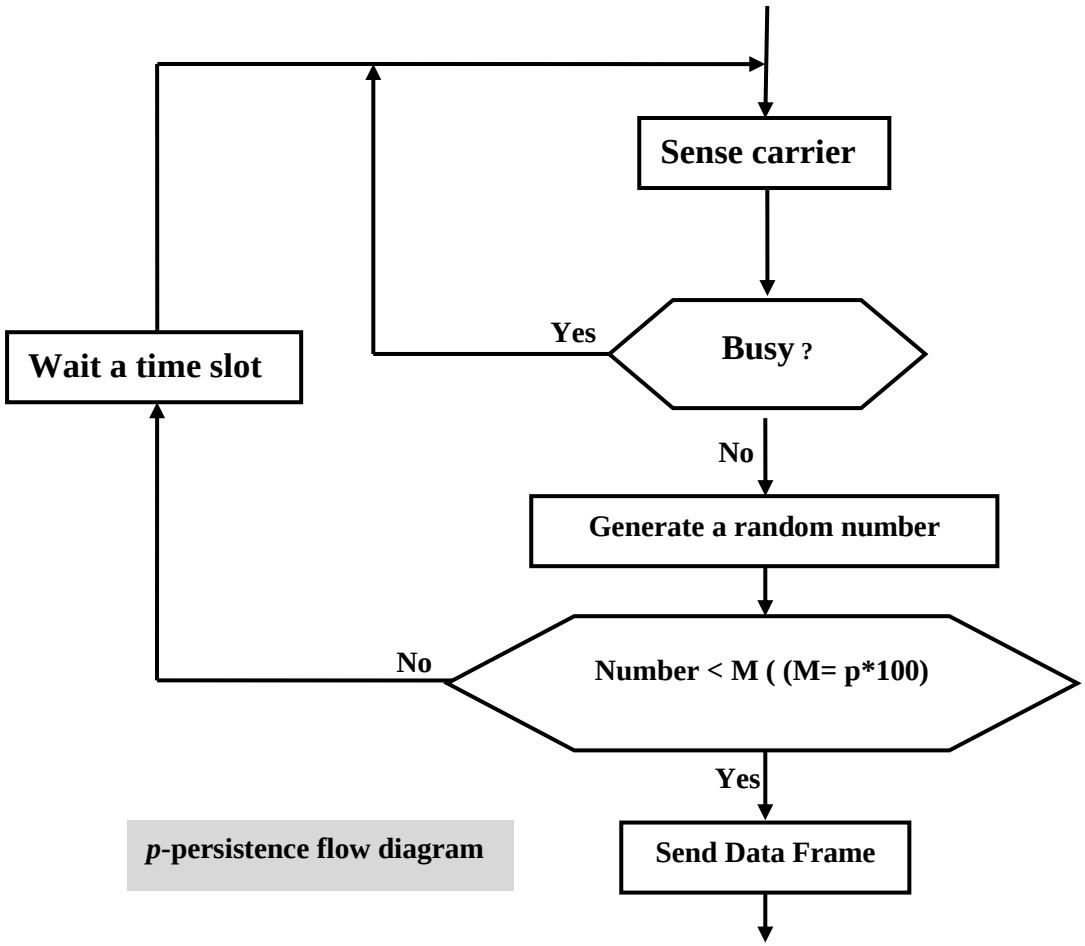
- **Non-persistence:** here the station senses the line, if it is idle it sends immediately. If the line busy; it waits a random time then senses the line again. Even random wait time reduces the chance of collision but it also reduces network efficiency.
- **1-Persistence:** here, after the station finds the line idle, it sends its data immediately (with probability 1). This method increases the chance of collision.
- ***p*-Persistence:** in this strategy after the station finds the line idle, it may or may not sends its data. Here the probability of sending is defined by p and probability of refraining is *(1-p)*. For example if *p=0.3* , then station sends with 30% of the time and refrains 70% of the time. The station generates a random number between 1 and 100. If the number generated is less than 30 the station sends its data else it waits one slot time before sensing the medium again. This method reduces the chance of collision and increases network efficiency.



Non-persistence flow



1-persistence flow diagram



p-persistence flow diagram

Multiple Access

CSMA/CD is a contention access method. Here no station is superior to another station and none of them are assigned control of others. Because all of the stations on the network are contending for access to the same network medium this phase is called the multiple access phase.

Collision detection

Even though an initial check is performed during the carrier sense phase, it is still possible for two systems on the network to transmit at the same time, causing a collision. For example, when a system performs the carrier sense, another computer has already begun transmitting, but its signal has not yet reached the sensing system. The second computer then transmits and the two packets collide somewhere on the cable. When a collision occurs, both packets are discarded and the systems must retransmit them.

The collision detection phase of the transmission process is the most important part of the operation. If the systems can't tell when their packets collide, corrupted data may reach the destination system and be treated as valid. Ethernet networks are designed so that packets are large enough to fill the entire network cable with signals before the last bit leaves the transmitting computer. This is why Ethernet packets must be at least 64 bytes long, systems pad out short packets to 64 bytes before transmission, and the Ethernet physical layer guidelines impose strict limitations on the lengths of cable segments.

As long as a computer is still in the process of transmitting, it is capable of detecting a collision on the network. On a UTP or fiber optic network, a computer assumes that a collision has occurred if it detects signals on both its transmit and receive wires at the same time. On a coaxial network, a voltage spike indicates the occurrence of a collision. If the network cable is too long or if the packet is too short, the probability of collision increased.

Jam signal

When a system detects a collision, it immediately stops transmitting data and starts sending a jam pattern instead. The jam pattern serves as a signal to each system on the network that a collision has taken place, that it should discard any partial packets it may have received, and that it should not attempt to transmit any data until the network has cleared. Jam pattern consists of 32-bit string of of alternating 0s and 1s.

Backoff time

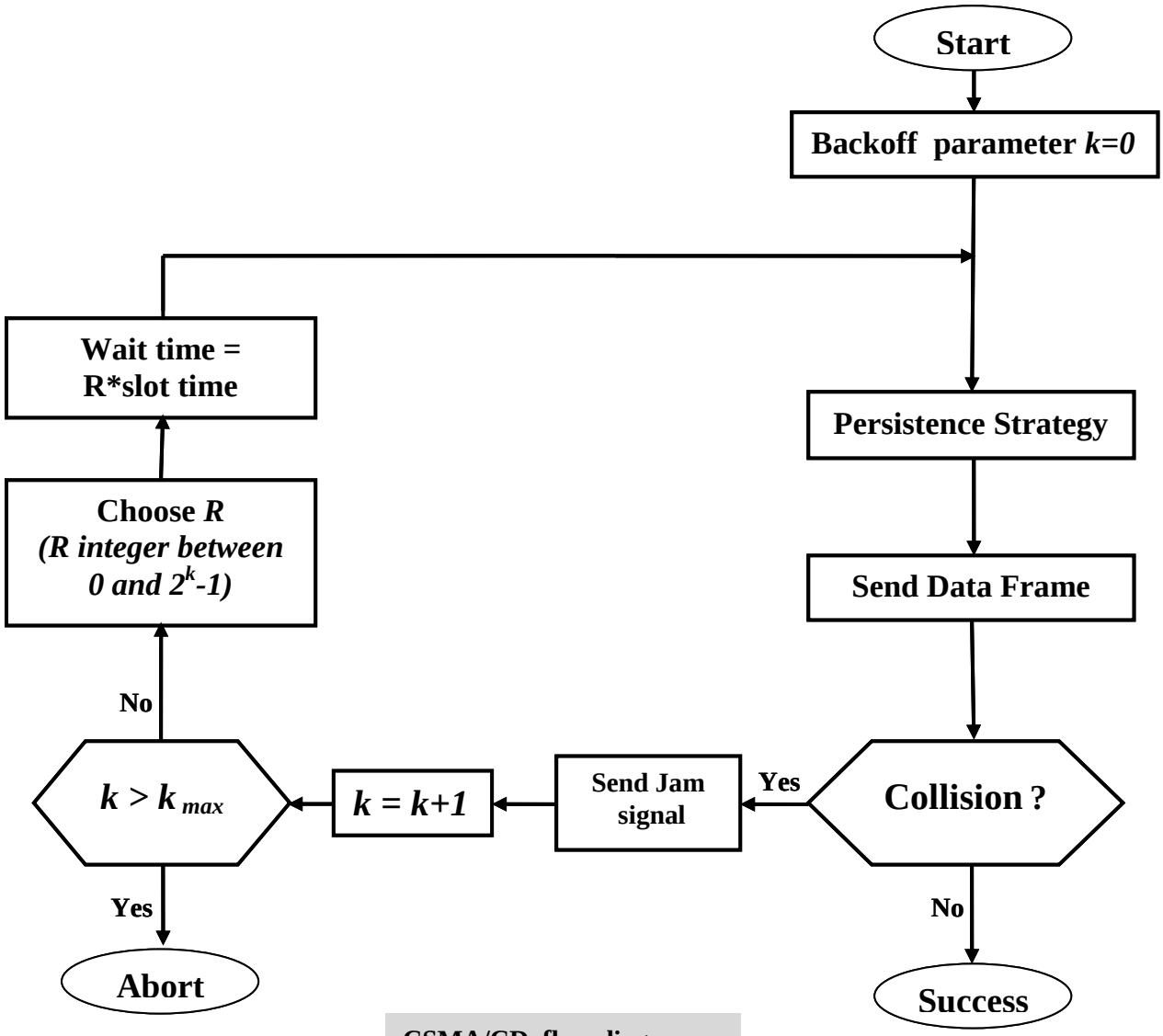
After transmitting the jam pattern, the system waits a specified period of time before attempting to transmit again. This is called the Backoff time, and both of the systems involved in a collision compute the length of their own backoff periods using a randomized algorithm called "Truncated Binary Exponential Backoff". They do this to try to avoid causing another collision by backing off for the same period of time.

Each station wants to transmit set a parameter called backoff parameter "k" to zero. It follows a persistence strategy and if the line is idle the station sends its data. After sending its data the station keeps monitoring the line. In case of collision the station sends a jam signal, increase "k" by one $(k=k+1)$, then calculating backoff period as

Backoff time= R × slot time

Where R : Random number between 0 and 2^k-1

When the station detects another collision it repeats this procedure until k reaches a predefined value "kmax" (usually k_{max} = 15), here the station give up and aborts trying to send its data.



CSMA/CD flow diagram

Example:-

In a Standard Ethernet network, a station detects a collision and succeed to send its data after two tries. Find the possible backoff times for each try.

Sol:

- In Standard Ethernet slot time = 51.2 micro sec
- now the backoff time can be calculated as follows:

Try	*k*	2^k-1	range	Backoff time (micro sec)
1	1	1	0 to 1	0 or 51.2
2	2	3	0 to 3	0, 51.2, 102.4, or 153.6
3	N/A	N/A	N/A	N/A

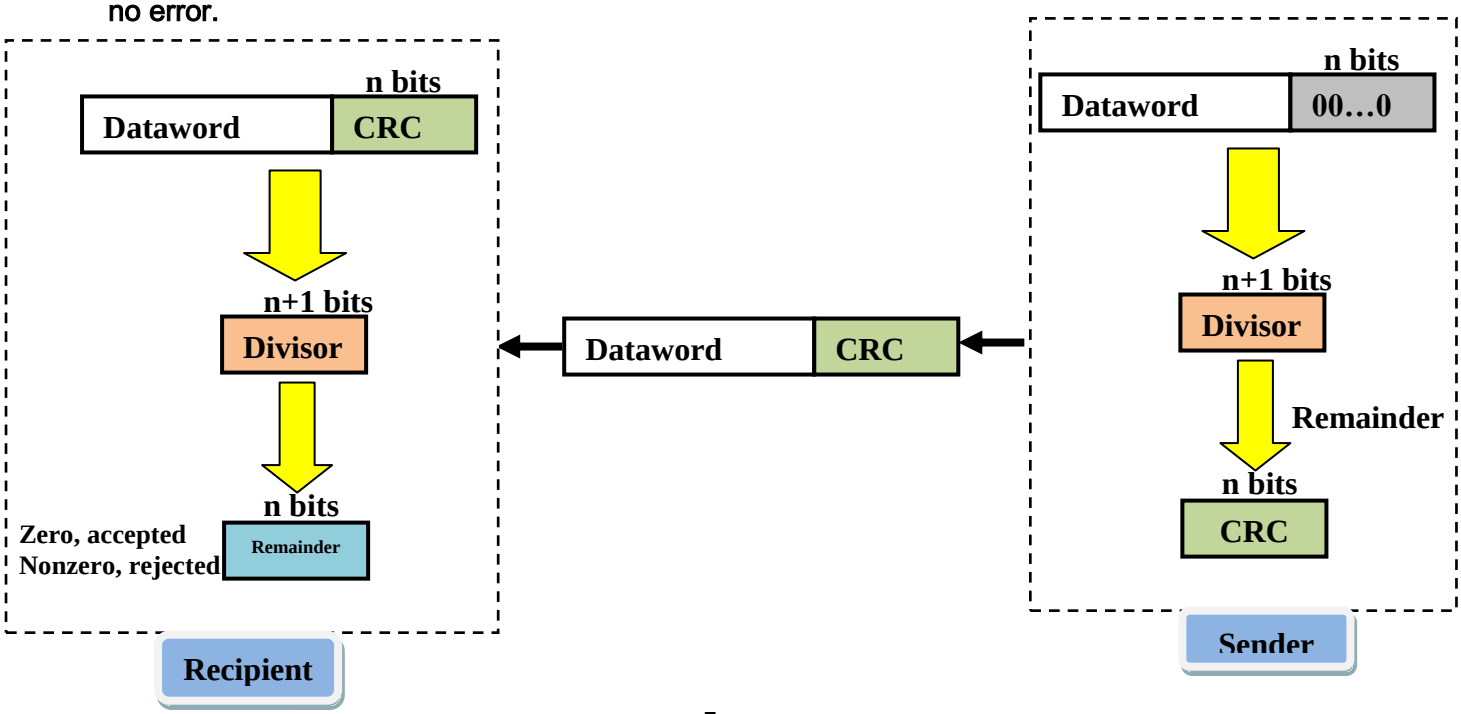
Because of the way CSMA/CD works, the more systems you have on a network or the more data the systems transmit over the network, the more collisions there are.

➢ Cyclic Redundancy Check (CRC):-

It is an error detection method by which a sequence of redundant bits called "CRC" or "CRC remainder" is appended to the end of a data word.

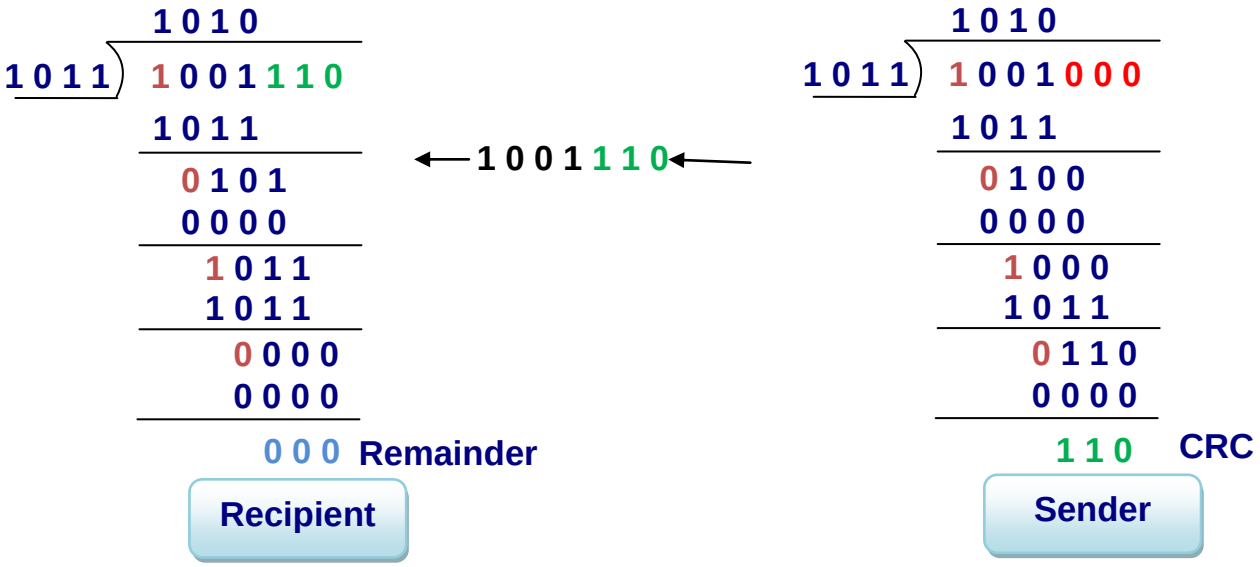
A predetermined divisor called the "generator" is used to achieve the CRC. First the dataword is appended by a specific number of zeros equals the length of the divisor minus one. Then it is divided by the generator. The reminder of the division process is the CRC which is appended to the dataword and sent.

When the data unit followed by CRC arrives the receiver, it treats the whole string as a unit and divides it by the same generator which should yield a zero remainder in case of no error.



Example:

Using the generator (1011), the data word (1001), the sender and the recipient handles CRC calculation and checking as follows.



Notes

1- Addition used in CRC generation and CRC verification is module-2 addition.
2- Division used here is binary division.

Polynomials:

To simplify the process of finding the CRC of binary data word. The data word and the generator can be written as polynomials as follows. As follows

$$b_n x^n + \ldots\ldots\ldots\ldots\ldots + b_2 x^2 + b_1 x^1 + b_0 x^0$$

where b_n can be 0 or 1

it should be noticed that the degree of polynomial to represent n-bit binary word is *(n-1)*.

Example:

Using the generator (1011), the data word (1001). Find how the sender and the recipient handles CRC calculation in a polynomial form.

Sol :

The data word must be appended with three zeros, so it comes(1001000) and it is written in polynomial form (x^6+x^3). The generator is written in the form (x^3+x+1).

$$x^3+x+1 \;\overline{)\; x^6 + x^3 + x^2 + x \;}\; x^3 + x$$

$$x^6 + x^4 + x^3$$

$$x^4 + x^2 + x$$

$$x^4 + x^2 + x$$

$$0$$

$x^6 + x^3 + x^2 + x$ ←

$$x^3+x+1 \;\overline{)\; x^6 + x^3 \;}\; x^3 + x$$

$$x^6 + x^4 + x^3$$

$$x^4$$

$$x^4 + x^2 + x$$

$$x^2 + x$$ **CRC**

zero
Remainder

Recipient **Sender**

Notes:-

In CRC generation using polynomial form,

1- module-2 addition is used here the terms of similar powers are added. In module-2 addition is similar to subtraction.
2- division is used by dividing the term of the greatest power in the dividend by the term of the greatest power in the divisor.

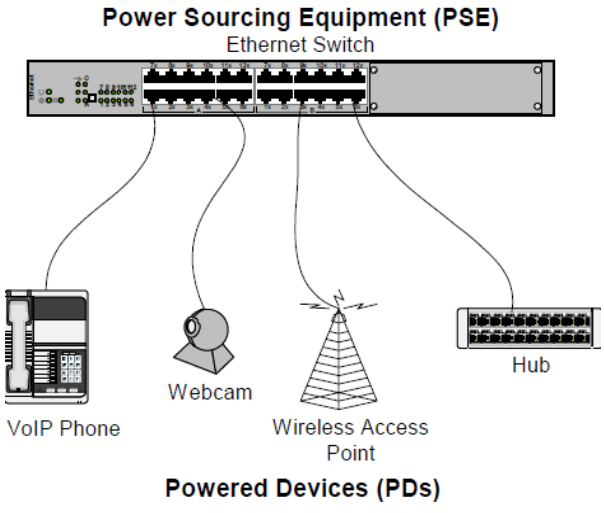
Note

Ethernet uses CRC-32 , the generator polynomial is

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$$

➢ Power over Ethernet (PoE):-

Power Over Ethernet technology allows Ethernet appliances that require power, called Powered Devices (PDs),such as IP telephones, wireless LAN Access Points, and network cameras to receive power as well as data over existing LAN cabling, without needing to modify the existing Ethernet infrastructure. A device that can source power such as an Ethernet switch is termed Power Sourcing Equipment (PSE. As an extension to the existing Ethernet standards, IEEE802.3af standard defines PoE.



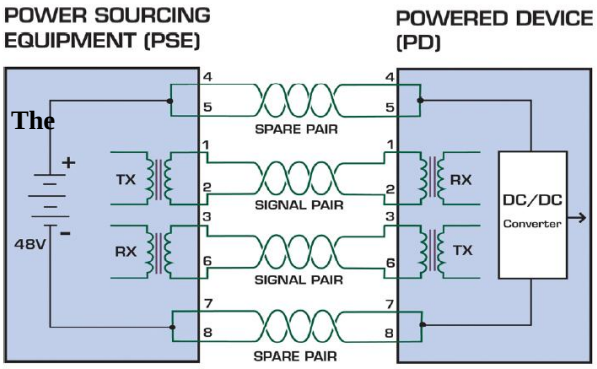
❖ Why to use PoE:

- It Simplifies installation and saves space - only one set of wires to bring to your appliance.
- PoE Saves time and money
- Minimal disruption to the workplace
- Safer - no AC voltages need to be added for additional network devices.
- Appliances can be shut down or reset remotely

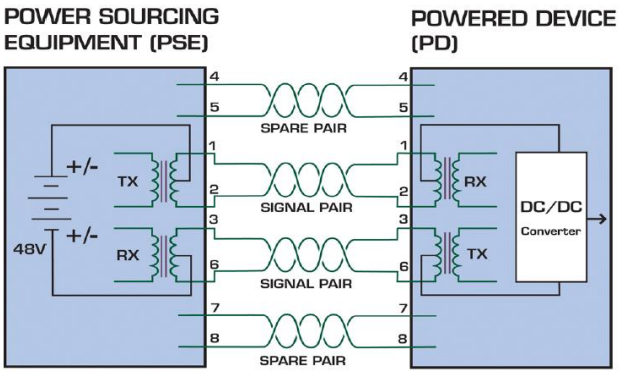
❖ Power Through the Cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these pairs are used for 10Base-T and 100Base-TX data. The specification allows two options for using these cables for power:

- Using spare pairs: The pair on pins 4 and 5 are connected together and form the positive supply, and the pair on pins 7 and 8 are connected and form the negative supply.
- Using data pairs: Since Ethernet pairs are transformer coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without upsetting the data transfer. In this mode of operation the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.



Power Through the Cable on the Spare Pairs



- Power Through the Cable on the Data Pairs

IEEE802.3af standard does not allow both pairs (spare and data) to be used. A choice must be made by the Power Sourcing Equipment (PSE) which applies power to either set of wires. Powered Device (PD) must be able to accept power from both options.

❖ PD discovery:

An obvious requirement of the specification is to prevent damage to existing Ethernet equipment. A discovery process, run from the PSE, examines the Ethernet cables, looking for devices that comply with the specification. It does this by applying a small current-limited voltage to the cable and checks for the presence of a 25k ohm resistor in the remote device. Only if the resistor is present, will the full wattage be applied.

❖ PD classification:

Once a PD is discovered, a PSE may optionally perform PD classification by applying a DC voltage and current to the port. If the PD supports optional power classification it will apply a load to the line to indicate to the PSE the classification the device requires. The power classes as outlined by IEEE 802.3af are as follows:

Class	*Power usage*
0	0.44 W to 12.95 W
1	0.44 W to 3.84 W
2	3.84 W to 6.49 W
3	6.49 W to 12.95 W
4	Reserved

❖ PD management:

Once the PSE has detected the PD's IEEE 802.3af power class, the PSE can manage the power allocation by subtracting the PD's class maximum value from the overall power budget. This allows for control and management of power allocation when there is not enough power available from the PSE to supply maximum power to all ports. On the other hand Any unclassified PD is considered to be a class 0 device.

The IEEE 802.3af standard supports delivery of up to 15.4 watts per port that may be used to deliver power to PoE devices. This allows quite a variety of possible devices to make use of the available power. The maximum power consumed by a PD, as specified by the standard, is 12.95 watts. The system provides the 'extra' power (up to 15.4 watts) to compensate for line loss. Some common PoE device power requirements are:

PD	*Power requirement*
IP phone	3-6 watts
Wireless AP	4-11 watts
IP camera	5-12 watts