# Ethernet Terminology and Errors

## 1. Terminology

### 1.1 Signal Quality Error (SQE)

The SQE test or 'heartbeat' is a test signal generated on the cable after every transmission to assess the ability of the transceiver to detect collisions. The test is a very short frame that is too short to look like a collision. Ethernet 1.0 did not have this in its standard and 802.3 says that repeaters must not connect to a transceiver that generates the SQE test because of the **Jam signal** that is designed to prevent redundant collisions from occurring. The option is normally available to turn off SQE test for this reason.

### 1.2 InterPacket Gap (IPG)

The IPG is the fixed time gap between Ethernet Frames. For 802.3 (10Mbps Ethernet) This is set at 9.6 micro seconds. Sometimes this is called the Inter-Frame Gap (IFG).

### 1.3 Promiscuous Mode

This mode is used by special network adaptors used in devices such as network analysers and transparent bridges. What happens is that the network controller passes ALL frames up to the upper layers regardless of destination address. Normally the frames are only passed up if they have that particular device's address, the destination address is checked and if it does not match that of the adapter then the rest of the frame is ignored. Network Analysers are interested in seeing all frames, regardless of the destination address so special adapters can be installed that run in Promiscuous mode and allow all frames to be sent to the buffer for capture and analysis.

### 1.4 Full-Duplex

Ethernet can exist between switch ports only and uses one pair of wires for transmit and one pair for receive. NICs for 10BaseT, 10BaseFL, 100BaseFX and 100BaseT have circuitry within them that allows full-duplex operation and bypasses the normal loopback and CSMA/CD circuitry. Collision detection is not required as the signals are only ever going one way on a pair of wires. In addition, **Congestion Control** is turned on which 'jams' further data frames on the receive buffer filling up.

### 1.5 Half-Duplex

Half-Duplex allows data to travel in only one direction at a time. Both stations use CSMA/CD to contend the right to send data. In a Twisted Pair environment when a station is transmitting, its transmit pair is active and when the station is not transmitting it's receive pair is active listening for collisions.

### 1.6 Propagation Delay

Propagation Delay, or Latency, is the time taken for a frame to traverse the media from the sending station to the receiving station. A 64 byte frame takes 51.2 microseconds to travel between stations, a 512 byte frame takes 410 microseconds and a 1518 byte frame takes 1214 microseconds, provided that there are no other devices between the stations. This marries with the fact that 10,000 bits traverse the network in 1 second. A bridge would typically add 300 microseconds to the latency to the network.

The **Path Delay Value** is the time it takes an Ethernet frame to travel the furthest distance across the network. It is made up of the sum of the Link Segment Delay Values (LSDV) plus the repeater and DTE delays and maybe some safety margin.

## 2. Error Conditions

## 2.1 Runt

A Runt is a frame that is shorter than 64 bytes (512 bits), which is the smallest allowable frame, and may have a corrupted FCS. It can be caused by a collision, dodgy software or a faulty port/NIC.

## 2.2 Long

This is a frame that is between 1518 and 6000 bytes long. Normally it is due to faulty hardware or software on the sending station.

## 2.3 Giant

This is a frame that is more than 6000 bytes long. Normally it is due to faulty hardware or software on the sending station.

## 2.4 Dribble

A frame that is defined as a 'dribble' is one that is greater than 1518 bytes but can still be processed. This could point to a problem where the IPG is too small or non-existent such that two frames join together.

## 2.5 Jabber

This is when a device is having problems electrically. Ethernet relies on electrical signalling to determine whether or not to send data, so a faulty card could stop all traffic on a network as it sends false signals causing other devices to think that the network is busy. This shows itself as a long frame (longer than 1518 bytes) with an incorrect FCS or is an alignment error. A NIC that is jabbering will send out a frame and then follow it with **A's** and **5's**, i.e. **101010101010...** or **0101010101...**, which are preamble bits indicating a falsely busy network.

### 2.6 Frame Check Sequence (FCS) Error, or CRC error

This defines a frame which may or may not have the right number of bits but they have been corrupted between the sender and receiver, perhaps due to interference on the cable. The IEEE 802.3 says that there should be no more than $10^{-8}$ errors, i.e. 1 in 82 x $10^{6}$.

### 2.7 Alignment Error

Frames are made up of a whole number of octets. If a frame arrives with part of an octet missing, and it has a Frame Check Sequence (FCS) error, then it is deemed to be an Alignment Error. This points to a hardware problem, perhaps EMF on the cable run between sender and receiver.

### 2.8 Broadcast Storm

An incorrect packet broadcast onto a network that causes multiple stations to respond all at once, typically with equally incorrect packets which causes the storm to grow exponentially in severity. When this happens there are too many broadcast frames for any data to be able to be processed. Broadcast frames have to be processed first by a NIC above any other frames. The NIC filters out unicast packets not destined for the host but multicasts and broadcasts are sent to the processor. If the broadcasts number 126 per second or above then this is deemed to be a broadcast storm. An acceptable level of broadcasts is often deemed to be less than 20% of received packets although many networks survive well enough on higher levels than this. The performance lower-specified workstations may be impacted by as little as 100 broadcasts/second. Some broadcast/multicast applications such as video conferencing and stock market data feeds can issue more than 1000 broadcasts/sec.

### 2.9 Collisions

Collisions are a normal occurrence on an Ethernet network. The more devices there are within a segment (Collision Domain) the more collisions are likely. A badly cabled infrastructure can cause unnecessary collisions due to a device being unable to sense a carrier and transmitting anyway.

If a collision rate is high then it may be worth while considering segmenting the network by way of a bridge or router. This reduces the chance of a collision occurring on each of the segment thereby releasing more bandwidth for real traffic.

A good guide to use is collisions should not total more than 1% of the frames transmitted. The following table gives a guide as to recommendations of collision levels with respect to bandwidth utilisation of a segment:

| %age Utilisation | Maximum %age Collisions |
|---|---|
| less than 20 | 1 |
| 20-49 | 5 |
| over 50 | 15 |

A **Late Collision** occurs when two devices transmit at the same time without detecting a collision. This could be because the cabling is badly installed (e.g. too long) or there are too many repeaters. If the time to send the signal from one end of the network to the other is longer than it takes to put the whole frame on to the network then neither device will see that the other device is transmitting until it is too late. The transmitting station distinguishes between a normal and a late collision by virtue that a late collision is detected after the time it takes to transmit 64 bytes. This means that a late collision can only be detected with frames of greater size than 64 bytes, they still occur for smaller frames but remain undetected and still take up bandwidth. Frames lost through late collisions are not retransmitted.

**Excessive Collisions** describe the situation where a station has tried 16 times to transmit without success and discards the frame. This means that there is excessive traffic on the network and this must be reduced.

For normal Ethernet traffic levels, a good guideline is if the number of deferred transmissions and retransmissions together make up for less than 5% of network traffic, then that is considered healthy.

A transmitting station should see no more than two collisions before transmitting a frame.

## 2.10 Jam

On detection of a collision, the NIC sends out a Jam signal to let the other stations know that a collision has occurred. A repeater, on seeing a collision on a particular port, will send a jam on all other ports causing collisions and making all the stations wait before transmitting. A station must see the jam signal before it finishes transmitting the frame, otherwise it will assume that another station is the cause of the collision.

Jamming is a term used to describe the collisions reinforcement signal output by the hub/repeater to all ports. The Jam signal consists of 96 bits of alternating 1s and 0s. The purpose is to extend a collision sufficently so that all devices cease transmitting.

Jamming is used when dealing with congestion. It is an to attempt to eliminate frame loss within the switch by applying "back pressure" to those end stations or segments that are consuming the switch buffer capacity. One way of accomplishing this is for the switch to issue an Ethernet "jam" signal when buffers fill beyond a design threshold level. Jam signals normally are the result of collision detection. When the sending end systems on the segment receive the jamming signal, they will back off for a random time period before attempting a retransmission.

Each transmitting node monitors its own transmission, and if it observes a collision (i.e. excess current above what it is generating, i.e. > 24 mA) it stops transmission immediately and instead transmits a 32-bit jam sequence. The purpose of this sequence is to ensure that any other node which may currently be receiving this frame will receive the jam signal in place of the correct 32-bit MAC CRC, this causes the other receivers to discard the frame due to a CRC error.

Go next to ***Ethernet Bridging***.