Ethernet Error Descriptions

The following sections describe the main error types that can be captured through a protocol analysis session.

Local Collisions
A local collision is an Ethernet packet that usually is less than 64 bytes in length and may contain a garbled Cyclic Redundancy Check (CRC) field. A local collision will be on the local segment. Collisions on a network are considered normal, especially in the CSMA/CD access method. Stations are supposed to collide, and when transmissions collide, they are supposed to listen and wait to retransmit. But certain levels are considered problems. When collisions are more than one percent of overall traffic, it is considered an issue.

Normally, if no problems exist on a network, a minor collision rate from one station does not indicate a major problem in general network communications. If, however, the collision rate is more then one percent of all traffic on an Ethernet, the NIC addre ss captured should be recorded, and the adapter should be troubleshot.

Although a high collision rate from one particular station can be a minor component of overall traffic levels, it should be addressed immediately. From a troubleshooting standpoint, if a high collision rate is transmitted from one station that is more than the one percent traffic level of the overall bandwidth utilized, that station card should be replaced or the connector should be checked within that particular station. Check the connections on the cabling connectors first, then actually replace the NIC board. The network should be re-analyzed to determine whether the error is still present on the network.

Excessive collisions from stations on a network can consume bandwidth and cause a transmission problem across a complete network. In such cases, it is important that the collision problem be troubleshot and the cause corrected. High collision rates from multiple stations on the Ethernet network may indicate cabling, transceiver or repeater problems; the complete network segment should be analyzed and troubleshot.

If one area of a network has multiple adapters transmitting CRC or collision errors in composite, that particular area of the network usually has a common factor such as a repeater

or wiring hub module. This is where the trial-and-error method takes place, but a protocol analyzer is invaluable because it picks up the addresses with the collision rates. At that point, if those addresses are itemized and found to be in the same area of the network, any common device should be located and replaced.

Remote Collisions

A remote collision is a collision packet usually less than 64 bytes in size with a corrupted CRC field value. These are packets that have filtered over from another segment. This may indicate that a specific node's NIC or transceiver on another side of a repeater has a problem.

A bridge or router isolates all collisions to their res pective local segment. Most protocol analyzers can detect when a collision is not local if the address fields are valid and not local. Sometimes false readings can occur in this area.

If a valid high remote collision is detected with an analyzer, you are going to have a tough troubleshooting session. If the cause of a node and segment problem is to be located specifically, it will require systematic troubleshooting by checking all the Ethernet segments attached to a repeater for their individual health at the physical layer. When a local collision is found on a particular segment, the next step is to locate the bad node and follow the replace-and-reanalyze approach.

Late Collisions

A late collision is a collision packet usually larger than 64 bytes with a corrupted CRC field value. This is a packet that will be on the local segment. If a collision occurs with less than the normal 64 bytes of transmission of a particular station generation, this means that there is a normal collision occurrence upon transmission.

If, however, the collision occurs with greater than 64 bytes of data on an Ethernet station transmission, this is considered "late" because it did not occur before the 64-byte transmission ratio. Late collisions can cause a high number of bytes to be transmitted in a train fashion because more bytes are on the network than with a normal collision under 64 bytes. More often this indicates that the station's NIC transmitting the collision cannot hear properly to stop its transmission and will continue to broadcast high collision rates on the network. This also may be captured as a form of excessive jamming. This usually is a problem with a network interface card, and the card should be replaced and the network re-analyzed.

CRC/Alignment Errors

On any Ethernet network, a CRC error can be captured in an analysis session. A CRC error is picked up by a protocol analyzer when the Ethernet packet has a byte-posi tioning problem.

The Ethernet packet is responsible for checking its transfer from station to station through general network communications with a CRC field. The CRC field is a math algorithm field used for calculating an Ethernet's packet contents for proper communication from station to station.

Normally, a sending station sends out a packet that has a CRC pattern in it that is supposedly standard. The receiving or destination station within an Ethernet network recalculates the frame contents to correlate whether it matches the proper CRC value. If a problem occurs in the error calculation and a difference arises, the packet possibly is corrupted and a CRC error may be generated by the station onto the network. If a CRC error generation is picked up, the analyzer usually records that CRC error and indicates that the sending station or the destination station has a corruption in packet transmission.

At times, CRC and alignment errors may be recorded as the same type of error. This is because they both really indicate a byte-alignment problem in transmissions. If CRC errors are recorded in a protocol analysis session above the two to three percent level of overall traffic on a network, they are considered excessive. It is possible that the group of stations involved in a transfer, on occurrence of a specific node sending of CRC transmissions, has a problem. All the addresses of transmitting nodes captured in a trace with frames in front and after the CRC error frame should be noted for the record. The problem may be in the group of stations. It is possible that a node NIC, transceiver, respective cabling or even a connected repeater or wiring hub port has failed. But relax, usually the station sending the CRC error will have a bad NIC or transceiver.

If CRC errors are high on a particular Ethernet segment, cable connections may have problems or improper grounding may exist throughout the network. The cabling and connections should be checked first. If th e problem is still present, the NIC should be replaced. The BNC T-connector, the tap connector and transceivers also can be one of the primary causes for this type of problem. But the most probable cause is the NIC sending the CRC. After checking the cabling infrastructure, replace the NIC. Next, the network should be re-analyzed to check for any errors related to the new NIC address. If problems are still present, multiport repeaters and wiring hubs also should be checked as a cause for the CRC errors.

It is possible to attribute this problem to one particular network station's NIC. The surest way to isolate this is through a protocol analysis session. Look very closely for a high number of CRC errors, because a high frequency indicates a definite problem for the sending station.

Long and Short Packets

As mentioned earlier, the Ethernet frame types have certain rules. Depending on the packet

type, frames can be from 64 bytes to 1,518 bytes in length. With the proper protocol analyzer, you can pick up two types of packets called short frames (runts) and long packets. A short or runt packet is any packet smaller than 64 bytes. Long packets are those larger than 1,518 bytes. These are considered problems on a network and an analyst should use a protocol analyzer to capture multiple transmissions of the occurrence. It is possible for a NIC, transceiver or even a corrupted LAN driver to generate long and short frames. The cause is usually isolated to the failing network interface card. Captured long or short packets may not include reliable address fields.

The analyst should identify the addresses attempting to communicate in the trace that are right before and after the long or short packets. Next, one by one remove the suspect nodes and re-analyze the network until the problem subsides. After the node area is located, the NIC, transceiver and NIC driver should be troubleshot.

Jabber

At times, Ethernet network interface card s and external transceivers also generate a problem called jabbering. This is when garbled bits of data are emitted within the frame sequence in a continuous transmission fashion. The packet length is usually more than 1,518 bytes. This can be identified by a protocol analyzer as a CRC error. As mentioned earlier, when nodes detect collisions they emit a normal JAM signal on the network segment to clear transmission. Sometimes certain nodes attempt to keep jamming the network due to excessive high collision rates; this also can be captured as high CRC or late collision error rate. The cause can be overloaded traffic levels. If the bandwidth- utilization levels are normal or low for the particular Ethernet segment, it is possible that the collision detection pair of a jamming node's NIC or transceiver cannot hear the network signal and may not know a collision has stopped. If this occurs, it continues to jam the network.

If a certain node on an Ethernet segment emits a lot of jabber, the node's NIC and transceiver should be troubleshot through consecutive replacement and re-analysis.

If an Ethernet network has intermittent high network bandwidth usage that causes performance problems, the cause can be re-created by loading the network with traffic-generation features in a protocol analyzer. But you must be careful when using this technique. First, be aware of the current network usage and any possible impacts to the network-user community. Second, you really have to understand all the Ethernet network bandwidth considerations discussed earlier, including the actual maximum bandwidth available, the overall network bandwidth baseline view and individual Ethernet node bandwidth consumption. Make sure that a proper baseline is performed on the lower and upper layers of the Ethernet.

November 15, 1996

 Print This Page

 E-mail this URL