INTEGRATION NOTE

October, 1997

Prepared By
Novell Integration
Business Unit, Compaq
Computer Corporation

CONTENTS

LAN Driver Statistics for Novell Drivers

This integration note describes the statistics to diagnose network problems via the Novell MONITOR modules. The statistics supplement the diagnostic information that would normally be obtained with a protocol analyzer or network monitor and gives an estimate of network and controller activity.

ECG043/1097

NOTICE

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements. Compaq does not warrant products other than its own strictly as stated in Compaq product warranties.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Compaq, Compaq Insight Manager, ProLiant, SmartStart, NetFlex, registered United States Patent and Trademark Office.

Netelligent is a trademark and/or service mark of Compaq Computer Corporation.

intraNetWare, NetWare 3, NetWare 4, NetWare Loadable Module, NetWare Storage Management Services, NetWare SMS, Novell, Novell Directory Services, and NDS and are trademarks of Novell, Inc.

Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

LAN Driver Statistics for Novell Drivers

First Edition (October, 1997)
043A/1097

EXECUTIVE SUMMARY

The Compaq network interface controller (NIC) drivers provide a number of statistics to aid in the diagnosis of network problems. These statistics can be viewed with MONITOR.NLM. Each statistic is listed in this document includes a description of its purpose as well as provides suggestions to counter problems and reduce the number errors reported.

INTRODUCTION

The Compaq network interface controller (NIC) drivers provide a number of statistics to aid in the diagnosis of network problems. These statistics can be viewed with MONITOR.NLM. Information such as Packets Received and Packets Sent are common to every protocol and are reported for every controller. Others like Collisions or Beacons are particular to one protocol or another (Ethernet and Token Ring, respectively). The statistics supplement the diagnostic information that would normally be obtained with a protocol analyzer or network monitor and give an estimate of network and controller activity. Most of these statistics will increase during normal operation. Occasional errors do not necessarily indicate a problem.

NETFLEX AND DUALSPEED CONTROLLER STATISTICS

Send OK Single Collision Count

The number of single collision packets: This counter contains the number of packets that are involved in a single collision and are subsequently transmitted successfully.

These errors show that the network has light to moderate traffic. If single collisions become more frequent, the count for multiple collisions escalates.

Send OK Multiple Collision Count

The number of multiple collision packets: This counter contains the number of packets that are involved in multiple collisions and are subsequently transmitted successfully.

These errors mean that the network is experiencing moderate to heavy traffic. If multiple collisions become more frequent, the count for excessive collisions escalates.

Send OK But Deferred

The number of packets deferred before transmission: This counter contains the number of packets whose transmission was delayed on its first attempt because the medium was busy. Packets involved in any collisions are not counted. Frames that wait before transmission are counted. This statistic will be incremented often during normal operation on a busy network.

Deferred transmissions occur when the network is extremely busy; so busy that the NIC did not try to transmit. High counts of multiple collisions and excessive collisions also occur.

Deferred transmissions indicate that this segment of the LAN is overcrowded. Reduce the traffic by reorganizing the LAN. For example, if you have 100 stations on one Ethernet bus, break it into two Ethernet segments by adding a NIC to your server. In this way you can balance the load by putting 50 stations on one segment and 50 on the other. If a few isolated stations create the traffic, put them on a separate segment.

Send Abort from Late Collision

Late collisions may be a symptom of cabling problems. A late collision is one that occurred 64 bytes or more into the packet.

Late collisions may be an indication that a segment is longer than allowed by the wiring specifications. For example, if you are using 10BASE-2 wiring, also known as Thinnet, the maximum segment length is 185 meters.

A station will believe it has control of the cable segment if it has already transmitted 64 bytes. If another node at the far end of the segment has not yet seen the packet, and transmits, this packet will collide with the first transmission after the first 64 bytes have been sent. Ensure that your segment length does not exceed the maximum length allowed.

Because the location of cabling problems can be very difficult to detect on an Ethernet network, you may want to "shorten" an Ethernet segment (remove portions of the network to isolate problems) until the problems are no longer seen, and then expand the network until the problem recurs.

If this counter increments quickly in a short period of time, it may mean that the network card is running in half duplex mode, but your hub port is configured for full duplex mode. Compare your network card’s configuration with the hub port’s configuration.

Send Abort from Excess Collisions

The number of packets aborted during transmission due to excessive collisions: This counter contains the number of packets that, due to excessive collisions, are not transmitted successfully. A station may attempt to transmit up to 16 times before it must abort the attempt. Once the abort occurs, this counter increments.

If you see an increase in deferred transmissions as well as excessive collisions, the network is extremely busy and this segment of the LAN is overcrowded. Reduce the traffic by reorganizing your LAN or adding a NIC to the server. For example, if you have 100 stations on one Ethernet bus, break it into two Ethernet buses by adding a NIC to your server. In this way you can balance the load by putting 50 stations on one bus and 50 on the other. If there are a few isolated stations creating the traffic, try placing them on a separate bus.

Faulty components may be the cause of excessive collisions. Check the following:

- This counter will increment with each transmit frame if you are using coaxial cabling (on the 10B2 connector) and the cable is disconnected.
- Segment too long: Nodes at the far end of the cabling system transmit, unaware that a station at the other end has already gained control of the medium by transmitting the first 64 bytes of a frame.
- Failing cable: Packet data traveling through shorted or damaged cabling may become corrupt before reaching the destination station.
- Segment not grounded properly: Improper grounding of a segment may allow ground-induced noise to corrupt data flow.
- Improper termination: If a cable segment is not properly terminated, allowing the signal to be absorbed upon reaching the end of the segment, a partial signal will bounce back and collide with existing signals.
- Taps too close: Follow the minimum recommended spacing between cable taps to ensure minimal reflection build-up and data distortion.
- Noisy cable: Interference or noise produced by motors or other devices can distort the signals and cause CRC/Alignment errors.
- Deaf/partially deaf node: A faulty station that cannot hear the activity is considered a deaf node. If you suspect a deaf node, replace the NIC or transceiver.
- Failing repeater, transceiver, or controller: Repeaters, transceivers, and controllers can disrupt the network signal, transmit erroneous signals on the wire, or ignore incoming packets. Perform the following steps:
    1. If your NIC is continuously transmitting, it causes erroneous signals, or "jabber." Replace a jabbering transmitter to ensure proper network performance.
    2. Swap out the transceiver, transceiver cable, and transceiver attachment point, one at a time. If you find a faulty component, replace it.
    3. Check your hub. This component may be at fault. Use the diagnostics from the hub manufacturer to help you determine if a problem exists.

Send Abort from Carrier Sense

The number of packets transmitted with carrier sense errors: This counter contains the number of times that the carrier sense signal from the physical layer interface was not asserted or was de-asserted during transmission of a packet without collision.

The carrier sense signal is an ongoing activity of a data station to detect whether or not another station is transmitting. Carrier sense errors are detected when a station transmits a frame and does not detect its own signal on the wire.

If you receive carrier sense errors, check the following:

- Failing cable: Packet data traveling through shorted or damaged cabling may cause a signal loss. Ensure that your cable is working and plugged in properly.
- Segment not grounded properly: Improper grounding of a segment may allow ground-induced noise to interrupt the signal. Ensure that you have properly grounded all segments.
- Noisy cable: Interference or noise produced by motors or other devices can interrupt the signals.
- Deaf/partially deaf node: A faulty station that cannot hear the activity is considered a deaf node. If you suspect a deaf node, the network interface card or transceiver should be replaced.
- Failing repeater, transceiver, or controller: Repeaters, transceivers, and controllers can disrupt the network signal, transmit erroneous signals on the wire, or ignore incoming packets. Perform the following steps:
    1. Swap out the transceiver, transceiver cable, and transceiver attachment point, one at a time. If you find a faulty component, replace it.
    2. If none of the items listed above help you isolate the problem, you may need to replace the Multi-Access Unit (MAU) or hub. Use a network analyzer to isolate the problem area.

Send Abort from Excessive Deferral

The number of packets aborted due to excessive deferrals: This counter contains the number of packets that, due to excessive deferrals, are not transmitted successfully. This counter is incremented when the number of transmission attempts is greater than 16.

Receive Abort from Bad Frame Alignment

The number of packets received with alignment errors:

The alignment of a frame is checked by the receiver after the packet has failed the Cyclical Redundancy Check (CRC). Misaligned packets do not end on an 8-bit boundary. All packets contain a set number of bytes and must end after a defined number of bytes. Packets that do not end on a byte boundary fail the alignment check.

If you are using a 100-Mbit adapter in your server and the Intel PRO/100 adapter in your clients, you may see a large number of these errors. The problem can be alleviated by adding the following line to the LINK DRIVER E100ODI section of your client's NET.CFG files:

```
THRESHOLD 200
```

If your network continues to experience an increasing number of CRC/Alignment errors, check for the problems listed under the bullet: Send Abort from Excess Collisions.

LOW/HIGH Counter Statistics

Total Send/Receive OK Byte Count:

These counts are defined as 8 byte values. The LOW count is the lower 4 bytes of the count. The HIGH is the upper 4 bytes of the count. The HIGH will increment once every time the LOW reaches 4 billion. At that point, the LOW will start back at zero. Thus, in a normal situation, you will see a very active and very high count for the LOW statistic. The HIGH count statistic will be much smaller. An example of these types of counters is the Total Send OK Byte Count High and Total Send OK Byte Count Low.

PCNTNW.LAN CUSTOM STATISTICS

PCNTNW.LAN for the ProSignia Integrated NetFlex-L ENET and the Deskpro XL Integrated NetFlex ENET/PCI has these additional custom statistics.

Heart Beat Error

This error indicates that the collision inputs to the AUI port failed to activate within 20 network bit times after the chip terminated transmission.

Memory Time Out

This counter is incremented when the board does not get bus master resource to read or write to memory in the system.

Tx Babbling Error

Babble is a transmitter time-out error. It indicates that the transmitter has been on the channel longer that the time required to send the maximum length frame. BABL will be set if 1519 bytes or greater are transmitted.

Tx Under Flow Error

This error indicates that a frame transmission was aborted because the board could not get the data from memory in time.

Tx Buffer Error

This error indicates that the frame buffers which were queued for transmission were not set up correctly by the software.

Rx ECB's Over 16 Meg Count

This is a standard statistics counter which counts receive Event Control Blocks located above 16 Megabytes.

Tx ECB's Over 16 Meg Count

This is a standard statistics counter which counts transmit Event Control Blocks located above 16 Megabytes.

Packets Used 2 ECBs

This is a statistic counter indicating that a packet used 2 Event Control Blocks.

CPQNF3.LAN CUSTOM STATISTICS

CPQNF3.LAN has these additional custom statistics.

TLAN Device Revision (X.X)

This statistic will be a two-digit number that represents the version of ThunderLAN that is used on your controller. For instance, if this value is 23, then that means that the TLAN version in use is v2.3.

Adapter Check Count

This counts the number of adapter checks that occur and indicates a possible hardware problem. A console error message that details the problem will be generated. The adapter will be reset and operation should continue. The Adapter Reset statistic will also increment.

At the next scheduled maintenance, bring down the server and run Compaq Diagnostics to determine if the board should be replaced.

Transmit Timeout Errors

This counter is incremented when a frame does not transfer within the expected amount of time. The adapter will be reset and operation should continue. The Adapter Reset statistic will also increment.

If this counter increments rapidly in a short period of time, check to ensure that the cables are properly connected. The Link Status LED should be lit if the driver is loaded and the adapter is connected to a hub. If this statistic still increments, power off the system and check the following:

Check the module on the NetFlex-3 Controller to ensure that it is correctly installed.

Check the seating of the NetFlex-3 Controller into its slot.

If all of these elements appear to be in working order:

1. Swap out the adapter and adapter cable one at a time. If you find a faulty component, replace it.
2. Check your hub. This component may be at fault. Use the diagnostics from the hub manufacturer to help you determine if a problem exists.

Send Abort Link Failures

This indicates how many transmitted packets have failed to transmit due to link failures.

Transmit Packets Copied

Indicates how many packets have been copied by the driver before transmission. This counter enables you to monitor inefficient NLMs running on the server. NLMs that use up to 16 fragments transmitted per packet may cause this counter to be incremented.

A typical file server will never see this counter increment.

Oversized Receive Errors

If a packet is received that is larger than the maximum allowed on Ethernet, this counter will be incremented. A high number of these errors indicates that a node has malfunctioned and is transmitting oversized frames. You can use a network analyzer to determine which node on the network is causing the problem.

Driver Operating Time (minutes)

This indicates the approximate time in minutes that the driver has been operating.

Link Speed (bits per second)

This indicates the speed that the adapter is running. Use this information to ensure that the adapter is operating in the same mode as the device to which it is connected.

Duplex Mode (0=Half, 1=Full)

This indicates the duplex mode in which the adapter is operating. Use this information to ensure that the adapter is operating in the same mode as the device to which it is connected.

Promiscuous Mode (0=Off, 1=On)

This statistic indicates whether Promiscuous Mode is currently turned on or off and can be used to verify the operation of network analyzer products such as Novell's LANalyzer NLM. (When the LANalyzer is capturing network data, Promiscuous Mode will be on).

Network Link Status (0=up, 1=down)

This statistic reports the current status of the link. Zero indicates the link is working (up). One indicates that there is no communication with the hub (down). If this statistic is one, check your cables and connections. If none of these solutions alleviate the problem, try changing the cable or resetting the hub.

VG Transitions Into Training

A training session occurs before a controller is given access to the network. Twenty four packets are sent to the hub and echoed back. When this occurs successfully, data can be transferred on the network from a controller. If a hub or controller detects interference or invalid data control sequences, training will occur.

This counter tracks the number of times the controller enters the training state. If this count goes up rapidly, the controller is disconnecting/reconnecting to the hub numerous times. Excessive transitions into training may mean a bad cable.

1. Swap out the controller and controller cable one at a time. If you find a faulty component, replace it.
2. Check your hub. This component may be at fault. Use the diagnostics from the hub manufacturer to help you determine if a problem exists.
3. Run Compaq Diagnostics. If none of these suggestions clear the problem, contact your service provider. You may need a driver upgrade.

VG Training Failures

This statistic counts the number of times a training session has failed. For example, this statistic will increase if your controller is disconnected from the hub because periodically the controller attempts to connect to the hub. If this statistic increments rapidly, check the following:

1. Make sure your adapter is connected to the hub using proper cabling.

2. Check your hub. This component may be at fault. Use the diagnostics from the hub manufacturer to help you determine if a problem exists.
3. Run Compaq Diagnostics. If none of these suggestions clear the problem, contact your service provider. You may need a driver upgrade.

LAN Driver Token Ring Statistics

This section contains a list of statistics reported for the Compaq Token Ring controllers.

These following errors are called network soft errors:

- Line Errors
- Burst Errors
- Lost Frame Errors
- Frame Copied Errors
- Token Errors

They do not affect the operation of the network but they can affect performance if they become excessive. They should be considered as a group. If any of these counters is incrementing as a large percentage of the frames received or transmitted, it usually indicates a problem with the wiring or the board. During normal operation these numbers will occasionally increment. This does not necessarily indicate a problem. More information about each error can be found below.

Line Errors

This item will increment each time a station detects a line error. Each station either repeats or copies a frame and checks the frame for validation. If the data in the frame is corrupted, each station that detects the corrupted frame will increment its own line error count.

If you see an excessive number of line errors, check for the following:

Failing cable: Packet data traveling through shorted or damaged cabling may become corrupt before reaching the destination station. This will cause line errors.

Segment not grounded properly: Improper grounding of a segment may allow ground-induced noise to corrupt data flow, which will cause line errors.

Noisy cable: Interference or noise produced by motors or other devices can distort the signals and cause CRC/Alignment errors, which will increment the line error count.

If you cannot find the problem after checking the above conditions, use a network analyzer to isolate the station that is corrupting the frame. The analyzer should indicate which station is causing the problem, and let you know if the NIC should be replaced.

Burst Errors

This item increments every time the adapter detects the absence of clock transitions. Burst errors occur in Token Ring networks when the signal is momentarily disrupted. Each time a station asserts itself into the ring or de-asserts itself from the ring, a burst error may occur.

If you detect that one station has an abnormally high burst error count compared to other stations, you may need to replace the NIC. For example, if most stations average 2 burst errors per day, and one station shows 27, that station may have a faulty NIC. The station that is directly downstream of the device causing the problem usually detects the burst error. Use the Upstream Address of the station detecting Burst Errors to determine the faulty NIC.

If excessive burst errors continue to occur on the ring, you may need to replace the Multi-Access Unit (MAU) or hub. Use a network analyzer to isolate the problem area.

Frame Copied Errors

See AC error for more information.

AC errors

AC errors are also referred to as Address Recognized Indication/Frame Copied Indicator (ARI/FCI) errors and occurs when a station detects that an upstream station did not correctly set the bits on a frame.

If an AC error occurs, perform the following steps during your next planned maintenance:

1. Ensure that the NIC is compliant with the protocol in use. The NIC that did not set the bit (the station directly upstream of the station that reported the problem) is not participating in the low level protocol and may not be completely compliant with 802.5 protocol.
2. Replace the NIC to see if the problem still occurs.

Token Errors

Token Errors are reported by the active monitor due to one of the following reasons:

1. The active monitor detects that a frame has gone around the ring more than once, either because the sender de-asserted from the ring before stripping the frame, or because there are two active monitors present on the network. The active monitor will purge the network and clear the condition in either case.
2. A station reserved a token at a high priority and then de-asserted itself from the network. The active monitor will detect the token traversing the ring more than once as it searches for the station that requested the high priority. The active monitor will purge the ring.
3. The active monitor detects that no token or frame is received for 10 milliseconds. This usually occurs when a station asserts or de-asserts from the ring. If this counter escalates rapidly, it is usually caused by several stations asserting themselves onto the ring, or de-asserting themselves at the same time. For example, this condition could occur when the power is off temporarily and then returned. In this example, several stations would try to assert themselves onto the ring all at the same time, disrupting the signal. If this condition appears to occur for no known reason, however, you may need to check your Multi-Access Unit (MAU). Use a network analyzer to isolate the problem area.
4. The active monitor detected a token that was returned to it containing a token violation. You will also see line errors along the ring. The active monitor will purge the ring, but you should also check for the following:

Failing cable: Packet data traveling through shorted or damaged cabling may become corrupt before reaching the destination station and cause line errors and token errors.

Segment not grounded properly: Improper grounding of a segment may allow ground-induced noise to corrupt data flow and cause line errors and token errors.

Noisy cable: Interference or noise produced by motors or other devices can distort the signals and cause CRC/Alignment errors, which will increment the line error count and may cause token errors.

If you cannot find the problem after checking the above conditions, use a network analyzer to isolate the station corrupting the frame. The analyzer should indicate which station is causing the problem, and let you know if the NIC should be replaced.

Abort Delimiter

This item increments when a station transmits an abort delimiter while transmitting.

An aborted transmit occurs if the NIC is unable to complete the transmission of a frame that it has already started onto the network. For example, if the NIC was unable to access its packet buffer memory fast enough to keep pace with sending the data stream onto the wire, the NIC will abort the transmit. When a NIC aborts the transmit, it places a special bit sequence on the wire known as an abort delimiter, which signals to other stations on the Token Ring that the packet data is invalid.

Many NICs do not support aborting transmits, preferring instead to shut down with a fatal error and remove the NIC from the ring. Those NICs that support aborting transmits will report this error. If this error is reported, run the diagnostics from the NIC manufacturer.

Lost Frame Errors

This error indicates that a sending station was unable to complete the transmission because the frame that was sent never returned to the originator. When a station sends a frame, that frame normally returns after completing the circuit. If the frame does not return intact, this error will increment.

These errors may occur if another station asserts itself on a ring or de-asserts itself from the ring, interrupting the clock cycle. Large noise spikes, such as lightning, could also cause these errors.

If you see excessive Lost Frame errors, there may be a problem with the Multi-Access Unit (MAU) or hub. Use a network analyzer to isolate the problem area.

If other errors are occurring, they may help you pinpoint the most likely source of the problem:

Line Errors and Lost Frame Errors: Check for bad cabling. Packet data traveling through shorted or damaged cabling may become corrupt before reaching the destination station, or may not return to the originator intact. Ensure that no large motors are causing noise on the cables.

Burst Errors and Lost Frame Errors: Check to see if nodes are asserting onto or de-asserting off the ring. Excessive network traffic getting on and off the ring will cause a high number of lost frame errors. Run the diagnostics from the MAU connector manufacturer to see if there is a problem with the MAU.

Lost Frame Errors only: Run the diagnostics from the MAU connector manufacturer to determine if a problem exists with the MAU. If the MAU is working correctly, large noise spikes may be the cause of the problem.

Last Ring Status

This item indicates the current interface status when the NIC is active on the ring. This field can be one of, or a sum of, the following values:

00000000h: OK. No problems have been detected.

00000020h: Ring Recovery. The active monitor changes from one station to another when the current active monitor de-asserts itself from the network, or has detected a problem with itself. Check other error counts to see if a problem exists.

00000040h: Single Station. This NIC has detected that it is the only NIC on the ring. This condition might be caused by the network administrator choosing to isolate the NIC, or from a Multi-Access Unit (MAU) or hub failure. Check your MAU or hub. Use the diagnostics from the MAU manufacturer to help you determine if a problem exists.

00000100h: Remove Received. While this NIC was trying to get on the network, the manager station issued a "Remove station from the ring" command. See your network administrator to determine why the station was removed from the ring.

00000400h: Auto Removal Error. When beaconing occurs, the stations immediately upstream and downstream of the network fault de-assert themselves from the ring and begin a self test. If an error occurs with the self test, the NIC is flagged with this error and is not allowed back on the ring. Replace the NIC.

00000800h: Lobe Failed. The lobe self-test failed. One of the wires that runs from the Multi-Access Unit (MAU) to this station may have a problem. This NIC may also have a problem.

Check the following:

Failing cable: Ensure that your lobe wire is intact.

Failing repeater, transceiver or controller card: Repeaters, transceivers, and controller cards can disrupt the network signal or transmit erroneous signals on the wire.

If your NIC is continuously transmitting, it will cause erroneous signals, or "jabber." Replace a jabbering transmitter to ensure proper network performance.

Swap out the transceiver, transceiver cable, and transceiver attachment point, one at a time. If you find a faulty component, replace it.

Check your Multi-Access Unit (MAU) or hub. This component may be at fault. Use the diagnostics from the MAU manufacturer to help you determine if a problem exists.

00001000h: Transmit Beacon. This error occurs when there is a break on the Token Ring or you have a defective NIC on the ring. If you see even one transmit beacon, investigate the problem immediately. The break is detected by the station immediately downstream of the break when that station stops receiving tokens or frames. This station then sends a series of beacon frames around the ring to notify the ring that a break has occurred immediately upstream.

00004000h: Hard Errors. This error will usually occur in conjunction with transmitted beacons. It increments each time a station receives or sends a beacon, thus occurring numerous times when a beacon is being transmitted.

00002000h: Soft Errors. This item increments when the NIC detects recoverable errors. The NIC will correct the error, but the error will be reported to the LAN management station and counted. Check other error counts to determine if a serious error has occurred.

00008000h: Signal Loss. This error will usually happen in conjunction with other errors, such as burst errors, token errors, line errors, and transmitted beacons. Check other error conditions to determine if a serious error has occurred. Otherwise, there may be a problem with this NIC.

00020000h: No status.

Frequency Errors

These errors occur when a station detects that the active monitor is not working in the proper frequency. Ring recovery will occur and another active monitor will be chosen.

The active monitor generates a clock signal, which it passes to each standby monitor. The standby monitor compares this signal to its own reference clock. If the signal is not within the proper frequency boundaries, a frequency error occurs.

NOTE: Not all stations will report this error, because not all NIC manufacturers support this feature. This error is not common and if there is a problem with the active monitor, other errors usually occur that will help you determine the station that is at fault.

If you see frequency errors, use a network analyzer to determine which station was the active monitor causing the problem. Remember when you use your analyzer that the station with the problem is not the current active monitor -- the active monitor experiencing the problem was replaced when the problem was detected.

Internal Errors

The NIC has detected a problem with itself. Run the diagnostics from the NIC manufacturer. You may need to replace the NIC.

Upstream Node Address

Use this information to identify who is next in the ring and to manage your network.

Last Ring ID

This contains the value of the local ring ID.

Last Beacon Type

This contains the value (in hexadecimal) of the last beacon Medium Access Control (MAC) frame seen by this NIC.

The MAC frame types are:

01 Set Recovery Mode: The frame type is only generated by an attached product acting as a recovery station. (NetFlex Controllers will not generate this beacon type.)

02 Signal Loss: A signal loss condition was detected during the monitor contention process.

03 Bit Streaming: A monitor contention timeout occurred and no claim token MAC frames were received during the contention period.

04 Contention Streaming: A monitor contention could not be resolved with 1 second due to one or more claim token MAC frames being received.