Troubleshooting OSI Layers 1–3

In this two-part white paper series, learn to quickly locate and resolve problems across the OSI layers using the Troubleshooting Cheat Sheet.

User complaints never come at an opportune time. You are already being pulled in 20 directions when a user complains of slow Internet or email access. With few details and limited time to solve the problem, it's easy to overlook sound troubleshooting practices.

Not sure where to begin? The easiest place to start is by understanding as much as you can about the user's experiences. Mike Motta, NI University instructor and troubleshooting expert, places the typical user complaints into three categories: Slow Network, Inability to Access Network Resources, and Application-Specific Issues. Based upon the answers to the questions outlined in the following Troubleshooting Cheat Sheet, you'll gain a better understanding of the symptoms and be able to isolate the issue to the correct layer of the Open Systems Interconnection (OSI) model. Then you can begin troubleshooting.

Top 3 user complaints

- Slow network
- Inability to access network resources
- Application-specific issues

Complaint	What to Ask	What it Means
Slow Network	· What type of application is being used? Is it web-based? Is it commercial, or a homegrown application?	· Determines whether the person is accessing local or external resources.
	· How long does it take the user to copy a file from the desktop to the mapped network drive and back?	· Verifies they can send data across the network to a server, and allows you to evaluate the speed and response of the DNS Server.
	· How long does it take to ping the server of interest?	· Validates they can ping the server and obtain the response time.
	· If the time is slow for a local server, how many hops are needed to reach the server?	· Confirms the number of hops taking place. Look at switch and server port connections, speed to the client, and any errors.
Inability to Access Net-Work Resources	· What task is the user attempting to perform?	· Indicates whether the action is limited to a specific resource such as a mapped drive on a server or multiple network resources.
	· What type of application is the user attempting to access?	· Similar to the above question on application type, this may point to a problem with multiple internal servers.
Application-Specific Issues	· What's the 3-way handshake time?	· Identifies potential points where a slowdown might be occurring.
	· What's the server processing time?	· Points to whether the server is taking too long to process data.
	· How much data are you pulling from the application and sending across the network?	· Assesses whether the application is sending data in an expected and efficient way.

For additional information on application-specific issues, check out Mike Motta's Tech Tips.

Getting Started: The First 3 Layers

With these questions answered, working through the OSI model is a straightforward process. With the exception of Layer 1, each layer of the OSI model relies on the next lower layer to provide services as specified. Requests drop down and are completed, as every layer interacts with the next layer, both above and below.

When dealing with different layers, understanding how each delivers data and functions impacts how you will troubleshoot.

Layer Highlights and Functions

Physical Layer

- If it can blind or shock you, think Physical Layer
- Defines physical characteristics of cables and connectors
- Provides the interface between network and network devices
- Describes the electrical, light, or radio data stream signaling

Data Link Layer

- Converts signals into bits which become the packet data that everyone wants
- Performs error detection and correction of the data streams
- Manages flow and link control between the physical signaling and network
- Constructs and synchronizes data frame packets

Network Layer

- Logical addressing, routing, and packet generation
- Carries out congestion control and error handling
- Route monitoring and message forwarding

Getting Started: The First 3 Layers

With these questions answered, working through the OSI model is a straightforward process. With the exception of Layer 1, each layer of the OSI model relies on the next lower layer to provide services as specified. Requests drop down and are completed, as every layer interacts with the next layer, both above and below.

When dealing with different layers, understanding how each delivers data and functions impacts how you will troubleshoot.

Layer Highlights and Functions

Physical Layer

- If it can blind or shock you, think Physical Layer
- Defines physical characteristics of cables and connectors
- Provides the interface between network and network devices
- Describes the electrical, light, or radio data stream signaling

Data Link Layer

- Converts signals into bits which become the packet data that everyone wants
- Performs error detection and correction of the data streams
- Manages flow and link control between the physical signaling and network
- Constructs and synchronizes data frame packets

Network Layer

- Logical addressing, routing, and packet generation
- Carries out congestion control and error handling
- Route monitoring and message forwarding

Let's Get Physical

Generally speaking, Physical Layer symptoms can be classified into two groups of outage and performance issues. In most cases, investigating outage issues is the easiest place to begin, as it's a matter of confirming the link light is out or that a box is not functioning. Additionally, validating equipment failure is a matter of replacing the cable or switch and confirming everything works.

"I can't tell you how many Physical Layer issues are overlooked by people pinging or looking at NetFlow for the problem, when in reality it's a Layer 1 issue caused by a cable, jack, or connector," said Tony Fortunato, Senior Network Performance Specialist and Instructor with the Technology Firm.

"I jokingly tell analysts if you are close to the problem, it's time to take a walk and take a look at the cables. Be sure the issue isn't as simple as a cable pinched in a door. Thirty percent of the issues I fix are a result of me going for a walk," he said.

Physical-layer tool box

- Network analyzer
- Snmp poller
- Cable tester

The next step in investigating Physical Layer issues is delving into performance problems. It's not just dealing with more complex issues, but also having the correct tools to diagnose degraded performance. For example, if you're diagnosing an issue with slow email being caused by a physical issue, you need to have statistics enabled on the network equipment. That allows you to find physical-level errors, such as CRC or alignment errors that indicate performance problems. Then, confirm your analysis tools can view those errors either via packet capture with a TAP or SNMP polling.

Assessing Physical Performance Errors

When using a network analyzer capable of capturing packets with CRCs to diagnose performance issues, you may notice that the errors generated can point you in the direction of what's causing the Physical Layer problem. As a result, these errors can be divided into intelligent and non-intelligent errors.

Intelligent Errors:
An intelligent host is smashing into your network signal and corrupting the data.

Example: Overloaded WiFi network or a busy channel.

Non-Intelligent Errors:
An outside entity is causing noise that interferes with the signal or flow of data across the network.

Example: A microwave interfering with a WiFi signal.

Understanding Cabling Specifications

As cabling is essentially the heart of the Physical Layer, a simple rule of thumb is - When in doubt, start with your cables. The following characteristics are critical to understand when investigating:

- **Link Activation and Deactivation**
  This is the green light that should appear when you plug your computer into the switch. Although a good start, it doesn't mean there isn't a cabling issue. When you see the green light, you're verifying the ability to receive a signal but not to transmit.

- **Voltage Levels**
  When plugging a copper cable into a switch, verify there is enough voltage to support data flow. If you have the wrong type of cable or too long of a run, voltage levels may be reduced to the point that you won't receive a link light.

  If the link light sporadically turns on and off, this could be a sign of marginal voltage strength. Whether building your own cables or purchasing from a reputable manufacturer always test cable integrity.

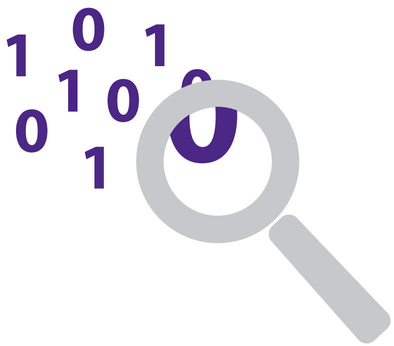
- **Data Rates**
  Data rate specifications for 1 Gb, 10 Gb, and 40 Gb require different cables (cat 5e or cat 6). Even though you may connect a cat 6 cable between computer and wall, verify that the cabling behind the wall is also up to specification.

  It's the same thing with wireless classifications of 802.11 a/b/g/n/ac, which correspond to the strength and/or quality of the signal. View these as suggested speeds rather than what will be achieved. Many variables can prevent the signal from reaching the advertised data rate.

- **Maximum Transmission Unit (MTU)**
  MTU defines how big your packets can be. If you're not using the maximum size, then network efficiency will be impacted. Verify that packet size is optimized.

  Application, server, and driver patches and updates are known culprits for knocking the packet size down unbeknownst to the network engineer.

Damage to or misconfiguration of any of the Physical Layer components can affect connectivity at every layer. Additionally, these problems can easily be misdiagnosed for upper-layer issues. A good understanding and review of Physical Layer concepts will prevent a lot of troubleshooting headaches down the road.



Application, server, and driver patches and updates are known culprits for knocking the packet size down unbeknownst to the network engineer.

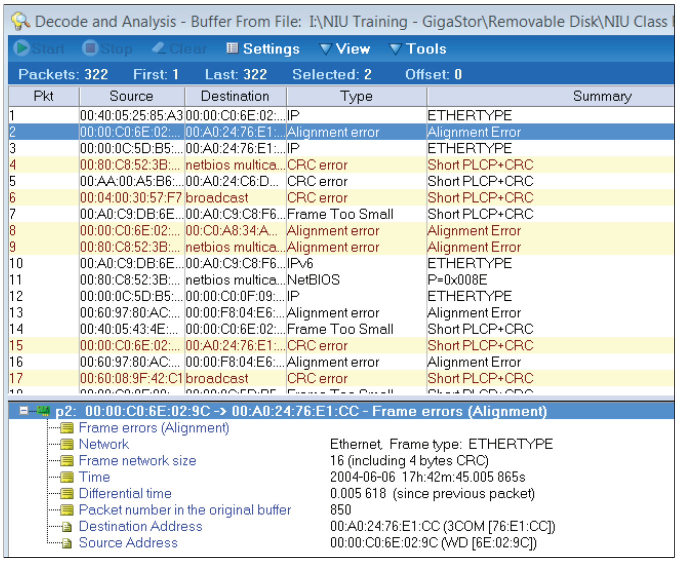
Data Link Layer and Sub-Layers

Data Link is the second layer of the OSI model and is comprised of two sub-layers -- the Logical Link Control (LLC) Layer and Media Access Control (MAC) Layer.

LLC: Interprets electricity, light, and WiFi into ones and zeros, which become the data packets.

MAC: Responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel. The sublayer uses MAC protocols to ensure that signals sent from different stations across the same channel don't collide.

"The easiest way to understand the Data Link Layer and the role of MAC is to think of a Layer 2 switch," said Fortunato. "Layer 2 doesn't deal with bits, rather it deals primarily with addresses represented by the MAC Layer. With every device having a MAC address, the sole concern of the Layer 2 switch is understanding how data gets from Port A to Port B. The switch has a table with two pieces of information – the address and the port. And that's it."



Decode and Analysis - Buffer From File: I:\NIU Training - GigaStor\Removable Disk\NIU Class

Packets: 322 First: 1 Last: 322 Selected: 2 Offset: 0

Pkt	Source	Destination	Type	Summary
1	00:40:05:25:85:A3	00:00:C0:6E:02:...	IP	ETHERTYPE
2	00:00:C0:6E:02:...	00:A0:24:76:E1:...	Alignment error	Alignment Error
3	00:00:0C:5D:B5:...	00:A0:24:76:E1:...	IP	ETHERTYPE
4	00:80:C8:52:3B:...	netbios multica...	CRC error	Short PLCP+CRC
5	00:AA:00:A5:B6:...	00:A0:24:C6:D...	CRC error	Short PLCP+CRC
6	00:04:00:30:57:F7	broadcast	CRC error	Short PLCP+CRC
7	00:A0:C9:DB:6E...	00:A0:C9:C8:F6...	Frame Too Small	Short PLCP+CRC
8	00:00:C0:6E:02:...	00:C0:A8:34:A...	Alignment error	Alignment Error
9	00:80:C8:52:3B:...	netbios multica...	Alignment error	Alignment Error
10	00:A0:C9:DB:6E...	00:A0:C9:C8:F6...	IPv6	ETHERTYPE
11	00:80:C8:52:3B:...	netbios multica...	NetBIOS	P=0x008E
12	00:00:0C:5D:B5:...	00:00:C0:0F:09:...	IP	ETHERTYPE
13	00:60:97:80:AC:...	00:00:F8:04:E6:...	Alignment error	Alignment Error
14	00:40:05:43:4E:...	00:00:C0:6E:02:...	Frame Too Small	Short PLCP+CRC
15	00:00:C0:6E:02:...	00:A0:24:76:E1:...	CRC error	Short PLCP+CRC
16	00:60:97:80:AC:...	00:00:F8:04:E6:...	Alignment error	Alignment Error
17	00:60:08:9F:42:C1	broadcast	CRC error	Short PLCP+CRC

p2: 00:00:C0:6E:02:9C -> 00:A0:24:76:E1:CC - Frame errors (Alignment)

Frame errors (Alignment)	
Network	Ethernet, Frame type: ETHERTYPE
Frame network size	16 (including 4 bytes CRC)
Time	2004-06-06 17h:42m:45.005 865s
Differential time	0.005 618 (since previous packet)
Packet number in the original buffer	850
Destination Address	00:A0:24:76:E1:CC (3COM [76:E1:CC])
Source Address	00:00:C0:6E:02:9C (WD [6E:02:9C])

As displayed in the Observer Analyzer, Common Layer 2 errors include CRC, Alignment, Too Small, and Too Large.

Did You Know?

If cabling isn't causing the problem, analyzers such as Wireshark or the Observer Analyzer can be used to view the individual frames taken from the media to locate anomalies. Software-based analyzers relying on a standard network adapter may be unable to detect MAC layer errors.

Corrupted Packet Flooding

It's critical for the switch to know what ports you're on. If this is incorrect, this can directly impact network performance. This is easy to spot when MAC addresses change due to a corrupt or errant packet. For example, if the known MAC address for the client is A-A-A but a corrupt packet reports the MAC address as A-A-1, the Layer 2 switch can respond in two ways:

1) If the packet is changed due to an error, it will trigger a CRC error and the switch drops the packet.

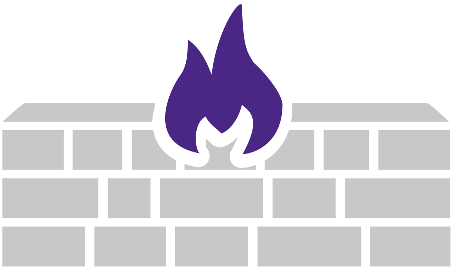
2) The switch isn't configured to check for errors, it simply passes the packet along and attempts to resolve the issue. Without knowing where the MAC address goes, it sends a copy of the packet to every port on that subnet or VLAN. The end result is that network engineers waste a long time locating the source of this packet flooding.

Flooding from MAC Misconfigurations

The second common issue at the Data Link Layer is flooding due to MAC misconfiguration issues. If a server has two cards to handle load balancing or failover, some of the protocols used will change the server MAC address. In this case, both cards have a single shared imaginary MAC address established by the server. This can also result in packet flooding, if the switch doesn't know where the MAC address belongs.

"I saw this type of flooding occur on a healthcare organization's network I was troubleshooting," said Fortunato." I plugged my analyzer into a common switch port, and proceeded to capture over 800 megabytes of data on a regular port. I thought it was a SPAN port, but the engineer informed me it was a normal port. This is common with switches, firewalls, routers or load balancers, where two NICs are sharing the same MAC address on a single device."

When you are implementing load balancing, verify with the manufacturer that the switch handles the specific type of load balancing being utilized and how to correctly configure the device. Although many switches are capable of learning and tuning to support load balancing, by default they may not be set up properly which results in flooding causing an unexplained network crash.



Be Aware

Due to security concerns, some organizations turn off ICMP. The challenge is applications that rely on ICMP for notification may fail without warning.

Network Layer Problems

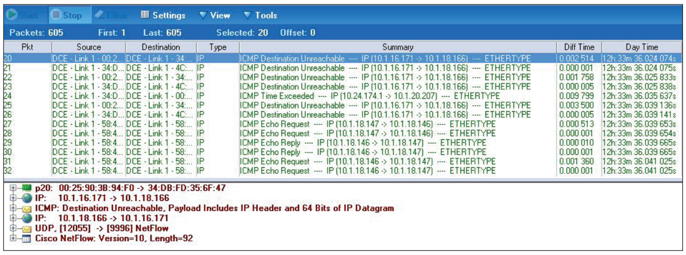
Both the Network and Data Link Layers are involved in aspects of data delivery, and understanding how each layer delivers data impacts troubleshooting. Where the Data Link layer is represented by the Layer 2 switch, the Network Layer is represented by a router. In routing data, the router is sending data packets to the network where the destination or end-point resides. Using mail delivery as an analogy, the router is reading the equivalent of your zip or postal code and sending it to the local post office.

It's the switch with a table of MAC addresses and ports that delivers the data to the destination (host or user). This is similar to the mail carrier bringing a letter from the local post office to your house.

"Typically, in the Network layer, the problems are going to be routing problems,"says Mike Motta. "Routes to nowhere. Wrong subnet masks, wrong default gateways, are the kinds of things that I typically find."

Finding the source of problems in the Network Layer requires smarter tools. "Using some of the built in tools that devices have like ping and traceroute, and a protocol analyzer like Observer® Analyzer is a good place to start. Typically you're looking for ICMP (Internet Control Message Protocol) messages coming back from the router telling you if there's a better route to get where you're trying to reach, ICMP redirects, telling you about wrong masks, things like that. The routers are sometimes smart enough to help us out if you know how to use a protocol analyzer."

"ICMP messages coming back from the router will tell us of wrong masks, wrong default gateways, wrong routes and route tables," says Motta. "Use the packets to look for ICMP messages. Also did the frame go to the right MAC address of the router or did it go to a different MAC address, or MAC address of a different router? These are all questions to ask."



Packets: 605 First: 1 Last: 605 Selected: 20 Offset: 0

Pkt	Source	Destination	Type	Summary	Diff Time	Day Time
20	DCE - Link 1 - 00:2...	DCE - Link 1 - 34:...	IP	ICMP Destination Unreachable ---- IP (10.1.16.171 -> 10.1.18.166) ---- ETHERTYPE	0.002 514	12h:33m 36.024 074s
21	DCE - Link 1 - 34:D...	DCE - Link 1 - 4C:...	IP	ICMP Destination Unreachable ---- IP (10.1.16.171 -> 10.1.18.166) ---- ETHERTYPE	0.000 001	12h:33m 36.024 075s
22	DCE - Link 1 - 00:2...	DCE - Link 1 - 34:...	IP	ICMP Destination Unreachable ---- IP (10.1.16.171 -> 10.1.18.166) ---- ETHERTYPE	0.001 758	12h:33m 36.025 833s
23	DCE - Link 1 - 34:D...	DCE - Link 1 - 4C:...	IP	ICMP Destination Unreachable ---- IP (10.1.16.171 -> 10.1.18.166) ---- ETHERTYPE	0.000 005	12h:33m 36.025 838s
24	DCE - Link 1 - 34:D...	DCE - Link 1 - 00:...	IP	ICMP Time Exceeded ---- IP (10.24.174.1 -> 10.1.20.207) ---- ETHERTYPE	0.009 799	12h:33m 36.035 637s
25	DCE - Link 1 - 00:2...	DCE - Link 1 - 34:...	IP	ICMP Destination Unreachable ---- IP (10.1.16.171 -> 10.1.18.166) ---- ETHERTYPE	0.003 500	12h:33m 36.039 136s
26	DCE - Link 1 - 34:D...	DCE - Link 1 - 4C:...	IP	ICMP Destination Unreachable ---- IP (10.1.16.171 -> 10.1.18.166) ---- ETHERTYPE	0.000 005	12h:33m 36.039 141s
27	DCE - Link 1 - 58:4...	DCE - Link 1 - 58:...	IP	ICMP Echo Request ---- IP (10.1.18.147 -> 10.1.18.146) ---- ETHERTYPE	0.000 513	12h:33m 36.039 653s
28	DCE - Link 1 - 58:4...	DCE - Link 1 - 58:...	IP	ICMP Echo Request ---- IP (10.1.18.147 -> 10.1.18.146) ---- ETHERTYPE	0.000 001	12h:33m 36.039 654s
29	DCE - Link 1 - 58:4...	DCE - Link 1 - 58:...	IP	ICMP Echo Reply ---- IP (10.1.18.146 -> 10.1.18.147) ---- ETHERTYPE	0.000 010	12h:33m 36.039 665s
30	DCE - Link 1 - 58:4...	DCE - Link 1 - 58:...	IP	ICMP Echo Reply ---- IP (10.1.18.146 -> 10.1.18.147) ---- ETHERTYPE	0.000 001	12h:33m 36.039 665s
31	DCE - Link 1 - 58:4...	DCE - Link 1 - 58:...	IP	ICMP Echo Request ---- IP (10.1.18.146 -> 10.1.18.147) ---- ETHERTYPE	0.001 360	12h:33m 36.041 025s
32	DCE - Link 1 - 58:4...	DCE - Link 1 - 58:...	IP	ICMP Echo Request ---- IP (10.1.18.146 -> 10.1.18.147) ---- ETHERTYPE	0.000 001	12h:33m 36.041 025s

```
p20:  00:25:90:3B:94:F0 -> 34:DB:FD:35:6F:47
IP:   10.1.16.171 -> 10.1.18.166
ICMP: Destination Unreachable, Payload Includes IP Header and 64 Bits of IP Datagram
IP:   10.1.18.166 -> 10.1.16.171
UDP, [12055]  -> [9996] NetFlow
Cisco NetFlow: Version=10, Length=92
```

Use Observer Analyzer to view ICMP messages and investigate routing errors, the network path, and potentially failing devices.

In addition to routing-related messages, another ICMP message to consider while troubleshooting the Network Layer is an indication of incorrect packet size. The protocol is changing the size of the packets to make things work, but when it can't, it sends an error message stating:

Fragmentation required, but the Do Not Fragment Bit is set. Fragmentation is required.

It also displays the appropriate packet size that should be sent. Network analysis tools pick up the proper size and may report this message. If proper packet size isn't achieved, the application will either drop the packets or disconnect.

Conclusion

For faster troubleshooting at any layer, begin with a solid understanding of how the issue affects the user. Using the right performance management tools along with the OSI model, you'll be able to more effectively apply analysis and identify root cause.

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you,
visit viavisolutions.com/contacts.

Product specifications and descriptions in this document are subject to change without notice.

troubleshootingosilayers1–3-wp-ec-ae
30176217 901 0315