Troubleshooting Wired Networks

by Sophia

WHAT'S COVERED

In this lesson, you will learn more about troubleshooting network problems, especially problems with wired networks. You will learn to first check all the “simple stuff” and how to approach problem resolution. We won’t be covering any new networking terminology in this lesson because you have all the foundational background material from previous tutorials.

Specifically, this lesson will cover the following:

1. Narrowing Down the Problem

Troubleshooting computers and networks is a combination of art and science, and the only way to get really good at it is by doing it. When initially faced with a network problem in its entirety, it’s easy to get totally overwhelmed. That’s why it’s a great strategy to start by narrowing things down to the source of the problem. To help you achieve that goal, it’s always wise to ask the right questions.

REFLECT

You can begin doing just that with the following list of questions to ask yourself:

- Did you check the super simple stuff (SSS)?
- Is it hardware or software that is causing the problem?
- Is it a workstation problem or a server problem?
- Which segments of the network are affected?
- Are there any cabling issues?

1a. Check the Simple Stuff

A simple stuff list really does include things that are this obvious, and sometimes so obvious no one thinks to check for them.

- Check to verify login procedures and rights.
- Look for link lights and collision lights.
- Check all power switches, cords, and adapters.
- Look for user errors.

The Correct Login Procedure and Rights

If you've set up everything correctly, your network's users absolutely have to follow the proper login procedure in order to successfully gain access to network resources. If they don't do that, they will be denied access. First, a user must enter their username and password flawlessly. Sounds easy, but sometimes people make a mistake, don't realize it, and report a network problem. A common problem is bad typing; people accidentally enter the wrong username or password.

You can restrict how many times a user can log in to the network simultaneously. If you've set that up, and a user tries to establish more connections than you've allowed, access will be denied. If a user is denied access to the network or its resources, they might think there is a network problem even though the network operating system is doing what it should.

Network Connection LED Status Indicators are a link light. These lights are those little light-emitting diode (LED) found on both the network interface card (NIC) and the switch. It's typically green and labeled Link or some abbreviation of that. A link light indicates that the NIC and switch are connected at Layer 2 (Data Link). If the link lights are lit up on both the workstation's NIC and the switch port to which the workstation is connected, it's usually safe to assume that the workstation and switch are communicating just fine. Some devices have two lights per port: a link light that stays solid and an activity light that flashes as data is sent or received.

All computer and network components must be turned on and powered up to function properly. Most systems include a power indicator (a power, or PWR, light). The **power switch** typically has an "On" indicator, but the system or device could still not have power if all the relevant power cables aren't actually plugged in, including the power strip.

The best way to troubleshoot power problems is to start with the most obvious device and work your way back to the power-service panel where power to the device begins. There could be a number of power issues between the device and the service panel, including a bad power cable, bad outlet, bad electrical wire, tripped circuit breaker, or blown fuse, and any of these things could be the actual cause of the problem that appears to be device-death instead.

Every cable has two ends, and both must be plugged into something for the connection to work. Sometimes **operator error** problems may be the answer. It could be that the user simply doesn't know how to use the system. Maybe you're dealing with someone who is poorly trained, and the problem is operator error (OE).

Before you jump to the conclusion that it is an OE, ask the user in question to reproduce the problem in your presence, and pay close attention to what they do. Understand that doing this may require a great deal of patience, but it's worth your time and effort if you can prevent someone who doesn't know what they're doing from causing serious harm to networked devices or creating vulnerabilities in your security.

Even if you suspect user error, always check out the problem thoroughly. If the problem and its solution aren't immediately clear to you, try the procedure yourself, or ask someone else at another workstation to do so. Don't just leave the issue unsettled or make the assumption that it is a user error or a chance abnormality.

2. Is it Hardware or Software That is Causing the Problem?

A hardware problem often rears its ugly head when some device in your computer is faulty or fails outright. A failure is easy to discern because when you try to do something requiring that particular piece of hardware, you can't do it and instead get an error telling you that you can't do it. Even if your hard disk fails, you'll probably get warning signs before it actually stops working, like a Disk I/O error or something similar.

Solutions to hardware problems usually involve one of the following three things:

- Changing hardware settings
- Updating device drivers
- Replacing defective hardware

If your hardware has truly failed, it's time to get out your tools and start replacing components. If this isn't one of your skills, you can either send the device out for repair or replace it. Because a system could be down for a while, anywhere from an hour to several days, it's good to keep backup hardware available. Do backup all data, files, hard drive, everything, and do so on a regular basis.

When assessing networks, software problems are often difficult to diagnose, so consider visiting the manufacturer's support website to get software updates and patches or searching for information about the problem in a knowledge base. Sometimes you can identify what is wrong from the precise message the software provides about the source of the problem. Messages saying the software is missing a file or a file has become corrupt are helpful because you can usually get your problem fixed quickly by providing that missing file or by reinstalling the software. Neither solution takes very long, but the downside is that whatever you were doing before the program shut down will probably be at least partially lost; so again, back up your data often.

2a. Is it a Workstation Problem or a Server Problem?

The first thing you've got to determine when troubleshooting a given problem category is whether only one person or a whole group has been affected. If the answer is only one person (think a single workstation), solving the issue will be pretty straightforward. If more than one person is affected, your problem may involve the network, especially if several users are experiencing trouble.

HINT

If it's a single-user situation, your first line of defense is to try to log in from another workstation within the same group of users. If you can do that, the problem is definitely the user's workstation, so look for things like cabling faults, a bad NIC, power issues, and operating systems.

However, if a whole department can't access a specific server, take a look at that particular server, and start by checking all user connections to it. If everyone is logged in correctly, the problem may have something to do with individual rights or permissions. If no one can log in to that server, including you, the server probably has a communication problem with the rest of the network. And if the server has totally crashed, either you'll see messages telling you all about it on the server's monitor or you'll find its screen completely blank, which are indicators that the server is no longer running. And keep in mind that these symptoms may vary among network operating systems.

2b. Which Segments of the Network are Affected?

If multiple segments are affected, you may be dealing with a network-address conflict. Remember that IP addresses must be unique across an entire network. So, if two of your segments have the same static IP subnet addresses assigned, you'll end up with duplicate IP errors, which is a situation that is difficult to troubleshoot and can make it tough to find the source of the problem.

HINT

If all of your network's users are experiencing the problem, it could be a problem with a server everyone accesses. Another possibility is that other network devices like your main router or hub may be down, making network transmissions impossible and usually meaning a lot more work on your part to fix.

Adding wide area network (WAN) connections to the mix can complicate matters, so find out if stations on both sides of a WAN link can communicate. If those stations can't communicate, then you need to check everything between the sending station and the receiving one, including the WAN hardware, to find the source of the outage. WAN devices have built-in diagnostics that tell you whether a WAN link is working okay, which really helps you determine if the failure has something to do with the WAN link itself or with the hardware involved.

2c. Is it Bad Cabling?

Once you've figured out whether the problem is related to one workstation, a network segment, or the whole network, you must then examine the relevant cabling. Are the cables properly connected to the correct port? Check the patch cables running between a workstation and a wall jack. Also, check the NIC and if there is no link light blinking, you may have a bad patch cable to blame.

An understanding of the physical issues that can happen on a network when a user is connected via cable (usually Ethernet) is critical information to have in your troubleshooting repertoire.

Because many of today's networks still consist of large amounts of copper cable, they may suffer from the same physical issues that have plagued networking since the very beginning. Newer technologies and protocols have helped to a degree, but they haven't made these issues a thing of the past yet.

Some physical issues that still affect networks are listed and defined in the table below.

Damaged Cable	The first things to check when working on cabling are the cable connectors to make sure they haven't gone bad. After that, look to make sure the wiring is correct on both ends by physically checking the cable pinouts.
Bad Port	In some cases, the issue is not the cable but the port into which the cable is connected. On many devices ports have LEDs that can alert you about a bad port. For example, a router or switch will usually have an LED for each port and the color of the LED will indicate its current state. In most cases, the lack of any light whatsoever indicates an issue with the port.
Transceiver Mismatch	Interfaces that send and receive are called transceivers. When an NIC is connected to a port, the duplex and speed settings must be the same between the two transceivers, or issues will occur. If the speed settings do not match, there will be no communication.
Crosstalk	Crosstalk refers to signal bleed between two adjacent wires that are carrying a current. Network designers minimize crosstalk inside network cables by twisting the wire pairs together, putting them at a 90-degree angle to each other. The tighter the wires are twisted, the less crosstalk you have, and newer cables like Cat 7 cables really make a difference because of their construct, which addresses many crosstalk issues.
Attenuation	As a signal moves through any medium, the medium itself will degrade the signal because of interference by particles in the medium that construct the medium. This phenomenon is known as attenuation and is common in all kinds of networks. While signals traversing fiber-optic cables don't attenuate as fast as those on copper cable, they still do eventually.
Latency	Latency is the delay typically incurred during the processing of network data. A low-latency network connection is one that generally experiences short delays, while a high-latency connection generally suffers from long delays. Many security solutions may negatively affect latency. For example, routers take a certain amount of time to process and forward any communication.
Jitter	Jitter occurs when the data flow in a connection is not consistent; that is, it increases and decreases in no discernable pattern. Jitter results from network congestion, timing drift, and route changes. Jitter is especially problematic in real-time communications like IP telephony and videoconferencing.
Shorts	A short circuit, or short, happens when the current flows through a different path within a circuit than it's supposed to; in networks, they're usually caused by some type of physical fault in the cable. You can find shorts with circuit-testing equipment, but because sooner is better when it comes to getting a network back up and running, replacing the malfunctioning cable is your best option.
Interference	Electromagnetic interference (EMI) and radio frequency interference (RFI) occur when wireless signals interfere with the normal operation of electronic circuits. Computers happen to be really sensitive to sources of this. For example, TV and radio transmitters, which create a specific radio frequency as part of their transmission process, increase incidents of interference. Your only way around this is to use shielded network cables like shielded twisted pair (STP) or to run EMI/RFI-immune fiber-optic cable throughout your entire network.

Bottlenecks	Bottlenecks are areas of the network where the physical infrastructure is not capable of handling the traffic. In some cases, this is a temporary issue caused by an unusual burst of traffic. In other scenarios, it requires an upgrade of the infrastructure or redesign of the network to alleviate the bottleneck. The result of a bottleneck is poor performance.

SUMMARY

In this lesson, you learned more about troubleshooting network problems, especially those with wired networks. You learned to first check all the “simple stuff” and about how to approach problem resolution by **narrowing down the problem** by figuring out if it is **hardware or software that is causing the problem**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**