The MSP's 'QUICK FIX' guide to troubleshooting common network problems

EPITIRO

Wireless network problems – from slow or patchy connectivity to full-blown outages – can be a cause of significant inconvenience, frustration and lost productivity for business customers and employees alike.

For managed service providers (MSPs), finding the source of issues can prove equally exasperating.

In the following guide, we consider seven of the more common network problems and how they can be easily resolved.

1

Slow network speeds

The underlying causes of slow internet performance – one of the more common complaints faced by IT professionals, manifest in symptoms such as slow page loads and video buffering – can be attributed to one or more of the following:

Not enough bandwidth for the traffic

If one of the channels through which your data is travelling is not wide enough, that channel will cause congestion and the traffic can slow. The bandwidth limits may be at the Wi-Fi radio, the Ethernet connections to the gateway switch, or the connection provided by your internet service provider (ISP).

The destination is a long way away

The server you are trying to access may be on the other side of the country, or even across an ocean. The journey time from your device to the destination and back will limit the speed at which you get a response. This results in high latency, or high 'ping' times.

Your data is not taking the shortest route

Modern IT networks have many checkpoints, for safety and security, from firewalls and VPNs to proxy servers. There is also a proliferation of different routes or paths to your destination. The internet highways over which your data travels are owned and operated by many companies, some are fast while others are painfully slow backroads. Your data may transit from one provider's connection to another on its way to its destination.

The 'engine' is not powerful enough

In some cases, old laptops, PCs, phones, or network servers cannot keep up with the demands of high-resolution graphics delivered over a speedy internet highway.

THE FIX

There are tools available to help you identify the likely cause within these broad categories:

The equipment needs an upgrade

Most laptops, desktops and phones more than four or five years old will be unable to deliver the latest available speeds and resolutions. While they may still work, they are more likely to appear slow and lethargic next to newer devices. The slower clock speeds in older Central Processor Units (CPUs) and Graphics Processor Units (GPUs), coupled with slower and less memory often make them under-powered engines.

Older equipment may not support the latest technical standards. This can be a new super-efficient Coder/Decoder (CODEC) required to deliver high-quality video or reliable speech over an IP connection, or handle the latest multi-user streaming or Teams application.

Another limitation could be the Wi-Fi chip, or its supporting driver software. An old device might still be limited to the Wi-Fi standards of yesterday - 802.11b and 802.11g, which only support narrower bandwidth channels on more congested 2.4GHz radios. Although 802.11n works on the 5GHz band, it does not support the latest coding and modulation methods required to deliver the highest speeds. The most commonly used standard, 802.11ac, which was introduced back in 2013, is now being replaced by the latest 802.11ax (Wi-Fi 6) radios.

It is easy to identify the age or model of your equipment. There are usually stickers or codes on the hardware identifying the model number and a quick internet search will let you know when it was made and what the tech-specs are. Another option is to browse the 'Settings -> About' menu on the device and it will usually reveal the contents of its technical heart.

THE FIX

It takes too long to get a response

This is easily identified with what is commonly called a 'ping' or 'latency' test. This test sends a small package of data to the destination server – its IP address, and a response package is immediately returned by the server. The exact time the package was sent and then received by the sender is measured and the Round Trip Time (RTT) is presented, usually in thousandths of a second (ms). Free ping test software is widely available.

Latency, or ping measurements, of 20ms or less are considered good. When the result is around 50 – 100ms, the communication link may need to slow itself down to wait for acknowledgments from the other end.

How do you know if the slow response is simply physical distance or a meandering path with detours? One option is to look at your geography relative to the location you are trying to reach. If you are on a remote island or a long way from internet infrastructure, you may never achieve optimal latency or a 'low ping' until more internet infrastructure comes to you. If, however, you are in a modern city or town, it is more likely that your internet route is slowed by roadblocks and traffic detours.

Again, free software can help you. Running a 'traceroute' application will identify the path taken between machine and destination. Most will identify how many 'hops' between different networks are taken, how long each hop was, and what (if any) packet loss was experienced by each hop. A traceroute can be help identify if your service provider is handing off your traffic to a low-cost, slow network provider.

Although most ISP supplied routers are set up to use DNS (Domain Name System) servers operated by the ISP, if necessary, you can adjust DNS settings to use the most appropriate and best performing public DNS servers.

Hiccups on router hops may have to be resolved by the ISP because of an issue on its network or within the hosting providers' domain. Sometimes, however, the problem may lie within the client's own network.

THE FIX

Not enough internet bandwidth for the traffic

Identifying this can be tricky because the available bandwidth from the internet and the competing traffic are continually changing. First, identify the theoretical, or maximum, bandwidth you believe you have.

What are you paying your ISP to provide? Are your speeds the same for upload and download? Having fast download but slow upload may be fine for web-browsing, but you are going to suffer on two-way video calls. Many ISPs offer far-slower upload than download. This is due to the limitations based on their legacy technology and is particularly prevalent if your ISP relies on the old telephone or cable TV infrastructure to deliver internet (DSL/ADSL).

Is the advertised bandwidth the same as the real bandwidth? Close to 1Gbps can be realized on a gigabit service over Ethernet, but you will not typically measure higher than 600Mbps over Wi-Fi for that service, even if it is feeding into a high-end Wi-Fi 6 access point connected to the latest Android phone.

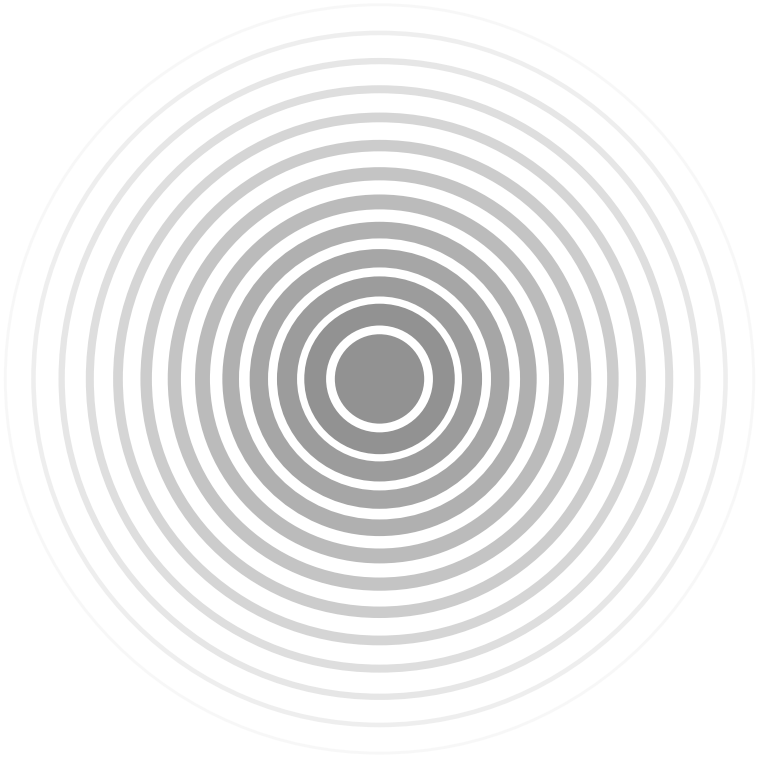
How many users and devices are simultaneously using the service? Slow performance can often be a result of bandwidth congestion, particularly in businesses and organisations that employ a lot of devices and process large quantities of data.

The solution may ultimately call for an upgrade to network speed and capacity. This should be accompanied by upgraded hardware, including the latest switches, servers and routers to minimise bottlenecks.

2

Poor radio signal

Wi-Fi's airwave transmissions are inevitably less reliable than wired network connections. This is due to two main factors – the radio signal is too weak, or there are other signals drowning out or interfering with the one you want.



A weak signal can simply be a result of the distance between the Wi-Fi access point and the client device. A typical Wi-Fi system only provides a strong enough signal for a high-speed connection when you are within one or two hundred feet of the access point. Obstructions can also be a cause, particularly thick or metal objects, which can create 'shadows' or areas of very weak signal.

Interference with the signal from your Wi-Fi access point, meanwhile, can derive from a variety of radio transmission sources. The frequency used by a microwave oven, for example, sits in the middle of the most used Wi-Fi band – 2.4GHz. A poorly shielded or damaged microwave can transmit signals that drown-out your Wi-Fi. Badly designed electric motors, circuits, and lighting can also all emit noisy radio waves that interfere with your signal.

The most common problem, however, is neighboring Wi-Fi networks and access points. If your neighbor's network has been set up to transmit in non-recommended channels, which is common, they can cause a lot of interference. Best practice for operating in the 2.4GHz band is to use channels 1, 6 and 11, which provides for maximum separation and minimum interference.

Many installers or DIY users, however, configure their networks to run in other bands – often believing that those will be better, as other networks are not typically using them. Operation in these bands emit more interference into the recommended bands and receive more interference. If you have a neighboring system using a non-preferred frequency in the 2.4GHz band, it may be the cause of your performance issues.

THE FIX

Ensure that there is a clear path, if possible, between your Wi-Fi access point and the Wi-Fi devices. Mounting the access point in the ceiling or in an open space is generally recommended. If the device must be mounted behind furniture, or in an IT closet, try to ensure that there is space around it and that the surrounding materials are thin and non-metallic.

Perform a Wi-Fi scan and observe which Wi-Fi networks are being seen, at what signal levels and in which channels. There are many free Wi-Fi scan apps and PC tools that do this. If your equipment uses the 2.4GHz band, configure your system in the lesser used channels 1, 6 or 11.

If your interference is being caused by a source other than another Wi-Fi system, you may need to investigate with a dedicated Wi-Fi surveying tool or a traditional spectrum analyzer.

An upgrade to Wi-Fi 6 can help here. Wi-Fi 6 employs Basic Service Set (BSS) coloring, which 'marks' shared frequencies. This enables access points to determine if channels are too busy, or if they can transmit simultaneously.

3

Wireless access point failings and limitations

Wireless access points can underperform, or stop working, for a variety of reasons. Older devices may lack important tech functionality, leaving them incompatible with more modern devices.

Earlier 802.11b/g/n versions, will often struggle in busy environments, with multiple client connections to support. Wider channel specifications, along with several other radio design improvements supported in 802.11ac (Wi-Fi 5) and 802.11ax (Wi-Fi 6), were implemented to more reliably deliver higher speeds and many more simultaneous connections, with good quality of service (QoS) to all users.

THE FIX

Firstly, ensure firmware is up-to-date. More recent capabilities and key bug-fixes may be available on your existing access points with a firmware upgrade. To check this, login to your access point, or controller, as an admin user and review the settings menu. You will usually see information relating to the installed firmware version. A quick search on your manufacturer's website should reveal the latest versions available and allow you to update.

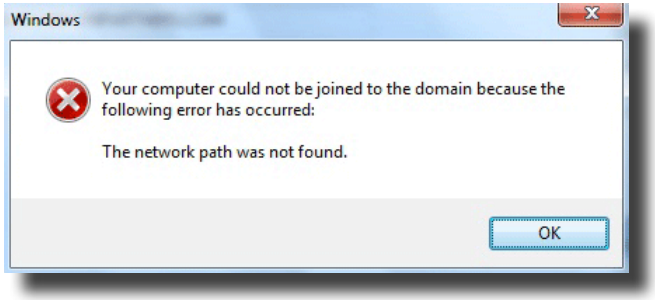
You may also need to update hardware. Some of the more recent innovations, such as MU-MIMO, require more antennas than earlier versions. These capabilities can only be realized with replacement hardware. If your hardware is failing or struggling and it is not at least 802.11ac (wave 2) or 802.11ax, you should also look to replace it.

4

DNS faults

If a DNS (Domain Name System) server is down, or if there is a problem with a device's DNS settings, access to the internet or specific applications may not be possible.

Error messages can include 'DNS name does not exist', 'network path cannot be found' and the 'IP address could not be found'.



THE FIX

Network devices should be checked to see what DNS servers they are using. DNS test tools can help identify connection issues and the servers responsible. A DNS will sometimes be rendered unavailable by a temporary server outage.

In some cases, devices may be configured to use their own DNS servers, ignoring the server assigned by DHCP.

Local network routers operating as DNS servers, meanwhile, will occasionally lead to them being overloaded. Changing network settings to run on a DHCP (Dynamic Host Configuration Protocol) configuration and directly access your DNS servers can significantly reduce errors.

It should be remembered that DNS errors will often be caused at the user end. The solution may be as simple as clearing the DNS cache or updating a web browser.

5

IP address duplication or exhaustion

When two devices on a network share the same IP address, conflict and connectivity problems can result. This invariably manifests with an "address already in use" or "address conflict" error message.

This problem can be caused when two or more DHCP servers exist on the same network with colliding configuration. They may be configured to issue the same ranges of IP addresses, for example.

IP-related connection issues can also arise as a result of IP address exhaustion – where the number of DHCP clients is larger than the number of available IP addresses in the address pool.

THE FIX

DHCP configuration is often to blame for IP address duplication. The DHCP may be assigning an IP address that is already in use (often low-numbered addresses at the beginning of the subnet) to a new network device. The new device may have its own DHCP server, which can be disabled to solve the problem, or router configurations can be changed so addresses are assigned from the top end of the subnet.

If you have more than one DHCP server on the same subnet, ensure they are each configured to issue IP addresses in different ranges to avoid the same address being allocated to different devices.

IP address exhaustion can also be resolved via the DHCP settings. In this case, by expanding the size of the address pool.

Where users are connecting to the internet without a local router, IP addresses may be limited to the allocation from the ISP. Here, the solution would be to purchase a standalone router or Wi-Fi access point.

Upgrading from IPV4 to IPV6 will ultimately help mitigate exhaustion of IPv4 addresses, allowing every device to have its own public IP address. An upgrade will also offer improved Wi-Fi performance by boosting routing capabilities.

6

Single device connection failures

When network connectivity problems relate to a single device, more often than not, the problem will reside with the device's hardware or software.

THE FIX

Check that device drivers are up-to-date and that network cards are working. Also check that network adaptors are configured correctly with the right IP, subnet and DNS servers.

Problems will also be commonly caused by firewall setting. Ensure web traffic ports are open – notably port 443 for encrypted HTTP traffic and port 80 for unencrypted traffic. For email, the common ports are 25, 587, 465, 110 and 995.

A DHCP server should be used to ensure uniform configuration to all network devices.

7

Double NAT (Network Address Translation) errors

Double NAT problems can be hard to detect as they do not affect basic activities, such as web browsing. They can however impact services such as Voice-over-IP, VPNs, secure SSL connections and online video games.

The problem occurs when two routers are connected, and each is performing Network Address Translation.

THE FIX

Update the network configuration so there is only one router responsible for Network Address Translation. A common solution can involve configuring one of the routers to act as a bridge.

EPITIRO

Epitiro Holdings, Inc.

5300 Westview Drive, Suite 306
Frederick, MD 21703, USA

1.844.EPITIRO (+1.301.304.6183)

Info@Epitiro.com

Sales@Epitiro.com

Support@Epitiro.com