



Title:

Network related troubleshooting

Summary/ Intro:

Guide can be used when the client is not able to make connection to the network

Steps:

Step 1: Troubleshooting network connectivity

Typical symptoms of an issue with network connectivity are:

- Error messages indicating “device not found” or that the connection has timed out.
- Applications slowing down, video and audio communication becoming laggy or even impossible to make.
- Domain syncing or authorization jobs take longer than usual – or fail completely – due to timeouts.
- Inability to communicate with devices located in the cloud (or over the internet), on the same network, and even in the same subnet.

The troubleshooting steps to take to resolve such network connectivity issues include:

- **Checking hardware** Check all your devices to make sure everything is connected properly, has been switched on, and is working well. Make sure all switches are in the



correct positions. Power cycling the device is a good idea. Also try turning it off and on.

- **Running ipconfig** This is perhaps one of the best troubleshooting tools in a network administrator's arsenal. You can use it to perform three major tests:
 - **Test connectivity** Ping a remote device to test connectivity.
 - **Find out your IP address** You can find IP details about your device to check for any misconfigurations.
 - **Reset your IP address** You can use the tool to refresh your IP address and get a new one to check for a DHCP error.
- **Running tracert** This is another basic tool that allows for testing the connectivity of devices, the route data packets take, the distance that is travelled (in seconds), and how healthy the connection is.
- **Running nslookup** This network administration command-line tool is used to test the DNS to determine whether there's a problem with a target server. Check out our article [nslookup: How to Check DNS Records – Step-by-Step Walkthrough](#) on how to use this tool to get the best out of your testing.



```
Command Prompt
C:\>nslookup www.google.com
*** Can't find server name for address 147.100.100.34: Non-existent domain
*** Can't find server name for address 147.100.100.5: Non-existent domain
*** Default servers are not available
Server: Unknown
Address: 147.100.100.34

Non-authoritative answer:
Name: .com
Address: 24.235.10.4

C:\>
```

A typical nslookup error – non-existent domain

- **Perform audit trails and log checks** Administrators make it a point to keep an eye on their network's usage and access history. Logs and audits are always good sources of information about what went wrong and give a clue about what can be done.
- **Kill unnecessary applications** Some applications can interfere with your network connection. Software solutions like [proxies](#), antiviruses, and anti-malware tend to block packets. Firewalls select traffic that passes through the network and misconfigurations could lead to unintentional disruption of traffic (or even bring to a complete halt).
- **Divide and conquer** Troubleshooting the network without these applications – the proxies, antiviruses, and anti-malware, i.e. – should be done with care, though. Letting down all defenses isn't an easy network administration decision to make. All access to the outside world (internet) should first be cut. Also, partial testing should be done to check each subnet for issues – and not the whole network – if possible.

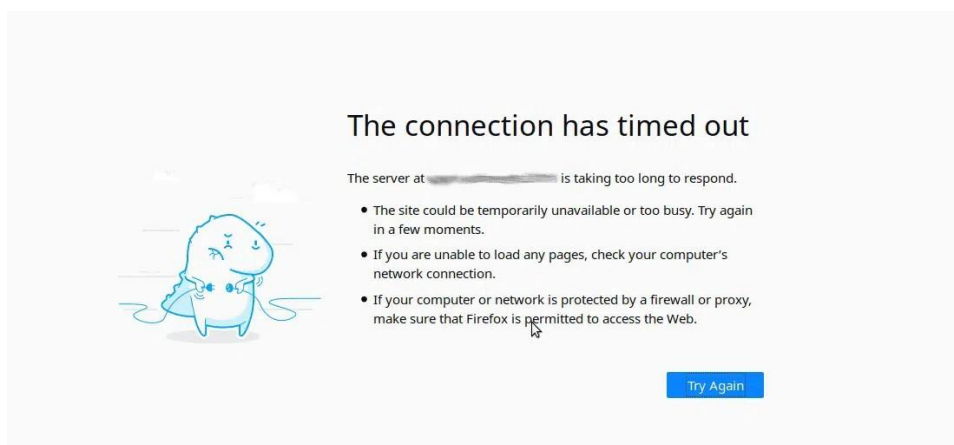
Step 2: Troubleshooting bandwidth issues

Typical symptoms of bandwidth issues are:

- Websites take forever to complete loading, return timeout errors, or don't load at all.



- Apps don't sync with servers and could even fail after timeouts.
- Client-server corporate solutions fail to update or retrieve data slowly.
- Communications between connected devices, and downloading or uploading normal file sizes, take ages – if it happens at all.



Connection timed out – a good sign of network connectivity issues

Loss of bandwidth can cause a whole network to come to a slowdown. Therefore, finding and eliminating bottlenecks should also be a part of troubleshooting network connectivity.

- **Look for the signs** You don't even need a tool to find issues with your bandwidth. Are your applications too slow? Are your videos suddenly taking longer to buffer? Do you get "connection timed out" error messages from your connectivity devices?
- **Slow delivery** Another indication would be the slow delivery of packets. These could be emails taking too long to reach recipients or tracert (traceroute) showing long hop times.
- **Use monitoring tools** If you need a graphical presentation of the bandwidth usage on your network, you can choose one of the tools listed in our post [5 Best Free Bandwidth Monitoring Tools for 2022- Network Traffic Usage](#).



Although you can simply pay for more bandwidth, this will be addressing the symptoms and not the root causes.

Step 3: Troubleshooting connectivity device configuration issues

Troubleshooting connectivity devices configuration issues can be divided into two major parts:

Configuration issues with connected devices

Examples of such devices include browsers, applications, laptops, mobile devices, and servers.

Typical symptoms of issues with such connected devices are:

- These devices have trouble connecting – or don't connect at all – even when the network is working perfectly.
- Someone else on the network, with the same type of connected devices, has no issues while you do.
- The connection issues were first noticed after configuration changes or updates were done on the devices.
- Network configuration – IP address, domain, authentication, privileges – change brings connectivity down.

Every device that is connected to a network needs the correct configuration before it can go online. This, as can be imagined, is a complicated undertaking and a broad topic.

Every device has its required configuration settings for it to connect to the internet correctly. In case of issues with such configurations, the only advice we can give you here is that you

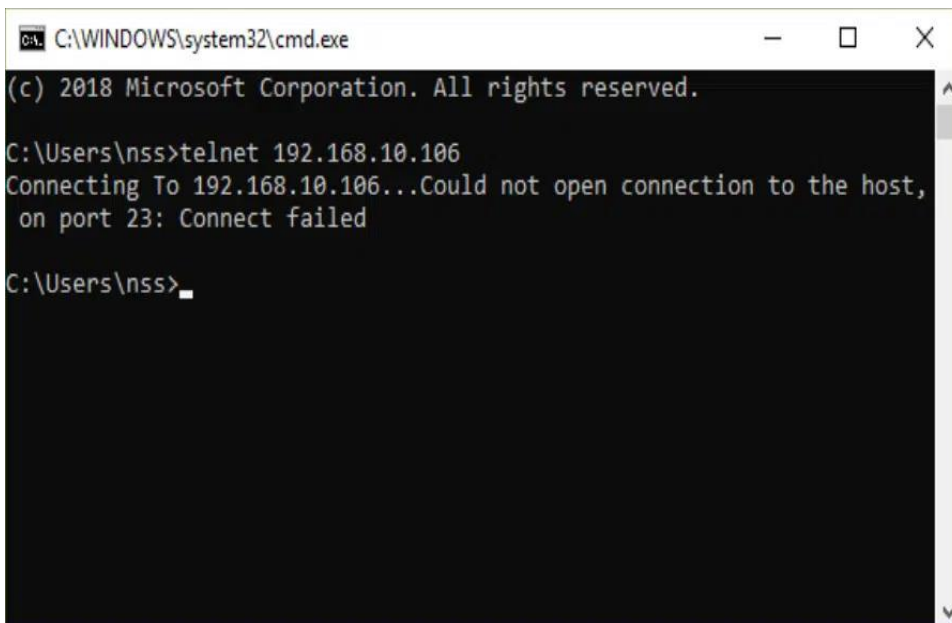


will need to get the support for the software or hardware from the products' makers and proceed accordingly.

After all, browsers, computers, servers, and mobile devices come under this category and all have unique configurations.

Some basic troubleshooting steps that can be taken include:

- Checking browser configuration, clearing the cache, reinstalling the browser, and trying switching to other browsers.
- Devices like laptops and PCs can try to [telnet](#) into the nearest router – a successful connection implies there are no hardware issues.



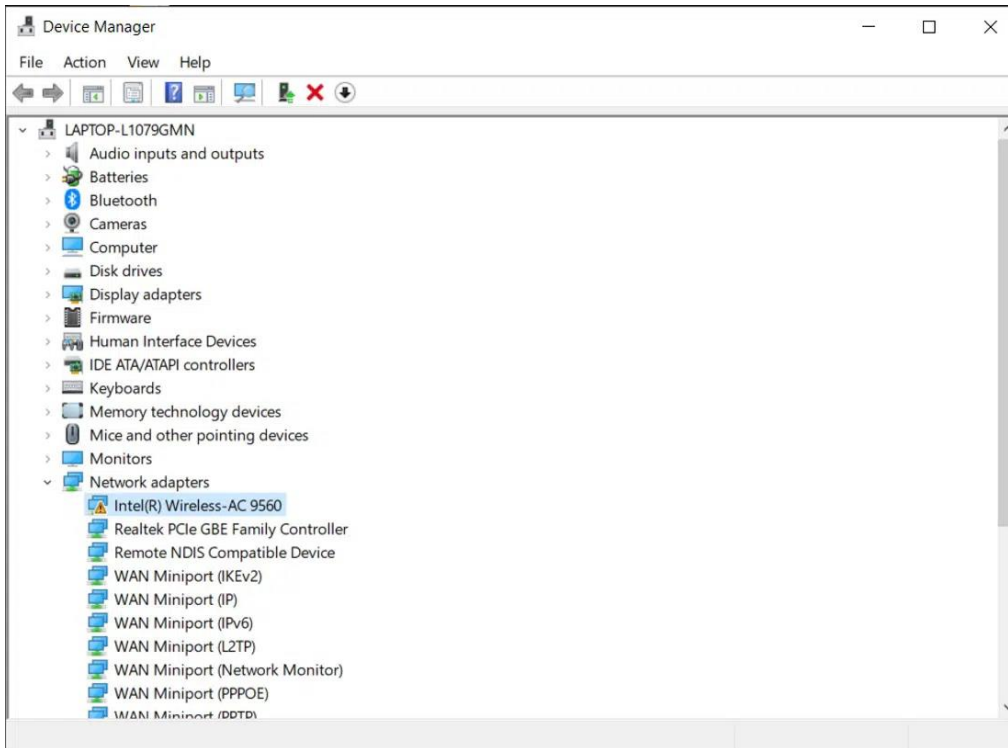
```
C:\WINDOWS\system32\cmd.exe
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\nss>telnet 192.168.10.106
Connecting To 192.168.10.106...Could not open connection to the host,
on port 23: Connect failed

C:\Users\nss>
```

Connect failed error – implies telnet couldn't open port 23 on the target host

- Rebooting the computer, server, or mobile device – updating all software, uninstalling recently installed applications, updates or upgrades.
- You can also [check for hardware conflicts](#).



A common hardware conflict like that with network adapters can cause a communication failure

A good administrator always has a backup of everything under their control and in case of a failure, they can revert to an older version – back to a restore point, that is.

Configuration issues with connectivity devices

Examples of such tools include hubs, routers, switches, gateways, and firewalls.

Typical symptoms of issues with such connectivity devices are:

- The devices have trouble maintaining network connections – or don't connect them at all – even when the rest of the network is working perfectly.
- The other, similar, connectivity devices have no issues – just one or a few of them.



- The issues were noticed when configuration changes or updates were done on the devices – they stopped working or there was a noticeable [latency](#) on the network.
- There were changes made in network configuration – IP address, domain, authentication, privileges – which brought the connectivity down.

Every connectivity device in a work has a specific task to perform. Depending on the location, a failed connectivity device can cause a network to lose packets or even drop connections completely.

The drivers for connection hardware like Wi-Fi adapters, NICs, and serial ports can affect connectivity if the latest versions haven't been installed. On the other hand, a driver update could bring a previously well-working device down. Administrators should make sure there are no conflicts by testing them before bringing them online.

Some basic troubleshooting steps that can be taken:

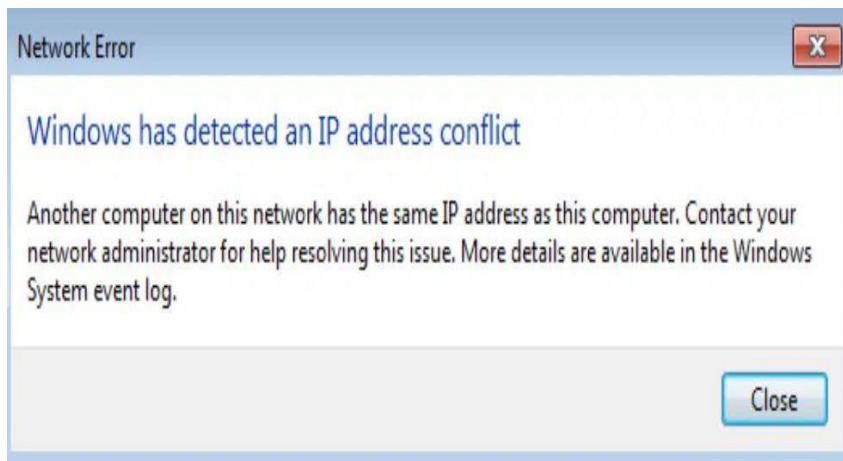
- Reboot the router, switch, or modem – these devices normally clear their caches and refresh their configurations which, in turn, could get rid of basic issues.
- Firmware updates can fix issues; therefore, administrators can simply run updates on their devices and see if it fixes the problem.
- Worst case scenario is that they might need to factory-reset the device and restart the configuration from the ground up.

Step 4: Troubleshooting IP and addressing issues

Typical symptoms of IP and addressing issues are:



- You get an error message about your IP address including one warning you about “... IP address conflict” or, in case of hosted sites, “This site can’t be reached... server IP address could not be found.”



IP address conflicts are signs of poor network configuration and administration

- Specific devices can’t access local shared assets like folders, servers, portals, and printers – even though everyone else does.
- Inability to sign into the domain – even with the right credentials being submitted.
- Your TCP command-line tools – like PING and TRACERT – return errors.

Now, although we have seen how CLI connectivity testing tools like IPCONFIG and tracert can uncover a lot of information about a network it is still a manual task. Also, when we talk about IP and connectivity issues we are talking about the misconfiguration of IP addresses for client devices, as well as connectivity devices – which is a lot of devices when considering the average network size.

All this means that administrators looking to troubleshoot IP and connectivity issues will need to [automate pinging and tracing](#) tasks.



Examples that could lead to issues include:

- Assigning the wrong IP address to a device or plugging it into the wrong subnet.
- Collision of IP addresses in the same subnet or on the network.
- The DHCP server is not assigning IP addresses or has run out of them.
- Wrong subnet mask being assigned thus curbing the IP range of a device.
- Using the wrong DNS configuration or assigning the wrong gateway and making it impossible for the device to connect beyond its subnet.
- Misspelling of device or domain names.

Next, there is the issue with accounts, roles, and privileges. Network and system administrators need to keep track of every account that is permitted to access digital assets.

Apart from the users, the assets themselves need to have permission to be on the network. It isn't uncommon for administrators to block communication between devices or networks. The Marketing group of users might not be allowed to access assets on the IT subnet. Therefore, troubleshooting such issues needs to start with checking permissions as it avoids having to unnecessarily tamper with devices' configurations.

Let us not forget that there are networks that intentionally block ping and traceroute packets to remain hidden. This means that just because you can't use these tools doesn't mean there is any connectivity issue.

Ultimately, if everything seems fine on your network, but the issue remains unresolved, you may need to contact your ISP to find out if there are any issues on their side, and inform them that everything on your side of the network is working fine and that it is just not connecting with any device beyond your perimeter.



Created By: Raiden Peake

Credit goes to Viren Govender