Troubleshooting Internet Connectivity - Home Lab

Lab Overview

This is a home lab for teaching you how to troubleshoot internet connectivity. You will take a follow-the-path approach where you trace the connection from a client machine all the way to the desired website. For each hop, you will identify the signs that a particular device is not functioning properly. You will also learn to identify and resolve common issues with that type of device on the network.

The goal of this lab isn't to teach you the fastest way to resolve network connectivity issues. It is to teach you about the different parts of a network and how they relate and work together to facilitate a connect to a website. This will help you develop a better understanding of how a network works and how to systematically troubleshoot all parts of a network.

Lab Outline

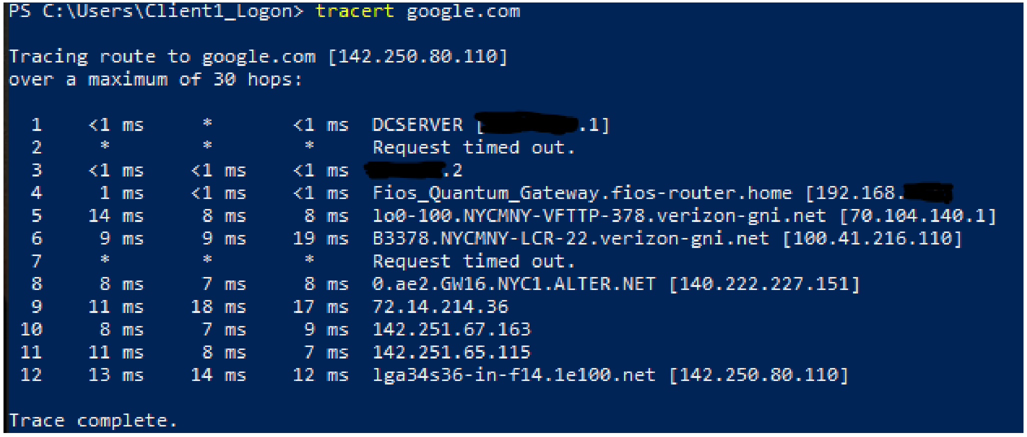
1. Lab Setup
    a. Diagram of the network path
2. Client Machine
    a. Restart and Update
    b. Firewalls
    c. Malware
    d. Troubleshoot NIC
3. Domain Controller
    a. DHCP Server
    b. DHCP Client Machine Troubleshooting
    c. DNS Server
    d. DNS Client Troubleshooting
4. Router / Default Gateway
5. ISP Network
6. Website Is Down
7. Conclusion

Lab Setup

This lab will consist of two virtual machines running on Oracle Virtual Box. One machine will run Windows Server 2019 and will function as the domain controller. This machine will also serve as the DHCP server and DNS server. The second machine will run Windows 10 Enterprise and will function as a client machine. It will connect to the domain controller through an internal private network.

A network packet will commonly take a path like the one in the diagram below. This will be the path that you will attempt to troubleshoot in this lab.

The complete path is Client Machine -> Domain Controller [DHCP Server & DNS Server] -> Router/Default Gateway -> ISP Routers -> Website Server.



```
PS C:\Users\Client1_Logon> tracert google.com

Tracing route to google.com [142.250.80.110]
over a maximum of 30 hops:

  1    <1 ms     *       <1 ms  DCSERVER [[redacted].1]
  2     *        *        *     Request timed out.
  3    <1 ms    <1 ms    <1 ms  [redacted].2
  4     1 ms    <1 ms    <1 ms  Fios_Quantum_Gateway.fios-router.home [192.168.[redacted]
  5    14 ms     8 ms     8 ms  lo0-100.NYCMNY-VFTTP-378.verizon-gni.net [70.104.140.1]
  6     9 ms     9 ms    19 ms  B3378.NYCMNY-LCR-22.verizon-gni.net [100.41.216.110]
  7     *        *        *     Request timed out.
  8     8 ms     7 ms     8 ms  0.ae2.GW16.NYC1.ALTER.NET [140.222.227.151]
  9    11 ms    18 ms    17 ms  72.14.214.36
 10     8 ms     7 ms     9 ms  142.251.67.163
 11    11 ms     8 ms     7 ms  142.251.65.115
 12    13 ms    14 ms    12 ms  lga34s36-in-f14.1e100.net [142.250.80.110]

Trace complete.
```

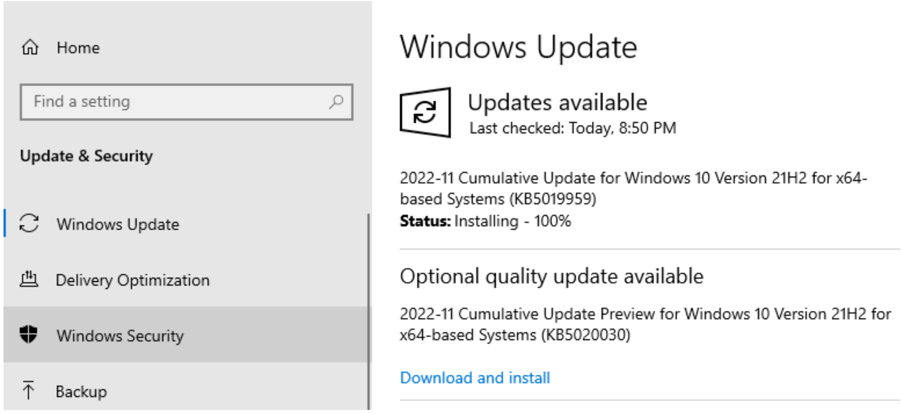
Client Machine

Let's start the troubleshooting process with the client machine which has internet connectivity issues. It's important to always question the obvious. Sometimes the problem can be caused by something as simple as a disconnected ethernet cable. Here are some other things to check on the client machine before you start troubleshooting the network.

1. Restart and Update

a. Software can just break on its own sometimes. Start by trying to restart the program you are using. Internet browsers often have many tabs open and use a lot of resources. Closing and restarting the browser is a quick option to try. Also closing all programs and restarting the machine will fix issues more often than you think.

b. Updating the applications and the operating system on your machine can also be an easy fix. There might be bug fixes and critical issues that are patched with the latest updates. Updates will also fix any files that may have been damaged or missing. Updating the operating system is also one of those methods that will often fix more problems than you think.



Windows Update

Updates available

Last checked: Today, 8:50 PM

2022-11 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5019959)

Status: Installing - 100%

Optional quality update available

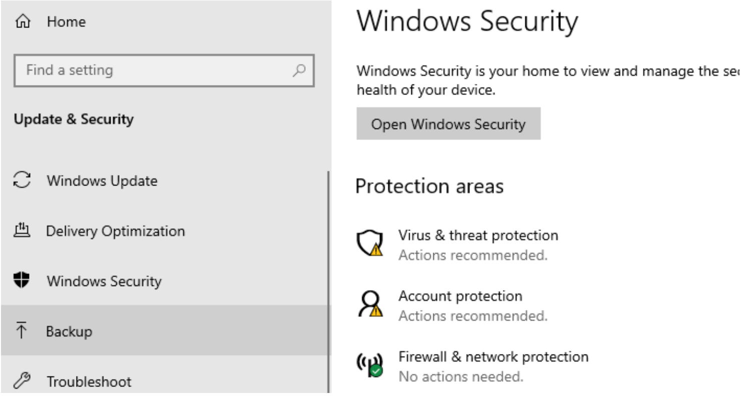
2022-11 Cumulative Update Preview for Windows 10 Version 21H2 for x64-based Systems (KB5020030)

2. Firewalls

The firewall is also commonly responsible for many issues with connectivity. It can perceive an outgoing or incoming connection to an application as malicious and block it. You will have to allow the app through the firewall or add a new outgoing or incoming rule to the firewall to resolve this issue.

a. Allow Applications Through Firewall

Allow the application through the firewall by going to Settings -> Windows Security -> Firewall & Network Protection.



Windows Security

Windows Security is your home to view and manage the se
health of your device.

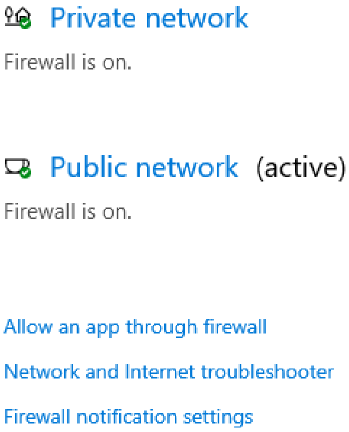
Protection areas

Virus & threat protection
Actions recommended.

Account protection
Actions recommended.

Firewall & network protection
No actions needed.

Then you click on Allow an app through firewall.


Private network

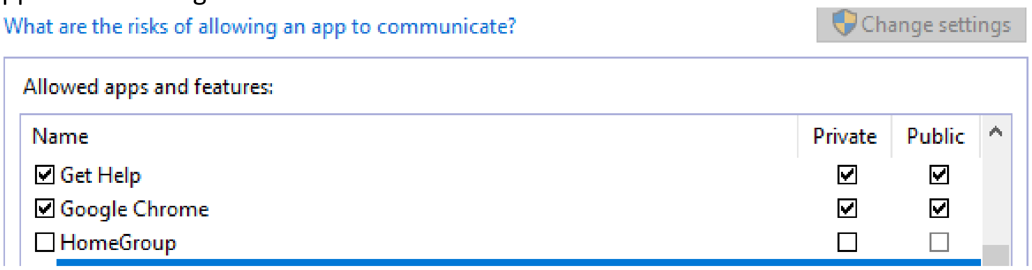
Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings

Scroll down and find the application with connectivity issues. You can click the Change settings button then check the private and public boxes as needed to allow the application through the firewall.

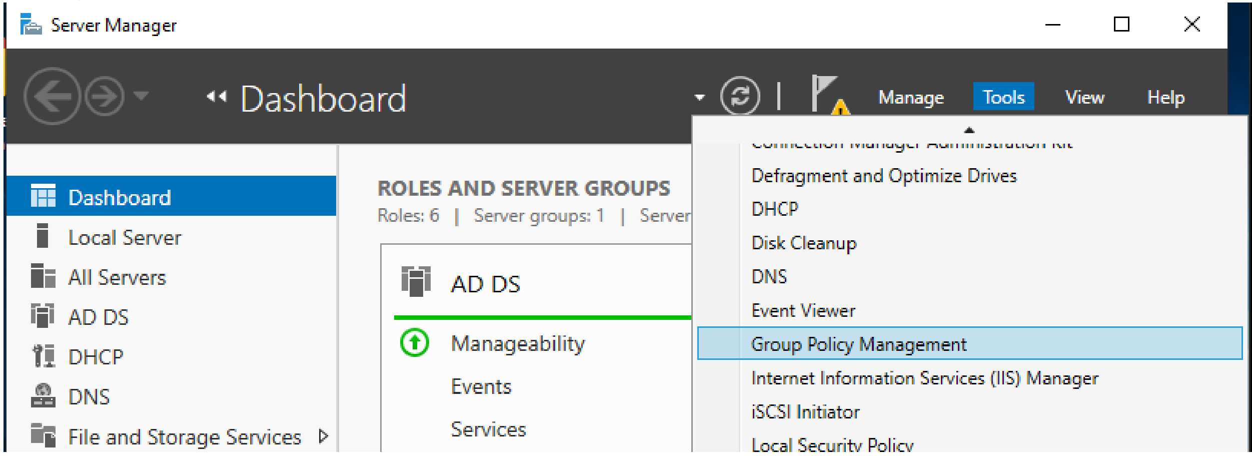


Allowed apps and features:

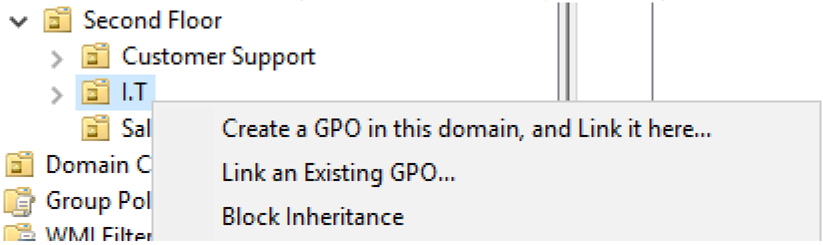
Name	Private	Public
☑ Get Help	☑	☑
☑ Google Chrome	☑	☑
□ HomeGroup	□	□

b. Add New Firewall Rules

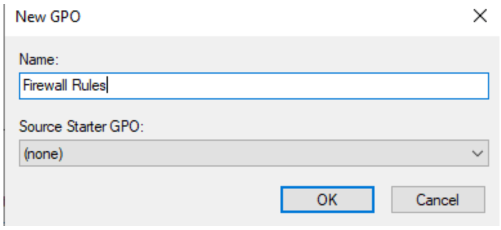
You can also edit or add new outgoing or inbound firewall rules. This will allow you to edit what ports and protocols are allowed or blocked. You do this by going to the domain controller and opening Server Manager. Go to Tools -> Group Policy Management.



You will now navigate to the OU in your organization that you want to apply this new firewall rule to. Right click on the OU and select Create a GPO in this domain and Link it here. If there is an existing firewall GPO, then you can right click on it and select Edit.



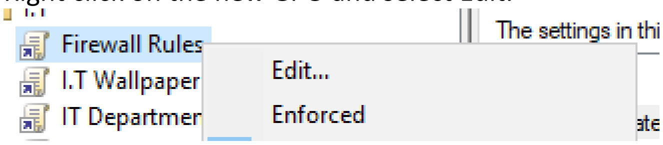
Give the new GPO a name then click ok.



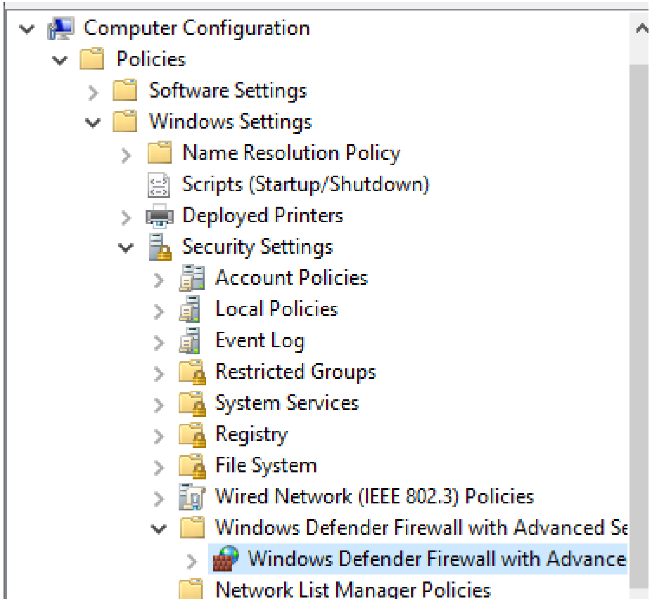
Name: Firewall Rules

Source Starter GPO: (none)

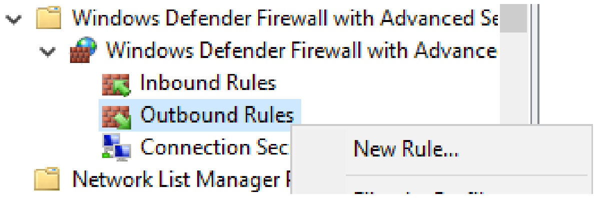
Right click on the new GPO and select Edit.



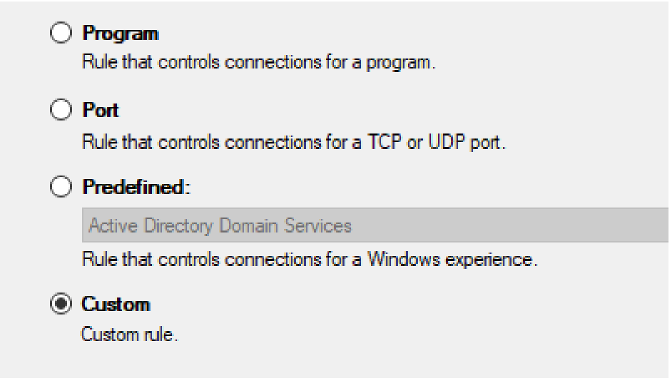
Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Defender Firewall with Advanced Security – LDAP.



Expand the submenu for Windows Defender Firewall with Advanced Security. You can now select between creating an outbound or inbound rule. For this lab you can right click on outbound rules and select new rules.


Windows Defender Firewall with Advanced Se
Windows Defender Firewall with Advance
Inbound Rules
Outbound Rules
Connection Sec
Network List Manager I
New Rule...

Select the Custom option and click next.



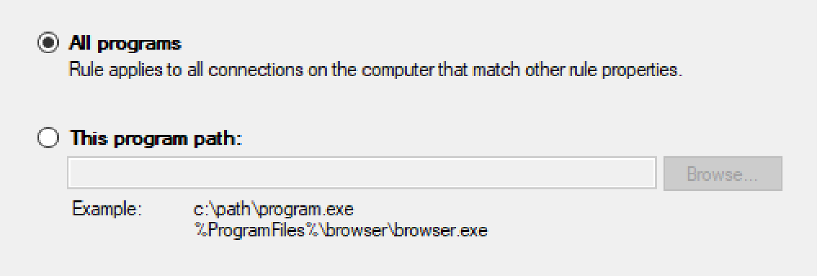
○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Active Directory Domain Services
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

For this lab we will attempt to allow all programs to make outgoing connections. To do this, select All programs, then Next.

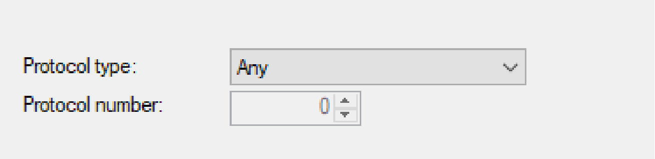


● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

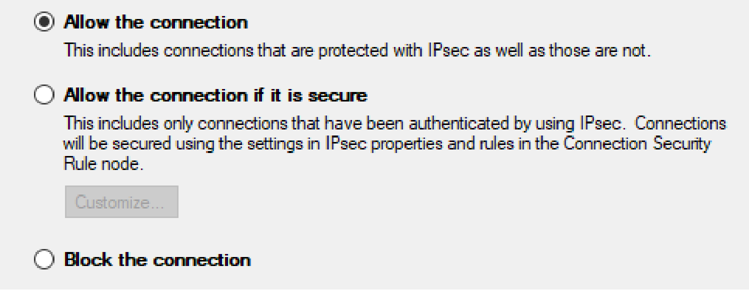
Set protocol type to any. Then click Next until you see the page in the next step below.



Protocol type: Any

Protocol number: 0

Select Allow the connection. Then click Next until you see the page in the next step below.

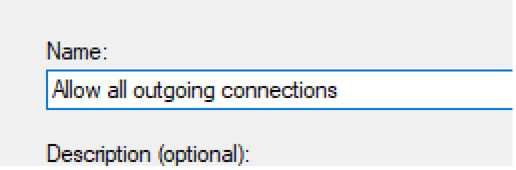


● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

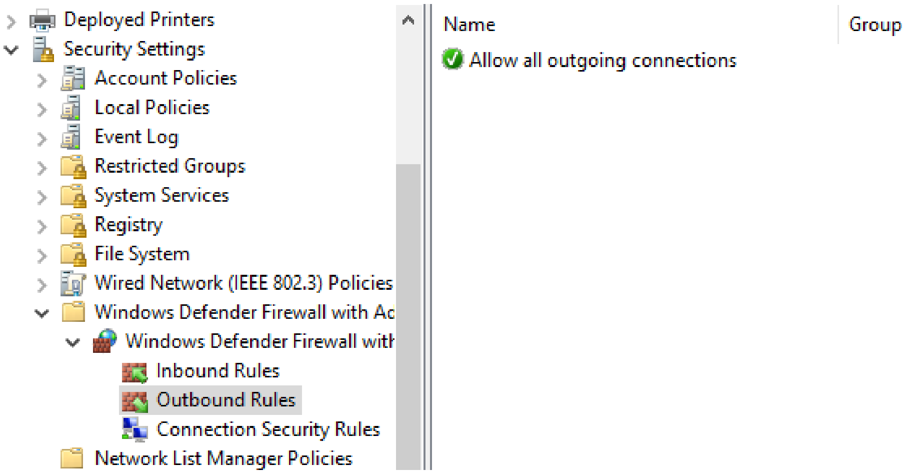
Give the rule a name. Then click to the end to complete the process.



Name: Allow all outgoing connections

Description (optional):

You can now see the new rule in the outbound rules page in Group Policy Management Editor. You can edit or disable the new rule from here.

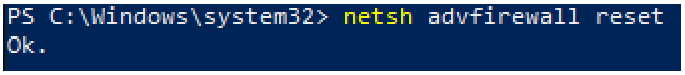

Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Ac
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies

Name	Group
✓ Allow all outgoing connections	

c. **Reset Firewall Rules**

If you believe that a firewall rule may be the cause of network connectivity issues, then you can try to temporally turn off the firewall to see if the connection is then restored.

If you can't identity which firewall rule is causing the issue, you can reset the firewall rules back to their default settings. You can do this by using the command "netsh advfirewall reset".



```
PS C:\Windows\system32> netsh advfirewall reset
Ok.
```

3. Malware

Malware on a client machine can cause it to have connectivity issues. This can be the malware trying to prevent the user from attempting to remove it. The malware will try to stop the user from updating their machine or downloading a program to get rid of the malware. The malware can also consume all available resources or connection bandwidth in its attempt to send data from the machine to a remote server. This infection might spread to other machines so you will have to isolate this machine and immediately elevate this issue to resolve it as soon as possible.

4. Troubleshoot NIC

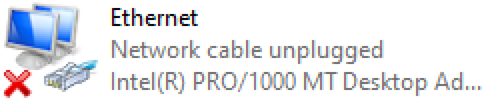
If you have tried everything and can't solve the connection issues, then the issue might be with the NIC on the client machine. It could be a software or even hardware related issue.

a. **Signs of Faulty NIC**

A sign that the NIC is going bad is if the connection is intermittent. This can show up with websites being intermittently slow to load. Downloads failing halfway. You can also test by going to an internet speed test website and seeing if the connection speed is consistent verses jumping up or down.

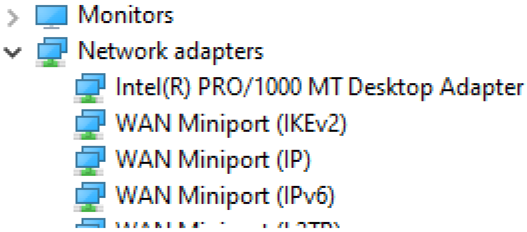
b. **Network Adapter Options**

You can also go to settings -> Network & Internet -> Change adapter options. Here you can look to see if there are any obvious issues. You can see if the NIC adapter is missing entirely or is displaying an error that might give you a hint of what the issue is.

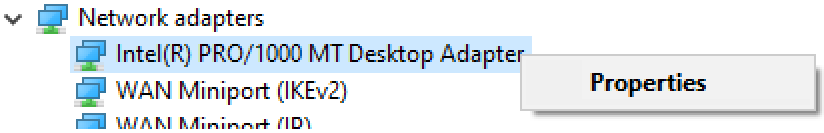


c. **Device Manager**

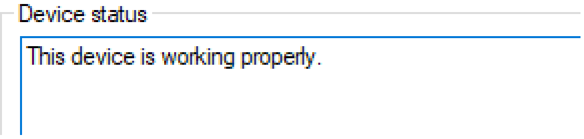
You can also check if the Network adapter is identified by the client machine by using device manager. Open Device Manger and scroll down to Network adapters. Expand the menu to see all adapters. If there are any issues, then the adapter might be missing completely or will show an error.



You can get more information by right clicking on an adapter and selecting Properties.



Here you can check the status of the adapter. If it is not working properly then you will see a display of the error.

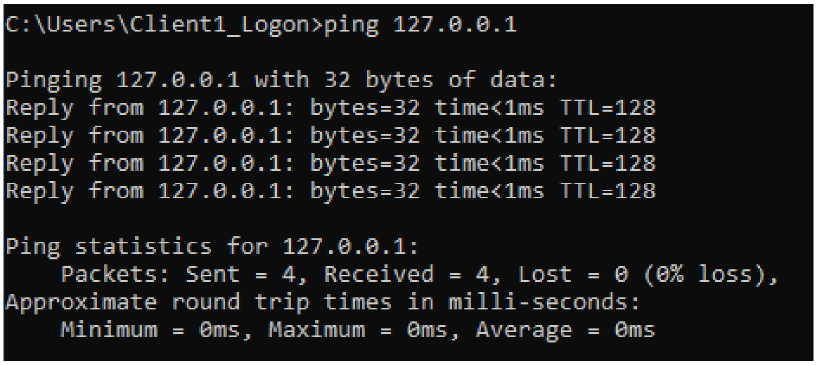


This device is working properly.

d. **Ping Test**

The more direct way to test if a NIC is faulty is to use a ping test. You do this by having the client machine ping itself. It will send packets to the NIC card and display the results.

To start the process, open the command prompt program or PowerShell and type “ping 127.0.0.1”. Then press enter to run the command. If the results show something similar to “Packets: Sent=4, Receive=0, Lost=4”, then the NIC is faulty. If the NIC is good, there should be no lost packets. You can run this test a few times to get a view of how often packets are being lost.



```
C:\Users\Client1_Logon>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

e. Resolve Hardware Related Problems

Start with the most obvious culprit. Is the ethernet cable properly plugged into the port. Is it showing signs of damage. You might have to try a new cable if you suspect it's a problem with the cable. Try to shake the cable when its plugged in. Is it in firmly or is it loose? When shaking the cable, does the LED on the port turn on as you move the cable. If it does, then it could be a bad port.

If the issue is not the cable, then you will have to replace the NIC card or motherboard if it is integrated. Before you do that however, you can insert a known good NIC card into the machine to see if that works. If the issue is resolved, then it is faulty hardware causing the problems.

i. **Hard Drive Swap**

A great way to determine if the connectivity issues are hardware verses software related is to boot into a different operating system on the same machine. You can do this by swapping the hard drive in the machine with a known good one. If the system booths and there are no issues, then it's a software issue. If it is still not fixed, then you know it's a hardware problem.

Most of the time the machine will find the new drive but if you are having issues then you can press the ESC/F10/F12 keys during boot. This will open the boot menu and allow you to manually select which drive to booth from.

f. Resolve Software Related Problems

If the issues are not hardware related, then they might be software related. Here are a few ways to resolve the software related issues.

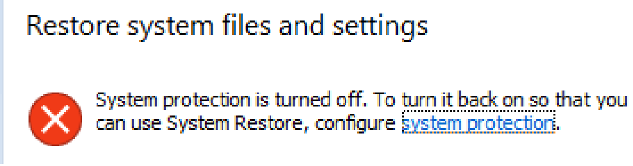
i. Boot Machine from Known Good State

If you have determined that that the issue could be software based, then you can booth the machine using a known good backup or perform a system restore. This is the fastest path to resolving the issue and will work most of the time if it's a software problem.

1. Restore from System Restore Point

You should first try to perform a system restore if you have not created any backups of your system, or you recently installed new programs or updates onto your system.

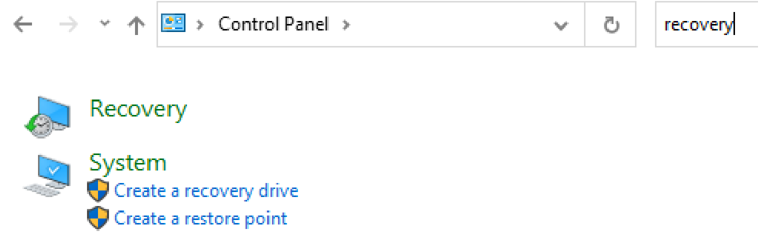
If system protection is not turned on, then you will not have any restore points and will not be able to use this method to restore the machine.



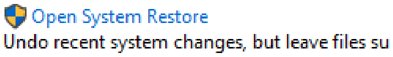
Restore system files and settings

System protection is turned off. To turn it back on so that you can use System Restore, configure system protection.

To perform a system restore, open Control Panel. Then in the control panel search box, search “recovery”. Select Recovery in the results.



Click open system restore.



Undo recent system changes, but leave files su

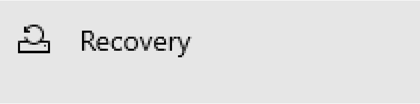
Click Next to go to the next page. You will see a list of system restore points. Select the one that you want to use to restore your system to. Then select Scan for affected programs. You will see a list of items which will be deleted if you proceed with the system restore. If you are ok with those items being deleted, then select close -> Next -> Finish.

2. **Resetting PC**

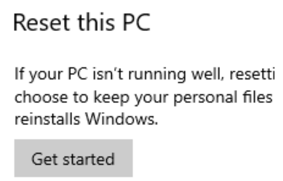
This is another method to use if system restore didn’t work. This option allows you to reinstall windows while keeping your files. You can do this from the settings or logon screen.

Unlike system restore, this method will delete all programs and change all settings back to default.

Reset your machine by going to Settings -> Update & Security -> Recovery.



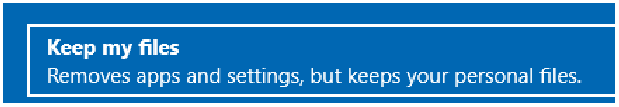
Under Reset this PC. Select Get Started.



Reset this PC

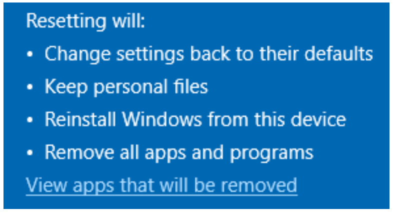
If your PC isn't running well, resetti
choose to keep your personal files
reinstalls Windows.

Select Keep my files.



Keep my files
Removes apps and settings, but keeps your personal files.

This process will keep your files but delete all programs and change settings back to default. Click the Reset button to begin the process.



Resetting will:

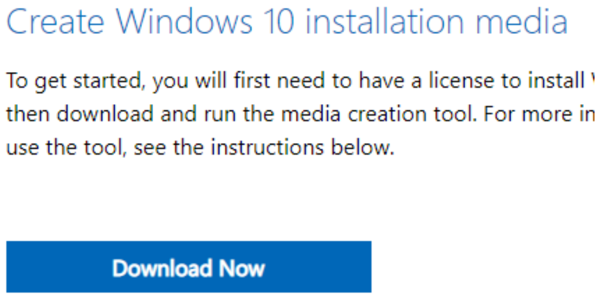
- Change settings back to their defaults
- Keep personal files
- Reinstall Windows from this device
- Remove all apps and programs

3. **Reinstall OS Using Installation Media**

If system restore and resetting your machine didn't work, then reinstalling the OS using Installation Media is the next option to try.

First you need to create a Windows 10 installation media. You will need to perform this process on another machine with a working internet connection. You can then transfer the installation media to the machine with connectivity issues.

Go to the link below and click Download Now under Create Windows Installation Media.
https://www.microsoft.com/en-us/software-download/windows10



Create Windows 10 installation media

To get started, you will first need to have a license to install
then download and run the media creation tool. For more in
use the tool, see the instructions below.

Once downloaded, double-click and open the installation media creation tool. Select Create installation media for another PC. Go through the standard windows installation process of choosing your preferred language, edition, etc. Save it to a USB drive and connect that to the machine with connectivity issues.

On the machine with connectivity issues, open file explorer and find the drive with the installation media on it. Double click the installation media to launch it and begin the process.

Select Change what to keep. Then select Keep personal files and Apps. Then select Next. Click Install to begin the installation process.

4. **Booth From Known Good Backup**

If you regularly save backups of your machines using the backup and restore feature, then you can simply restore your system from a backup or system image that you know is good.

To restore from a backup, hold shift while you press the restart button in the start menu. You can now click troubleshoot -> Advanced Options -> See more recovery options -> system image recovery.

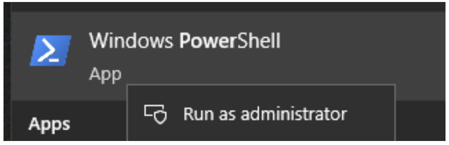
You can now follow the on-screen instructions and select the system image that you want to use for recovery.

ii. Troubleshooting Network Adapter Drivers

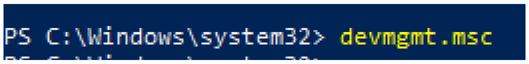
You can use Device Manager to fix software issues related to network adapter drivers.

You will need to open device manager with Admin right so that you have the correct permissions to uninstall and reinstall the correct drivers.

To do this, open PowerShell with admin rights.

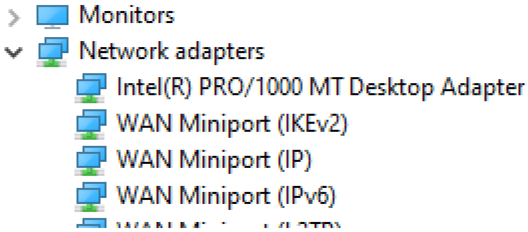


Then type in devmgmt.msc and press enter to launch device manager with admin rights. This will give you the permissions needed to uninstall and install drivers.

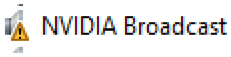


```
PS C:\Windows\system32> devmgmt.msc
```

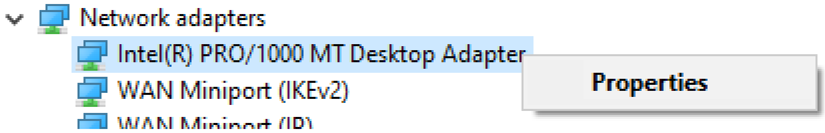
With Device Manger open, scroll down to Network adapters. Expand the menu to see all adapters. If there are any issues, then the adapter might be missing completely or will show an error.



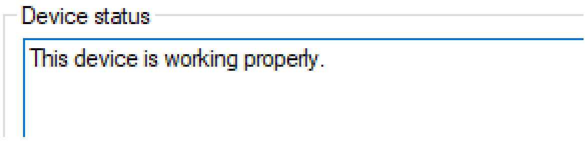
If there is an issue, then there will be a small hazard triangle over the adapter icon.



You can get more information about an adapter by right clicking on the adapter and selecting Properties.

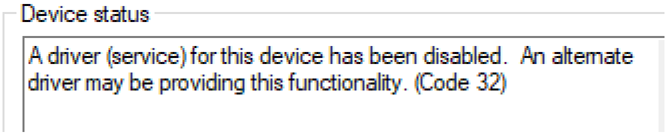


Here you can check the status of the adapter. If the device is working properly then it will show it is working properly, like below.



This device is working properly.

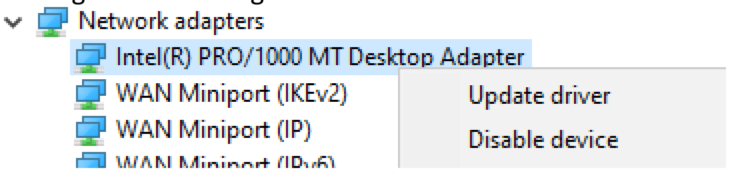
If it’s not working properly then you will see a display of the error.



A driver (service) for this device has been disabled. An alternate driver may be providing this functionality. (Code 32)

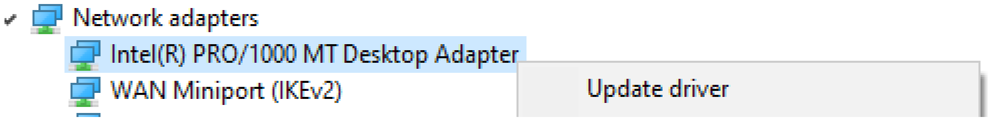
1. **Toggle Off and On Network Drivers**
   Just like how turning a machine off and then on can solve many problems, the same can happen with devices in device manager.

   To do this, right click on the Network adapter and select Disable device. Then right click on it again and select Enable device.

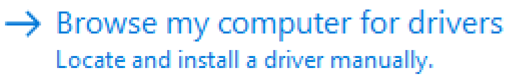


2. **Reinstall Network Adapter Drivers**
   You can fix network adapter driver issues by reinstalling or updating them. You will have to first find the driver on the manufactures website and download it. You can try searching the name of the driver in google and you will find the download for it.

   Once you have downloaded the driver, right click on the adapter and select Update driver.



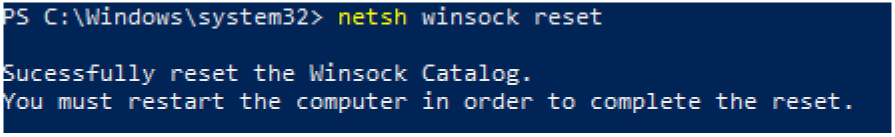
Then select Browse my computer for drivers. You can now navigate to where you saved the driver you downloaded earlier.


→ Browse my computer for drivers
Locate and install a driver manually.

iii. **Reset Winsock**

This is an API which operates between applications and the underlying communication protocols. Resetting its catalog back to the default settings might help solve network adapter problems.

First open PowerShell with Admin privileges. Enter the command "netsh winsock reset" and press enter to execute it. You can now restart the machine to complete the process.

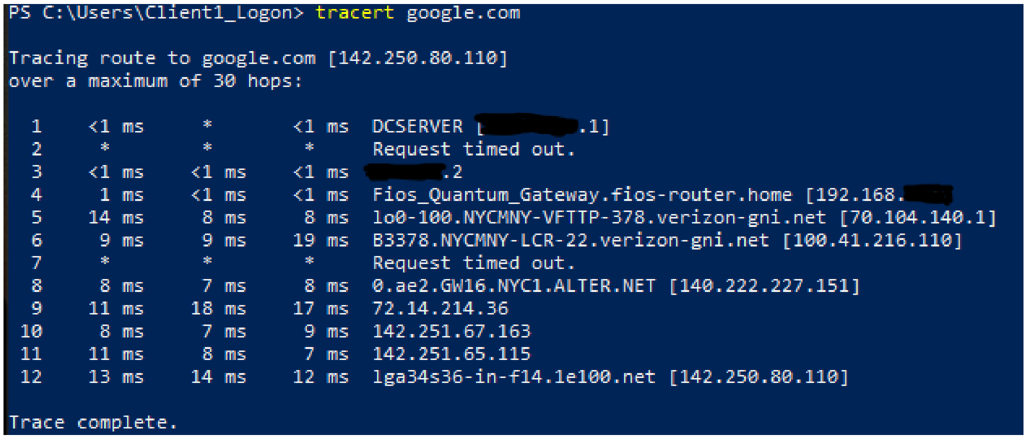

```
PS C:\Windows\system32> netsh winsock reset

Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
```

Domain Controller

The next step in the path is the domain controller. This machine will typically have all client machines on the private internal network connect to it. This allows the organization to control all traffic in and out of the network. This machine will also commonly serve as the DHCP and DNS servers for the network.

You can trace the path from a client machine all the way to a website using the tracert command in PowerShell. The most common way this is done is to use trace route to a popular website like google.com. The command for this is "tracert google.com". Below is the result from my test network to google.com.

The first hop from the client machine is the Domain Controller. The domain controller and the client machine are virtual machines. The client machines are connected to an internal private network. The 2nd hop attempt is a timed-out connection. From there you can see the 3rd hop is outside of the private internal network and is now inside my home network which the domain controller is connected to. From there, the 4th hop hits my home router. The 5th hop leaves my home network and is now hitting the ISP's routers on its way to Google's servers. At the 8th - 9th hop, you can see that the connection is now inside of google's servers. Eventually it lands at its final destination which is the web server for google.com.



```
PS C:\Users\Client1_Logon> tracert google.com

Tracing route to google.com [142.250.80.110]
over a maximum of 30 hops:

  1    <1 ms     *       <1 ms  DCSERVER [[redacted].1]
  2     *        *        *     Request timed out.
  3    <1 ms    <1 ms    <1 ms  [redacted].2
  4     1 ms    <1 ms    <1 ms  Fios_Quantum_Gateway.fios-router.home [192.168.[redacted]
  5    14 ms     8 ms     8 ms  lo0-100.NYCMNY-VFTTP-378.verizon-gni.net [70.104.140.1]
  6     9 ms     9 ms    19 ms  B3378.NYCMNY-LCR-22.verizon-gni.net [100.41.216.110]
  7     *        *        *     Request timed out.
  8     8 ms     7 ms     8 ms  0.ae2.GW16.NYC1.ALTER.NET [140.222.227.151]
  9    11 ms    18 ms    17 ms  72.14.214.36
 10     8 ms     7 ms     9 ms  142.251.67.163
 11    11 ms     8 ms     7 ms  142.251.65.115
 12    13 ms    14 ms    12 ms  lga34s36-in-f14.1e100.net [142.250.80.110]

Trace complete.
```

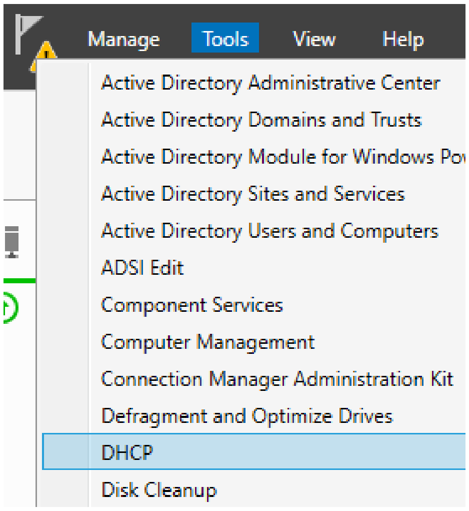
If there were any connection issues, then you would see some error like the Request timed out, but it would then commonly stop the connection from proceeding further beyond that hop. It's common to see one or two Request timed out errors but if the connection is not terminated there then it's not an issue that is blocking the connection.

Let's start with the domain controller and how we can troubleshoot it to solve potential connection issues. The machine running the domain controller itself will usually not have many problems related to connection issues. When these types of problems occur, its usually because of the DNS or DHCP servers. These often run on the domain controller.

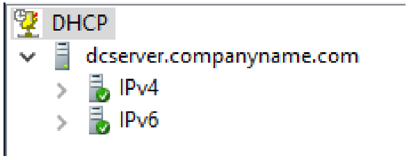
1. DHCP Server

Let's start with troubleshooting the DHCP server on the domain controller. The DHCP server is responsible for handing out IP addresses to machines on the network. Problems with the DHCP server might result in machines not being able to get a new IP address when they join the network or not being able to renew the lease on existing IP addresses.

To troubleshoot the DHCP server, open Server Manager on the domain controller and go to Tools -> DHCP.

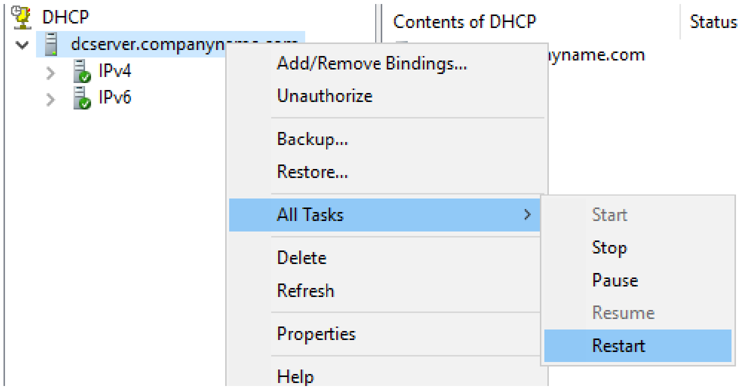

Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows Po
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
DHCP
Disk Cleanup

First look to see if the DHCP server is running. If everything is operating fine, then you will see a small green circle with a checkmark in it. If you don't see the green, then that might be an indicator that something is wrong, and you need to investigate more.

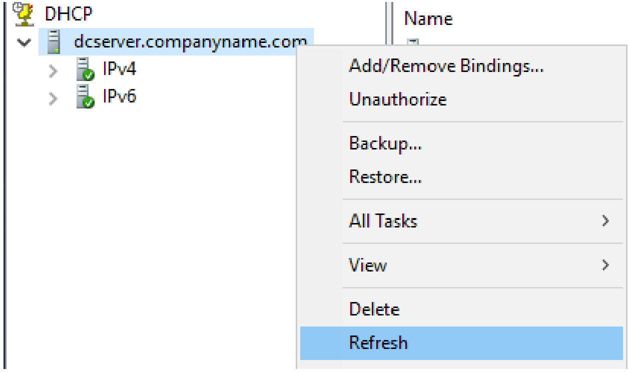


a. Restart Server

The fastest way to attempt to resolve issues with the DHCP server is to stop and then restart it. You do this by right clicking on the server's name and going to All Tasks, then selecting Restart.



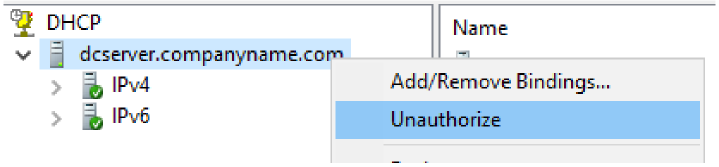
You may have to right click on the DHCP server and select refresh to see any updated changes.



b. Authorize Server

You should also check if the DHCP server is Authorized. DHCP servers which are joined to an active directory domain will typically continue to validate their authorization regularly. If a DHCP server fails to validate its authorization, then it will lose its ability to serve IP addresses.

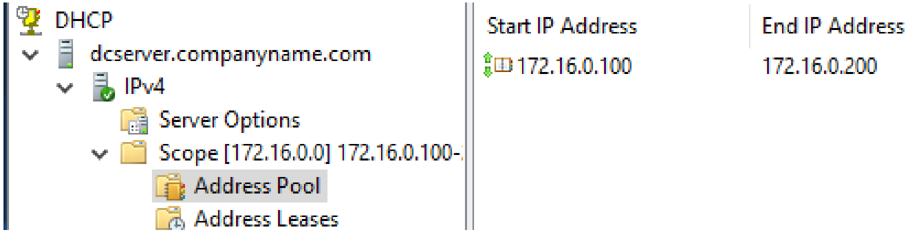
You can check if the DHCP server is authorized by right clicking on it and looking to see if there is an option to Unauthorize it. If the server was unauthorized, then there would be an option to authorize it only.



c. Verify IP Address Leases

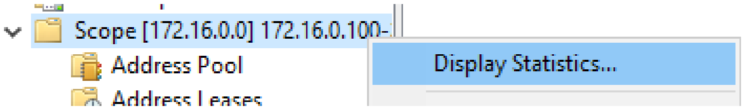
If the DHCP server is working properly then there might be an issue with the IP address leases being given out by the server. First check that the IP address ranges which the server is configured to give out is correct.

Navigate to IPv4 -> Scope -> Address Pool. Check all the available address pools and make sure that they are configured correctly.

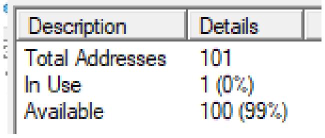


Start IP Address	End IP Address
172.16.0.100	172.16.0.200

Next check the Address Leases. If all of the available IP addresses are given out, then there might be too many machines on the network, and you will need to increase the size of the IP address pool. You can check this by right clicking on the scope and selecting Display Statistics.

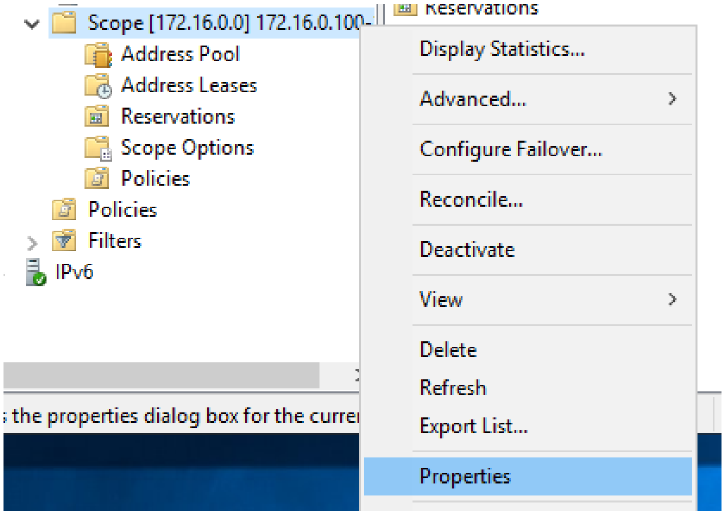


You will see the number of addresses being used and how many are available. If all addresses are being used, then you may need to increase the size of the scope.

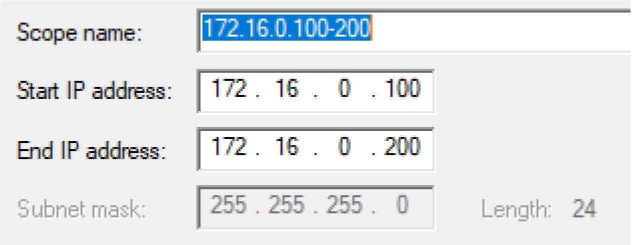


Description	Details
Total Addresses	101
In Use	1 (0%)
Available	100 (99%)

You can change the size of the scope by right clicking on the scope and selecting Properties.



You can now increase the size of the scope to accommodate a larger number of machines on your network.



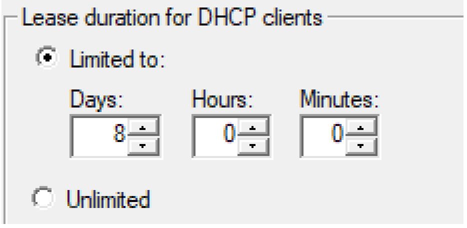
Scope name: 172.16.0.100-200

Start IP address: 172 . 16 . 0 . 100

End IP address: 172 . 16 . 0 . 200

Subnet mask: 255 . 255 . 255 . 0 Length: 24

You can also check the lease duration on this page. If they are too long, then it might take too long for the leases to be freed up and re-enter the pool again.



Lease duration for DHCP clients

● Limited to:

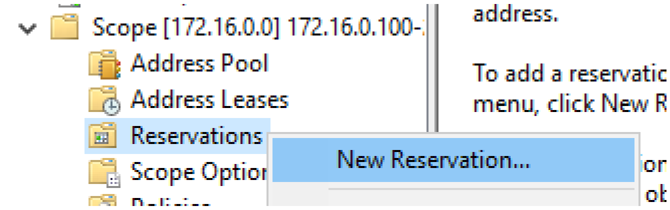
Days: 8 Hours: 0 Minutes: 0

○ Unlimited

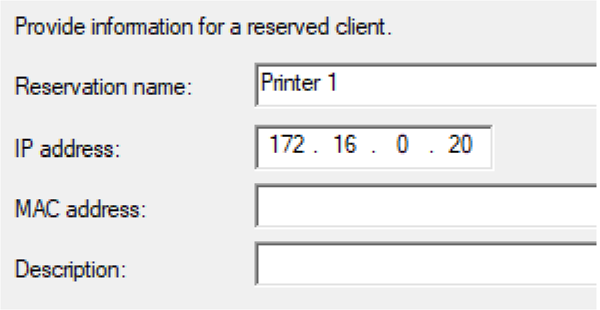
d. Static IP Addresses

You should also check if there are any devices on the network with a static IP address which have not been excluded from the DHCP scope. If a machine has a static IP address and it is not excluded from the scope, then another device might get assigned that IP address.

Create a reservation for a device by opening the scope and right clicking on Reservation. Select New Reservation.



You can then enter the IP address and the MAC address of the device to create the reservation.



Provide information for a reserved client.

Reservation name: Printer 1

IP address: 172 . 16 . 0 . 20

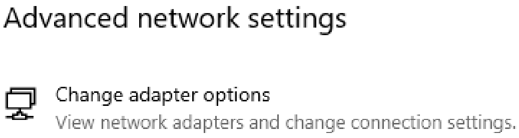
MAC address:

Description:

2. DHCP Client Machine Troubleshooting

If the DHCP server is working fine but there are still connectivity issues, then the problem is on the client side.

You can get more visibility on the client machine into what might be causing the issues by going to Settings -> network & Internet. Under Advanced Network Settings, select Change Sdapter Options.

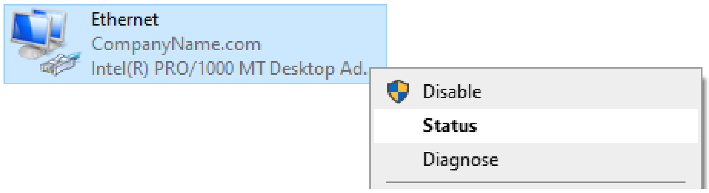


Advanced network settings

Change adapter options

View network adapters and change connection settings.

This will bring up the network adapters for the client machine. Right click on the adapter and select Status.

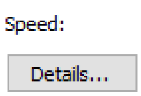


Ethernet

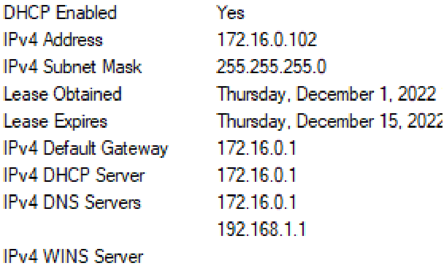
CompanyName.com

Intel(R) PRO/1000 MT Desktop Ad.

Select Details

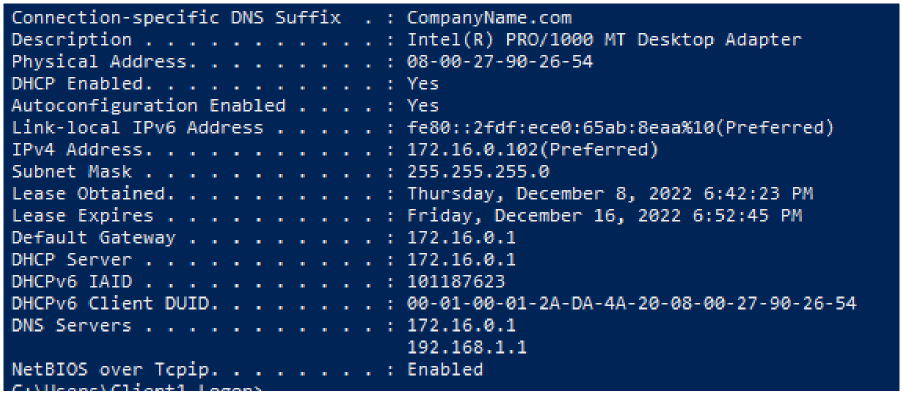


You can now see details about the network adapter on the client machine.



DHCP Enabled	Yes
IPv4 Address	172.16.0.102
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Thursday, December 1, 2022
Lease Expires	Thursday, December 15, 2022
IPv4 Default Gateway	172.16.0.1
IPv4 DHCP Server	172.16.0.1
IPv4 DNS Servers	172.16.0.1 192.168.1.1
IPv4 WINS Server	

You can also quickly view the same information by going into PowerShell and typing “ipconfig /all”.

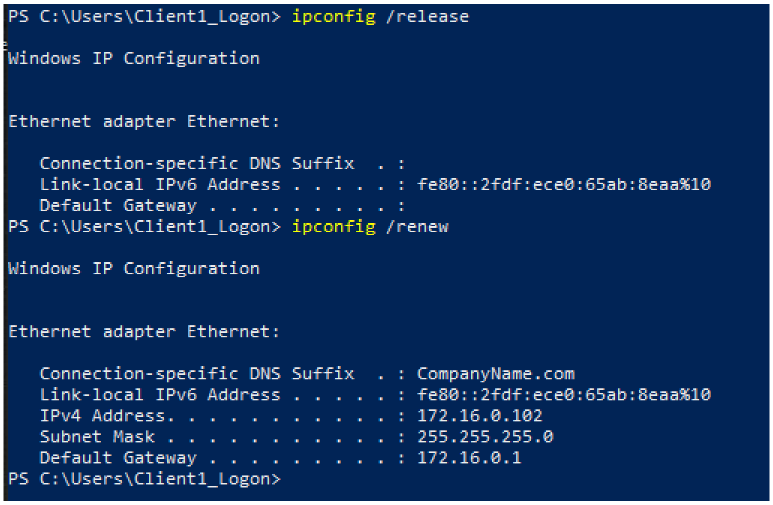


```
Connection-specific DNS Suffix  . : CompanyName.com
Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . . . . . : 08-00-27-90-26-54
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10(Preferred)
IPv4 Address. . . . . . . . . . . : 172.16.0.102(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Thursday, December 8, 2022 6:42:23 PM
Lease Expires . . . . . . . . . . : Friday, December 16, 2022 6:52:45 PM
Default Gateway . . . . . . . . . : 172.16.0.1
DHCP Server . . . . . . . . . . . : 172.16.0.1
DHCPv6 IAID . . . . . . . . . . . : 101187623
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-DA-4A-20-08-00-27-90-26-54
DNS Servers . . . . . . . . . . . : 172.16.0.1
                                    192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
C:\Users\Client1_Logon>
```

a. **Automatic Private IP Address**

If you see an IPv4 address within the range of 169.254.0.1 to 169.254.255.254, then that is a sign that the machine was given an automatic private IP address. If a machine powers on and can’t contact the DHCP server, then it will automatically give itself an IP address. This will be a private IP address which the machine will not be able to use to connect to the internet.

To fix this issue, you will have to release that IP address and request a new one from the DHCP server. To do this, open PowerShell and type in “ipconfig /release” to release the current IP address. Then type “ipconfig / renew” to request a new IP address from the DHCP server.

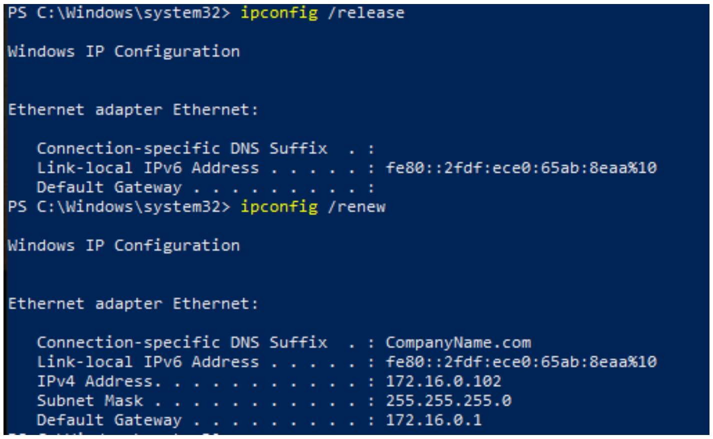


```
PS C:\Users\Client1_Logon> ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10
   Default Gateway . . . . . . . . . :
PS C:\Users\Client1_Logon> ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : CompanyName.com
   Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10
   IPv4 Address. . . . . . . . . . . : 172.16.0.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.0.1
PS C:\Users\Client1_Logon>
```

b. **Expired IP Address Lease**

You can also see when the IP address lease was obtained and when it will expire when you check the status of the network adapter. Sometimes a machine will think the IP it has is not expired even though it is. This can happen when a user leaves for vacation and leaves their machine on sleep or hibernate mode. When the user comes back from vacation and tries to start their machine, it will think no time has passed and the lease is still valid.

The fix for this issue is the same as we just used before. Open PowerShell and type in “ipconfig /release” to release the current IP address. Then type “ipconfig / renew” to request a new IP address from the DHCP server. If successful you will get a new IP address and a new lease which is accurate.

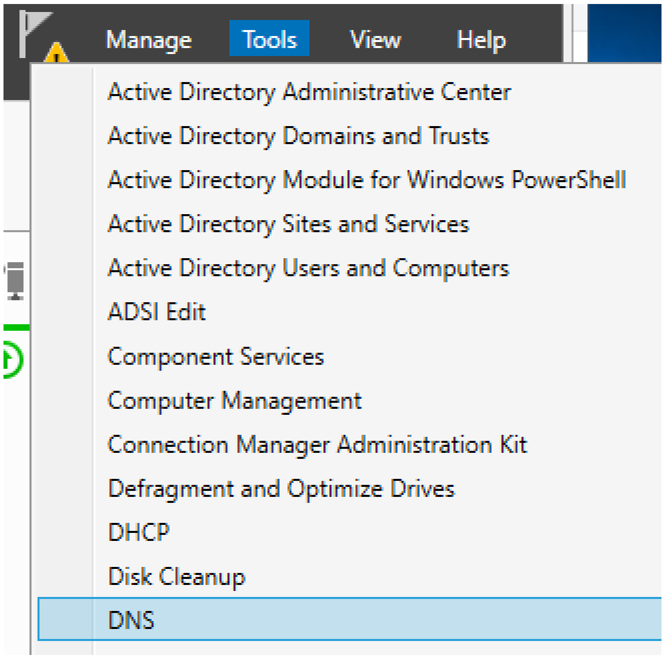


```
PS C:\Windows\system32> ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10
   Default Gateway . . . . . . . . . :
PS C:\Windows\system32> ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : CompanyName.com
   Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10
   IPv4 Address. . . . . . . . . . . : 172.16.0.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.0.1
```

3. DNS Server

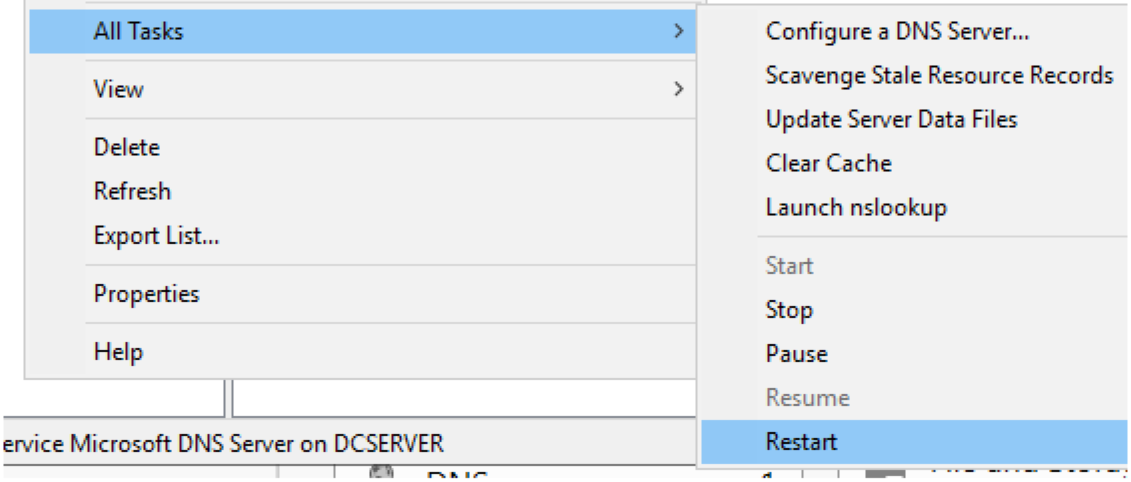
Next let’s troubleshoot DNS server related issues on the domain controller. The DNS server is responsible for name resolution on the network. You can still directly access machines using their IP addresses but that is not human readable. IP addresses can also change so that will make it difficult to communicate with other machines on the network. You will also not be able to navigate to websites using their domain name.

To start troubleshooting the DNS server, open Server manager on the domain controller and go to Tools -> DNS.


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS

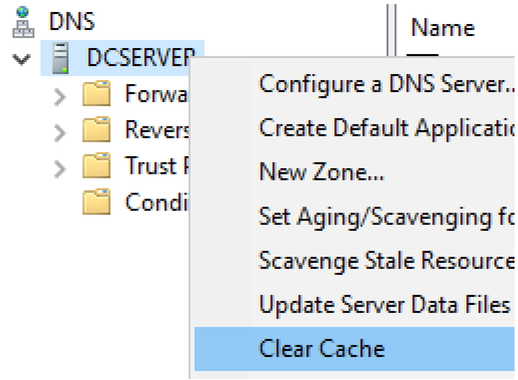
a. **Restart DNS Server**

The quickest way to attempt to solve DNS server related issues is to restart the DNS server. In DNS Manager, right click on the server and select All Tasks -> Restart.

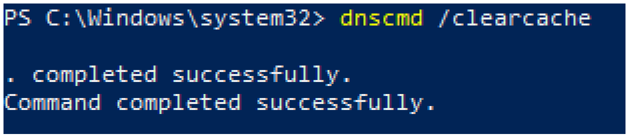


b. **Clear DNS Server Cache**

You can also then try to clear the DNS server cache. In DNS Manager, right click on the DNS server and select Clear Cache.



You can also user PowerShell to perform the same task by using the command "dnscmd /clearcache".



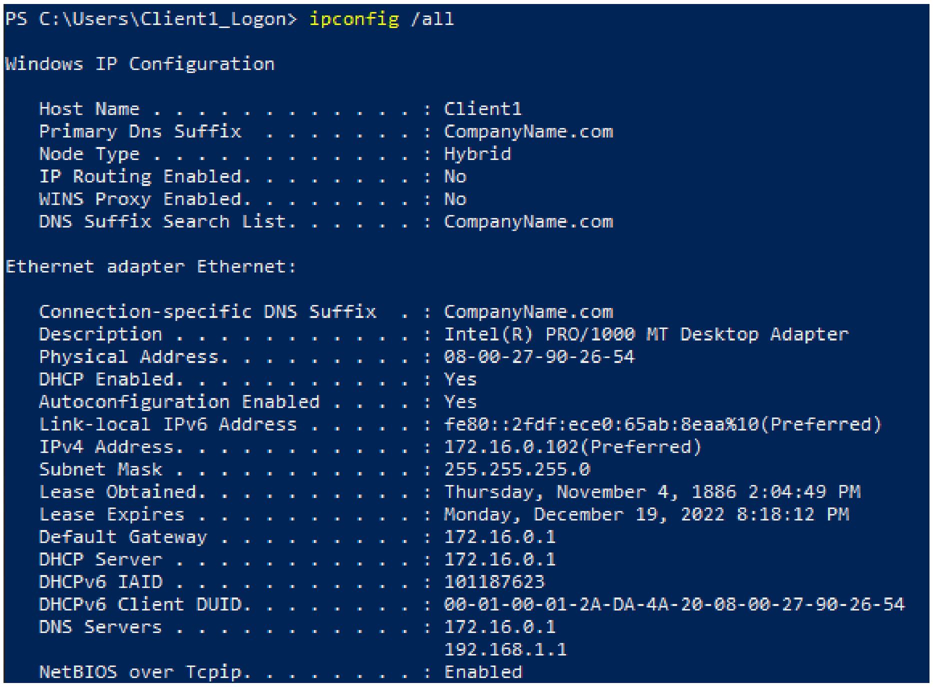
```
PS C:\Windows\system32> dnscmd /clearcache

. completed successfully.
Command completed successfully.
```

4. DNS Client Troubleshooting

If the cause of the connectivity issues is not the DNS server, then it is possibly a problem on the client side.

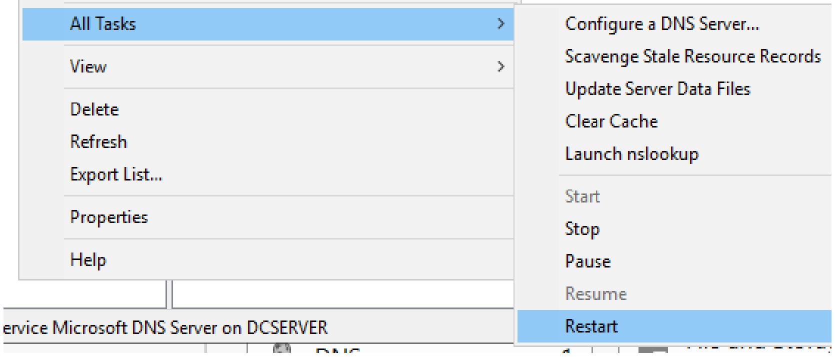
a. **Check DNS Server IP Configuration**

The first step to troubleshooting DNS issues on a client machine is to check the DNS configuration. You can do this by opening PowerShell and entering the command “ipconfig /all”. You are looking to see if the IP addresses of the DNS servers are correct.

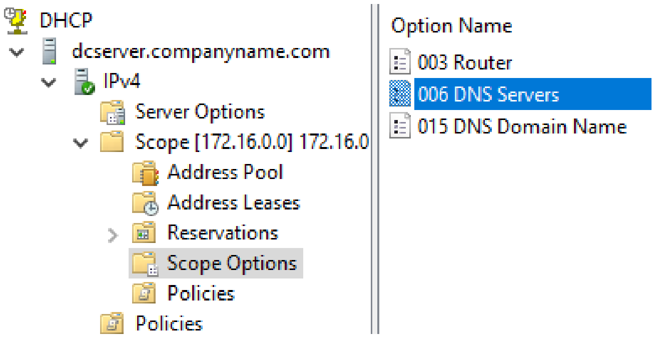


```
PS C:\Users\Client1_Logon> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Client1
   Primary Dns Suffix  . . . . . . . : CompanyName.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : CompanyName.com

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : CompanyName.com
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-90-26-54
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.0.102(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, November 4, 1886 2:04:49 PM
   Lease Expires . . . . . . . . . . : Monday, December 19, 2022 8:18:12 PM
   Default Gateway . . . . . . . . . : 172.16.0.1
   DHCP Server . . . . . . . . . . . : 172.16.0.1
   DHCPv6 IAID . . . . . . . . . . . : 101187623
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-DA-4A-20-08-00-27-90-26-54
   DNS Servers . . . . . . . . . . . : 172.16.0.1
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

If there is no IP address for the DNS servers, then there may be an issue contacting the DNS server. You can attempt to fix this by going to the domain controller and restarting the DNS server. Do this by opening Server Manager and go to Tools -> DNS. Then right click on the DNS server and go to All Tasks and select Restart.



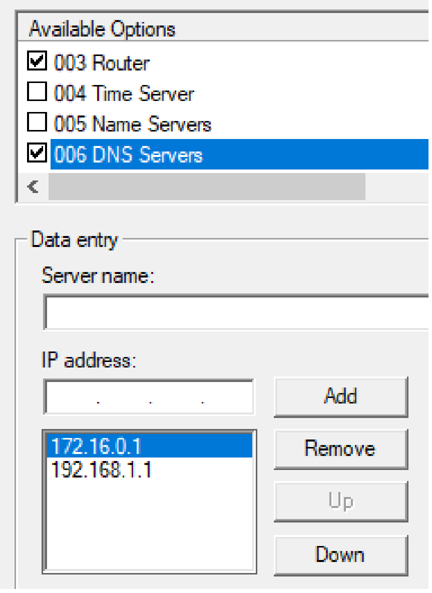
If the IP address of the DNS server is incorrect, then you can change it in two places. The first way is to open Server Manager on the domain controller. Then go to Tools -> DHCP. Go to IPV4 -> Scope -> Scope Options. You will see an option for DNS Servers. Select it.



DHCP
dcserver.companyname.com
IPv4
Server Options
Scope [172.16.0.0] 172.16.0
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies

Option Name
003 Router
006 DNS Servers
015 DNS Domain Name

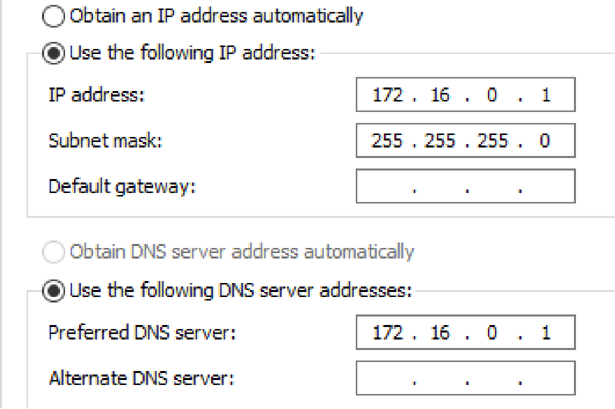
Select the option 006 DNS Servers. Now you will have the option to enter the correct IP address of the DNS server. If there are multiple DNS Servers, then you can also change the order of them so that the preferred one will be reached first.



Available Options
☑ 003 Router
□ 004 Time Server
□ 005 Name Servers
☑ 006 DNS Servers

Data entry
Server name:
IP address:
172.16.0.1
192.168.1.1

The second way to change the DNS server IP address is to go to settings -> Network & Internet -> Change Adapter Options. Right click on the network adapter and select Properties. Then select Internet Protocol Version 4, then click Properties. You can now change the DNS server IP address to the correct one.

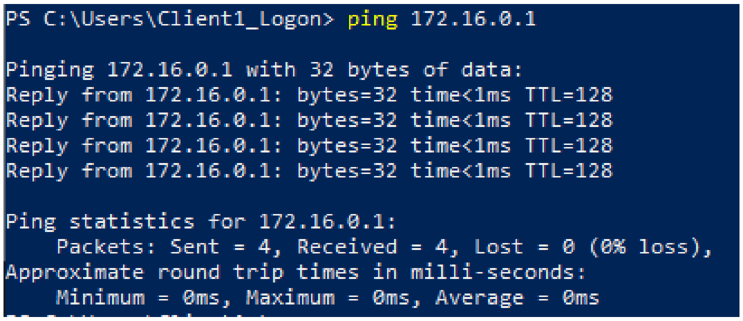


○ Obtain an IP address automatically
● Use the following IP address:
IP address: 172 . 16 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 172 . 16 . 0 . 1
Alternate DNS server: . . .

b. Verify DNS Server IP

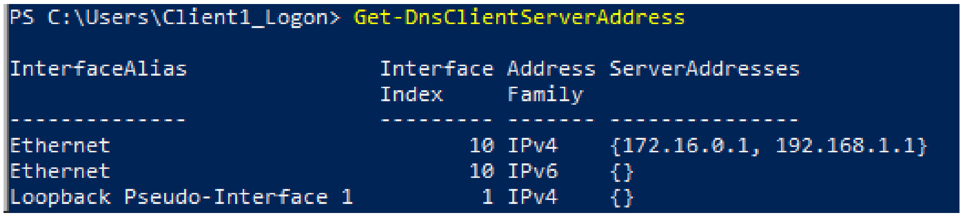
Now that you have checked that the DNS servers are configured with the correct IP addresses, you can now start troubleshooting the connection. Start by trying to ping the DNS servers to double check that the client can reach them. In PowerShell, enter the command ping followed by the IP address of the DNS server.



```
PS C:\Users\Client1_Logon> ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If you cannot reach the DNS server from the client, then you will have to double check that the DNS server is configured properly and is running. You may have to restart the client machine and check the connections and cables.

Another way to verify the DNS server's IP address is to use the command "Get-DnsClientServerAddress". This will Display the network adapters on the machine and the IP addresses of the DNS servers associated with those adapters.

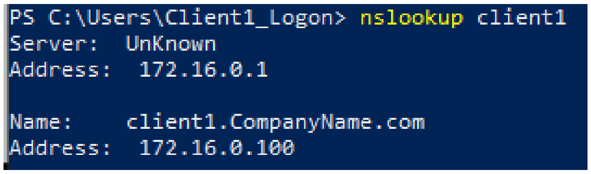


```
PS C:\Users\Client1_Logon> Get-DnsClientServerAddress

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
--------------               --------- ------- ---------------
Ethernet                            10 IPv4    {172.16.0.1, 192.168.1.1}
Ethernet                            10 IPv6    {}
Loopback Pseudo-Interface 1          1 IPv4    {}
```

c. Verify DNS Server Will Respond Correctly

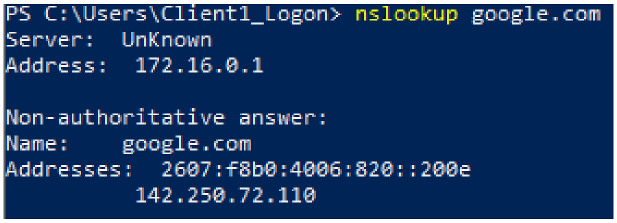
Now that you can ping the DNS server and confirmed that there is a connection between it and the Client machine, you can now test if the DNS server will respond correctly to requests. You can do this by using the nslookup command. It uses the server's DNS cache instead of the client's DNS cache. This will let you know if the server has the correct records. This can also be helpful to verify if the DNS server in which the client machine is pulling the DNS records from is the local DNS server verses one which is outside of the network. The local DNS server will be able to resolve the names of machines on your network. A public DNS server will not be able to.

Query the DNS server by using the nslookup command followed by the name of a machine on your network. Preferably the client machine with connectivity issues.



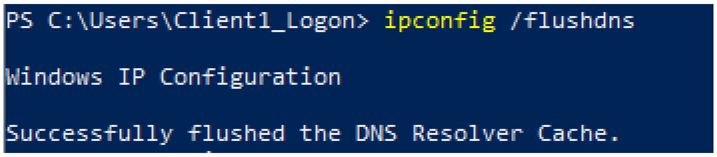
```
PS C:\Users\Client1_Logon> nslookup client1
Server:  UnKnown
Address:  172.16.0.1

Name:    client1.CompanyName.com
Address:  172.16.0.100
```

Next, test a well-known public website like google.com. If you can resolve a well-known public website but not a machine on your local network, then you might be connecting to a public DNS server instead of one on your local network. You will have to double check that you configured your DNS server correctly.



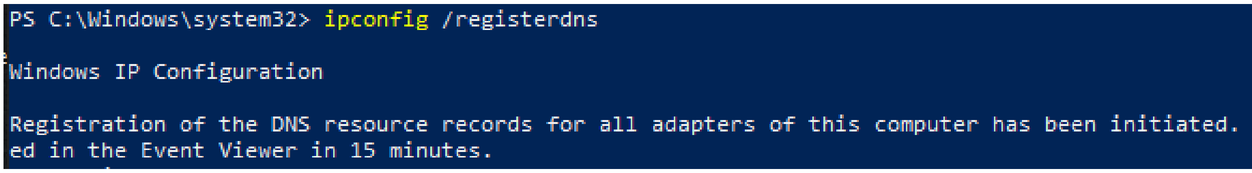
```
PS C:\Users\Client1_Logon> nslookup google.com
Server:  UnKnown
Address:  172.16.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4006:820::200e
          142.250.72.110
```

If you still can't resolve the name of the client machine, then there might be an issue with the records on the DNS server. You can try to fix this issue by clearing the DNS resolver cache on the Client machine. Use the command "ipconfig /flushdns" to do so.



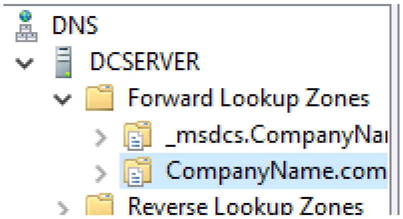
```
PS C:\Users\Client1_Logon> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

After you clear the resolver cache, you can also try to make sure the DNS record for the client machine is registered with the DNS server. Do this by using the command "ipconfig / registerdns".

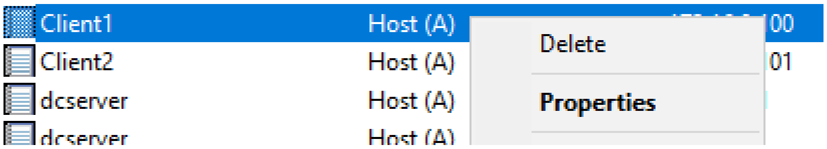


```
PS C:\Windows\system32> ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated.
ed in the Event Viewer in 15 minutes.
```

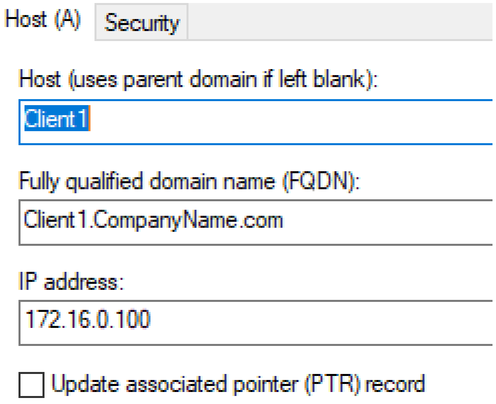
You can also manually look at the DNS records yourself by going to the domain controller and opening Server Manager. Then go to Tools ->DNS. Click on the DNS server and open Forward Lookup Zones. Then find your organization domain name and click on that. This will bring up the list of all DNS records on the server.



You can then delete or edit these records. Right click on a record and select Properties to edit it.



You can change the host name of the record and the IP address associated with that host name.



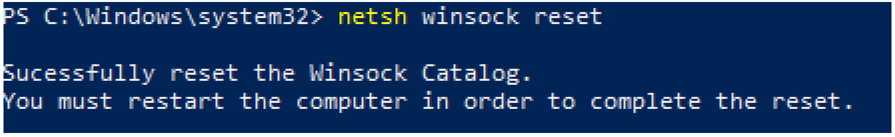
Host (uses parent domain if left blank):
Client1

Fully qualified domain name (FQDN):
Client1.CompanyName.com

IP address:
172.16.0.100

□ Update associated pointer (PTR) record

You can also try resetting the winsock catalog back to its default settings. First open PowerShell with Admin privileges. Enter the command “netsh winsock reset” and press enter to execute it. You can now restart the machine to complete the process.



```
PS C:\Windows\system32> netsh winsock reset

Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
```

Router / Default Gateway

With our client machine and domain controller confirmed to be working fine. Let’s look at the next hop in the path out of the network. It is the default gateway. On all networks, you will have to eventually go through the default gateway before you exit the network. The default gateway is often also the router. A router is typically thought as the hardware provided by an ISP which is in most residential homes. In an office setting, any machine which does routing can be considered a router. On many networks the machine which runs the domain controller will also serve as the DNS server, DHCP server, default gateway and the router.

For this lab, the router will be a machine which is configured to be the default gateway and performs the routing for the network. Since it is a machine, the solutions to troubleshooting any other machine will also apply here also. Let’s go through the steps of troubleshooting this machine.

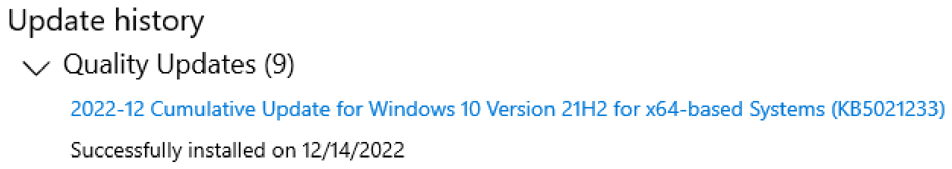
1. **Check Cables and Connections**
   First check all cables and connections to the machine to make sure everything is plugged in properly. Check if the ethernet port is plugged in properly. See if the LED light on the ethernet port comes on when you move the cable around. That might be a sign of a bad cable or port.

2. **Restart Machine**
   If the machine has been running for a long time, then closing all programs and performing a restart might help fix the issue.

3. Check For Recent Updates

You should also check to see if there were any updates within the last day or two which were recently installed on the machine. If so, then that might be the cause of the connectivity issues.

Check for the latest updates by going to Settings -> Update and Security. Then click on View Update History. You will see the latest updates and the dates in which they were install on.



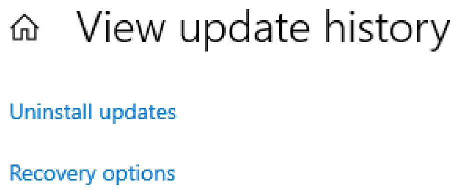
Update history

Quality Updates (9)

2022-12 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5021233)

Successfully installed on 12/14/2022

You can uninstall an update by clicking the Uninstall Updates button on the upper left. You can then click on the last update and click the Uninstall button to start the uninstallation process.



View update history

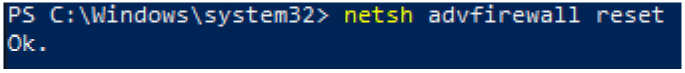
Uninstall updates

Recovery options

4. Turn Off Antivirus and Firewall

A trigger-happy antivirus or firewall might block the connection for a machine if it sees activity which might be suspicious. You can test if the antivirus or firewall is blocking the connection by temporarily turning them off to see if that has an effect on the connectivity issues.

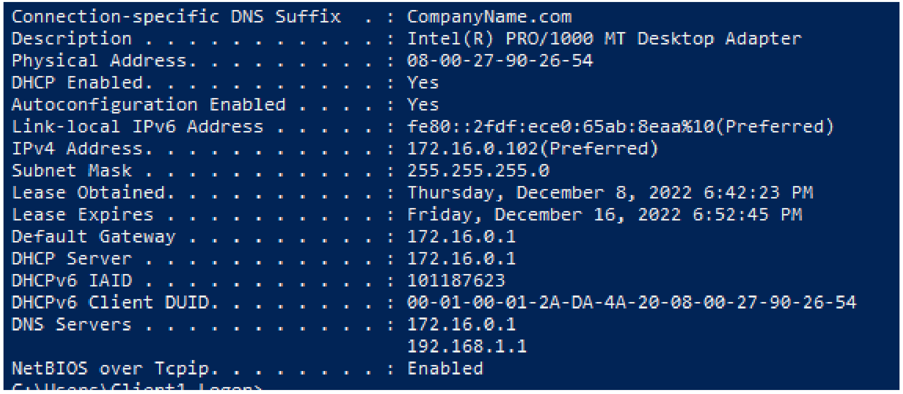
If you believe that a firewall rule may be the cause of the network connectivity issues but can't identity which one it is, then you can reset the firewall rules back to their default settings. You can do this by using the command "netsh advfirewall reset".



```
PS C:\Windows\system32> netsh advfirewall reset
Ok.
```

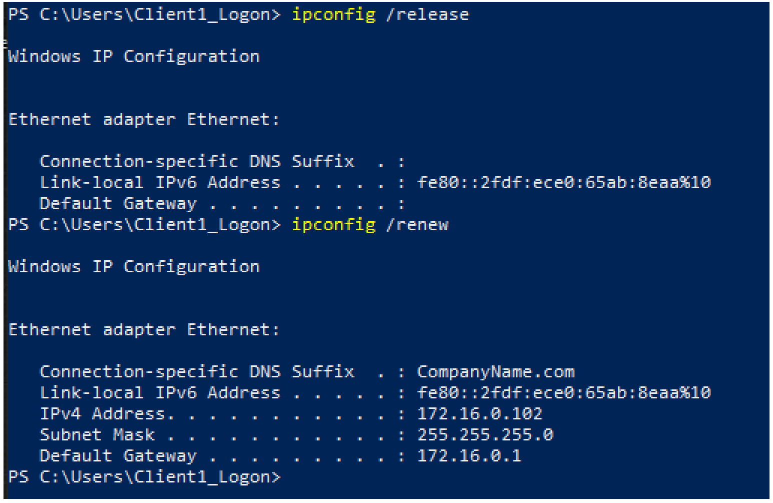
5. Check IP Configuration

You should also check that the machine has received an IP address from the DHCP server. You can quickly view the network connectivity information by going into PowerShell and typing "ipconfig /all". If there is no IP address, then you may have to go through the DHCP troubleshooting steps we did earlier.



```
Connection-specific DNS Suffix  . : CompanyName.com
Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . . . . . : 08-00-27-90-26-54
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10(Preferred)
IPv4 Address. . . . . . . . . . . : 172.16.0.102(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Thursday, December 8, 2022 6:42:23 PM
Lease Expires . . . . . . . . . . : Friday, December 16, 2022 6:52:45 PM
Default Gateway . . . . . . . . . : 172.16.0.1
DHCP Server . . . . . . . . . . . : 172.16.0.1
DHCPv6 IAID . . . . . . . . . . . : 101187623
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-DA-4A-20-08-00-27-90-26-54
DNS Servers . . . . . . . . . . . : 172.16.0.1
                                    192.168.1.1
NetBIOS over Tcpip. . . . . . . . : Enabled
C:\Users\Client1.Logon>
```

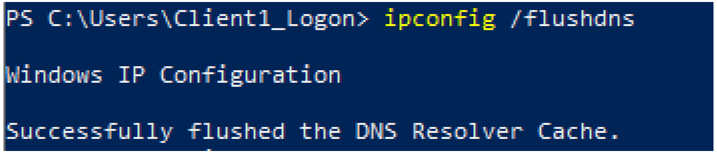
If there is an issue with the IP address, then you can try to release and then request a new IP address. To do this, open PowerShell and type in “ipconfig /release” to release the current IP address. Then type “ipconfig / renew” to request a new IP address from the DHCP server.



```
PS C:\Users\Client1_Logon> ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10
   Default Gateway . . . . . . . . . :
PS C:\Users\Client1_Logon> ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : CompanyName.com
   Link-local IPv6 Address . . . . . : fe80::2fdf:ece0:65ab:8eaa%10
   IPv4 Address. . . . . . . . . . . : 172.16.0.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.0.1
PS C:\Users\Client1_Logon>
```

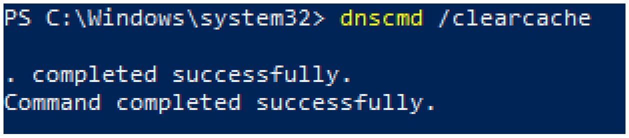
6. **Check DNS Settings and Configuration**

   You can also check the DNS server configuration when using the “ipconfig /all” command. If the DNS server has the right IP address, then you can try to clear the DNS cache using the command “ipconfig /flushdns” to see if that resolves the connectivity issues.



```
PS C:\Users\Client1_Logon> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

   You can also try to clear the DNS cache on the DNS server by using the command “dnscmd /clearcache”.

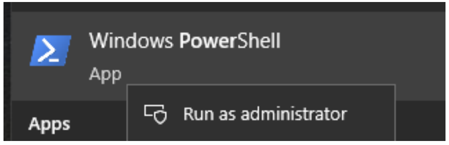


```
PS C:\Windows\system32> dnscmd /clearcache

. completed successfully.
Command completed successfully.
```

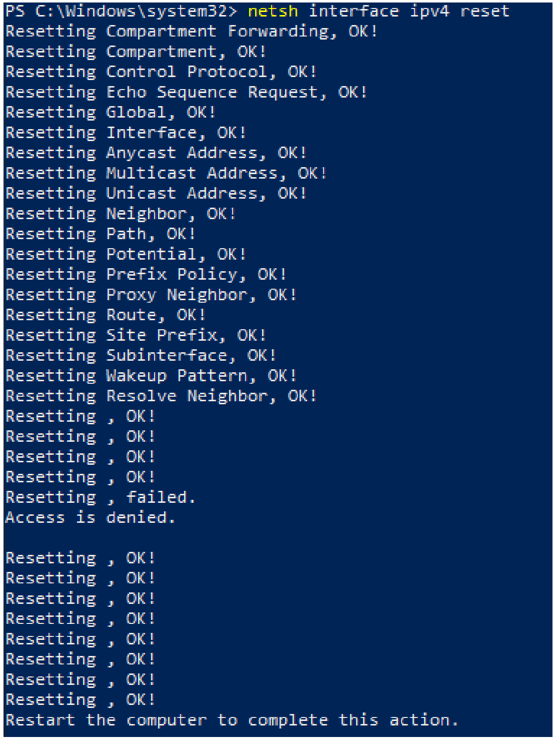
7. **Reset TCP/IP Stack**

   One way to fix issues with the default gateway is to reset the TCP/IP stack. This will reset those settings back to default. This can help resolve misconfigured IP settings. You may have to reconfigure the network settings on the machine to get it working again after this.

   To do this, open PowerShell with administrator privileges.



Enter the command “netsh interface ipv4 reset”. You can also enter the command “netsh interface ipv6 reset” if your network uses IPV6. Restart the machine to see if the changes fixed the network connectivity issues.

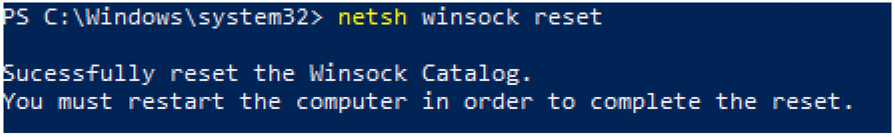


```
PS C:\Windows\system32> netsh interface ipv4 reset
Resetting Compartment Forwarding, OK!
Resetting Compartment, OK!
Resetting Control Protocol, OK!
Resetting Echo Sequence Request, OK!
Resetting Global, OK!
Resetting Interface, OK!
Resetting Anycast Address, OK!
Resetting Multicast Address, OK!
Resetting Unicast Address, OK!
Resetting Neighbor, OK!
Resetting Path, OK!
Resetting Potential, OK!
Resetting Prefix Policy, OK!
Resetting Proxy Neighbor, OK!
Resetting Route, OK!
Resetting Site Prefix, OK!
Resetting Subinterface, OK!
Resetting Wakeup Pattern, OK!
Resetting Resolve Neighbor, OK!
Resetting , OK!
Resetting , OK!
Resetting , OK!
Resetting , OK!
Resetting , failed.
Access is denied.

Resetting , OK!
Resetting , OK!
Resetting , OK!
Resetting , OK!
Resetting , OK!
Resetting , OK!
Resetting , OK!
Resetting , OK!
Restart the computer to complete this action.
```

8. **Reset Winsock**

   If resetting the TCP/IP configurations does not fix the issue, then you can try to also reset the winsock catalog.

   First open PowerShell with Admin privileges. Enter the command “netsh winsock reset” and press enter to execute it. You can now restart the machine to complete the process.



```
PS C:\Windows\system32> netsh winsock reset

Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
```

9. **Reset Network**

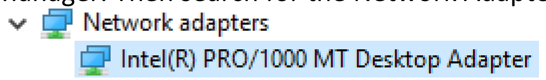
   A quick way to reset a machines network settings is to use the Network Reset feature. This will reset all network related settings back to their defaults. This will also uninstall and reinstall the network adapters on the machine. You will have to restart your machine and reconfigure the network settings on the machine after preforming the Network Reset.

   Go to settings -> Network & Internet. Scroll down and click Network Reset.

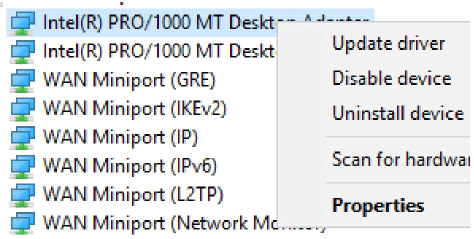
   Click the Reset now button to start the process. Restart the machine to complete the process.

10. **Check Network Driver Power Settings**
    If the machine is turning off the network adapters to save power, then that can cause network connectivity issues. It can cause intermittent network connectivity issues or even complete loss of connectivity if it is unable to reconnect to the network when the adapters are eventually turned back on.

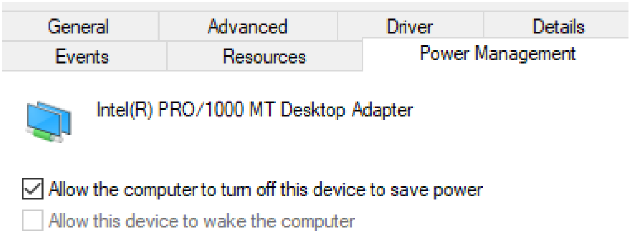
    You can change the power management settings for the network adapters by going to Device Manager. Then search for the Network Adapters category.



Right click on the network adapter and select Properties.



Go to the Power Management tab and uncheck Allow the computer to turn off this device to save power. Then click ok.



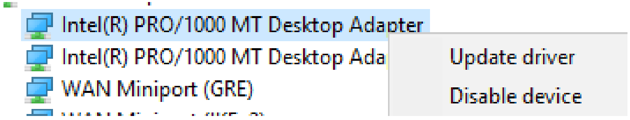
☑ Allow the computer to turn off this device to save power

☐ Allow this device to wake the computer

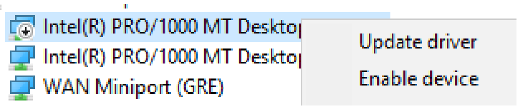
You may have to restart the machine or attempt to reconnect to the network to allow the changes to take effect.

11. **Disable Then Re-Enable Network Adapters**
    You can also troubleshoot the network adapters by turning them off and then on again to see if that resolves the connectivity issues.

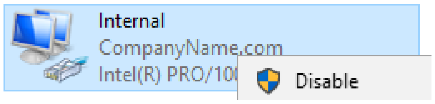
    You can open Device Manager and navigate to the Network Adapters category. Right click on the adapter and select Disable Device.


Intel(R) PRO/1000 MT Desktop Adapter
Intel(R) PRO/1000 MT Desktop Ada
WAN Miniport (GRE)
Update driver
Disable device

Wait one to two minutes and then right click the adapter and select Enable Device.

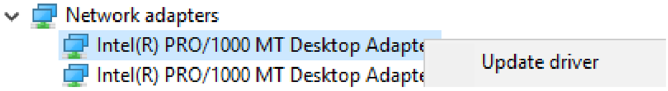


You can also perform the same action by going to Settings -> Network & Internet. Then select Change Adapter Options. You can now right-click on the adapter and select Disable. Wait for one to two minutes, then right-click on the adapter again and select Enable.

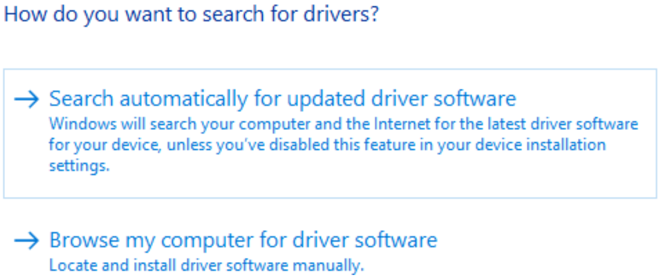


12. Update Network Adapter Drivers

Outdated drivers can also be the cause of network connectivity issues. You can update the network drivers by opening Device Manager and opening the Network Adapters category. Right click on the adapter you want to update and select Update Driver.


Network adapters
Intel(R) PRO/1000 MT Desktop Adapte
Intel(R) PRO/1000 MT Desktop Adapte
Update driver

For the lab, we will go with the option of “Search automatically for updated driver software”. This will automatically search for the drivers for your system. If it can’t find the drivers automatically, then you will have to search online to find the latest network drivers for your machine. Then you can select “Browse my computer for driver software”. You can then navigate to where you saved the driver update.


How do you want to search for drivers?

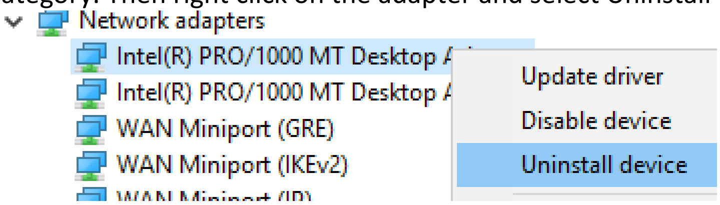
→ Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

→ Browse my computer for driver software
Locate and install driver software manually.

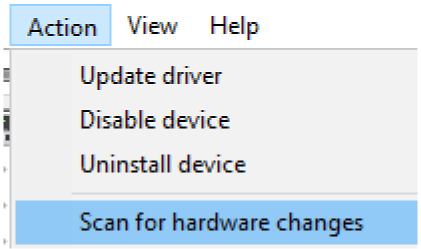
a. Uninstall Then Reinstall Network Drivers

If your system is already running the latest network adapter drivers, then you can try to uninstall the drivers and reinstall them. You will have to first find the manufactures website and find the download for the driver.

To uninstall the driver, go to Device Manager. Navigate to the Network Adapters category. Then right click on the adapter and select Uninstall Device.



If you go to Action and select Scan for Hardware Changes. The system will automatically reinstall the driver from the file it has on the system. You may also have to restart your system for this to take effect. If it does not find an existing driver file to use, then there will be a small yellow triangle next to the adapter. The name might also change to a generic adapter name.

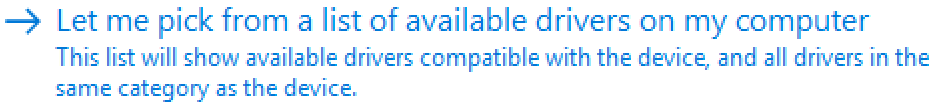


You can install the driver file you downloaded from the manufactures website by right clicking on that adapter and select Update Driver. Then you can select “Browse my computer for driver software”. You can then navigate to where you saved the driver file. Follow the steps and complete the installation.

b. Change Network Adapter Drivers to Generic

If you suspect the connectivity issues are caused by the drivers but you can’t find updated drivers to download; you can try to use other drivers which have been installed on the machine already.

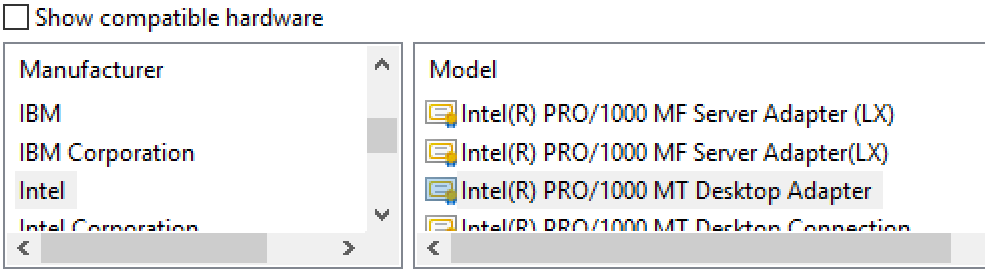
In Device Manager, right click on the network adapter driver and select Update Driver. Select “Browse my computer for driver software”. Then select “Let me pick from a list of available drivers”. This will show the available drivers which are compatible.



→ Let me pick from a list of available drivers on my computer

This list will show available drivers compatible with the device, and all drivers in the same category as the device.

If you don’t want to use any of those drivers, then you can also uncheck the “Show compatible hardware box”. You can then browse and select the drivers you want to use based on manufacture and then model. Once you made your selection, you can click next to install that driver.

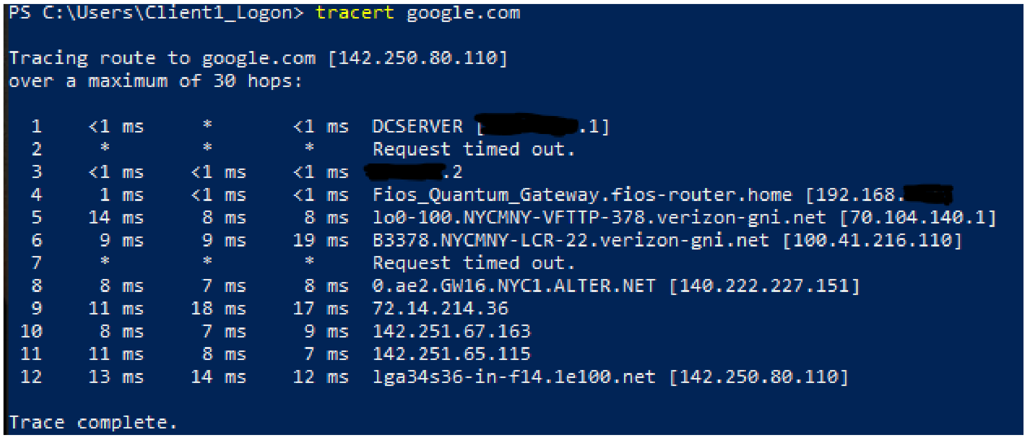


☐ Show compatible hardware

Manufacturer	Model
IBM	Intel(R) PRO/1000 MF Server Adapter (LX)
IBM Corporation	Intel(R) PRO/1000 MF Server Adapter(LX)
Intel	Intel(R) PRO/1000 MT Desktop Adapter
Intel Corporation	Intel(R) PRO/1000 MT Desktop Connection

ISP Network

Once a packet is past your default gateway, it is out of your network. The packet will now travel through your ISP’s network. If you use the tracert command and see that the packets stop progressing at one of the ISP’s routers, then that’s a sign that there might be an issue with your ISP. The only way to fix connection problems that arise from your ISP is to call them and have them fix the issue on their end.



```
PS C:\Users\Client1_Logon> tracert google.com

Tracing route to google.com [142.250.80.110]
over a maximum of 30 hops:

  1    <1 ms     *       <1 ms  DCSERVER [[redacted].1]
  2     *        *        *     Request timed out.
  3    <1 ms    <1 ms    <1 ms  [redacted].2
  4     1 ms    <1 ms    <1 ms  Fios_Quantum_Gateway.fios-router.home [192.168.[redacted]
  5    14 ms     8 ms     8 ms  lo0-100.NYCMNY-VFTTP-378.verizon-gni.net [70.104.140.1]
  6     9 ms     9 ms    19 ms  B3378.NYCMNY-LCR-22.verizon-gni.net [100.41.216.110]
  7     *        *        *     Request timed out.
  8     8 ms     7 ms     8 ms  0.ae2.GW16.NYC1.ALTER.NET [140.222.227.151]
  9    11 ms    18 ms    17 ms  72.14.214.36
 10     8 ms     7 ms     9 ms  142.251.67.163
 11    11 ms     8 ms     7 ms  142.251.65.115
 12    13 ms    14 ms    12 ms  lga34s36-in-f14.1e100.net [142.250.80.110]

Trace complete.
```

Website Is Down

If the packet made it through your ISP’s network, then the problem might be with the website you are trying to reach. If you use the tracert command and see “Request timed out” for the target website’s servers, then the issue might just be with that website’s servers. You can quickly test this by navigating to another well-known website.

Conclusion

For this lab we used the tracert command to trace the path of a packet from a client machine, all the way to a well-known website. We then looked at each hop the packet took. For each type of machine on the network, we stepped through the process of troubleshooting those machines. This gave us a better understanding of the different types of machines on the network and the roles they played in facilitating a network connection.

Source:
Firewall ports
https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-outbound-port-rulev
https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/open-the-group-policy-management-console-to-windows-firewall-with-advanced-security

firewall and antivirus
https://windowsreport.com/antivirus-blocking-internet-wifi/

NIC Troubleshooting
https://community.fs.com/blog/troubleshoot-network-adapter-problems-in-windows.html
https://superuser.com/questions/728239/how-can-i-diagnose-suspected-nic-issues
https://www.dell.com/support/kbdoc/en-us/000179426/how-to-troubleshoot-and-resolve-any-wired-nic-issues-with-a-desktop-pc

restore system
https://support.microsoft.com/en-us/windows/recovery-options-in-windows-31ce2444-7de3-818c-d626-e3b5a3024da5#bkmk_use_installation_media_restore
setup and restore backups and images
https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c

backup guide

https://www.youtube.com/watch?v=mOyQAJqeZ48

windows backup video.

booth from known good drive
https://www.dell.com/support/kbdoc/en-us/000179426/how-to-troubleshoot-and-resolve-any-wired-nic-issues-with-a-desktop-pc

restore system to known good state
https://support.microsoft.com/en-us/windows/recovery-options-in-windows-31ce2444-7de3-818c-d626-e3b5a3024da5

troubleshooting network adapters
https://helpdeskgeek.com/networking/network-adapter-not-working-12-things-to-try/

troubleshoot DHCP server
https://learn.microsoft.com/en-us/windows-server/troubleshoot/troubleshoot-problems-on-dhcp-server

troubleshoot dhcp client
https://learn.microsoft.com/en-us/windows-server/troubleshoot/troubleshoot-problems-on-dhcp-client
troubleshoot DHCP
https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/troubleshoot-dhcp-guidance?source=recommendations

troubleshoot DNS
https://www.youtube.com/watch?v=_avtpeF9NPg
https://learn.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/troubleshoot-dns-client
https://learn.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/troubleshoot-dns-server
https://techgenix.com/10-ways-troubleshoot-dns-resolution-issues/

https://petri.com/an-active-directory-domain-controller-could-not-be-contacted/
https://phoenixnap.com/kb/dns-troubleshooting
https://www.hp.com/us-en/shop/tech-takes/how-to-resolve-dns-issues

https://www.oreilly.com/library/view/active-directory-cookbook/0596004648/ch13s12.html

fix default gateway
https://windowsreport.com/default-gateway-not-available-windows-10/
https://adamtheautomator.com/netsh-winsock-reset/

use netsh command
https://adamtheautomator.com/netsh/