How to Read the Network Utility Tool Results

The Network Utility provides a snapshot of network settings and diagnostic results. While the test is comprehensive some network settings that affect phone service may not be captured in the test. In the event of issues occurring that are likely related to network configuration, the firewall configuration may still need to be reviewed despite passing the Network Utility test.

Objective

To understand how to read and interpret Network Utility results. Results come from running the Network Utility Tool.

Applies To

• Networking

Procedure

Network Utility Results have the following categories:

• DNS Testing
• Ping Test
• NAT
• Outbound Connectivity
• System Info
• ALG Test
• Media Testing
• Fragmentation Testing
• Trace Route
• Bufferbloat
DNS Testing

DNS Testing tests the networks DNS against the 8x8 GTM (8x8 DNS) to verify devices are geo-routing to the correct data center. This testing is particularly useful with troubleshooting "Line Unregistered" for SRTP enabled lines, and call quality issues.

To identify geo-routing issues look through the DNS test results and locate the following message:

**Conflicting DNS resolutions: Two or more DNS Servers are in disagreement over**

As an example this user has a routing issue to the Polycom SBC as well as the Secure SBC (Extensions with SRTP enabled):

![DNS Test Result](https://support.8x8.com/equipment-devices/network-devices/how-to-read-the-network-utility-results)

The locations local DNS identified as: "[Local DNS Server 1]" is routing to the West coast, and the GTM (8x8's DNS) is routing to the East coast. This user happened to be located on the East coast. Using this information, we can see the user is geo-routing incorrectly using their DNS to the West coast server. To resolve this the user will need to change their DNS in use on the network.

### Additional information on DNS and Geo-Routing

- **DNS Result Destinations**
  - Georouting works on the public IP of the DNS server. MPLS, VPN's, and hosted DNS servers can falsely report geo-routing issues. It may be beneficial to review Virtual Office Analytics call quality reports to verify where the calls are truly routing.
  - Certain areas of the U.S. such as Illinois, Minnesota, and Texas as an example report routing issues quite frequently, despite there being no issue. The rule for this is if the tested location is west of the Mississippi River, it should be routed to the West coast. If you are located east of the Mississippi River you should be routed to the East Coast.
  - If located very close to the Mississippi you may be routing to the East Coast, but The West Coast is 10-15ms closer. This is not worth pursuing.
• The continuous test should be used as a source of information that an issue is present. Once an issue has been identified agents should move on to tools such as WinMTR and/or Ping Plotter to determine the source (ISP or LAN).

• The DNS tool does not properly handle queries if the GTM returns multiple IP's from the same subnet and may falsely report an error.

---

**Ping Test**

The ping test sends ping requests to each data center to check for high latency and/or packet loss over the connection. This test will not determine where the issue is coming from, only that a potential issue is present.

Use [WinMTR](https://support.8x8.com/equipment-devices/network-devices/how-to-read-the-network-utility-results) to get more detailed information on latency, packet loss and a potential cause for high latency and/or packet loss issues if the problem is consistent. If the issue is not consistent use [Ping Plotter](https://support.8x8.com/equipment-devices/network-devices/how-to-read-the-network-utility-results) for an extended test with time stamps. These tests will help determine where an issue is coming from if one is present.

The test below shows that ping requests within the United States, Canada, United Kingdom, and Hong Kong were fine but a warning message was provided for Australia.

---

**NAT**

The NAT test only determines the NAT type. This does not indicate any issues with the network as each firewall and router handle NAT differently.
Additional information on NAT and NAT Types

**Full Cone NAT (Static NAT)**

Full cone NAT (also known as one to one NAT) is the only type of NAT where the port is permanently open and allow inbound connections from any external host. A full cone NAT maps a public IP address and port to a LAN IP and port. Any external host can send data to the LAN IP through the mapped NAT IP and port. This type of NAT is also known as port forwarding. This is the least restrictive type of NAT as the only requirement is the connection comes in on a specific port - the one opened by the endpoint.

**Restricted Cone NAT (Dynamic NAT)**

A restricted cone NAT works in the fashion as full cone NAT, but adds additional restriction based on an IP address. The internal client must have first sent packets to an external host before it can receive packets from the external host. In terms of restrictions, the only requirement is that the packets come in on the mapped port and from an IP the internal client has sent packets to.

**Port Restricted Cone NAT (Dynamic NAT)**

Port restricted cone NAT functions the same as Restricted Cone NAT, but applies restrictions to ports as well. Restricted cone NAT will accept connections from any source port, a port restricted cone NAT restricts this further by only accepting connection from the IP and port it sent an outbound request to.

**Symmetric NAT (Dynamic NAT)**

Symmetric NAT applies restrictions in the same way as a port restricted cone NAT, but handles NAT translation differently. Symmetric NAT has its own unique issues. These issues stem from generating randomly generated ports and applying them to the client when reaching out to destinations. This NAT type does not use port preservation. For more information please see [this article](https://support.8x8.com/equipment-devices/network-devices/how-to-read-the-network-utility-results).

**Outbound Connectivity**

Outbound Connectivity testing indicates if ports are being blocked on the network, either individual ports or ranges on the firewall or router. If ports are blocked this could cause connectivity issues or dropped calls depending on what ports are blocked. The firewall should be configured per our guide on configuring a network for VoIP Services.

Below is an example of a test where ports are blocked:

![NAT Test Result](https://support.8x8.com/equipment-devices/network-devices/how-to-read-the-network-utility-results)
In contrast, below is an example of a test where all ports are available:

---
[08/23/2018 13:30:34] Running Outbound Connectivity Test
---
Running Outbound Connectivity Test on `netutil.8x8.com` <162.221.236.112>

- VO ports:
  All required TCP ports are available!
  All required UDP ports are available!

- VCC ports:
  All required TCP ports are available!
  All required UDP ports are available!

Test took 16 min 45.39 s
---

Additional Information on Outbound Connectivity Test

- Endpoint security applications (Anti-Virus or PC firewall applications) can cause this test to fail. It is suggested to disable these applications or add an exception in the application when running the network utility.
• This test may fail due to the router or firewall on the LAN having issues. In cases where there are no ports to open on the device (such as working with a Netgear), restart the router and retest. If the test continues to fail there may be an issue with the device itself (such as it's failing) or there is a firmware issue.

• This test can potentially fail if the subnet the connectivity test is running to is not white listed on the firewall. The location the customer is geo-routing to will be displayed at the top of the test as follows: Running Outbound Connectivity Test on 'netutil.8x8.com' <162.221.236.112>

---

System Info

Provides information about the computer that is running the test. This is especially useful for users running only Virtual Office Desktop. We can determine if the tested machine is meeting the minimum system requirements or is in an unsupported environment.
Additional Information on System Info

It is recommended to identify any potential VPN connections on the system information test. Additionally, we want to make sure the test is run on the same network as the phones.
ALG Test

ALG testing determines if ALG is enabled on the LAN. If ALG is enabled it can cause a multitude of issues such as dropped calls, echo, call termination, one-way audio, and no audio. If the test fails you will see the following message:

In contrast, here is an example of an ALG test with no errors:

Additional Information on the ALG test

- The ALG test verifies the checksum passed in the message at the server and at the client.
• If the checksum does not match the application will return "ALG detected" either at the server or at the client.
• If the message is not returned or a time out is received this typically indicates blocked ports or the message was modified and was dropped.
• When the time out message is received or no response is received the user will need to disable any endpoint security and verify ports 5060 and 5199 are allowed.

Media Testing

The media testing makes a series of mock calls to each data center. From this information, we can determine if there will be potential issues on calls due to packet loss, latency, or jitter. If the results are showing a warning or failure, the user will have call quality issues. Keep in mind this data is only relevant to the closest data center to the tested location, as well as the backup.

If the user is located in Canada, and the test provides a warning or failure to Australia, we would not take that as a valid fail. An example is provided below:

![Media Testing Results](https://support.8x8.com/equipment-devices/network-devices/how-to-read-the-network-utility-results)

### Fragmentation Testing

Fragmentation Definition:

Fragmentation is a technique that divides a data packet into smaller data packets so that they can be sent through a network that can only transfer small data packets. Fragmentation occurs during network transmission. When these packets are received at their destination, they are reassembled to their original data packet size.
Supporting Fragmentation:

In rare situations, signaling packets may become extremely large and require to be fragmented. If fragmentation is not supported there will be a loss of audio. 8x8 recommends that Fragmentation be supported by all network equipment, including routers.

If Fragmentation Fails:

We did find that Fragmentation may not be supported by your edge device. In rare situations, signaling packets may become extremely large and require to be fragmented. If fragmentation is not supported there will be a loss of audio. 8x8 recommends that Fragmentation be supported by all network equipment, including routers. 8x8 also recommends that your MTU be set to 1500 on all networking gear.

Below is an example of a Fragmentation test with a warning message:

---

Traceroute

This test runs a traceroute to the nearest data center to the tested location based on geo-routing information. If there is a consistent issue along the path to the data center you will be able to determine where it’s coming from on the traceroute.

This test is also useful for identifying the route the connection is taking from the local network to the path out to the public internet. If there is a second local IP, it is suggested to attempt to log into the device and verify it is in bridge or pass through mode. If it is not this could cause issues due to double NAT. Below is an example of a potential double NAT:
Additional Trace Route Information

- Keep in mind, if a machine is using an MPLS connection, a VPN, or multiple VLAN's the results seen on the test may not reflect as an accurate representation of a local issue. It is suggested to verify with the locations I.T. consultant how the machines are connected on the network.

- Some ISP's may have nodes that are not configured to show the public IP address on the route out over the public internet. It is possible that there may be local IP's reflected on the traceroute that do not indicate an issue.

Bufferbloat

Bufferbloat is the undesirable latency that comes from a router or other network equipment buffering too much data. Below is an example of a network with bufferbloat:

An example of a network without bufferbloat:
Additional Information on Bufferbloat

- This test does not always complete properly and may not be a good indication of issues on the LAN
- If excessive bufferbloat is detected it is suggested to power cycle the network and re-run the test to determine if the results were correct.
- If the test fails, there may be a potential firmware issue causing memory leaks and excessive buffering on the device. The user should update or roll back the firmware version they are using on their device and re-test.
- As a last resort, contact the device manufacturer for a solution to this issue. Although in all likelihood the device will need to be replaced at this point.