Troubleshooting Guide
HSCN IP network connectivity

Published January 2018
## Contents

1. **Introduction** 3  
   1.1 Purpose of document 3  
   1.2 Background 3  
   1.3 Intended audience 3  

2. **The HSCN and National Applications** 4  
   2.1 HSCN Solution Overview and Reporting 4  
   2.2 National Application Service Status and Reporting 5  

3. **Investigating and troubleshooting network connectivity problems** 6  
   3.1 Description of the problem 6  
   3.2 Network knowledge and documentation 7  
   3.3 Network Statistics and monitoring 7  
   3.4 The end device 7  
   3.5 Network troubleshooting techniques and the OSI model 8  
   3.6 Network tools for general troubleshooting 10  
   3.6.1 IP Addresses and URLs to use with troubleshooting tools 10  
   3.6.2 Ping 11  
   3.6.3 Traceroute 12  
   3.6.4 Traceroute and Network Latency 13  
   3.6.5 PathPing 15  
   3.6.6 Nslookup 16  
   3.6.7 Netstat 16  
   3.6.8 Arp 17  
   3.6.9 Route 17  
   3.6.10 Telnet 17  
   3.6.11 Other Utilities 17  
   3.7 Network troubleshooting application suites 18  
   3.7.1 Network monitoring and discovery tools 18  
   3.7.2 SNMP trapping 19  
   3.7.3 MIB browsers 19  
   3.7.4 Attack identification and simulation 20  
   3.7.5 Network Packet Sniffers 20  
   3.8 Speed test tools 21  
   3.9 IP Address Management 22  
   3.9.1 Subnet and IP Calculator 22  
   3.9.2 DHCP 22  
   3.9.3 IP address management tools 23  

4. **Appendix A – Fault Diagnostics Flow Chart** 24
1 Introduction

1.1 Purpose of document

The purpose of this document is to provide advice and guidance when troubleshooting network connectivity. This guide provides an effective and straightforward approach to troubleshooting network connectivity problems as well as more complex issues that may be encountered with application performance.

This guidance document provides a step by step guide to using specific tools and techniques that will resolve or rule out issues that commonly cause network connectivity problems. This will enable some issues to be fully resolved, or will assist in determining next steps by helping to exclude particular network and infrastructure elements as potential issues.

1.2 Background

The Health and Social Care Network (HSCN) Programme will deliver new and significantly different network services for health and social care as part of its remit to provide successor services to the current N3 network. The HSCN will create the effect of a single network across health and social care providers and their partners. All health and social care organisations (in England) are within scope of the HSCN solution, supporting integrated care delivery.

This guide will assist in troubleshooting simple network connectivity and application issues should they arise prior to, during, or following migration to the HSCN.

1.3 Intended audience

This guide is aimed at IT and network support teams and individuals within all Health and Social Care organisations who have responsibility for providing IT and network support to end users. Readers will have an understanding of local area network (LAN) and wide area network (WAN) design, PC network configuration, the Open Systems Interconnect (OSI) model, TCP/IP, and a number of basic networking and troubleshooting tools and utilities that are included in most popular PC and network operating systems.
2 The HSCN and National Applications

2.1 HSCN Solution Overview and Reporting

The HSCN will create a 'network of networks' established through adherence to common and open standards.

Provided by many suppliers, HSCN will act like a single network. It will allow health and social care providers to deliver, share and consume services from anywhere on HSCN and with anyone else on HSCN - regardless of their location or network supplier.

HSCN adopts the 'network peering architectural principle.' This supports regional and national collaboration with access to existing national applications and the NHS Spine.

HSCN includes a number of resources that provide various types of information including network status and performance reporting for consumer connectivity services.

The Legacy N3 Network, known as the Transition Network (TN), continues to provide the High Speed Customer Reporting (HSCR) tool which automates the production of reports on the TN consumer connectivity services. HSCR generates textual and graphical performance reports based upon information gathered from management systems used to monitor and maintain the consumer’s network connection. The HSCR application can be accessed via the BT Service Portal and provides three main types of reporting:

- **Customer Reports** – Textual and graphical performance reports in MS Word format, generally weekly and monthly, and available to download. A drop-down menu in this part of the HSCR application will list the reports to which a customer has access.
• **Dashboard Reports** – The dashboard shows a list of devices that are available to the customer. Each device can be clicked to view more detail, including the site address, router type and IP address. The status of the service for CPU, Memory, Bandwidth, Packet Loss, Delay and Jitter are all represented by red, amber or green traffic lights:

- ⚫ indicates a threshold has been breached within the previous 24 hrs
- 🟠 indicates a threshold has been breached within the last week
- 🟢 indicates that the threshold has not been breached within the last week
- ⬜ indicates that there is no data available

Historic data is available for the previous forty-five days. It is also possible to view current or projected data by selecting the Current or Projected buttons. Data under the Current data view is available to the start of the current hour. Projected data is available for some parameters such as CPU utilisation and Bandwidth utilisation only. Projected data is based on an extrapolation of historic and current data.

• **Real-time Reports** - This Real Time Performance report option allows the customer to select a router or an interface on a router and display near real-time data in the form of a chart. Reports can be generated for Router CPU and Buffer Utilisation or Interface statistics over your unique specification of the reporting period. See the Help and Support section of the HSCR application for more information on this and the other reporting options.

HSCN Consumer Network Service Providers (CN-SPs) will offer similar status and reporting tools and resources. This will depend on the connectivity service you have procured.

### 2.2 National Application Service Status and Reporting

The NHS Digital Service Management function manages and protects live service for all of NHS Digital major IT systems. There are over 70 systems that cover all areas of health and social care. The national systems covered by service status statistics include the national legacy N3 network (TN), Spine Core, Care Identity Service, Secondary Uses Service, NHS e-Referral Service, Hospital Episode Statistics, Clinical Indicators, a number of systems that support trusts, plus GP and prescription dispensing systems. For more information please go to [https://digital.nhs.uk/article/313/Service-Management](https://digital.nhs.uk/article/313/Service-Management).

From this page you can also access service status information, reports, and incident data. These pages can be accessed via a TN connection here: [http://nww.digital.nhs.uk/servicemanagement/status/](http://nww.digital.nhs.uk/servicemanagement/status/).

This will take you to the following Service Status page showing the status of each system and a clickable map for incidents by geographical area.
This page also provides a number you can call if you are experiencing service issues and the status shown does not reflect your situation, as well as a link to subscribe to communication lists if your role requires you to be informed of Higher Severity Service Incidents by email.

# 3 Investigating and troubleshooting network connectivity problems

## 3.1 Description of the problem

When an end user logs a call with your helpdesk or a call comes through to you that relates to a problem with network connectivity or application performance the first step is to ensure that the user has provided sufficient information to describe the problem. If not, it is important to obtain full details of the issue from the end user. For example, if the user has reported “It’s taking forever to transfer a file” or “I cannot connect to the server, the server must be down”, ask the user the right questions to gain more information about the problem, such as “Are any other files transferring slowly?”, “Have you tried to connect to any other servers?”

It is important to gather as much detail as possible about the reported problem. A useful guide is “What, Where, When, How Much”.

- **WHAT**: Which devices, links, interfaces, hosts, applications have the problem?
- **WHERE**: Location - on what VLAN, subnet, segment, is the problem observed?
- **WHEN**: Timing - when did we first see the problem? Is the problem reoccurring?
• **HOW MUCH**: How big is the problem? Is the problem getting worse?

Documenting where you cannot see the problem may also be useful as you can look for differences between where the problem exists and where is doesn’t. You can then look for changes that relate to these differences and this may help to identify the cause.

### 3.2 Network knowledge and documentation

If the problem described by the end user requires further investigation using network based tools and techniques it is important to have good knowledge of the local network as well as a detailed set of design documentation. This should include at least a detailed network diagram, showing locations, routers, and IP subnets. In addition to this, an inventory of network equipment with software versions and device configurations will be useful. Knowledge of the protocols and applications that are running on the network is essential. This will help to identify the path the traffic should take and to choose the most appropriate tests, tools, and techniques to employ to investigate the issue. It can also be important to capture changes within this documentation. If the documentation is up to date and includes a record of changes in topology, configuration and software changes, hardware replacements this may correlate with the reported problem and thus help to identify the cause.

In addition to up to date documentation, it is useful to have access to a Network discovery tools. Such applications can scan the network for known device heuristics. When a device heuristic is found at a particular address, the network discovery tool logs the location and its believed device type. See the section on **Network monitoring and discovery tools** later in this document for more information.

### 3.3 Network Statistics and monitoring

If you have access to a local network monitoring system or other network statistics capture software/appliance this can provide another set of data to help diagnose the reported problem. It is important that this system is capable of capturing error statistics, as well as those for utilisation. A typical set of statistics collected by the network monitoring system would include traps and syslog messages, network and device load, CPU, memory, environmental data, throughput, response times and so on. The system should also be capable of keeping (and/or or exporting) historical data. Using the data from this system will enable the troubleshooter to see trends and patterns and changes in network and device load to better pinpoint the potential cause of the problem. See the section on Network Monitoring later in this document for more information.

### 3.4 The end device

There are a number of simple checks that should be carried out to ensure that the end device is working and configured correctly and can connect to the network. These are to:

- Check the network interface card (NIC), wired or wireless, is installed correctly
- Check that the correct and up to date software drivers are installed
- Check the network interface card is connected to the network. Use a software utility like ‘ipconfig’ (Windows PCs) or ‘ifconfig’ (UNIX, Linux) to check that the network card
is connected to the network and that the appropriate IP address, subnet, and gateway configuration is present. Typical output is shown below.

```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix. : 
Link-local IPv6 Address . . . . . : fe80::345f:d30f:114:45e9%13
IPv4 Address . . . . . . . . . . : 192.168.132.23
Subnet Mask . . . . . . . . . . : 255.255.255.128
Default Gateway . . . . . . . . : 192.168.132.1
```

- If the output from ‘ipconfig’ reports that the network is not connected, you should check the following
  
  o For wired networks, check that the wall socket is working and is connected at the patch panel (in the comms cabinet) to a live port on the active networking equipment e.g. hub/switch;
  
  o For wireless networks, check that the nearest wireless hub or ‘hotspot’ is working and that any security configuration required to connect end devices to the wireless network are enabled.

- You can also use the ‘ping’ tool to check local network card connectivity. At a command prompt try:
  
  o ‘ping localhost’ or ‘ping 127.0.0.1’

  This will show whether the NIC is installed correctly and TCP/IP is configured on the interface.

### 3.5 Network troubleshooting techniques and the OSI model

Before you begin to troubleshoot the network problem, it is important to decide on the technique you think may be most effective for the given problem. This document does not attempt to prescribe or recommend a particular technique over any other, but to simply assert that having a good technique for finding the problem will help to quickly identify where the root cause exists. In addition, this document includes details of a varied set of tools and techniques that will help the network support engineer work towards a solution.
One commonly used framework for troubleshooting that helps structure your response to a known network problem is the International Standards Organization (ISO) Open Systems Interconnect (OSI) model. The intended audience of this document should already be familiar with OSI model. It’s the framework that encapsulates much of modern networking, and most network protocols live somewhere within its seven layers. It can be useful as a troubleshooting guide for triaging an unknown problem on the network.

The OSI model can be extended into a framework for problem isolation. The diagram shows the seven layers in the OSI model and some issues that typically occur related to each layer. Each of the layers is discussed below.

- **At the Physical layer**, problems typically involve some break in the physical connectivity that makes up the network. Broken network connections, cabling and connector issues, and hardware problems that inhibit the movement of electricity from device to device typically indicate a problem at this layer.

- **At the Data Link layer**, we move away from purely electrical problems and into the configuration of the interface itself. Data Link problems often have to do with Address Resolution Protocol (ARP) problems in relating IP addresses to Media Access Control (MAC) addresses. These can be caused by speed and duplex mismatching between network devices or excessive hardware errors for the interface. An incorrectly configured interface within the device operating system (OS) or interference for wireless connections can also cause problems at the Data Link layer.

- **At the Network layer**, we begin experiencing problems with network traversal. Network layer problems typically occur when network packets cannot make their way from source to destination. This may have something to do with incorrect IP addressing or duplicate IP addresses on the network. Problems with routing data or ICMP packets across the network or protocol errors can also cause problems here. In extreme cases, an external attack can also spike error levels on network devices and cause problems identified at the Network Layer.

- **At the Transport layer**, we isolate problems that typically occur with TCP or UDP packets in Ethernet networks. These may have to do with excessive retransmission errors or packet fragmentation. Either of these problems can cause network performance to suffer or drop completely. Problems at this layer can be difficult to track down because unlike the lower layers they often don't involve a complete loss of connectivity. Additionally, Transport layer problems can often involve the blocking of traffic at the individual IP port layer. If you've ever been able to ping a server but cannot connect via a known port, this can be a Transport layer problem.

- **The Session, Presentation, and Application layers** are often lumped together because more recent interpretations of the OSI model tend to grey the lines between these three layers. The troubleshooting process for these three layers involves problems that have to do with applications that rely on the network. These applications could involve DNS, NetBIOS, or other resolution, application issues on
residing OSs, or high-level protocol failures or misconfigurations. Examples of these
high-level protocols are HTTP, SMTP, FTP, and other protocols that typically "use the
network" rather than "run the network." Additionally, specialized external attacks such
as "man-in-the-middle" attacks can occur at these levels.

Network problems can and do occur at any level in the model. And because the model is so
highly understood by network administrators, it immediately becomes a good measuring
stick to assist with communicating those problems between triaging administrators.

References
This section is taken from an excerpt from "Network troubleshooting and diagnostics,"
Chapter 4 of The Shortcut Guide to Network Management for the Mid-Market, written by
Greg Shields and published by Realtimepublishers.com. You can read more here.

More explanatory information on the OSI model can be found online and the document itself
can be downloaded from the ISO site here.

3.6 Network tools for general troubleshooting
This section describes a number of widely available tools that can assist with troubleshooting
a network problem.

A number of these tools require a destination (IP address or URL) to be specified. The first
section here includes a number of suggested locations on the HSCN and the Internet that
can be used.

3.6.1 IP Addresses and URLs to use with troubleshooting tools

HSCN/TN Hosted Test Locations
The following locations are suggested as targets for testing inside the HSCN/TN.

- HSCN DNS - Primary: 194.72.7.137; Secondary: 194.72.7.142
- NHS Electronic Staff Record system (ESR) - https://esr.mhapp.nhs.uk

Internet Testing Locations
The following locations are suggested as targets for testing communication with the Internet.

- NHS Choices - http://www.nhs.uk
- Google UK - http://www.google.co.uk
- Google public DNS server - 8.8.8.8

3.6.1.1 Proxy Test

The destination below is an Internet hosted resource that attempts to shows details of any proxy
servers you are using.

- https://whatismyipaddress.com/proxy-check
3.6.2 Ping

The ping tool sends an ‘echo’ request to a destination and, if successful, receives an ‘echo’ reply in return. As a general networking tool, the ping utility can be used to check end-to-end network connectivity, can show baseline network performance, and can help to find data-dependent problems. A suggested test is to try to ‘ping’ the default gateway to ascertain if communication between it and the end device is possible.

- Ping the ‘default gateway’. The default gateway is the router configured for this end device as the connection or ‘hop’ to the next network. Obtain the IP address of the default gateway from the ‘ipconfig’ command and at the command prompt type:

  o ‘ping ‘ n.n.n.n (where n.n.n.n is the default gateway IP address)

The ping tool can also be used to test the network path to determine whether communication with destinations outside the local area network is possible.

- Ping a destination outside the local network. A suggested destination is the HSCN DNS. If this is successful it shows that network and routing configuration is in place for communication to the central HSCN. At a command prompt type:

  o ‘ping 194.72.7.137’ or ‘ping 194.72.7.142’

  If a ping to the HSCN DNS is not successful you can try other services connected to the HSCN/TN, some examples are:

  o http://nww.digital.nhs.uk/
  o https://esr.mhapp.nhs.uk
  o https://portal.national.ncrs.nhs.uk

- Ping a destination on the Internet. A number of destinations are suggested in the section above.

- Firewalls and other local devices. If this second ping to a device on the HSCN/TN is not successful, check with your second line network support team to confirm that there are no other devices that may be causing the communication to fail such as proxy servers, Firewalls etc.

- Ping a specific application host. If the reported issue is lack of connectivity to an application hosted on the HSCN, obtain an IP address of that application (or data centre) and try a ping test to that destination using similar commands given in the previous examples. Even if this test fails however it does not mean that the end device cannot connect or that the application is not available. Some hosted services will explicitly disallow responses to a ‘ping’ request to prevent network attacks.

The ping tool generally returns two pieces of information: whether the source can reach the destination (and, by inference, vice versa), and the round-trip time (RTT) or a 2 way Latency, typically in milliseconds (ms). The RTT returned by ping should be used only as a comparative reference because it can depend greatly on the software implementation and hardware of the system on which ping is run. When using ping, first try to ping from the source to destination device by IP address. If the ping fails, verify that you are using the correct address and try the ping again. Then try to ping from the source to the destination device by name. If the ping fails, verify that the name is correctly spelled and that it refers to
the destination device, and then try the ping again. If you can ping the destination by both name and address, it would suggest that the problem is an upper-layer TCP/IP issue.

Depending upon the end-device operating system, the ping tool may have various options. These include a ‘repeat count’ which allows the troubleshooter to specify the number of times the ping is repeated. This can be used to generate extended amounts of network traffic or ‘stress’-test response times or network connectivity. Most ping utilities allow the user to specify the packet size used for the ping. This can help identify data dependent problems or can be used for network-layer packet generation. For more ping options check the OS documentation.

Some drawbacks of ping are that:

- It increases network load
- It Uses artificially high TTL value
- Often routers lower the priority for ping to prevent Denial of Service (DoS) attacks
- It Only does network-layer checks
- It Does not pinpoint network problems
- It Should not be used to check DNS records

### 3.6.3 Traceroute

In addition to a simple ‘ping’ test you can use a ‘traceroute’ utility to obtain a more detailed view of communications along the network path to the destination. Traceroute uses the ICMP Echo Request, ICMP Time Exceeded, and ICMP Echo Reply packets. Traceroute can help to narrow down connectivity issues and provide baseline network layer performance on a hop-by-hop basis.

At a command prompt, type: ‘tracert’ (Windows device) or ‘traceroute (Linux/Unix). The output will attempt to show statistics at each router or network ‘hop’ along the path. The output should look something like this:

```plaintext
>tracert google.com
Tracing route to GOOGLE.COM [216.58.204.78] (NOTE: IP address subject to change).
over a maximum of 30 hops:
  1     1 ms     1 ms     1 ms  192.168.132.2
  2     1 ms     1 ms     1 ms  192.168.198.226
  3    16 ms    16 ms    16 ms  192.168.220.1
  4    18 ms    17 ms    17 ms  192.168.1.197
  5    16 ms    17 ms    21 ms  192.168.69.51
  6    16 ms    17 ms    17 ms  10.97.91.2
  7    17 ms    17 ms    17 ms  10.215.219.97
  8    23 ms    22 ms    23 ms  10.100.100.14
  9    23 ms    23 ms    23 ms  217.36.152.73
 10    23 ms    23 ms    23 ms  172.16.195.243
 11    24 ms    23 ms    23 ms  172.16.195.131
 12    24 ms    24 ms    24 ms  217.35.210.165
 13    26 ms    28 ms    30 ms  core2-te0-10-0-6.ealing.ukcore.bt.net
      [62.6.200.69]
 14    25 ms    26 ms    25 ms  peer6-te0-9-0-11.telehouse.ukcore.bt.net
      [213.121.193.150]
 15    25 ms    25 ms    25 ms  195.99.126.185
 16    40 ms    25 ms    25 ms  72.14.233.201
```
The traceroute utility comes with several options depending upon the operating system and version. These include the ability to specify the maximum number of hops above the default of 30, although if this has to go above 64 this would usually indicate a routing problem. For more traceroute options check the OS documentation.

There are a number of drawbacks associated with the traceroute utility, such as:

- ICMP messages may be filtered
- Different IP stacks respond differently to traceroute
- Latency figures may not be accurate with regard to applications

### 3.6.4 Traceroute and Network Latency

Network latency is the term used to indicate any kind of delay that happens in data communication over a network. Network connections in which small delays occur are called low-latency networks whereas network connections which suffer from long delays are called high-latency networks. There are three primary types of network induced latency:

- **Serialization Delay** - The delay caused by having to transmit data through routers/switches in packet sized chunks. Should not be considered a major issue in modern network as packets sizes have remained very much the same but interface are generally much faster.

- **Queuing Delay** - The time spent in a router’s queues waiting for transmission. This is mostly related to line contention (full interfaces), since without congestion there is very little need for a measurable queue.

- **Propagation Delay** - The time spent “in flight”, in which the signal is traveling over the transmission medium. This is primarily a limitation based on the speed of light or other electromagnetic wave propagation.

To understand the output from a tracert, like that above, requires an answer to the question: “How is traceroute latency calculated?” The following gives a simplified explanation:
• Timestamp when the probe packet reply, ICMP (MS Windows uses this protocol, others use UDP), is launched

• Timestamp when the reply ICMP is received

• Subtract the difference to determine round-trip value

• Routers along the path do not do any time ‘processing’
  o They simply reflect the original packet’s data back to the SRC
  o Many implementations encode the original launch timestamp into the probe packet, to increase accuracy and reduce state

• But remember; only the ROUND TRIP is measured
  o Traceroute shows the hops on the forward path BUT shows latency based on the forward PLUS reverse paths. Any delays on the reverse path will affect your results!

Timestamps for MS Windows use the ICMP protocol as mentioned above, but remember that TCP may be far better to negotiate firewalls if tracerouting is needed beyond general routers in a network.

As mentioned above, the main contributions to network latency are Serialization Delay, Queuing Delay, and Propagation Delay. Identifying and Interpreting if the latency that you are seeing in the traceroute is ‘normal’ or not is therefore crucial – since this may potentially create the need to contact a network supplier to log a call. If you see a high latency e.g. >500ms on your traceroute, you need to know where the destination router is located because this may indeed be a normal propagation delay due to distance, since propagation delay in fibre networks adds a millisecond to every 62.5 miles, approximately.

Note: Because TCP/IP does not store path information in its packets, it is possible for a packet to have a working path from the source to the destination (or vice versa), but not to have a working path in the opposite direction. For this reason, it may be necessary to perform all troubleshooting steps in both directions along an IP path to determine the cause of a connectivity problem.

‘False’ Latency
It is important to note is that the architecture of modern routers is very different depending on whether you are forwarding packets or sending packets to the router. Forwarding packets through the router is done via the routers Data Plane using multiple paths. Packets that are forward packets to the router are channelled through the Control Plane. Other protocols (e.g. BGP, SNAP, monitoring, or someone working on the router will consume CPU time. This will increase CPU load, and hence time to process packets, no matter if the Data Plane or Control Plane is used. As scheduling within routers is not used, this can cause a random ‘spike’ effect manifesting itself in ‘false’ latency problems when in actual fact the delay is ‘normal’. The most infamous process which causes these spikes is called ‘BGP Scanner’ and runs every 60 seconds on all Cisco IOS devices. Hard limits to most vendor routers...
mean that only a certain number of ICMP packets will hit in any one second, but not all may be responded to, hence again potentially providing a false view of latency.

The most important rule is that if there is ‘real’ latency then:

- Latency will continue or increase for all future hops in the traceroute
- The ‘spikes’ mentioned above mean absolutely nothing in the middle of the trace if they do not continue forward

Remember to perform traceroute tests at varied times throughout a working or non-working period and look for consistency in the output trace.

### 3.6.5 PathPing

The PathPing tool is a route tracing tool that combines features of Ping and Tracert with additional information that neither of those tools provides. PathPing sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop. Since PathPing shows the degree of packet loss at any given router or link, you can pinpoint which routers or links might be causing network problems. PathPing is supplied in Windows NT and above.

Below is a typical PathPing report. Note that the compiled statistics that follow the hop list indicate packet loss at each individual router.

```
D:\>pathping -n testpc1
Tracing route to testpc1 [7.54.1.196] over a maximum of 30 hops:
  0 172.16.87.35
  1 172.16.87.218
  2 192.168.52.1
  3 192.168.80.1
  4 7.54.247.14
  5 7.54.1.196

Computing statistics for 125 seconds...

<table>
<thead>
<tr>
<th>Hop</th>
<th>RTT</th>
<th>Source to Here</th>
<th>This Node/Link</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0/ 100 = 0%</td>
<td>0/ 100 = 0%</td>
<td>172.16.87.35</td>
</tr>
<tr>
<td>1</td>
<td>41ms</td>
<td>0/ 100 = 0%</td>
<td>0/ 100 = 0%</td>
<td>172.16.87.218</td>
</tr>
<tr>
<td>2</td>
<td>22ms</td>
<td>16/ 100 = 16%</td>
<td>3/ 100 = 3%</td>
<td>192.168.52.1</td>
</tr>
<tr>
<td>3</td>
<td>24ms</td>
<td>13/ 100 = 13%</td>
<td>0/ 100 = 0%</td>
<td>192.168.80.1</td>
</tr>
<tr>
<td>4</td>
<td>21ms</td>
<td>14/ 100 = 14%</td>
<td>1/ 100 = 1%</td>
<td>7.54.247.14</td>
</tr>
<tr>
<td>5</td>
<td>24ms</td>
<td>13/ 100 = 13%</td>
<td>0/ 100 = 0%</td>
<td>7.54.1.196</td>
</tr>
</tbody>
</table>

Trace complete.
```
When PathPing is run, the first results you see list the route as it is tested for problems. This is the same path that is shown via Tracert. PathPing then displays a busy message for the next 125 seconds (this time varies by the hop count, requiring 25 seconds per hop). During this time PathPing gathers information from all the routers previously listed and from the links between them. At the end of this period, it displays the test results.

The two rightmost columns — "This Node/Link Lost/Sent=\%" and "Address" — contain the most useful information. The link between 172.16.87.218 (hop 1), and 192.168.52.1 (hop 2) is dropping 13 percent of the packets. All other links are working normally. The routers at hops 2 and 4 also drop packets addressed to them (as shown in the "This Node/Link" column), but this loss does not affect their forwarding path.

The loss rates displayed for the links (marked as a "|" in the rightmost column) indicate losses of packets being forwarded along the path. This loss indicates link congestion. The loss rates displayed for routers (indicated by their IP addresses in the rightmost column) indicate that those routers' CPUs or packet buffers might be overloaded. These congested routers might also be a factor in end-to-end problems, especially if packets are forwarded by software routers.

For more information about PathPing, including switches (command line options) for the utility, refer to the Microsoft TechNet pages [here](#).

### 3.6.6 Nslookup

The Nslookup tool is used to query a Domain Name Service for IP address and host names. This is useful as client-side DNS failures give a false positive for a connectivity problem while server-side failures can cause sluggish service connection times.

When you start Nslookup, it shows the host name and IP address of the DNS server that is configured for the local system, and then display a command prompt for further queries. If you type a question mark ( ? ), Nslookup shows all available commands. You can exit the program by typing exit.

To look up a host's IP address using DNS, type the host name and press Enter. Nslookup defaults to using the DNS server configured for the computer on which it is running, but you can focus it on a different DNS server by typing server < name> (where < name> is the host name of the server you want to use for future lookups). Once another server is specified, anything entered after that point is interpreted as a host name.

For more information about Nslookup refer to the Microsoft TechNet pages [here](#).

### 3.6.7 Netstat

Netstat shows the state of the active network connections on a host. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port. It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports. For more information on using Netstat and its options/switches, type “netstat /?” at the command prompt or visit the MS TechNet pages [here](#).
3.6.8 Arp

The Address Resolution Protocol (ARP) is a communications protocol used for resolution of Internet layer addresses into link layer addresses, a critical function in the Internet protocol suite. ARP was defined by RFC 826 in 1982 and is Internet Standard STD 37. ARP is also the name of the program for manipulating these addresses in most operating systems.

In Microsoft Windows Arp allows you to view and modify the ARP cache. If two hosts on the same subnet cannot ping each other successfully, try running the arp -a command on each computer to see whether the computers have the correct media access control (MAC) addresses listed for each other. You can use Ipconfig to determine a host's correct MAC address.

You can also use Arp to view the contents of the ARP cache by typing arp -a at a command prompt. This displays a list of the ARP cache entries, including their MAC addresses.

For more information about the Arp command visit the Microsoft TechNet pages here.

3.6.9 Route

In MS Windows, the ‘Route’ command is used to view and modify the IP routing table. Route Print displays a list of current routes that the host knows. Route Add adds routes to the table. Route Delete removes routes from the host's routing table.

For more information about the Route command visit the Microsoft TechNet pages here.

3.6.10 Telnet

Telnet (short for TELetypenetwork) is a network protocol used to provide a command line interface for communicating with a device. Telnet is used most often for remote management but also sometimes for the initial setup for some devices, especially network hardware like switches, access points, etc. As a troubleshooting tool, Telnet can be useful to test connectivity to a remote host. Telnet provides a bidirectional interactive text-oriented communication facility using a virtual terminal. In MS Windows, you will need to enable the Telnet Client through the Control Panel. To do this, go to the Programs and Features section of Control Panel and click on ‘Turn Windows features on or off’. From the Windows Feature window, selecting Telnet Client and then clicking OK will enable Telnet.

For more information about the Telnet command for Windows visit the Microsoft TechNet pages here.

3.6.11 Other Utilities

In addition to those described above, there are a wide range of utilities available for multiple operating systems. Some are available for either Windows or Unix/Linux family and some are available for both. The list below includes some that may be useful.

- Pchar
  - Based on PathChar
  - Measures Network performance on a per-hop and total path basis
  - IPv4 and IPv6
o Useful in isolating network problems

**Netcat (nc)**

- Similar in operation to telnet
- Tests application connectivity
- Can test TCP and UDP services

**Note** – There are many other applications that provide this type of functionality. Examples include **putTY** and **Tera Term**. The selection of one over the other is strictly a personal preference.

- **Host** – Unix tool similar in functionality to the NSLookup Windows command
- **Dig** – Linux tool similar in functionality to the NSLookup Windows command

## 3.7 Network troubleshooting application suites

This section briefly describes a number of application suites that extend the network troubleshooters toolkit and can be essential for the efficient and successful operation of the corporate network.

### 3.7.1 Network monitoring and discovery tools

Network monitoring tools can either be a component of your NMS or a separate utility. In either case, a network monitoring tool is used to record and analyse the characteristics within its configured network. Network monitoring tools can monitor for network performance as well as network outage and device resource use. They typically aggregate multiple network devices into a single user interface for cross-device analysis. Some features in a network monitoring tool that are critical for the troubleshooting process are:

- Multiple device capability
- Traffic graphing support
- Device resource use monitoring
- Alerting and notification via multiple mediums
- SMS/text messaging support
- SNMP management
- Traffic analysis
- Built-in traffic filters and aggregators

Sometimes part of the network monitoring system and sometimes a separate application, Network Discovery tools can scan the network for known device heuristics. When a device heuristic is found at a particular address, the network discovery tool logs the location and device type.

Numerous Network Discovery software solutions exist and each has a specific mechanism for seeking out devices -- by IP address, MAC address, SNMP response, DNS entry, or even
individual switch port on switching devices. Some features useful in a network discovery tool are:

- NMS integration
- Multiple IP range entry
- Fast scanning
- Device heuristic databases with SNMP
- Switch port mapping
- Data export to common file formats

### 3.7.2 SNMP trapping

SNMP trap receiving tools are out-of-band tools that can receive, analyse, and display low-level trap information from an SNMP-enabled device for purposes of troubleshooting and SNMP analysis outside the NMS. SNMP trap editing tools allow for the editing of trap templates to customize NMS response when traps occur. These tools incorporate some needed features for advanced SNMP manipulation, such as:

- Data export to common file formats
- Trap manipulation
- Tree view
- Trap mimicking and simulation

SNMP trapping is commonly an integral part of the Network Monitoring system or tool.

### 3.7.3 MIB browsers

Management Information Bases (MIBs) are databases of characteristics about network devices. Those databases are released by the manufacturer and house readable and writeable information about the configuration and status of the network device. A MIB Browser is a specialized tool that can peer into the data inside a MIB and pull out relevant Object ID (OID) information. Remember that OIDs are little more than strings of numbers used as unique addresses for device data. A good MIB Browser will include a pre-populated database of known OIDs and their related data. It will also enable the ability to “walk the MIB tree,” gathering all known data from that MIB and presenting it to the administrator.

The real power of an effective MIB Browser is in its ability to view and search the MIB for relevant information and allow the administrator to modify and customize that information as necessary. A good MIB Browser will typically include this functionality:

- Remote device support
- Large database of known OIDs
- View/search/walk via tree-view
- Editing functions
• Reading/writing support
• Multiple-device support

MIB Browsers are primarily used as customization tools for the SNMP-enabled devices plugged into your NMS.

3.7.4 Attack identification and simulation

Administrators unfamiliar with the changes in a network's functionality during an external attack situation will be unprepared for fending off that attack once it occurs. Attack identification and simulation tools enable the administrator to identify when common network attacks occur such as broadcast storms, cache poisoning, replay attacks, and so on. They also allow for the simulation of such attacks upon a network to monitor and analyse the behaviour of that network as well as to assist in preparing the network against a real attack by an outside attacker.

Attack identification tools such as network intrusion detection systems and network intrusion protection systems can be complicated to install and manage due to the prevalence of false positives and false negatives such systems can generate. Features of interest in either type of tool include:

• Performance monitoring elements
• Identification databases with real-time update
• Multiple attack profiles
• Dictionary and brute force capabilities
• Network device security checks
• Port scanning
• Network jamming
• Remote TCP resetting

It is important to note that such tools have the capability of inhibiting the successful operation of the network so must be used with great care and by technicians who are fully skilled in their operation.

3.7.5 Network Packet Sniffers

Network Packet Sniffers are application programs that can analyse what is actually happening on the wire by intercepting and logging traffic on a network. A Packet Sniffer (also known as a Network Analyser or Protocol Analyser) is useful for measuring performance and connectivity, and can help to establish a network performance baseline.

Packet sniffers work by intercepting and logging network traffic that they can 'see' via the wired or wireless network interface that the packet sniffing software has access to on its host computer.

On a wired network, what can be captured depends on the structure of the network. A packet sniffer might be able to see traffic on an entire network or only a certain segment of it,
depending on how the network switches are configured, placed, etc. On wireless networks, packet sniffers can usually only capture one channel at a time unless the host computer has multiple wireless interfaces that allow for multichannel capture.

Once the raw packet data is captured, the packet sniffing software must analyse it and present it in human-readable form so that the person using the packet sniffing software can make sense of it. The person analysing the data can view details of the 'conversation' happening between two or more nodes on the network.

Network technicians can use this information to determine where a fault lies, such as determining which device failed to respond to a network request.

Packet sniffers can be very useful when analysing network problems. There are numerous hardware solutions available on the market, as well as many software applications including freeware. This document does not describe, promote, or endorse any particular solution. General information on packet analysers, as well as specific information about particular brands, can be found easily through an Internet search engine.

### 3.8 Speed test tools

A very easy test that can be used to both determine the Internet bandwidth available to a specific host and to determine the quality of an Internet connection is the use of one of the many online speed tests tools. Whilst there are other, more detailed, methods that can be used to determine the speed or capacity of the network connection between your network and a given destination, online speed check utilities are an easy and quick way to obtain a good idea of how the network is performing, between your end site and that used by the chosen speed check tool. These tools can be useful when measuring how long it is going to take to upload or download information from a local to remote host. The measurement given in the speed test results can also be used to determine whether the connection is offering the amount of bandwidth that was purchased from the Internet provider. Some online speed test tools can provide an indication of the quality of the connection by measuring the ping response times and jitter amounts over a short period of time. This information can be used to determine a likelihood of how well the measured connection will deal with certain types of high demand traffic like Voice over IP (VoIP) or gaming. When using any of these tools it is important to consider the following:

- Keep in mind that some amount of bandwidth difference is expected between the quoted bandwidth purchased and the measured bandwidth
- The results of free online speed test tools may not be used as an alternative to bandwidth measurements (or other contracted service levels) given for your connection to the HSCN or legacy N3 service;
- Be clear on how the online speed test obtains and presents its results
- Bear in mind that these are 'snapshot' views and the time they were run may be significant in terms of how busy your network (and Internet connection) is

Online speed test tools are generally an ‘indicator’ of performance and bandwidth and can be useful as part of the network troubleshooters toolkit. Popular online tools include:

- [http://www.speedtest.net/](http://www.speedtest.net/)
- [http://www.thinkbroadband.com/speedtest](http://www.thinkbroadband.com/speedtest)
- [http://www.broadbandspeedchecker.co.uk/](http://www.broadbandspeedchecker.co.uk/)
3.9 IP Address Management

This section describes a set of tools to specifically deal with the management and maintenance of IP addresses. The tools discussed in the following sections are designed to assist with that process of managing the scope of IP addresses on your network.

3.9.1 Subnet and IP Calculator

A subnet and IP calculator can be used to ensure a correct IP address selection and with this a correct IP address configuration. The applications/tools available vary in functionality. An IP subnet mask calculator generally enables subnet network calculations using network class, IP address, subnet mask, subnet bits, mask bits, maximum required IP subnets and maximum required hosts per subnet. Results of the subnet calculation usually provide the hexadecimal IP address, the wildcard mask, for use with ACL (Access Control Lists), subnet ID, broadcast address, the subnet address range for the resulting subnet network and a subnet bitmap. Variants (or other functionality) may include CIDR network calculations using IP address, subnet mask, mask bits, maximum required IP addresses and maximum required subnets and give the wildcard mask, CIDR network address (CIDR route), network address in CIDR notation and the CIDR address range for the resulting CIDR network etc.

As with other applications in this space, they are many and varied with free and paid applications available for download as well as online tools that are generally free to use.

3.9.2 DHCP

Interestingly, although the automatic assignment of addresses through the Dynamic Host Configuration Protocol (DHCP) is considered a network function, its administration is usually done by systems administrators. This is usually the case with small and medium-sized networks because the server that handles the DHCP service resides not on a network device but instead on a server.

However, the management of DHCP scopes can leak into the role of the network administrator in situations in which DHCP scopes fill up. In networks with many DHCP scopes at high utilization, when the scope fills to 100%, users interpret the resulting lack of network connectivity as a network problem. In those situations, the network administrator is often the first to be called in to troubleshoot the problem.

Including DHCP scope monitoring tools in your network administrators’ toolset can help in these situations as full scope problems are difficult to track down using other tools. When considering a DHCP scope monitoring tool, look for one with capabilities that include:

- tabular user interface
- support for BIND and Windows-based DHCP
- alerting and notification
- visual identification of full and near-full scopes

Problems associated with full and nearly-full DHCP scopes can be a troubleshooting nightmare. This is because the client error messages associated with a full DHCP scope in
many OSs are unclear. Also, the resolution to the problem is often a re-segmenting of the network to add new subnets. It is for this reason many networks utilize multiple full Class C networks for workstation networks.

If you are having issues with full or nearly-full scopes due to machines that repeatedly come on and off the network, consider reducing the DHCP lease time to a very short amount of time before re-segmenting the network. DHCP renewal traffic is very minimal on today’s networks and the added traffic from the increased number of DHCP lease renewals should not significantly impact network performance.

3.9.3 IP address management tools

Where the intersection of the systems and the network administrator can cause difficulty is in the management of available IP addresses for subnets not serviced by DHCP. In typical networks, these subnets often house the network servers and server infrastructure. Because servers are critical components of the network, management of their IP address space is important to ensuring their uptime and availability.

In early networks, systems administrators often use a "ping and pray" approach to finding an available IP address on a server subnet. In this approach, they ping various addresses on the server subnet and look for the first one that does not respond. They then configure the new server with that IP address and "pray" that it wasn't in use by a server experiencing an extended outage. In dynamic situations with servers going up and down for extended periods, this can be especially problematic.

A better approach to using "ping and pray" is to incorporate an IP address management tool that monitors for use of IP addresses in critical subnets. The tool can store the last known-connected device for each IP as well as notify the administrator how long that IP address has either been used or has gone unused. When looking for such a tool, consider features such as:

- forward and reverse DNS lookups
- data export to common file formats
- active monitoring
- database storage
- SNMP support
4 Appendix A – Fault Diagnostics Flow Chart

Issue discovered → Issue logged with 1st line support → Issue data capture

- Multiple people and/or systems affected?
  - Yes → Investigate site/PC, local system issue
  - No → Local hosted system issue only?
    - Yes → Known service issue?
      - Yes → Report as known issue
      - No → Internet application(s) affected?
        - Yes → Entire site network is down?
          - Yes → Site has power?
            - Yes → Resolve electricity supply issue
            - No → Site otherwise normal?
              - Yes → Resolve flood/fire or other site issue
              - No → Are other HSCN/TN services working?
                - Yes → Transition Network (TN) site
                  - Yes → Log fault with BT
                  - No → Log fault with CN-SP
                - No → Are Internet services working?
                  - Yes → Issue replicated cross ISPs?
                    - Yes → Raise issue with application provider
                    - No → Issue persists without a proxy?
                      - Yes → Log fault with local ICT - Proxy Issue
                      - No → Confirmed HSCN/TN application(s)
                        - Yes → Local Internet Service?
                          - Yes → Raise fault with local Internet provider
                          - No → Issue replicated cross ISPs?
                            - Yes → Raise issue with application provider
                            - No → Issue persists without a proxy?
                              - Yes → Log fault with local ICT - Proxy Issue
                              - No → Issue replicated cross ISPs?
                                - Yes → Raise issue with application provider
                                - No → Issue persists without a proxy?