

LOCATING NETWORK PROBLEMS

Common Causes of Network Problems

Accepting that other causes of *network* problems exist, the two most common of problems on a wired network are faulty *hardware* and virus infection. Although one could be forgiven for thinking that these issues would only affect individual PCs, they can in fact both have very wide-reaching consequences; for example, a damaged network cable on a single computer can bring an entire network to a halt. *Wireless* networks are equally prone to these threats as well as other performance-degrading factors.

Performance Monitoring

You may already be familiar with the Windows Task Manager, a background utility which identifies which processes are currently running on a computer and lists basic performance .

Task Manager can be accessed by right-clicking on the Task Bar (the list at the bottom of your screen showing all open applications) or by pressing **Ctrl+Alt+Del** together. It is useful to familiarise yourself with what the statistics reported in the Task Manager mean, especially the CPU Usage and

Network Utilization – even if you don't fully understand what they mean, as they can be the first step in identifying the location of a problem.

Other operating systems (e.g. Linux, Apple Mac) like have similar tools (e.g. Activity *monitor* on Mac OS X accessed via Applications -> Utilities).

CPU Usage identifies how much the computer/server's CPU (Central Processing Unit, or "brain" – is working). The higher the number, the more it is doing.

Network Utilization states how much data is being sent over the computer's network connection. There are no "correct values" here and they will fluctuate as the network is used, but it can be helpful to know what is normal for your network so that you know when something abnormal is happening. You should record these values for a variety of workstations and your servers.

Layout

In order to trace the source location of a problem on your network, it will be necessary to know how the network is laid out, in terms of which switches serve which PCs and how they are connected to each other (include diagrams)

Record-Keeping

It is important to keep a record of the information gathered above for future reference, updating it each time a major change is made (e.g. new PCs or

more *software* added). Remember to print this record out, as it may be inaccessible at the time of crisis if the whole network becomes unavailable.

Tracing the Problem

When a problem occurs on your network, the process of identifying it should be considered as a two-stage process. Firstly, one must locate the source of the problem, i.e. the faulty PC or device, and then identify the cause, i.e. what is wrong with that equipment (this article just addresses the first of these two stages).

Server reboot

In the event of total network failure, a good first step is to restart the server; this is far from a guaranteed fix, however will address a large number of possible problems. If the problem persists after the reboot, have a look at the Windows Task Manager and compare the current figures to those identified in the base lining described earlier in the article. If the server is functioning normally, then the problems resides elsewhere on the network.

Identifying the problem device

If a server reboot has not cleared the problem, or if it is localised to one specific area of your network (e.g. all the PCs in one office), then the problem most likely resides with a specific device so the next job is to identify exactly which one.

Note - if the problem is a localised one, then the following steps need only be taken on the *switch* which is serving the affected PCs, otherwise they should be carried out on the main switch (i.e. the one into which the server is connected).

In order to identify the exact location of the problematic device, you should start by restarting the main switch (using the power button on it if present, or simply removing the cable from the back for ten seconds or so) and see if the network returns to normal. If it does not, then remove all the network cables from the main switch, restart it again and then re-connect the cables one-by-one, testing the network performance after each one by connecting a PC to the main switch and attempting to access files on the server. In doing this, it should be possible to identify which cables cause the change in network behaviour.

Using the network diagrams gathered earlier, identify the device to which that cable connects, as that is the source of the problem. This cable could be connected to just one PC, in which case the source has been identified, or it may connect to another switch serving a number of PCs. If this is the case, then the process must be repeated on that second switch until the problem has been traced to a single PC.

For more detailed information on diagnosing individual computers, see the KnowledgeBase article “Network Troubleshooting – Workstations”.

Problems Specific to Wireless Networks

Wireless networks can experience many of the same problems as a wired network, since they share many common characteristics, however there are a number of additional factors which can affect their performance, the biggest of which is the strength of the radio signal. The strength of a wireless signal can be seen by looking at the indicator in the system notification area, that is, the collection of small icons by the clock in the corner of the screen.

As the computer and wireless access point get further apart, or as more obstacles (e.g. walls, desks, filing cabinets) get in the path, the signal between them weakens causing a slower transmission and eventually data loss or corruption. Interference from other electrical equipment, especially microwave ovens, can also have an adverse effect on signal strength.

When placing access points and, where possible, wireless computers, it is important to consider the signal strength and work to minimise the disruption as much as possible. If a wireless network is experiencing generally poor performance, it would be worth placing more access points around the building and/or boosting the signal with the use of additional or larger aerials (note that not all devices allow for this).

Tracing an Intermittent Problem

Intermittent problems are one of the hardest to identify, as their cause – and sometimes resolution – are harder to trace. This does not, however, mean it is impossible. Desktop computers, laptops and servers all keep a record of various problems and notifications in the Event Viewer (in Windows, accessible from Start > Control Panel > Administrative Tools > Event Viewer). The Event Viewer logs both positive information e.g. “Virus protection software is up-to-date” as well as negative, so should you focus on the Error and Warning notices and disregard the Information ones. Again, other operating systems will have similar tools.

Minimising the Impact of Network Problems

While some problems can neither be avoided nor predicted, there are some simple steps which can be taken to reduce the likelihood of problems and to minimise their impact when they do occur.

Spare parts

If possible, it is advisable to keep a small collection of spare parts which can be used in times of crisis. At the very least, keep a spare network switch as it could take your supplier a few days to get you a new one, during which time some or all of your network would be unusable; having a spare switch, even a very cheap and

basic one, would allow you to keep operating while a more suitable permanent replacement were found. Similarly, an old PC could be kept in reserve for use whilst one of your others was being repaired or replaced.

Closing Remarks

This article is by no means an exhaustive list of all the problems which your network could experience, however it serves as a basic guide to the more common problems and will hopefully enable you to cope them should they arise, saving you the time, inconvenience and the potential cost of a call to your regular support provider. Even if it doesn't fully resolve your problem, it may offer your support provider valuable insight into the problem, reducing the total time, and cost, of finding a solution.

Source: <http://www.ictknowledgebase.org.uk/networkproblems>