



## Information Sheet 500 Network Analysis Service

Unique to 500 Limited is its Network Analysis Service utilising 500's 'VoIP Doctor' system. This dedicated Linux-based product can be installed at a client's site to be employed prior to installation to ensure a network is VoIP-ready. In addition, it can be used post installation for continued pro-active monitoring of both your local and wide area networks and associated devices and can be configured to send automated alerts. This enhanced aspect of our service includes:

- Network Discovery
- Benchmarking & Faulting Assessment
- Traffic Analysis
- Issues & Recommendations
- Network Topology Diagram
- Utilisation Assessment
- Traffic Generation
- Summarised Report

This information sheet is designed to provide a brief overview of the functionality provided.

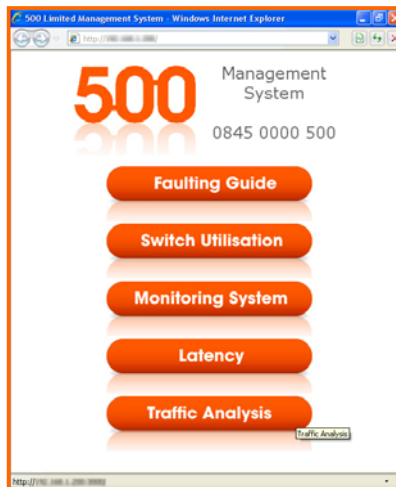


Figure 1 Web-based front-end menu

### Discovery...

Our engineer attends site to map the network topology using enterprise grade industry recognised tools. A combination of the generated 'street map' of your network coupled with our skill-sets mean that we can then quickly identify any potential problematic 'streets', pressure points or areas of congestion.

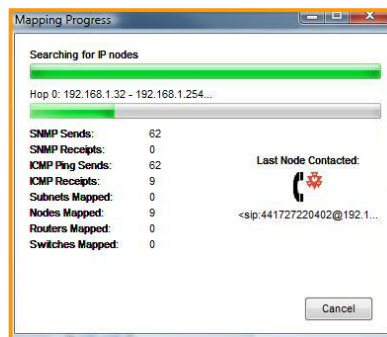


Figure 2 Network discovery in progress

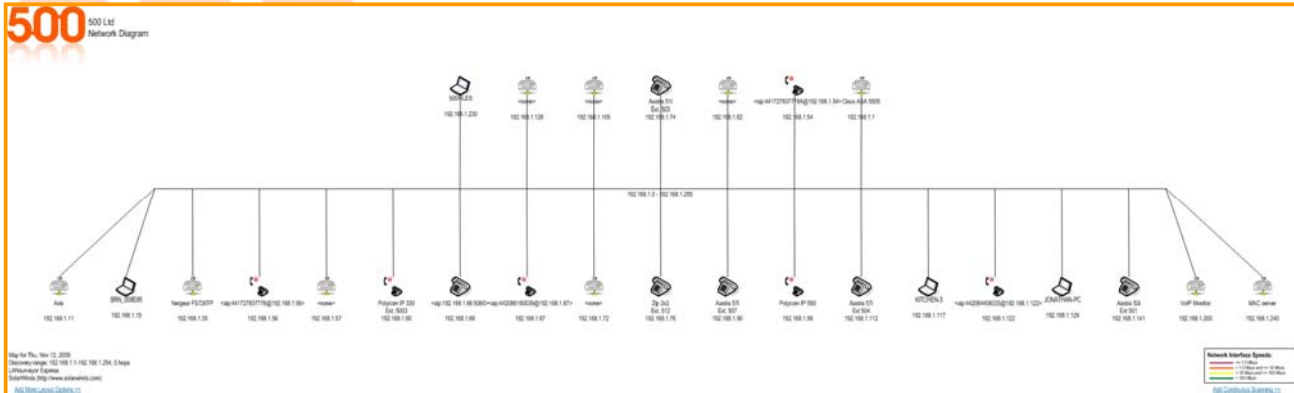


Figure 3 Resulting Network Topology Diagram

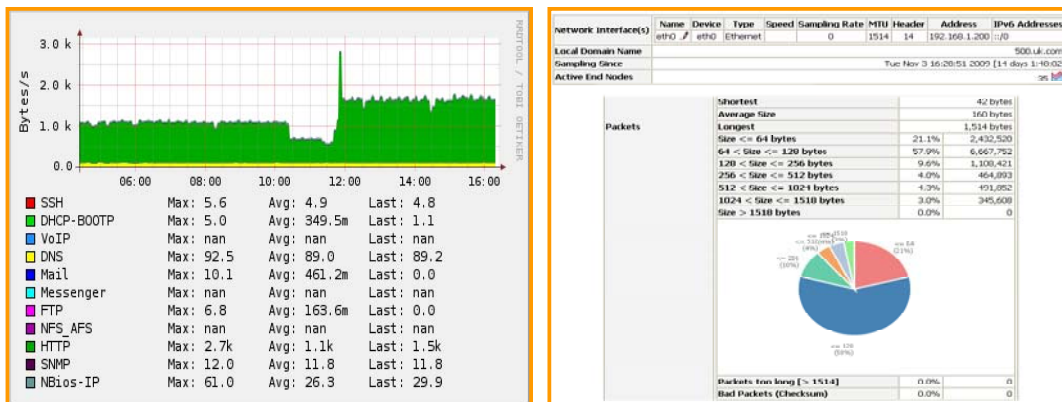
**"85% of networks are not ready for VoIP.  
What's even more shocking is that 75% of companies that do not perform  
a pre-implementation analysis of their network infrastructure  
will not realize a successful implementation"** [Gartner, 2008]

## Utilisation...

With an accurate 'street map' produced and any areas that require attention identified, benchmarking and assessing throughput with port scans and traffic traces indicate problematic areas.

The system is left in place to 'soak test' which builds up a picture of your network utilisation over time, ideally at least one week's activity cycle in order to baseline typical network utilisation. This allows us to identify, for example, irregular traffic bursts which in turn may allow additional network optimisation recommendations to be made.

'Drilling down' further, we can view the volume of each type of traffic and its purpose, identifying its legitimacy and any potential cause for concern. Where applicable we can then identify the top five issues or recommendations relating to VoIP.



Figures 4a-b Utilisation by traffic type

## Traffic Analysis & Generation...

Optionally, we can use tools to generate the level of traffic that VoIP produces. This enables us to obtain advance true to life figures regarding network quality in order to assess if common VoIP-related issues that can occur, such as latency/jitter. Regardless, our ability to analyse traffic type and volume allows us to quickly identify which network hosts are responsible for the lion share of traffic.

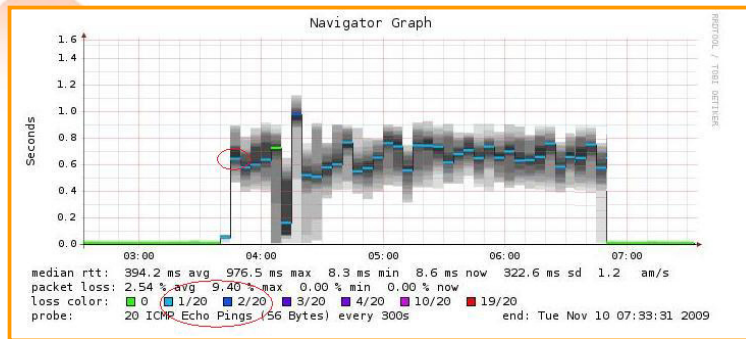


Figure 5 Latency graph

Network Traffic [All Protocols]: All Hosts - Data Sent+Received														Data: [ All ] [ Sent Only ] [ Received Only ]						
Host	Domain	Data	TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI	IPv6	STP	IPSEC	GSPF	IGMP	Other	
blackbox		867.9 MBytes	53.7 %	752.6 MBytes	69.3 MBytes	45.2 MBytes	0	0	0	0	882.2 KBytes	0	0	0	0	0	0	0	0	0
0.0.0.0		324.6 MBytes	20.1 %	322.5 MBytes	428.1 KBytes	0	0	0	0	0	1.6 MBytes	0	0	0	0	0	0	0	660	0

Figure 6 Traffic analysis by device/host

## Monitoring...

Our status map provides an instant visual object-orientated view of your network, detailing how your network is connected and clearly identifying if a single failure in a chain is causing underlying devices which may also be flagged as failed.

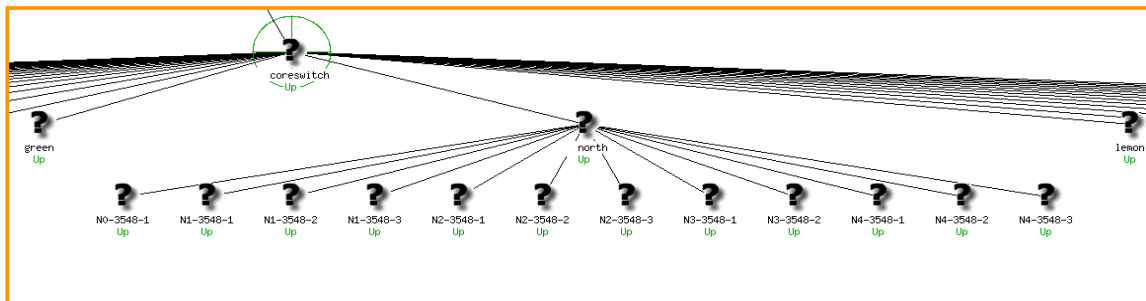


Figure 7 Status map

## Non-disclosure...

As a thorough network analysis of this type requires unencumbered access to a client's network, we voluntarily sign a non-disclosure agreement prior to assessment. In addition, we also advocate an in-house IT resource 'shadow us'. We can also supply engineers that are bound by the Official Secrets Act 1989 and are 'SC Cleared' (that is, Security Cleared by the Government Defence Vetting Agency, the security clearance level required to access government and military networks).

## Contact...

If you have any questions please contact us on 0845 0000 500 (option 3) or email us at [info@500.uk.com](mailto:info@500.uk.com).

## Document history...

Date / Ref.	Author	Change
01/10/2009	DH, SR	First approved release.