

Onsite Analysis Report

Network Health and Design Report
for XYZ Company

1	Background.....	3
2	Overview	3
3	Network Design	5
4	Analysis.....	6
4.1	General Network Health	6
4.1.1	Utilisation	6
4.1.2	Protocol Distribution.....	8
4.1.3	Packet Size Distribution	9
4.1.4	Top Talkers	9
4.1.5	Traffic Map.....	10
4.1.6	Network Error Reports	10
5	Recommendations.....	11
5.1	Network Design	11
5.1.1	Network Segmentation	11
5.1.2	Core Design	11
5.1.3	Resiliency Protocols.....	13
5.1.4	Security.....	13
5.2	Remote Users	14
5.3	Wireless.....	14
5.4	General Development	14
5.4.1	IP Addressing	14
5.4.2	Print Servers	14
5.5	Network Management	15
5.5.1	Standardisation	15
5.5.2	Remote Administration	15
5.5.3	Network Monitoring.....	15
5.6	Training	16
6	Appendices	17
6.1	Recommended Kit List	17
6.1.1	Core Switches	17
6.1.2	Server Switch.....	17
6.1.3	Access Switches	17
6.2	Installation.....	18
6.3	Switch Configuration Recommendations.....	19
6.3.1	VTP.....	19
6.3.2	Spanning Tree	19
6.3.3	VLANs and IP Addressing	19
6.3.4	HSRP.....	19
6.3.5	DHCP	19
6.3.6	Static Routes.....	19

1 Background

The purpose of this report is to provide a detailed state of the network at this point in time and provide a recommended design for the local area network moving forward.

The network at XYZ Company was installed approximately 5 years ago when the organisation moved into the current building. The network has been added to as required over the years. However, there has not been a formal design that has been adhered to in the ongoing network development.

It is the desire of the IT department at XYZ Company to develop a network which can be easily managed, maintained and understood by the department. From discussions with the IT Department the areas of focus were:

- Network Segmentation:** The network is currently using a flat structure which is not optimal for a network of this size.
- Security:** The ability to have differing levels of security for different areas of the network.
- Wireless:** The future implementation of wireless services must be considered in the network design.
- Network management:** There is currently no real way to manage the internal network infrastructure. The design should provide the ability to manage and monitor the network.
- Resilience:** There is an acceptable network downtime of up to 30 minutes, but periods longer than this should be avoided.

2 Overview

The local area network at the Dover Street site is composed of a switch cabinet on each floor. Each cabinet contains the patch panels for the floor and up to three switches. Each cabinet is connected to the Core Switch cabinet in the basement by 6 fibre pairs. Currently only 2 fibre pairs are in use at a time.

The Access switches on each floor have no automated resilience, in the event of a failure on a fibre link the switch would need to be re-patched to a different fibre pair. The network core also has no automated redundancy, in the event of a core switch failure the second core switch is available to be connected to the access switches.

In general the switches have no configuration at all on them. The 3500XLs have IP addresses in the 192.168.0.0/24 range configured on VLAN 1. No switches are configured with passwords or for remote administration.

It was identified that there are a number of different user types on the network:

- Lab Users: Non corporate equipment on corporate network
- Non Commercial users (Advertising, Accounts)
- Commercial
- Boardroom & Wireless: A Mix of Corporate and external users
- IT Department
- Production

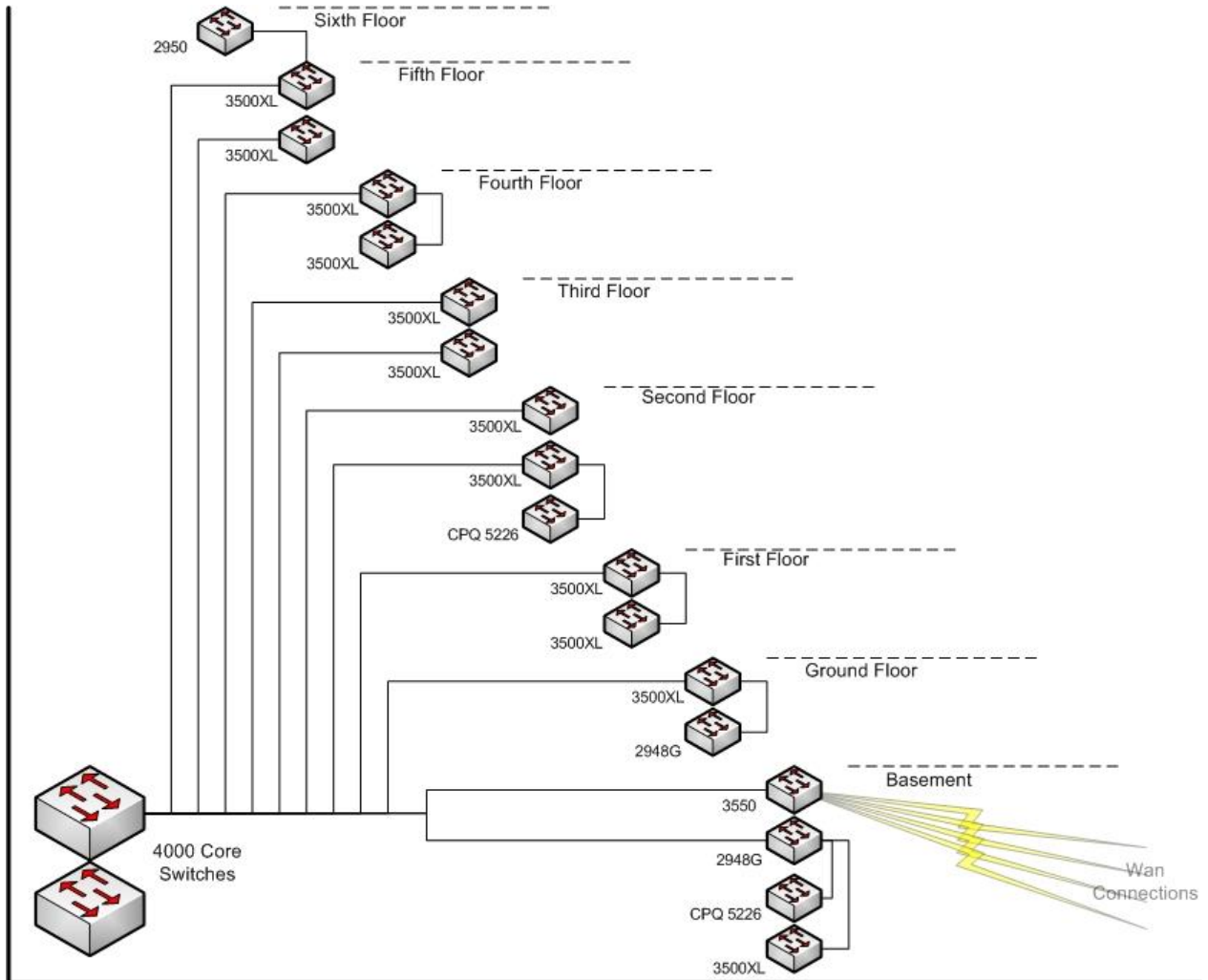
The following table provides a breakdown of the switches, software versions and port utilisation.

Floor	Switch	Model	Software Version ¹	Hardware Modules	No Ports	No Patched	No Active
6	N/A	2950	2950-i6q4l2-mz.121-9.EA1	N/A	24	22	13
5	Top	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	35	30
5	Bottom	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	23	21
4	Top	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484 WS-G5484	48	38	31
4	Bottom	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	43	31
3	Top	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	47	42
3	Bottom	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	42	35
2	Top	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	48	29
2	Middle	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	45	29
2	Bottom	Cpq 5226	Unknown	N/A	24	24	12
1	Top	3500XL	c3500XL-c3h2s-mz-120.5.2-XU	WS-G5484	48	45	36
1	Bottom	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484 WS-G5484	48	43	34
0	Top	2948G	cat4000.4-5-3	GLC-SX-MM GLC-SX-MM	48	14	12
0	Bottom	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	48	33
-1	Top	3550	Unknown	WS-G5484	48	48	47
-1	Middle 1	2948G	cat4000.4-5-3	GLC-SX-MM	48	45	28
-1	Middle 2	Cpq 5226	Unknown	N/A	24	22	13
-1	Bottom	3500XL	c3500XL-c3h2s-mz-120.5-XU	WS-G5484	48	16	7
-1	Top	4003	cat4000.5-1-1a	WS-4012 WS-4306-GB WS-4306-GB	12	12	0
-1	Bottom	4003	cat4000.5-1-1a	WS-X4012 WS-4306-GB WS-4306-GB	12	12	12

¹ It should be noted that due to the cabling and switch locations, it was not possible to access all of the switches without uncabling, and this was not appropriate. In these cases the software versions are listed in red.

3 Network Design

Below is a diagram showing the current network design



As previously mentioned the network is based around a flat network with access level switches on all floors. Each switch is connected to the Core switch via fibre cables. A second core switch is available in case of failure for a manual failover.

4 Analysis

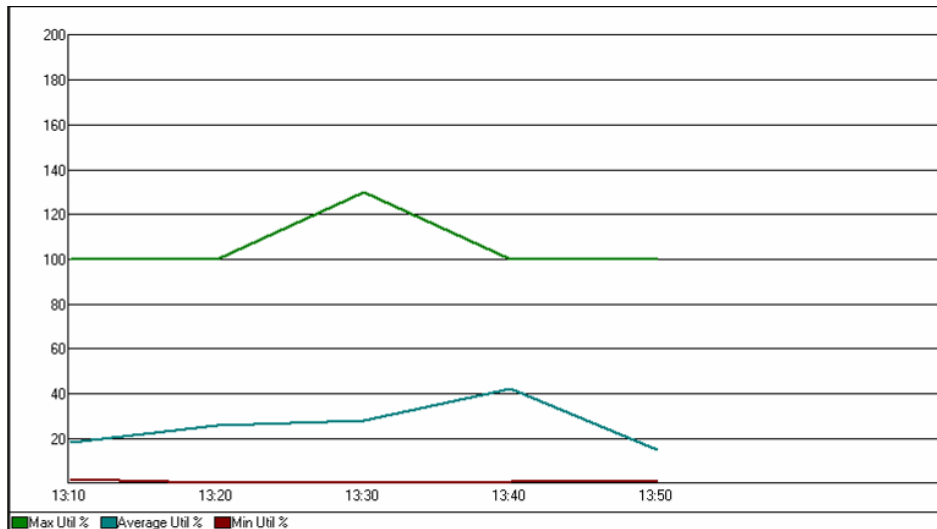
4.1 General Network Health

The following sections provide an overview of the general health of the network. It should be noted that this data is a snapshot of information and can only provide a baseline of the network at that point in time. For a greater understanding ongoing monitoring should be performed to understand how the network performs a various times during the day.

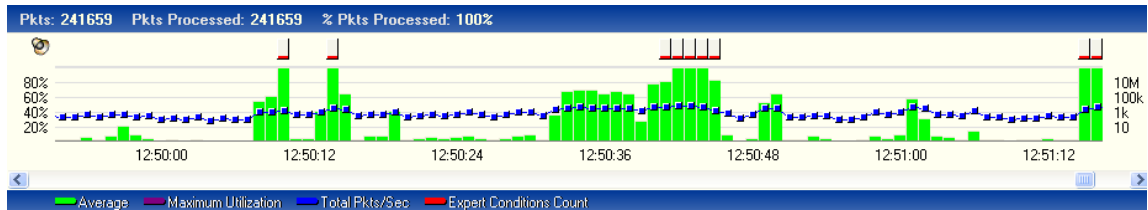
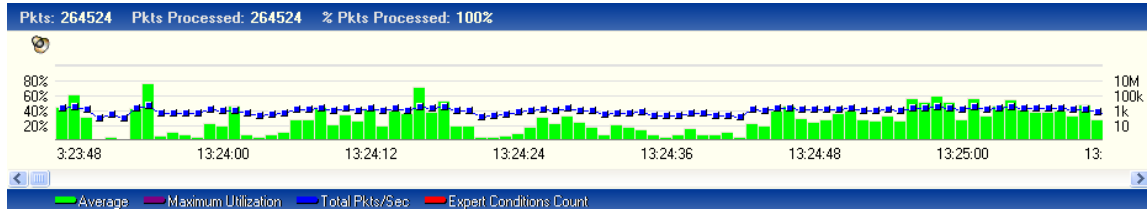
The analysis was performed by connecting a laptop to the Cisco 2948G switch in the basement. Network Observer was used to collect the data. The monitoring was performed on VLAN1 (the default segment to which all the systems connect). Two functions on the application were used, Network Trending was run for the whole monitoring period and the Packet Capture was used to collect a number of snapshots of network data over the monitoring period.

4.1.1 Utilisation

The network utilisation on average is running between 20 and 40%. This is acceptable for normal network, however, it should also be noted that the network is regularly peaking at high levels. If the network utilisation is high, user will start to see lower response times, intermittent errors and disconnections. To avoid this occurring in the future additional capacity should be identified now.



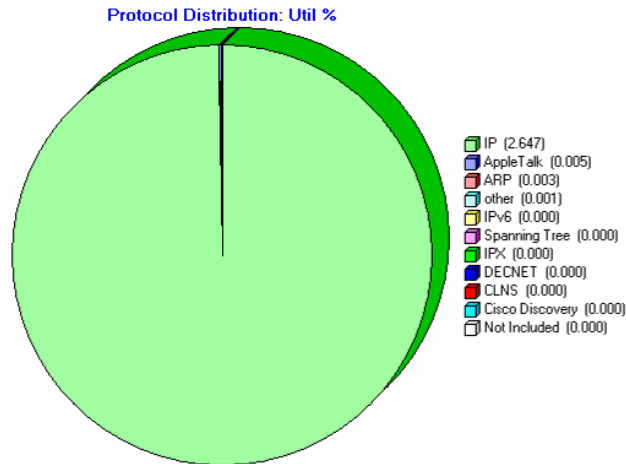
The following 2 graphs are captures from the packet capture application that was used to monitor the network. The top trace shows that the general network usage at an acceptable 40%. The second trace shows the peaks that are occurring on the network. As they are short lived there will be little effect on the users, however, as network usage increase over time the situation will only deteriorate.



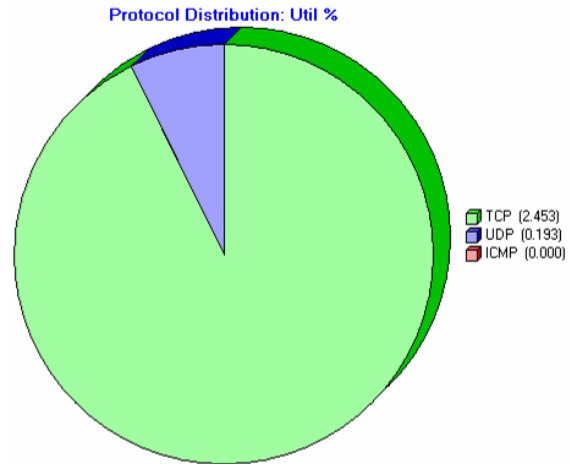
4.1.2 Protocol Distribution

The charts below detail the distribution of the protocols on the network. The vast majority of the traffic is either "Microsoft-DS" or the "Other" classification. Looking further into the data it is suggested that this traffic the Microsoft-DS traffic is Windows File and Print traffic. The "Other" traffic is mainly "AFP over TCP" which the AppleTalk protocol running within TCP, also accessing file and print data.

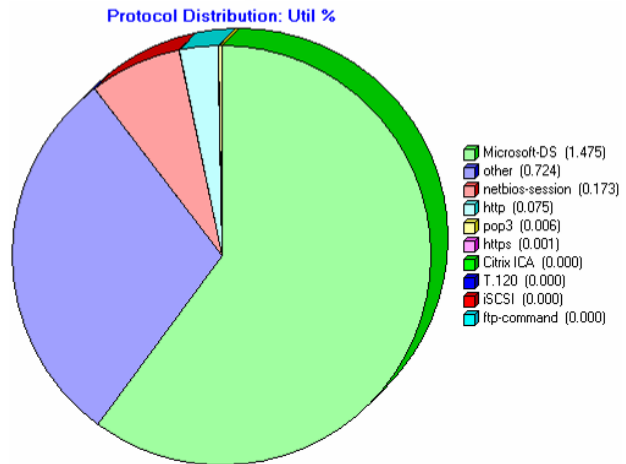
All Protocols



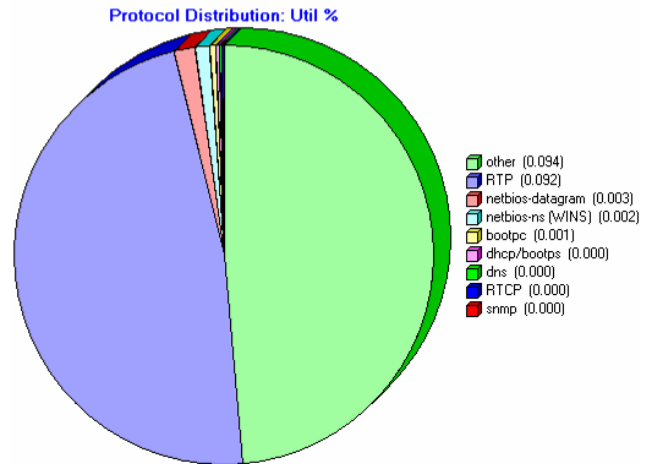
IP Protocols



TCP Protocols

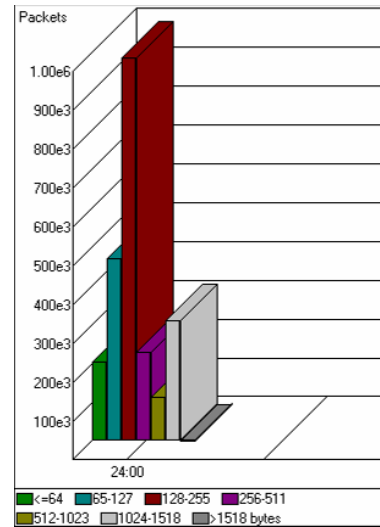


UDP Protocols



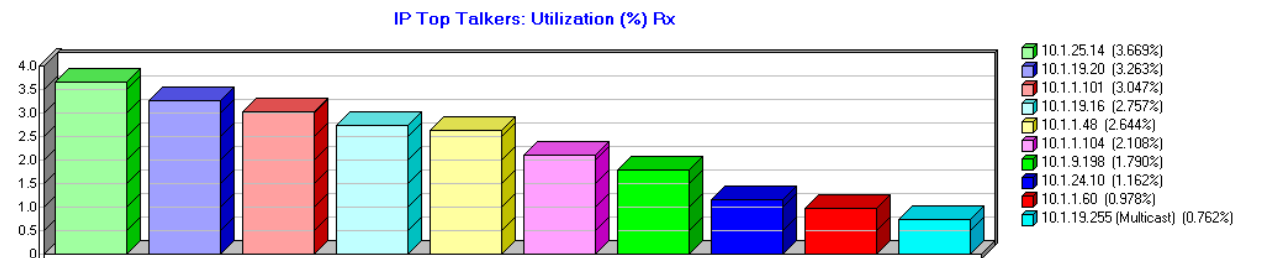
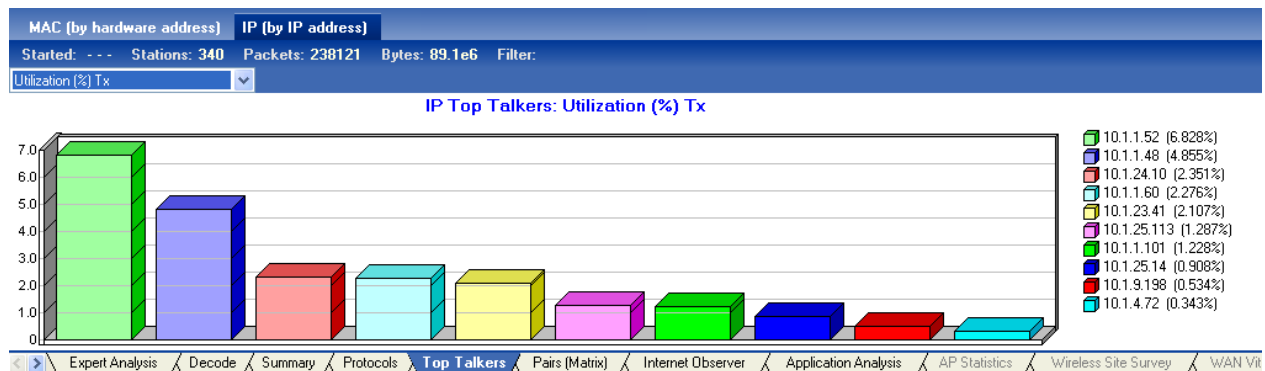
4.1.3 Packet Size Distribution

This graph shows the distribution of Packet size on the network. This shows that there is not a high proportion of runts or giant on the network (small or large packets), so there is not a concern.



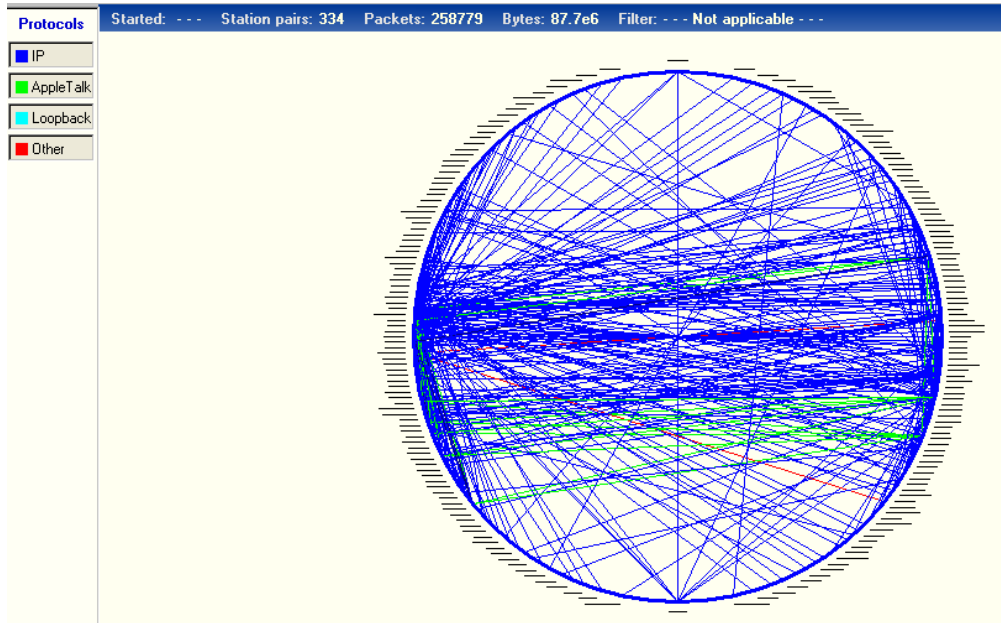
4.1.4 Top Talkers

The following graphs provide details of the top talkers seen on the network. You would expect that the servers are commonly the busiest nodes on the network. In the event that specific nodes regularly appear in this list then additional analysis may be required.



4.1.5 Traffic Map

Due to the complexity of the network connections and the number of nodes on the network segment, the traffic map is not particularly useful, however, it is included here for interest.



4.1.6 Network Error Reports

During the monitoring a number of errors were reported, an example of which are:

Network Conditions Summary	
Problem ▲	Count
ICMP Destination Unreachable	5
ICMP Redirect	1
Maximum utilization exceeded 80.0% (times)	22
TCP excessive retransmissions	1
Too fast TCP retransmissions	2
UDP excessive retransmissions	1

The main issues suggested are the network utilisation. Once again although it may not be an issue the users are aware of at the moment in the future they may be affected in the future. The remaining errors are ICMP errors which are not unusual for a network of this size. The retransmission are, also, not unusual for a network of this size and are likely to be caused by the spikes of high utilisation.

5 Recommendations

5.1 Network Design

As discussed above the current network design is based around a flat network structure. This type of network is only really suitable for small networks. As XYZ Company is now in the region of 300-400 nodes, a flat network design is not really suitable.

Some of the restrictions on a flat network design are:

- High numbers of broadcasts and ARP requests on the network cause increased utilisations on switches and computers
- Unable to effectively implement advanced features such as security, quality of service, VOIP
- Difficulty in implementing network management

5.1.1 Network Segmentation

In medium to large networks, the recommendation is to implement a hierarchal solution segmenting the network into separate areas (VLANs) these areas are connected via high performance routers or layer 3 switches. The segmentation of the network into VLANs can be customised to your requirements some common configurations are:

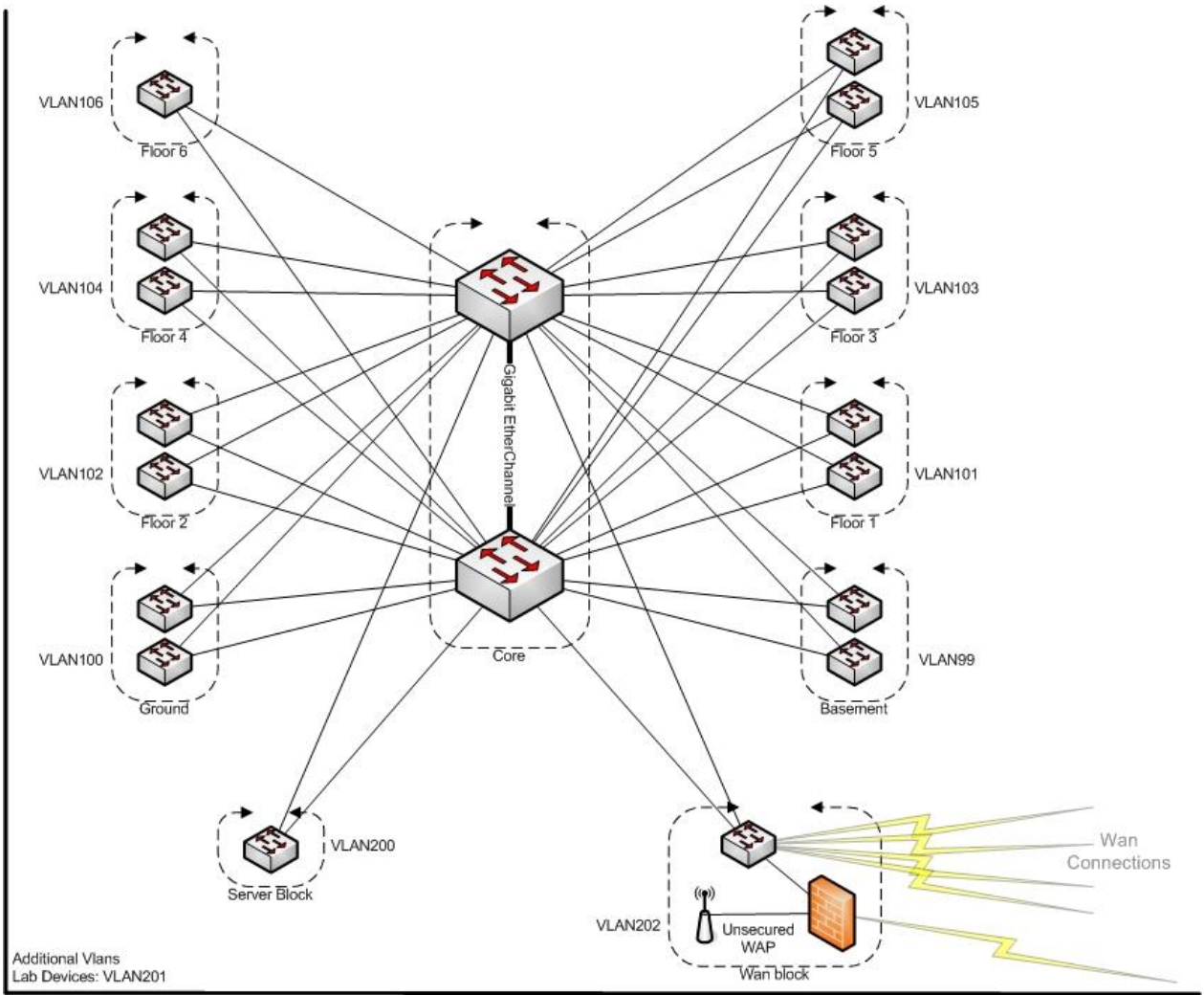
- Location: Building, floors
- Business Units: Accounts, Sales, etc.

After discussion with the IT department, it was felt that, segmenting the network to the level of each magazine would result in a complicated network requiring too much administration for moves and changes. In this case a better option would be to the segment the network into VLANs around floors. Additional VLANs can then be added for Servers, Network management, Lab systems etc.

5.1.2 Core Design

The recommended design for this network would be a "dual collapsed core" as this provides a resilient and high performance network. The Diagram below shows a recommended structure for this type of network. This provides a resilient structure which can support the failure of either a core switch or a switch connection to the core. In the event of either of these failures, the infrastructure will, within 60 seconds bypass the failed device or connection and the network will continue to work without interaction from the IT department.

In addition separate VLANs have been added to the structure to separate the servers and the WAN connections from the rest of the network. This allows security and other access restrictions to be implemented as required between each section of the network.



5.1.3 Resiliency Protocols

To allow the new network design to perform correctly, a number of network protocols would need to be run to ensure that the switches and the users can access the network at all times.

- Spanning Tree: Each floor switch will be connected to both core switches, if both of these links are active at the same time there is a risk that a loop will form and data could be lost within the network. To avoid this occurring spanning tree should be configured on the network. This will ensure that only one link is used at a time and in the event of a link failure it will automatically change over to the redundant link.
- Port fast and Backbone fast: To ensure that spanning tree correctly uses the links on the network, each port should be configured with the correct setting. Uplinks should use backbone fast and the access links should use port fast. This will ensure that the ports can be used as quickly as possible in the event of a network change.
- VTP: To ensure that the configurations of the VLANs are consistent across the network VTP should be used. This allows a switch to be designated as the server and all maintenance of the VLANs can then be completed on that switch. The changes will then propagate to the remaining switches.
- HSRP: The hot standby routing protocol is used to provide a consistent default gateway to the users in the event of a core switch failure. In this design, the core switches will act as routers switching IP traffic between the VLANs. As a result of this each VLAN will need a default gateway to use to connect to the other VLANs and the internet. To avoid each core switch having its own IP address, HSRP is used to provide a virtual IP address in each VLAN for use as a default gateway.

5.1.4 Security

The security of the network is currently very open. The internal security is being implemented by the servers and active directory permissions. This is in general an acceptable solution. However, in the XYZ network there is one user type which, it is considered, may require restricted or more closely monitored access.

The Lab users receive external systems from suppliers for testing and analysis. These systems could accidentally bring viruses, trojans and other malware into the network. Although there are currently no restrictions on these users there may be a requirement in the future. There are three ways of addressing this need:

- Restrict access via access-lists: If the lab users are segmented in their own VLAN a separate set of network permissions can be allocated to these users, which would restrict their access to network services. For example, the lab users should not have access to the accounts server so the switches could be configured to restrict access to these servers.
- Monitor/ Manage Data with a firewall: If a higher level of control is required on the network a firewall or similar device could be deployed to restrict the types of traffic that entered the corporate network from Lab VLAN. A device such as the Cisco ASA 5500 could be used, this would provide transparent firewalling, anti-virus and intrusion prevention services on the connection into the corporate network. These services could be provided in an almost transparent manner which would be invisible to most users.
- Clean Access: This is an easily deployed software solution that can automatically detect, isolate, and clean infected or vulnerable devices that attempt to access your network. It identifies whether networked devices such as laptops, personal digital assistants, even game consoles are compliant with your network's security policies and repair any vulnerabilities before permitting access to the network.

5.2 Remote Users

There are a number of remote users, a few users VPN to access the network via the sidewinder firewall. The remainder are based in the branch offices and connect over the leased line connections. Although at this stage we are not recommending increasing the security on these areas, the network design can be used in the future to add these restrictions.

5.3 Wireless

Wireless was identified as an area in which development was required. Wireless is an inherently insecure method of access a corporate network as the traffic and access cannot be controlled to keep it inside the building. Because of this, the security is something that will need to be examined. At XYZ Company it was identified that there are two differing requirements. Firstly, the Boardroom, here users are external users who primarily need access to the internet. Secondary, on the second floor there is a requirement for internal users to have access to the corporate network. These requirements would require differing security configurations.

Network Connections

Second Floor: Connect directly into the network, second floor VLAN
Boardroom: Should be connected to a DMZ

Security

Configuration of wireless security is a trade off between security and functionality. The following are a series of recommendations. A decision will be required on the security configuration and what compromise is acceptable to the users and the IT department:

- Change Standard SSID
- Disable SSID Broadcast
- Enable Encryption (WEP or WPA)
- Restrict Access via MAC address
- Use 802.1x and external authentication to control access
- Locate the AP Externally and require corporate users to connect via an IPSEC VPN.

5.4 General Development

5.4.1 IP Addressing

It was identified that the IP addressing on the internal network is currently provided via static IP. With the implementation of the VLAN structure this will be come an onerous task to maintain the different subnets. For a network this size DHCP should be used to allocate IP address. A central DHCP server can be used to provide the IP addresses for all VLANS and will provide the correct IP addresses and setting as they are requested.

5.4.2 Print Servers

The current environment has no print servers and all printers are manually configured on each PC. This results in a lot of additional configuration and management that could be simplified. One or more print servers should be configured. These could then manage all prints going to the printers and would allow PCs to browse for available printers without having to configure each one with an IP address and driver. We would also recommend that the printers are provided with a static IP address on the management VLAN (or a printer VLAN if required). As this would easier management as the printers are then segmented from the user systems.

5.5 Network Management

5.5.1 Standardisation

The currently installed switches come from 2 manufactures, Cisco and Compaq. The Cisco switches installed run 2 totally different operating systems, IOS and the older CatOS. The recommendation would be to remove or replace the Compaq and the Older CatOS switches. This would result in the IT Department only having a single set of commands to use and understand.

The IOS version installed on each switch should where possible be standardised for each model. This permits easy maintenance of each device and allows any spares to be ready for use to replace any similar switch.

5.5.2 Remote Administration

Each switch is capable of being managed remotely, depending on the age this can be completed via Telnet, Web or via an external management application. As a first step, all switches should have a management IP address configured and usernames and passwords setup for administration. This would ease the administrative burden as changes can be made from a central location.

As a next step, an external management application could be considered to provide a central console for managing the internal switches. An example of this is CiscoWorks or the Cisco Network Assistant².

5.5.3 Network Monitoring

There are two real requirements on the network for network monitoring and analysis, trending and sniffing. The recommendation would be to use an application that could permanently monitor network use and collate statistics on usage. This could then be used for capacity planning and analysis. The second function required is network sniffing, if a fault occurs on the network it is important to quickly be able to see what is actually occurring on the network and collect that data for later analysis.

An example of an application that would provide these functions is Network Instruments Observer. It also has the advantage that it can provide expert analysis of network errors which the packet sniffer has observers and therefore, can make fault finding significantly easier.

This application should be installed on a dedicated workstation connected to the network for monitoring. Then in the event of an issue it is ready for use with out the need for additional preparation

² The Cisco Network Assistant 2.0 is available as a free download, however, it does have a number of restrictions on the number and model of devices. So, long term it may not be a suitable solution.

5.6 Training

Because the network design would substantially change there are a number training requirements that would need to be covered to permit the IT department to continue the management of the network.

- Desktop Moves and changes: How to move a user within a floor and between floors
- Maintaining VLANs: If a new VLAN is required, IT should be able to add the VLAN and then configure the correct switch port to use the VLAN
- Software upgrades: Ability to upgrade software on the switches to a new version
- Configuration Maintenance: Backup, and replace configurations on switches allowing replacement and disaster recovery
- Monitoring: Configuration of SPAN and RSPAN to permit the monitoring of network traffic
- User accounts: Addition and removal of user accounts, password changes
- Network Monitoring Application: Basic use of the network monitoring application

In addition the IT department suggested the following areas of training. These areas could be used for further training as they depend on in depth networking knowledge and understanding which would be developed as the understanding of the network increases.

- Ability to anticipate issues (capacity planning)
- Implementation of a warning system for issues
- Maintenance procedures
- Identification of bottlenecks

6 Appendices

6.1 Recommended Kit List

The following is a kit breakdown of what would be required to implement the solution details above.

6.1.1 Core Switches

Upon investigation the Cisco 4003 chassis cannot support the required upgrade to a higher performance supervisor module. The minimum Supervisor module that would be required is a Supervisor Engine II-Plus. However this is only supported in the 4006 chassis and above. Hence to implement this solution the core switches would need to be replaced with 2 Cisco 4500 switches.

The recommended switch chassis would be a Cisco 4506 providing 6 slots, this will give expansion in the future if required. The current WS-X4306-GB would be reused in the new chassis, this will provide the required 18 1000-SX ports required.

Description	Part Code	Quantity
Catalyst 4500 Chassis (6-Slot),fan, no p/s	WS-C4506	2
Catalyst 4500 1400W AC Power Supply (Data Only)(Spare)	PWR-C45-1400AC=	2
Catalyst 4500 Supervisor II-Plus (IOS), 2GE,Console(RJ-45)	WS-X4013+=	2
Catalyst 4500 Gigabit Ethernet Module, 6-Ports(GBIC) (Spare)	WS-X4306-GB=	2
1000BASE-SX Short Wavelength GBIC (Multimode only)	WS-G5484=	12
SC to ST Fibre Optic Patch Cables	N/A	12

This specification is based on connecting 16 switches to the core switches and using 2 connections for uplinks between the switches. If additional capacity is required additional WS-X4306-GB cards, GBICs and cables would be required.

6.1.2 Server Switch

The servers switch block should provide a minimum of 24 10/100/1000 ports to permit the migration of the current servers over to gigabit network cards.

Description	Part Code	Quantity
Cisco 3560G-24TS-24 Ethernet 10/100/1000 and 4 SFP	WS-C3560G-24TS-E	1
Gigabit Ethernet SFP, LC connector, SX transceiver	GLC-SX-MM=	2
LC to ST Fibre Optic Patch Cables	N/A	2

6.1.3 Access Switches

All the current Cisco 3500XL (except one) are running version 12.0.5XU software. The most current is 12.0.5WC11 which is only a minor revision of the software. The benefit of upgrading to this new version of the software is unlikely to be beneficial unless a problem is identified.

In the network design all the switches will require 2 uplinks, as an estimate an additional 12 GBICs and Fibre cables will be required to connect the existing switches to the second core switch.

Description	Part Code	Quantity
1000BASE-SX Short Wavelength GBIC (Multimode only)	WS-G5484=	12
SC to ST Fibre Optic Patch Cables	N/A	12

It has been recommended that the switch types should be standardised, with this in mind the following breakdown is recommended.

- 6th Floor: Replace Switch with standard including fibre uplinks
- 5th Floor: Leave 2 x 3500XL in place add additional uplinks
- 4th Floor: Leave 2 x 3500XL in place add additional uplinks
- 3rd Floor: Leave 2 x 3500XL in place add additional uplinks
- 2nd Floor: Re-patch active ports to leave 2 x 3500XL in place add additional uplinks. If required add additional standard switch
- 1st Floor: Leave 2 x 3500XL in place add additional uplinks
- Gnd Floor: Leave 1 x 3500XL in place add additional uplinks, Replace 5226 with standard switch
- Basement: Re-patch to remove 5226, Leave 3500XL and 3550 in place add additional uplinks

The standard switches that are recommended would be Cisco 2948G or Cisco 3560

Replacement Access switch parts:

Description	Part Code	Quantity
Cisco 2950 Switch 48 10/100 ports + two 1000BASE-X ports	WS-C2950G-48-EI	2
1000BASE-SX Short Wavelength GBIC (Multimode only)	WS-G5484=	4
SC to ST Fibre Optic Patch Cables	N/A	4

6.2 Installation

This is a basic list of the installation process for the switched solution:

- Day 1
 - Prepare Core, server and replacement access switches
 - Configure VLANs, Etc.
 - Prepare DHCP
 - Use Spare 3500XL to prepare configurations for remaining access switches
- Day 2
 - Installation of core switches
 - Installation of server switch
 - Reconfiguration of Floor switches
- Day 3
 - Continued reconfiguration of floor switching
 - Testing
- Day 4
 - Live day
 - Onsite for ½ day to ensure that all is working as expected
- Remaining Days 1.5
 - Recommend days are put aside for training and the deployment of advanced features such as intra-VLAN security.

It is recommended that days 2 and 3 would be weekend based working to avoid disruption to the users.

6.3 Switch Configuration Recommendations

6.3.1 VTP

Domain: XYZ
Servers: Core Switch A & Core Switch B
Password: For security a password should be used

6.3.2 Spanning Tree

Primary Server: Core Switch A
Secondary Server: Core Switch B
Backbone Fast: All Trunk Ports
Port Fast: All access Ports

6.3.3 VLANs and IP Addressing³

VLAN	Description	IP Addresses
1	Network Management	10.1.1.0/24
99	Basement	10.1.99.0/24
100	Ground Floor	10.1.100.0/24
101	Floor 1	10.1.101.0/24
102	Floor 2	10.1.102.0/24
103	Floor 3	10.1.103.0/24
104	Floor 4	10.1.104.0/24
105	Floor 5	10.1.105.0/24
106	Floor 6	10.1.106.0/24
200	Server	10.1.200.0/24
201	Lab	10.1.201.0/24
202	WAN Connections	10.1.202.0/24

6.3.4 HSRP

A HSRP group should be configured for each VLAN and a virtual IP address provided for use as the default gateway (e.g. 10.1.XXX.254)

6.3.5 DHCP

A central server should be configured with an IP scope for all VLANs except VLAN 1 (which will use static IPs).

Default Gateway, DNS and Wins server should also be specified in the scopes.

6.3.6 Static Routes

No dynamic routing protocols were seen on the network. As the network is not changing on a regular basis the added complexity of a dynamic protocol is not warranted. Static routes should be configured to send data to the correct networks and to the internet.

³ The VLAN numbers and IP subnets are arbitrary values and can be changed as required. The numbers used within this document were selected for ease of use.