

## School Network Assessment August 2006

### 1.1 SUMMARY

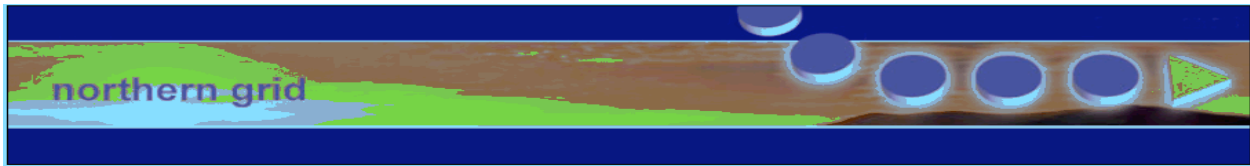
The ICT suites are well resourced and managed. Modern well-equipped workstations run the XP operating system. The user's desktop is securely locked down stopping unauthorised applications from being run and configuration changes being made. The domain login and application access times were all within acceptable levels. The network was very quiet as the assessment was conducted during the summer holiday period. DNS lookups and trace checks were all within expected tolerances. The server farm was effectively managed with a couple of notable exceptions. The web server was susceptible to attack and requires patching; some routine housekeeping tasks were not recently carried out. File systems had high levels of fragmentation RAID management software was not installed stopping effective monitoring of the RAID server array.

The Network Ranger product provides an easy to use, consistent and reliable workstation and application management solution and was effectively deployed. No monitoring or management of the network infrastructure was possible as no administration access was available. SNMP was not activated on any of the switches. The use of four mobile wireless trolleys when in use would significantly impact on the performance of the whole network, as broadcasts generated at the WAP would be propagated throughout the switch network. The wireless systems also posed a security threat as encryption and authentication was not enforced when users connect to the network.

The lack of any switch management may be allowing configuration and device problems to go unnoticed. The 3Com 4400 access switches are well specified and currently adequate as long as desktop connectivity at 100M is acceptable. The 3Com 4900 aggregation (core and distribution) switch lacks sufficient Gigabit ports and may need to be upgraded in the near future. The email and proxy filtering services are inadequate and do not fulfil BECTA requirements. The RM Easymail service lacks any inappropriate banned word list and the Freedom2teach filtering service requires manual database entry for URL filtering. Despite three levels of filtering, access to well-known inappropriate content was still possible.

The NEN connection and routing is not working correctly as Audio Networks hosted by LGfL the most popular NEN resource is not accessible. I am informed that their local RBC has routing issues. The school and ISP should ensure these issues are remedied as soon as possible. The ISP has confirmed that the utilisation of the schools 10M LES link to the Internet is low and always below 30%. Web response times, as measured by Pakateer, are within specified parameters.

Management and technical support on the LAN was of a high quality but the lack of available documentation needs to be addressed. Physical network diagrams, security policies, AUP and backup and disaster recovery solutions all need to be compiled and documented to ensure security, consistency and quality across the network.



Baselining the network and continuously monitoring for changes are critical to maximising performance, identifying error conditions and determining where future investment is needed.

## **1.2 SCOPE AND METHODOLOGY**

The following issues were considered: application and configuration management, network security, network availability and performance and administrative management. During the healthcheck a questionnaire was completed, school technical staff were interviewed. The server, workstation and network infrastructure configuration and management were assessed.

Traffic analysis would normally be adopted to assess the operational characteristics of the network under load. As the assessment was requested to be carried out during the summer holiday period it was agreed that a security and vulnerability scan would provide more useful results. The key network services of application and file storage, email, secure remote access and Internet/NEN access would be individually assessed to ensure compliance with DfES/BECTA recommendations.

## **1.3 BACKGROUND**

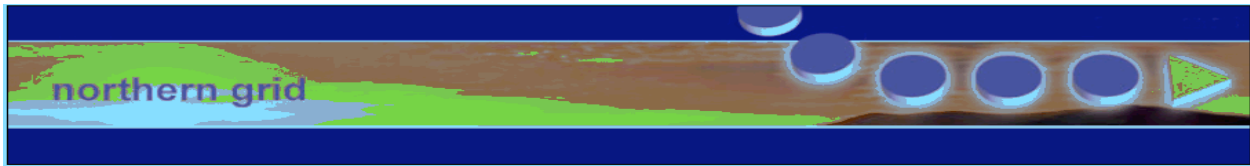
The school is a co-educational comprehensive and has approx 1073 pupils in the 11 – 18 age group. The school has over 300 static desktop PC's running the windows XP operating system. Eighty-five laptops in 4 trolleys access the network using wireless connections. All core servers operate windows 2003. Two servers are used for authentication and file storage. The remaining servers are used for providing web, exchange email and SQL database services.

The fully switched network comprises 3Com 4400 switches used at the edge to provide desktop connectivity at 100Mb. Aggregation switched services utilising 3Com 4900 at the core provided a Gigabit backbone. The topology used is that of a conventional star. No edge switch stacking was configured or required. The physical network infrastructure is concentrated within seven ICT training suites, the wireless systems facilitating school wide access to the network.

## **1.4 GENERAL SECURITY**

### ***1.4.1 Network***

Static desktops are well secured however any laptop or portable device could physically connect to the network and have IP information delivered via DHCP. To access network resources requires domain login. The 3Com 4400 can be used to suppress protocols and unwanted applications maximising bandwidth. Ports used by network games and programs can be blocked protecting bandwidth, network availability and pupil productivity.



To activate these measures requires administration access. The 3Com 4900 switch has a limited number of Gigabit ports making it a likely component for future replacement or upgrade.

### **Recommendations**

- Evaluate deploying Link aggregation (LACP), which allows doubling or quadrupling of the current uplink bandwidth by bundling two or four Gigabit ports into one logical port. LACP provides improved performance and resilience and would allow the creation of a 4G backbone due to the low number of available ports on the 4900 a replacement aggregation switch is required.

[http://www.northerngrid.org/ngflwebsite/netassess/link\\_aggregation.ppt](http://www.northerngrid.org/ngflwebsite/netassess/link_aggregation.ppt)

#### ***1.4.2 Server***

All servers are regularly updated to install the latest windows security service packs and security patches. RAID is widely deployed on the servers. Management software on one server was not installed resulting in lack of performance monitoring. RAID can recover data from a single disk failure. RAID management software monitors how well the RAID card is working in addition to the drive units. RAID card failures although rare often result in multiple drive data corruption that is unrecoverable except by tape backup.

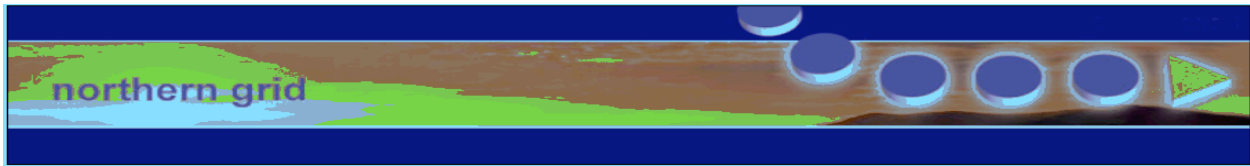
The system partition of alpha file server had 22% file fragmentation. This level of fragmentation indicates lack of general housekeeping and will impair server performance. All servers should utilise Gigabit Ethernet cards if sufficient switch ports are available. The error logs indicated a healthy server! The Active Directory had accounts that were no longer in use; these accounts should be disabled or deleted during routine maintenance.

### **Recommendations**

- Unused accounts removed or disabled.
- RAID Management software universally installed and monitored.
- Carry out routine housekeeping i.e. defragmentation, log checks, cleanup etc
- Consider installing multiple NICs to increase file server to switch bandwidth.
- Future storage should be based on SAN technology.
- Maintain the AD database check for database corruption, check synchronisation between servers and remove or disable all unused objects.

#### ***1.4.3 Workstation***

Network access required a domain login; the pupils' desktop was very secure with the control panel options were disabled. No access to the run command line was available. The C drive was protected blocking the use of applications to be used to run OS utility programs.



New pupils are requested to create a password when they first login. The password policy ensures that regular password changes are enforced. User applications are delivered to the desktop by the Network Ranger product based on the user's account group. Antivirus software is installed and automatically updated. The workstation's CD ROM units were disabled and BIOS password protection activated blocking unauthorised access. A restricted set of applications and learning resources were available limiting ICT use within some subject areas.

### **Recommendations**

- Improve the number and variety of resources that are available to encourage take-up across the curriculum.

### ***Wireless***

Wireless systems inherently pose a significant security risk and can impact negatively on network performance unless guidelines are followed. The current configuration offers very poor security. The WAP SSID's are broadcast and encryption systems are not enforced. The wireless access points are connected to the core network for server and Internet access rather than using a VLAN or DMZ. Wireless systems are used to extend the network across the school. Unfortunately the reliance on this solution makes it difficult to embed media rich ICT resources across the curriculum. The Ukerna recommendation is that a maximum of eight stations per wireless access point should be configured. With 802.11g the practical maximum bandwidth is 11M. With eight stations connected each station has 1M or less available bandwidth since wireless broadcasts and management data consume approx 10%. Adding a WAP to a switch network is equivalent to adding a hub to an individual switch port.

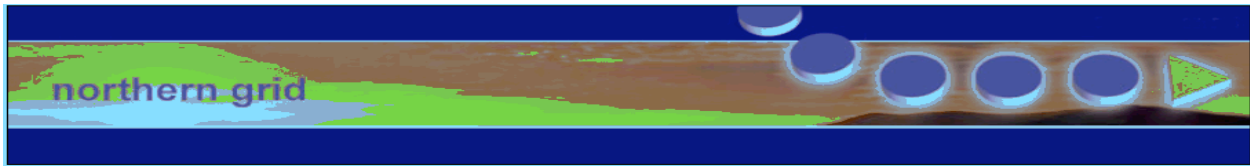
### **Recommendations**

- SSID names given should not be associated with the school.
- The SSID should not be broadcast.
- WPA encryption should be used and consideration given to using a RADIUS authentication server.
- The physical network infrastructure should be extended to provide uniform performance for all clients. Any wireless connectivity should be used sparingly to compliment a school wide physical network
- Restrict wireless clusters to eight stations per WAP

(BECTA Functional Specification 1.2.3, 2.2.2, 2.2.5, 2.2.6 and 3.4.2)

### ***1.4.5 Vulnerability Scan Results***

All servers were running services that weren't required. These services pose a potential security risk and wherever possible should be disabled.



The mail server (10.132.52.13) SNMP community string can be guessed providing useful information for any potential attacker.

Alpha server (10.132.52.11) has weak encryption as it accepts SSL 2 connections. IIS6 is not fully patched

SQL server (10.132.52.18) is running telnet. Using telnet is not recommended as logins, passwords and commands will be transferred in clear text. This server remote host is vulnerable to a "heap overflow". This problem is critical and urgently requires patching.

Web server (10.132.53.212) the FTP server can be forced to connect to third parties hosts by using the PORT command. Upgrade or change FTP server. Anonymous account active, disable if not required. OpenSSL is older than 0.9.7db leaving it susceptible to a Denial of Service attack. Upgrade current version. It may be possible using root and anonymous accounts to attack the server, as they have no passwords set. VNC server installed, if not required remove. SNMP community string can be guessed, change or disable.

### **Recommendations**

- Disable SNMP if not used. If you do use supply a community string that cannot be guessed.
- Disable SSL 2 and use SSL 3 whenever possible.
- Install all OS and server application security patches.
- Ensure all application accounts are password protected.

## **1.5 NETWORK PERFORMANCE**

Switched networks are susceptible to broadcast storms and packet corruption. The operating system Windows XP is not particularly noisy so the amount of broadcast traffic on the network should be low. Packet corruption occurs commonly as devices develop intermittent faults or as a consequence of malicious software being present on the network. By using SNMP and Switch management software these symptoms can be clearly seen and the cause quickly identified facilitating rapid resolution. As no visibility is available intermittent faulty devices or malicious software on unprotected or unauthorised stations can go unnoticed for long periods of time impacting on multiple workstation performance.

The ISP provider runs Packateer on the WAN connection to monitor the response time of web activity. They have confirmed that no problems have been encountered in recent months. The LES10 circuit has low utilisation never exceeding 30%.

### **Recommendations**

- Activate switch management software and SNMP or alternatively use a basic protocol analyser i.e. Netmon to monitor irregular traffic or packet sizes on the network when network under load.

- Discuss with your ISP to perform close monitoring of WAN traffic patterns during light and heavy loading periods and request to see the results. The Packateer monitoring software will be able to identify any noticeable change in response times.

(BECTA Technical Specification 4.2.1 and 4.2.2)

## 1.6 TOPOLOGY AUDIT

The edge switches comprise the 3Com 4400 they are an affordable, intelligent 10/100M and are fully manageable. The 4400 are a suitable cost effective solution allowing 100Mb desktop connectivity with potential dual Gigabit uplinks. The edge switches currently have 1Gb uplinks to the aggregation layer, which utilises a 3Com 4900 12-port distribution switch. Although this switch is discontinued it has proved to be reliable its major weakness are its lack of 1Gb and 10Gb ports. WAN connectivity is achieved by using a LES10 circuit terminating at a 155Mb ATM network. The ISP protects the school network through the use of a Juniper Netscreen firewall that provides transit to the National Educational Network and Internet.

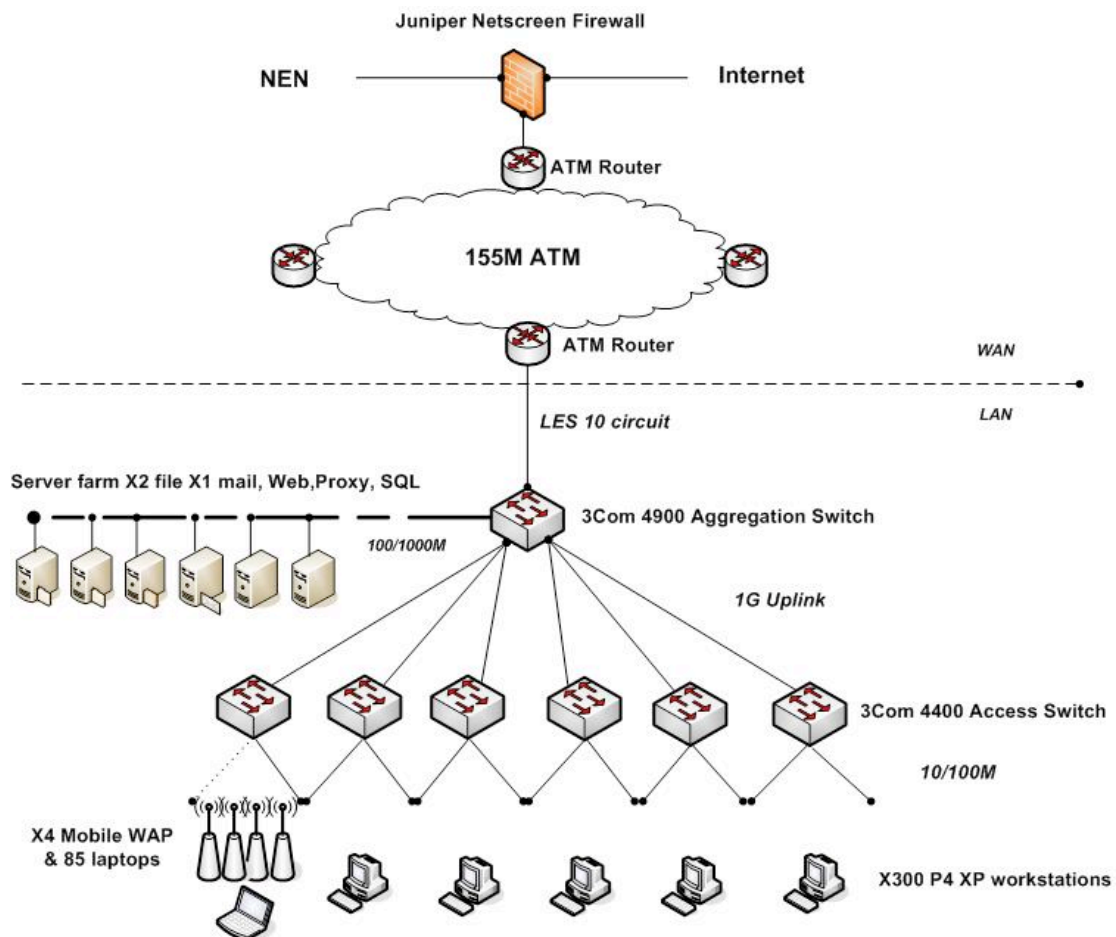
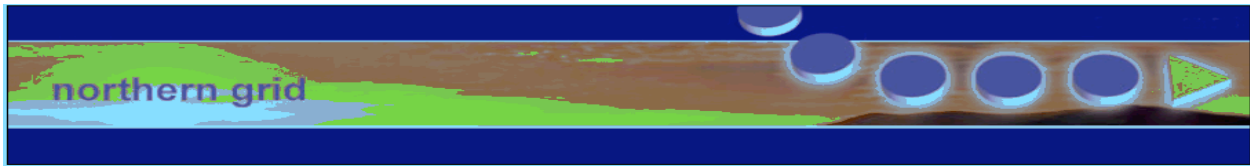


Fig 1 School Network



## **Recommendations**

- It is unlikely that this infrastructure working to specification would create a traffic bottleneck and impair user experience. The exception would be when wireless hubs are connected.
- The LES10 connection to the ATM may not meet your future needs. An evaluation and monitoring of the traffic from LAN to WAN is advised before considering upgrading this LES circuit. Your ISP provider can provide this monitoring service, as the software is already in place.
- Duplex mismatching between the switches is unlikely. The switches are all from the same vendor however mismatched connections between workstations and the edge switches and server to aggregation switch are not uncommon.
- The 3Com 4400 and 4900 switches allow link aggregation. The current Gigabit backbone could be effectively doubled as two Gigabyte modules can be combined to provide edge to distribution uplinks.
- The 4900 switch should be replaced or combined with another 3Com aggregation switch offering more Gigabit ports (over provision) that also offers a level of redundancy.

(BECTA Technical Specification 4.2.2 and 4.2.3)

## **1.7 SERVICES**

### ***1.7.1 Email***

The RM Easymail product is used for staff email. Currently no dedicated email provision is available for pupils. The email service has antivirus software installed; this correctly blocked the sending of an exe file attachment. The content of the email was not scanned for inappropriate language as required by the DfES/BECTA. No banned wordlist was in operation making the current service unsuitable for school use.

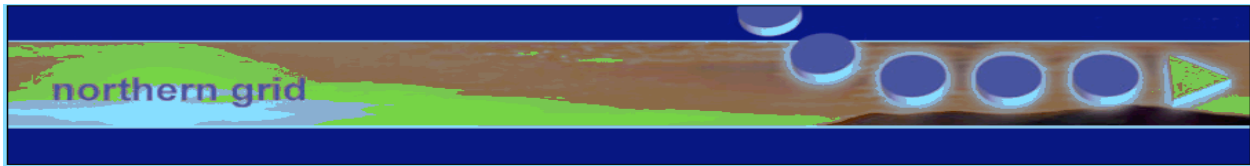
## **Recommendations**

- Setup a school wide email service that both staff and pupils can use.
- This email service requires antivirus, anti spamming software and requires the adoption of a banned wordlist to restrict inappropriate language.

(BECTA Functional Specification 1.2.5)

### ***1.7.2 URL Filtering***

The filtering system has three levels. At the top level the ISP applies the Internet Watch Foundation list of illegal web sites twice daily. At the WAN level RM Safetynet categories are applied universally. At the school level banned websites are added manually using the Freedom2teach proxy-filtering server.



The school filtering is only applied to pupil accounts. Despite the multiple layers of filtering a standard pupil account is able to access websites with well-known violent, illegal software, game and inappropriate content. Proxy services can be used to circumvent the most powerful filtering services the Google translator can be inappropriately used check out the article <http://www.oreillynet.com/pub/h/4807>

All but one of the social networking sites was accessible. Educating the pupils and staff to the risks is important. A policy for your school is therefore necessary if these sites are continued to be allowed.

***NB These sites were accessed with the knowledge and approval of the school as part of the security checks in the presence of the Network Manager.***

The CEOP website <http://www.thinkuknow.co.uk/fun/social.aspx> and the presentation “Good Practise for Child Safety” Home Office Project Group available from the URL [http://www.northerngrid.org/ngflwebsite/netassess/social\\_networking.pdf](http://www.northerngrid.org/ngflwebsite/netassess/social_networking.pdf) are good sources of useful information.

### **Recommendations**

- The school should replace Freedom2teach filtering system with a solution that has passed the ISP accreditation. BECTA is currently accrediting a number of solutions that provide content delivery, caching and filtering using internal and external databases.
- Block Google translator if not used.

(BECTA Functional Specification 4.2.1)

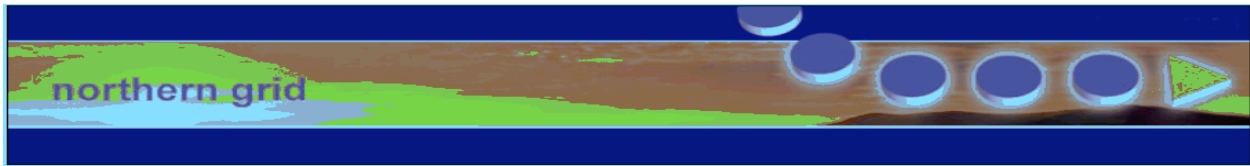
### ***1.7.3 NEN resources***

All schools within a RBC should be able to access central NEN resources the most popular are British Pathe News and Audio Networks. The school is able to access the news archive of British Pathe News however it is not able to access the music store of Audio Networks. On investigation I was informed by the schools ISP that North West Learning Grid currently provides your NEN connection and they are have some serious routing issues and are investigating.

### **Recommendations**

- Audio Networks <http://audio.lgfl.org.uk/> is an excellent popular music resource and is available to your school free of charge as a consequence of multiple RBC purchase.
- Contact your local RBC and your ISP to resolve the NEN routing issue.

(BECTA Functional Specification 1.2.3)



#### ***1.7.4 Caching***

The Freedom2teach server has a transparent and pre-caching capability I did not see any evidence that the pre-caching was used. More sophisticated caching systems can mirror content that would allow classes to connect locally for content rather than across the Internet. The advanced forms of caching improve network reliability and minimises Internet access improving the user's web browsing experience.

#### **Recommendations**

- BECTA is currently accrediting a number of solutions that provide content delivery, advanced caching, and filtering using internal and external databases. Evaluate the recommended systems as replacement for Freedom2teach unit.

(BECTA Functional Specification 4.2.1)

#### ***1.7.5 Secure Remote Access***

Staff are able securely access their network files using the Ranger Outpost solution. Users can exchange files in both directions between their network home area and their local workstation. The remote access program does not provide a physical connection and is therefore secure.

#### **Recommendations**

- Extend the take up of this remote service to include pupils.
- The school needs to decide the granularity of access made available to different groups of individuals from remote locations. Limitation of the Ranger Outpost solution may require looking at alternative secure VPN solutions i.e. Citrix SSL

(BECTA Functional Specification 2.2.3)

#### ***1.7.6 Backup and Disaster Recovery***

Never keep a tape in active rotation for more than a year or 35 uses, AIT-2 Sony drives offer high capacity allied with high speed. They are less reliable than DLT due to the helical scan techniques used. The documented backup policy should stipulate the backup policy in operation, how often tapes are replaced and by whom, any error messages need to be documented and investigated. After each backup a record of the transactions needs to be made in a logbook. The backup plan requires regular full or partial recovery of data to ensure that data is reliably being backed up.

No disaster recovery plan has been devised, it is unlikely that all data is recoverable should a major incident occur. Substantial funding for Learning Platforms has been made available by the DfES over the next couple of years.

These platforms will offer pupils and staff data storage areas that will be available 24/7 across the Internet. These platforms installed at RBC or LA level will require secure and reliable data backup and disaster recovery solutions. It is likely that an integrated email and messaging system will also be included.

### **Recommendations**

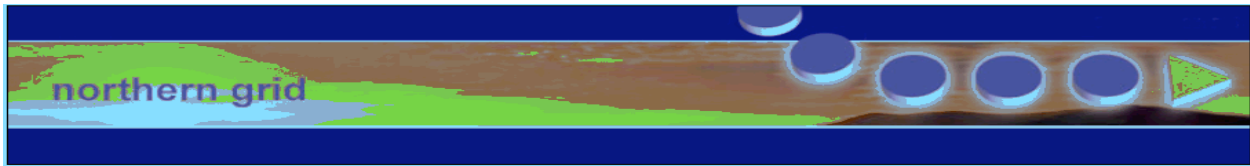
- Recommend full backups carried out every 4 weeks and incremental backups daily during workdays.
- Keep full backups for at least 12 months.
- Log each tape use and replace after 35 uses. Carry out partial or full tape backup restore every 6 months onto spare server.
- Investigate LTO tape backup technology for future use.
- Discuss with LA and RBC future learning platform plans. BECTA have devised a set of requirements this should be the basis of the future Learning Platform for your region.
- The Active Directory database is not currently part of the backup solution add AD to your backup policy.

#### ***1.7.7 Future Scalability***

Reduction in reliance of the wireless network is a high priority. The 3Com 4900 switch port availability is low give consideration to a replacement switch. The school's storage requirements are likely to exceed current capacity within the next 1-2 years consider the deployment of SAN solution. Investigate single points of failure on the network and have some strategy for resolving core equipment failure. Consider technical support agreement or purchase spare equipment.

### **Recommendations**

- Extend physical network to cover majority of school.
- Replace 3Com 4900 aggregation switch
- Deploy iSCSI SAN storage solution
- Ensure single point of failure equipment can be repaired or replaced within 4 hours



## **1.8 RESOURCES**

BECTA Functional and Technical Specification

[http://schools.becta.org.uk/downloads/functional\\_spec\\_institutional\\_infrastructure.doc](http://schools.becta.org.uk/downloads/functional_spec_institutional_infrastructure.doc)

[http://schools.becta.org.uk/downloads/techspec\\_institutional\\_infrastructure.doc](http://schools.becta.org.uk/downloads/techspec_institutional_infrastructure.doc)

BECTA ISP accreditation

[http://ispsafety.ngfl.gov.uk/matrix\\_home.php](http://ispsafety.ngfl.gov.uk/matrix_home.php)

Child Exploitation and Online Protection

<http://www.thinkuknow.co.uk/>

Internet Watch Foundation

<http://www.iwf.org.uk/>

Northern Grid ESafety

[http://www.portal.northerngrid.org/ngflportal/custom/files\\_uploaded/uploaded\\_resources/1924/September\\_e\\_safety\\_newsletter.pdf](http://www.portal.northerngrid.org/ngflportal/custom/files_uploaded/uploaded_resources/1924/September_e_safety_newsletter.pdf)

Northern Grid Acceptable User Policy

<http://www.northerngrid.org/ngflwebsite/xxx/NortherngridAUP.doc>